

Intune & Knox Platform for Enterprise

Apr 2021
Samsung R&D Centre UK
(SRUK)

1. Pre-requisites for Knox Platform for Enterprise
2. Configure Android Enterprise
3. Android Enterprise Deployment Modes
 - Work Profile
 - Fully Managed Device
 - Fully Managed Device with a Work Profile/Work Profile on Company Owned Device
 - Dedicated Device
4. Configure Knox Service Plugin [KSP]
5. Configure Knox Platform for Enterprise

Contacts:

sruk.rtam@samsung.com

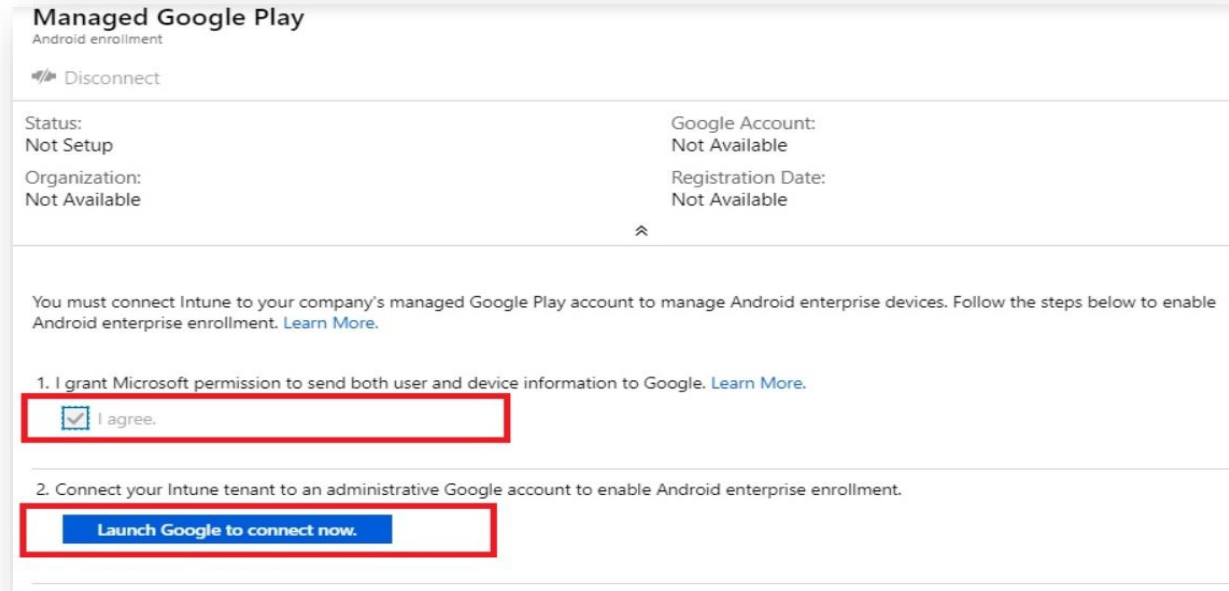
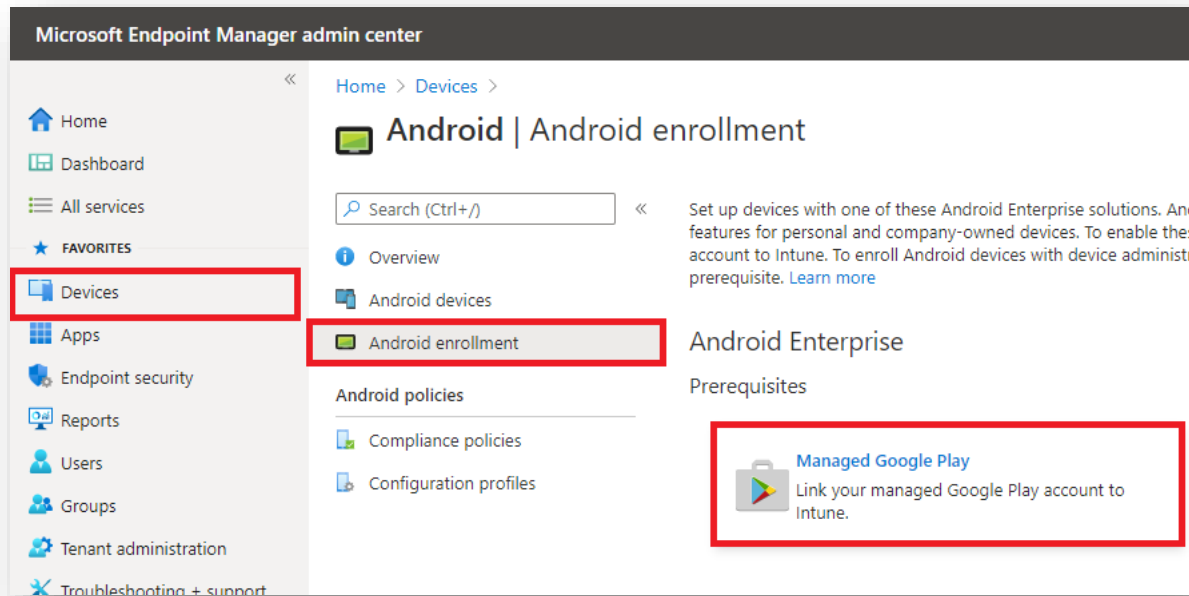
Knowledge Base:

<https://docs.microsoft.com/en-us/mem/intune/>

1. Obtain access to Microsoft Endpoint Manager - Endpoint Manager is the new home for Microsoft Intune. The Intune link within Azure is no longer accessible and Administrators should access the console by using the link: <https://endpoint.microsoft.com>
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

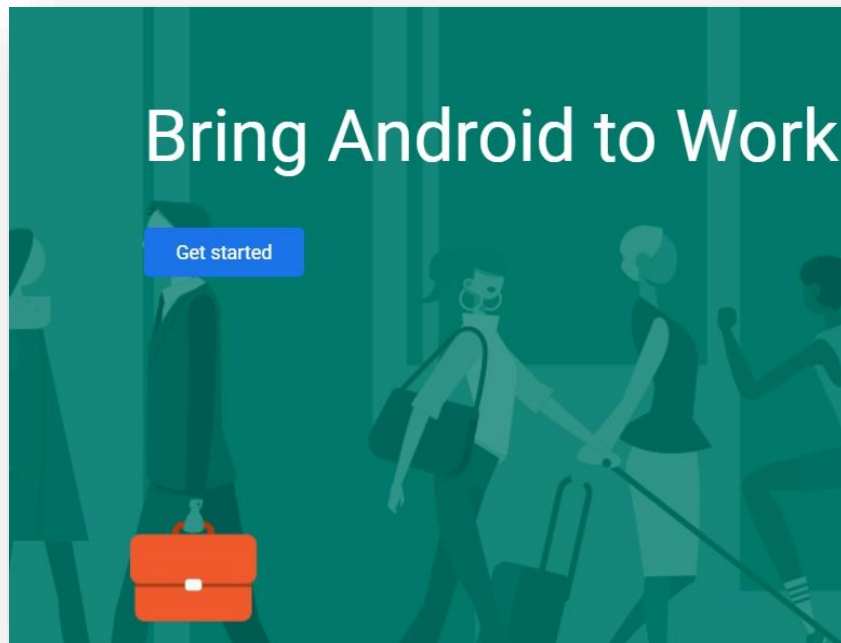
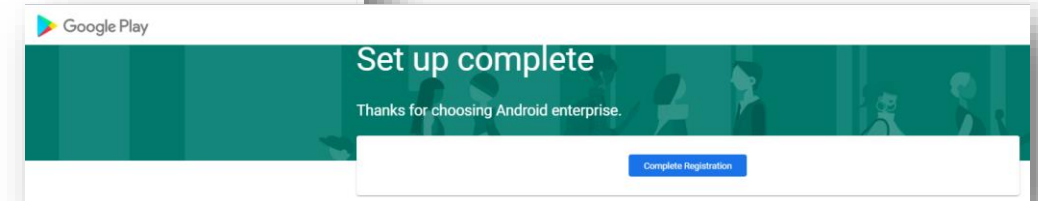
Configure Android Enterprise

- Within Microsoft Endpoint Manager, navigate to: Devices > Android > Android enrollment
- Select Managed Google Play
- Tick I agree and click Launch Google to connect now



Configure Android Enterprise

- Sign into your Google account and select Get Started
- Fill out the Contact details page, tick the Managed Google Play agreement page and then select Confirm. These text fields are not mandatory, so you can alternatively leave them blank and just tick the Managed Google Play agreement and then select Confirm
- Click Complete Registration to complete the Android Enterprise configuration and return to Microsoft Endpoint Manager

A Google Play "Contact details" form. The header is teal with the Google Play logo. Below the header, it says "Contact details" and "We need some details about your key contacts". A paragraph of text explains that contact details are required for data protection regulations. Below this, there are two sections: "Data Protection Officer" and "EU Representative". Each section has three input fields: "Name", "Email", and "Phone". At the bottom, there is a checkbox labeled "I have read and agree to the Managed Google Play agreement." and a "Confirm" button.

