



BlackBerry UEM 12.14 & Knox Platform for Enterprise

May 2021
Samsung R&D Centre UK
(SRUK)

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]

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:

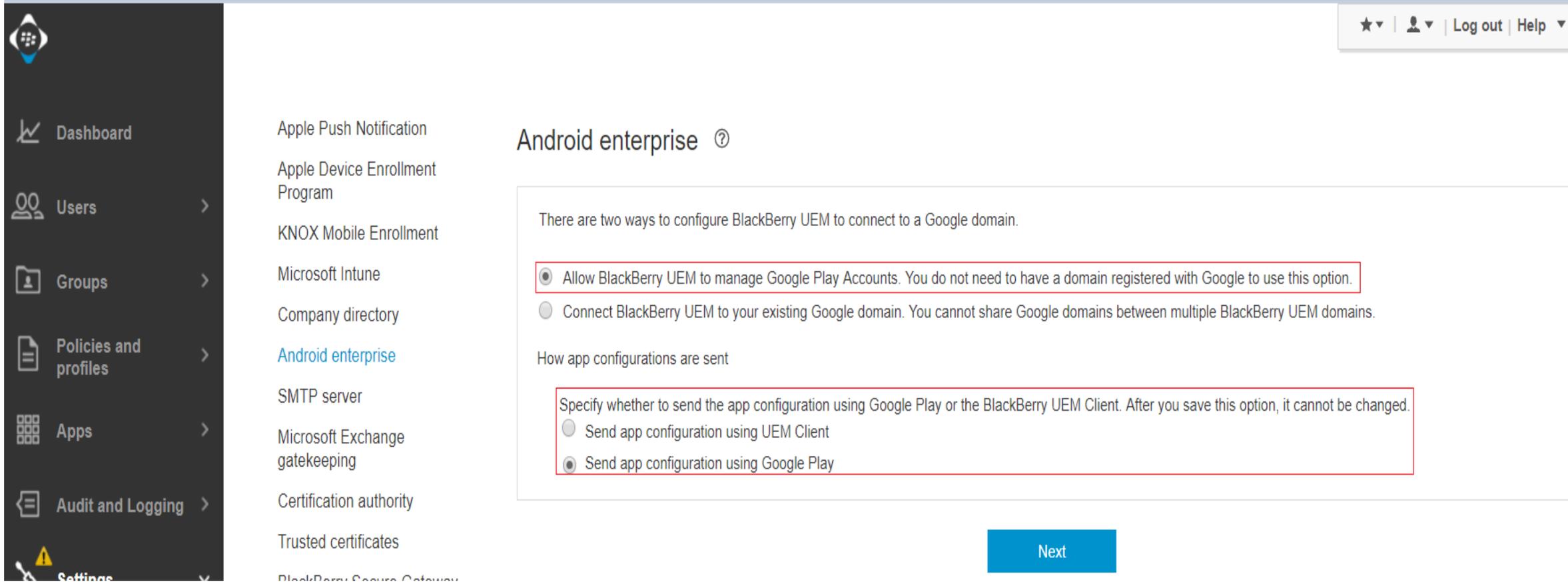
<https://www.blackberry.com/uk/en/products/endpoint-management/blackberry-enterprise-mobility-suite>

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.



The screenshot shows the BlackBerry UEM console interface. On the left is a dark sidebar with navigation options: Dashboard, Users, Groups, Policies and profiles, Apps, Audit and Logging, and Settings. The main content area is titled "Android enterprise" and contains the following text and options:

There are two ways to configure BlackBerry UEM to connect to a Google domain.

- Allow BlackBerry UEM to manage Google Play Accounts. You do not need to have a domain registered with Google to use this option.
- Connect BlackBerry UEM to your existing Google domain. You cannot share Google domains between multiple BlackBerry UEM domains.

How app configurations are sent

Specify whether to send the app configuration using Google Play or the BlackBerry UEM Client. After you save this option, it cannot be changed.

- Send app configuration using UEM Client
- Send app configuration using Google Play

A blue "Next" button is located at the bottom right of the configuration area.

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.



