

# Intune & Knox Platform for Enterprise

June 2022  
Samsung R&D Centre UK  
(SRUK)

# Agenda

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

# Intune Collateral & Contacts

**Contacts:**

[sruk.product@samsung.com](mailto:sruk.product@samsung.com)

**Knowledge Base:**

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

# Pre-Requisites

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

Microsoft Endpoint Manager admin center

The screenshot shows the Microsoft Endpoint Manager admin center interface. On the left, there's a navigation menu with various options like Home, Dashboard, All services, Favorites, Devices (which is highlighted with a red box), Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. In the center, the user is on the 'Android | Android enrollment' page under the 'Devices' section. The page includes a search bar, an 'Overview' section, and a 'Prerequisites' section. The 'Prerequisites' section contains a 'Managed Google Play' button, which is also highlighted with a red box.

Managed Google Play

Android enrollment

Disconnect

Status: Not Setup

Organization: Not Available

Google Account: 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.](#)

This screenshot shows the 'Managed Google Play' configuration page. It displays basic information about the status (Not Setup) and organization (Not Available). It also shows that no Google account is available. Below this, there's a note about connecting Intune to a managed Google Play account. Two steps are outlined: 1. Granting Microsoft permission to send user and device information to Google, with a checked 'I agree.' checkbox. 2. Connecting the Intune tenant to an administrative Google account. A prominent blue button at the bottom right says '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

The image consists of three screenshots from the Google Play Admin console:

- Screenshot 1: Welcome Screen**  
The first screenshot shows a teal-colored landing page with the heading "Bring Android to Work" and a large "Get started" button. In the bottom left corner, there is an icon of a briefcase.
- Screenshot 2: Contact Details Step**  
The second screenshot shows the "Contact details" step of the setup process. It asks for details about key contacts, specifically a Data Protection Officer and an EU Representative. Both sections have "Name", "Email", and "Phone" fields. A note at the top states: "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." Below the fields is a checkbox for agreeing to the "Managed Google Play agreement". At the bottom right are "Previous" and "Confirm" buttons.
- Screenshot 3: Setup Complete Screen**  
The third screenshot shows a confirmation screen with the message "Set up complete" and "Thanks for choosing Android enterprise." It features a "Complete Registration" button.

# Android Enterprise Deployment Modes

## Deployment Modes

Android Enterprise can be deployed in the following 5 deployment modes

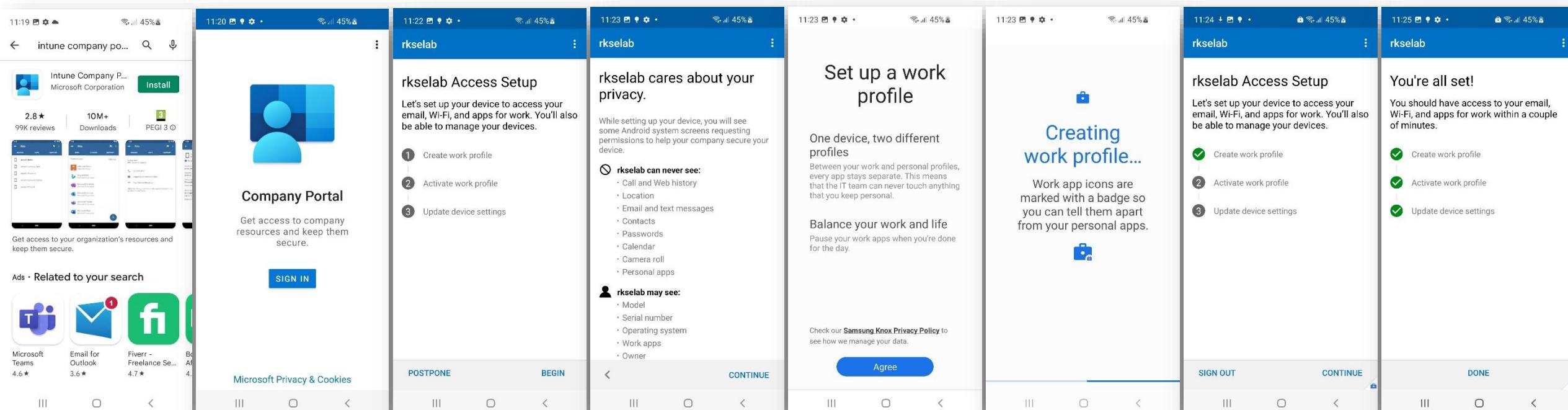
1. Work Profile [*formerly known as Profile Owner or PO*]
2. Fully Managed Device [*formerly known as Device Owner or DO*]
3. Fully Managed Device with a Work Profile [*formerly known as Company Owned Managed Profile or COMP*] on Android 10 or before
4. Work Profile on Company Owned Device or WPC on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

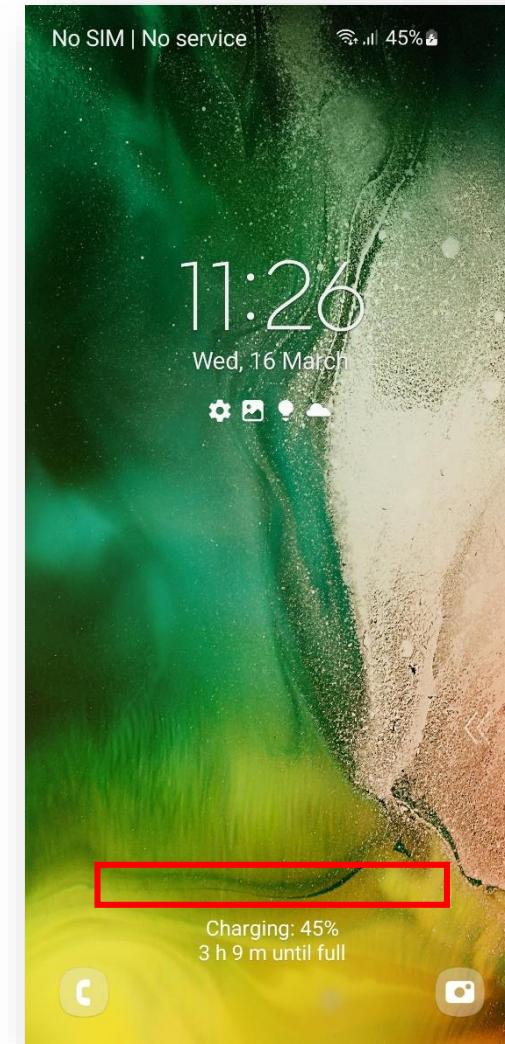
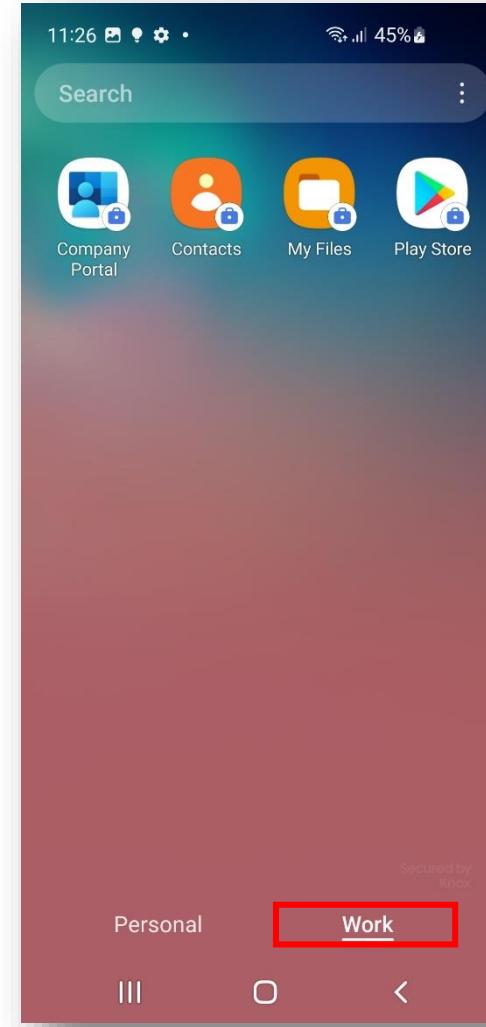
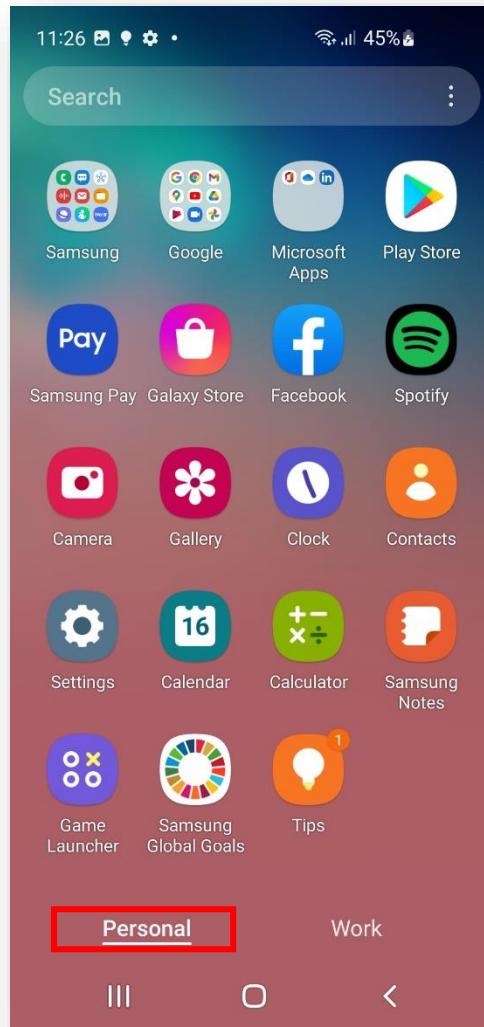
Creating work profile...