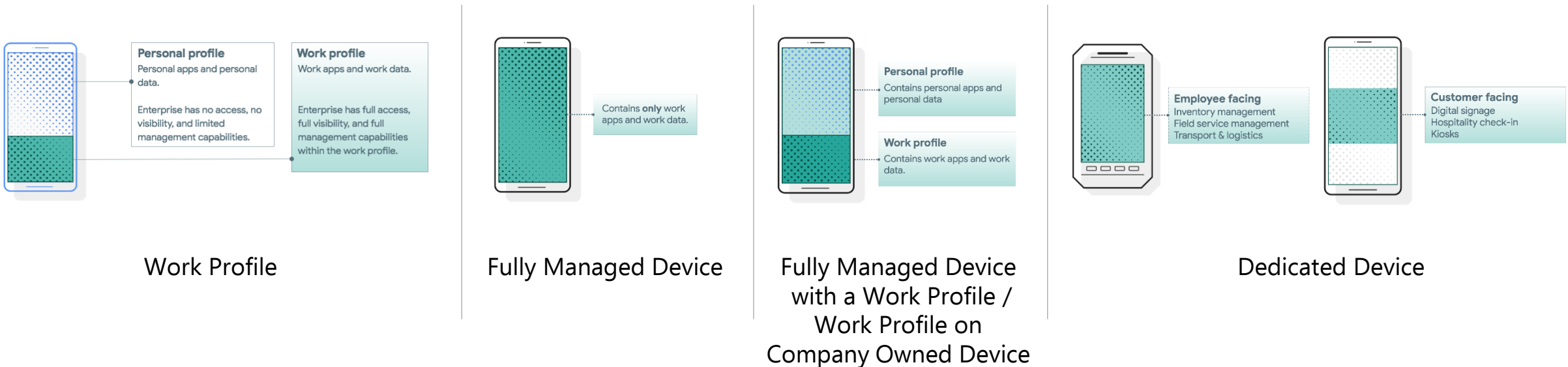
Android Enterprise Deployment Modes

Deployment Modes

Android Enterprise can be deployed in the following 4 deployment modes

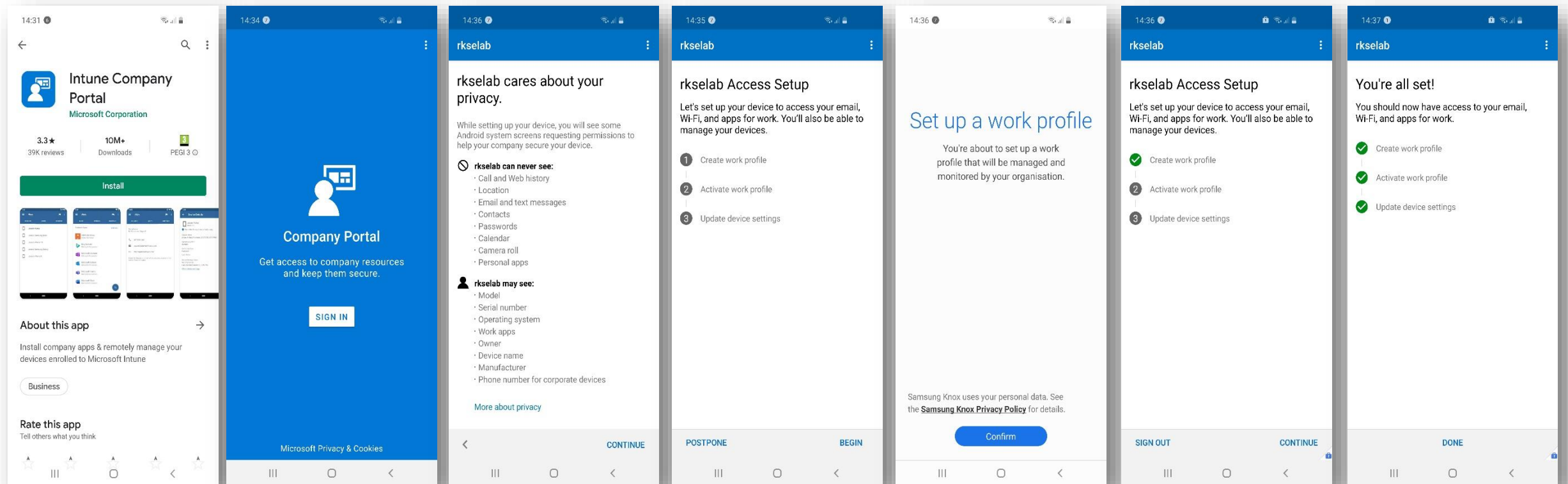
1. Work Profile [*formerly known as Profile Owner or PO*]
2. Fully Managed Device [*formerly known as Device Owner or DO*]
3. Fully Managed Device with a Work Profile [*formerly known as Company Owned Managed Profile or COMP*], now on Android 11 or later, known as Work Profile on Company Owned Device or WPC
4. Dedicated device [*formerly known as COSU*]

Intune can support all 4 of these deployment modes. In this next section we will show you how to configure each of these 4 deployment modes in Intune for your device fleet.



Android Enterprise: Work Profile Enrollment

Once you link your Google account, Android Enterprise Work Profile enrollment is enabled by default. To Work Profile enroll, follow the below steps:



Install Intune Company Portal
From Google Play Store

SIGN IN

CONTINUE

BEGIN

Confirm

CONTINUE

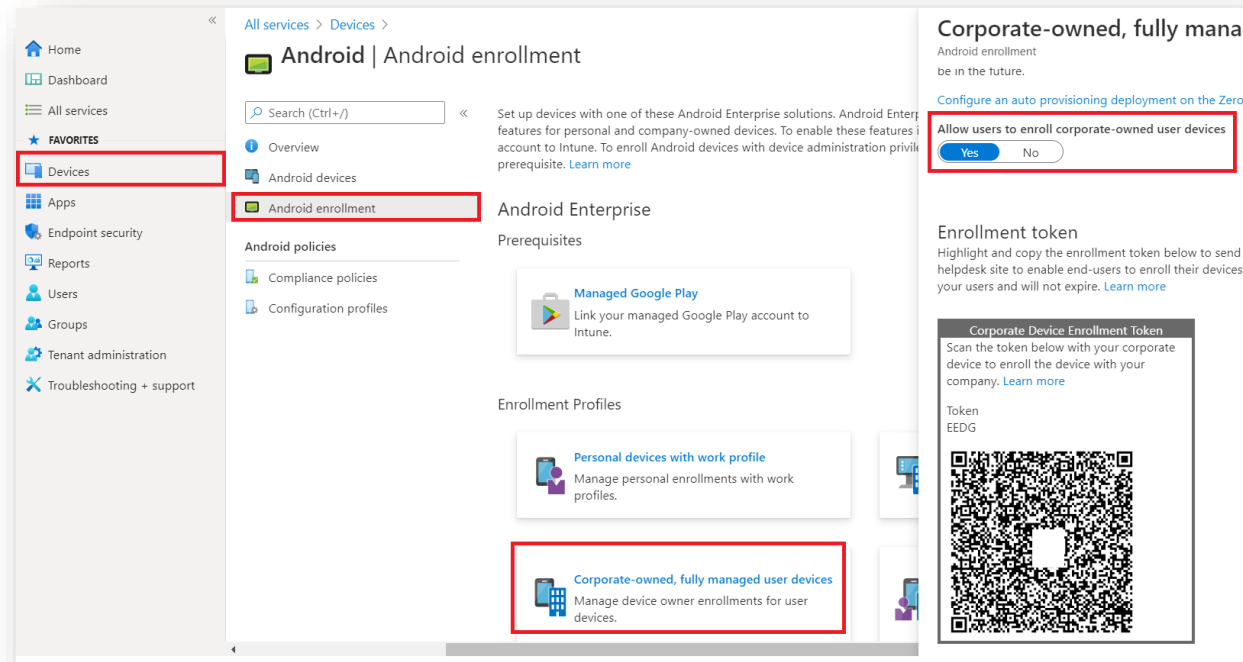
DONE

Android Enterprise: Fully Managed

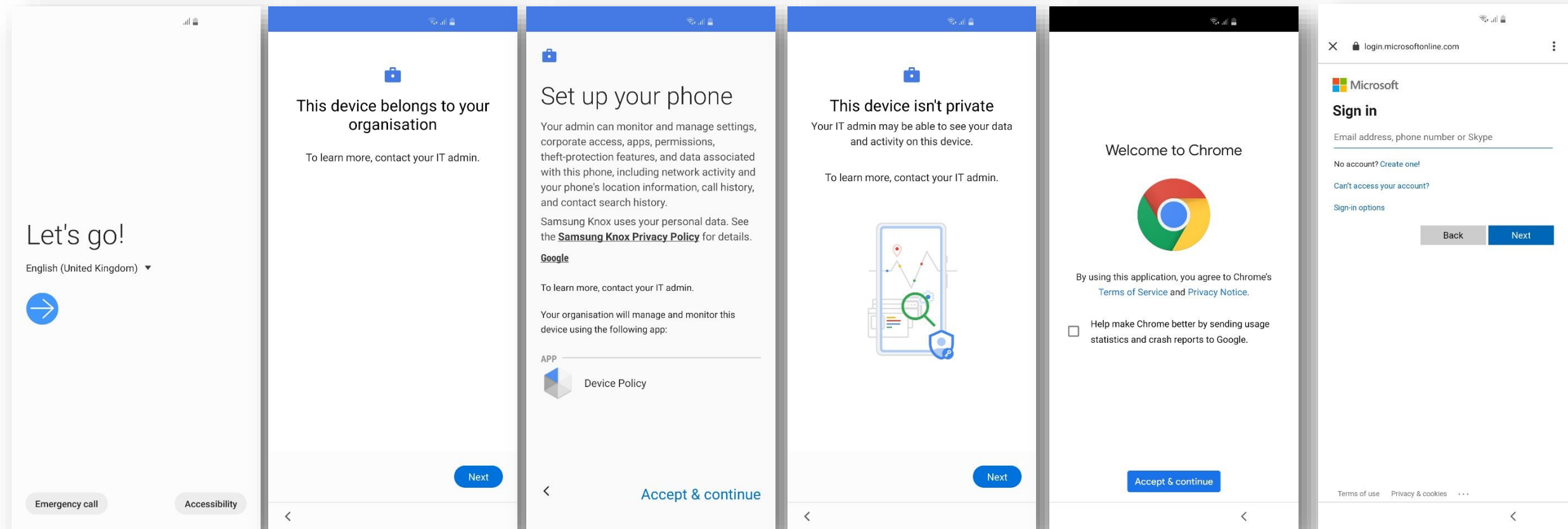
- Within Microsoft Endpoint Manager, navigate to: Devices > Android > Android enrollment
- Select Corporate-owned, fully managed user devices
- Make sure Allow users to enroll corporate-owned user devices is set to Yes
- If you're using KME, you can use the Token to simplify the enrollment steps and force the user to enroll into your tenant. Copy and Paste the below JSON code into Custom JSON Data field in your KME Profile, changing YOUR TOKEN to the Token displayed in your Corporate Device Enrollment Token.

```
{"com.google.android.apps.work.clouddpc.EXTRA_ENROLLMENT_TOKEN":"YOUR TOKEN"}
```

- If you're not using KME you should provide the QR code shown under Enrollment token to your end users. You will need to print screen this or copy the image and email it to your end users. The QR code should then be scanned on the initial setup screen which is explained in the next slide.



