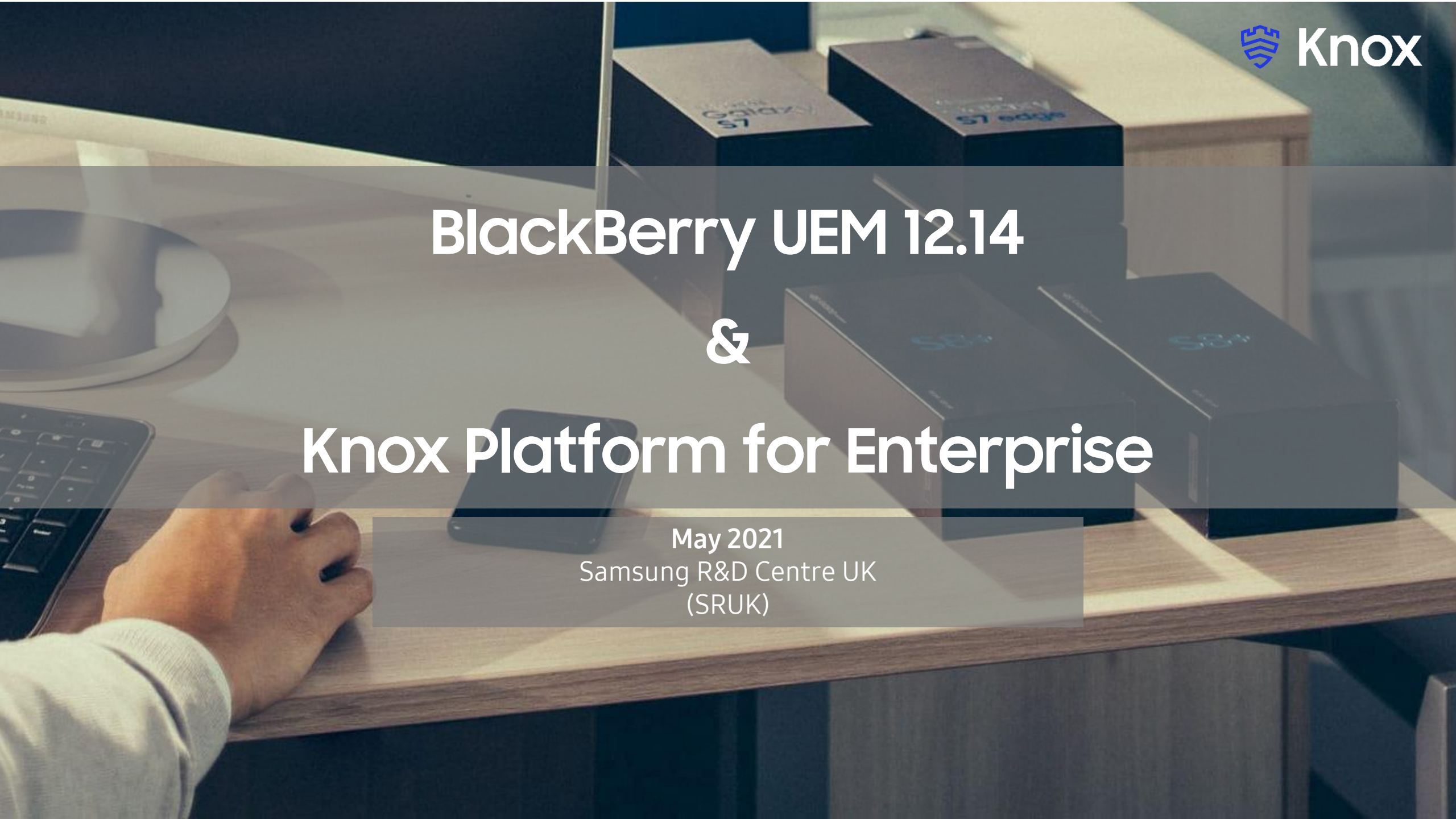


BlackBerry UEM 12.14

&

Knox Platform for Enterprise

May 2021

Samsung R&D Centre UK
(SRUK)

Agenda

1. How to gain access to BlackBerry UEM
2. Pre-requisites for Knox Platform for Enterprise
3. Configure Android Enterprise
4. Android Enterprise Deployment Modes
   - BYOD
   - Company-owned Device
   - Fully Managed Device with a Work Profile/Work Profile on Company Owned Device
   - Dedicated Device
5. Managed Google Play [MGP] Configuration
6. AppConfig in BlackBerry UEM
7. Configure Knox Platform for Enterprise : Standard Edition
8. Configure Knox Platform for Enterprise : Premium Edition
9. Configure Knox Service Plugin [KSP]

BlackBerry UEM Collateral & Contacts

Contacts:

sruk.rtam@samsung.com

Knowledge Base:

http://help.blackberry.com/en/

http://support.blackberry.com/kb

https://www.youtube.com/watch?v=WTcuFOmpQQk

BlackBerry Solution:

https://www.youtube.com/user/BlackBerry

Trial Access:

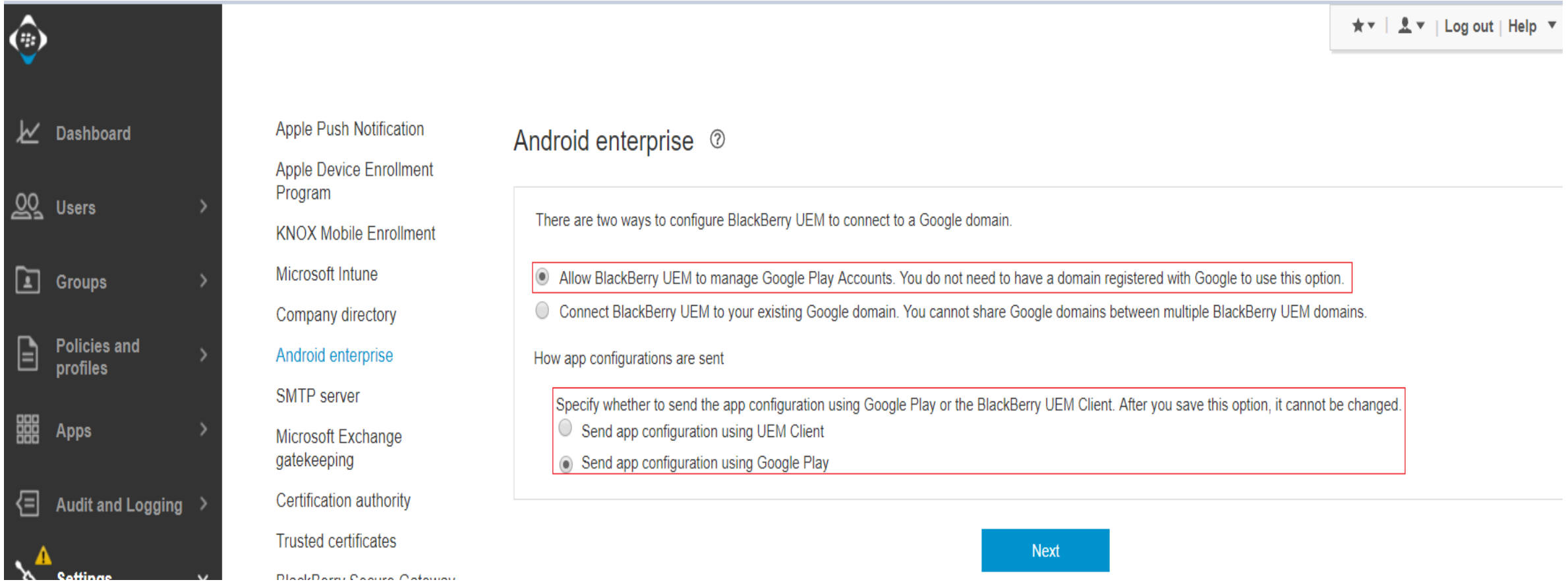
https://www.blackberry.com/uk/en/products/endpoint-management/blackberry-enterprise-mobility-suite

Pre-Requisites for Knox Platform for Enterprise

1. **Obtain access to BlackBerry UEM console**
2. **A Gmail account for the Android Enterprise Binding**
3. **Consider what enrollment method to use:**
   - Knox Mobile Enrollment (KME)
   - QR Code enrollment
   - NFC
   - Token (afw#BlackBerry)
   - Manual (Applicable to BYOD only)

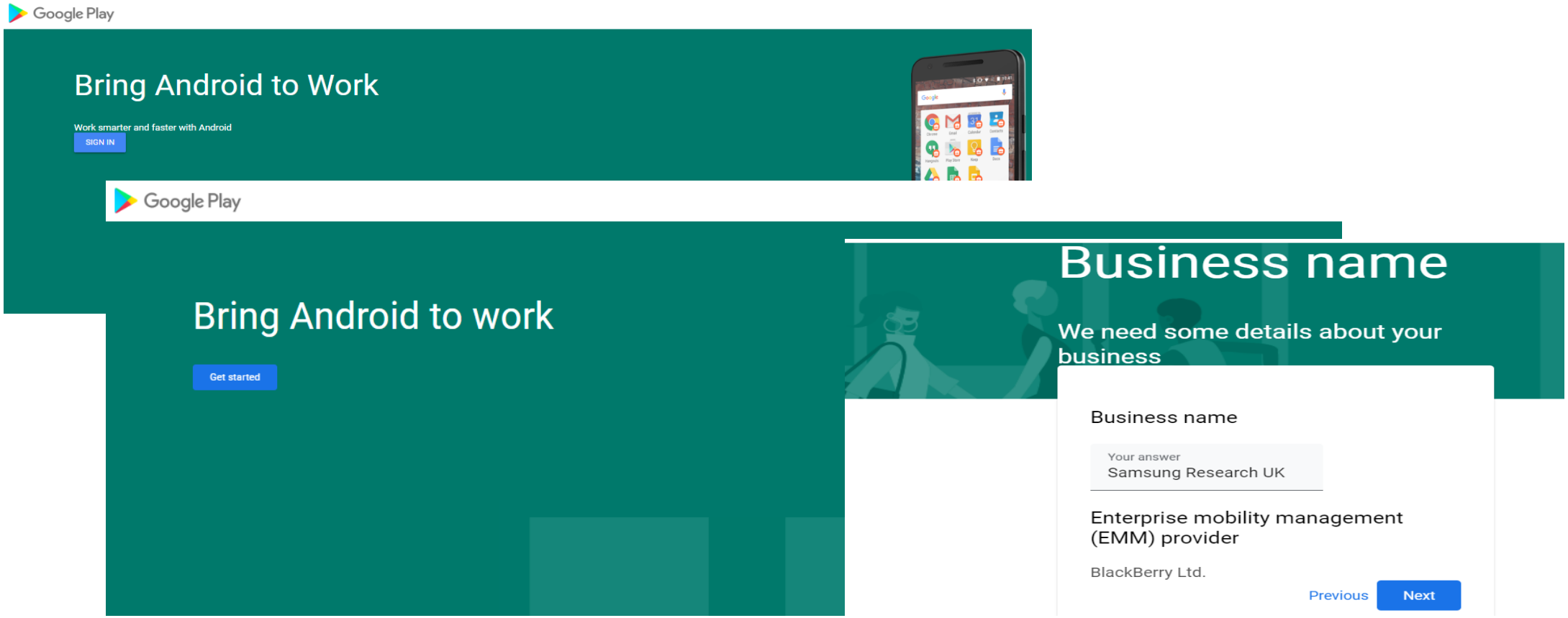
Configure Android Enterprise

- Log into BlackBerry UEM console. Navigate to: **Settings -> External Integration -> Android Enterprise**
- Select ways to configure BlackBerry UEM connection to Google domain and how app configuration are to be sent.
- Select Next to be directed to the Google Play Screen.



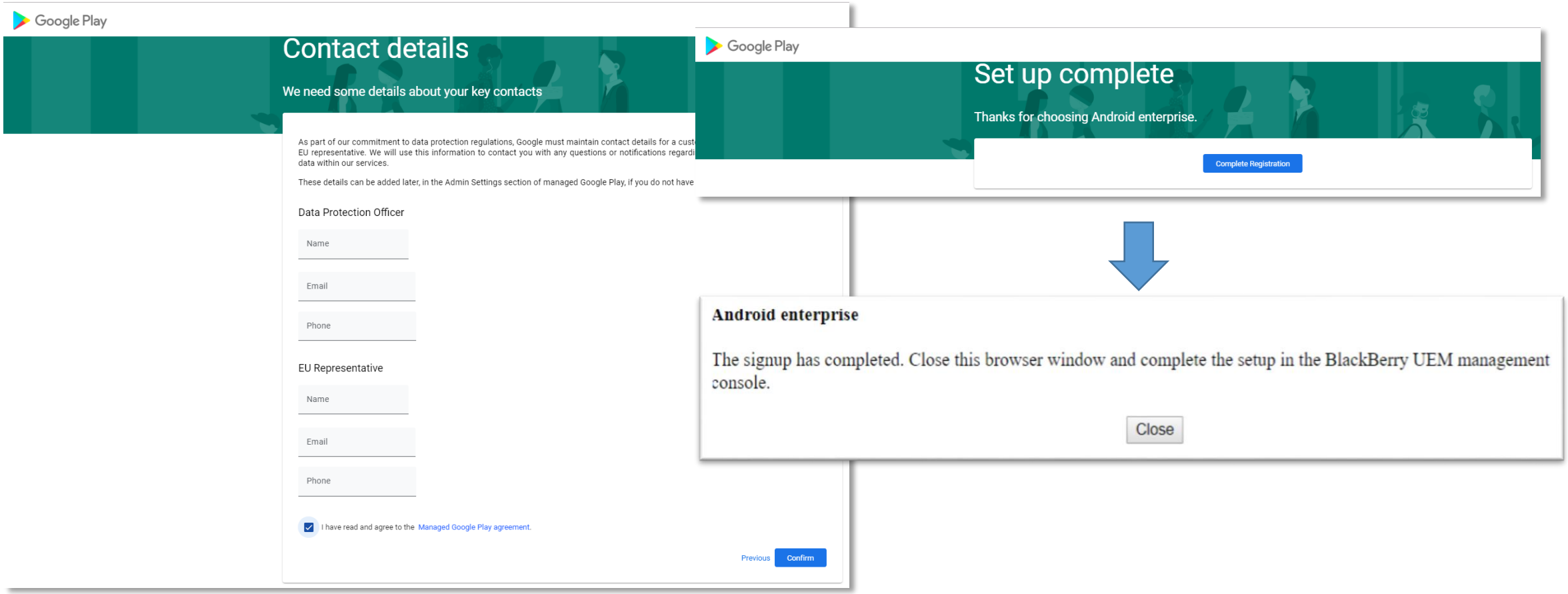
Configure Android Enterprise

- You will then get redirected to a Google Play screen. Click **SIGN IN** to sign with a Gmail Account
- Fill out your Business name and Select **Next** to allow BlackBerry UEM to be your EMM provider.



