



# Intune & Knox Platform for Enterprise

June 2022  
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.product@samsung.com](mailto:sruk.product@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
- Select I agree and click Launch Google to connect now

The screenshot shows the Microsoft Endpoint Manager admin center interface. The left-hand navigation pane is visible, with the following items: Home, Dashboard, All services, FAVORITES, Devices (highlighted with a red box), Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area shows the breadcrumb path: Home > Devices > Android | Android enrollment. Under the 'Android enrollment' section, there are two sub-items: Overview and Android devices (both highlighted with red boxes). Below this, under 'Android Enterprise', there is a 'Prerequisites' section containing a card for 'Managed Google Play' with the text 'Link your managed Google Play account to Intune.' This card is also highlighted with a red box.

The screenshot shows the 'Managed Google Play' configuration page. At the top, it says 'Managed Google Play' and 'Android enrollment'. Below this, there is a 'Disconnect' button. The page displays the following status information:

Status:	Not Setup	Google Account:	Not Available
Organization:	Not Available	Registration Date:	Not Available

Below the status information, there is a message: '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.](#)'

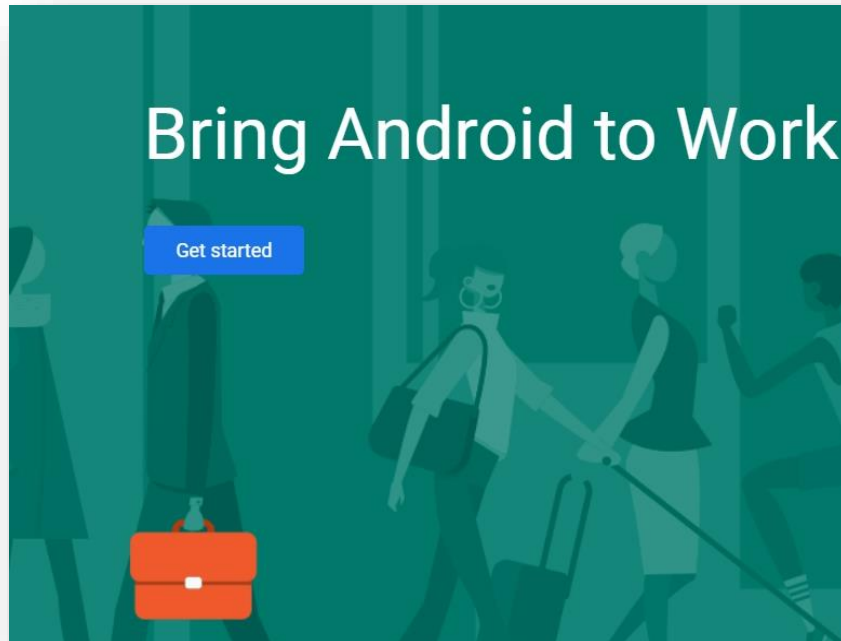
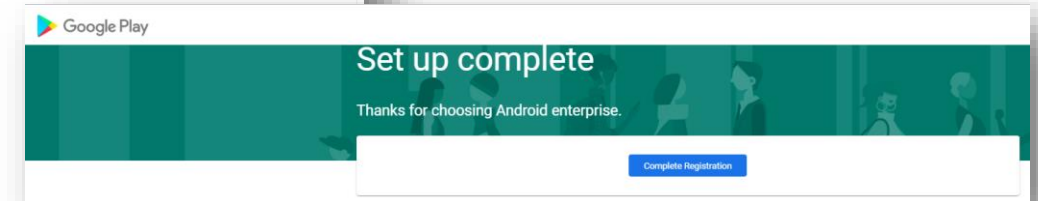
The page lists two steps:

1. I grant Microsoft permission to send both user and device information to Google. [Learn More.](#)  
 I agree. (This checkbox is highlighted with a red box)
2. Connect your Intune tenant to an administrative Google account to enable Android enterprise enrollment.

At the bottom of the page, there is a blue button labeled 'Launch Google to connect now.' (This button is highlighted with a red box).

# 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 screenshot of the 'Contact details' form in the Google Play console. The form is titled 'Contact details' and includes a sub-header 'We need some details about your key contacts'. It contains two sections: 'Data Protection Officer' and 'EU Representative', each with input fields for Name, Email, and Phone. A checkbox at the bottom is checked, with the text 'I have read and agree to the Managed Google Play agreement.' A 'Confirm' button is located at the bottom right.

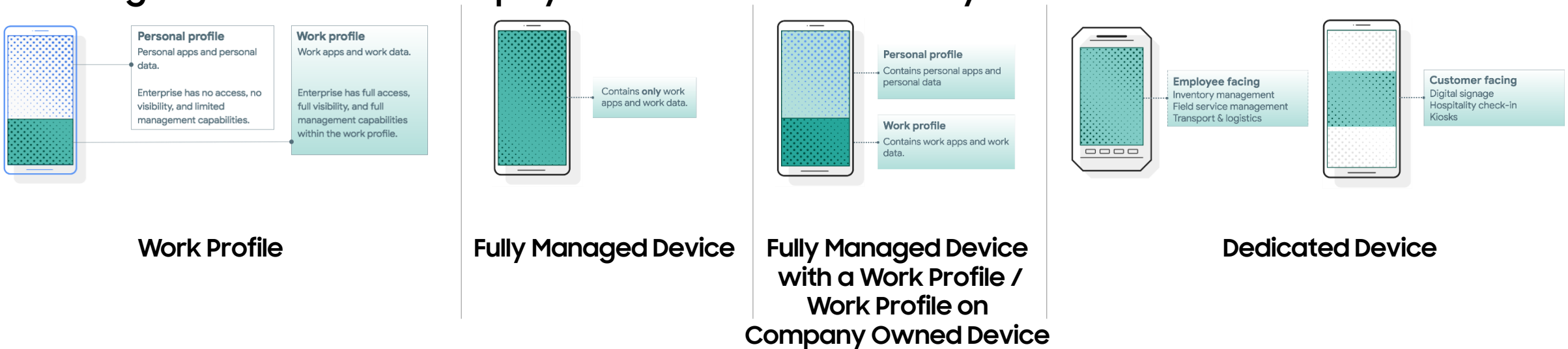
# Android Enterprise Deployment Modes

## Deployment Modes

Android Enterprise can be deployed in the following 5 deployment modes

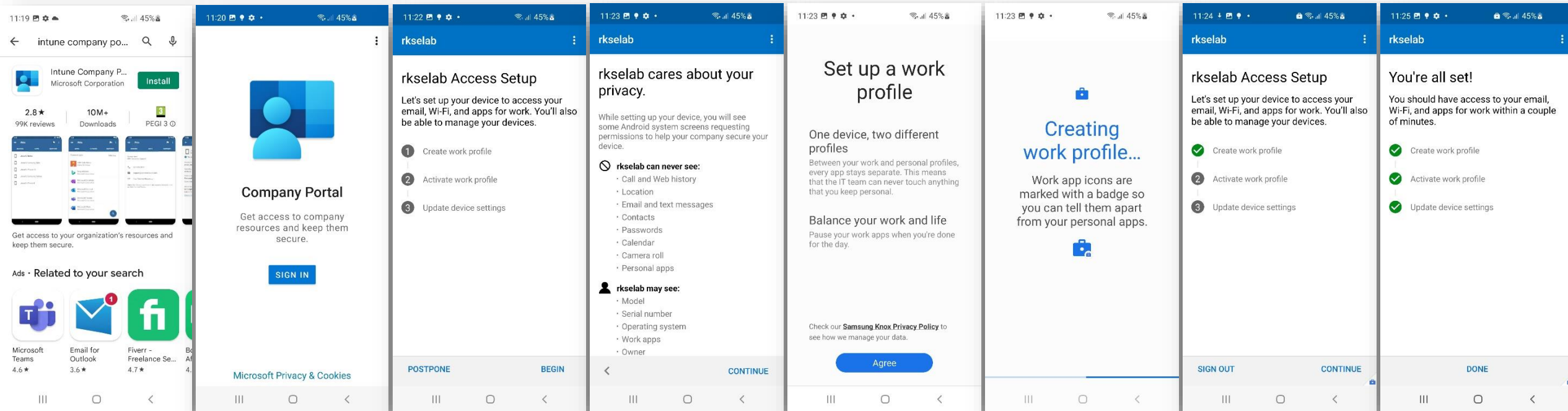
1. Work Profile [*formerly known as Profile Owner or PO*]
2. Fully Managed Device [*formerly known as Device Owner or DO*]
3. Fully Managed Device with a Work Profile [*formerly known as Company Owned Managed Profile or COMP*] on Android 10 or before
4. Work Profile on Company Owned Device or WPC on Android 11 or later
5. Dedicated device [*formerly known as COSU*]

Intune can support all 5 of these deployment modes. In this next section we will show you how to configure each of these 5 deployment modes in 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 And then enter your username and password

BEGIN

CONTINUE

Agree

Creating work profile...

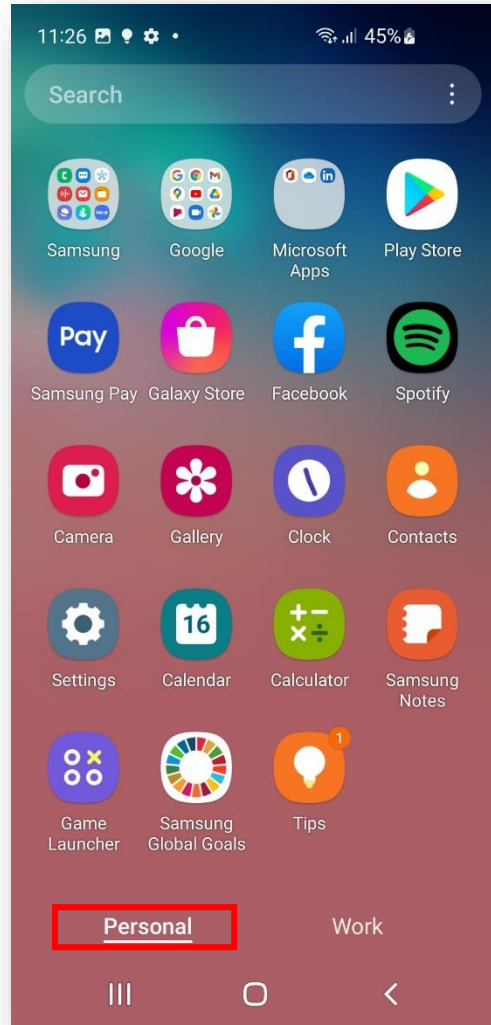
CONTINUE

DONE

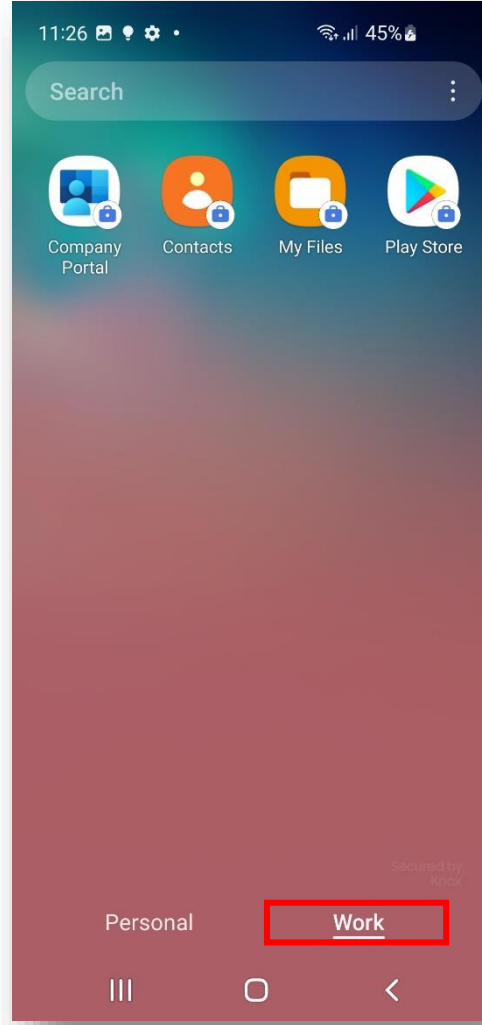


# Android Enterprise: Work Profile Enrollment

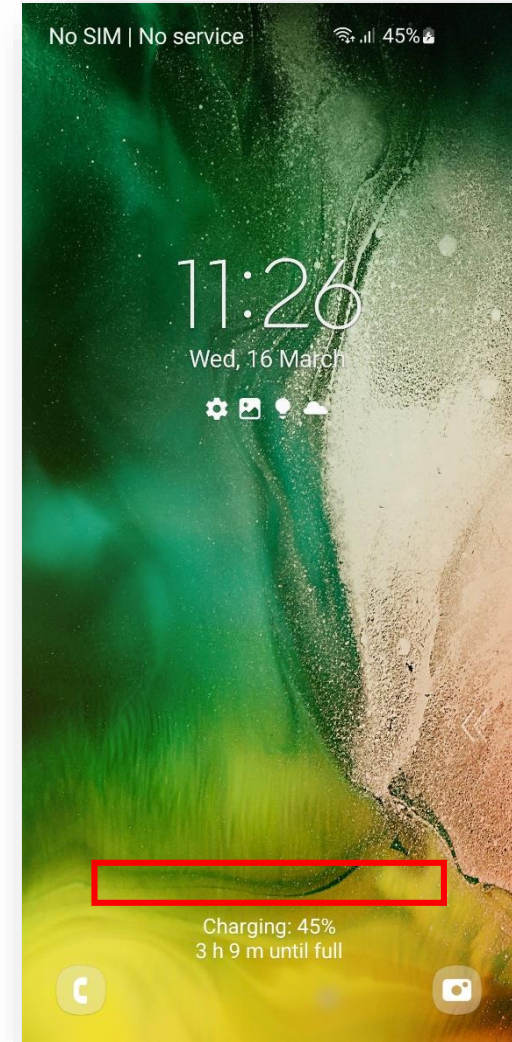
How to tell that Work Profile has been successfully set up:



Personal Tab



Work Tab



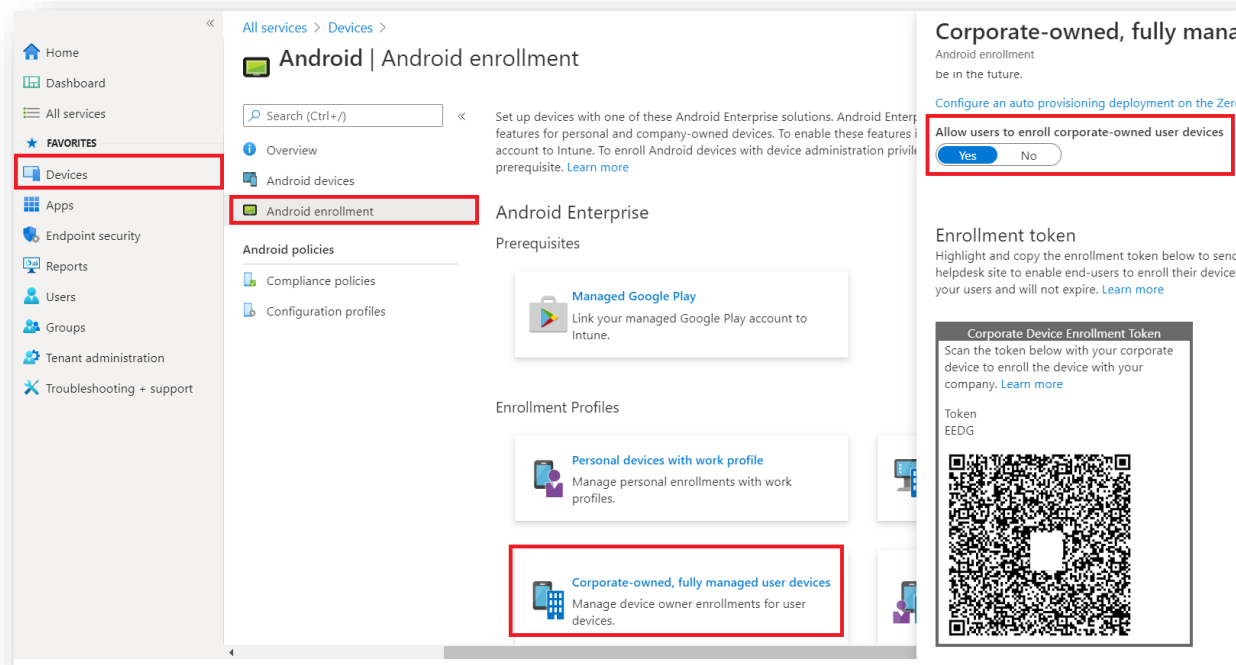
No mention of device belonging to your organization on lock screen

# Android Enterprise: Fully Managed

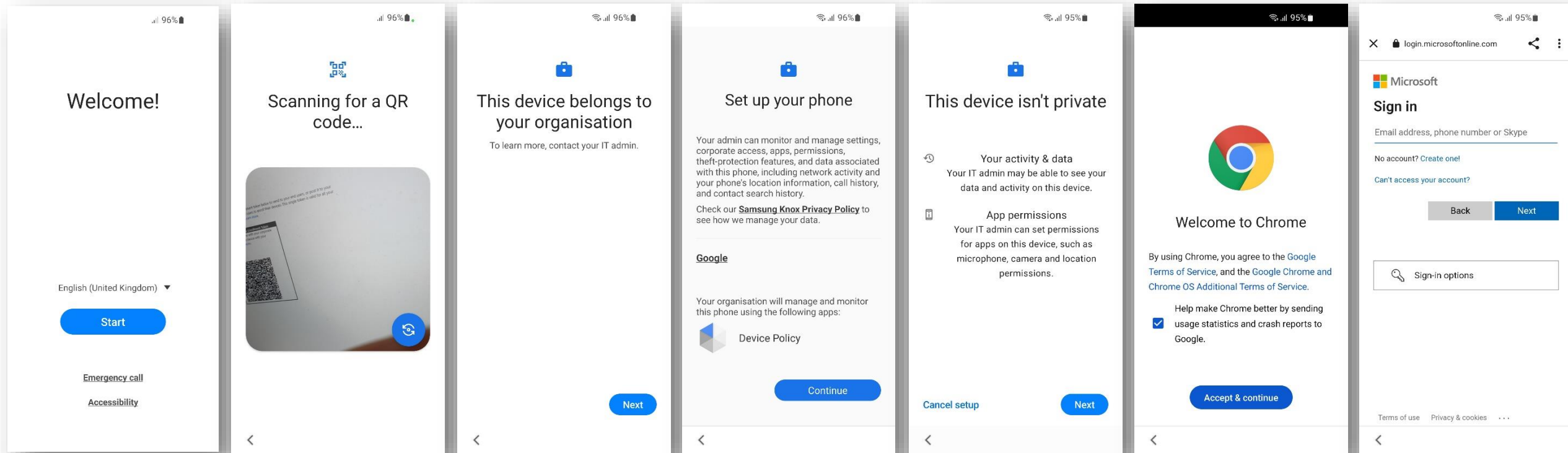
- Within Microsoft Endpoint Manager, navigate to: Devices > Android > Android enrollment
- Select Corporate-owned, fully managed user devices
- Make sure Allow users to enroll corporate-owned user devices is set to Yes
- If you're using KME, you can use the Token to simplify the enrollment steps and 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 (with QR code 1/2)