Android Enterprise: Fully Managed Enrollment



Tap anywhere on the screen 7 times and scan the enrollment QR code

Next

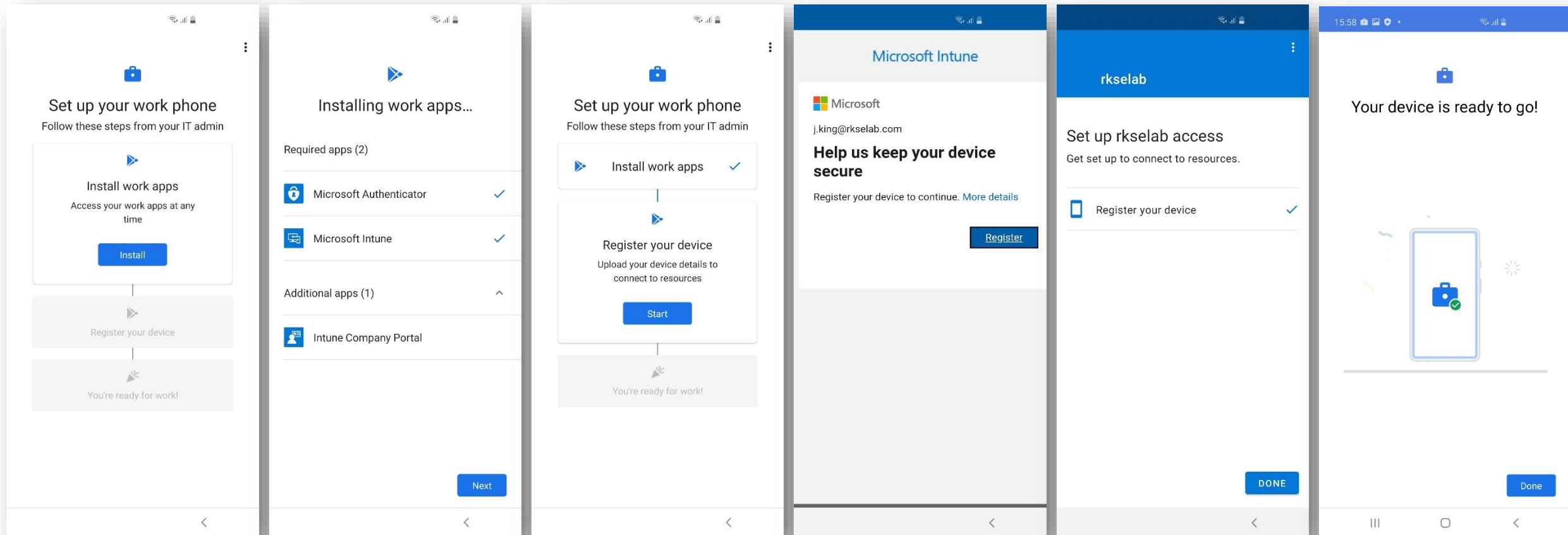
Accept & continue

Next

Accept & continue

Sign in with your Office 365 account

Android Enterprise: Fully Managed Enrollment



Install

Next

Start
or
Set Up

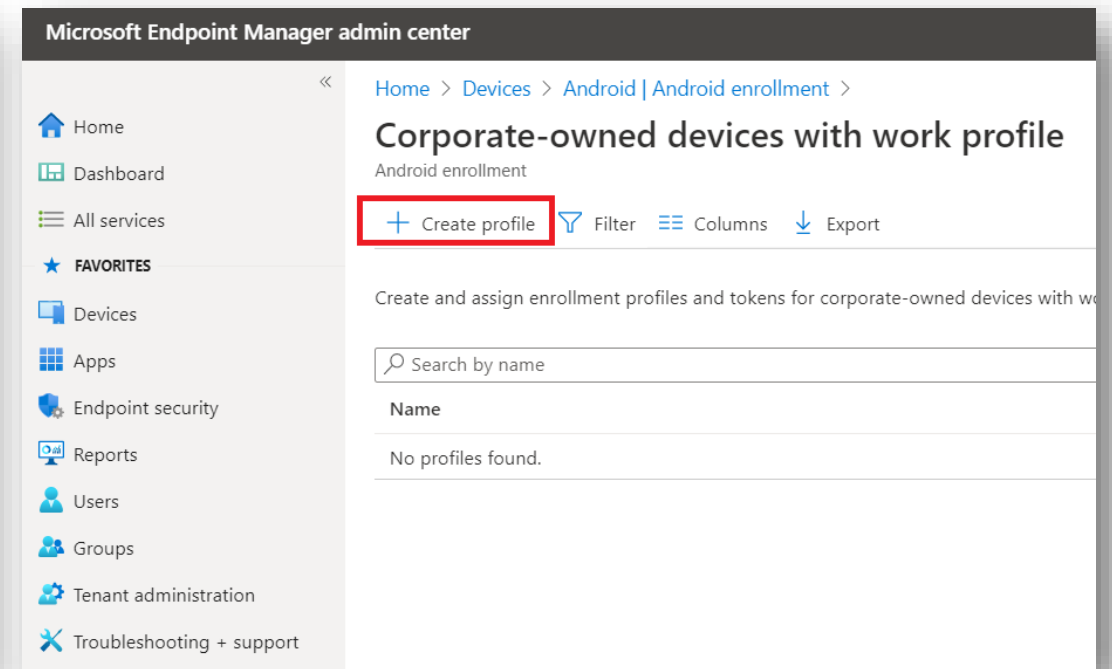
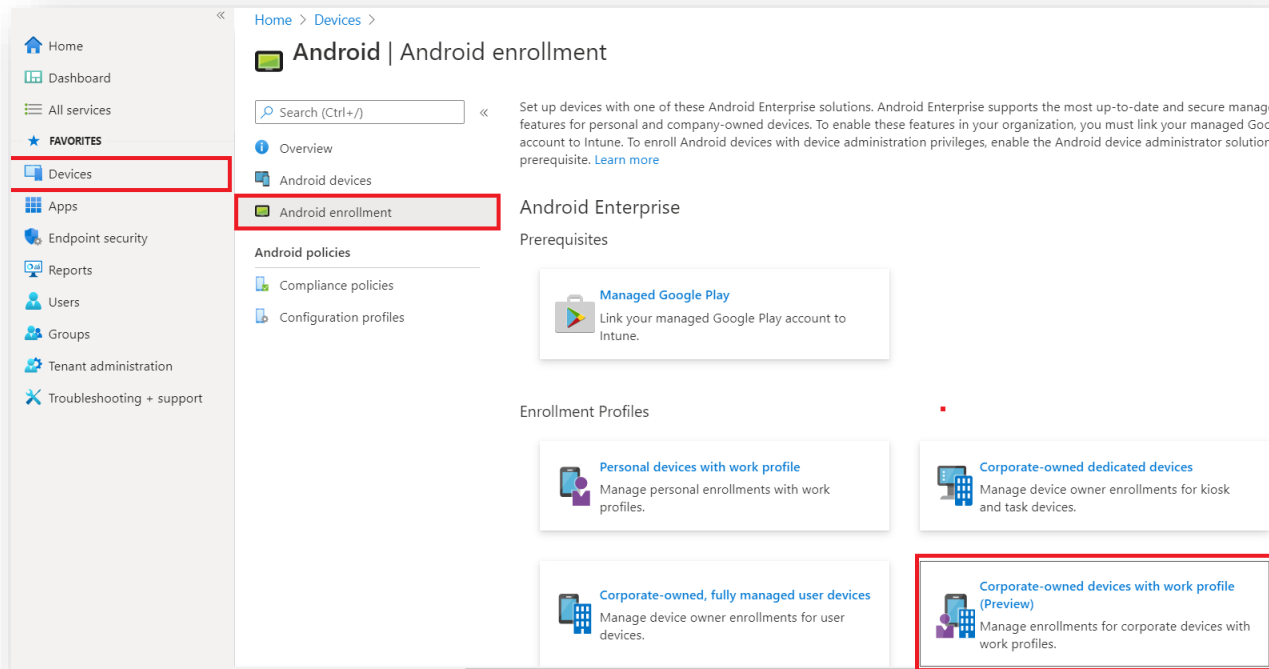
Register

DONE

Done

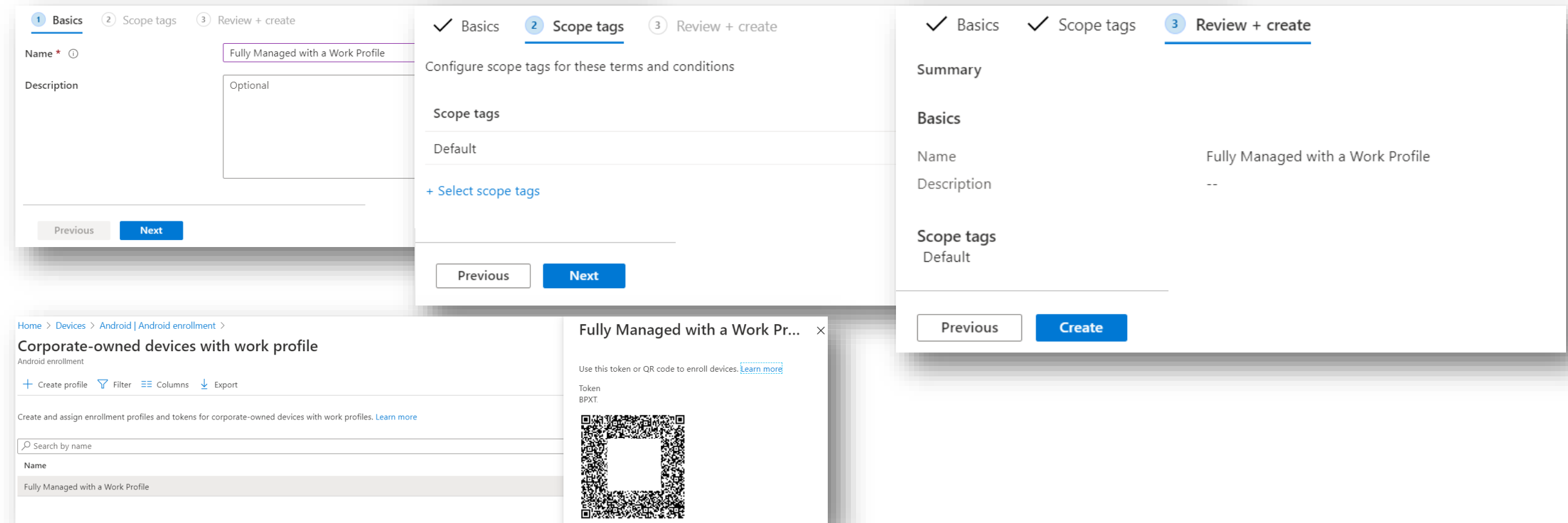
Android Enterprise: Fully Managed with a Work Profile (COMP or WPC)

- Within the Microsoft Endpoint Manager console, navigate to: Devices > Android > Android enrollment
- Select Corporate-owned devices with work profile (Preview)
- Select Create profile



Android Enterprise: Fully Managed with a Work Profile (COMP or WPC)

- Enter a Name, select Next
- Select a scope tag (optional) select Next
- Select Create
- To view your Token and QR code, select your profile in the profiles list
- If you're using KME, you can use the Token to simplify the enrollment steps and force the user to enroll into your tenant. Copy and paste the below JSON code into Custom JSON Data field in your KME Profile, changing YOUR TOKEN to the Token displayed in your Corporate Device Enrollment Token.
`{"com.google.android.apps.work.clouddpc.EXTRA_ENROLLMENT_TOKEN":"YOUR TOKEN"}`
- If you're not using KME you should provide the QR code shown in your enrollment profile to your end users. You will need to print screen this or copy the image and email it to your end users. The QR code should then be scanned on the initial setup screen which is explained in the next slide.



The image displays three sequential screenshots of the Google Admin console's Android Enterprise interface, illustrating the steps to create a 'Fully Managed with a Work Profile'.

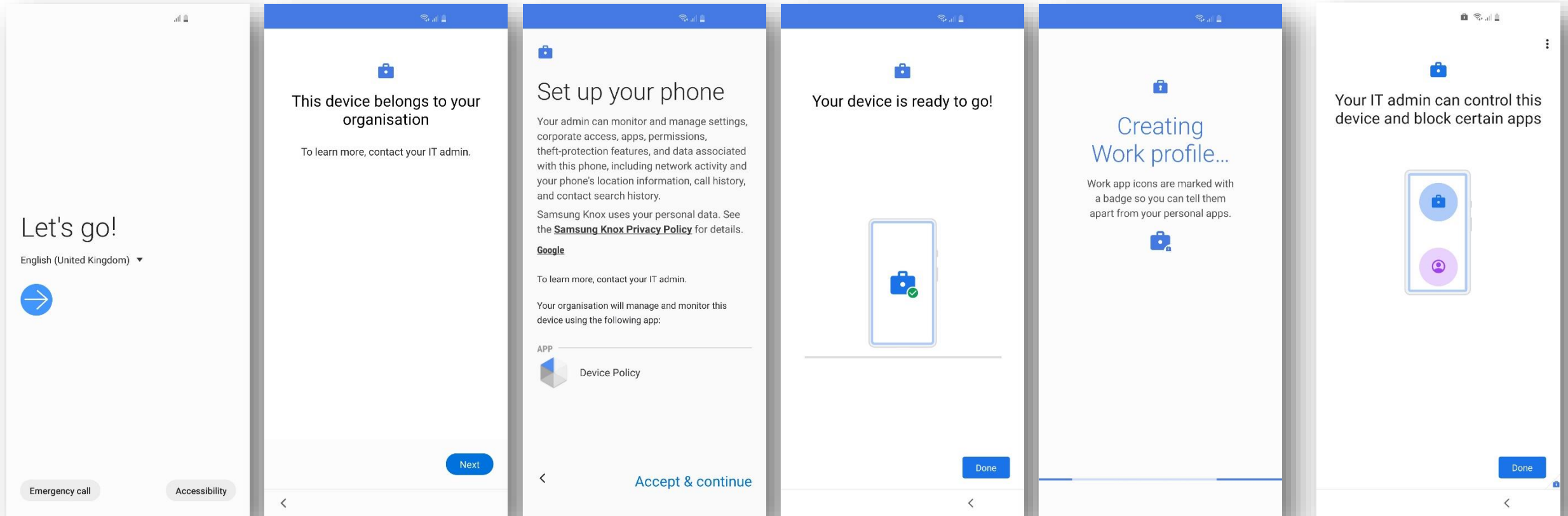
Step 1: Basics
 The first screenshot shows the 'Basics' tab selected. The 'Name' field is populated with 'Fully Managed with a Work Profile'. The 'Description' field is optional. Navigation buttons 'Previous' and 'Next' are at the bottom.