CONTINUE

DONE

# Android Enterprise: Work Profile Enrollment

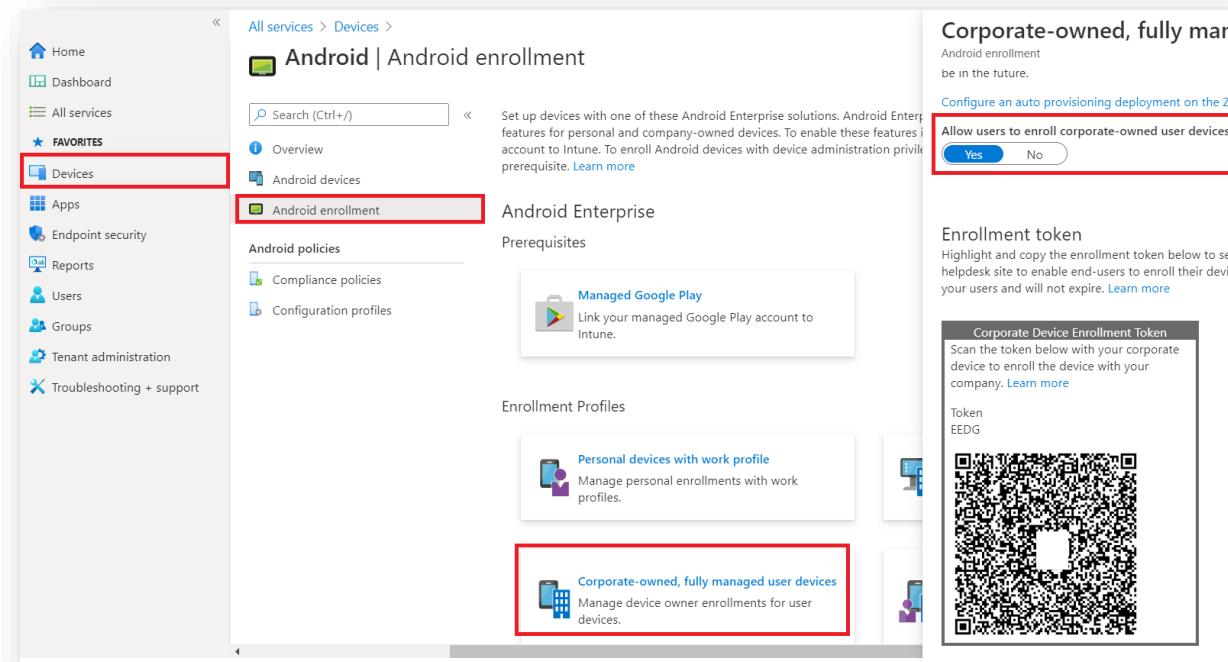
How to tell that Work Profile has been successfully set up:



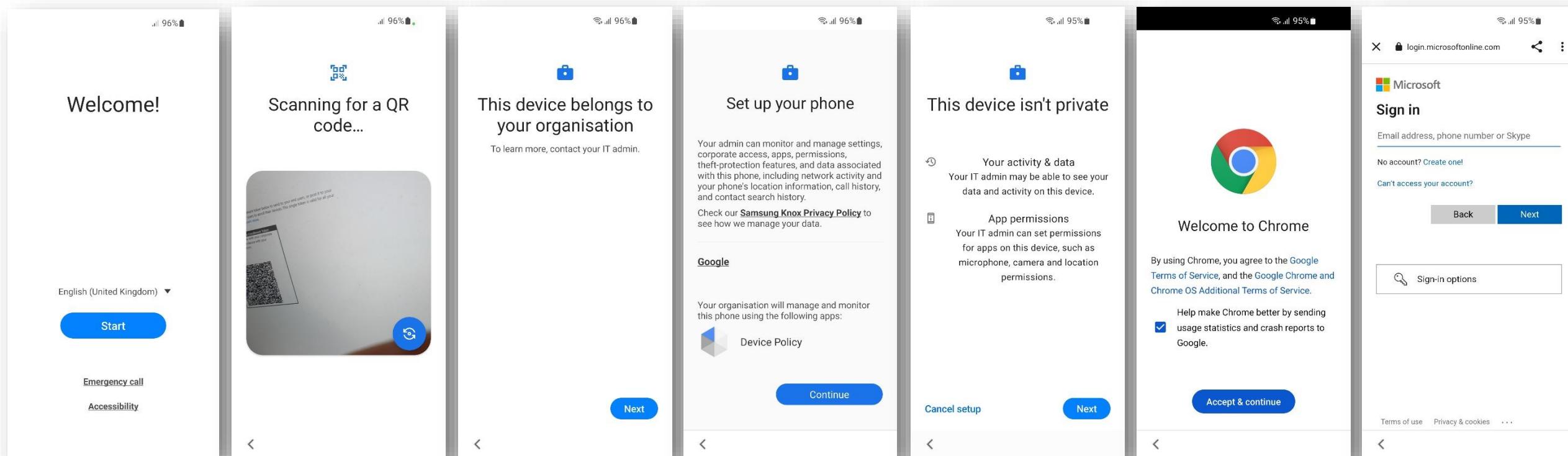
No mention of device belonging  
to your organization  
on lock screen

# 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

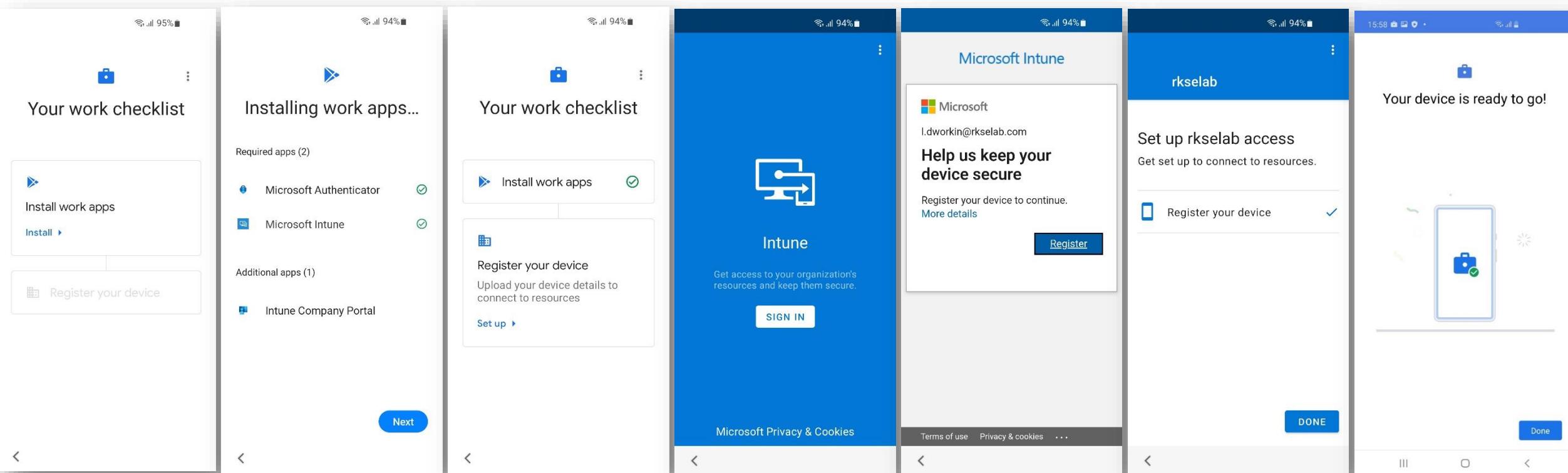
Continue

Next

Accept & continue

Sign in with your  
Office 365 account

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



Install

Next

Set Up

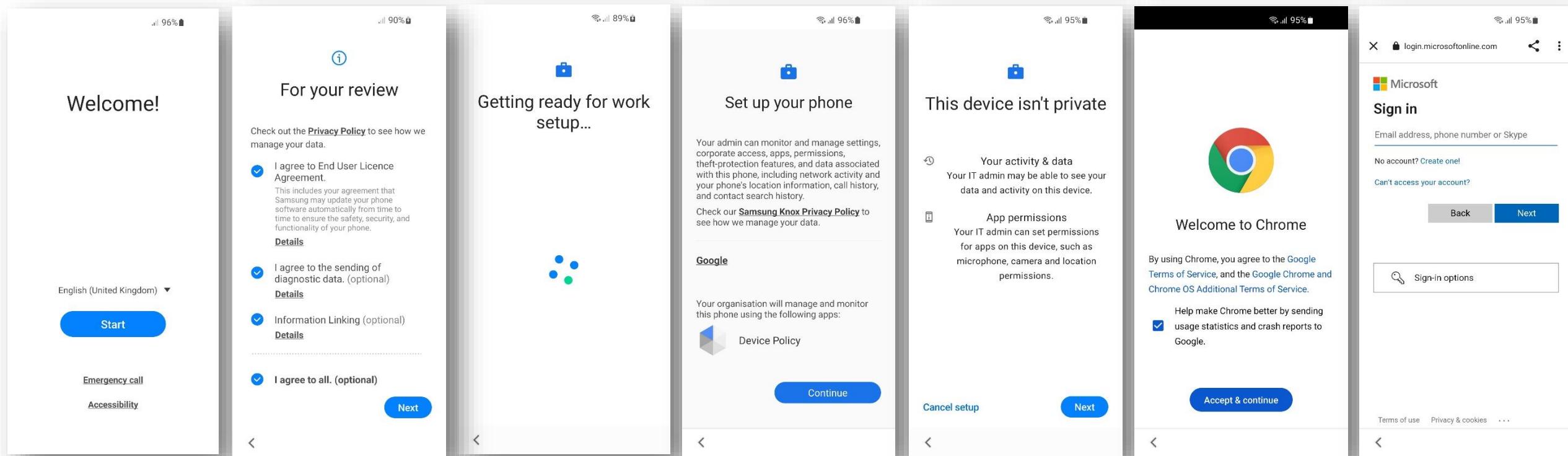
SIGN IN  
and enter your  
Office 365  
password

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...