Tap anywhere on the screen 6 times

Scan the enrollment QR code

Next

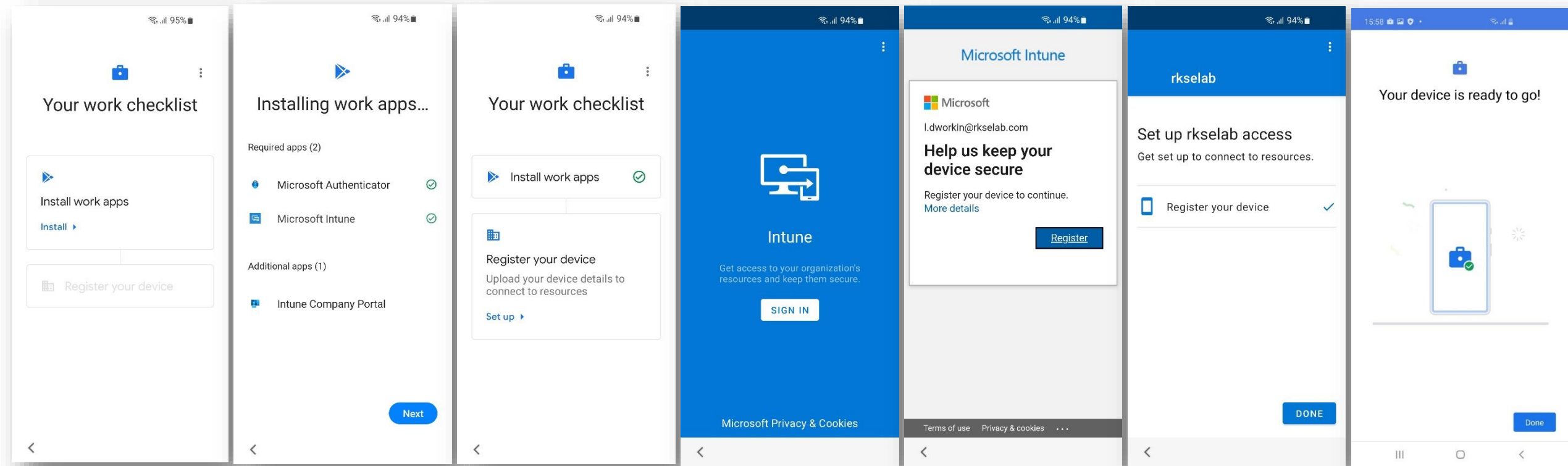
Continue

Next

Accept & continue

Sign in with your Office 365 account

# Android Enterprise: Fully Managed Enrollment (with QR code 2/2)



Install

Next

Set Up

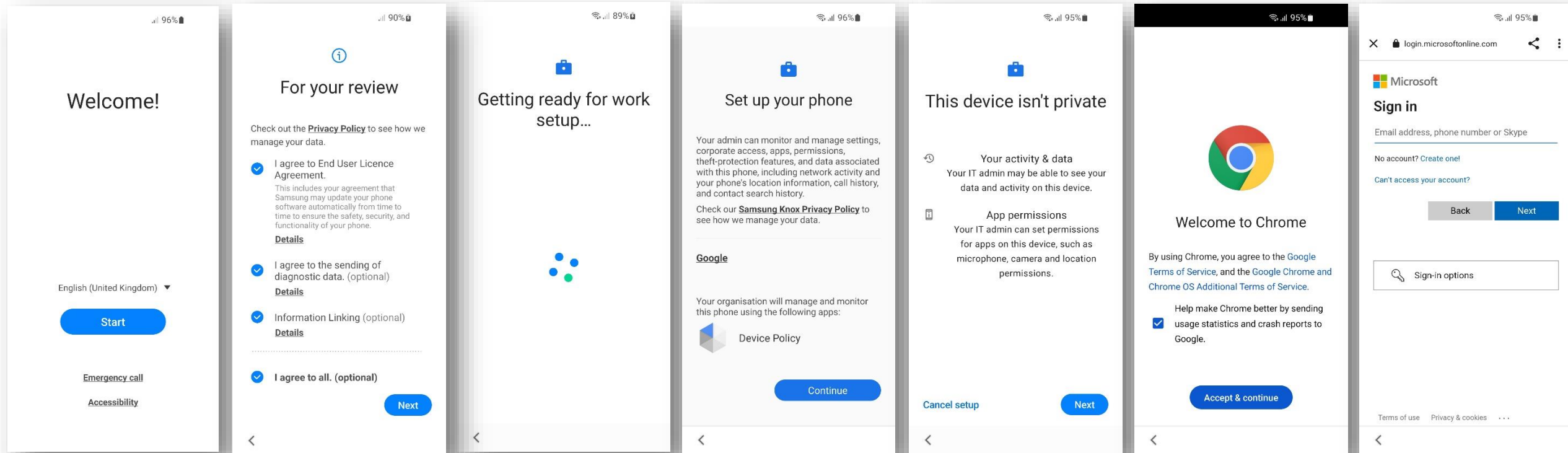
**SIGN IN  
and enter your  
Office 365  
password**

Register

DONE

Done

# Android Enterprise: Fully Managed Enrollment (with KME 1/2)



Click Start

Agree to some or all and Click Next

Knox Mobile Enrollment will update if necessary, then Getting ready for work setup...

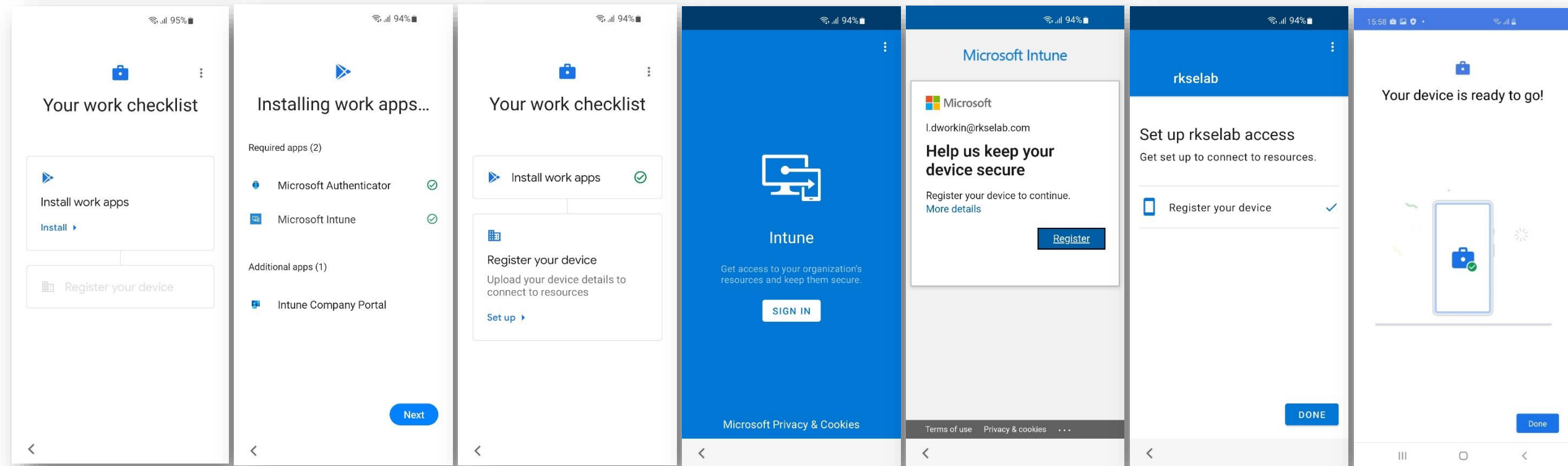
Continue

Next

Accept & continue

Sign in with your Office 365 account

# Android Enterprise: Fully Managed Enrollment (with KME 2/2)



Install

Next

Set Up

**SIGN IN  
and enter your  
Office 365  
password**

Register

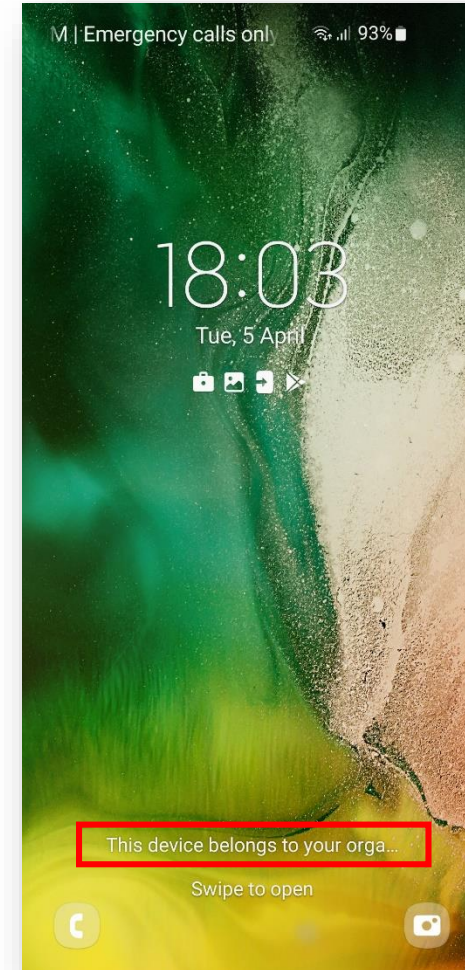
DONE

Done

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



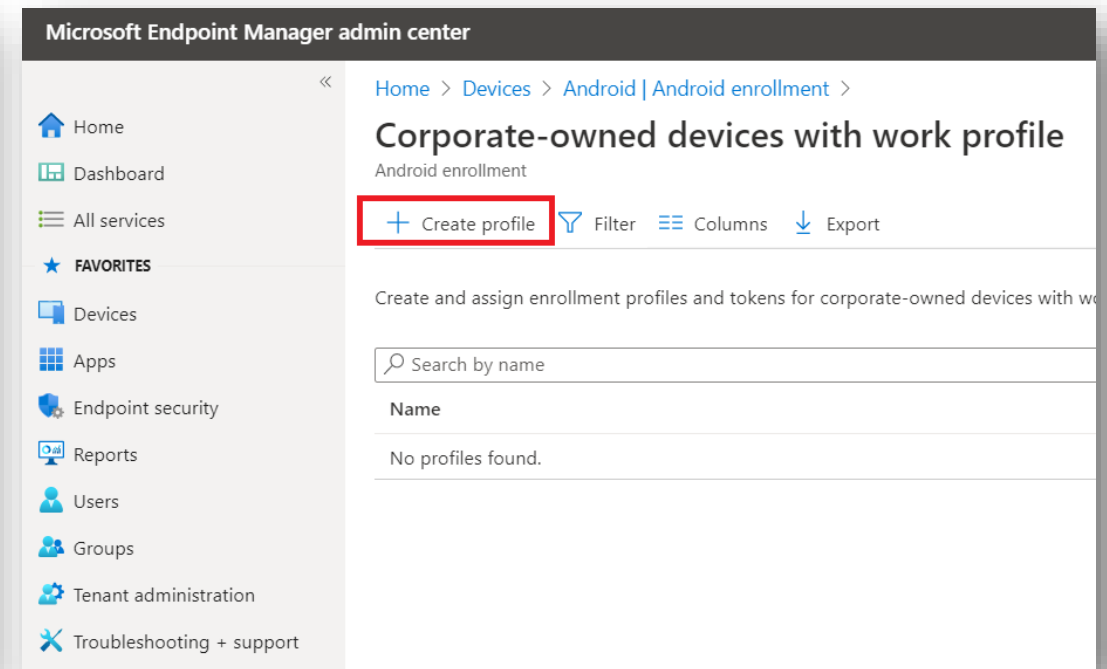
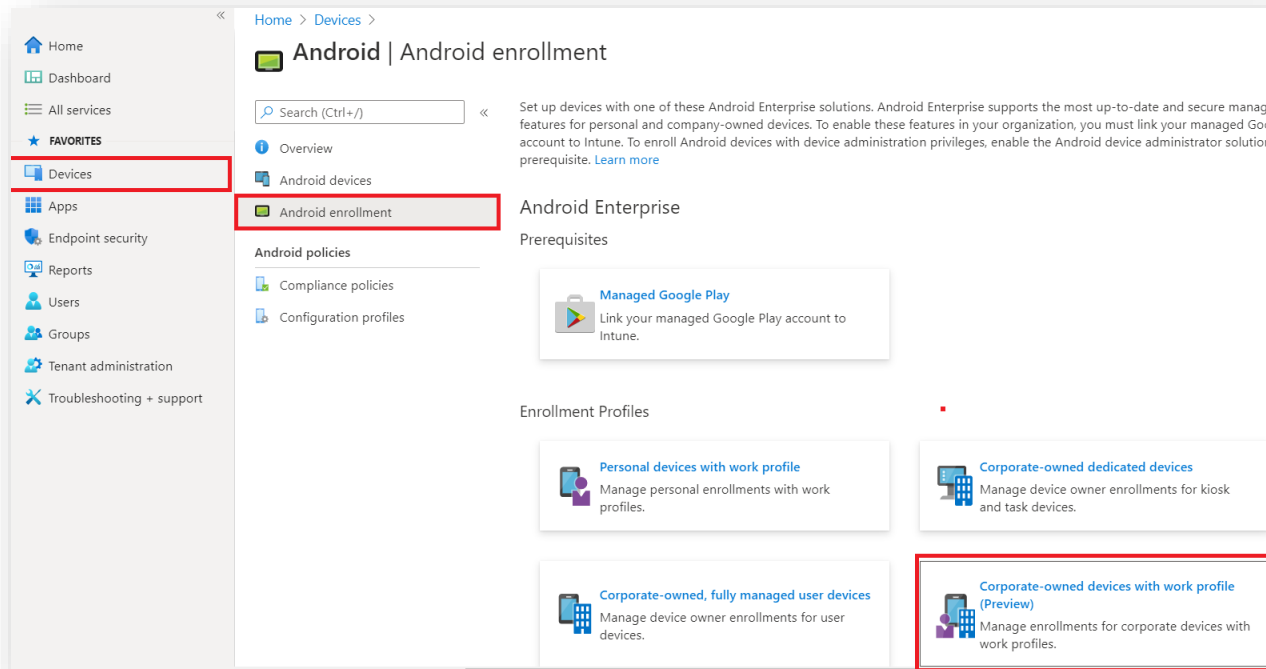
Sparse set of applications including Intune



Device belongs to your organization on lock screen

# 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



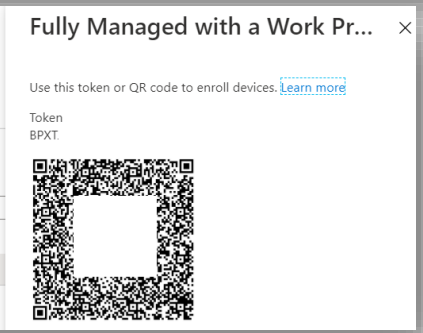
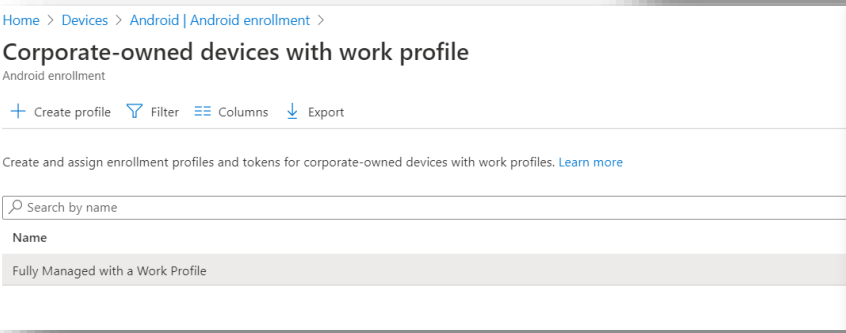
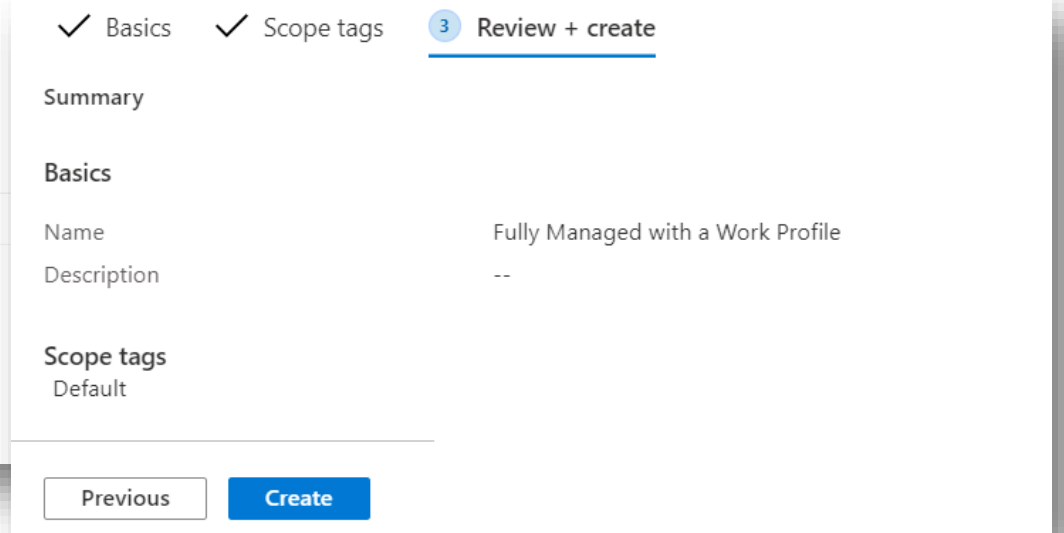
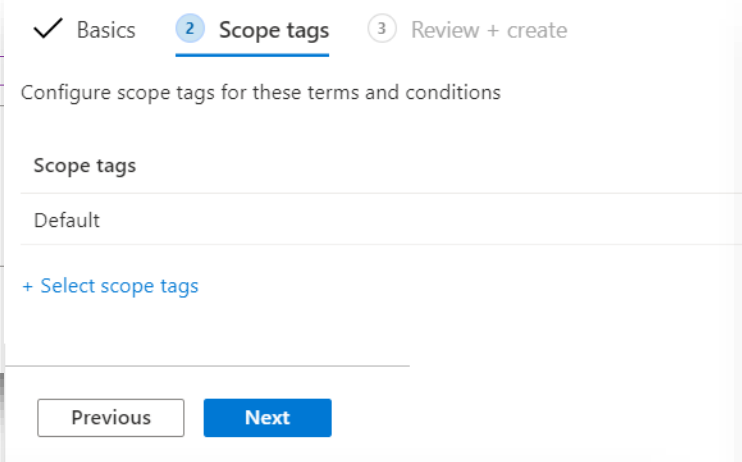
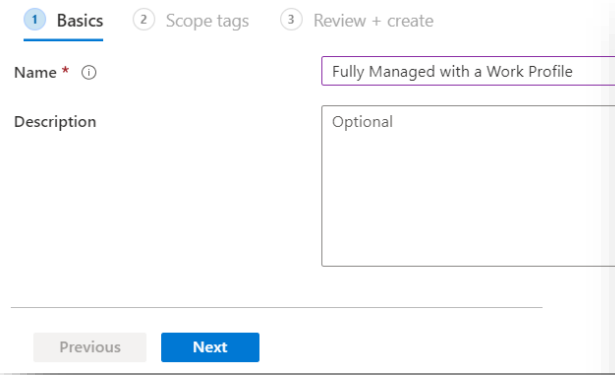


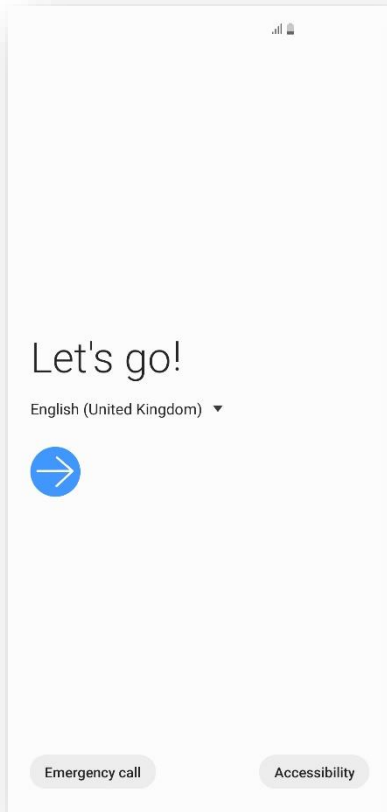
# Android Enterprise: Fully Managed with a Work Profile (COMP or WPC)

- 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.
 