Step 2: Scope tags
 The second screenshot shows the 'Scope tags' tab. It prompts the user to 'Configure scope tags for these terms and conditions'. A 'Default' scope tag is listed. A '+ Select scope tags' link is available. Navigation buttons 'Previous' and 'Next' are at the bottom.

Step 3: Review + create
 The third screenshot shows the 'Review + create' tab. It provides a summary of the configuration: Name 'Fully Managed with a Work Profile' and Description '--'. Under 'Scope tags', 'Default' is listed. 'Previous' and 'Create' buttons are at the bottom.

Profile List and QR Code
 Below the main steps, two additional screenshots are shown. The left one is a table titled 'Corporate-owned devices with work profile' under the 'Android enrollment' section. It lists the created profile: 'Fully Managed with a Work Profile'. The right one is a modal window titled 'Fully Managed with a Work Pr...' showing the enrollment token 'BPXT.' and a QR code for device enrollment.

Android Enterprise: Fully Managed with a Work Profile Enrollment or WPC



Tap anywhere on the screen 7 times and scan the enrollment QR code

Next

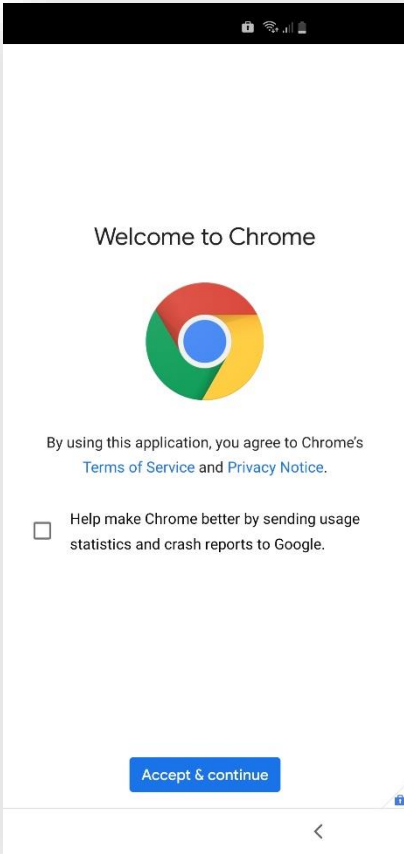
Accept & continue

Done

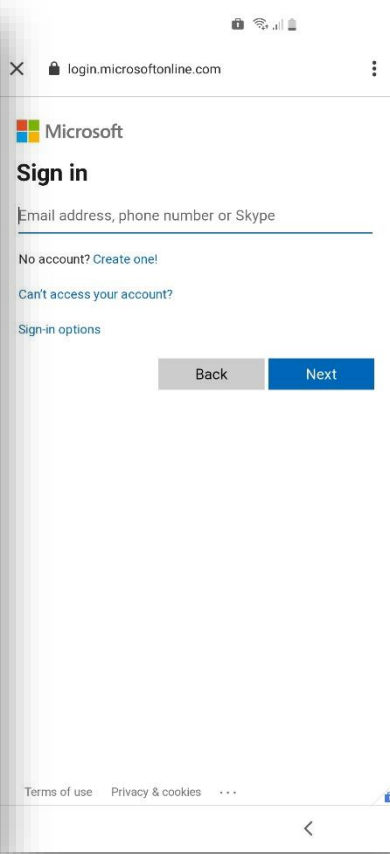
Wait

Done

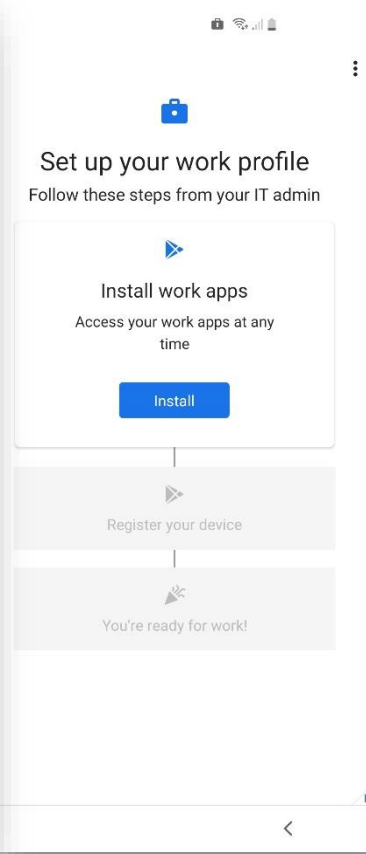
Android Enterprise: Fully Managed with a Work Profile Enrollment or WPC



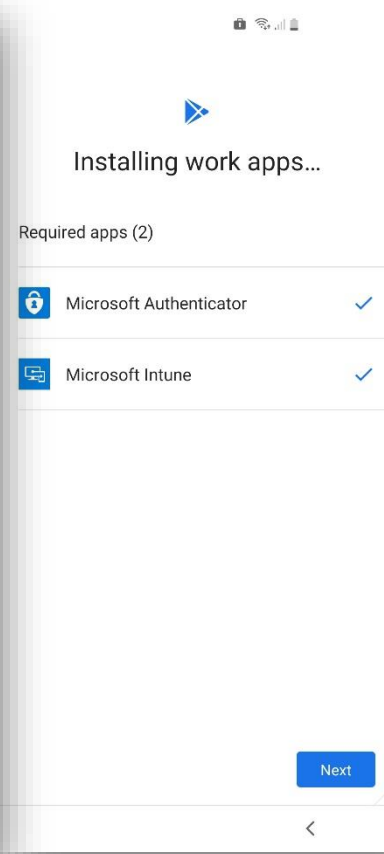
Accept & continue



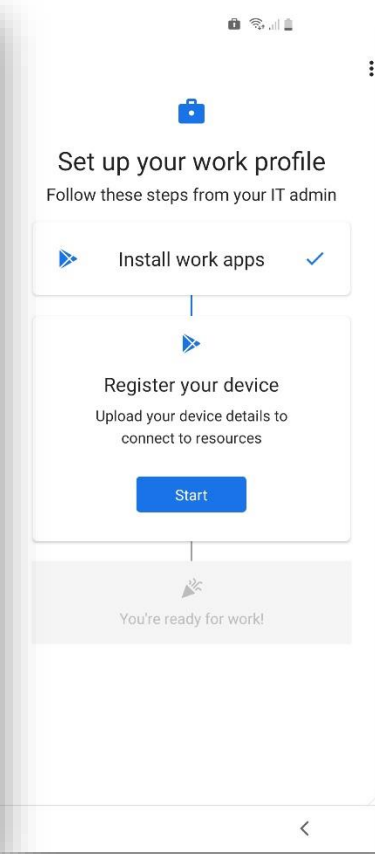
Sign into your
Office 365 account,
then select Next



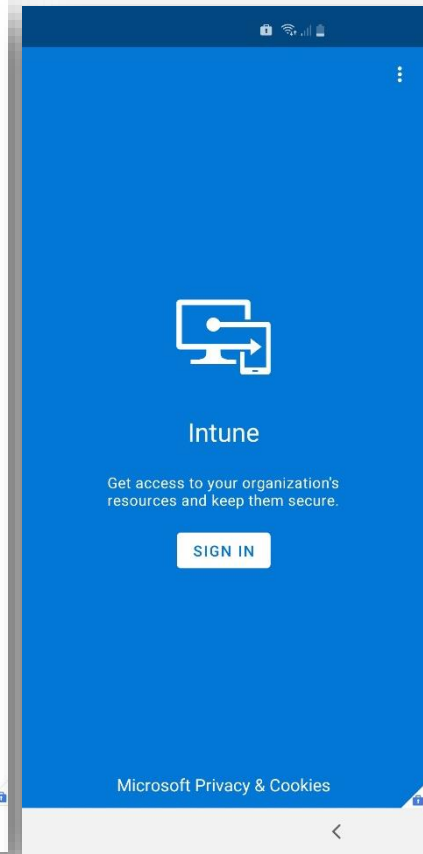
Install



Next

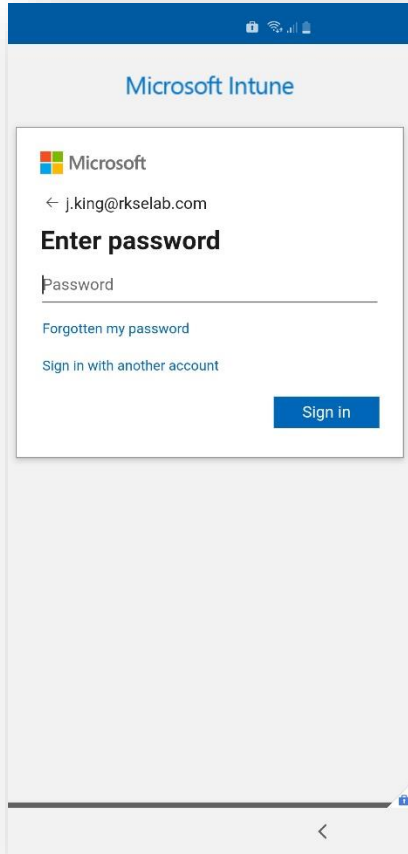


Start
or
Set Up

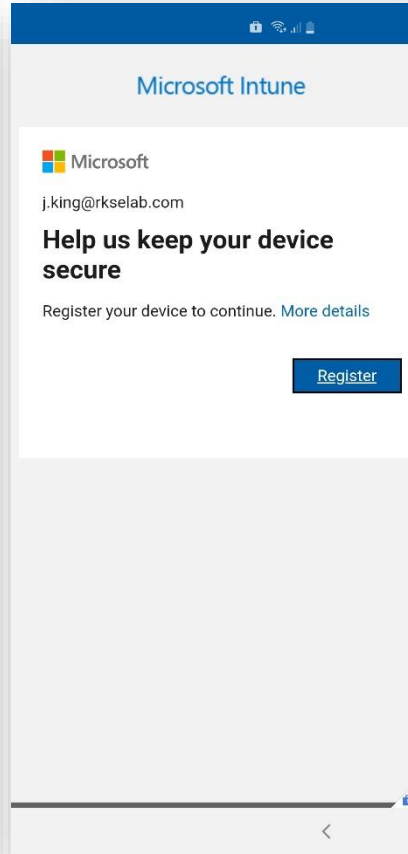


SIGN IN

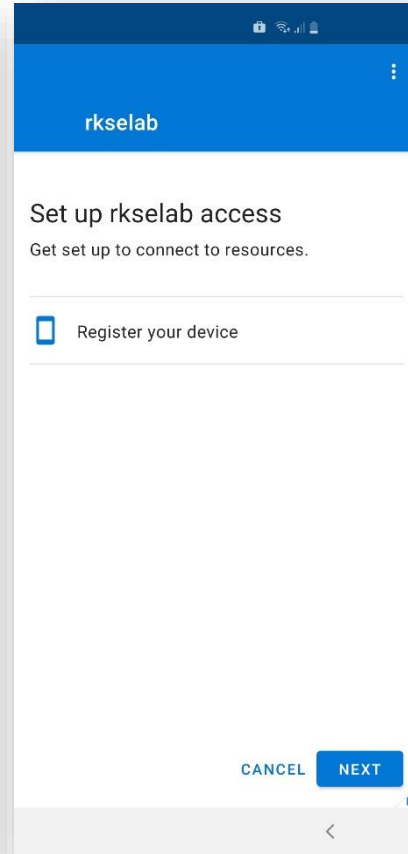
Android Enterprise: Fully Managed with a Work Profile Enrollment or WPC