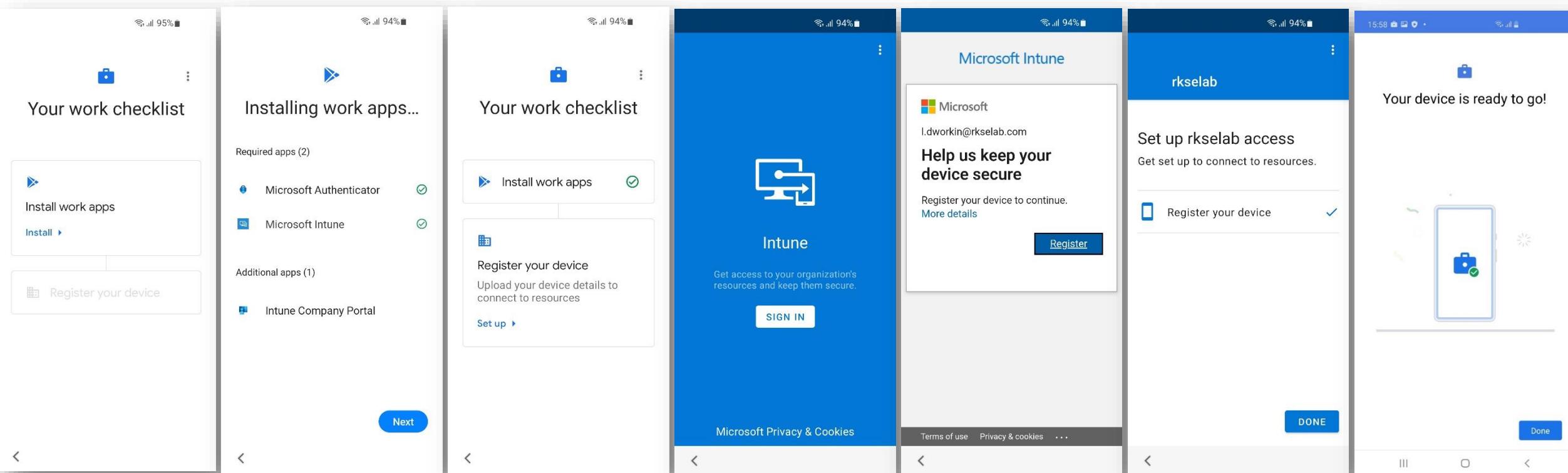
**Continue**

**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

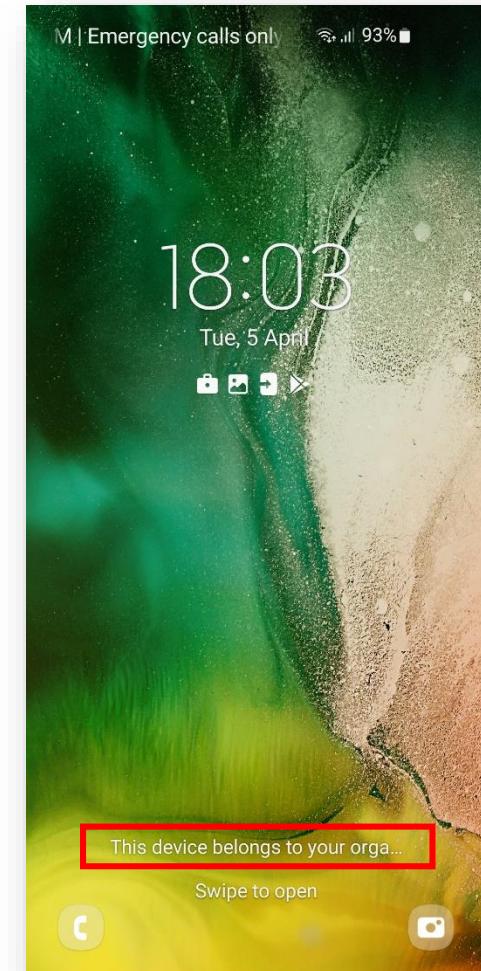
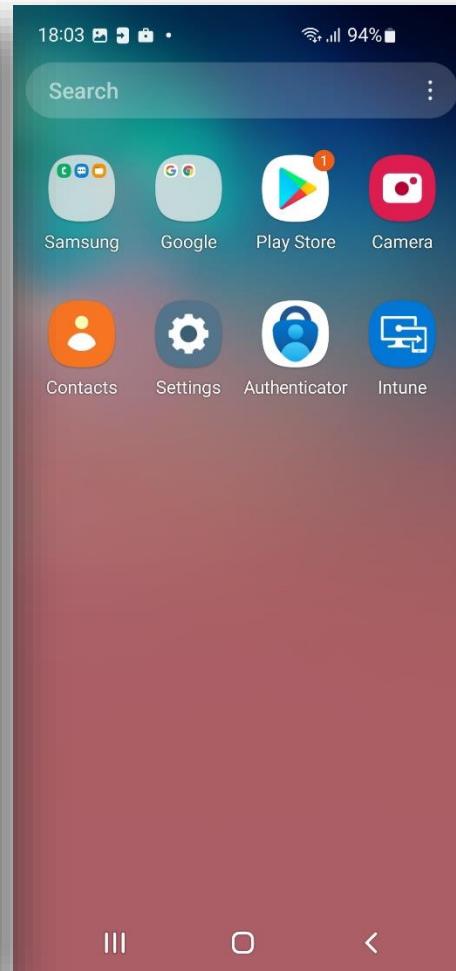
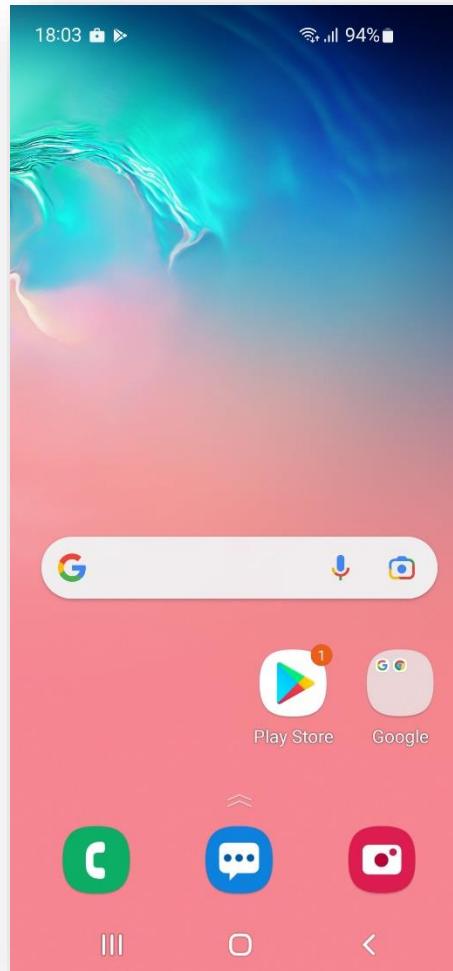
Register

DONE

Done

# Android Enterprise: Fully Managed Device Enrollment (QR code or KME)

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

The image displays two side-by-side screenshots of the Microsoft Endpoint Manager admin center interface.

**Left Screenshot:** Shows the "Android | Android enrollment" page. The left sidebar has a red box around the "Devices" item. The main content area shows "Android Enterprise Prerequisites" with a "Managed Google Play" section. Below it are three enrollment profiles: "Personal devices with work profile", "Corporate-owned dedicated devices", and "Corporate-owned, fully managed user devices". The third option is highlighted with a red box.

**Right Screenshot:** Shows the "Corporate-owned devices with work profile" page under "Android enrollment". The left sidebar has a red box around the "Create profile" button. The main content area shows a search bar and a message stating "No profiles found."

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

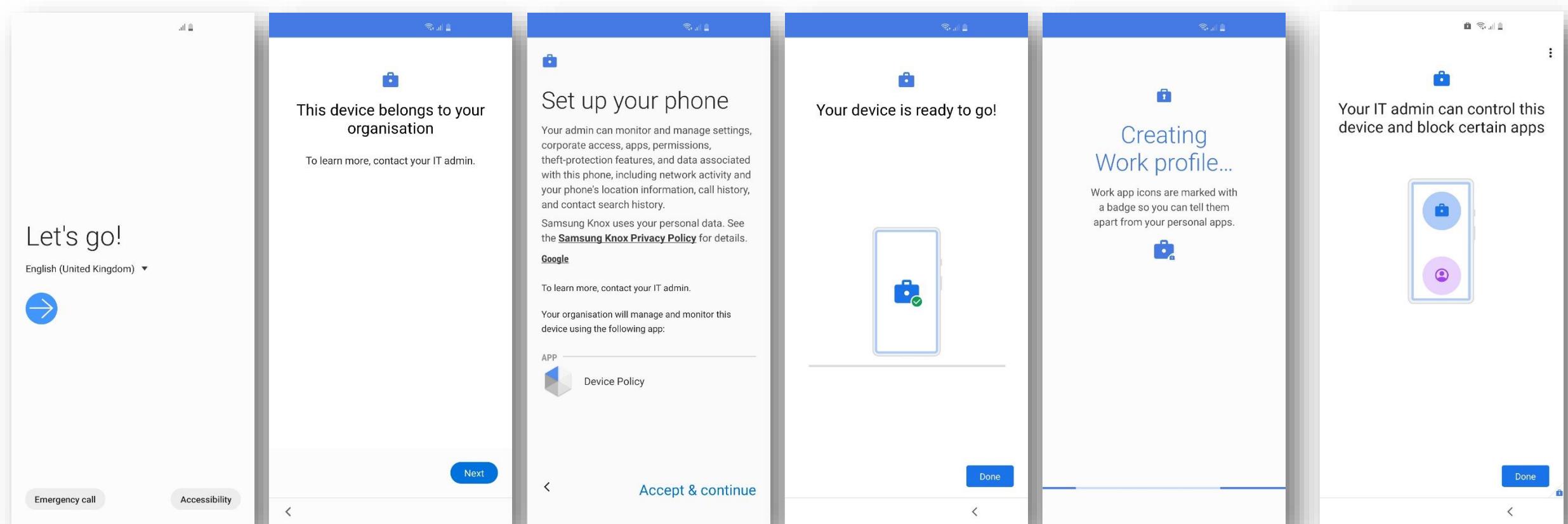
- Enter a Name, select Next
- Select a scope tag (optional) select Next
- Select Create
- To view your Token and QR code, select your profile in the profiles list
- If you're using KME, you can use the Token to simplify the enrollment steps and force the user to enroll into your tenant. Copy and paste 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 screenshot illustrates the three-step enrollment process for creating a work profile:

- Step 1: Basics**  
Name: Fully Managed with a Work Profile  
Description: Optional
- Step 2: Scope tags**  
Configure scope tags for these terms and conditions  
Scope tags: Default  
+ Select scope tags
- Step 3: Review + create**  
Summary  
**Basics**  
Name: Fully Managed with a Work Profile  
Description: --  
**Scope tags**  
Default  
QR code for enrollment

Below the enrollment steps, the "Corporate-owned devices with work profile" dashboard is shown, listing the created profile "Fully Managed with a Work Profile".