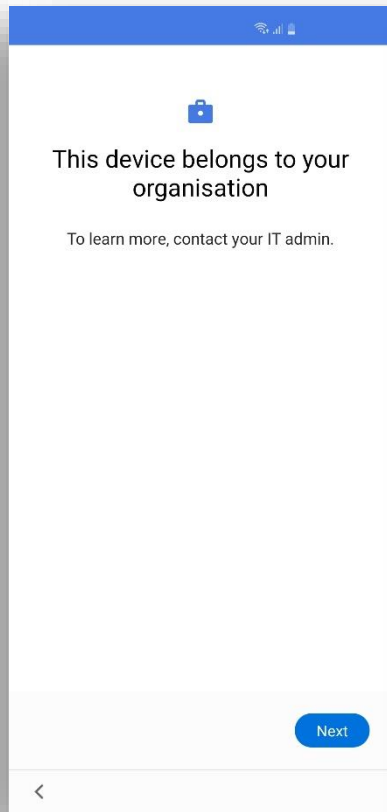
```

                {"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.

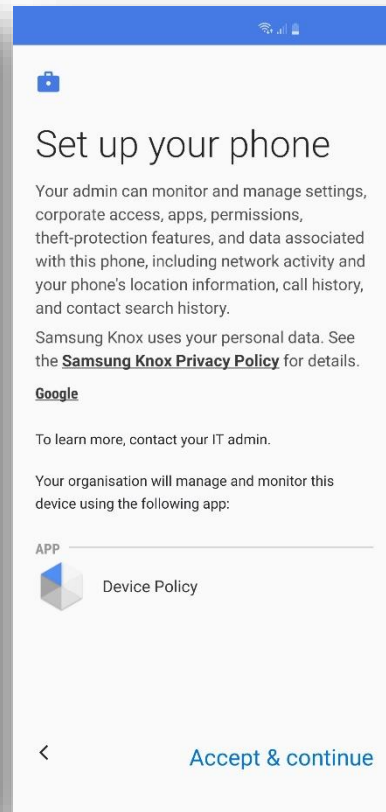




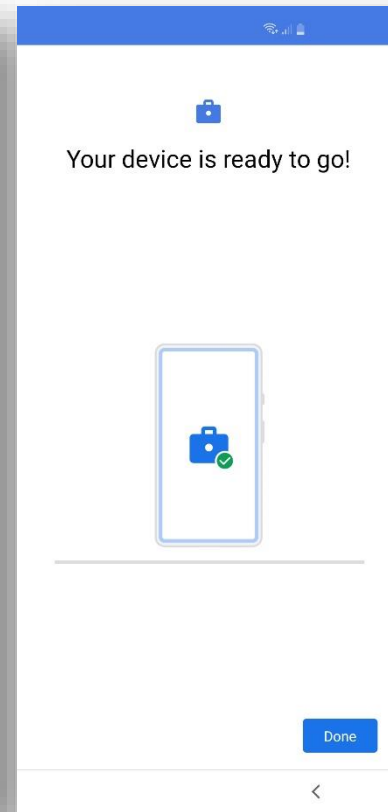
Tap anywhere on the screen 6 times and scan the enrollment QR code



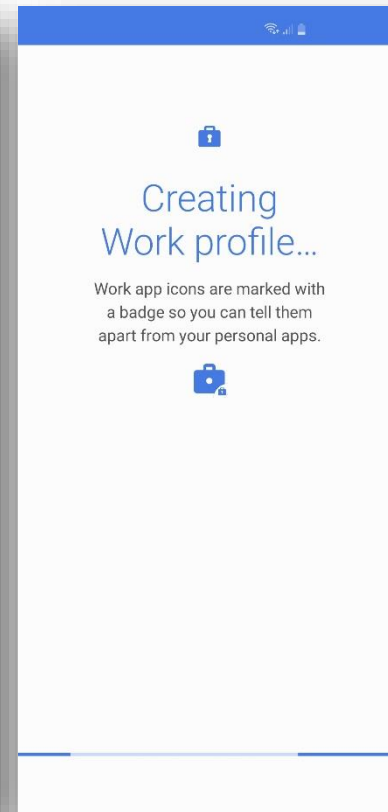
Next



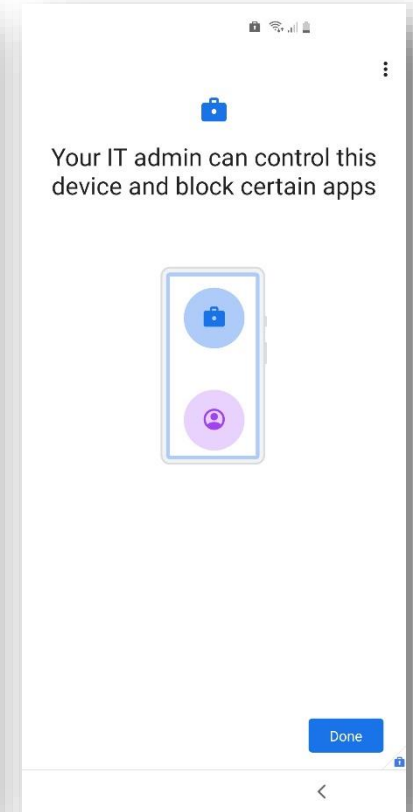
Accept & continue



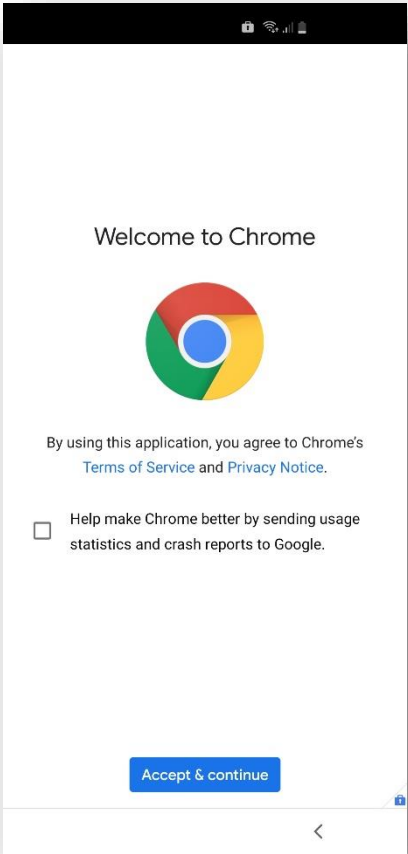
Done



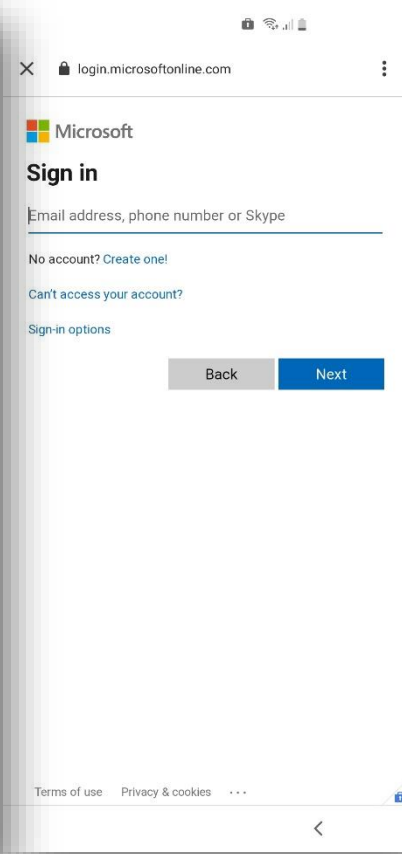
Wait



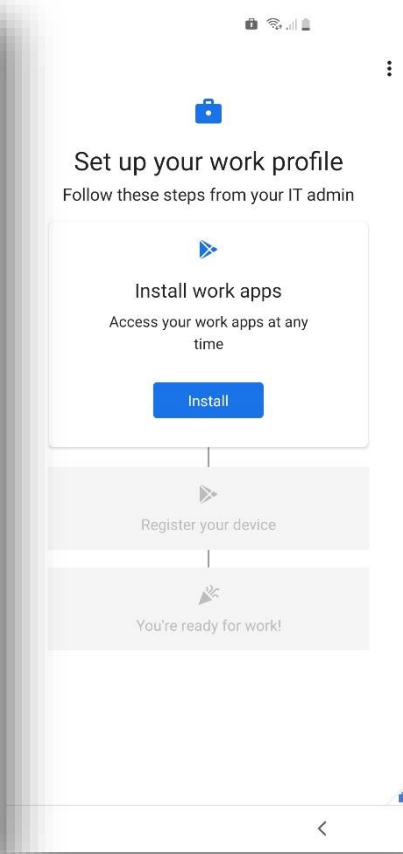
Done



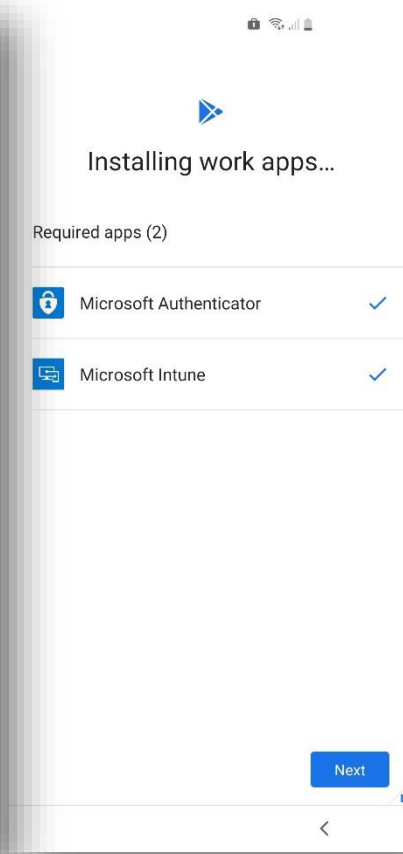
Accept & continue



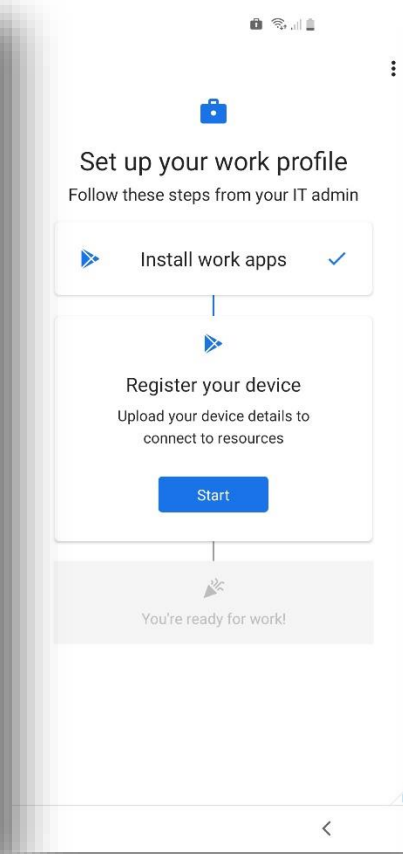
Sign into your Office 365 account, then select Next



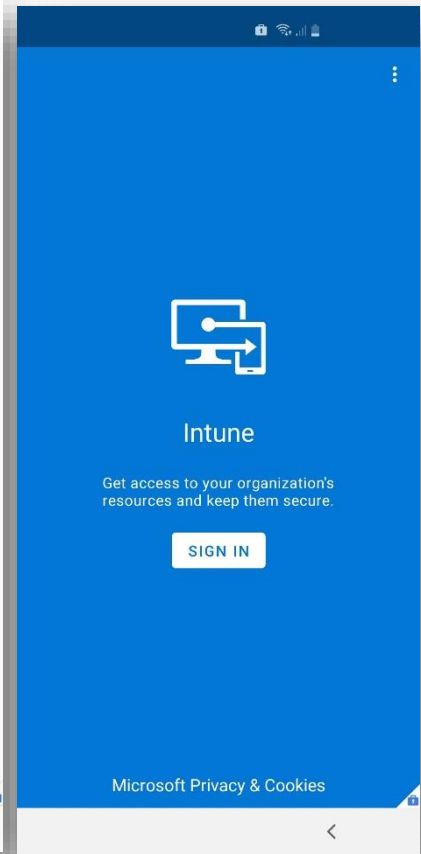
Install



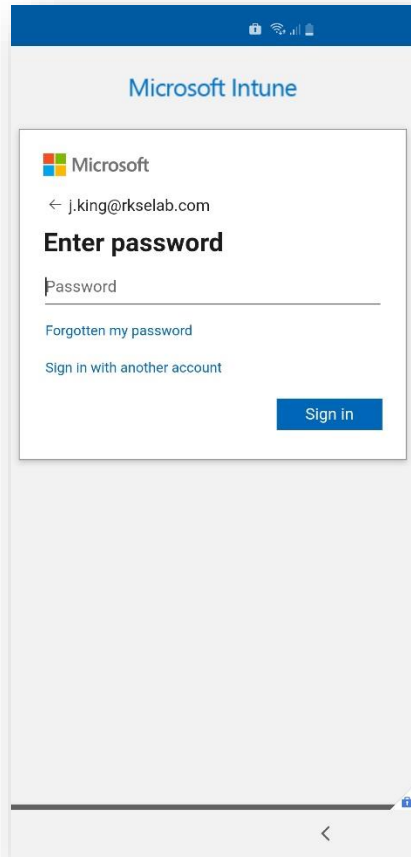
Next



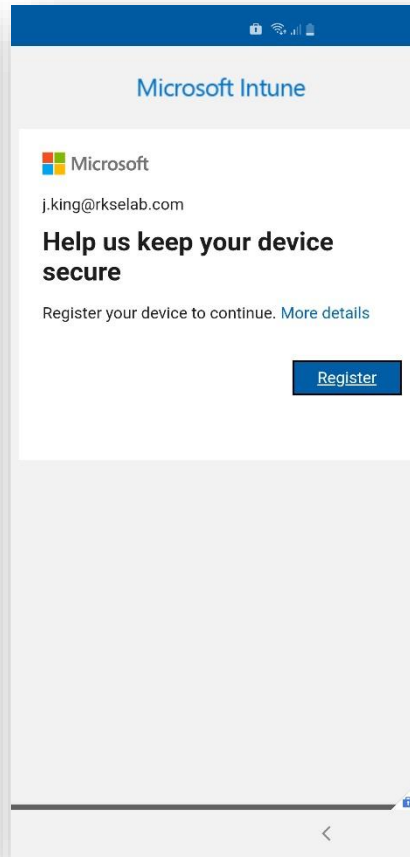
Start or Set Up



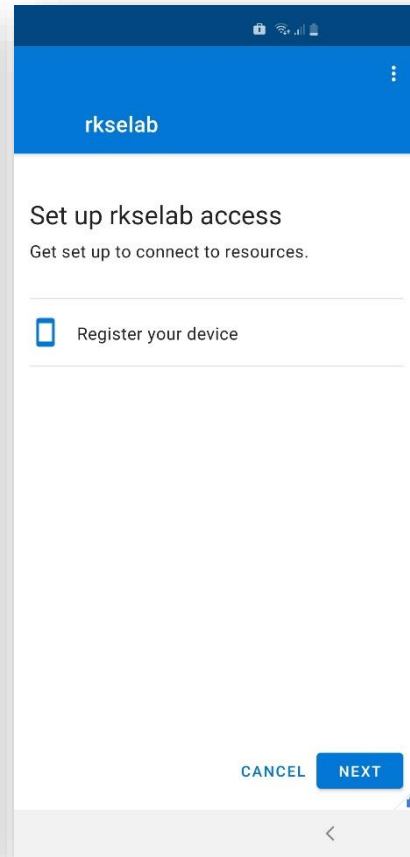
SIGN IN



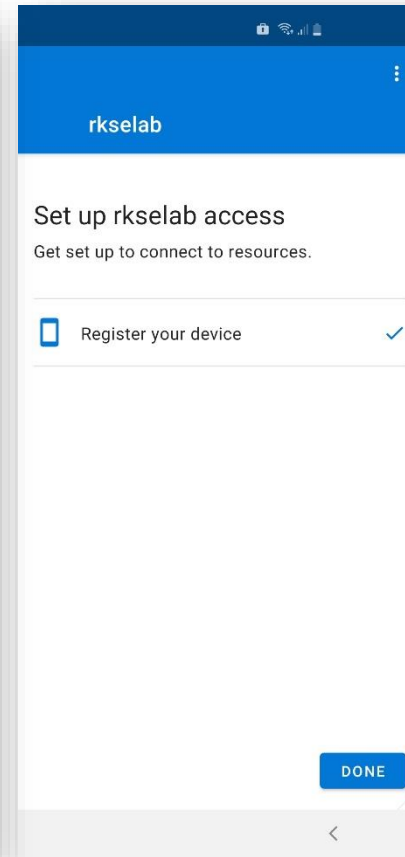
Sign in with your Office 365 account



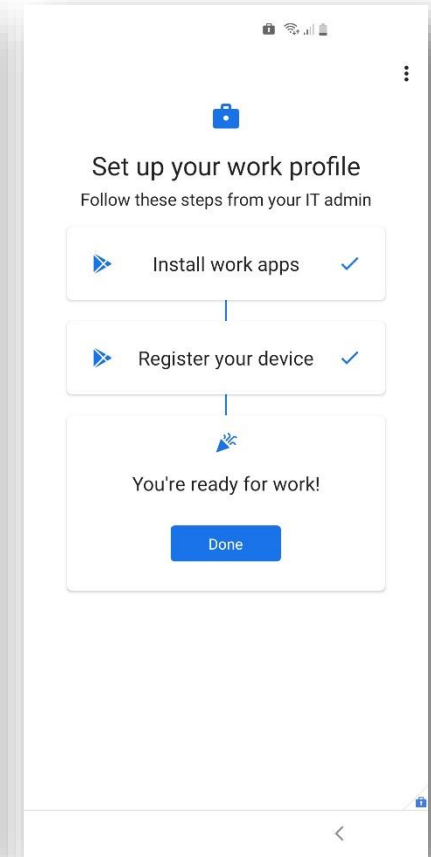
Register



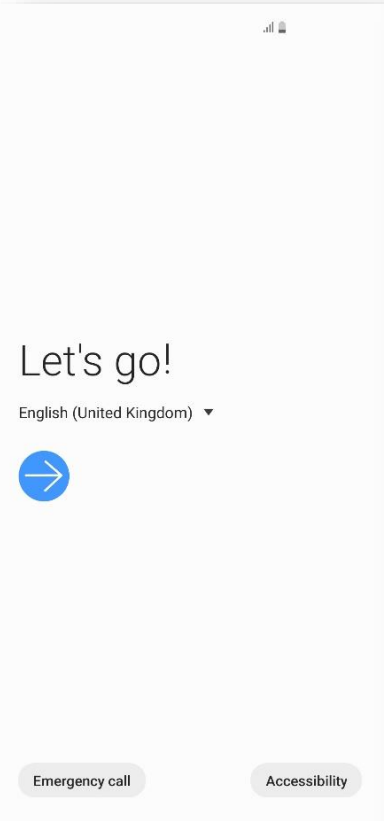
NEXT



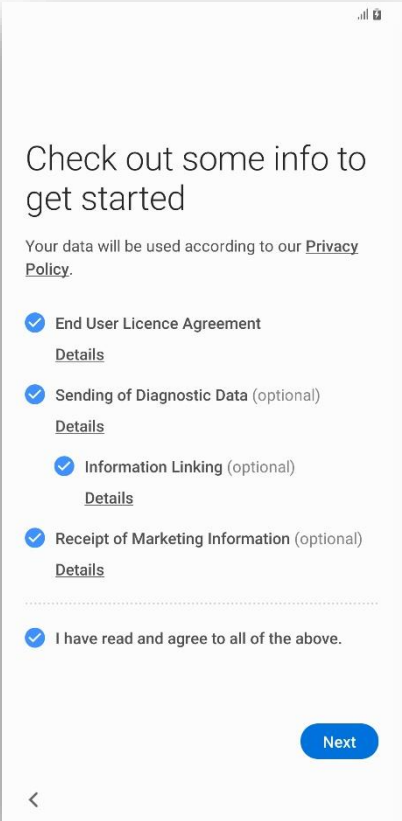
DONE



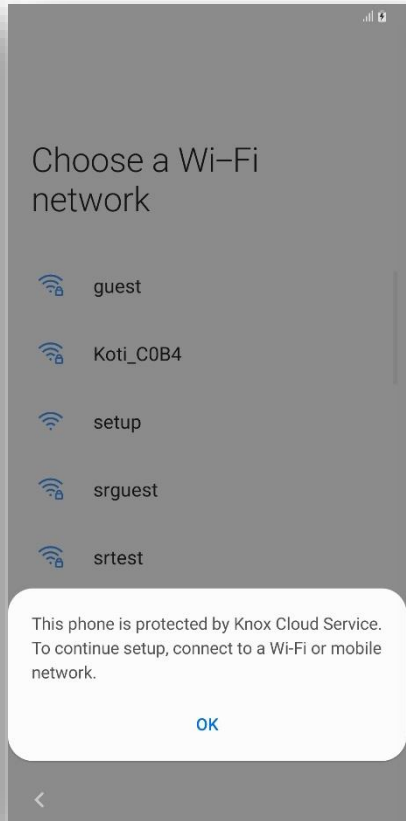
Done



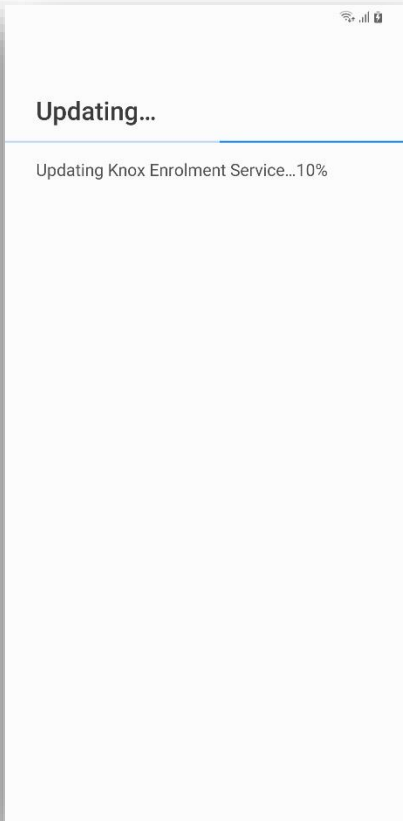
Click arrow to start



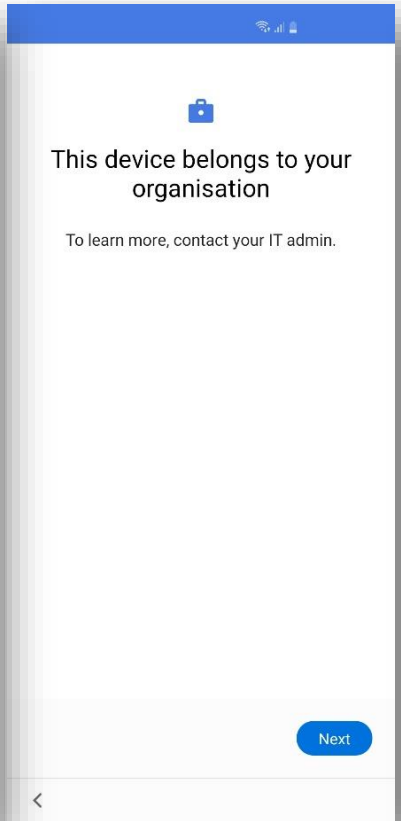
Next



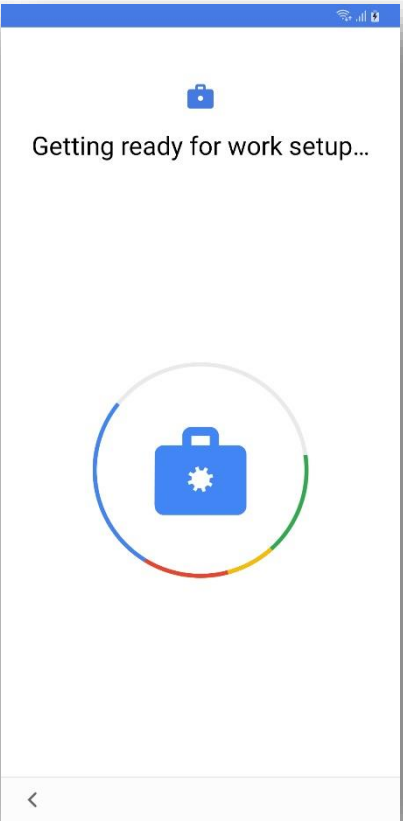
OK and connect to Wi-Fi



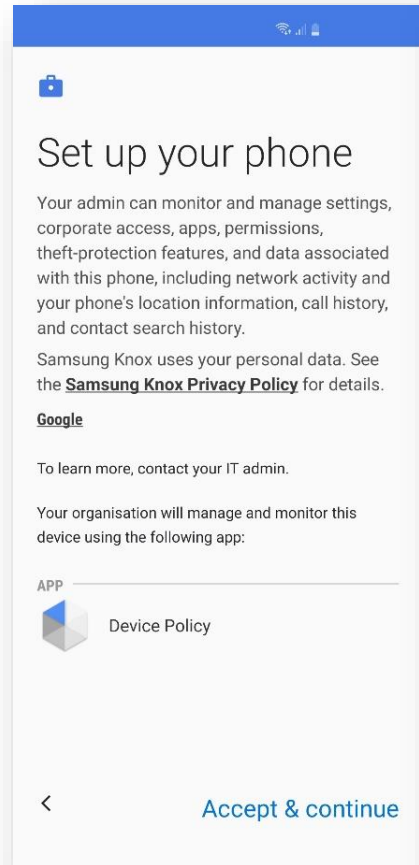
Wait for KME to update



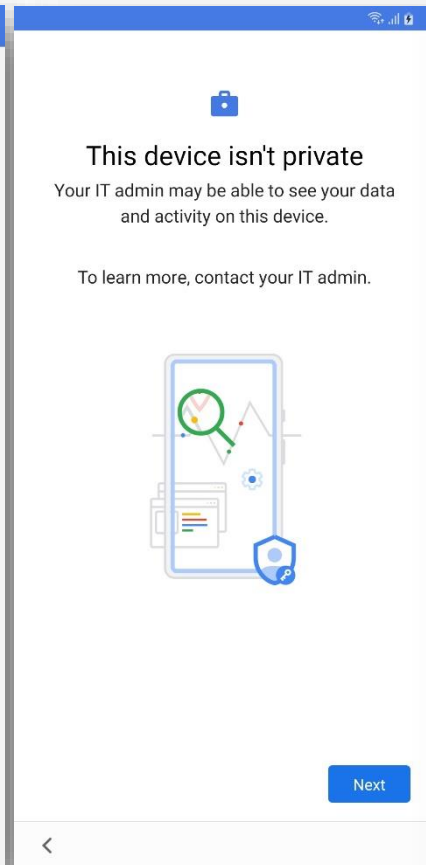
Next



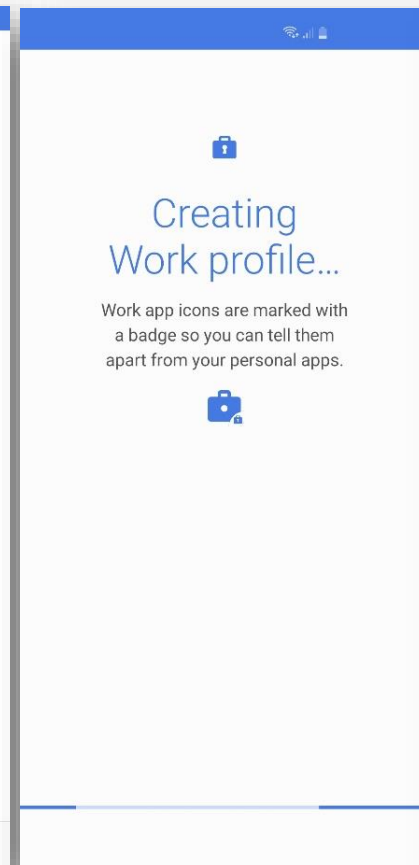
Get ready



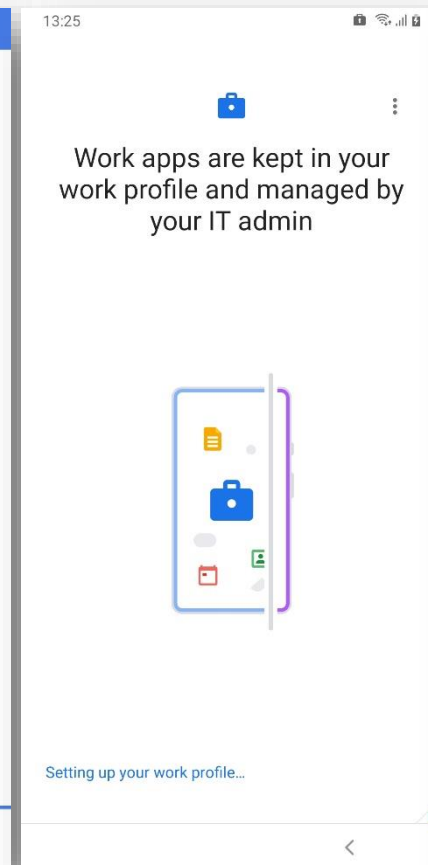
Accept & continue



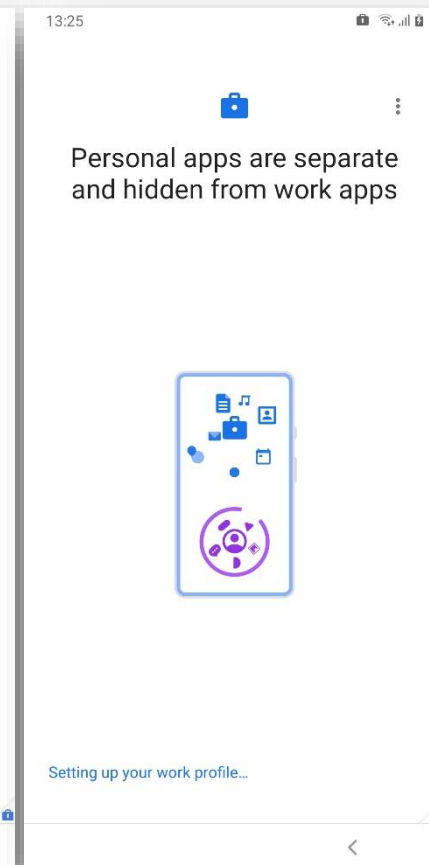
Next



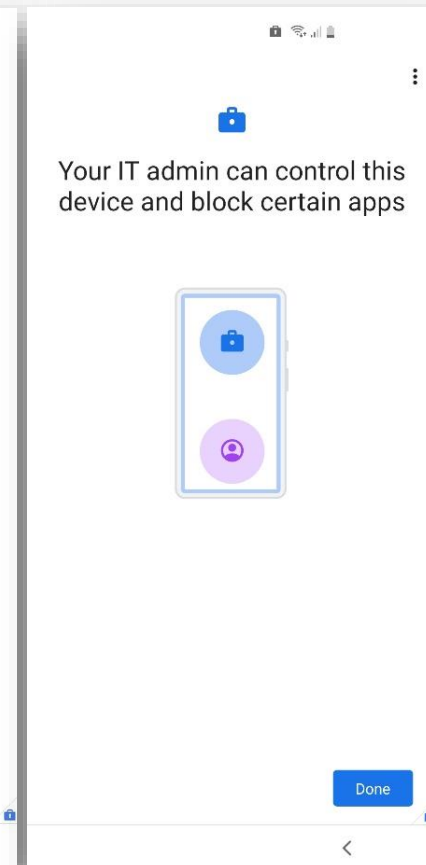
Wait



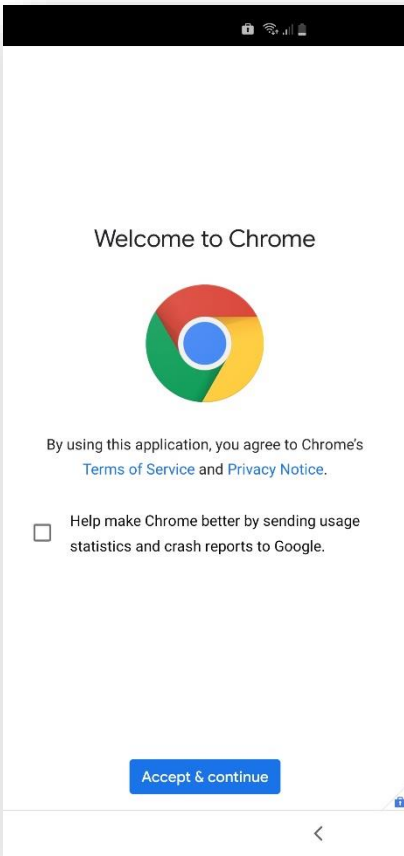
Wait



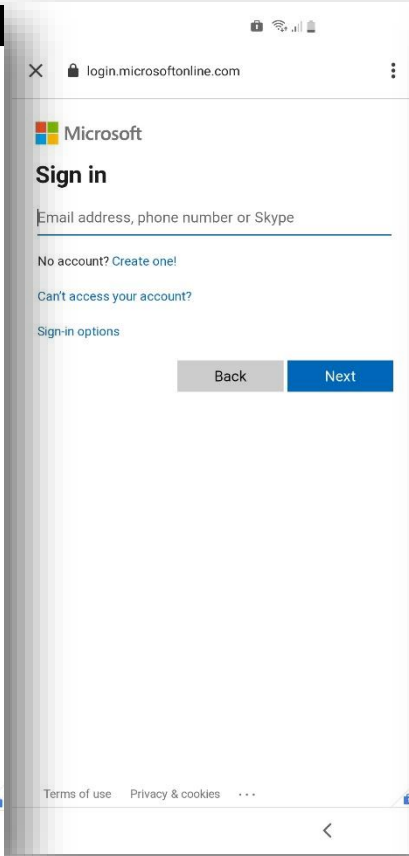
Wait



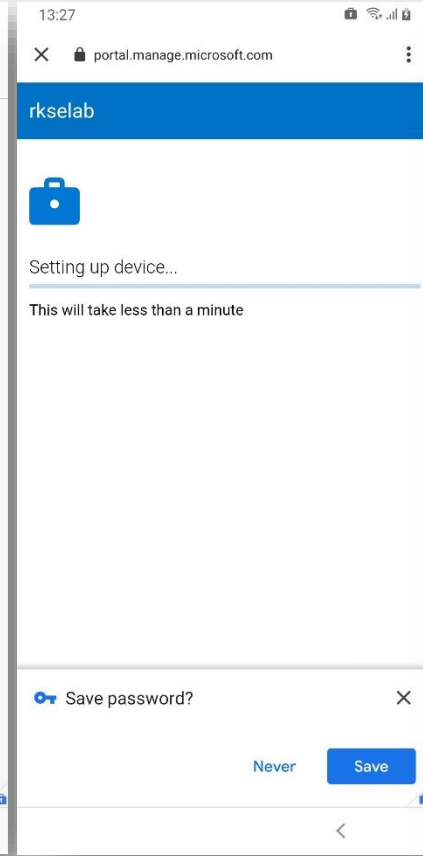
Done



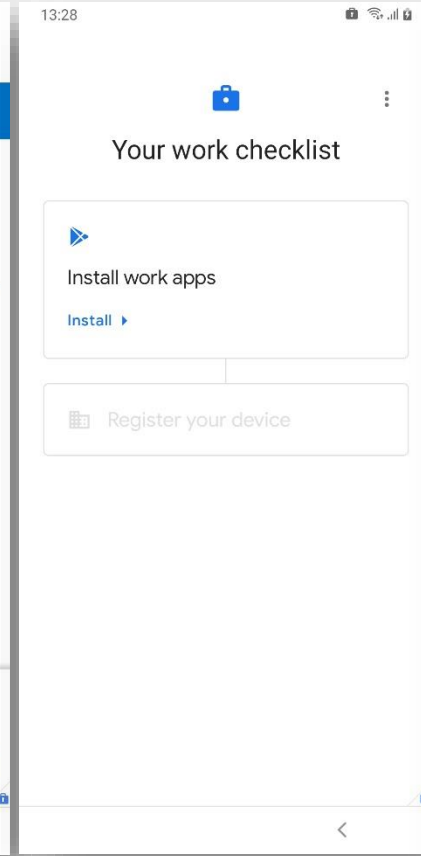
Accept & continue



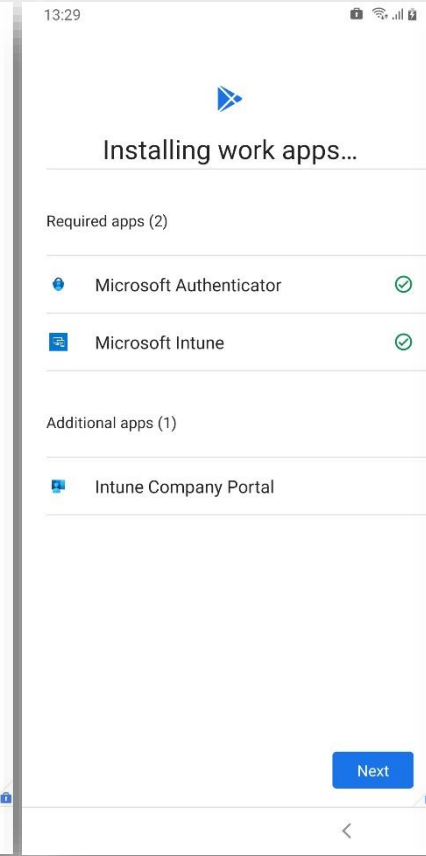
Sign into your Office 365 account, then select Next



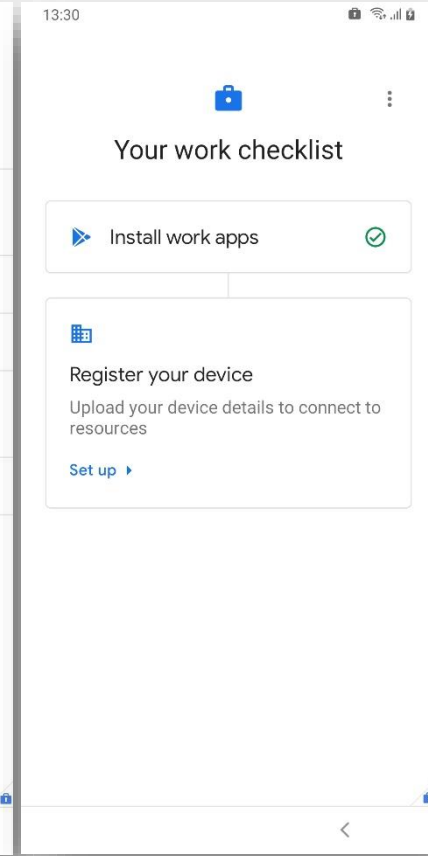
Never or Save for Password



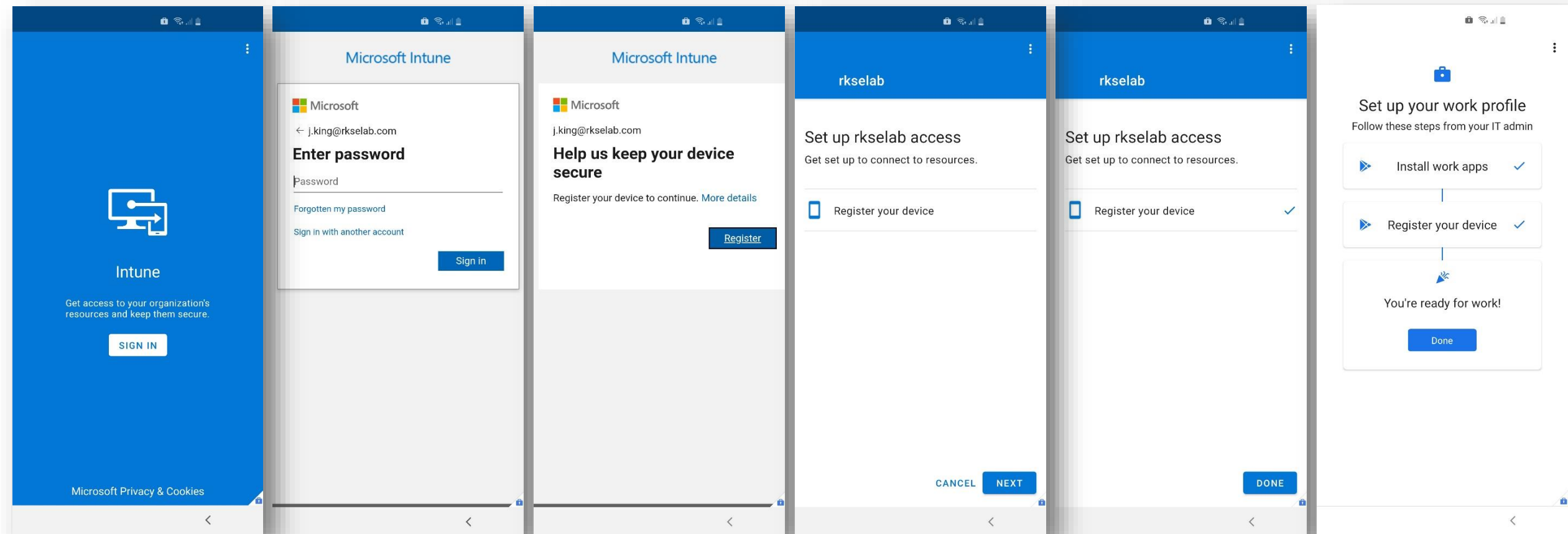
Install



Next



Set Up



SIGN IN

Sign in with your Office 365 account

Register

NEXT

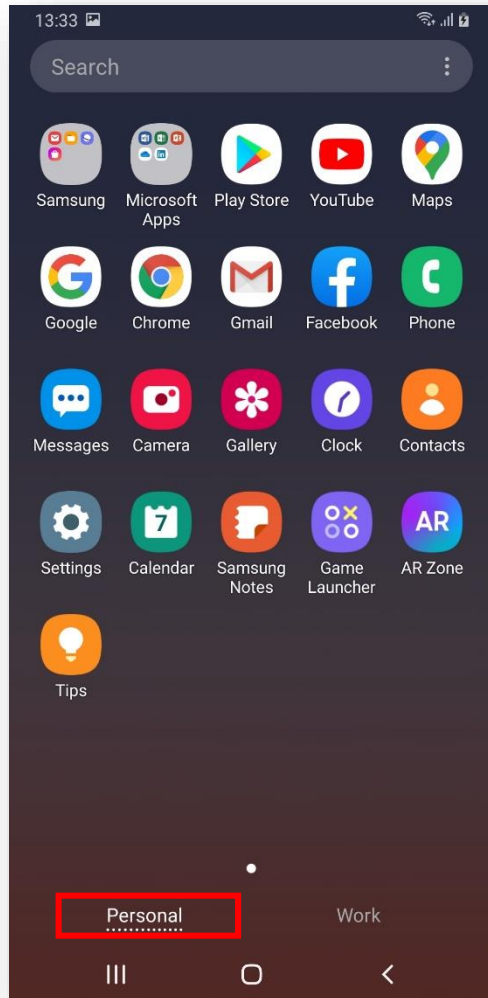
DONE

Done

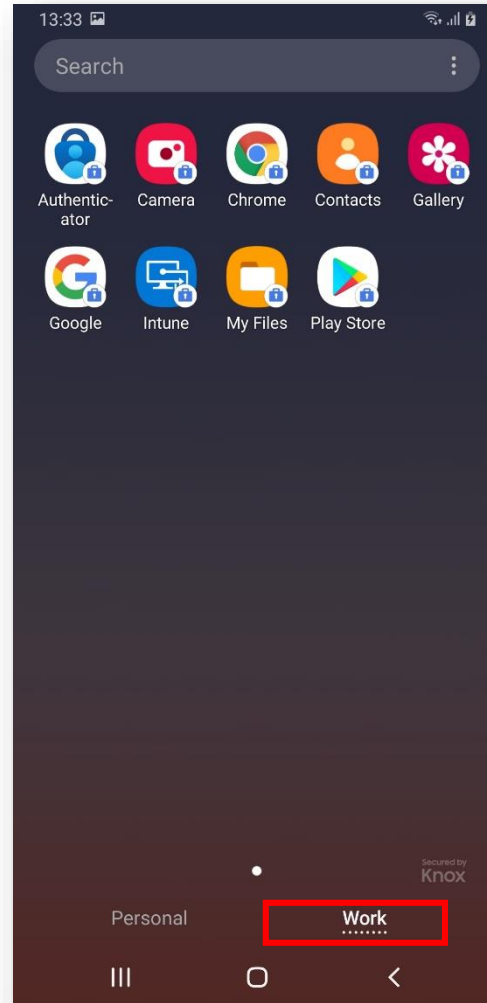