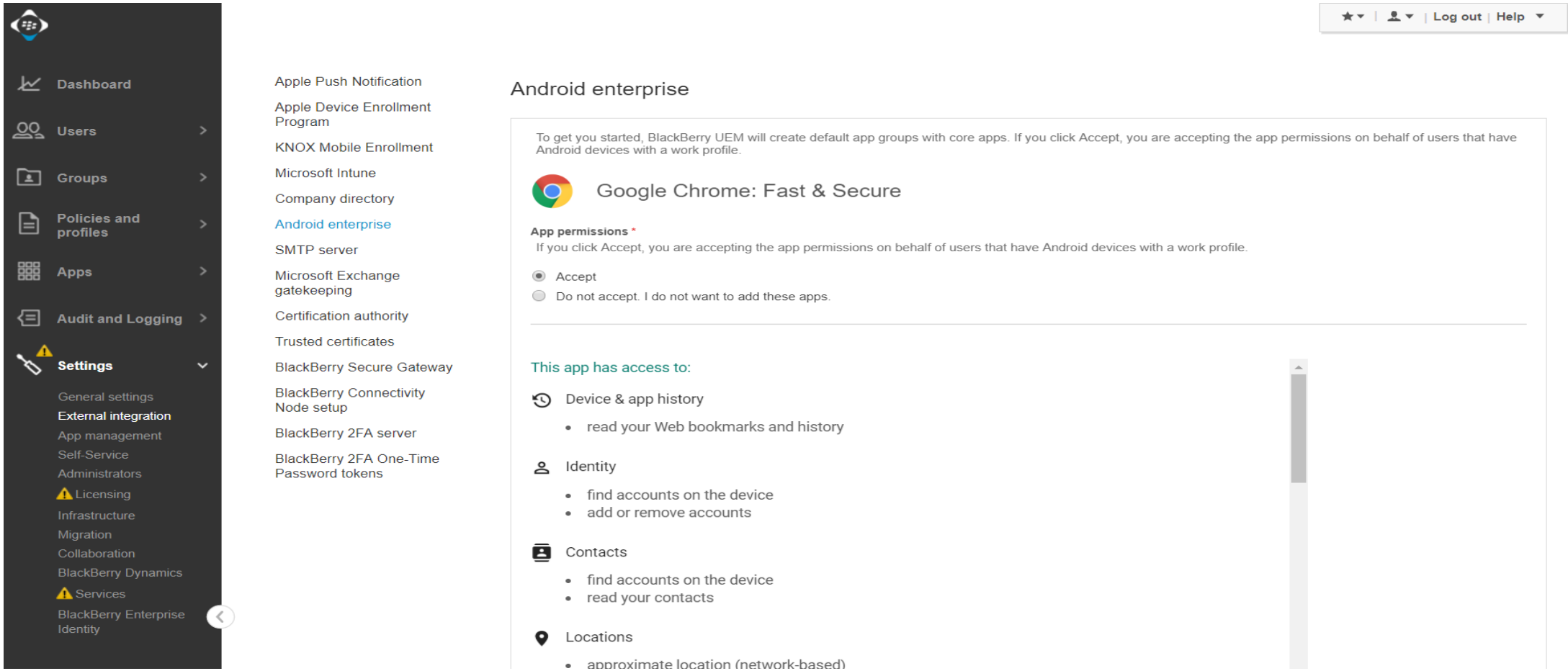
Configure Android Enterprise

- 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** and a message will be displayed as “The signup has completed.....”



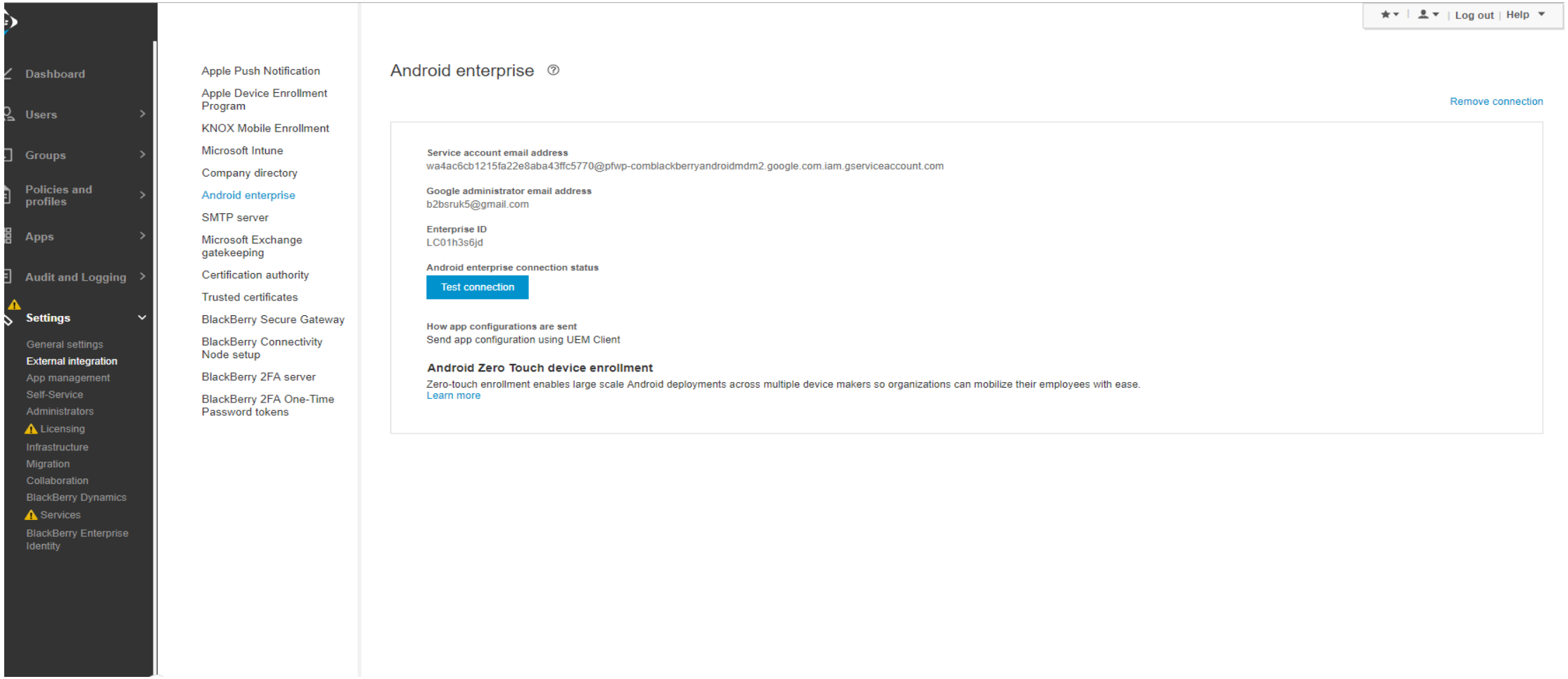
Configure Android Enterprise

- In BlackBerry UEM console, **Settings** -> **External Integration** -> **Android Enterprise** , Click to accept the permissions set for some or all the following apps*: Google Chrome, BlackBerry Connectivity, BlackBerry Hub+ Services, BlackBerry Hub, BlackBerry Calendar , Contacts by BlackBerry, Notes by BlackBerry* and *Tasks by BlackBerry.*



Configure Android Enterprise

- Android Enterprise is now fully configured



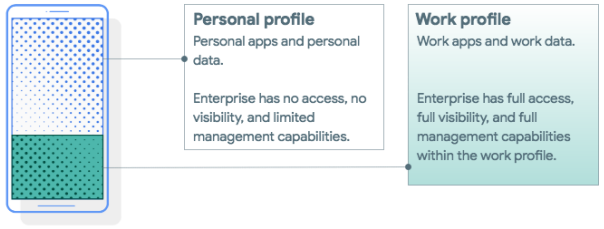
Android Enterprise Deployment Modes

Deployment Modes

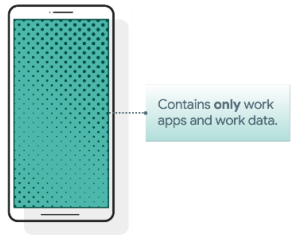
Android Enterprise can be deployed in the following 4 deployment modes

1. **BYOD** [*formerly known as Profile Owner or PO*]
2. **Company Owned 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** [*WPC, Available from Android 11*]
4. **Dedicated device** [*formerly known as COSU*]

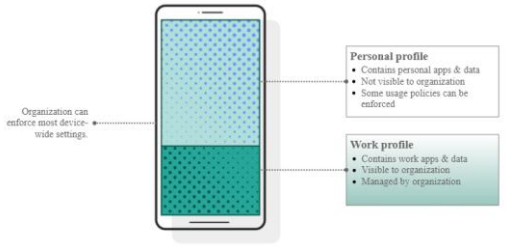
BlackBerry UEM can support 4 of these deployment modes. In this next section we will show you how to configure each of these 4 deployment modes in BlackBerry UEM for your device fleet.



Bring Your Own Device [BYOD]



Company-owned Device



Fully Managed device with a Work Profile / Work Profile on Company Owned Device

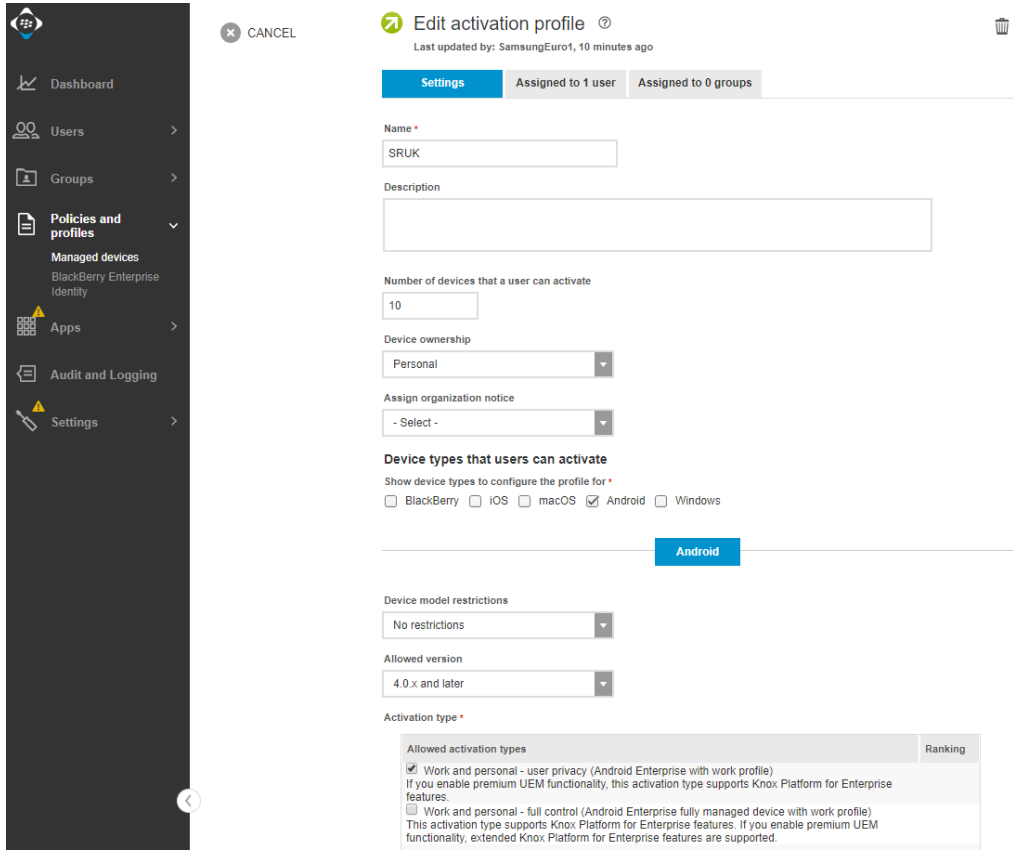
Dedicated Device

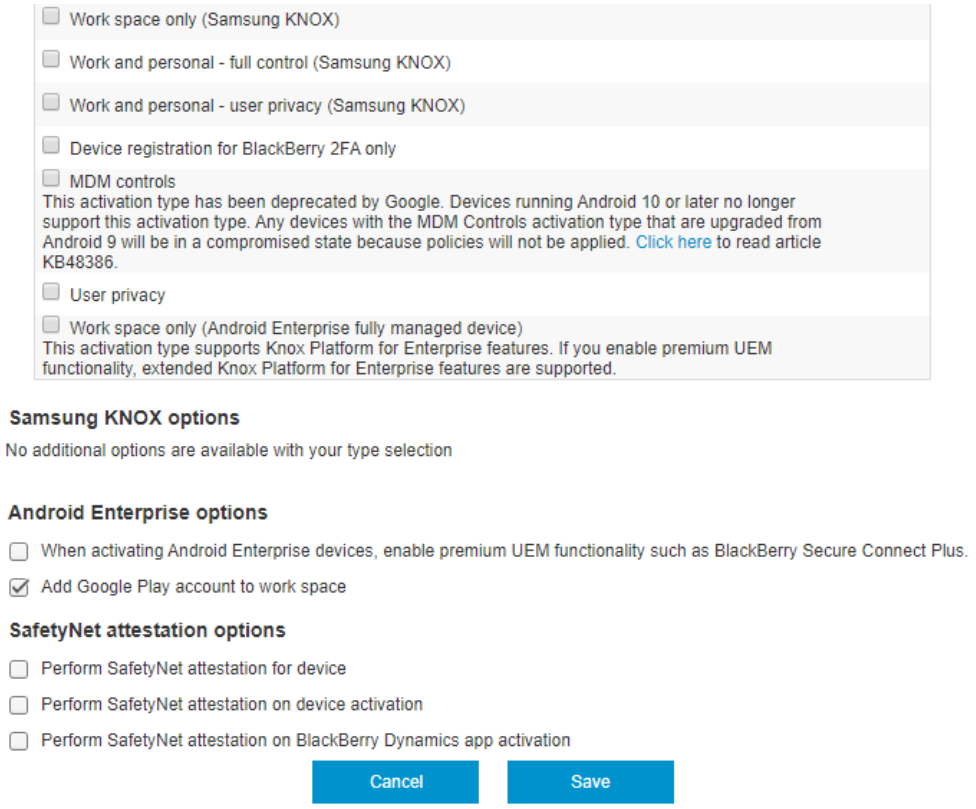
Android Enterprise BYOD Deployment

To enroll a device in the Android Enterprise BYOD deployment type, the final prerequisite is you need to create an Activation Profile and select “Work and personal - user privacy (Android Enterprise with work profile) as allowed activation type.

Assign this Activation Profile to the user to be enrolled.

- Go to *Policies and Profiles -> Under Policy , select Activation -> Activation Profile -> “+” sign*
- Fill the information requested and select “*Work and personal - user privacy (Android Enterprise with work profile)”* under activation type.