Bring Android to work

Get started

Business name

We need some details about your business

Business name

Your answer
Samsung Research UK

Enterprise mobility management (EMM) provider

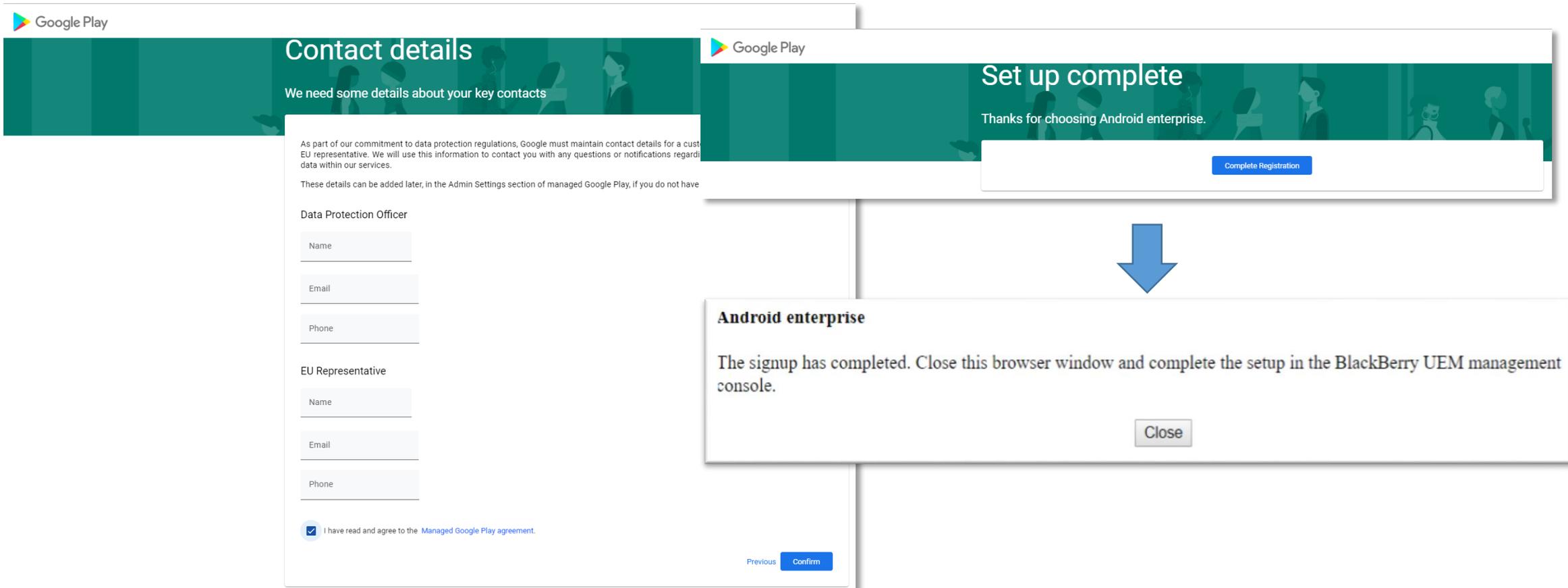
BlackBerry Ltd.

Previous

Next

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.....”



Contact details
We need some details about your key contacts

As part of our commitment to data protection regulations, Google must maintain contact details for a customer representative. We will use this information to contact you with any questions or notifications regarding data within our services.

These details can be added later, in the Admin Settings section of managed Google Play, if you do not have

Data Protection Officer

Name

Email

Phone

EU Representative

Name

Email

Phone

I have read and agree to the [Managed Google Play agreement](#).

Previous **Confirm**

Set up complete
Thanks for choosing Android enterprise.

Complete Registration

Android enterprise

The signup has completed. Close this browser window and complete the setup in the BlackBerry UEM management console.

Close

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*.

The screenshot shows the BlackBerry UEM console interface. On the left is a dark sidebar with navigation options: Dashboard, Users, Groups, Policies and profiles, Apps, Audit and Logging, and Settings (expanded). The main content area is titled 'Android enterprise' and features a 'Google Chrome: Fast & Secure' app card. The card includes a description, 'App permissions' section with radio buttons for 'Accept' (selected) and 'Do not accept', and a list of permissions under 'This app has access to:'. The permissions listed are: Device & app history (read your Web bookmarks and history), Identity (find accounts on the device, add or remove accounts), Contacts (find accounts on the device, read your contacts), and Locations (approximate location (network-based)). A top navigation bar contains 'Log out' and 'Help' options.

Configure Android Enterprise

- Android Enterprise is now fully configured

The screenshot displays the configuration interface for Android Enterprise. On the left is a dark sidebar menu with options: Dashboard, Users, Groups, Policies and profiles, Apps, Audit and Logging, and Settings (expanded). Under Settings, there are sub-items: General settings, External integration, App management, Self-Service, Administrators, Licensing, Infrastructure, Migration, Collaboration, BlackBerry Dynamics, Services, and BlackBerry Enterprise Identity. The main content area is divided into two columns. The left column lists various integration options: Apple Push Notification, Apple Device Enrollment Program, KNOX Mobile Enrollment, Microsoft Intune, Company directory, **Android enterprise** (highlighted in blue), SMTP server, Microsoft Exchange gatekeeping, Certification authority, Trusted certificates, BlackBerry Secure Gateway, BlackBerry Connectivity Node setup, BlackBerry 2FA server, and BlackBerry 2FA One-Time Password tokens. The right column is titled 'Android enterprise' and contains configuration details: Service account email address (wa4ac6cb1215fa22e8aba43ffc5770@pwp-comblackberryandroidmdm2.google.com.iam.gserviceaccount.com), Google administrator email address (b2bsruk5@gmail.com), Enterprise ID (LC01h3s6jd), and Android enterprise connection status with a 'Test connection' button. Below this, it states 'How app configurations are sent: Send app configuration using UEM Client'. At the bottom, there is a section for 'Android Zero Touch device enrollment' with a 'Learn more' link. In the top right corner of the interface, there are navigation links: a star icon, a user icon, 'Log out', and 'Help'.