# Android Enterprise: Fully Managed with a Work Profile Enrollment

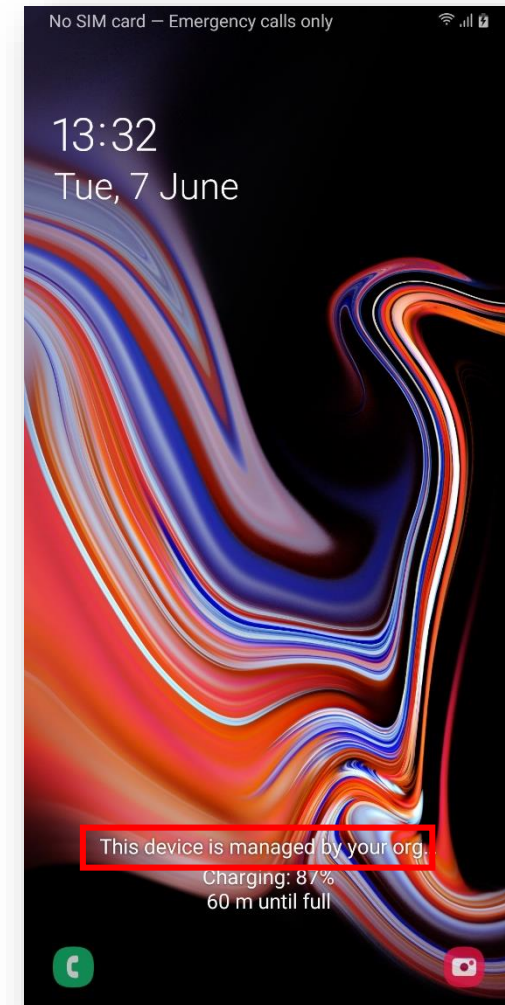
How to tell that Fully Managed with a Work Profile has been successfully set up:



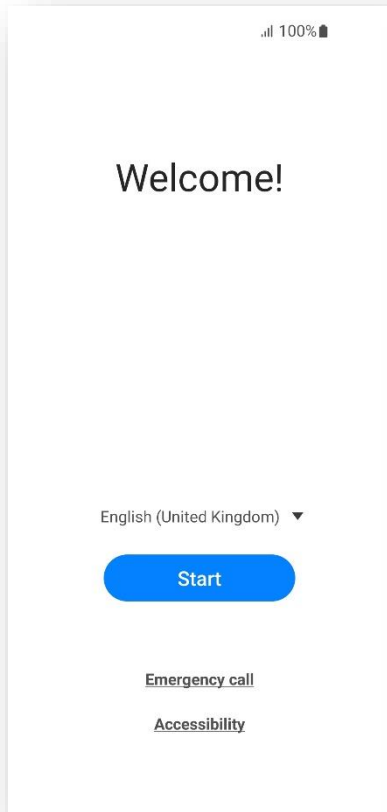
Personal Tab



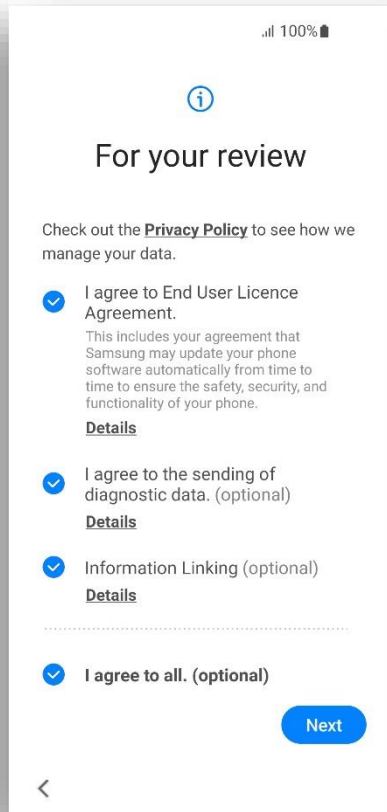
Work Tab



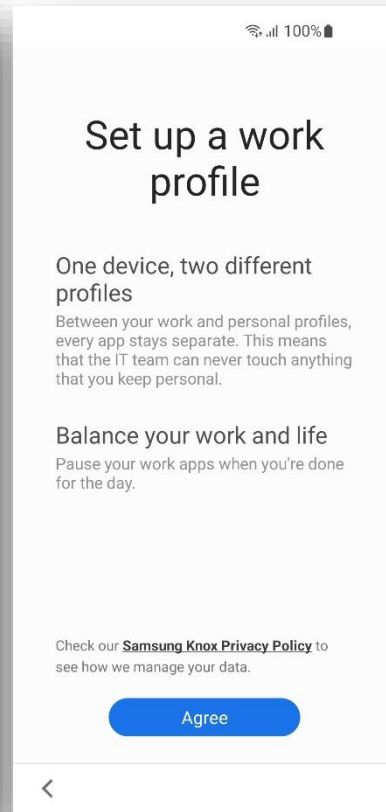
Device is managed by your organization on lock screen



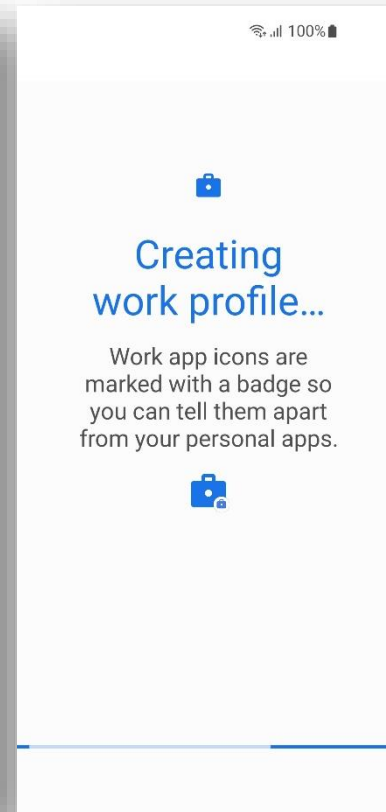
Start



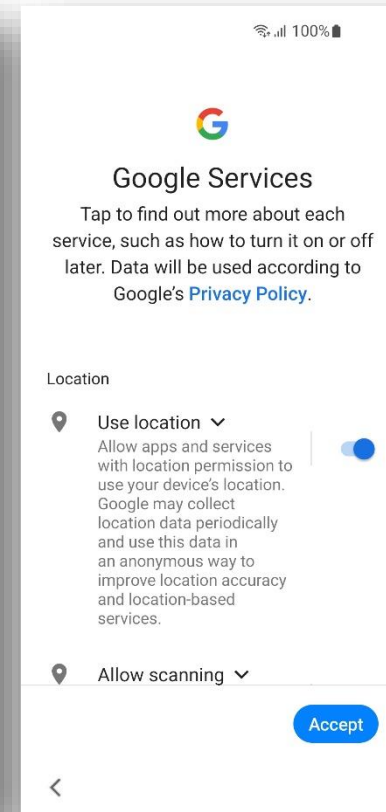
Next



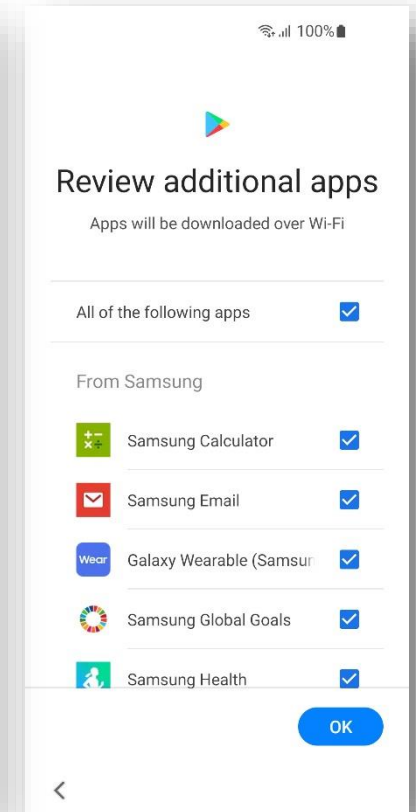
Agree



Wait

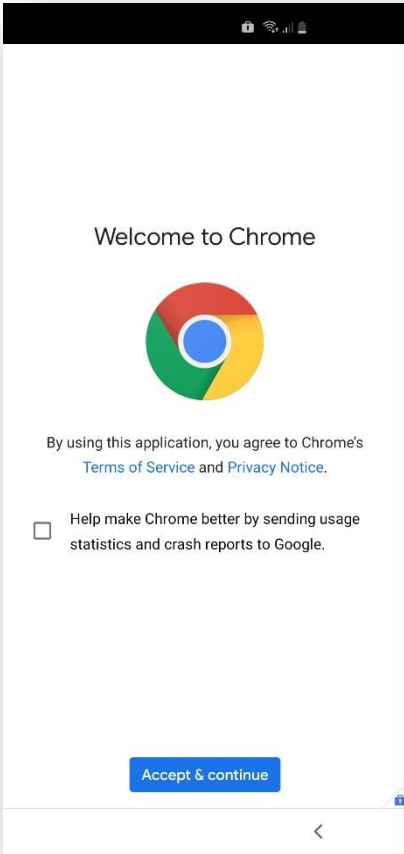


Accept

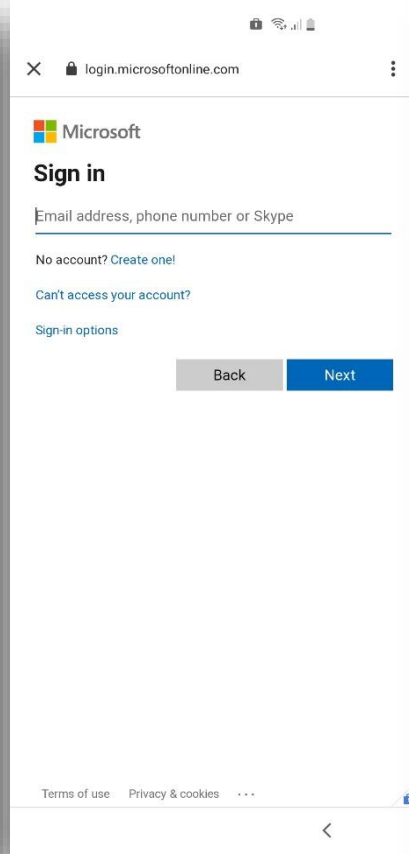


OK

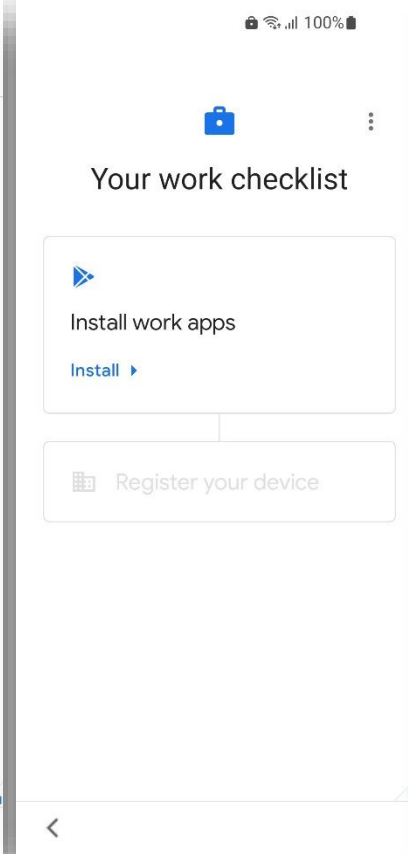
# Android Enterprise: Work Profile on Company Owned Device Enrollment



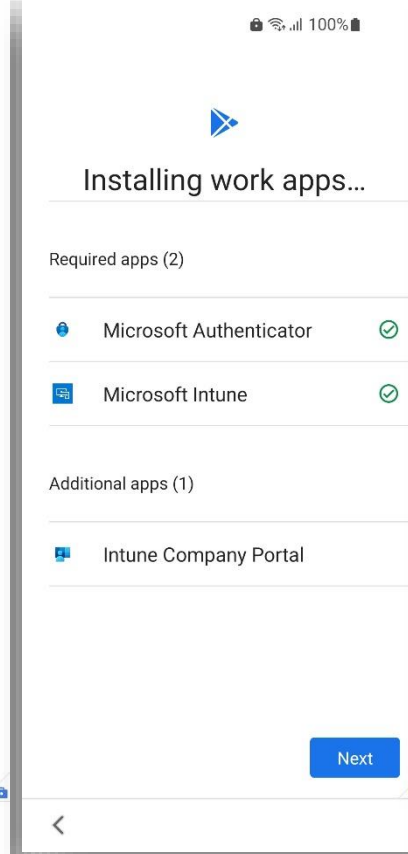
Accept & continue



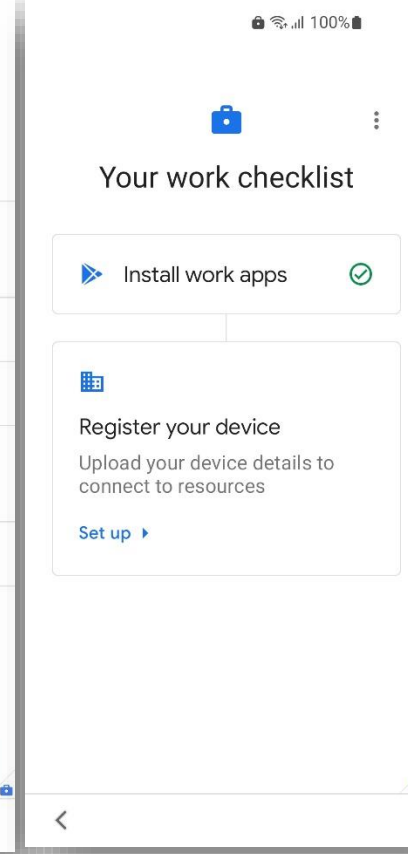
Sign into your Office 365 account, then select Next



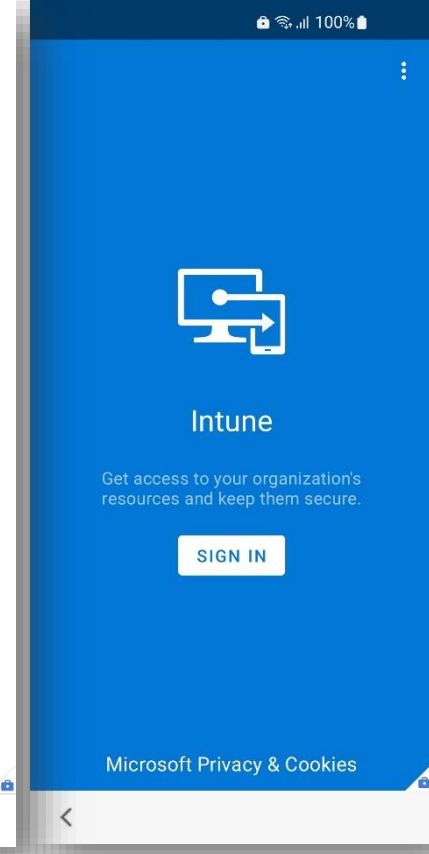
Install



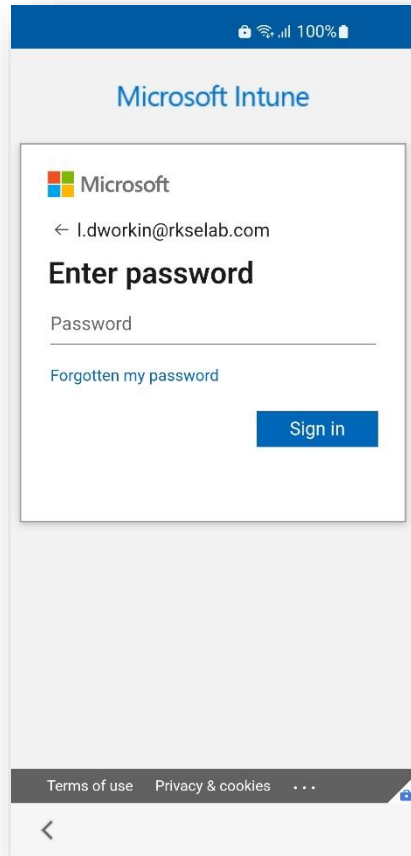
Next



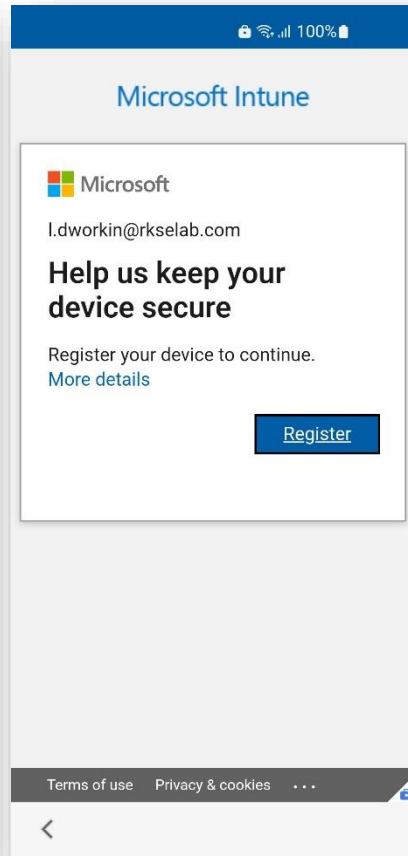
Set Up



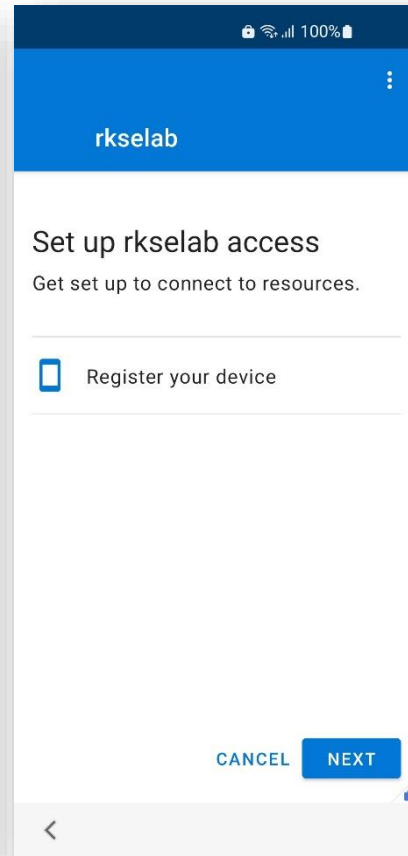
SIGN IN



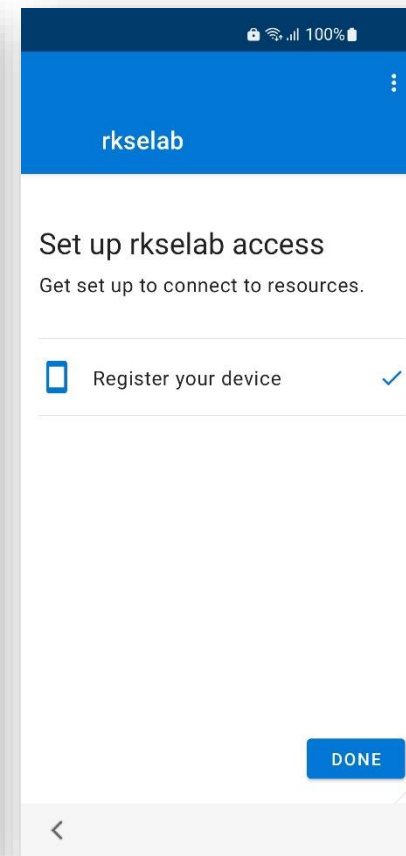
Sign in with your Office 365 account



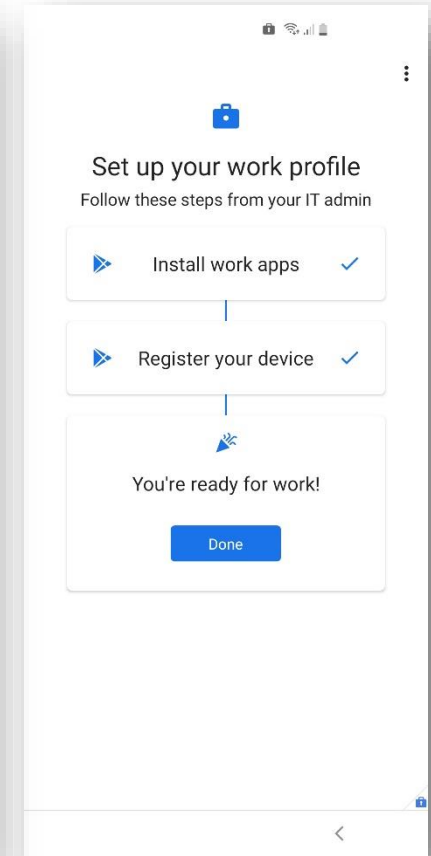
Register



NEXT

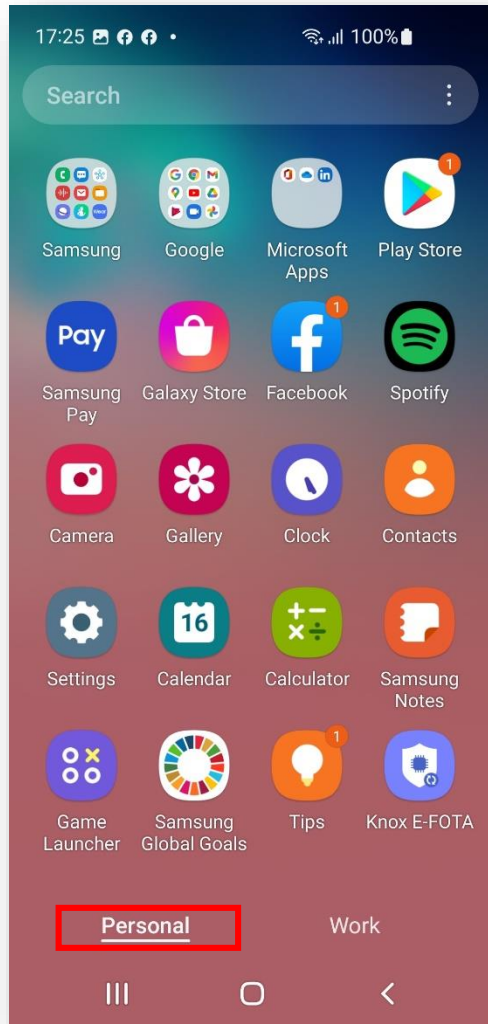


DONE

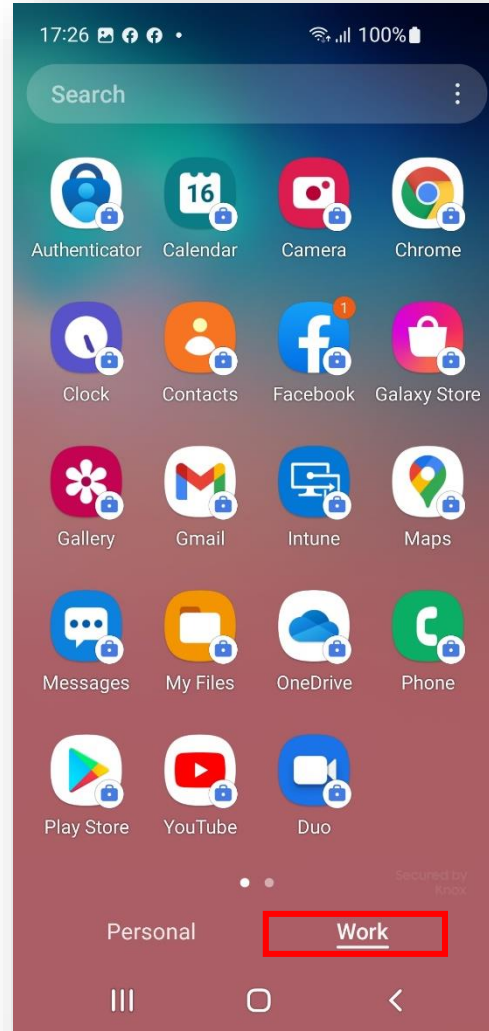


Done

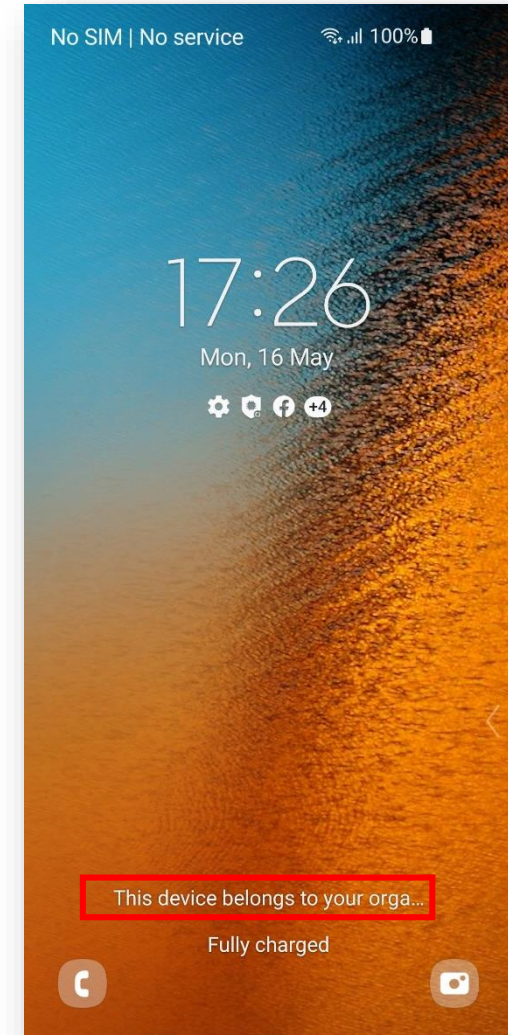
How to tell that Work Profile on a Company Owned Device has been successfully set up:



Personal Tab



Work Tab



Device is managed by your organization on lock screen

# Android Enterprise: Dedicated Device

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

The screenshot shows the Microsoft Endpoint Manager admin center interface. The breadcrumb navigation is "Home > Devices > Android | Android enrollment". The left sidebar contains navigation options: Home, Dashboard, All services, FAVORITES, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled "Android | Android enrollment" and includes a search bar, a "Managed Google Play" section with a link to "Link your managed Google Play account to Intune.", and an "Enrollment Profiles" section. The "Corporate-owned dedicated devices" profile is highlighted with a red box. Below it are other profiles: "Personal devices with work profile", "Corporate-owned, fully managed user devices", and "Corporate-owned devices with work profile (Preview)".