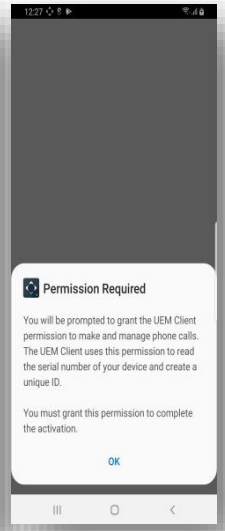


Android Enterprise BYOD Deployment

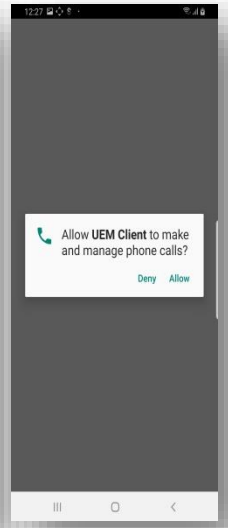
Now all you simply need to do is enroll your device by completing the following:

- On your device, go to the Google Play Store, download the BlackBerry UEM client, and enroll your device.

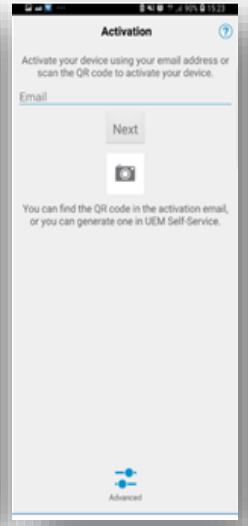
Install BlackBerry UEM Client from Google Play Store



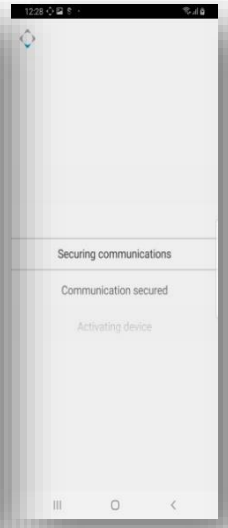
Accept the permission request



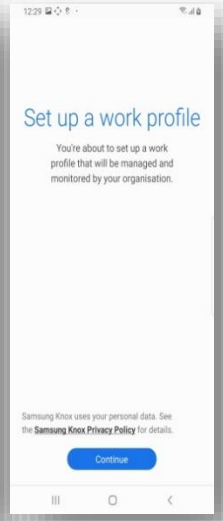
Allow UEM Client to ...



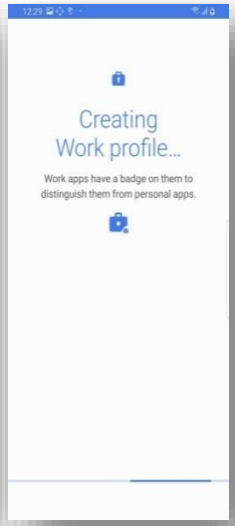
Enter Credentials



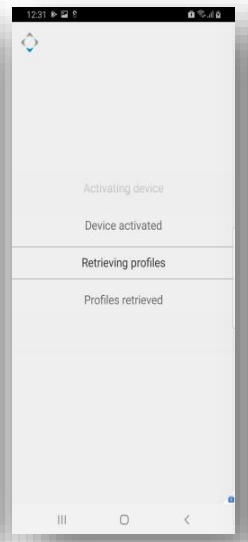
Start of the Enrollment



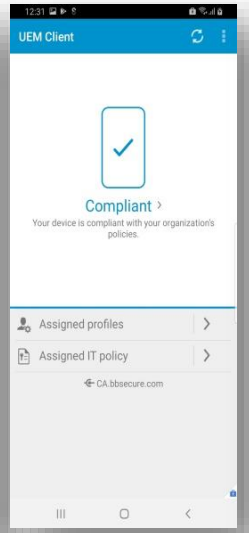
Click Continue to Set up a Work Profile



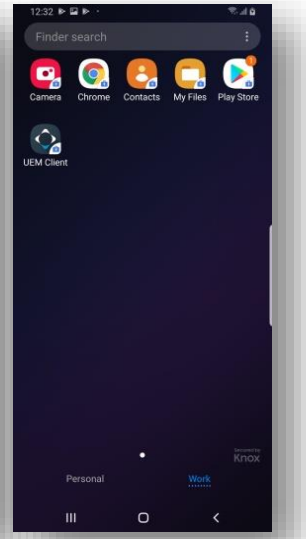
Creating Work Profile



Profiles being Retrieved



Device Enrollment Successful!



Inside the Work Profile

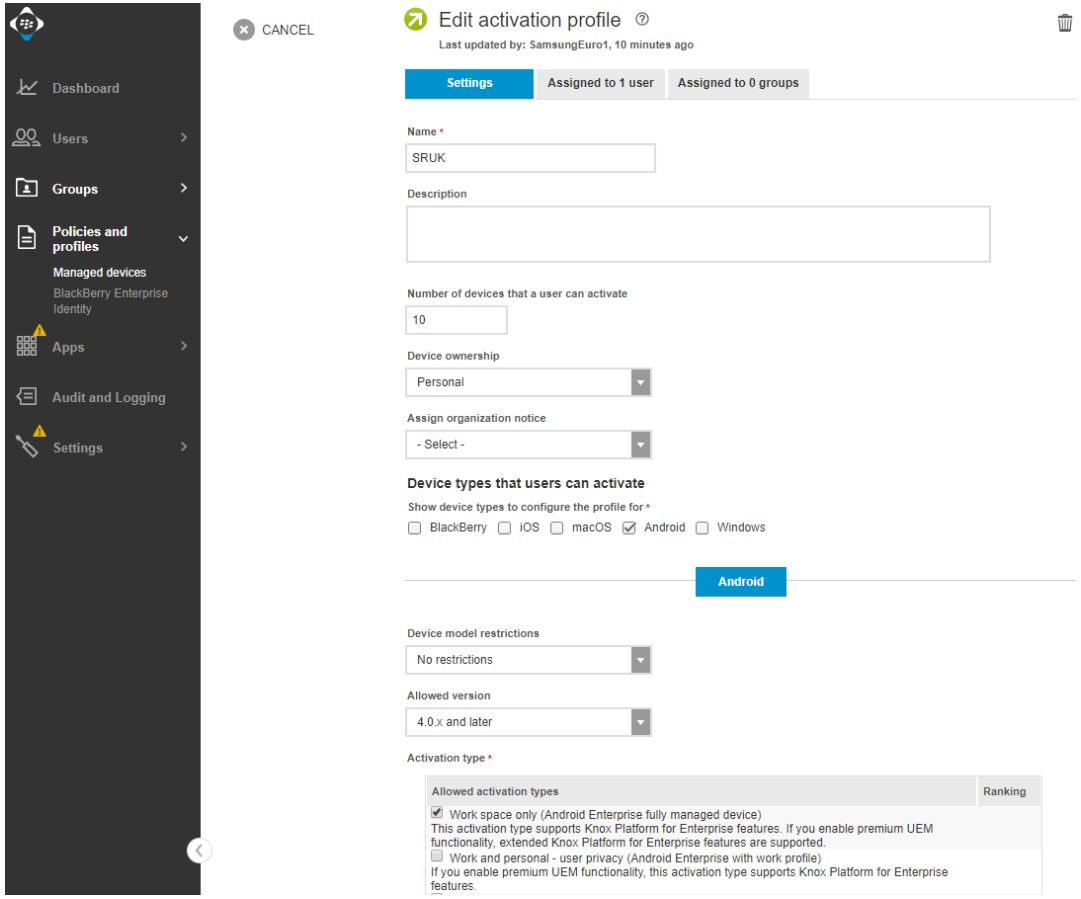
Android Enterprise: Company Owned Device

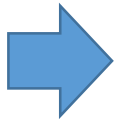
Android Enterprise Company Owned Device Deployment

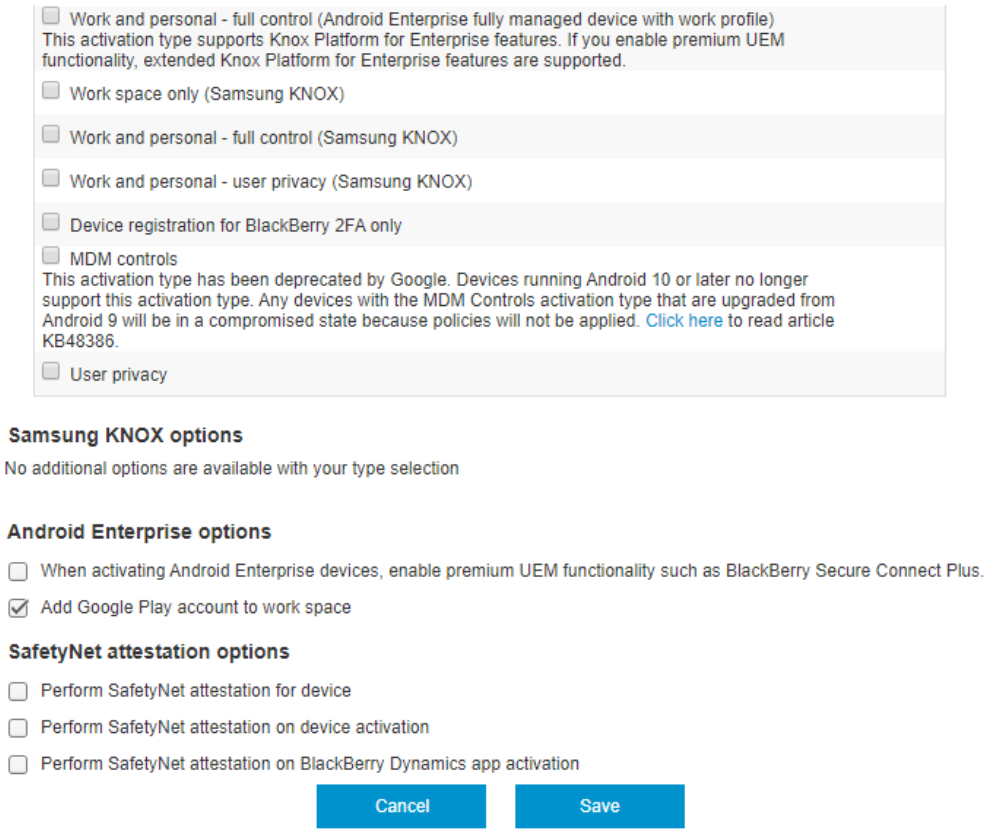
To enroll a device in the Android Enterprise Company Owned device deployment type, the final prerequisite is you need to create an Activation Profile and select “Work space only (Android Enterprise fully managed device) as allowed activation type.

Assign this Activation Profile to the user to be enrolled.

- Go to *Policies and Profiles -> Under Policy , select Activation -> Activation Profile -> “+” sign*
- Fill the information requested and select “*Work space only (Android Enterprise fully managed device)”* under activation type.







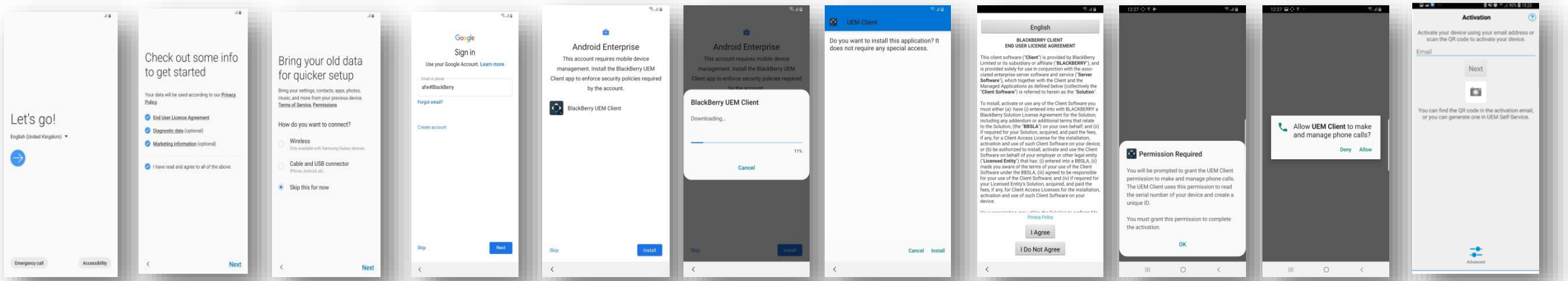
Android Enterprise: Company Owned Device

Android Enterprise Company Owned Device Deployment

To enroll your device as an Android Enterprise Company Owned device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 4 ways you can enroll your device into BlackBerry UEM as an Android Enterprise Company Owned device.

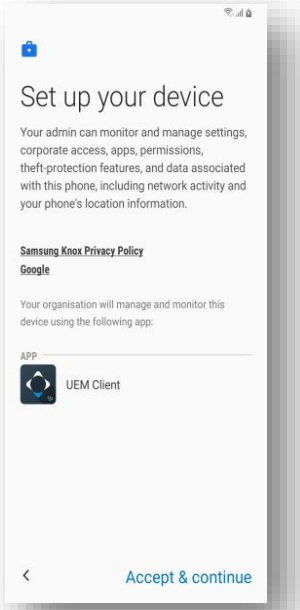
1. DPC Identifier [Also known as the hashtag method] **afw#BlackBerry**
2. QR Code Enrollment
3. NFC
4. Knox Mobile Enrollment

- Below is a screen-by-screen play to enroll your device using the DPC Identifier method.



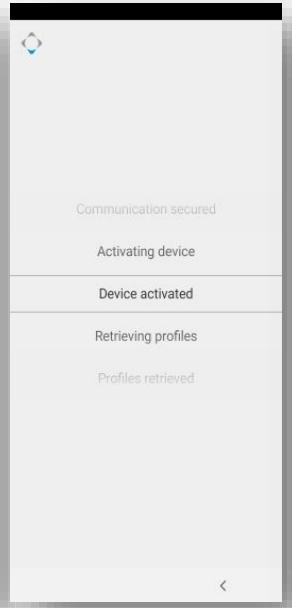
Android Enterprise: Company Owned Device

Android Enterprise Company Owned Device Deployment

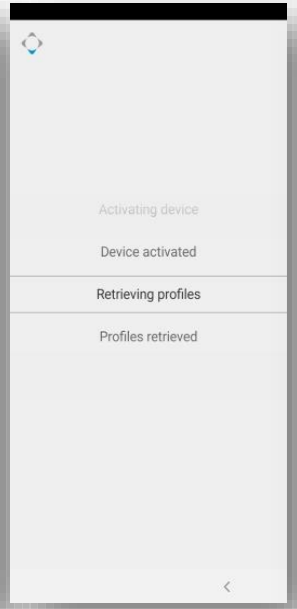


Accept & Continue

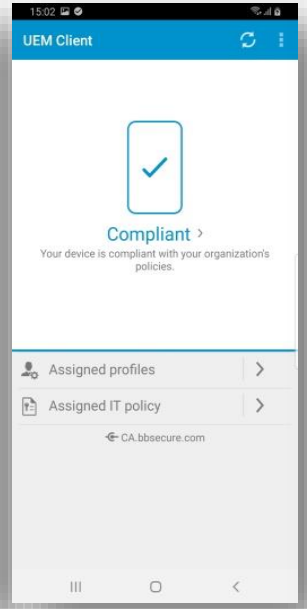
Setting up Work device



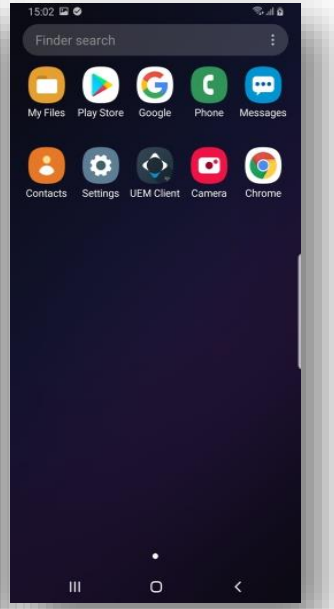
Device activated



Profiles being retrieved



Device Enrollment Successful!