# Android Enterprise: Fully Managed with a Work Profile Enrollment (QR code 1/3)



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

Next

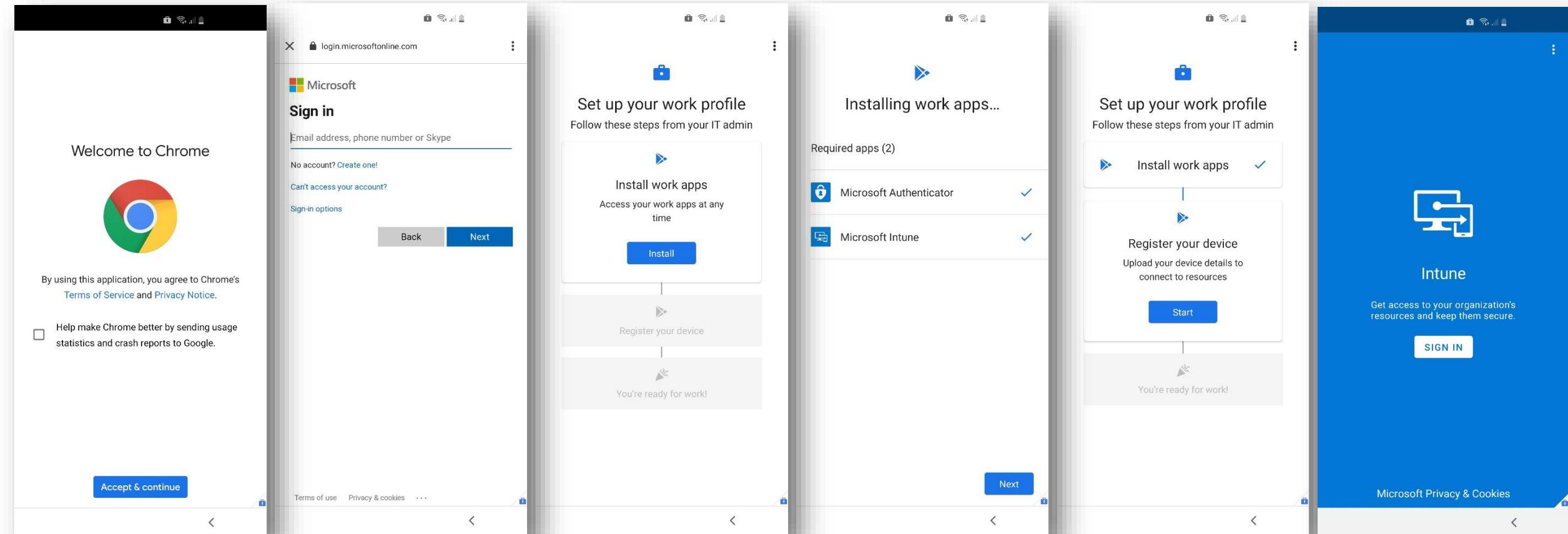
Accept & continue

Done

Wait

Done

# Android Enterprise: Fully Managed with a Work Profile Enrollment (QR code 2/3)



**Accept & continue**

**Sign into your  
Office 365 account,  
then select Next**

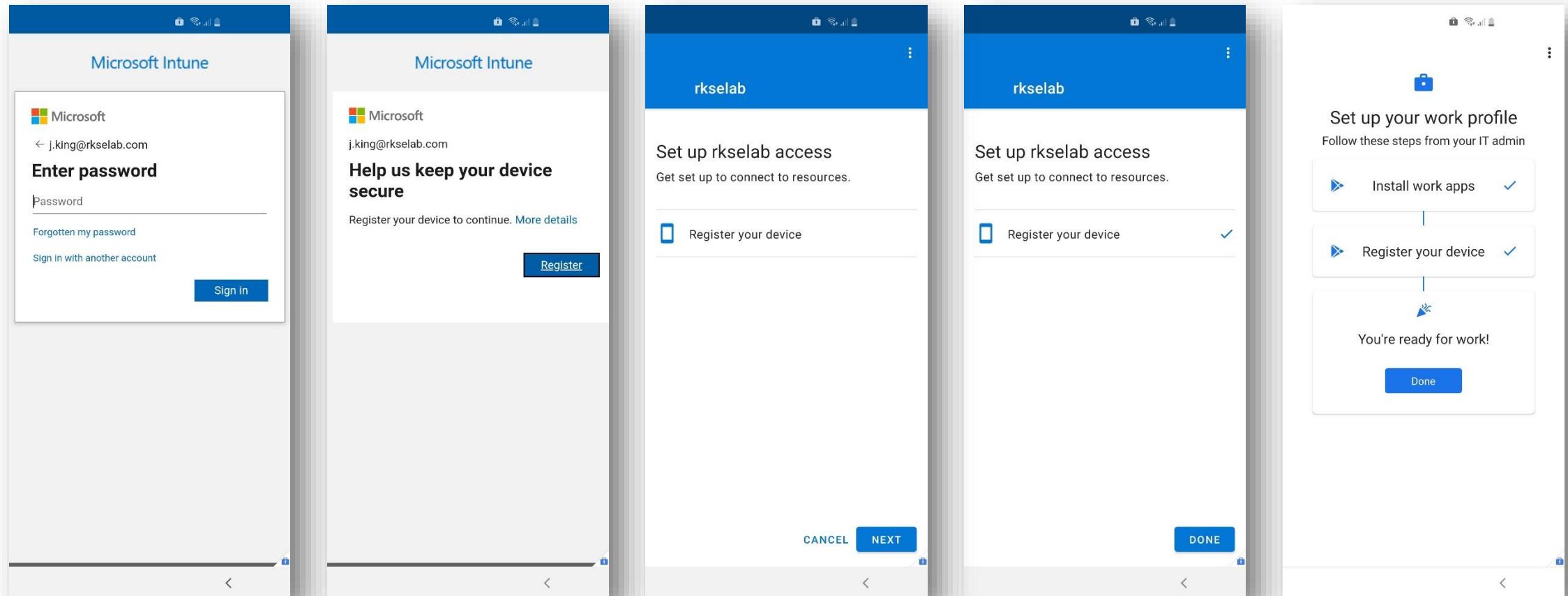
**Install**

**Next**

**Start  
or  
Set Up**

**SIGN IN**

# Android Enterprise: Fully Managed with a Work Profile Enrollment (QR code 3/3)



Sign in with your  
Office 365 account

Register

NEXT

DONE

Done

# Android Enterprise: Fully Managed with a Work Profile Enrollment (KME 1/4)



Let's go!

English (United Kingdom) ▾



Emergency call



Check out some info to get started

Your data will be used according to our [Privacy Policy](#).

- End User Licence Agreement  
[Details](#)
  - Sending of Diagnostic Data (optional)  
[Details](#)
  - Information Linking (optional)  
[Details](#)
  - Receipt of Marketing Information (optional)  
[Details](#)
- I have read and agree to all of the above.

Next



Choose a Wi-Fi network

- guest
- Koti\_C0B4
- setup
- srguest
- srtest

This phone is protected by Knox Cloud Service.  
To continue setup, connect to a Wi-Fi or mobile network.

OK



Updating...

Updating Knox Enrolment Service... 10%



This device belongs to your organisation

To learn more, contact your IT admin.

Next



Getting ready for work setup...