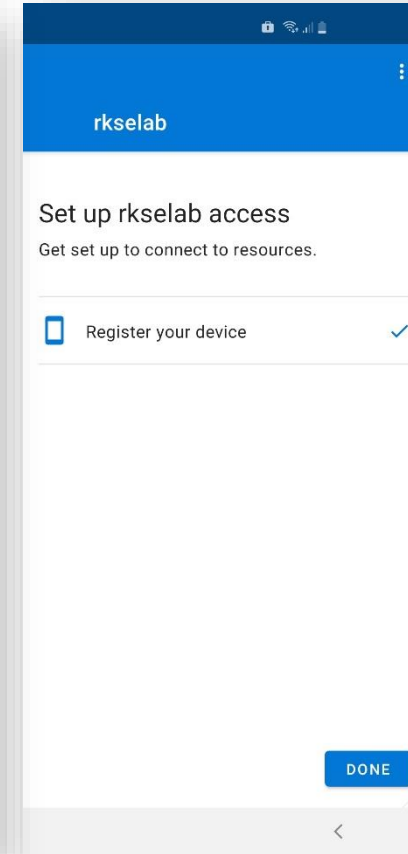
Sign in with your
Office 365 account



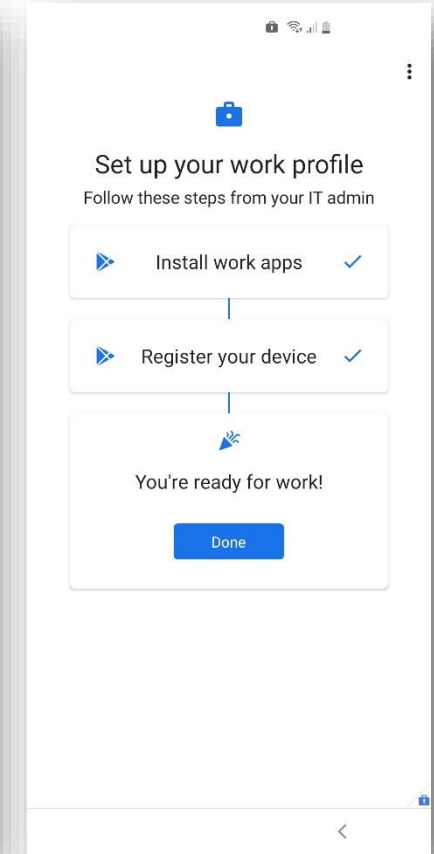
Register



NEXT



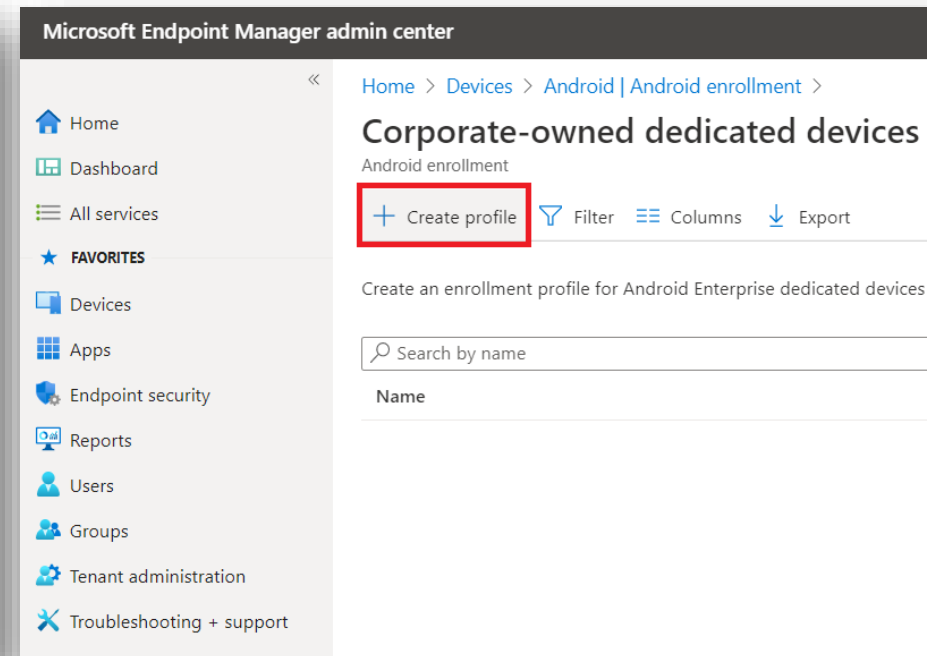
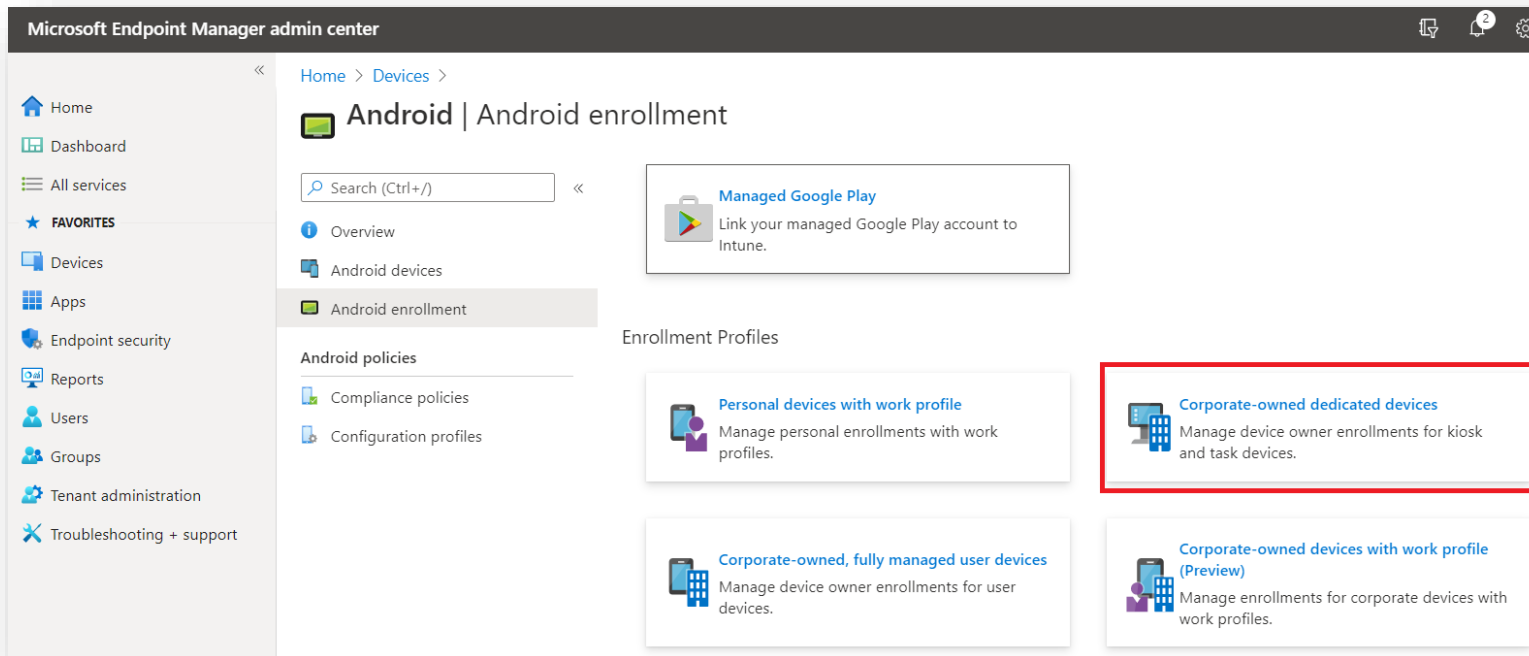
DONE



Done

Android Enterprise: Dedicated Device

- Within the Microsoft Endpoint Manager console, navigate to: Devices > Android > Android enrollment
- Select Corporate-owned dedicated devices
- Select Create profile



Android Enterprise: Dedicated Device

- Enter a Name and set a Token expiration date, then click Next
- Select a scope tag (optional) select Next
- Select Create
- To view your Token and QR code, select your profile in the profiles list
- If you're using KME, you can use the Token to simplify the enrollment steps and force the user to enroll into your tenant. Copy and paste the below JSON code into Custom JSON Data field in your KME Profile, changing YOUR TOKEN to the Token displayed in your Corporate Device Enrollment Token.
`{"com.google.android.apps.work.clouddpc.EXTRA_ENROLLMENT_TOKEN":"YOUR TOKEN"}`
- If you're not using KME you should provide the QR code shown in your enrollment profile to your end users. You will need to print screen this or copy the image and email it to your end users. The QR code should then be scanned on the initial setup screen which is explained in the next slide.

The collage illustrates the four-step process for creating a dedicated device profile:

- Step 1: Basics** - The 'Basics' tab is active. Fields include 'Name' (Kiosk Profile), 'Description' (Optional), and 'Token expiration date' (11/11/2020). 'Previous' and 'Next' buttons are at the bottom.
- Step 2: Scope tags** - The 'Scope tags' tab is active. It shows 'Configure scope tags for these terms and conditions' with a 'Default' tag and a '+ Select scope tags' link. 'Previous' and 'Next' buttons are at the bottom.
- Step 3: Review + create** - The 'Review + create' tab is active. It displays a 'Summary' section with the profile details: Name (Kiosk Profile), Description (--), and Token expiration date (11/11/20). Below this, the 'Scope tags' section shows 'Default'. 'Previous' and 'Create' buttons are at the bottom.
- Final View: Corporate-owned dedicated devices** - A table listing the created profile. The table has columns for 'Name' and 'Token expiration date'. The entry 'Kiosk Profile' is listed with an expiration date of '11/11/2020'. To the right of the table, a 'Kiosk Profile' card shows the 'Token' (HQMHE), 'Token expiration date' (11/11/20, 12:16 PM), and a QR code for enrollment.