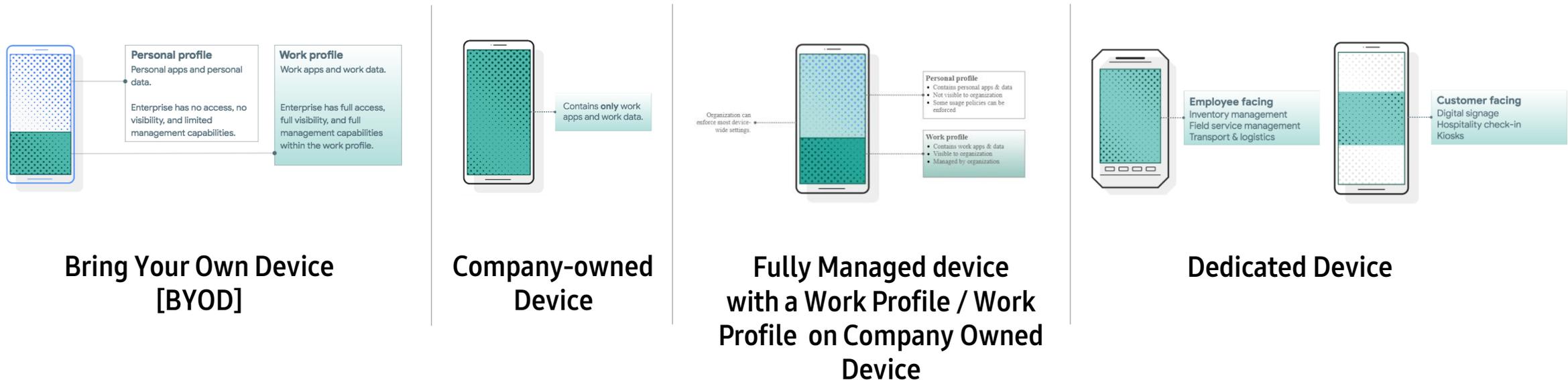
Android Enterprise Deployment Modes

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.



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.

Activation type options:

- Work space only (Samsung KNOX)
- Work and personal - full control (Samsung KNOX)
- Work and personal - user privacy (Samsung KNOX)
- Device registration for BlackBerry 2FA only
- MDM controls
This activation type has been deprecated by Google. Devices running Android 10 or later no longer support this activation type. Any devices with the MDM Controls activation type that are upgraded from Android 9 will be in a compromised state because policies will not be applied. [Click here to read article KB48386.](#)
- User privacy
- Work space only (Android Enterprise fully managed device)
This activation type supports Knox Platform for Enterprise features. If you enable premium UEM functionality, extended Knox Platform for Enterprise features are supported.

Samsung KNOX options
No additional options are available with your type selection

Android Enterprise options

- When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus.
- Add Google Play account to work space

SafetyNet attestation options

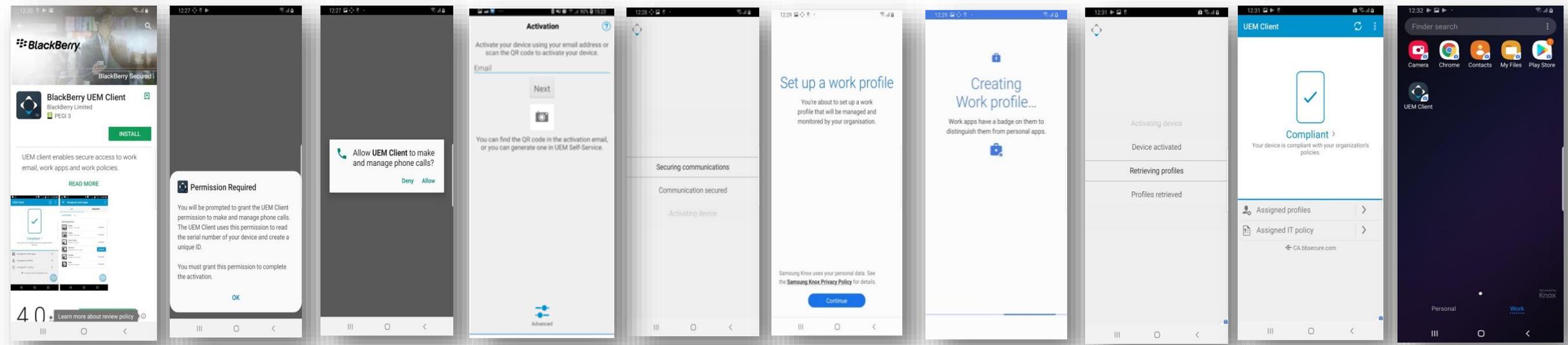
- Perform SafetyNet attestation for device
- Perform SafetyNet attestation on device activation
- Perform SafetyNet attestation on BlackBerry Dynamics app activation

Buttons: Cancel, Save

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 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.