The screenshot shows the Microsoft Endpoint Manager admin center interface for the "Corporate-owned dedicated devices" page. The breadcrumb navigation is "Home > Devices > Android | Android enrollment > Corporate-owned dedicated devices". The left sidebar is the same as in the previous screenshot. The main content area is titled "Corporate-owned dedicated devices" and includes a "Create profile" button highlighted with a red box, along with "Filter", "Columns", and "Export" options. Below this is a search bar labeled "Search by name" and a table with a "Name" header.

# 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.

**Basics**

Name \* ⓘ Kiosk Profile

Description Optional

Token expiration date \* ⓘ 11/11/2020

Previous Next

**Scope tags**

Configure scope tags for these terms and conditions

Scope tags

Default

+ Select scope tags

Previous Next

**Review + create**

Summary

**Basics**

Name Kiosk Profile

Description --

Token expiration date 11/11/20

**Scope tags**

Default

Previous Create

Home > Devices > Android | Android enrollment >

Corporate-owned dedicated devices

Android enrollment

+ Create profile Filter Columns Export

Create an enrollment profile for Android Enterprise dedicated devices and send a token to who will be enrolling the device. [Learn more](#)

Search by name

Name	Token expiration date
Kiosk Profile	11/11/2020

Kiosk Profile

Use this token or QR code to enroll

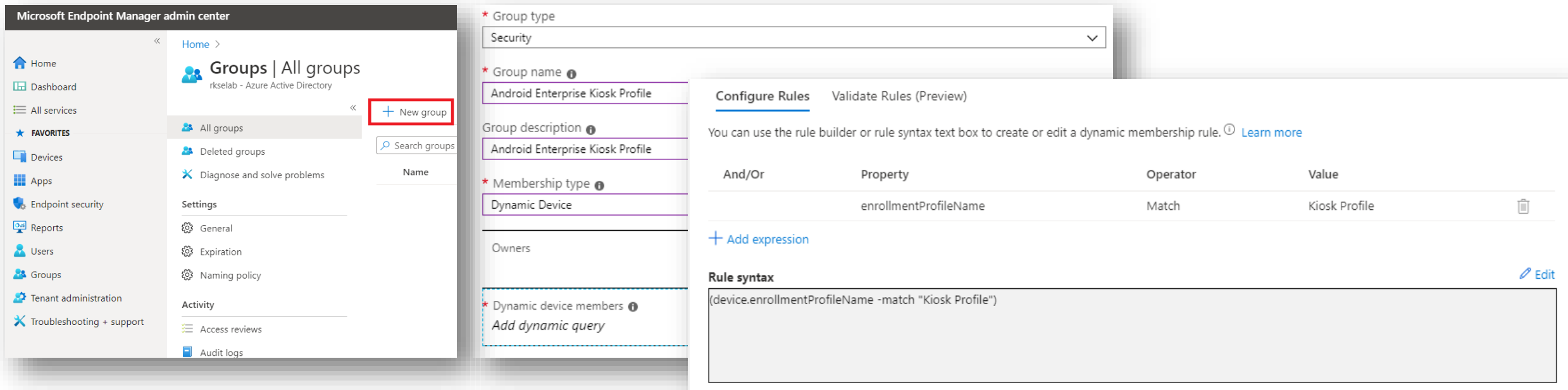
Token HQMHE

Token expiration date 11/11/20, 12:16 PM

# 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 shows the Microsoft Endpoint Manager admin center interface. On the left, the navigation pane includes Home, Dashboard, All services, and FAVORITES. The main area displays the 'Groups | All groups' page for 'rksealab - Azure Active Directory'. A red box highlights the '+ New group' button. The 'New group' dialog is open, showing 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' field contains the following expression: `(device.enrollmentProfileName -match "Kiosk Profile")`. An 'Edit' link is visible next to the rule syntax field.



# Android Enterprise: Dedicated Device

## Add the Managed Home Screen

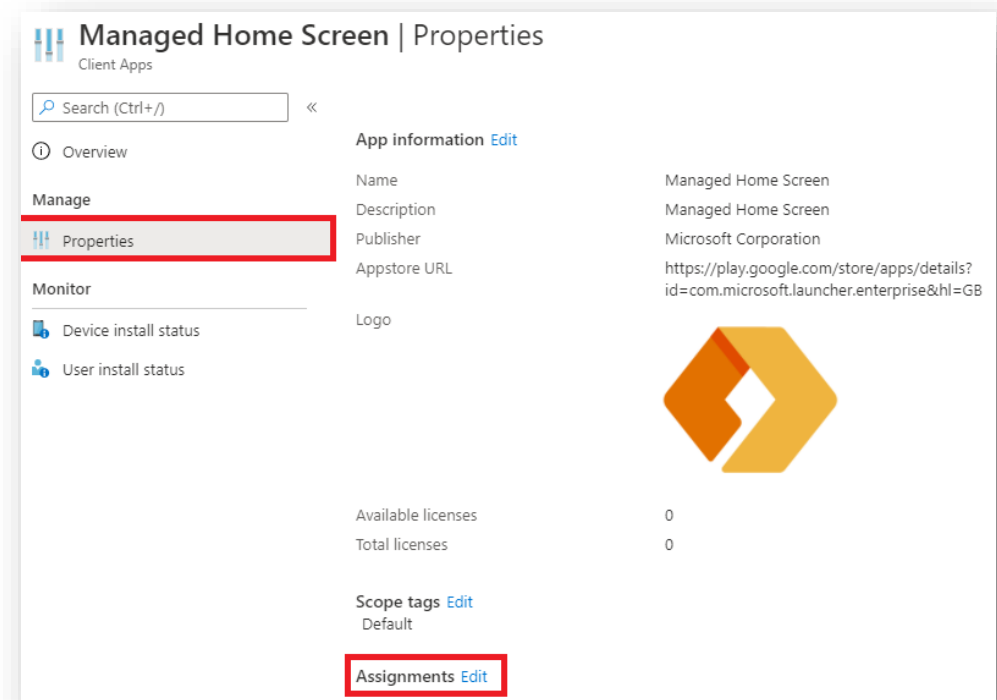
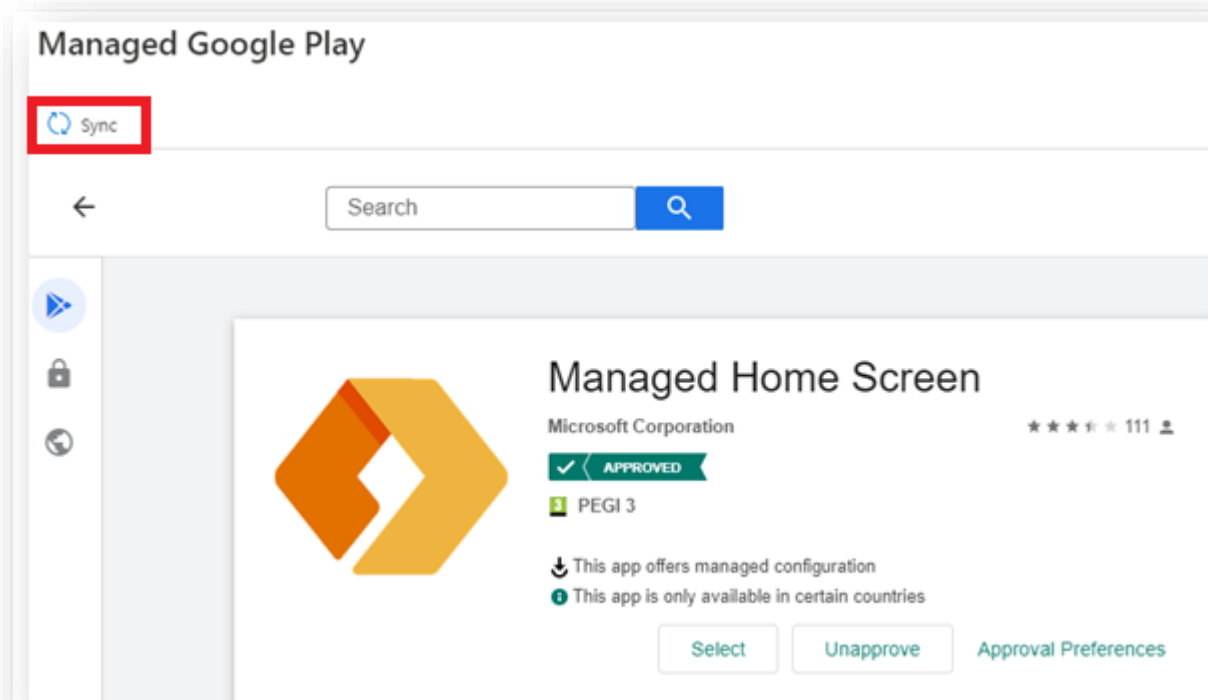