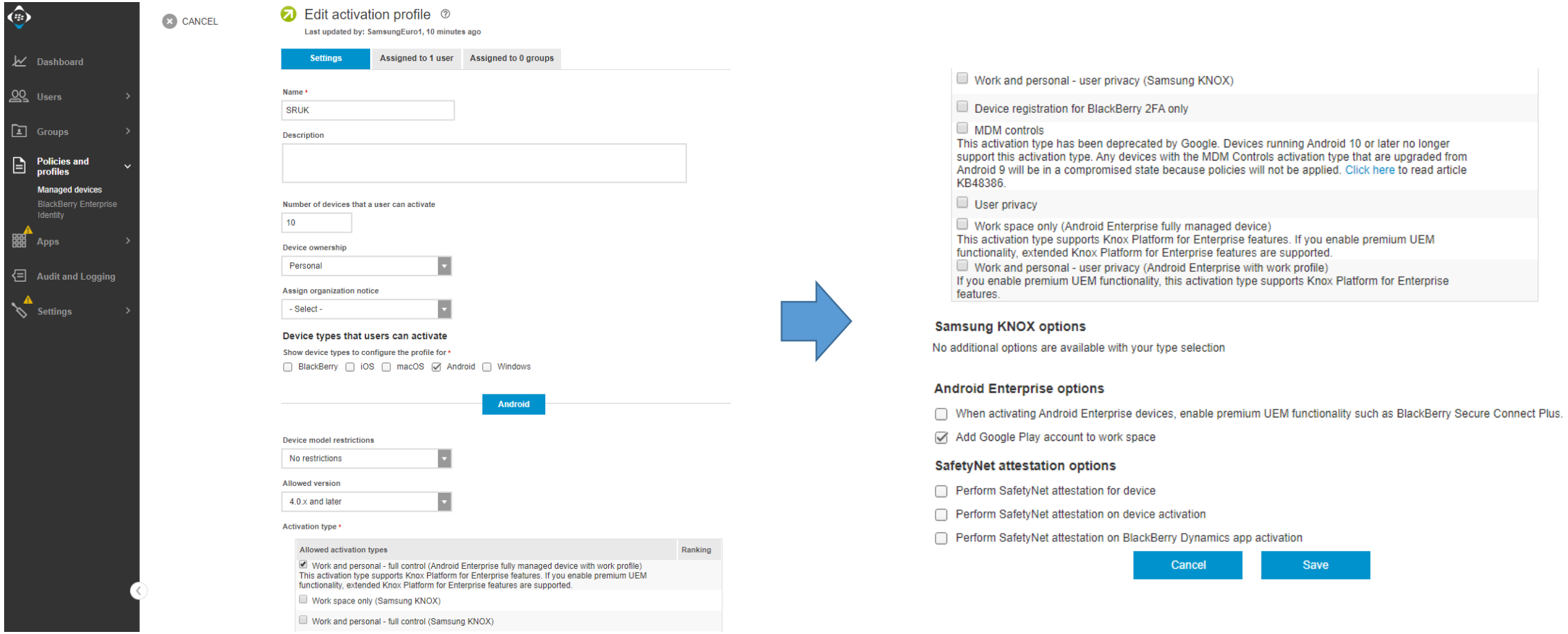
Device Area

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

To enroll a device in the Android Enterprise Fully Managed Device with a work profile type, the final prerequisite is you need to create an Activation Profile and select "Work and personal - full control (Android Enterprise fully managed device with work profile) as allowed activation type.

Assign this Activation Profile to the user to be enrolled.

- Go to *Policies and Profiles -> Under Policy, select Activation -> Activation Profile -> "+" sign*
- Fill the information requested and select "*Work and personal - full control (Android Enterprise fully managed device with work profile)* under activation type.



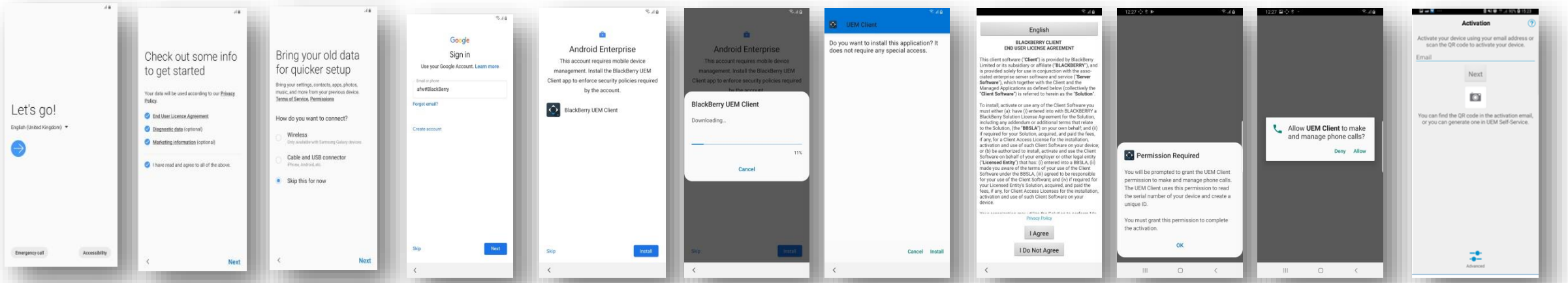
Android Enterprise: Fully Managed Device with a Work Profile (COMP)

Android Enterprise Fully Managed Device with a Work Profile (COMP) Deployment

To enroll your device as an Android Enterprise Fully Managed Device with a Work Profile type, you need to ensure the device is factory reset and at the welcome screen. From here, there are 4 ways you can enroll your device into BlackBerry UEM as an Android Enterprise Fully Managed Device with a Work Profile.

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

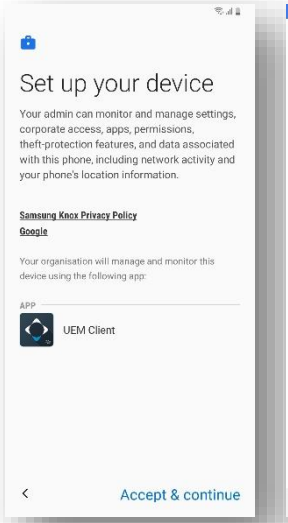
- Below is a screen-by-screen play to enroll your device using the DPC Identifier method.



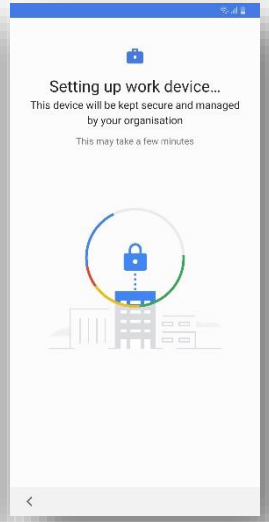
Click Start arrow | Accept T's & C's | Skip Backup | Enter **afw#BlackBerry** and click next | Select Install | UEM client being downloaded | Click Install | Agree to the license agreement | Accept the Permission | Allow UEM Client to ..... | Enter Credential for the enrollment

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

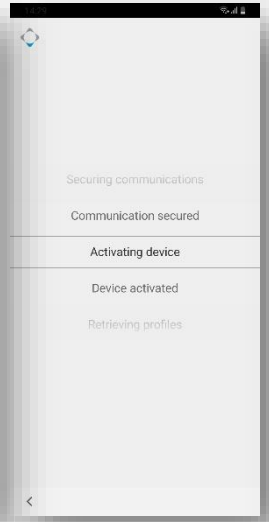
Android Enterprise Fully Managed Device with a Work Profile (COMP) Deployment



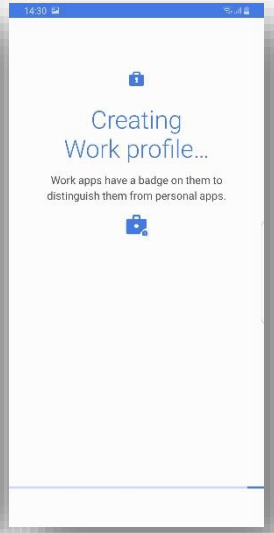
Accept & Continue



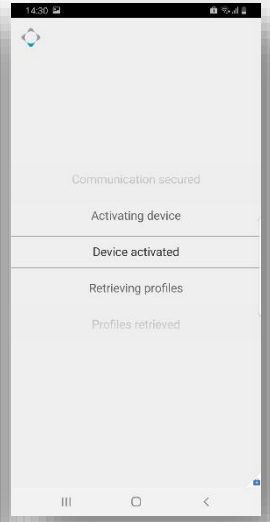
Setting up Work device



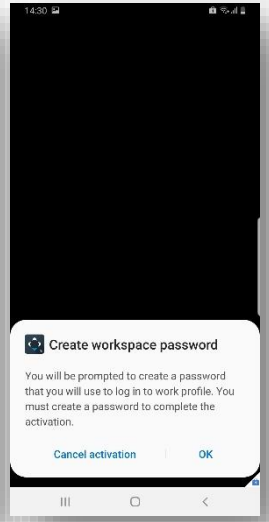
Activating device



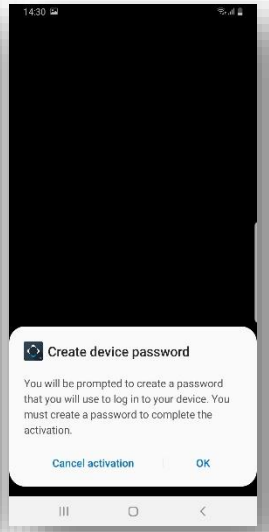
Profiles being retrieved



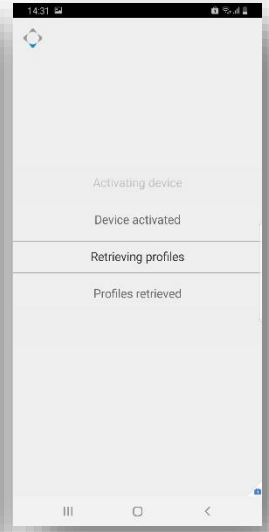
Device Enrollment Successful!



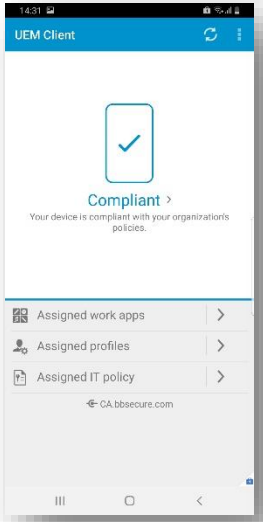
Work Profile password creation



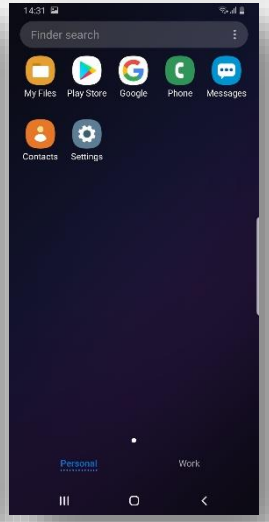
Device Password Creation



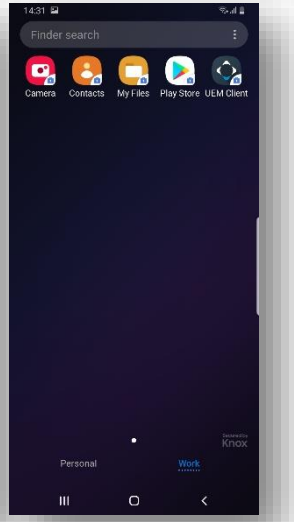
Profile Assignment



Device Enrollment Successful!



Device Area



Inside the Work Profile

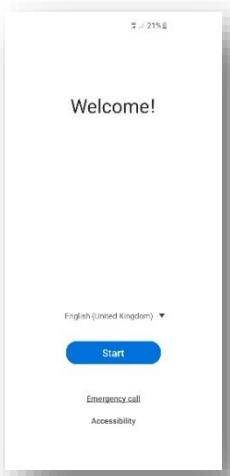
Android Enterprise: Work Profile on a Company Owned Device (WPC)

Android Enterprise Work Profile on a Company Owned Device (WPC) Deployment

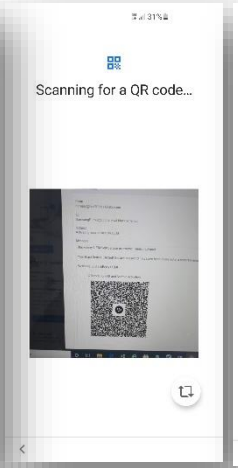
There are 2 ways you can enroll your device into Samsung Knox Manage as an Android Enterprise Work Profile on a Company Owned Device (**WPC**)

1. QR Code Enrollment
2. Zero Touch

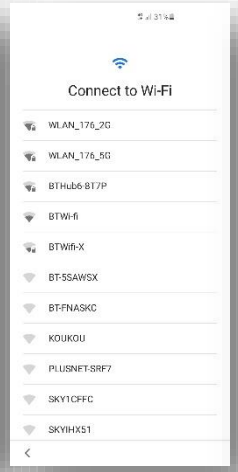
- Below is a screen-by-screen play to enroll your device using the QR Code Enrollment method.