Edit activation profile
Last updated by: SamsungEuro1, 10 minutes ago

Settings Assigned to 1 user Assigned to 0 groups

Name *
SRUK

Description

Number of devices that a user can activate
10

Device ownership
Personal

Assign organization notice
- Select -

Device types that users can activate
Show device types to configure the profile for *

BlackBerry iOS macOS Android Windows

Android

Device model restrictions
No restrictions

Allowed version
4.0.x and later

Activation type *

Allowed activation types	Ranking
<input checked="" type="checkbox"/> Work space only (Android Enterprise fully managed device) This activation type supports Knox Platform for Enterprise features. If you enable premium UEM functionality, extended Knox Platform for Enterprise features are supported.	
<input type="checkbox"/> Work and personal - user privacy (Android Enterprise with work profile) If you enable premium UEM functionality, this activation type supports Knox Platform for Enterprise features.	



<input type="checkbox"/> Work and personal - full control (Android Enterprise fully managed device with work profile) This activation type supports Knox Platform for Enterprise features. If you enable premium UEM functionality, extended Knox Platform for Enterprise features are supported.
<input type="checkbox"/> Work space only (Samsung KNOX)
<input type="checkbox"/> Work and personal - full control (Samsung KNOX)
<input type="checkbox"/> Work and personal - user privacy (Samsung KNOX)
<input type="checkbox"/> Device registration for BlackBerry 2FA only
<input type="checkbox"/> MDM controls This activation type has been deprecated by Google. Devices running Android 10 or later no longer support this activation type. Any devices with the MDM Controls activation type that are upgraded from Android 9 will be in a compromised state because policies will not be applied. Click here to read article KB48386.
<input type="checkbox"/> User privacy

Samsung KNOX options

No additional options are available with your type selection

Android Enterprise options

- When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus.
- Add Google Play account to work space

SafetyNet attestation options

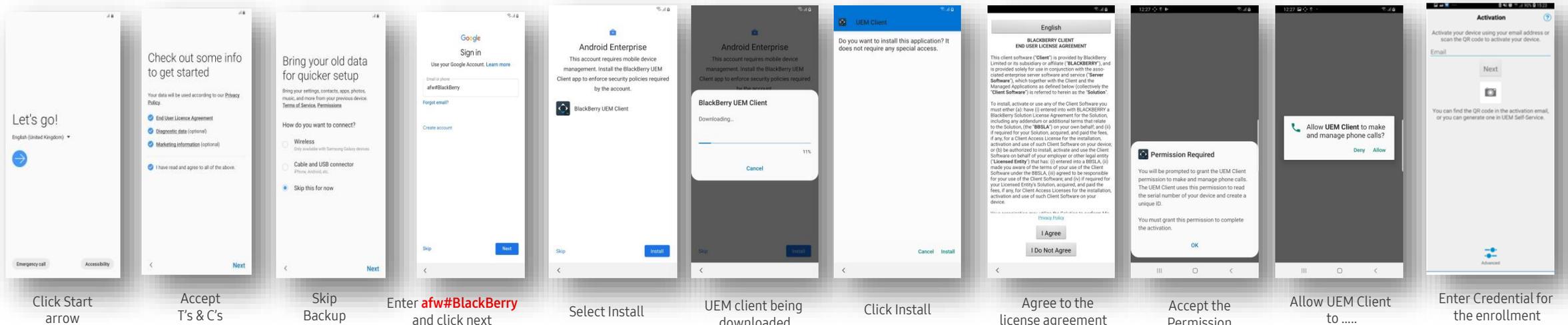
- Perform SafetyNet attestation for device
- Perform SafetyNet attestation on device activation
- Perform SafetyNet attestation on BlackBerry Dynamics app activation