Click arrow to start

Next

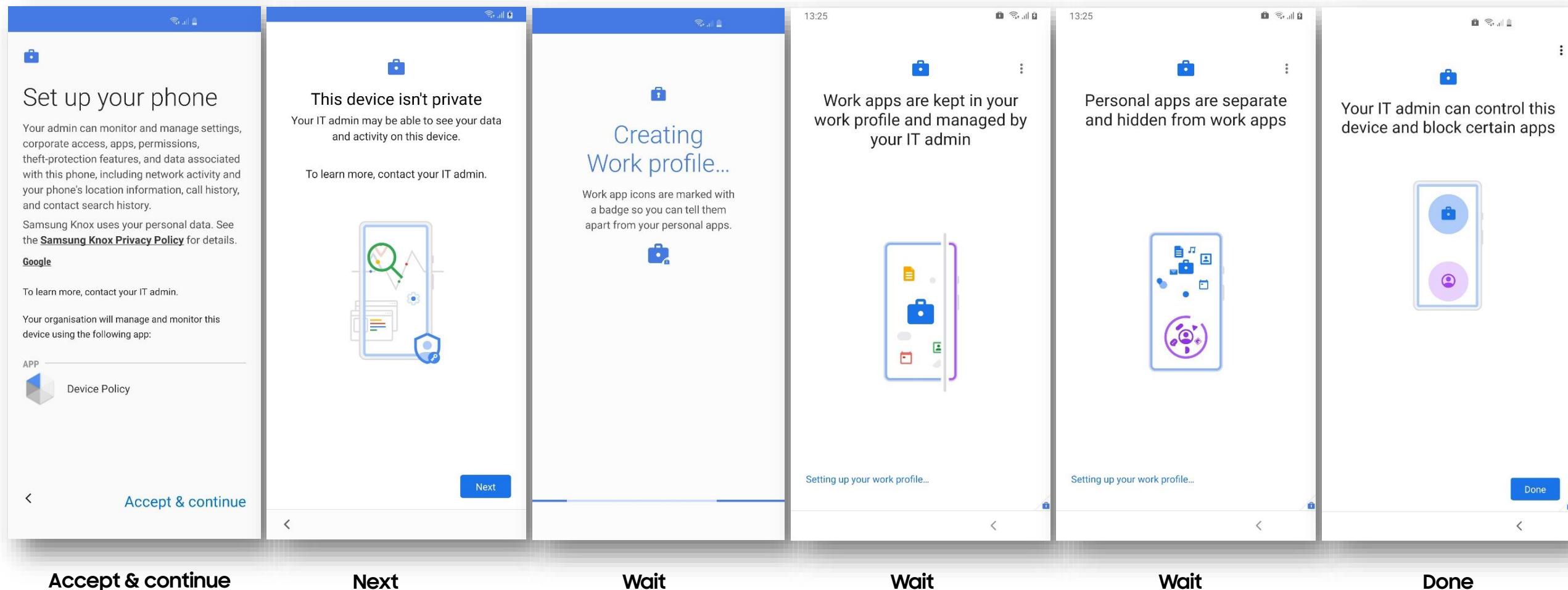
OK and connect to Wi-Fi

Wait for KME to update

Next

Get ready

# Android Enterprise: Fully Managed with a Work Profile Enrollment (KME 2/4)



Accept & continue

Next

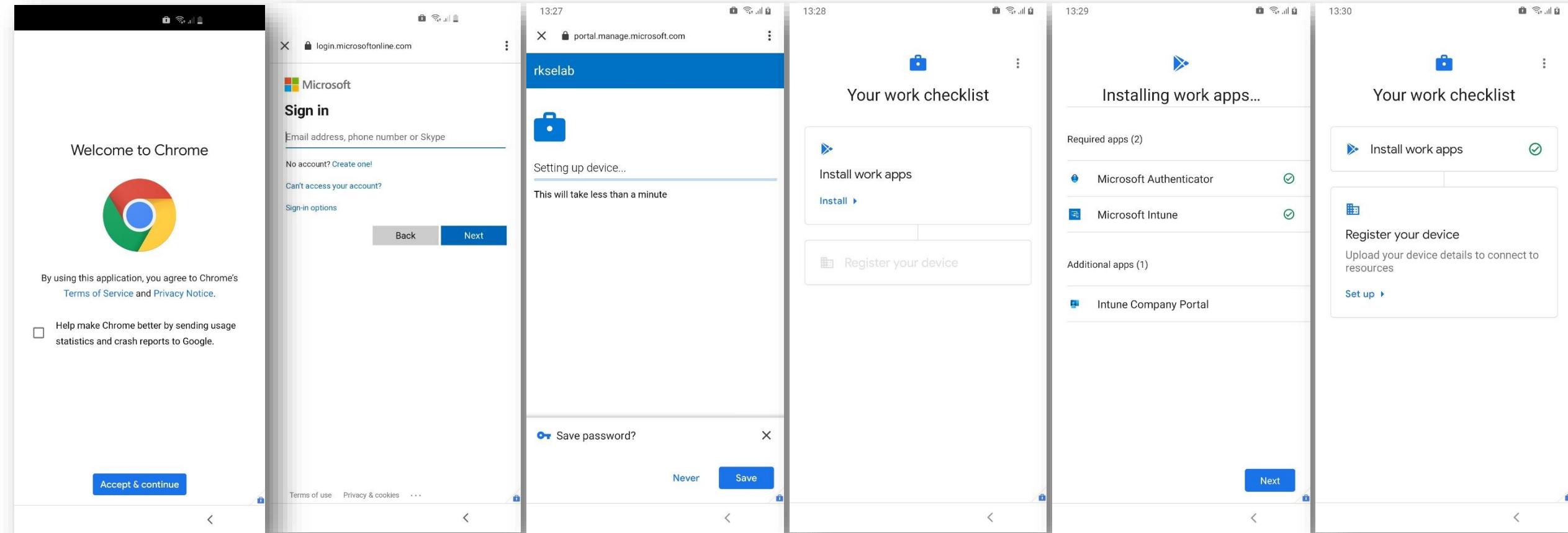
Wait

Wait

Wait

Done

# Android Enterprise: Fully Managed with a Work Profile Enrollment (KME 3/4)



Accept & continue

Sign into your  
Office 365 account,  
then select Next

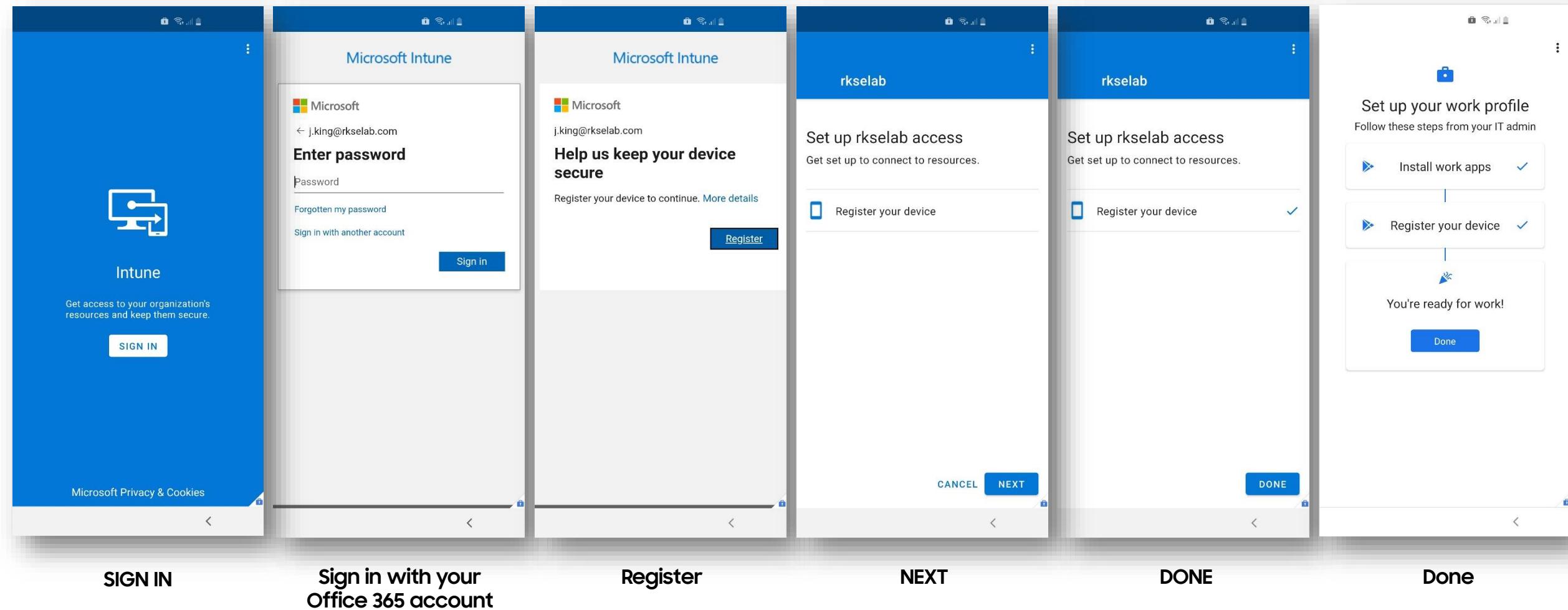
Never or Save  
for Password

Install

Next

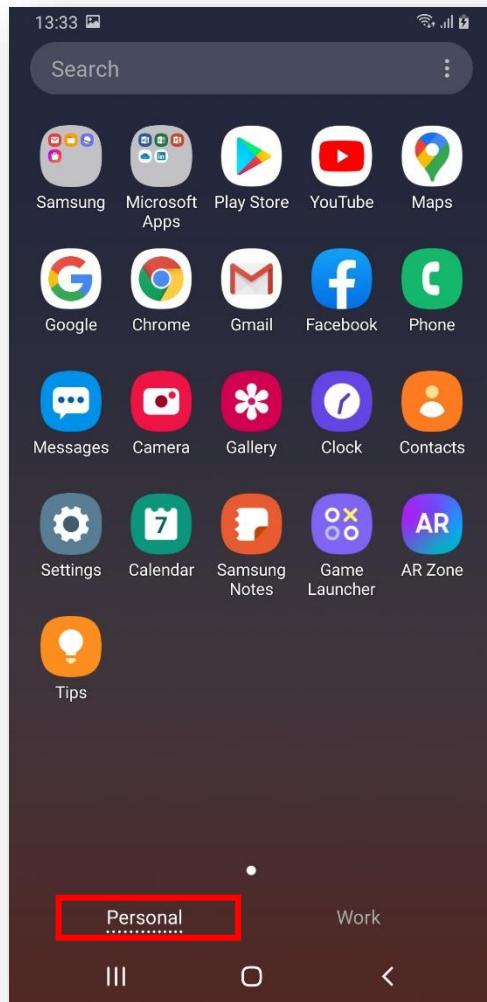
Set Up

# Android Enterprise: Fully Managed with a Work Profile Enrollment (KME 4/4)

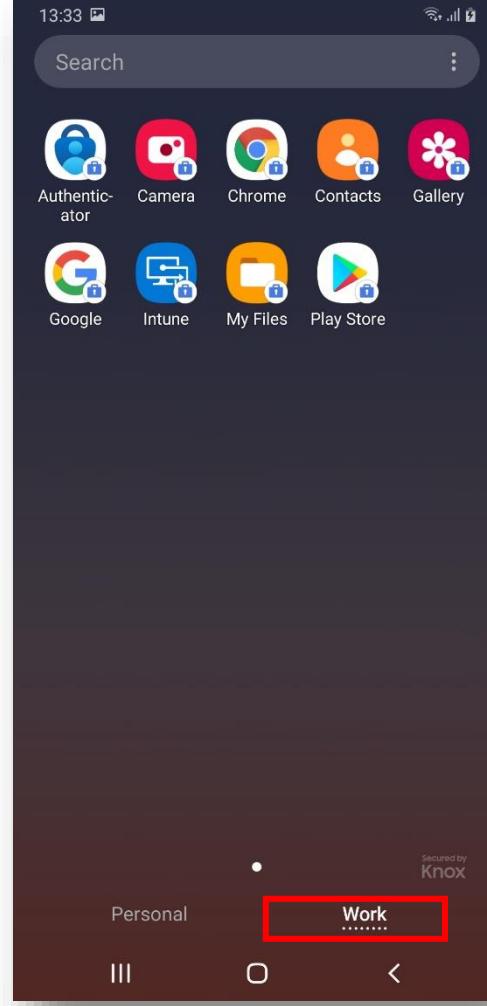


# Android Enterprise: Fully Managed with a Work Profile Enrollment

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



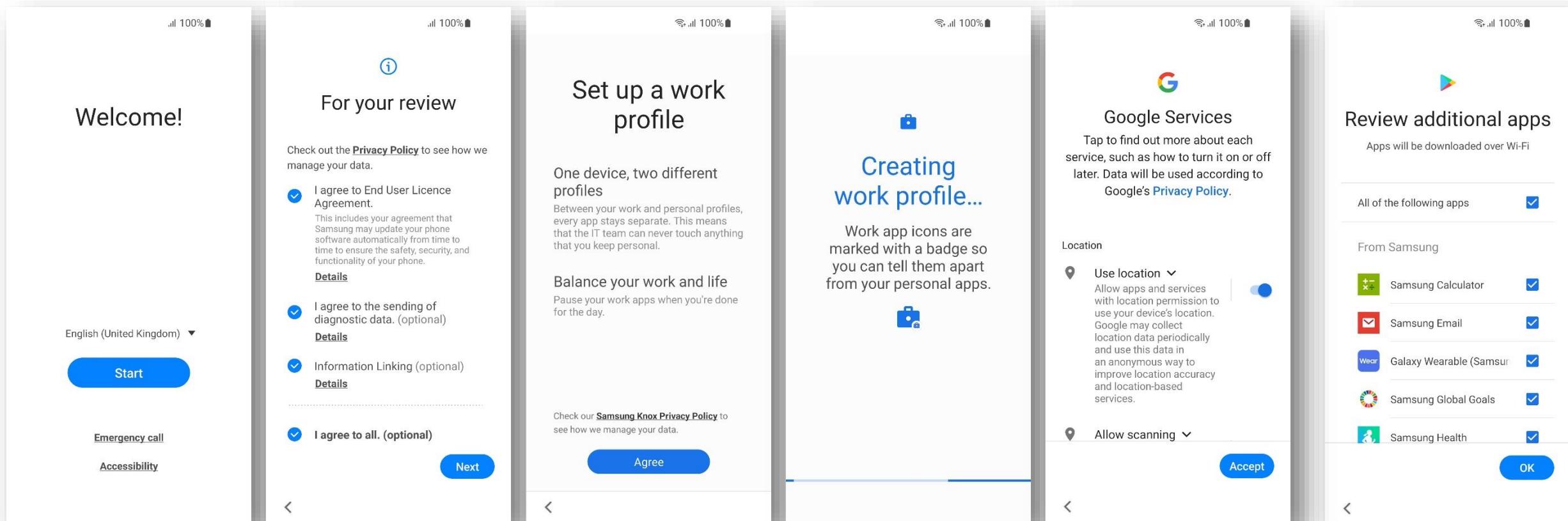
Personal Tab



Work Tab



Device is managed  
by your organization  
on lock screen



Start

Next

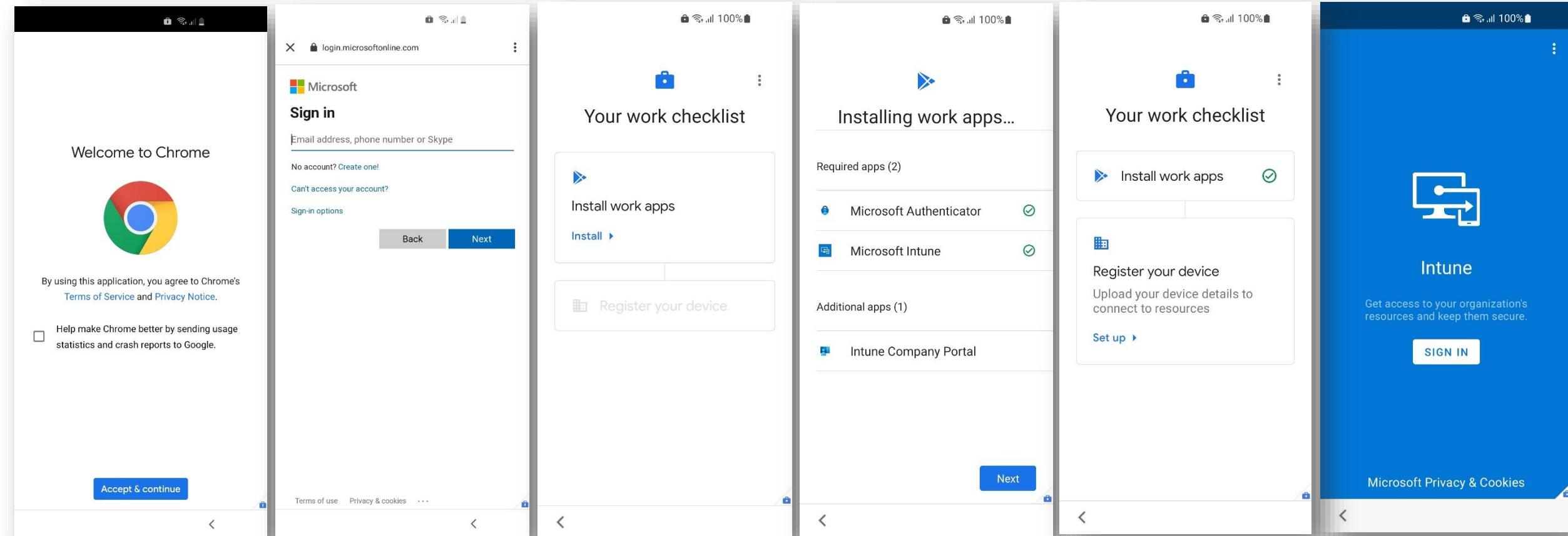
Agree

Wait

Accept

OK

# Android Enterprise: Work Profile on Company Owned Device Enrollment



**Accept & continue**

**Sign into your  
Office 365 account,  
then select Next**

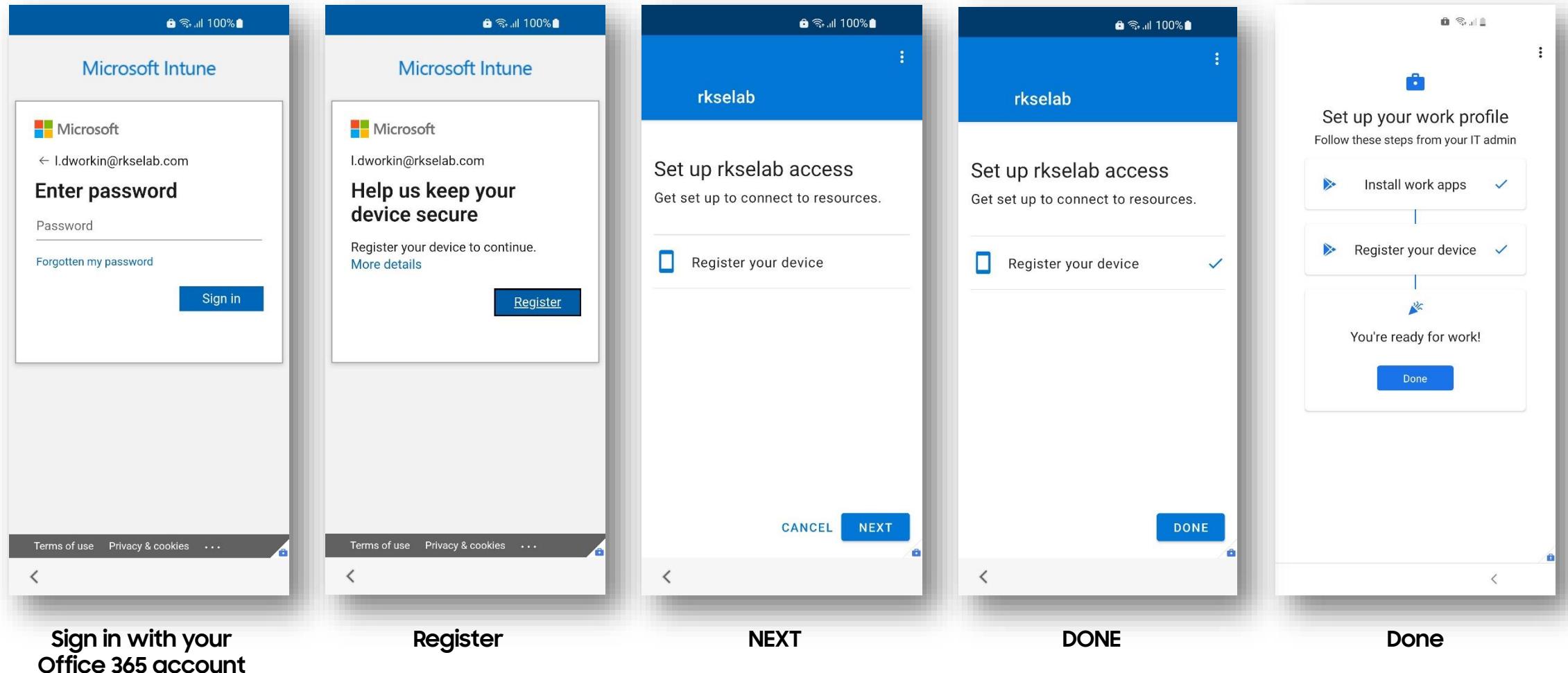
**Install**

**Next**

**Set Up**

**SIGN IN**

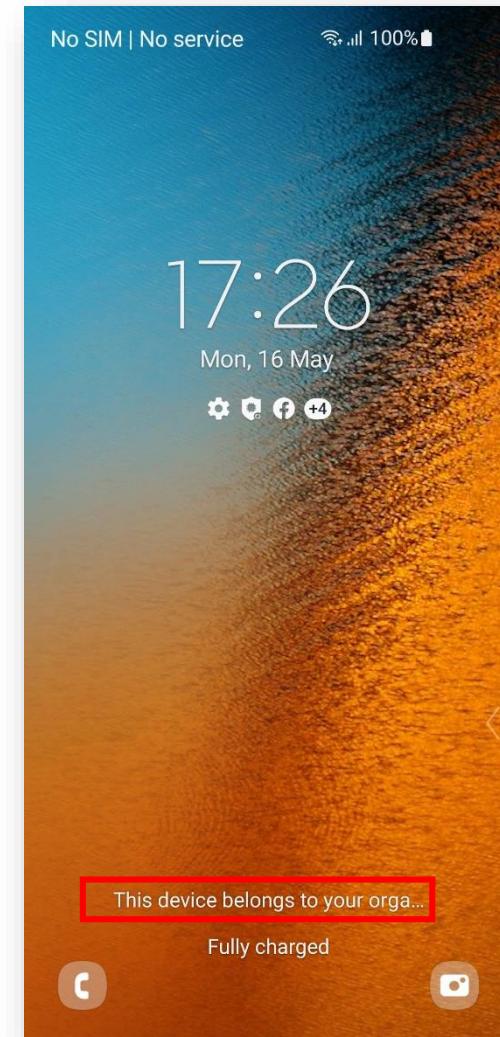
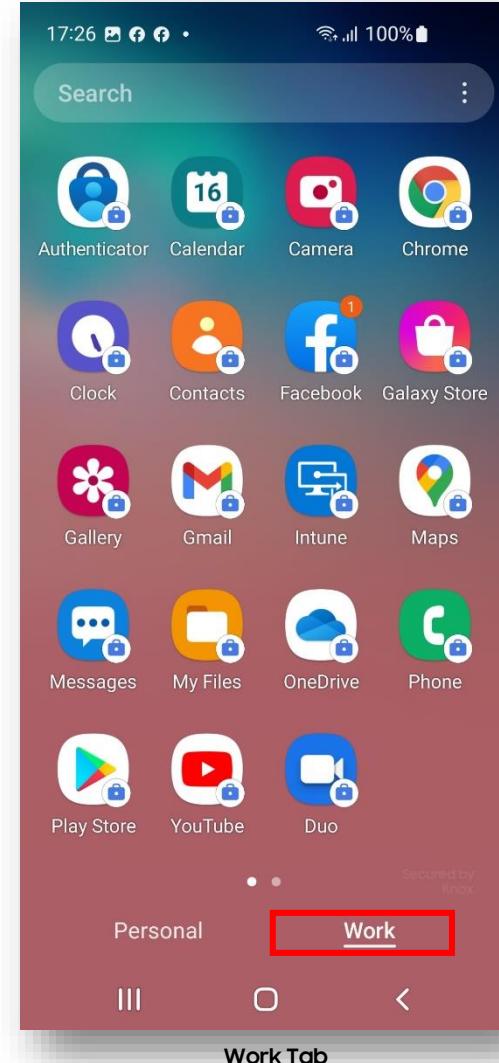
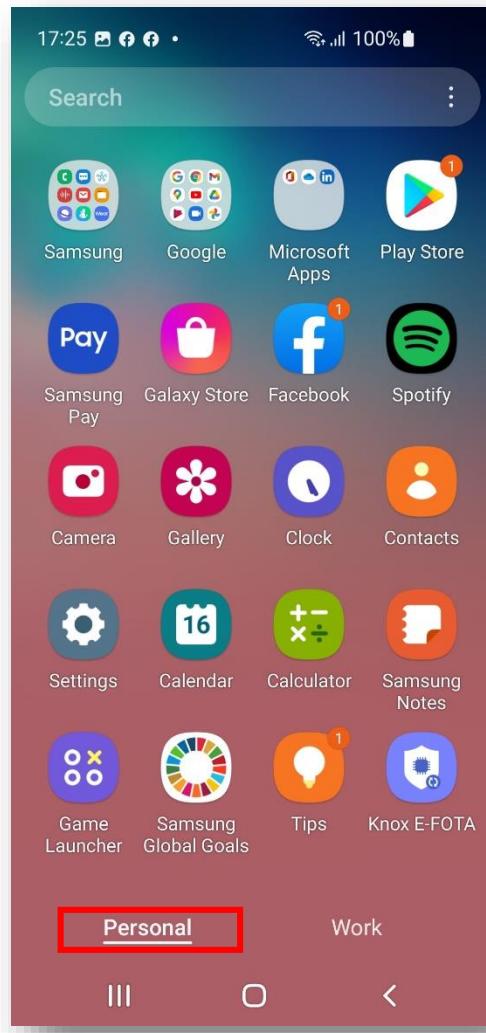
# Android Enterprise: Work Profile on Company Owned Device Enrollment



# Android Enterprise: Work Profile on a Company Owned Device Enrollment



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