Android Enterprise: Dedicated Device

Create an Azure Active Directory Group

- Within the Microsoft Endpoint Manager console, navigate to Groups and select New Group
- "Group type = Security" "Group name = Name of your choice" "Group description = Optional" "Membership type = Dynamic Device"
- Click Add dynamic query
- Add the following rule:
(device.enrollmentProfileName -match "Kiosk Profile")

The screenshot displays the Microsoft Endpoint Manager admin center interface. On the left, the navigation pane shows the 'Groups' section under 'All services'. The main area shows the 'Groups | All groups' page for 'rksealab - Azure Active Directory'. A red box highlights the '+ New group' button. To the right, a modal window for creating a new group is open. It shows the following configuration:

- Group type:** Security
- Group name:** Android Enterprise Kiosk Profile
- Group description:** Android Enterprise Kiosk Profile
- Membership type:** Dynamic Device
- Dynamic device members:** Add dynamic query

The 'Configure Rules' tab is active, showing a table with the following rule:

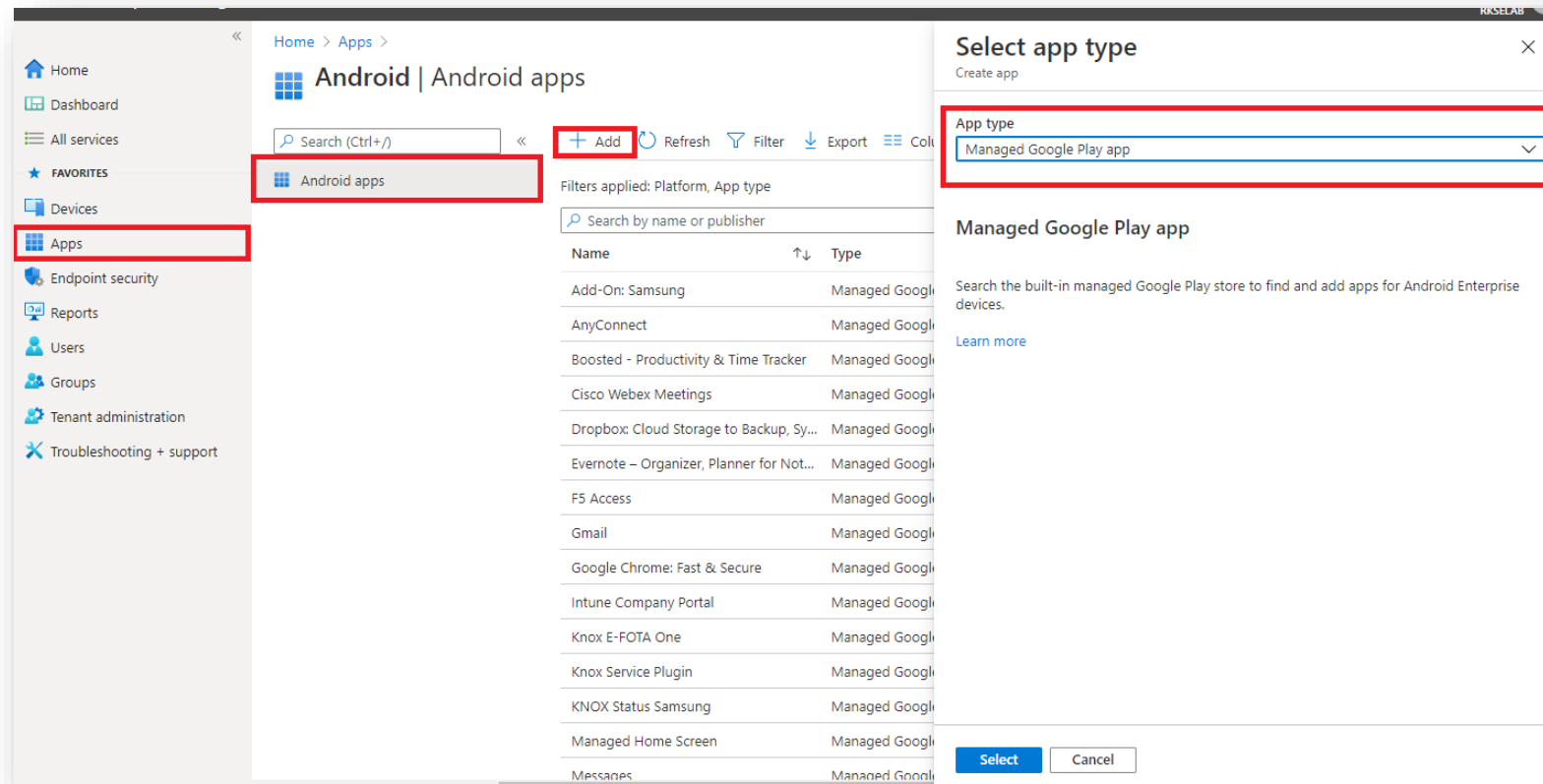
And/Or	Property	Operator	Value
	enrollmentProfileName	Match	Kiosk Profile

Below the table, the 'Rule syntax' text box contains the expression: (device.enrollmentProfileName -match "Kiosk Profile")

Android Enterprise: Dedicated Device

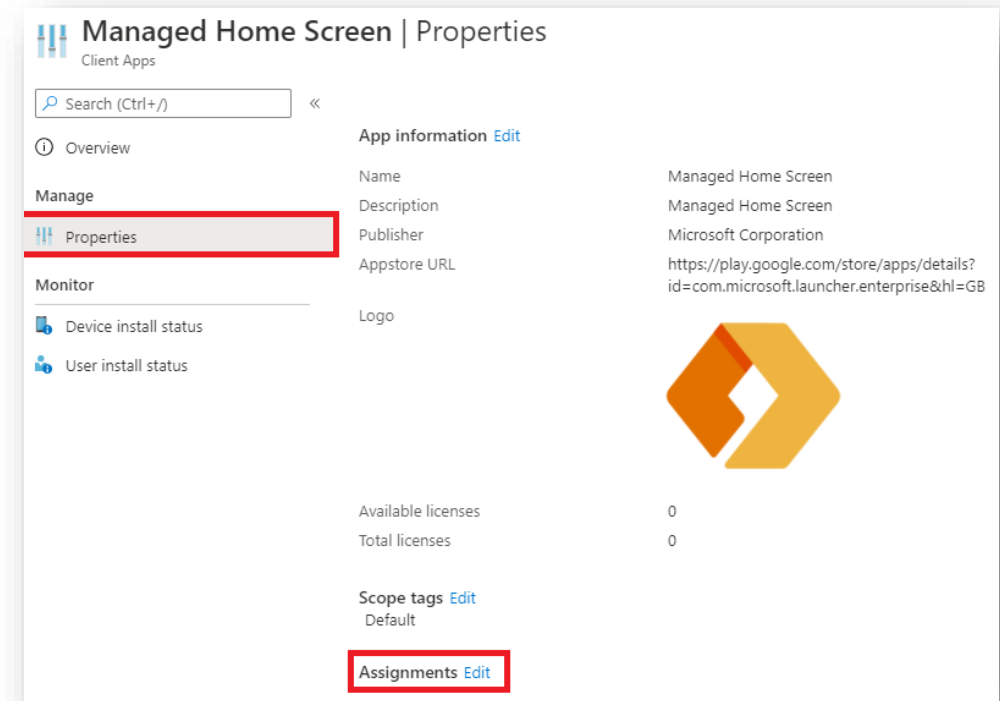
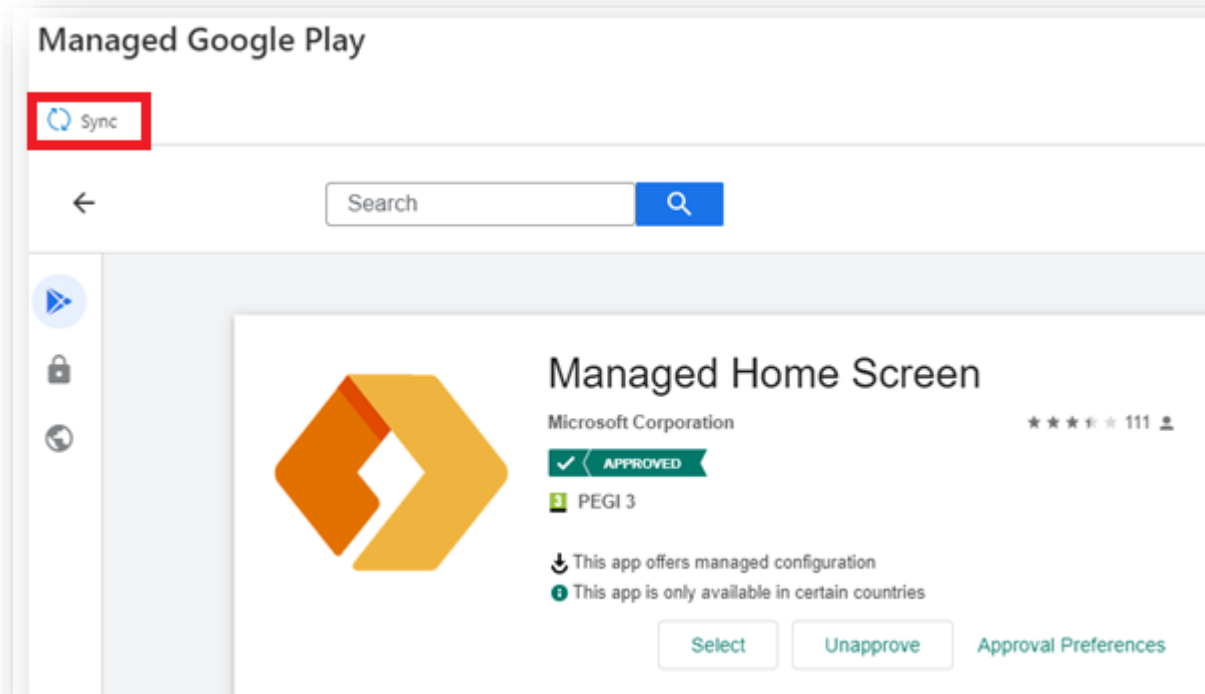
Add the Managed Home Screen

- Within Endpoint Manager, navigate to: Apps > Android apps
- Select Add
- Set the App type to: Managed Google Play app
- Click Select



Android Enterprise: Dedicated Device

- Search for the “Managed Home Screen” and approve the app.
- Press Sync to add the apps to the apps list.
- Click on the Managed Home Screen in the apps list and select Properties
- Select Edit next to Assignments



Android Enterprise: Dedicated Device

- Select Add group
- Search for and click on the Kiosk Device Group
- Click Select
- Click Review + save
- Click Save