- Within Endpoint Manager, navigate to: Apps > Android apps
- Select Add
- Set the App type to: Managed Google Play app
- Click Select

The screenshot shows the Microsoft Endpoint Manager console. The left-hand navigation pane has the 'Apps' menu item highlighted with a red box. The main content area is titled 'Android | Android apps' and features a '+ Add' button, also highlighted with a red box. Below the 'Add' button is a table of available apps. A modal window titled 'Select app type' is open on the right, with a dropdown menu set to 'Managed Google Play app' and a 'Select' button at the bottom.

Name	Type
Add-On: Samsung	Managed Google Play app
AnyConnect	Managed Google Play app
Boosted - Productivity & Time Tracker	Managed Google Play app
Cisco Webex Meetings	Managed Google Play app
Dropbox: Cloud Storage to Backup, Sy...	Managed Google Play app
Evernote - Organizer, Planner for Not...	Managed Google Play app
F5 Access	Managed Google Play app
Gmail	Managed Google Play app
Google Chrome: Fast & Secure	Managed Google Play app
Intune Company Portal	Managed Google Play app
Knox E-FOTA One	Managed Google Play app
Knox Service Plugin	Managed Google Play app
KNOX Status Samsung	Managed Google Play app
Managed Home Screen	Managed Google Play app
Messages	Managed Google Play app

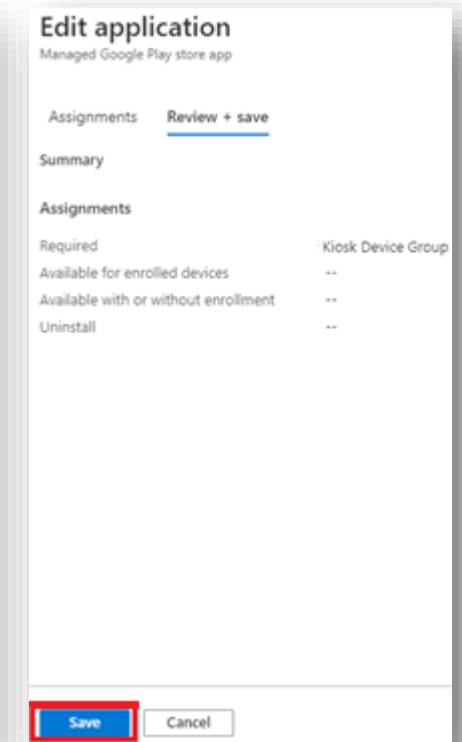
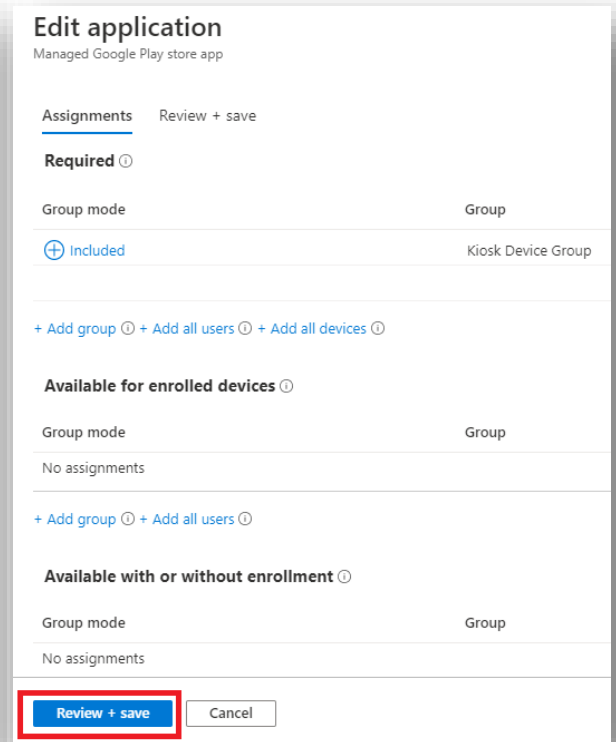
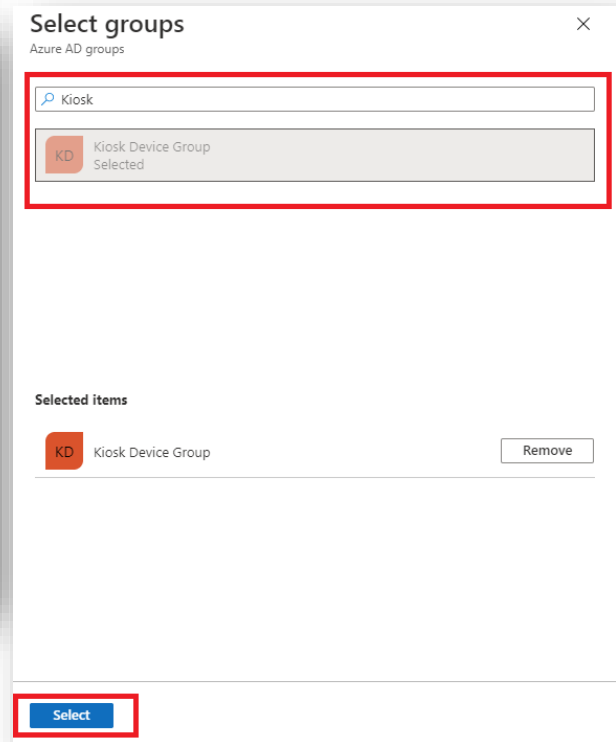
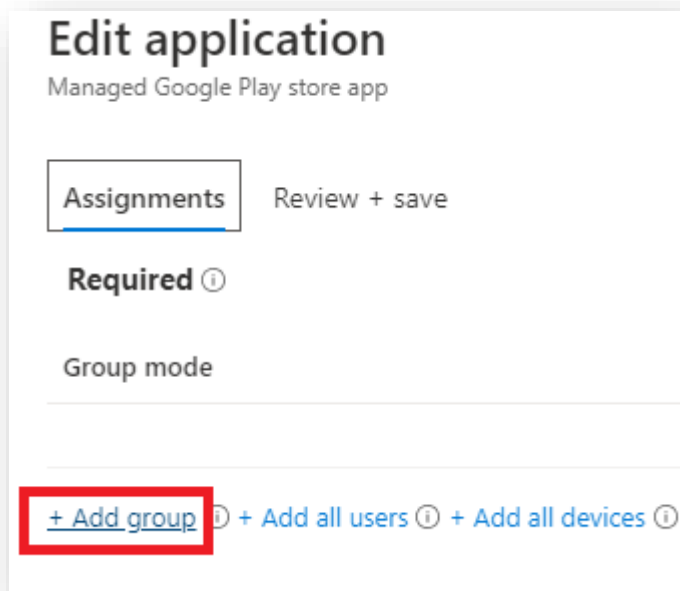
# Android Enterprise: Dedicated Device

- 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



# 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

The screenshot shows the Microsoft Endpoint Manager admin center interface. The left-hand navigation pane has 'Devices' highlighted with a red box. The main content area is titled 'Android | Configuration profiles'. A search bar is present with the text 'Search (Ctrl+ /)'. To the right of the search bar, a '+ Create profile' button is highlighted with a red box. Below the search bar, there is a table with columns for 'Profile Name', 'Platform', and 'Profile'. The 'Configuration profiles' link in the left-hand pane is also highlighted with a red box.