# Android Enterprise: Dedicated Device

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

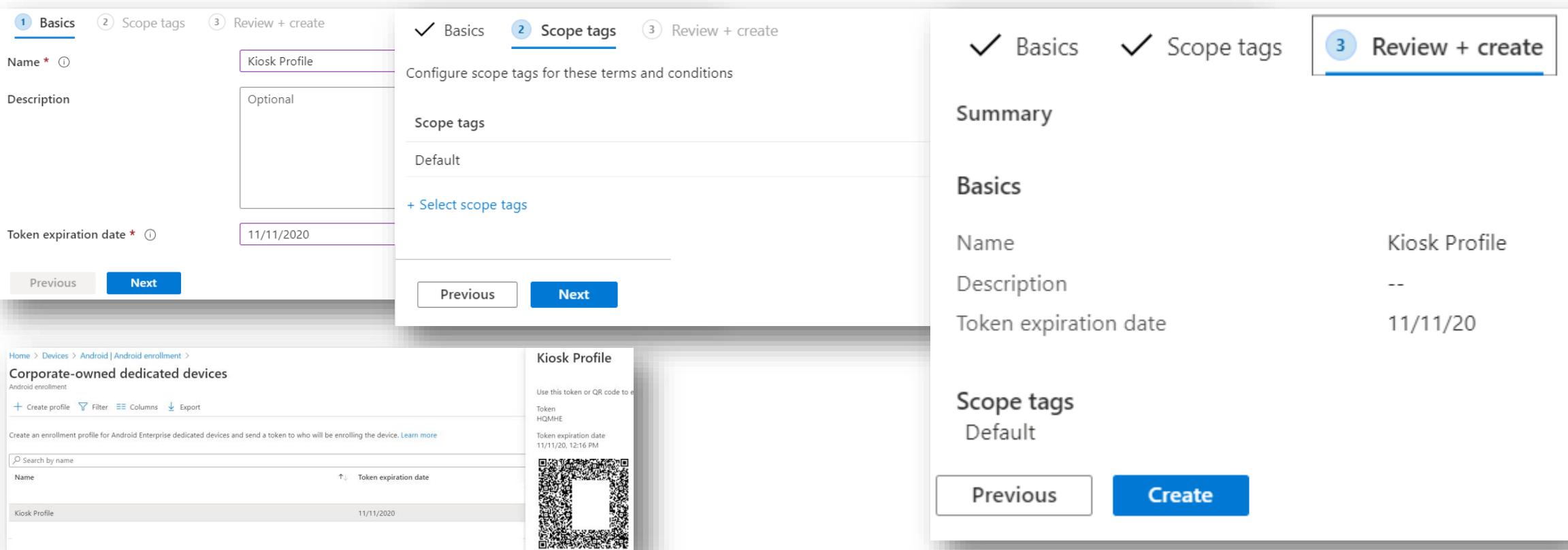
The image consists of two side-by-side screenshots of the Microsoft Endpoint Manager admin center.

**Left Screenshot:** The title is "Android | Android enrollment". The left sidebar shows "Android enrollment" is selected. The main area displays "Enrollment Profiles" with three options: "Personal devices with work profile", "Corporate-owned dedicated devices" (which is highlighted with a red box), and "Corporate-owned, fully managed user devices". A "Managed Google Play" section is also present.

**Right Screenshot:** The title is "Corporate-owned dedicated devices". The "Create profile" button is highlighted with a red box. The page instructions say "Create an enrollment profile for Android Enterprise dedicated devices". It includes a search bar and a "Name" input field.

# 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 screenshot shows the three-step enrollment process:

- Step 1: Basics** (Completed): Name: Kiosk Profile, Description: Optional, Token expiration date: 11/11/2020. Buttons: Previous, Next.
- Step 2: Scope tags** (Completed): Configure scope tags for these terms and conditions. Options: Default, + Select scope tags. Buttons: Previous, Next.
- Step 3: Review + create** (Active): Summary, Basics, Name: Kiosk Profile, Description: --, Token expiration date: 11/11/20. Scope tags: Default. Buttons: Previous, Create.