Android Enterprise Company Owned Device Deployment

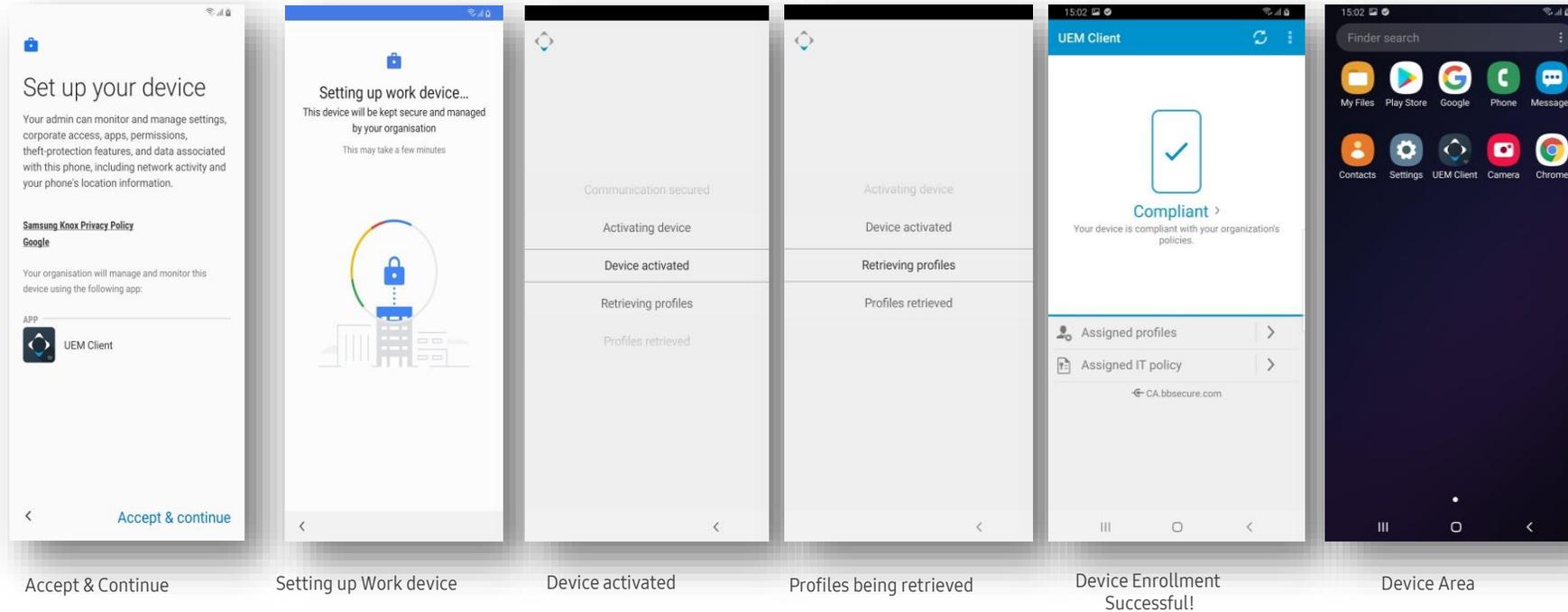
To enroll your device as an Android Enterprise Company Owned device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 4 ways you can enroll your device into BlackBerry UEM as an Android Enterprise Company Owned device.

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 Deployment



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.

Edit activation profile
Last updated by: SamsungEuro1, 10 minutes ago

Settings | Assigned to 1 user | Assigned to 0 groups

Name *
SRUK

Description

Number of devices that a user can activate
10

Device ownership
Personal

Assign organization notice
- Select -

Device types that users can activate
Show device types to configure the profile for *

BlackBerry iOS macOS Android Windows

Android

Device model restrictions
No restrictions

Allowed version
4.0.x and later

Activation type *

Allowed activation types	Ranking
<input checked="" type="checkbox"/> Work and personal - full control (Android Enterprise fully managed device with work profile) This activation type supports Knox Platform for Enterprise features. If you enable premium UEM functionality, extended Knox Platform for Enterprise features are supported.	
<input type="checkbox"/> Work space only (Samsung KNOX)	
<input type="checkbox"/> Work and personal - full control (Samsung KNOX)	

Work and personal - user privacy (Samsung KNOX)
 Device registration for BlackBerry 2FA only
 MDM controls
This activation type has been deprecated by Google. Devices running Android 10 or later no longer support this activation type. Any devices with the MDM Controls activation type that are upgraded from Android 9 will be in a compromised state because policies will not be applied. [Click here](#) to read article KB48386.
 User privacy
 Work space only (Android Enterprise fully managed device)
This activation type supports Knox Platform for Enterprise features. If you enable premium UEM functionality, extended Knox Platform for Enterprise features are supported.
 Work and personal - user privacy (Android Enterprise with work profile)
If you enable premium UEM functionality, this activation type supports Knox Platform for Enterprise features.

Samsung KNOX options
No additional options are available with your type selection

Android Enterprise options
 When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus.
 Add Google Play account to work space

SafetyNet attestation options
 Perform SafetyNet attestation for device
 Perform SafetyNet attestation on device activation
 Perform SafetyNet attestation on BlackBerry Dynamics app activation

Cancel Save

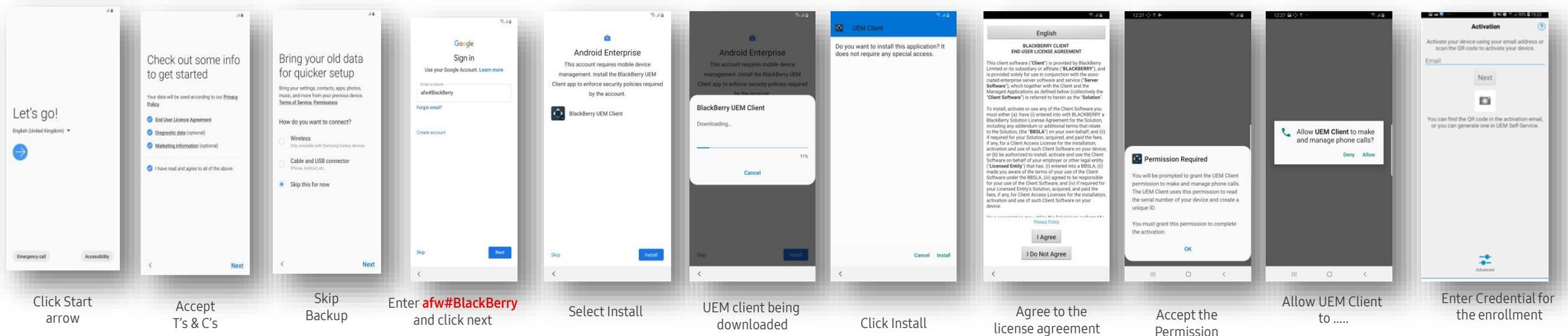
Android Enterprise: Fully Managed Device with a Work Profile (COMP)

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.