Tap 6 times to Initiate QR code Scan

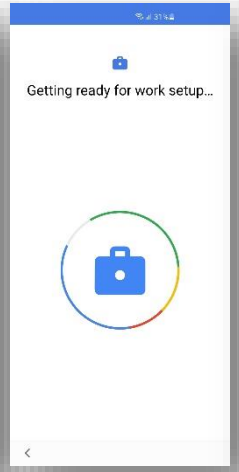


Scan QR code From the enrollment email

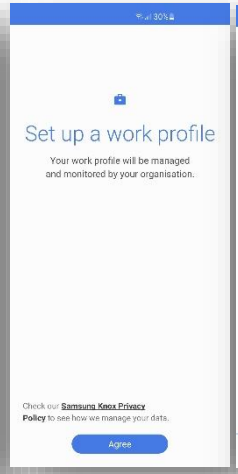


Connect to Wi-Fi

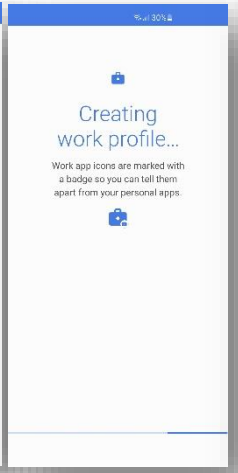
Select Next



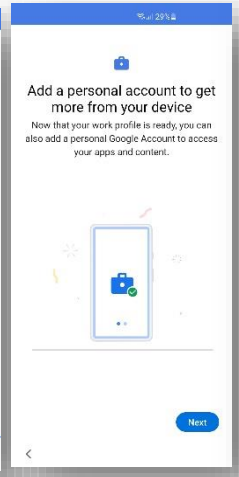
Work Setup



Agree



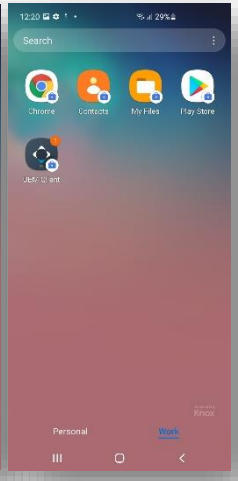
Creating Work Profile



Add personal account and follow on screen instructions

Creating Work Profile

Personal Space



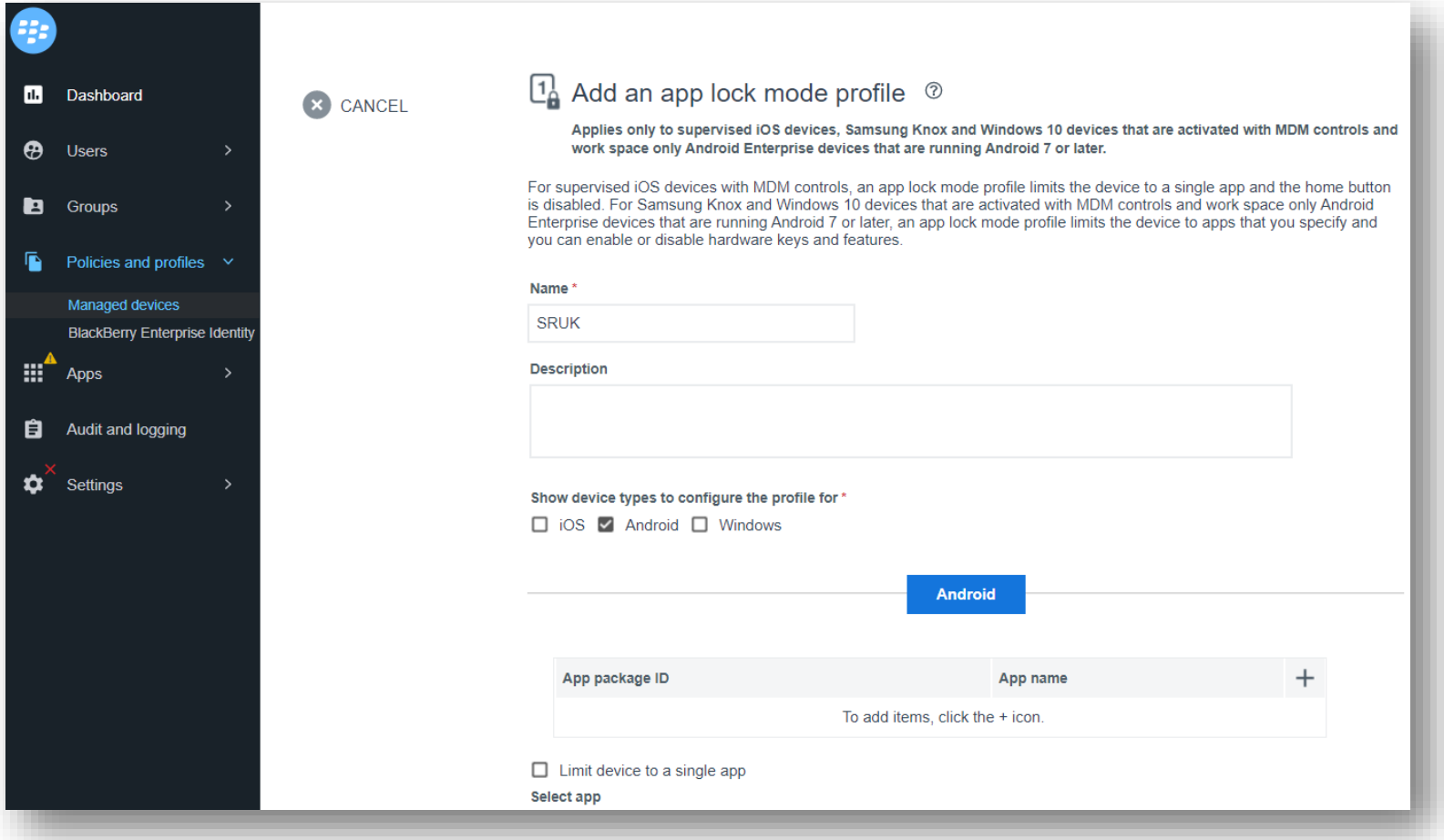
Work Space

Android Enterprise: Dedicated Device

Android Enterprise Dedicated Device Deployment

To enroll a device in the Android Enterprise Dedicated Device, you need to make sure that the Activation Profile is set as “Work space only (Android Enterprise fully managed device)”

The next step is to ensure that Policies and profile › App lock mode › select the + sign › Create and add app to lock mode profile › Assign to the right group or user.

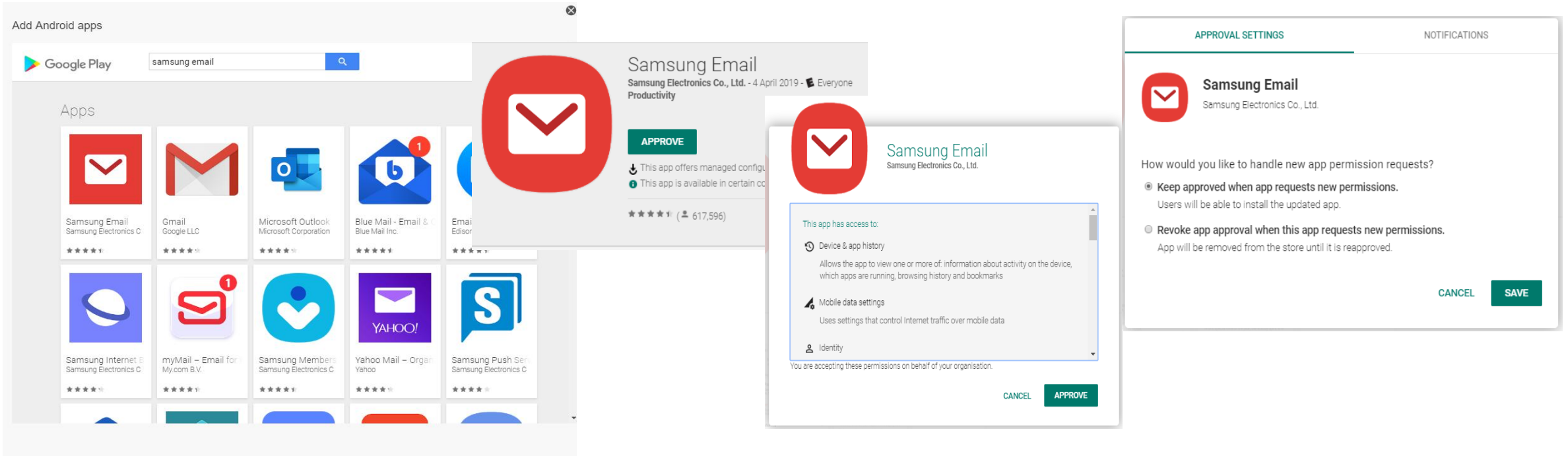


Please note that Dedicated Device enrollment is similar to Android Enterprise fully managed device.

Managed Google Play Configuration

In the Configuring Android Enterprise section of this document, we completed the majority of the work needed to configure applications to be used for Managed Google Play. All we have left to do is the following:

- In BlackBerry UEM console, go to **Apps** -> Click  -> **Google Play**
- Search for the App you want to distribute. For example; Samsung Email
- Click the **APPROVE** button.
- APPROVE the App Permission request
- Choose how you would like to handle new app permission requests and then click **SAVE**

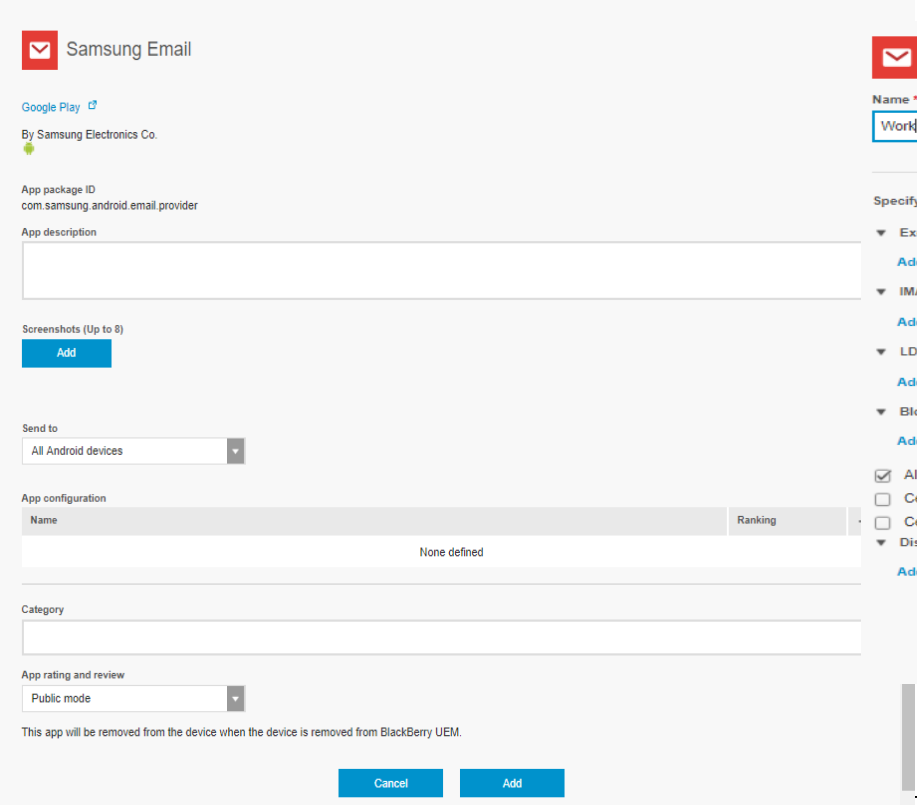


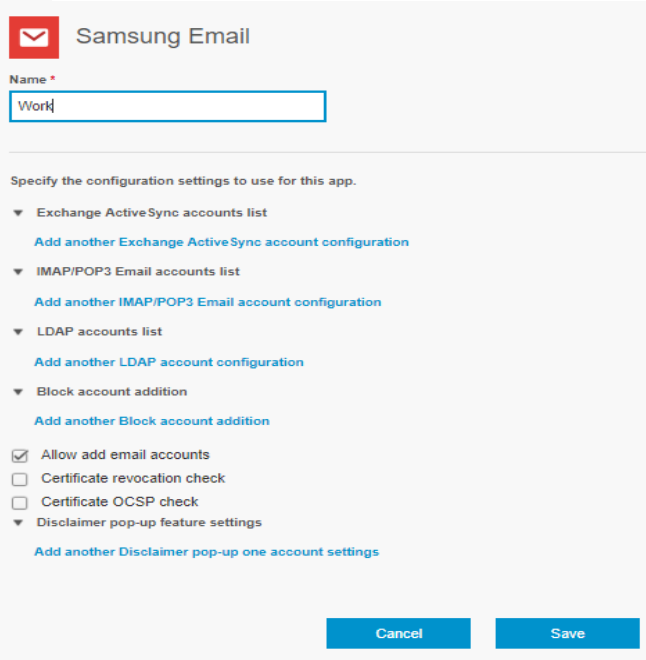
AppConfig on BlackBerry UEM

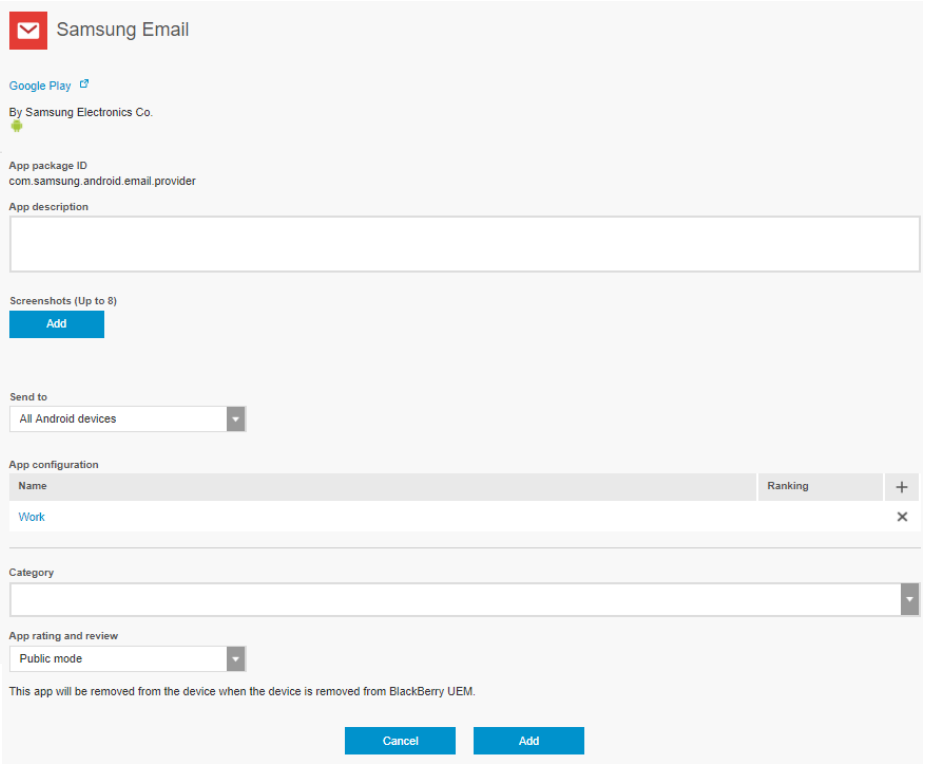
AppConfig

AppConfig enables you to send down application configuration profiles along with your managed apps when you distribute them through your Managed Google Play Store. This saves on having to have the UEM implement the required APIs for the app you are using so you can remotely configure it. To use AppConfig on BlackBerry UEM, follow the below instructions.

- From the previous slide, under *App configuration* -> Select the "+" -> Fill in the desired app configuration -> Select "Save"
- Click on Add; Now you can assign the Samsung email app to user.