Below the steps, there is a summary table:

| Name                  | Kiosk Profile |
|-----------------------|---------------|
| Description           | --            |
| Token expiration date | 11/11/20      |

At the bottom left, there is a link to "Corporate-owned dedicated devices" with a QR code and token information: Token: HQMHE, Token expiration date: 11/11/20, 12:16 PM.

# Android Enterprise: Dedicated Device

## Create an Azure Active Directory Group

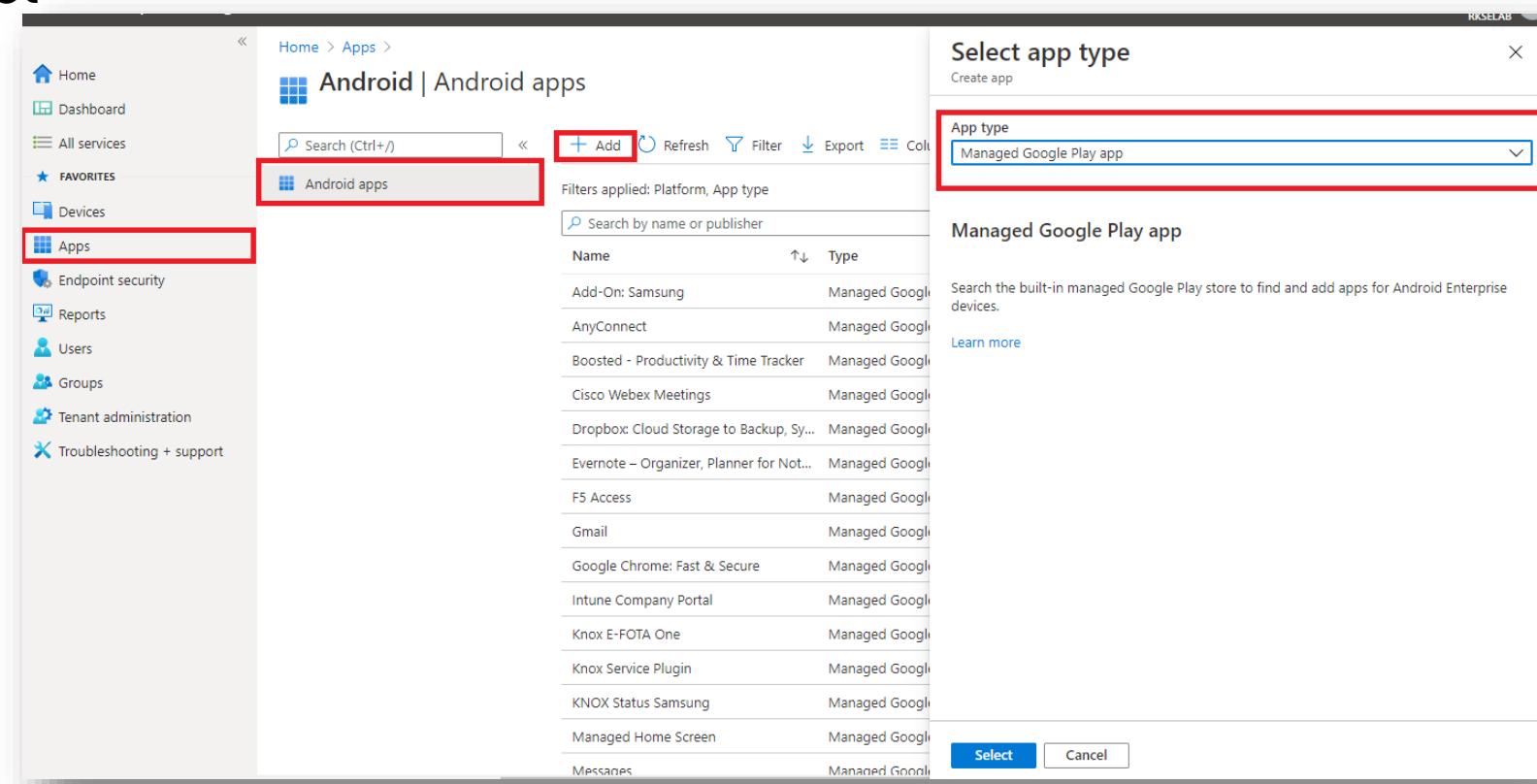
- Within the Microsoft Endpoint Manager console, navigate to Groups and select New Group
- "Group type = Security" "Group name = Name of your choice" "Group description = Optional" "Membership type = Dynamic Device"
- Click Add dynamic query
- Add the following rule:  
**(device.enrollmentProfileName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

The screenshot shows the Microsoft Endpoint Manager admin center interface. On the left, the navigation menu includes Home, Dashboard, All services, Favorites, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main area is titled 'Groups | All groups' under 'rkselab - Azure Active Directory'. A red box highlights the '+ New group' button. The 'Configure Rules' tab is selected, showing a table for defining membership rules. The first row defines a rule where the 'Property' is 'enrollmentProfileName', the 'Operator' is 'Match', and the 'Value' is 'Kiosk Profile'. Below this, there is a 'Rule syntax' section containing the expression '(device.enrollmentProfileName -match "Kiosk Profile")'. The 'Validate Rules (Preview)' tab is also visible.

# 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

**Managed Google Play**

Sync

Search

Managed Home Screen

Microsoft Corporation

APPROVED

PEGI 3

This app offers managed configuration

This app is only available in certain countries

Select Unapprove Approval Preferences

**Managed Home Screen | Properties**

Search (Ctrl+ /)

Overview

Manage

Properties (highlighted)

Monitor

Device install status

User install status

Name: Managed Home Screen

Description: Managed Home Screen

Publisher: Microsoft Corporation

Appstore URL: <https://play.google.com/store/apps/details?id=com.microsoft.launcher.enterprise&hl=GB>

Logo

Available licenses: 0

Total licenses: 0

Scope tags

Default

Assignments (highlighted)

# Android Enterprise: Dedicated Device

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

The image shows a sequence of four UI screens from a mobile management platform:

- Edit application** (Managed Google Play store app):
  - Assignments** tab is selected.
  - Required** section is expanded.
  - Group mode** is set to "Included".
  - + Add group** button is highlighted with a red box.
  - + Add all users**, **+ Add all devices** buttons are visible below the main area.
- Select groups** (Azure AD groups):
  - A search bar contains "Kiosk".
  - A list shows "Kiosk Device Group" with a "Selected" status, highlighted with a red box.
  - Select** button at the bottom is highlighted with a red box.
- Edit application** (Managed Google Play store app):
  - Review + save** button is visible.
  - Required** section is expanded.
  - Group mode** is set to "Included".
  - + Add group**, **+ Add all users**, **+ Add all devices** buttons are visible.
  - Available for enrolled devices** section is expanded.
  - Available with or without enrollment** section is expanded.
- Edit application** (Managed Google Play store app):
  - Review + save** button is highlighted with a red box.
  - Save** button at the bottom is highlighted with a red box.

# 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. On the left, the navigation menu is visible with 'Devices' selected. Under 'Devices', 'Configuration profiles' is also selected. In the main content area, the title is 'Android | Configuration profiles'. A red box highlights the 'Create profile' button in the top right of the toolbar. Below it is a search bar labeled 'Search by name'. A table lists 'Profile Name', 'Platform', and 'Profile type'. To the right, a modal window titled 'Create a profile' is open. It has fields for 'Platform' (set to 'Android Enterprise') and 'Profile' (set to 'Device restrictions'). Under 'Device restrictions', there is a note: 'Enable or disable device features, run apps on dedicated devices, control access to apps and content. This profile is for fully managed, dedicated, and corporate-owned work devices.' At the bottom of the modal, a red box highlights the 'Create' button.

# 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

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

Name \*  ✓

Description

Platform

Profile type

Previous Next

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

General

System security

Device experience Dedicated device

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

Select an app to use for kiosk mode \*

com.microsoft.teams Delete

+ 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 illustrates the process of creating a Kiosk Profile in the Microsoft Intune portal.

**Left Panel (Device restrictions):**

- Basics: checked
- Configuration settings: checked
- Scope tags: link
- Default: link
- + Select scope tags: link
- Previous: button
- Next:** button (highlighted with a red box)

**Middle Panel (Device restrictions - Assignments tab):**

- Basics: checked
- Configuration settings: checked
- Scope tags: checked
- Assignments: link (highlighted with a red box)
- Review: link

**Modal (Select groups to include):**

- Azure AD Groups search bar: Kiosk
- Result: KD Kiosk Device Group Selected (highlighted with a red box)
- Selected items: KD Kiosk Device Group (highlighted with a red box)
- Select button (highlighted with a red box)

**Right Panel (Review + create):**

- Basics: checked
- Configuration settings: checked
- Scope tags: checked
- Assignments: checked
- Review + create:** link (highlighted with a red box)

**Summary:**

- 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 ↑↓: Microsoft Outlook
- Package Name ↑↓: com.microsoft.office.o...
- App store URL ↑↓: Not configured
- Publisher: Microsoft
- Microsoft Teams: com.microsoft.teams
- App store URL ↑↓: Not configured
- Publisher: Microsoft

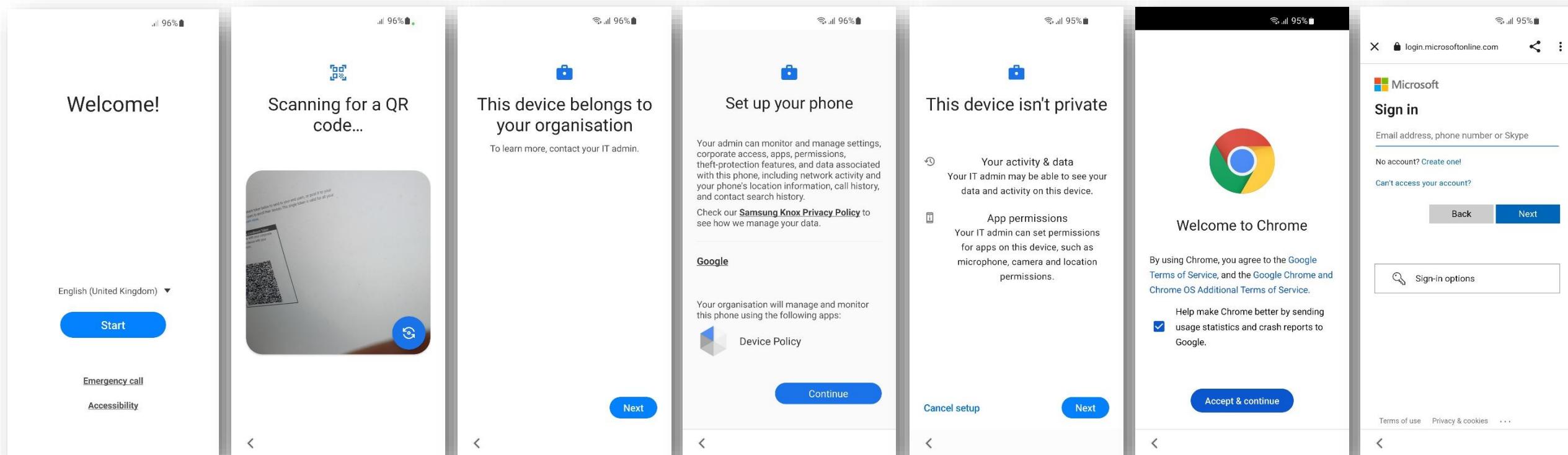
**Leave kiosk mode:**

- Enable: checked

**Buttons:**

- Previous: button
- Create:** button (highlighted with a red box)