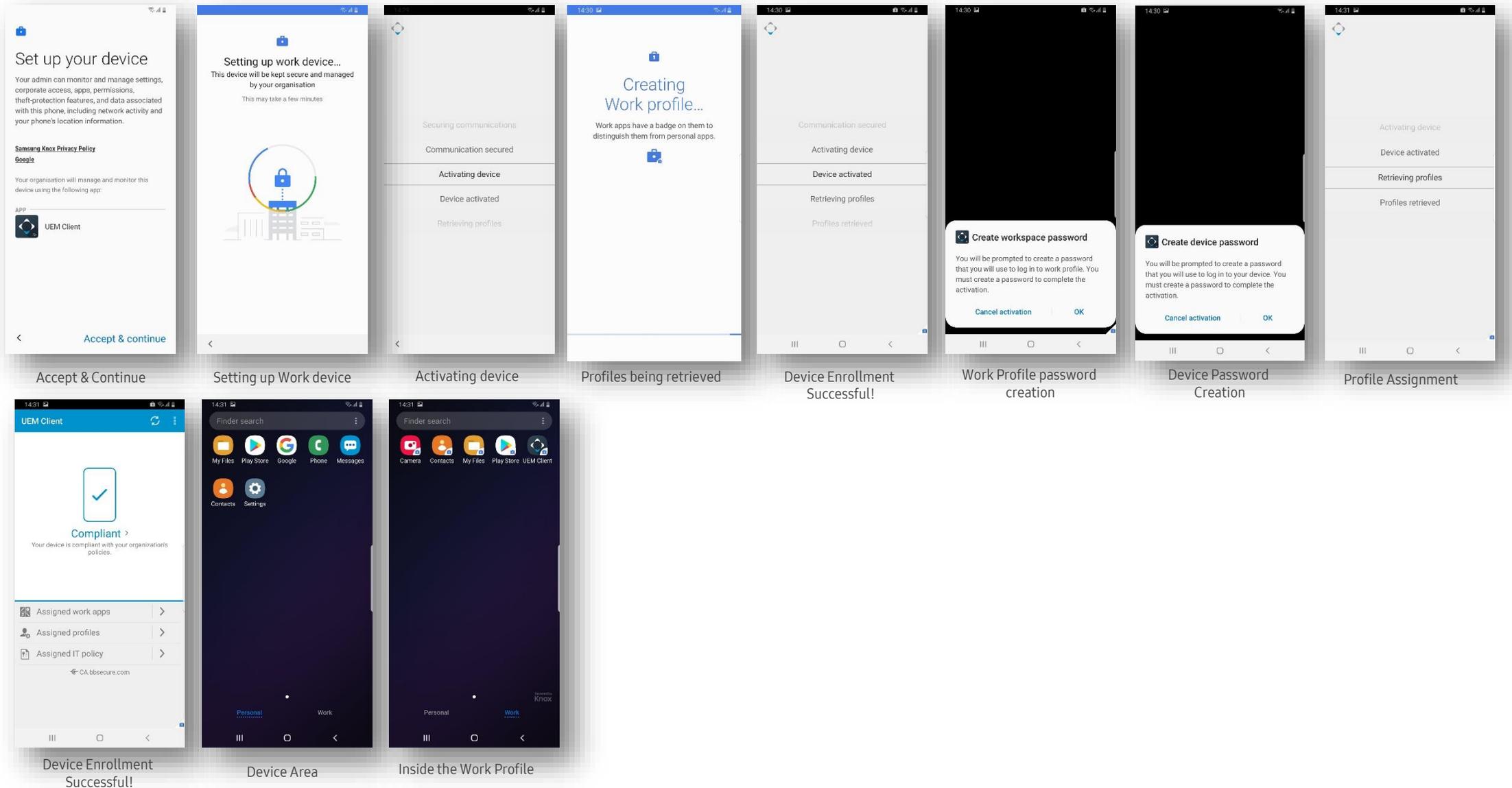
1. DPC Identifier [Also known as the hashtag method] **afw#BlackBerry**
2. QR Code Enrollment
3. NFC
4. Knox Mobile Enrollment