Configure Knox Platform for Enterprise : Standard Edition

Knox Platform for Enterprise : Standard Edition

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]

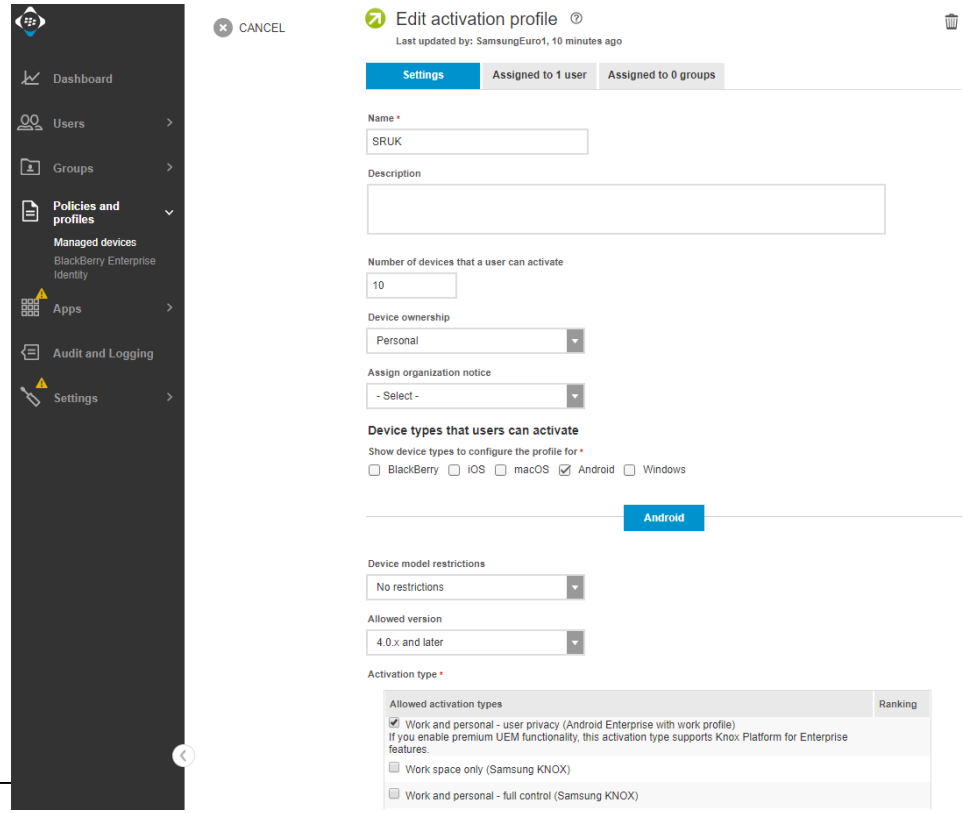
Knox Platform for Enterprise : Standard Edition offers free additional policies you can use to provide enhanced security, manageability and usability over your Samsung device fleet, running Android Enterprise on Oreo or above.

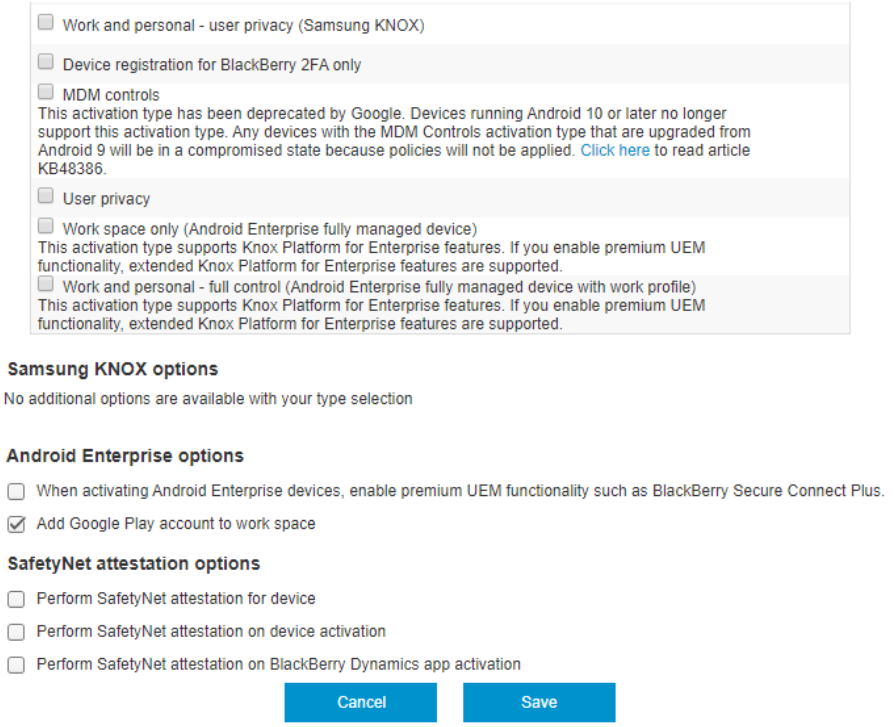
Configure Knox Platform for Enterprise : Standard Edition

Configure KPE : Standard Edition on BlackBerry UEM

To take advantage of the free additional APIs available in KPE Standard Edition, simply complete the below instructions.

- Navigate to *Policies and Profiles -> Under Policy , select Activation -> Activation Profile -> "+" sign*
- Fill the information requested and select your allowed activation types "*Work space only (Android Enterprise fully managed device)"*, *"Work and personal - full control (Android Enterprise fully managed device with work profile"* or *"Work and personal - user privacy (Android Enterprise with work profile)"*
- Under Android Enterprise options, untick "*When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus."*



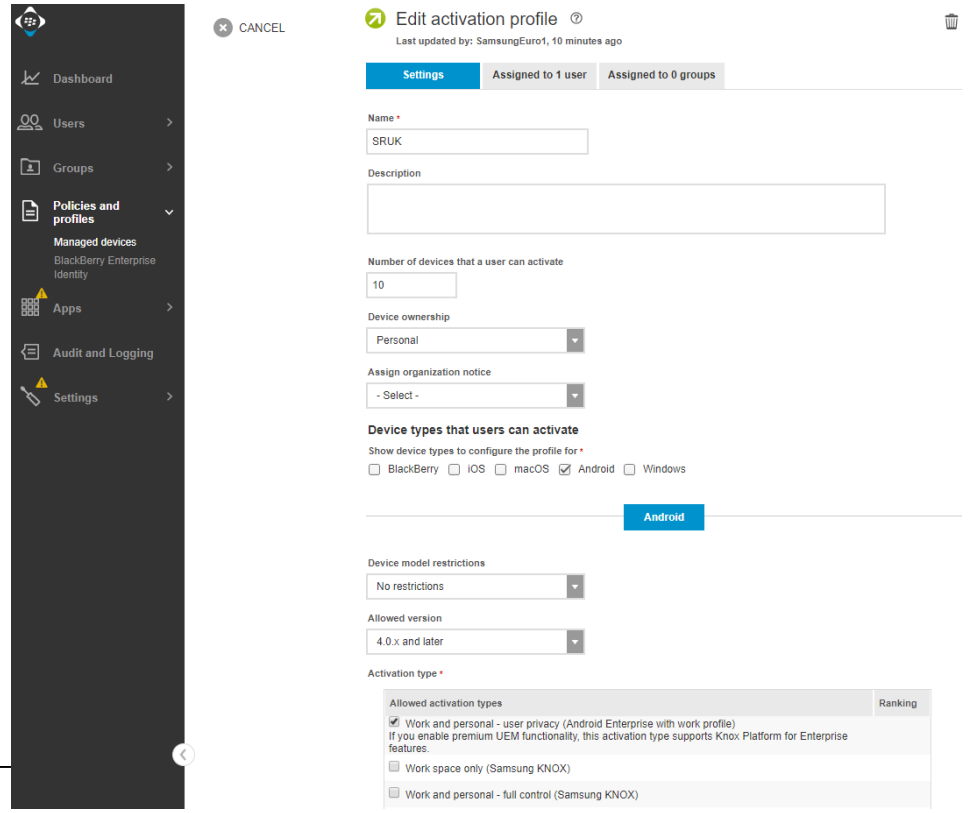


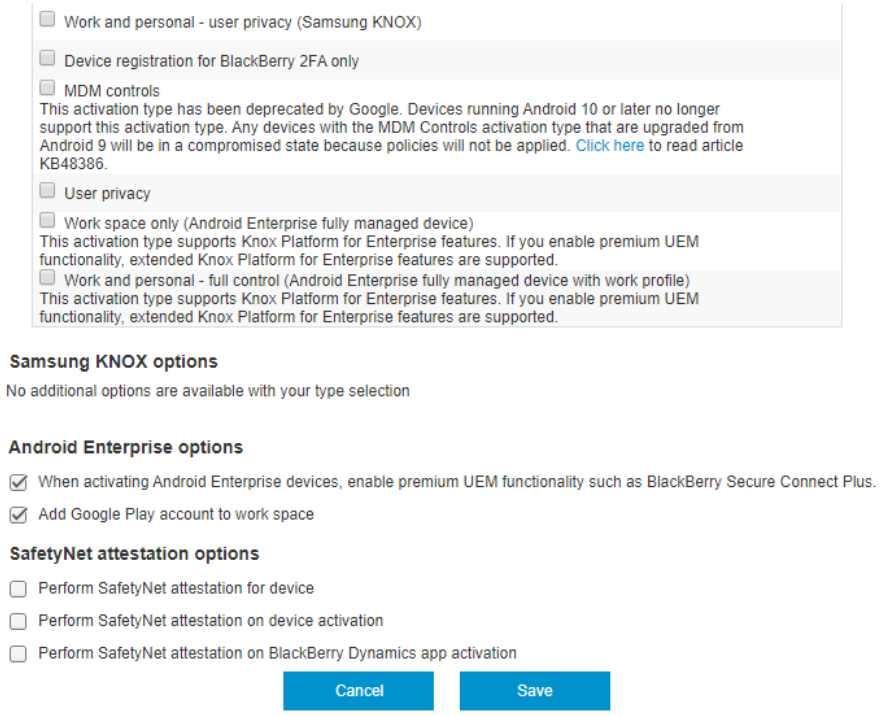
Knox Platform for Enterprise : Premium Edition

Configure KPE : Premium Edition on BlackBerry UEM

To take advantage of the paid additional APIs available in KPE Premium Edition, simply complete the below instructions.

- Navigate to *Policies and Profiles -> Under Policy , select Activation -> Activation Profile -> "+" sign*
- Fill the information requested and select your allowed activation types "*Work space only (Android Enterprise fully managed device)"*, *"Work and personal - full control (Android Enterprise fully managed device with work profile"* or *"Work and personal - user privacy (Android Enterprise with work profile)"*
- Under Android Enterprise options, tick "*When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus."*



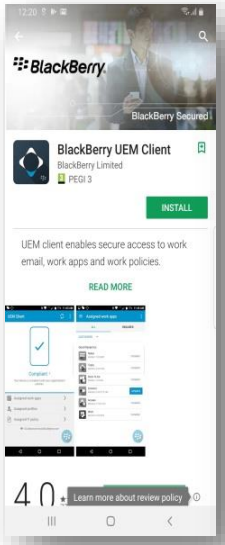


Knox Platform for Enterprise : Premium Edition

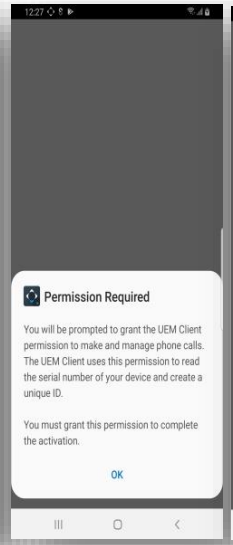
Android Enterprise BYOD deployment, Work Profile upgrade to KPE Premium

Now all you simply need to do is enroll your device by completing the following:

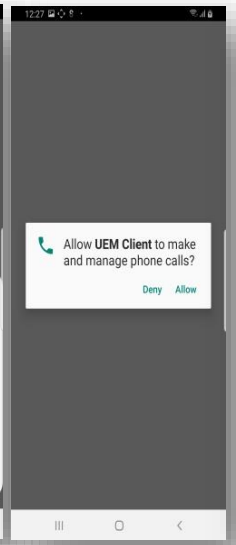
- On your device, go to the Google Play Store, download the BlackBerry UEM client, and enroll your device.



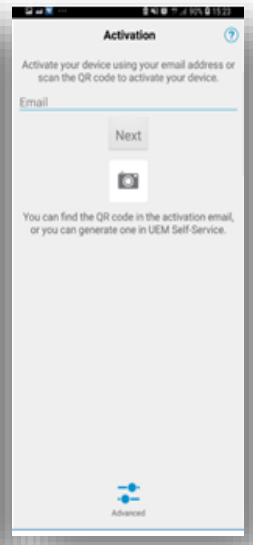
Install BlackBerry UEM Client from Google Play Store



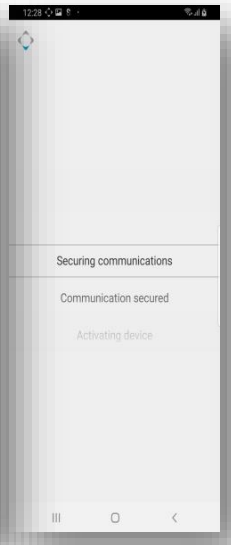
Accept the permission request



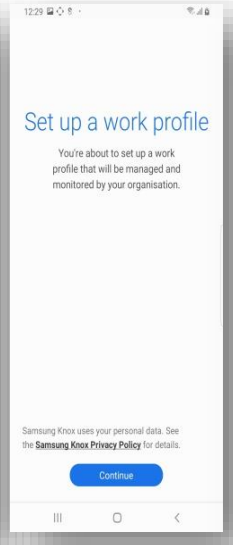
Allow UEM client to ...