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



Tap anywhere on  
the screen 6  
times

Scan the enrollment  
QR code

Next

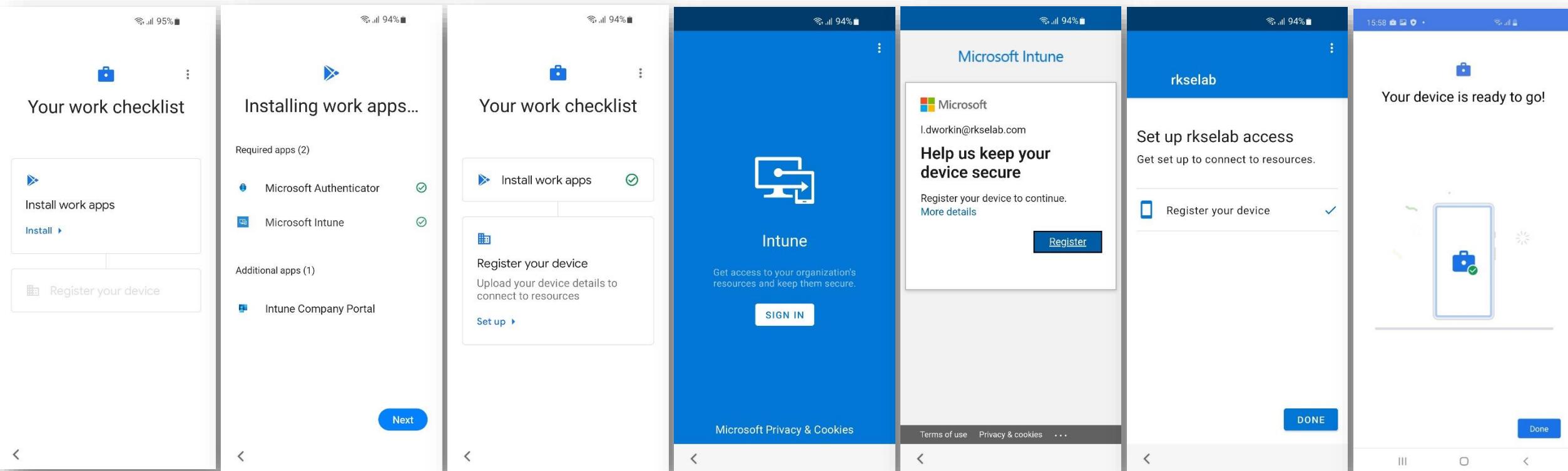
Continue

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

# Knox Platform for Enterprise

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:

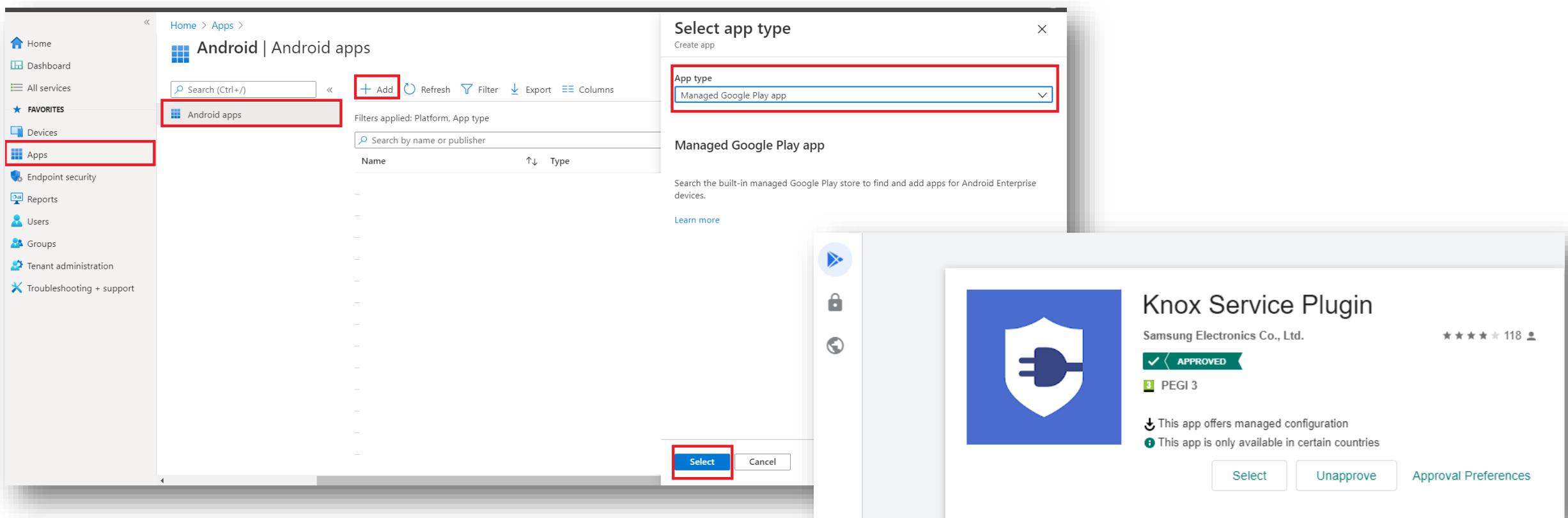
- Knox Platform for Enterprise : Standard Edition [FREE]
- Knox Platform for Enterprise : Premium Edition [FREE, or \$ for advanced options such as Dual DAR]

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



# 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

The screenshot illustrates the process of creating an OEMConfig profile for an Android Enterprise device. It consists of two windows: the main Microsoft Endpoint Manager admin center and a detailed configuration dialog.

**Main Window (Microsoft Endpoint Manager admin center):**

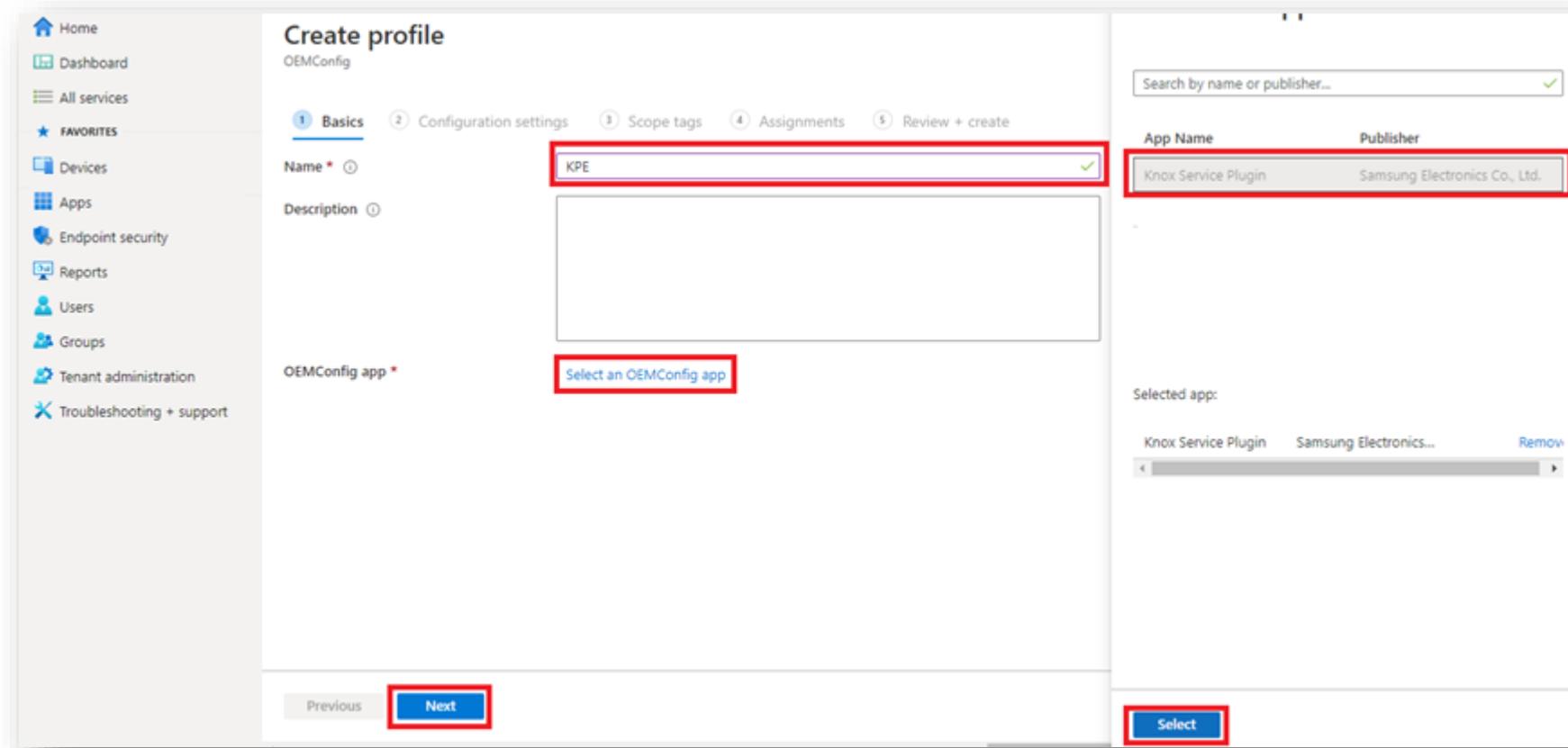
- The left sidebar shows navigation options like Home, Dashboard, All services, Favorites (Devices selected), Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support.
- The main content area is titled "Android | Configuration profiles".
- On the right side of the main window, there is a "Create profile" button highlighted with a red box.
- The "Configuration profiles" link in the bottom navigation bar is also highlighted with a red box.

**Detail Window (Create a profile):**

- This window is titled "Create a profile".
- It has dropdown menus for "Platform" (set to "Android Enterprise") and "Profile" (set to "OEMConfig"). Both dropdowns are highlighted with red boxes.
- A "Profile Name" input field is present below the dropdowns.
- A large blue "Create" button at the bottom is also highlighted with a red box.

# 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



# 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

## Samsung Knox Portal

- Set your desired configuration and select Next
- Scope tags are optional, select Next
- Choose an assignment and select Next
- Click Create

The image consists of three side-by-side screenshots of a web-based configuration interface for creating a Knox Profile.

**Screenshot 1: Configuration settings**  
This screenshot shows the 'Configuration settings' tab of the 'Create profile' wizard. It includes fields for 'Profile name' (set to 'KPE Profile') and 'KPE Premium License key' (set to 'XXX-XXXX-XXXX-XXX'). Other settings like 'Debug Mode' and various policy sections are shown but not highlighted.

**Screenshot 2: Assignments**  
This screenshot shows the 'Assignments' tab. The 'Assign to' dropdown is set to 'All users'. A note below states: 'When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.' Below this is a 'Selected groups' section which is currently empty.

**Screenshot 3: Review + create**  
This screenshot shows the final 'Review + create' step. It summarizes the profile details: Name 'KPE', Description '...', OEMConfig app 'Knox Service Plugin', Profile name 'KPE Profile', KPE Premium License key 'XXX-XXXX-XXXX-XXX', Scope tags 'Default', and Assignments 'Included groups: All users'. The 'Create' button at the bottom is highlighted with a red box.

# Document Information

**This is version 3.0 of this document.**

Thank you!