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



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

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



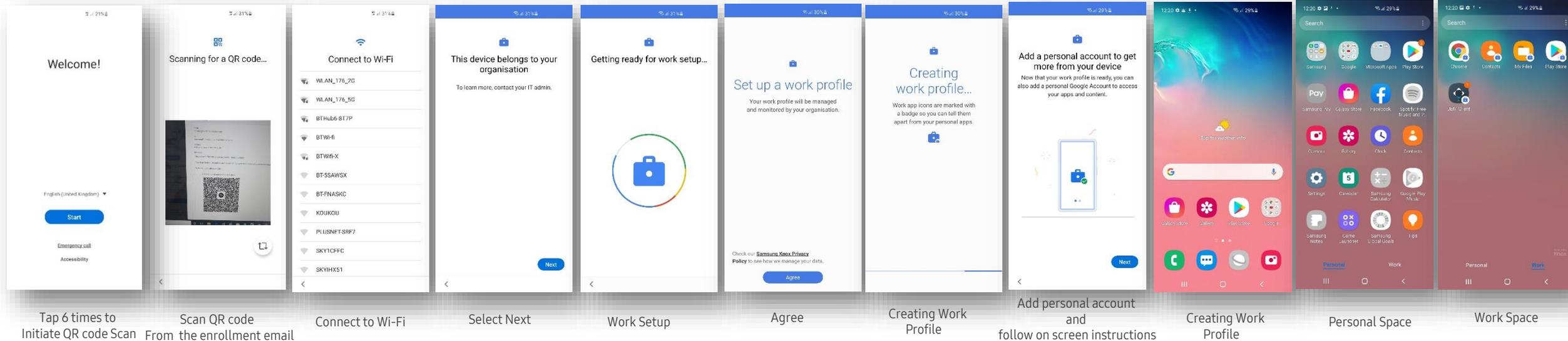
Android Enterprise: Work Profile on a Company Owned Device (WPC)

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.



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.

ADD AN APP LOCK MODE PROFILE

Applies only to supervised iOS devices, Samsung Knox and Windows 10 devices that are activated with MDM controls and work space only Android Enterprise devices that are running Android 7 or later.

For supervised iOS devices with MDM controls, an app lock mode profile limits the device to a single app and the home button is disabled. For Samsung Knox and Windows 10 devices that are activated with MDM controls and work space only Android Enterprise devices that are running Android 7 or later, an app lock mode profile limits the device to apps that you specify and you can enable or disable hardware keys and features.

Name *
SRUK

Description

Show device types to configure the profile for *
 iOS Android Windows

Android

App package ID	App name	+
To add items, click the + icon.		