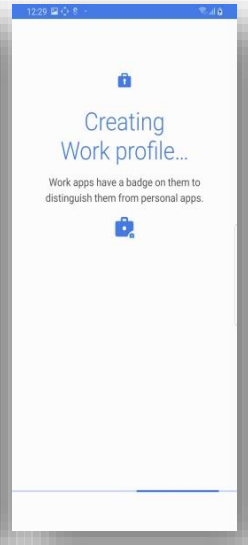
Enter Credentials



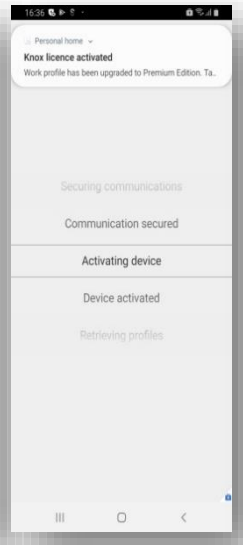
Start of the Enrollment



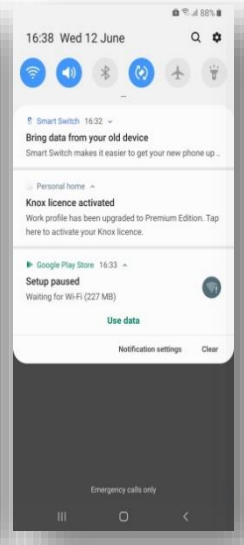
Click Continue to Set up a Work Profile



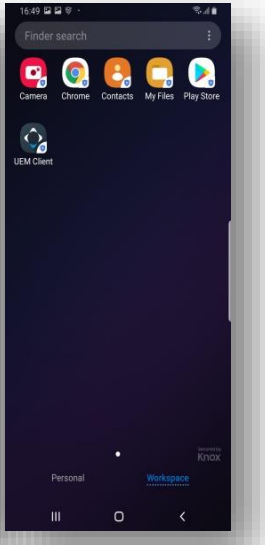
Creating Work Profile



KPE Premium Edition License activation request



Tap on Knox license activated notification to upgrade the Work Profile to KPE Premium

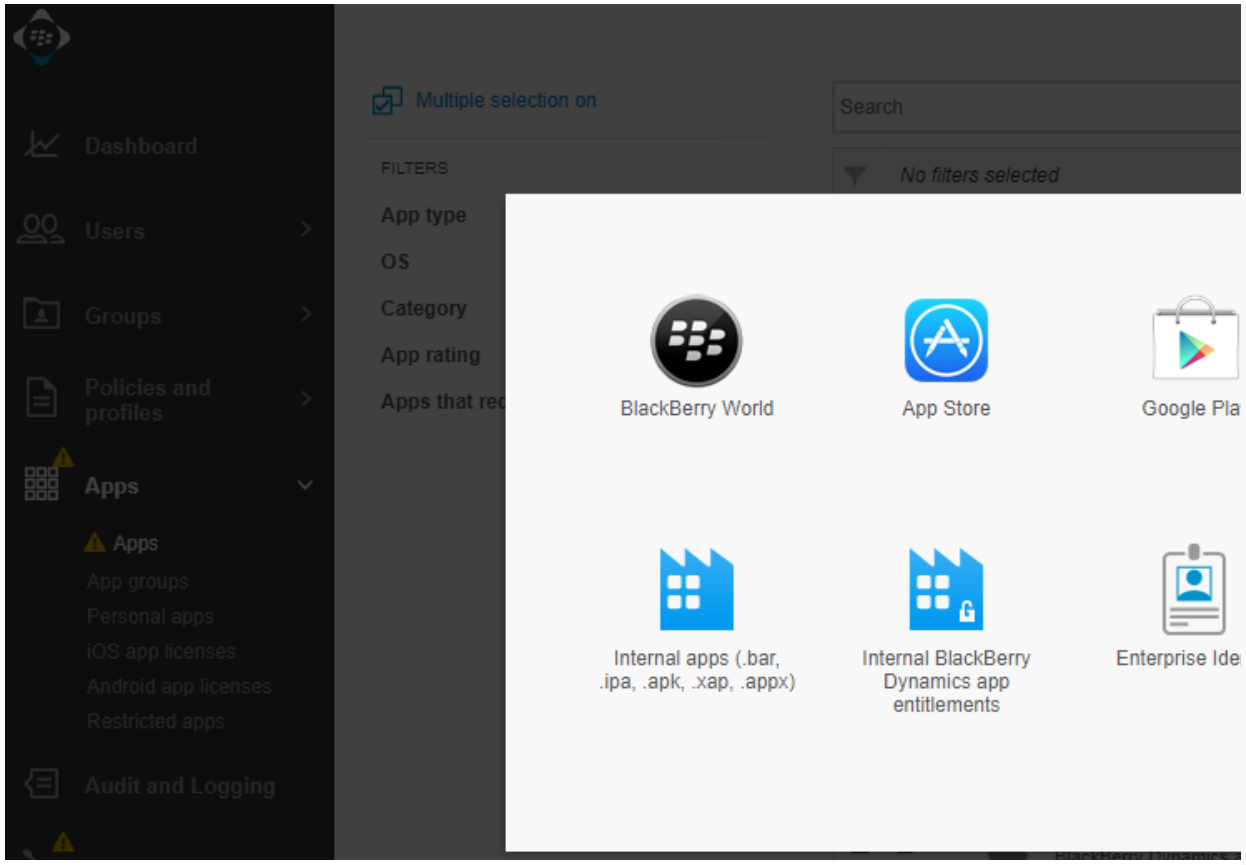


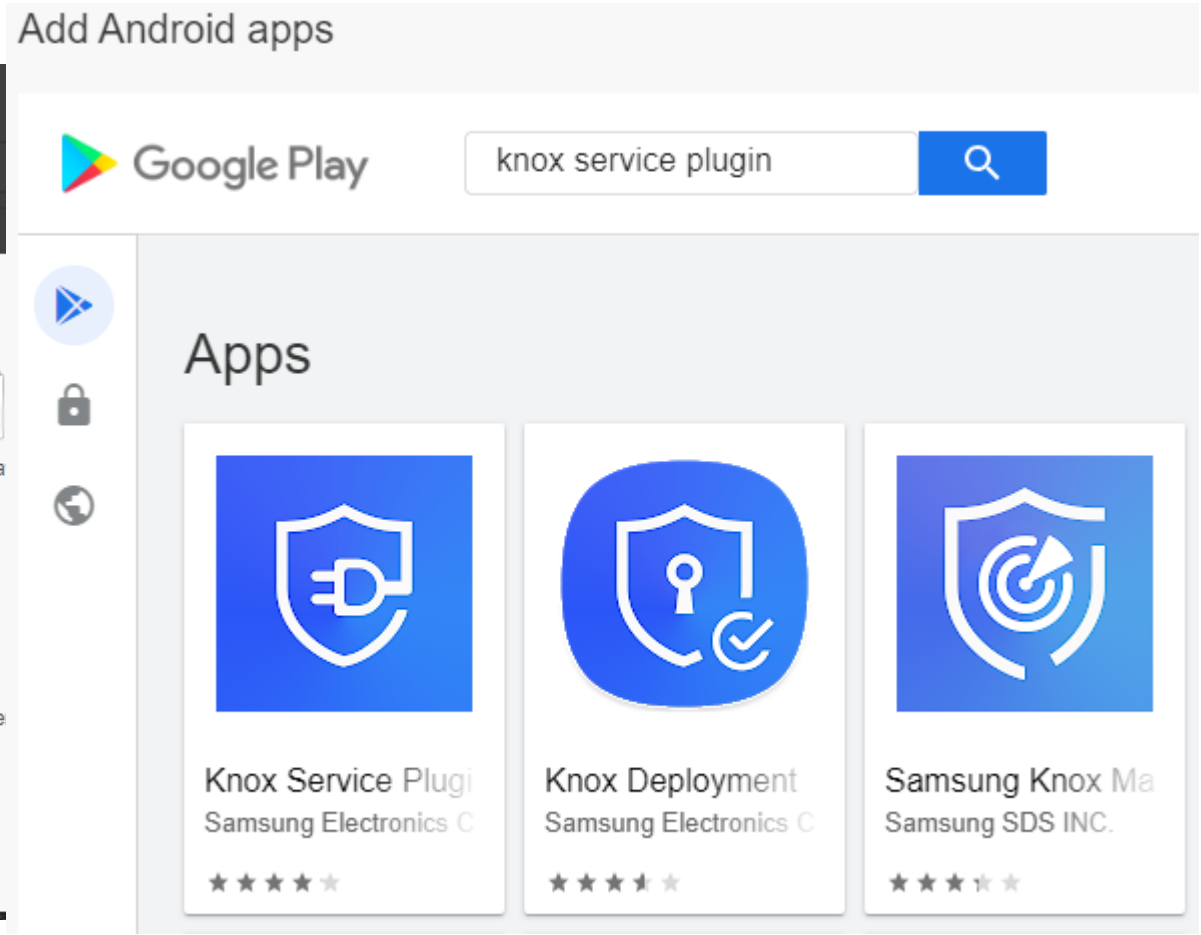
Work Profile device activated and Work Profile upgraded to KPE Premium

Knox Service Plugin [KSP]

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

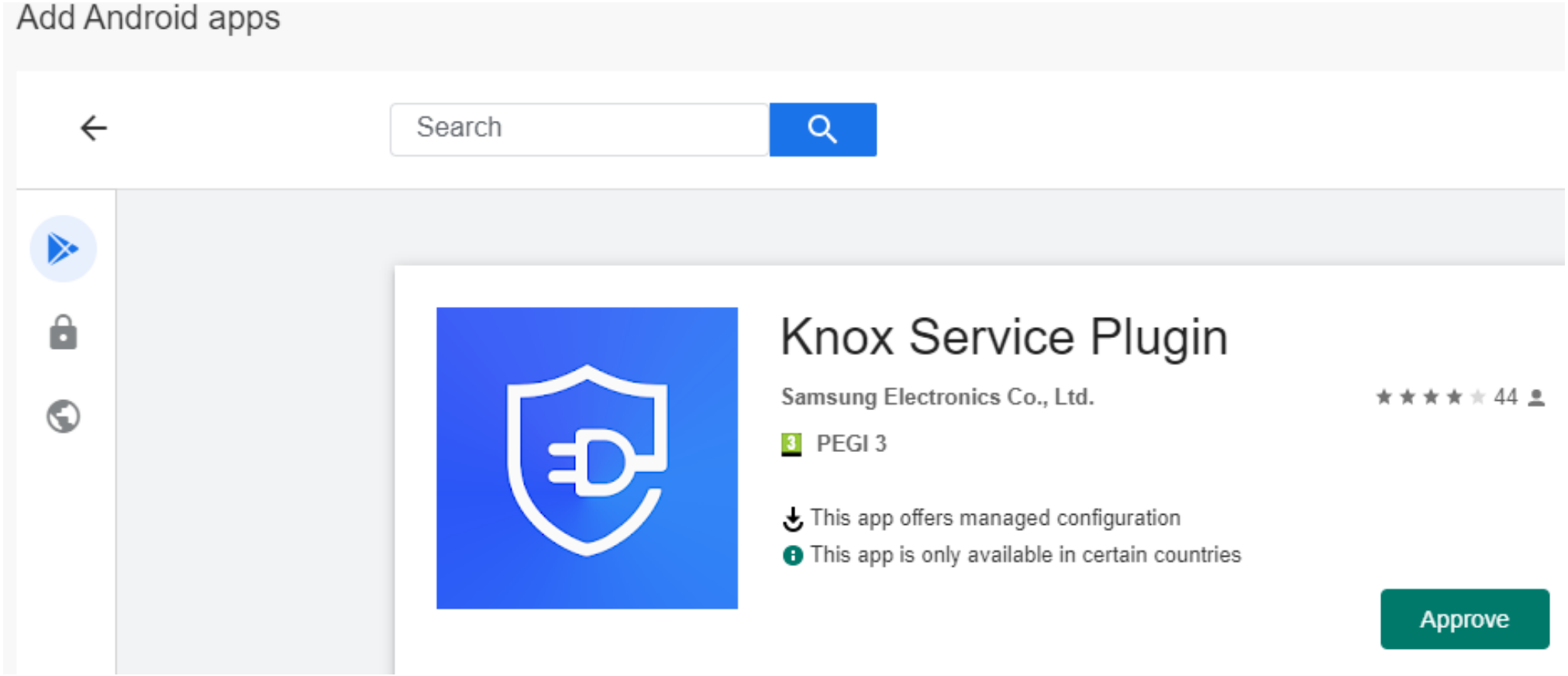
Navigate to *Apps ->*  *to add an app -> Google Play -> Search for Knox Service Plugin*





Knox Service Plugin [KSP]

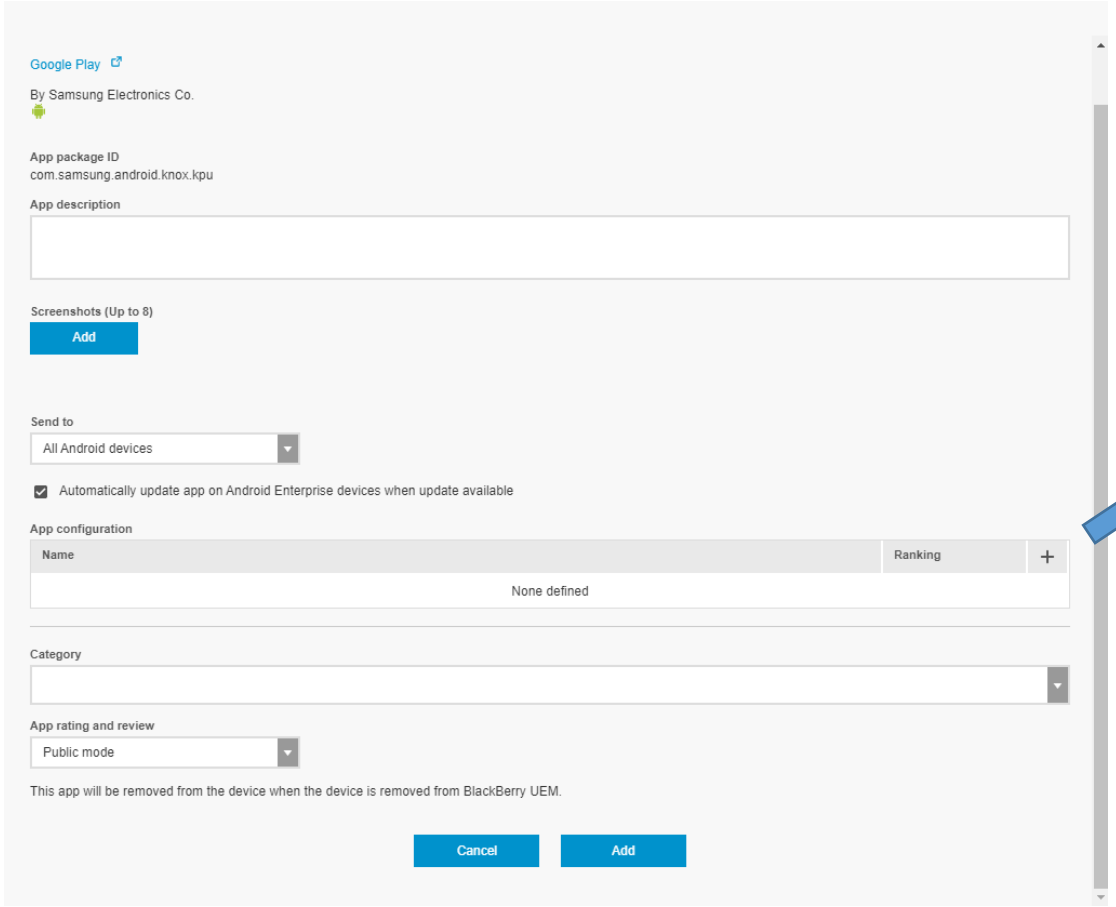
Approve etc...