The screenshot shows the 'Create a profile' form. The 'Platform' dropdown menu is set to 'Android Enterprise'. The 'Profile' dropdown menu is set to 'Device restrictions'. Below these fields, there is a section for 'Device restrictions' with a description: 'Enable or disable device features, run apps on dedicated devices, cor... This profile is for fully managed, dedicated, and corporate-owned wo...'. At the bottom of the form, a 'Create' button is highlighted with a red box.

## 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' step of the setup process. 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.

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

# 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

**Device restrictions**  
Android Enterprise

✓ Basics ✓ Configuration settings

Scope tags

Scope tags

Default

+ Select scope tags

Previous **Next**

Home > Devices > Android | Configuration profiles >

**Device restrictions**  
Android Enterprise

✓ Basics ✓ Configuration settings ✓ Scope tags **4 Assignments** 5 Review

Included groups

Assign to Selected groups

Selected groups

No groups selected

+ Select groups to include

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**

**Select groups to include**  
Azure AD Groups

Kiosk

Kiosk Device Group Selected

Selected items

Kiosk Device Group Remove

**Select**

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

**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

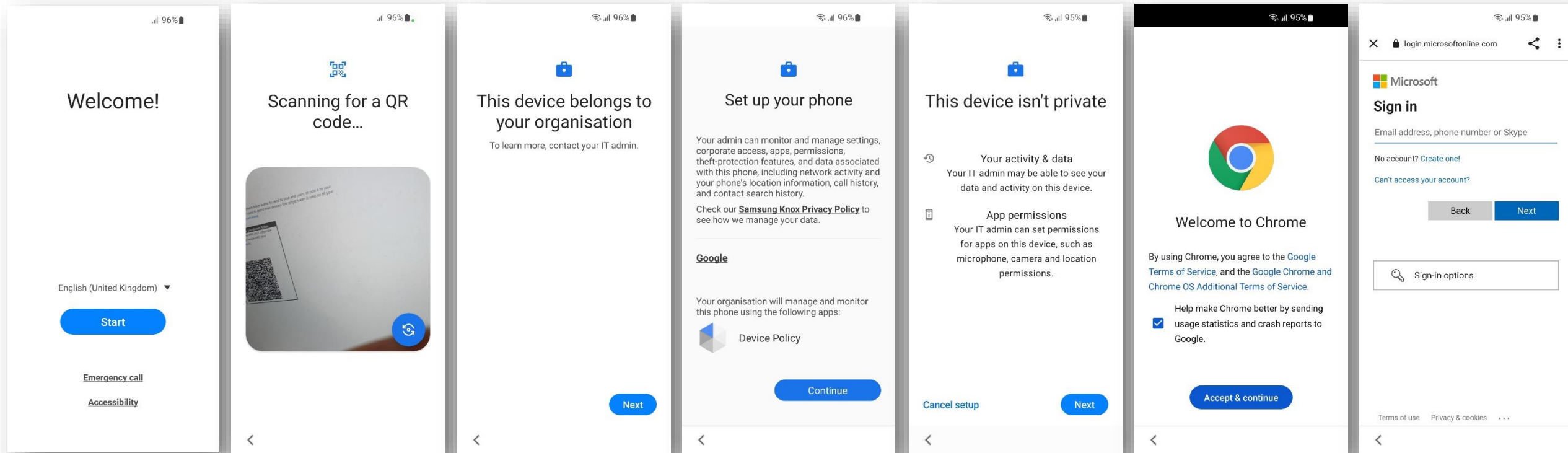
Kiosk mode Multi-app

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

Leave kiosk mode Enable

Previous **Create**

# Android Enterprise: Dedicated Device Enrollment (with QR code 1/2)



Tap anywhere on the screen 6 times

Scan the enrollment QR code

Next

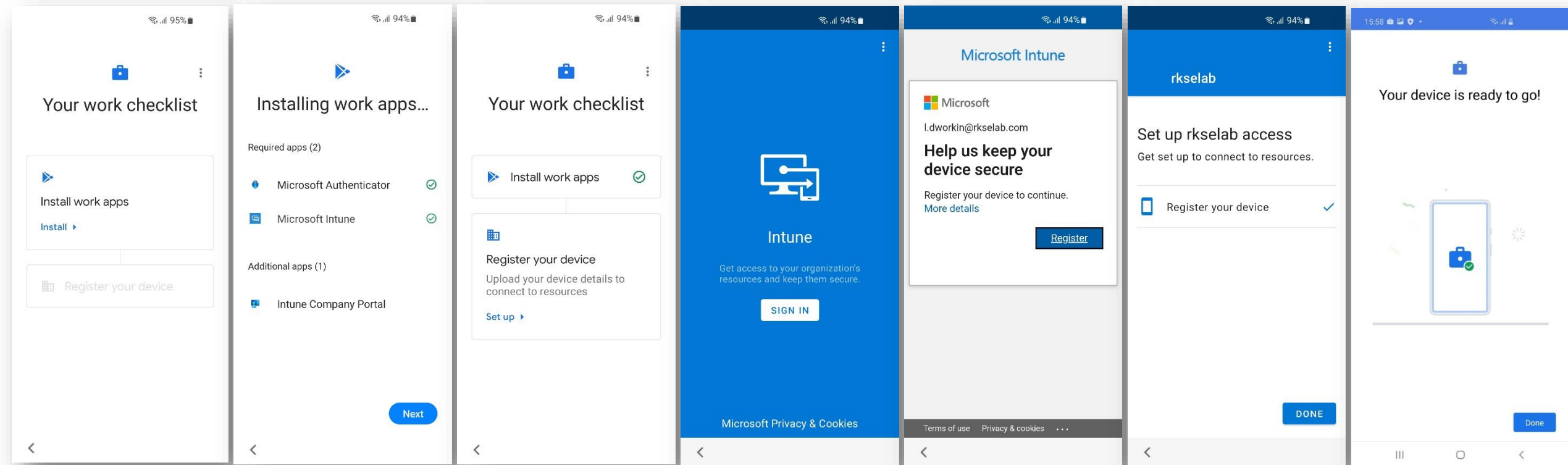
Continue

Next

Accept & continue

Sign in with your Office 365 account

# Android Enterprise: Dedicated Device Enrollment (with QR code 2/2)



Install

Next

Set Up

**SIGN IN  
and enter your  
Office 365  
password**

Register

DONE

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 [FREE, or \$ for advanced options such as Dual DAR]