Edit application
Managed Google Play store app

Assignments Review + save

Required ⓘ

Group mode

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

Select groups
Azure AD groups

Kiosk

KD Kiosk Device Group
Selected

Selected items

KD Kiosk Device Group Remove

Select

Edit application
Managed Google Play store app

Assignments Review + save

Required ⓘ

Group mode	Group
Included	Kiosk Device Group

+ 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	

Review + save Cancel

Edit application
Managed Google Play store app

Assignments Review + save

Summary

Assignments

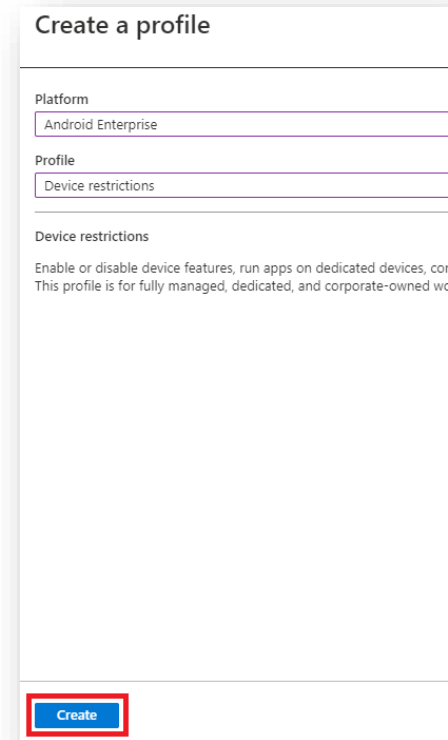
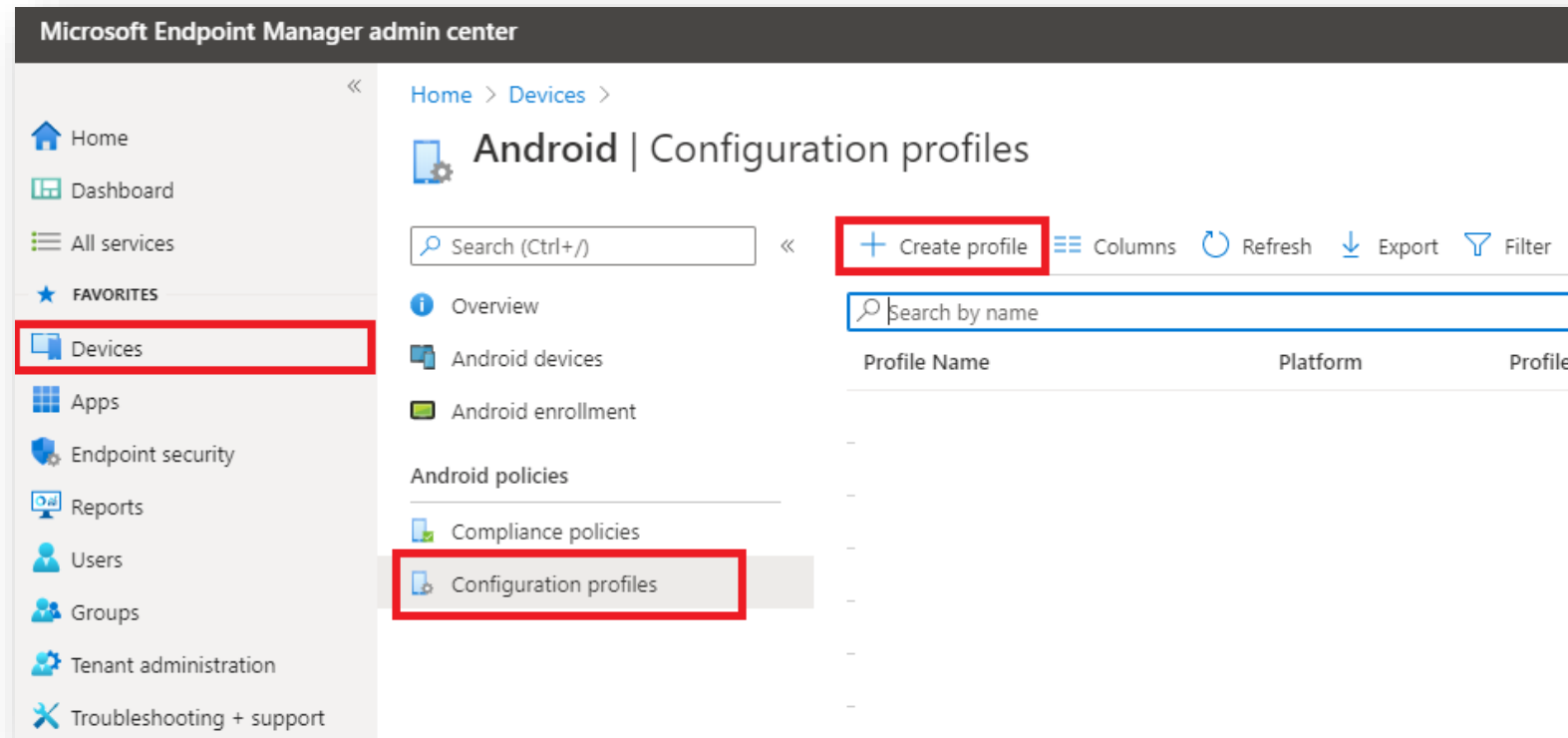
Required	Kiosk Device Group
Available for enrolled devices	--
Available with or without enrollment	--
Uninstall	--

Save Cancel

Android Enterprise: Dedicated Device

Create a Kiosk Profile

- Within Endpoint Manager, navigate to: Devices > Android
- Click Configuration profiles and then Create profile
- Set the Platform to Android Enterprise and the Profile to Device Restrictions
- Click Create



Android Enterprise: Dedicated Device

Create a Kiosk Profile

- Enter a Name and select Next
- Scroll down to Device experience
- Select Dedicated device for Enrollment profile type
- Choose whether you would like a Single or Multi-app mode
- Click Next

The screenshot shows the 'Basics' tab of the Android Enterprise console. The 'Name' field is filled with 'Kiosk Config' and has a green checkmark. The 'Description' field is empty. The 'Platform' is set to 'Android Enterprise' and the 'Profile type' is set to 'Device restrictions'. At the bottom, the 'Next' button is highlighted with a red box.

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

Name * Kiosk Config ✓

Description

Platform Android Enterprise

Profile type Device restrictions

Previous Next

The screenshot shows the 'Configuration settings' tab. The 'Device experience' section is expanded and highlighted with a red box. It contains the 'Enrollment profile type' dropdown set to 'Dedicated device', which is also highlighted with a red box. Below it, the 'Kiosk mode' dropdown is set to 'Multi-app'. At the bottom, the 'Next' button is highlighted with a red box.

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

General

System security

Device experience

Fully managed and dedicated devices
These settings only work for fully managed and dedicated devices.

Enrollment profile type ⓘ Dedicated device

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

Select an app to use for kiosk mode *

com.microsoft.teams

+ Select an app to use for kiosk mode

Previous Next

Android Enterprise: Dedicated Device

Create a Kiosk Profile

- Once you have created your configuration, select Next
- Scope tags are optional, select Next
- Click Select groups to include
- Search for and add the Kiosk Device Group, click Select
- Click Next and then Create

The screenshot displays the Android Enterprise console interface, specifically the 'Device restrictions' section. The interface is divided into several panels and a main configuration area.

Left Panel: Device restrictions

- Navigation tabs: Basics, Configuration settings, Scope tags, Assignments (selected), Review.
- Buttons: Previous, Next (highlighted with a red box).

Center Panel: Device restrictions

- Navigation tabs: Basics, Configuration settings, Scope tags, Assignments (selected), Review.
- Buttons: Previous, Next (highlighted with a red box).

Right Panel: Select groups to include

- Search bar: Kiosk (highlighted with a red box).
- Search results: Kiosk Device Group (Selected) (highlighted with a red box).
- Buttons: Select (highlighted with a red box), Remove.

Main Configuration Area: Review + create

- Navigation tabs: Basics, Configuration settings, Scope tags, Assignments, Review + create (selected).
- Buttons: Previous, Create (highlighted with a red box).

Summary

Basics

- Name: Kiosk Config
- Description: --
- Platform: Android Enterprise
- Profile type: Device restrictions

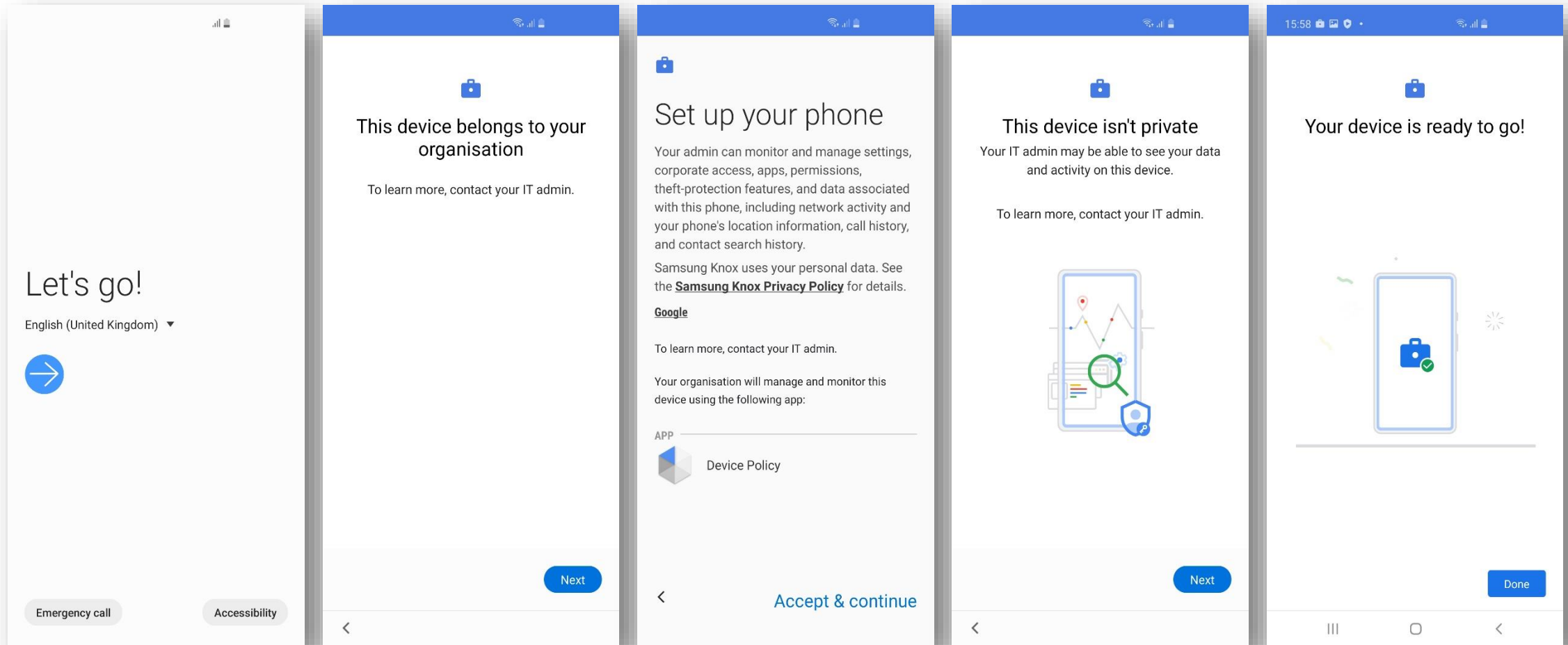
Configuration settings

- Leave kiosk mode code: 1234
- Enrollment profile type: Dedicated device
- Kiosk mode: Multi-app

App name ↑↓	Package Name ↑↓	App store URL ↑↓	Publish
Microsoft Outlook	com.microsoft.office.o...	Not configured	Microsof
Microsoft Teams	com.microsoft.teams	Not configured	Microsof