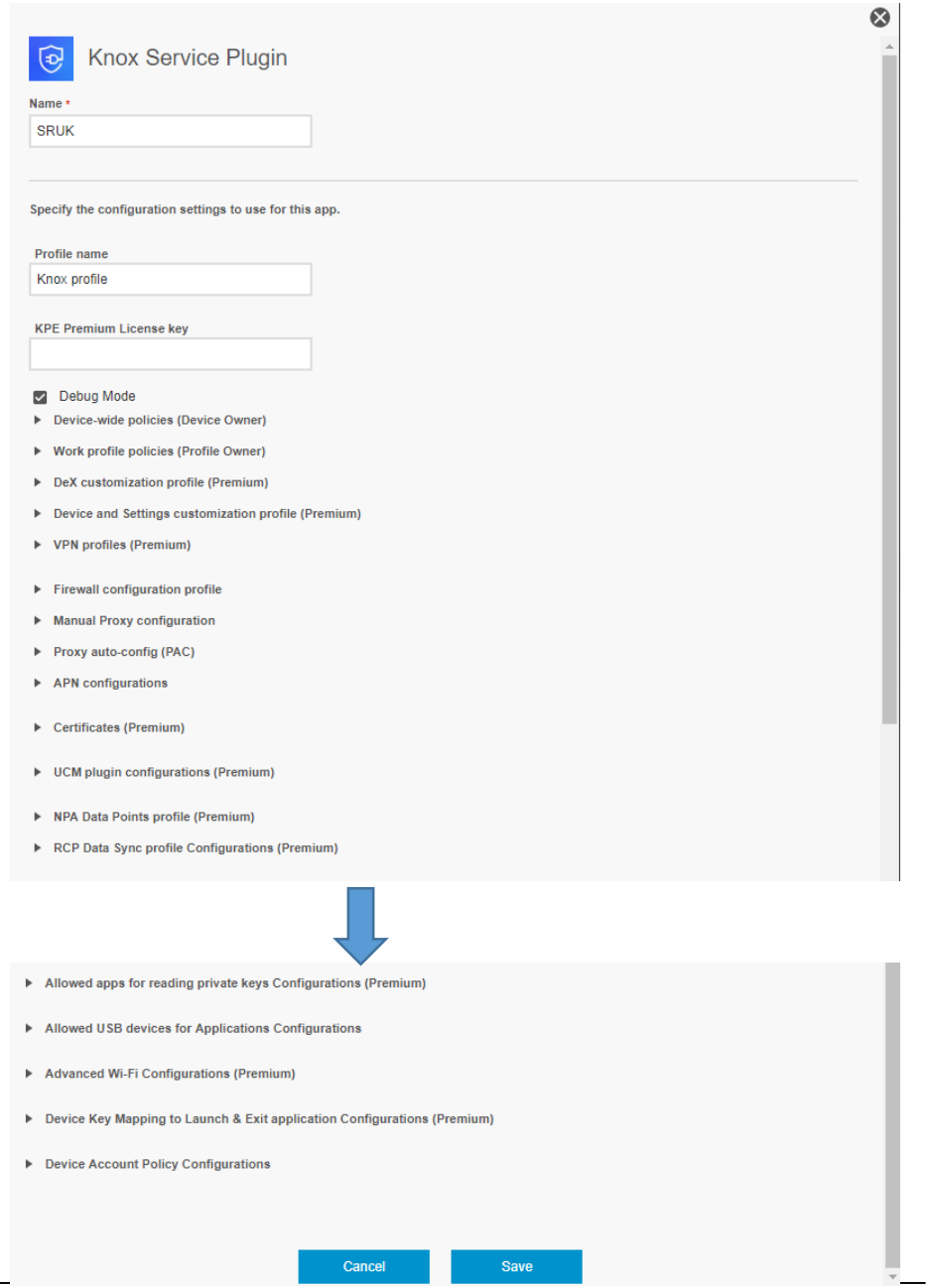


Knox Service Plugin [KSP]

Configure App Configuration

Select **+** under *App configuration* › a Knox Service Plugin windows will open ›
Fill in a *Name* › Expand Menu i.e *Device-wide Policies (Device Owner)* and Select a Policy and *Save*

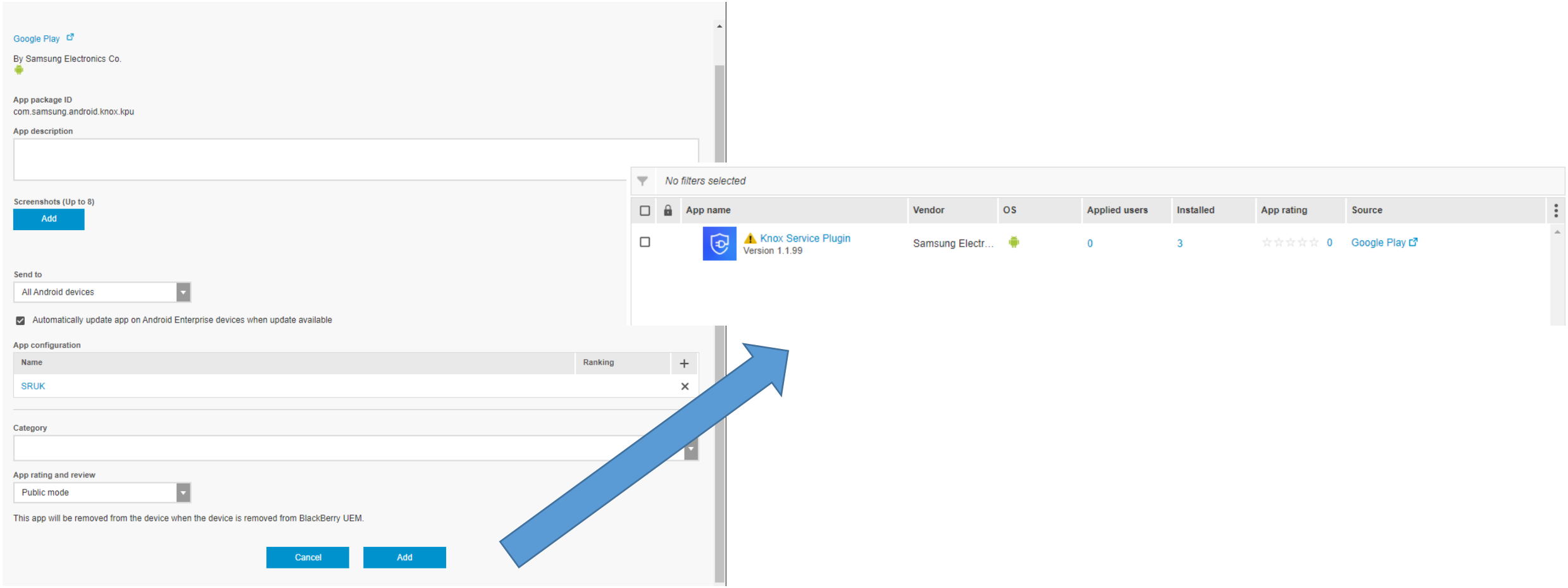




Knox Service Plugin [KSP]

Configure App Configuration

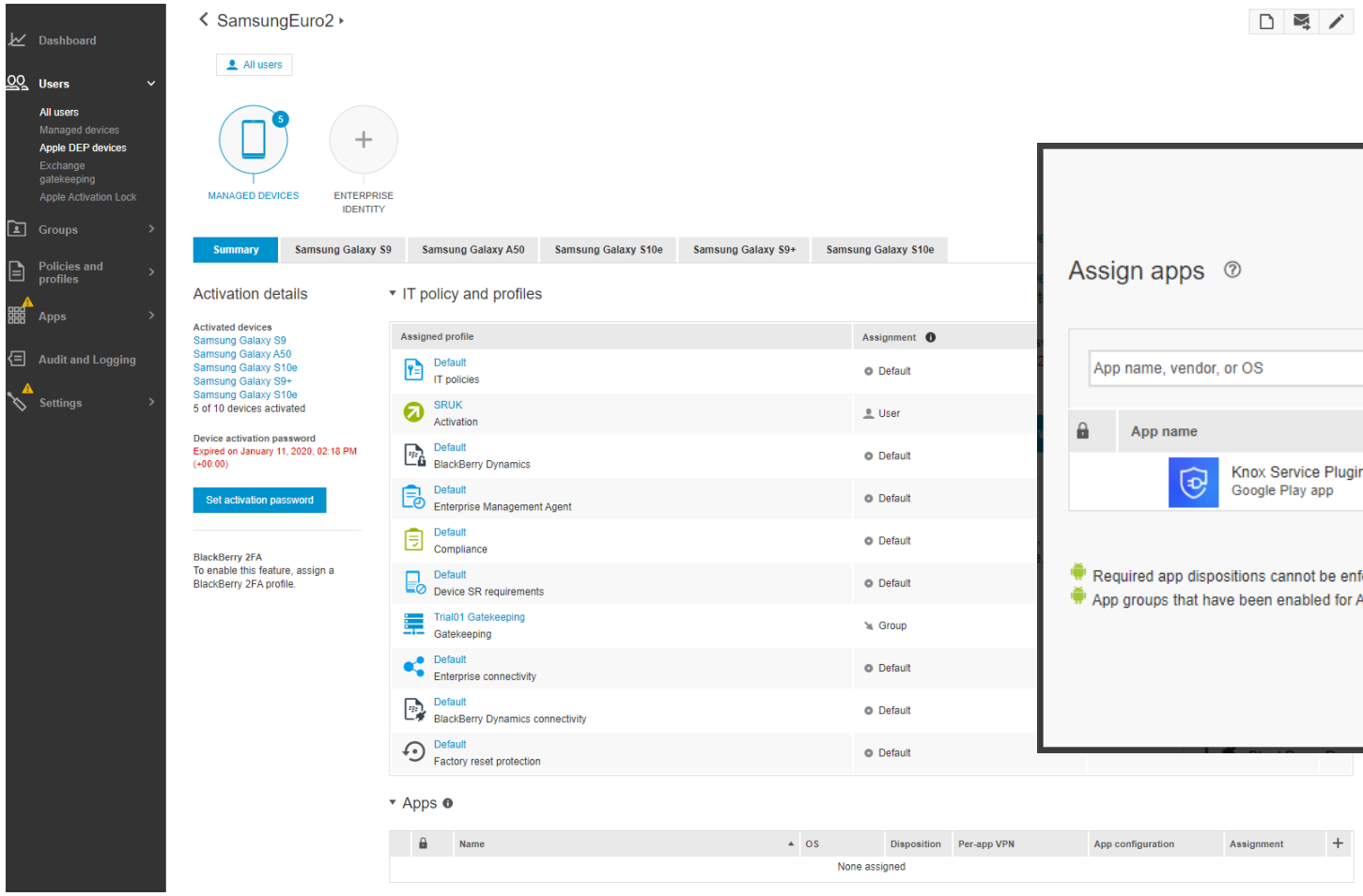
The app configuration created is visible under *App configuration* i.e SRUK and select *Add*



Knox Service Plugin [KSP]

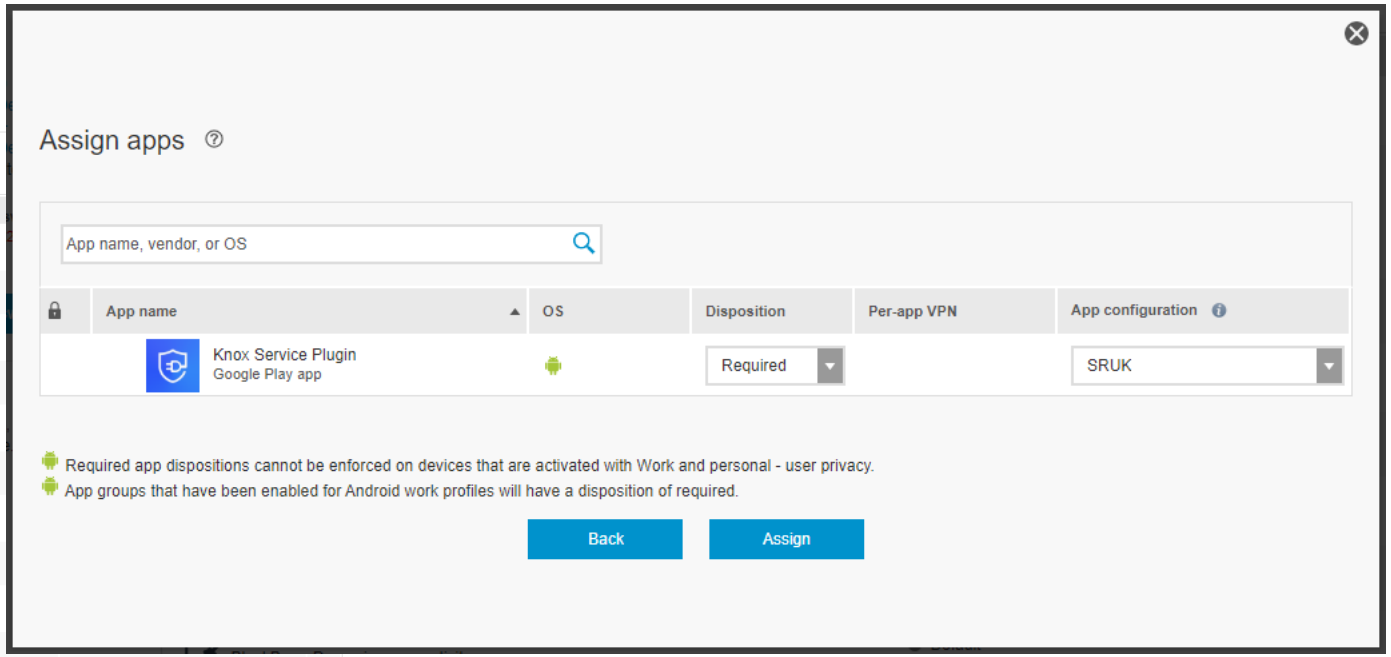
Assign Knox Service Plugin app to a user

Navigate to *Users*, Search and Select a user › Under **Apps**, select **+** sign to assign the KSP App



Disposition = *Required* to ensure the app is silently installed

App Configuration = Select the one created in page 28 i.e *SRUK* and select *Assign*

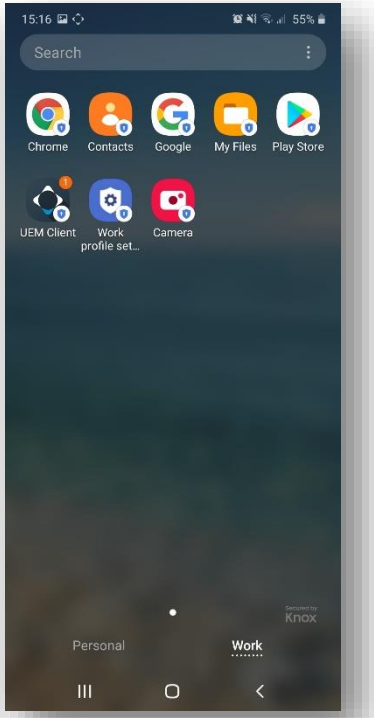


Knox Service Plugin [KSP]

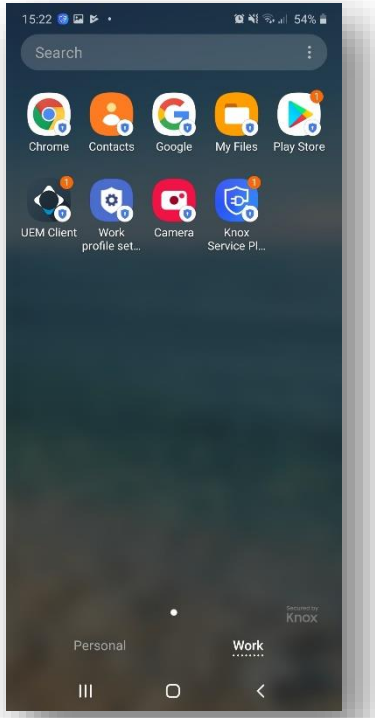
KSP deployment on the device

The below screen captures provide a view of the KSP app inside the Work Profile

Device enrolled as Work Profile



Inside the Work Profile prior to the KSP app deployment



KSP app deployed & visible * inside the Work Profile

* Please note the KSP is visible due to the fact debug mode has been enabled i n KSP configuration through managed app configuration

Document Information

This is version 2.3 of this document.

Thank you!

Knox