Knox Platform for Enterprise : Standard Edition offers free additional policies you can use to provide enhanced security, manageability and usability over your Samsung device fleet, running Android Enterprise 8.0 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 illustrates the process of adding a Managed Google Play app in the Endpoint Manager console. The main interface shows the 'Android | Android apps' section with the 'Add' button highlighted. 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 is visible, with the 'Select' button highlighted. A second modal window shows the 'Knox Service Plugin' app card, which is marked as 'APPROVED' and includes a 'Select' button.

Home > Apps > Android | Android apps

Search (Ctrl+/) << + Add Refresh Filter Export Columns

Filters applied: Platform, App type

Search by name or publisher

Name ↑↓ Type

Select app type

Create app

App type

Managed Google Play app

Managed Google Play app

Search the built-in managed Google Play store to find and add apps for Android Enterprise devices.

Learn more

Select Cancel

Knox Service Plugin

Samsung Electronics Co., Ltd. ★★★★★ 118

APPROVED

PEGI 3

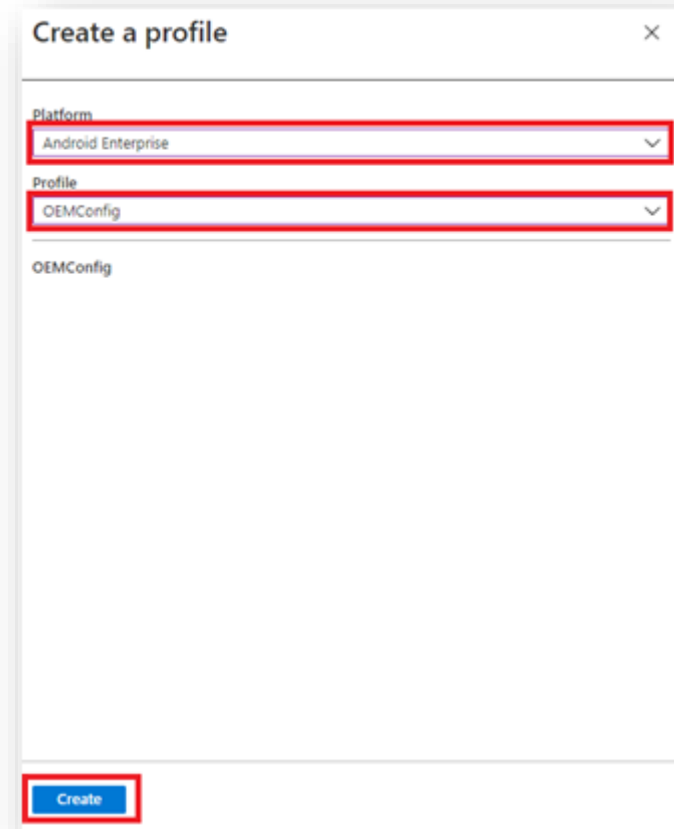
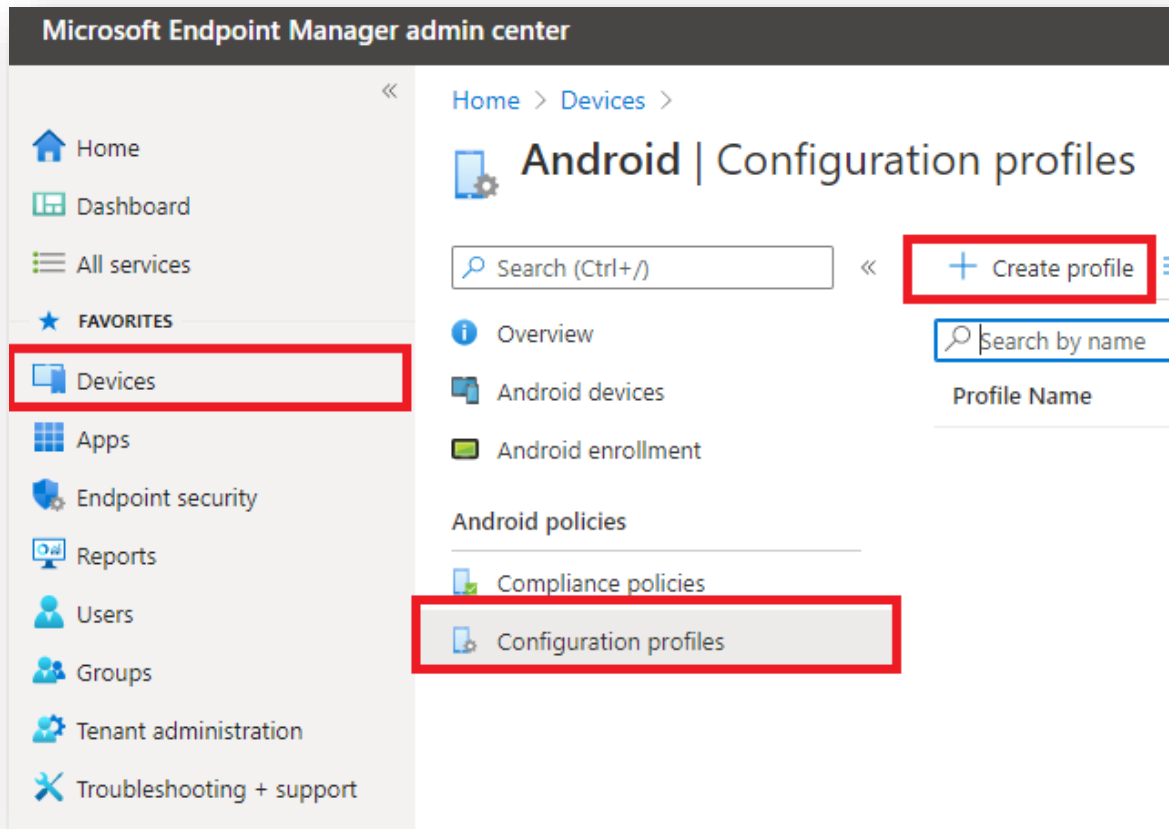
This app offers managed configuration

This app is only available in certain countries

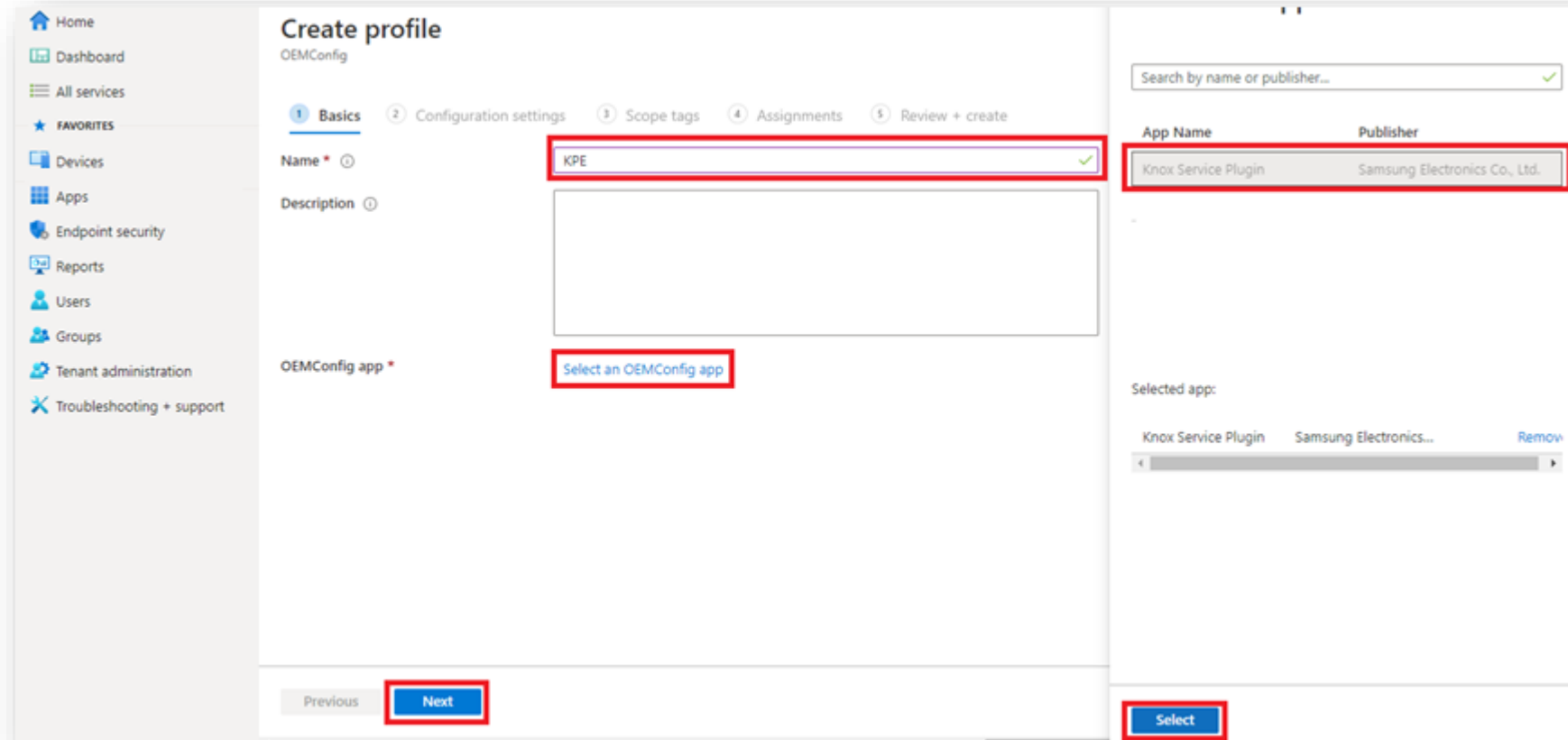
Select Unapprove Approval Preferences

# 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**



- 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...

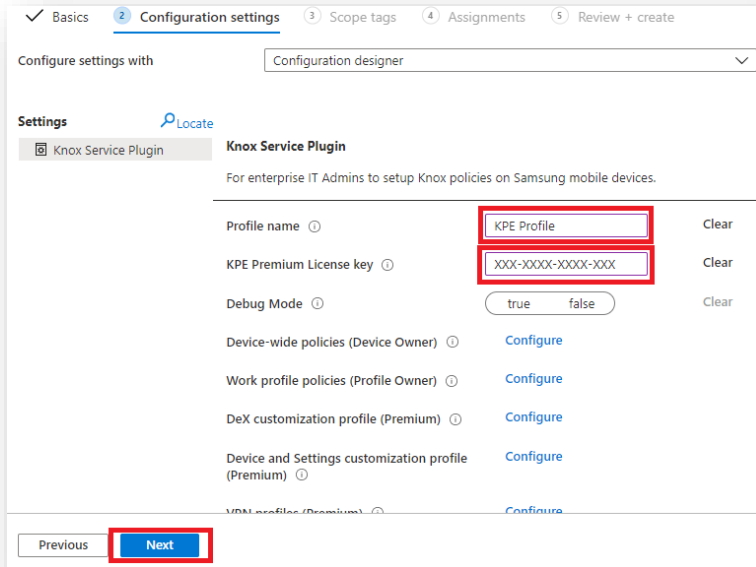
App Name	Publisher
Knox Service Plugin	Samsung Electronics Co., Ltd.

Selected app:

Knox Service Plugin Samsung Electronics...

# 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



Configuration 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 License key  Clear

Debug Mode  true  false Clear

Device-wide policies (Device Owner) [Configure](#)

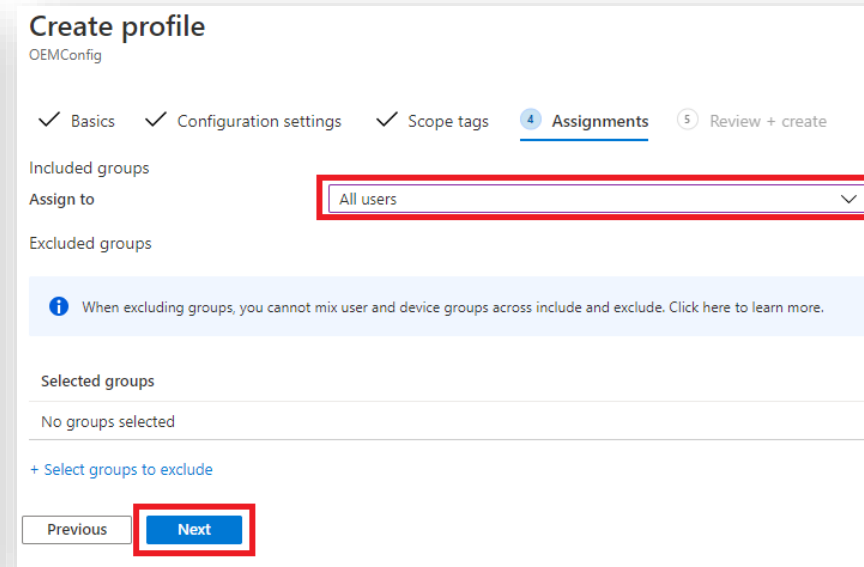
Work profile policies (Profile Owner) [Configure](#)

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

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

VDN profiles (Premium) [Configure](#)

[Previous](#) [Next](#)



**Create profile**

OEMConfig

[✓ Basics](#) [✓ Configuration settings](#) [✓ Scope tags](#) [4 Assignments](#) [5 Review + create](#)

Included groups

Assign to

Excluded groups

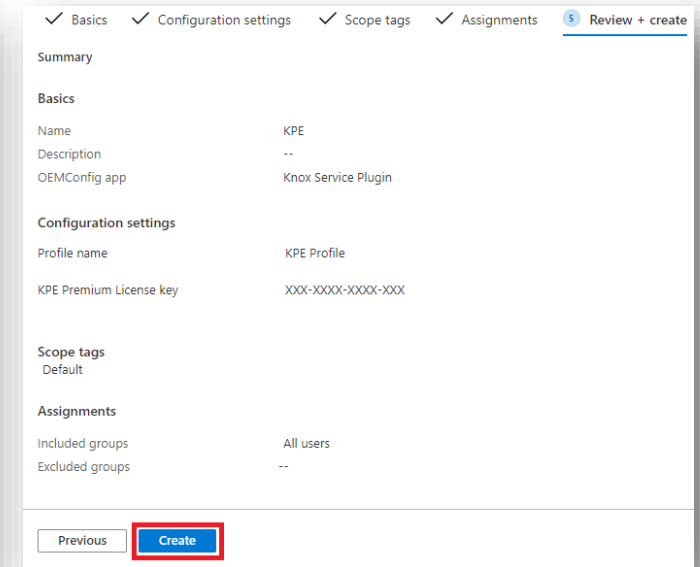
**i** When excluding groups, you cannot mix user and device groups across include and exclude. [Click here to learn more.](#)

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 3.0 of this document.**

**Thank you!**