Leave kiosk mode: Enable

Android Enterprise: Dedicated Device Enrollment



Tap anywhere on the screen 7 times and scan the enrollment QR code

Next

Accept & continue

Next

Done

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

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

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

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



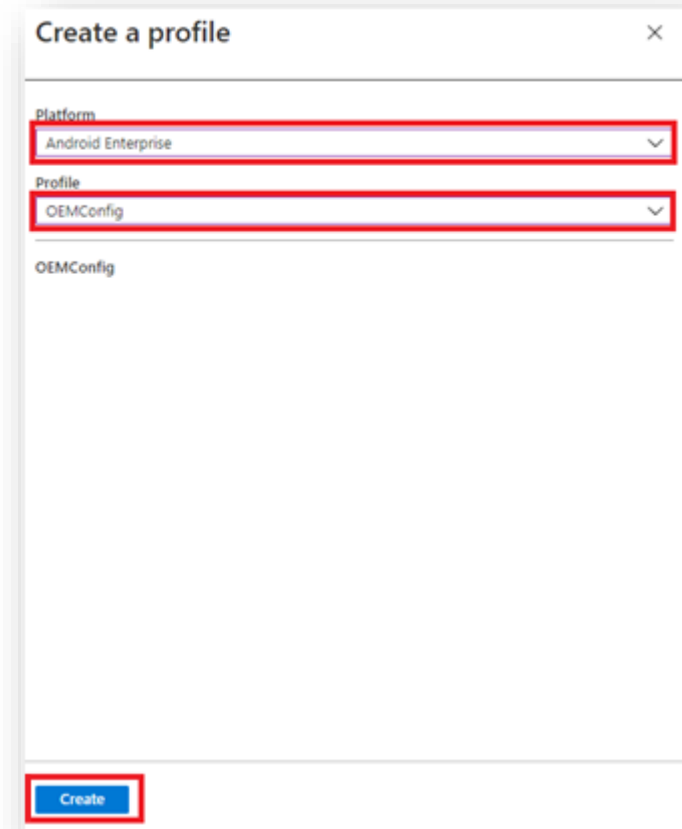
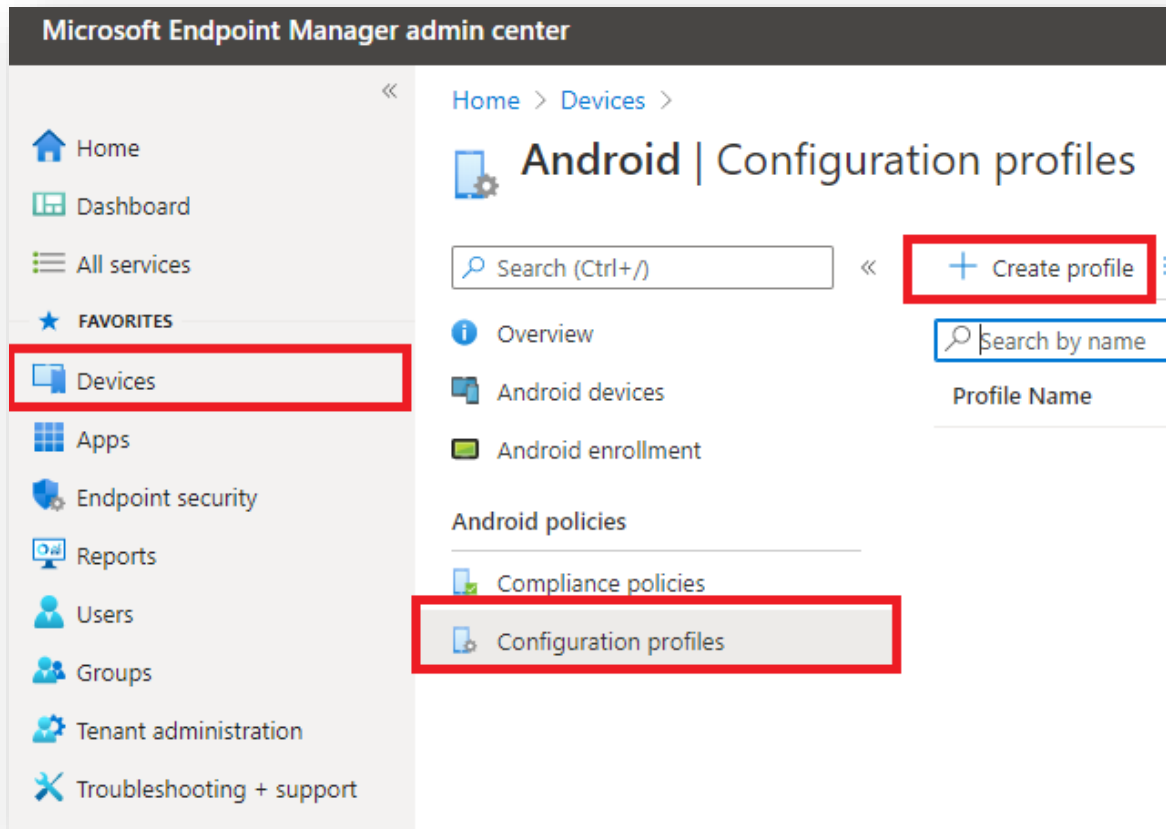
Knox Service Plugin

- Within the Endpoint Manager console, navigate to: Apps > Android apps > Add
- Set the App type to Managed Google Play app and click Select
- Search for and approve the Knox Service Plugin

The screenshot displays the Endpoint Manager console interface. On the left, the navigation pane shows 'Apps' selected. The main area is titled 'Android | Android apps' and includes an 'Add' button. A modal window titled 'Select app type' is open, showing 'Managed Google Play app' selected in the 'App type' dropdown. Below this, the 'Managed Google Play app' section shows a search bar and a 'Select' button. In the bottom right, a card for the 'Knox Service Plugin' by Samsung Electronics Co., Ltd. is shown, marked as 'APPROVED' with a PEGI 3 rating. The card includes a 'Select' button and an 'Unapprove' button.

Knox Platform for Enterprise

- Navigate to: Devices > Android > Configuration profiles
- Click Create profile
- Set the Platform to Android Enterprise
- Set the Profile to OEMConfig
- Click Create



Knox Platform for Enterprise

- Enter a Name
- Description is optional
- Click Select an OEMConfig app
- Search for and select the Knox Service Plugin
- Click Select
- Click Next

Create profile
OEMConfig

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

Name *

Description

OEMConfig app *

Search by name or publisher...

App Name	Publisher
Knox Service Plugin	Samsung Electronics Co., Ltd.

Selected app:

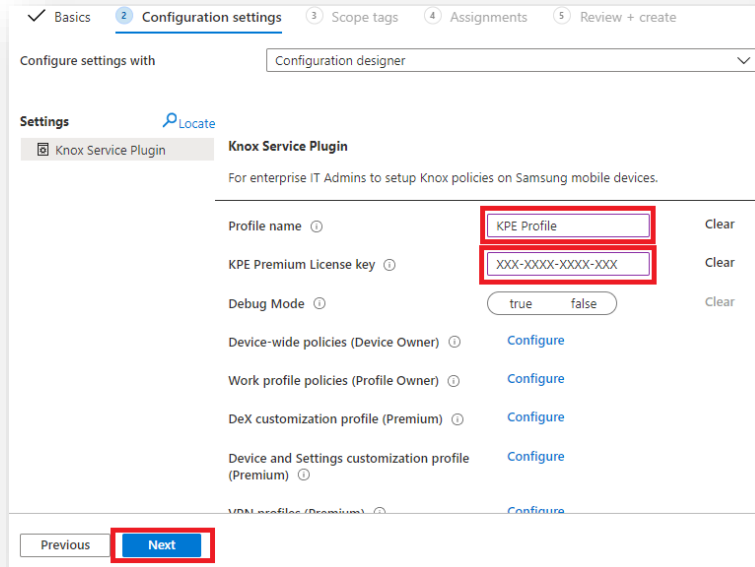
Knox Service Plugin Samsung Electronics... Remove

Previous **Next**

Select

Knox Platform for Enterprise

- Enter a Profile name
- To make use of the KPE Premium features, enter your KPE Premium License Key. This can be found in your Samsung Knox Portal
- Set your desired configuration and select Next
- Scope tags are optional, select Next
- Choose an assignment and select Next
- Click Create



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

Configure settings with Configuration designer

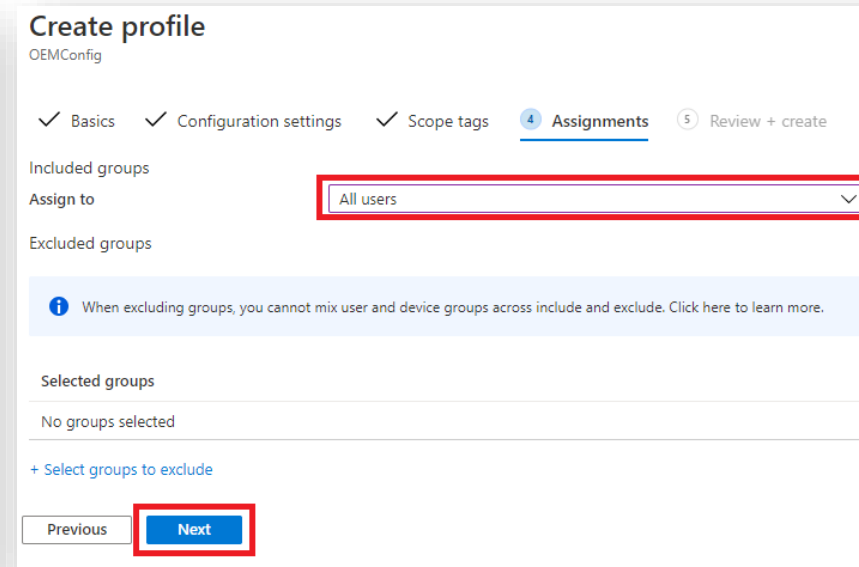
Settings [Locate](#)

Knox Service Plugin

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

Profile name	KPE Profile	Clear
KPE Premium License key	XXX-XXXX-XXXX-XXX	Clear
Debug Mode	<input checked="" type="radio"/> true <input type="radio"/> false	Clear
Device-wide policies (Device Owner)	Configure	
Work profile policies (Profile Owner)	Configure	
DeX customization profile (Premium)	Configure	
Device and Settings customization profile (Premium)	Configure	

Previous **Next**



Create profile OEMConfig

✓ Basics ✓ Configuration settings ✓ Scope tags 4 Assignments 5 Review + create

Included groups

Assign to All users

Excluded groups

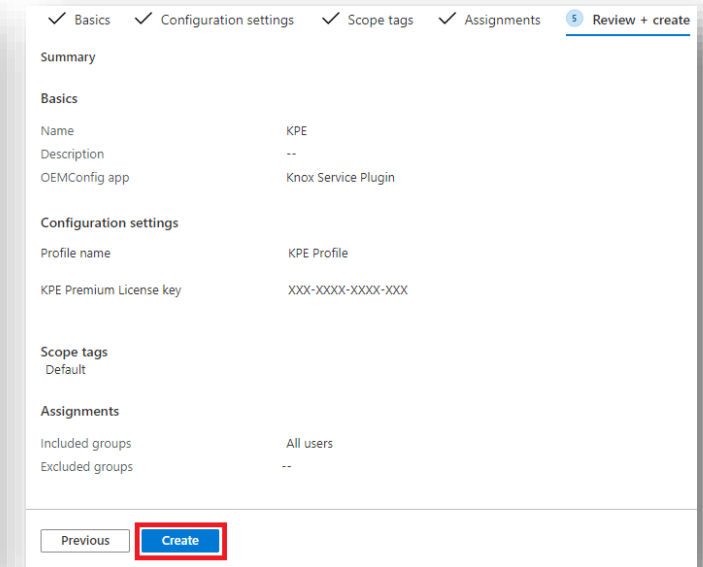
When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.

Selected groups

No groups selected

[+ Select groups to exclude](#)

Previous **Next**



✓ Basics ✓ Configuration settings ✓ Scope tags ✓ Assignments 5 Review + create

Summary

Basics

Name	KPE
Description	--
OEMConfig app	Knox Service Plugin

Configuration settings

Profile name	KPE Profile
KPE Premium License key	XXX-XXXX-XXXX-XXX

Scope tags

Default	
---------	--

Assignments

Included groups	All users
Excluded groups	--

Previous **Create**

This is version 2.2 of this document.

Thank you!