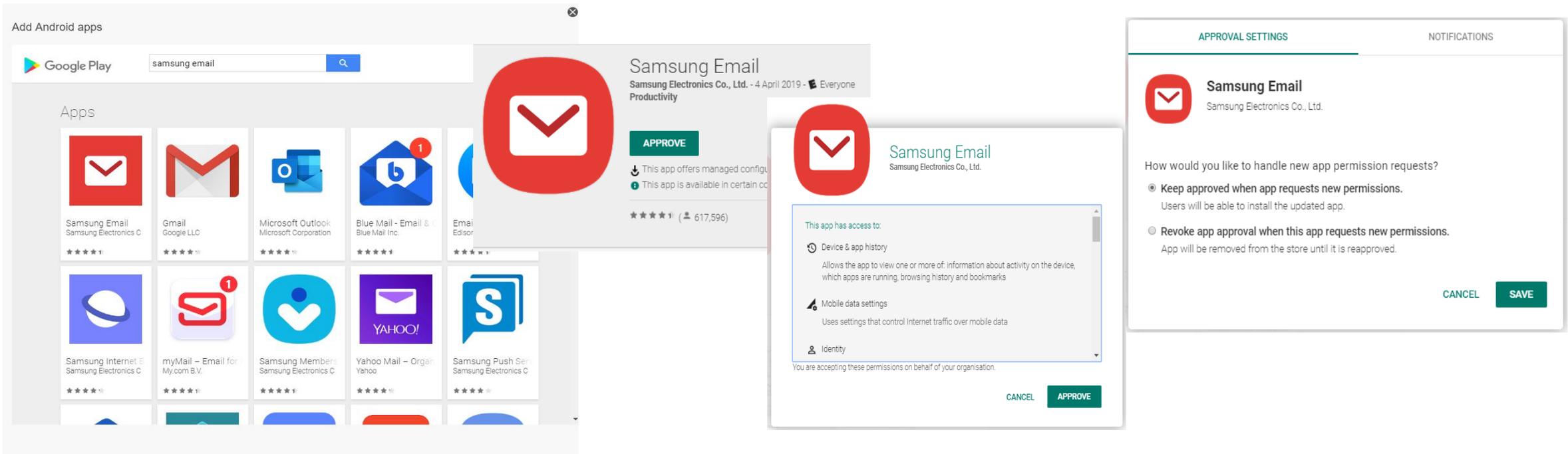
Limit device to a single app
Select app

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**

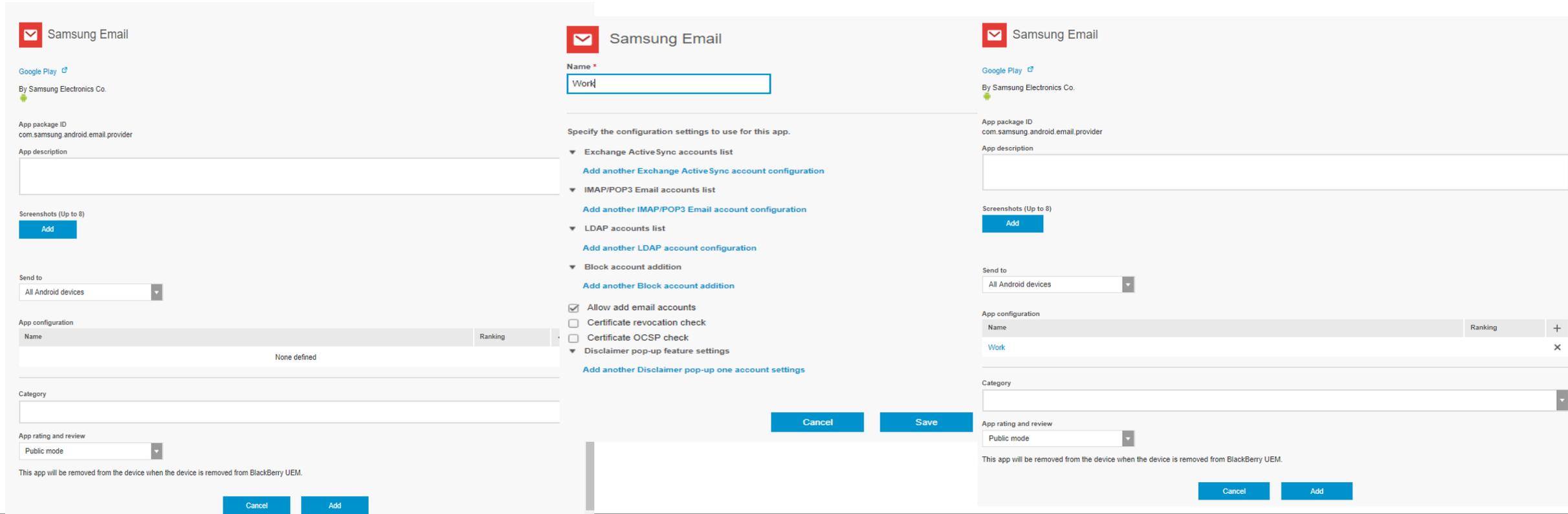


The screenshot illustrates the workflow in the BlackBerry UEM console for approving an app from Google Play. It shows the 'Add Android apps' screen with a search for 'samsung email'. The 'Samsung Email' app is selected, and the 'APPROVE' button is highlighted. A modal window displays the app's permissions: Device & app history, Mobile data settings, and Identity. A second modal window shows the 'APPROVAL SETTINGS' for Samsung Email, with 'Keep approved when app requests new permissions' selected.

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.



The image displays three sequential screenshots of the BlackBerry UEM interface for configuring the Samsung Email app. The first screenshot shows the app's basic information, including the package ID 'com.samsung.android.email.provider' and the 'Send to' dropdown set to 'All Android devices'. The second screenshot shows the configuration settings page, where the 'Name' field is filled with 'Work' and the 'Allow add email accounts' checkbox is checked. The third screenshot shows the final configuration summary page, with the 'Name' field set to 'Work' and the 'App rating and review' dropdown set to 'Public mode'. Each screenshot includes 'Cancel' and 'Add' buttons at the bottom.

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 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.*”

Samsung KNOX options

No additional options are available with your type selection

Android Enterprise options

When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus.

Add Google Play account to work space

SafetyNet attestation options

Perform SafetyNet attestation for device

Perform SafetyNet attestation on device activation

Perform SafetyNet attestation on BlackBerry Dynamics app activation

Cancel

Save

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.”*

Edit activation profile
Last updated by: SamsungEuro1, 10 minutes ago

Settings Assigned to 1 user Assigned to 0 groups

Name *
SRUK

Description

Number of devices that a user can activate
10

Device ownership
Personal

Assign organization notice
- Select -

Device types that users can activate
Show device types to configure the profile for *
 BlackBerry iOS macOS Android Windows

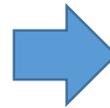
Android

Device model restrictions
No restrictions

Allowed version
4.0.x and later

Activation type *

Allowed activation types	Ranking
<input checked="" type="checkbox"/> Work and personal - user privacy (Android Enterprise with work profile) If you enable premium UEM functionality, this activation type supports Knox Platform for Enterprise features.	
<input type="checkbox"/> Work space only (Samsung KNOX)	
<input type="checkbox"/> Work and personal - full control (Samsung KNOX)	



Work and personal - user privacy (Samsung KNOX)

Device registration for BlackBerry 2FA only

MDM controls
This activation type has been deprecated by Google. Devices running Android 10 or later no longer support this activation type. Any devices with the MDM Controls activation type that are upgraded from Android 9 will be in a compromised state because policies will not be applied. [Click here](#) to read article KB48386.

User privacy

Work space only (Android Enterprise fully managed device)
This activation type supports Knox Platform for Enterprise features. If you enable premium UEM functionality, extended Knox Platform for Enterprise features are supported.

Work and personal - full control (Android Enterprise fully managed device with work profile)
This activation type supports Knox Platform for Enterprise features. If you enable premium UEM functionality, extended Knox Platform for Enterprise features are supported.

Samsung KNOX options

No additional options are available with your type selection

Android Enterprise options

- When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus.
- Add Google Play account to work space

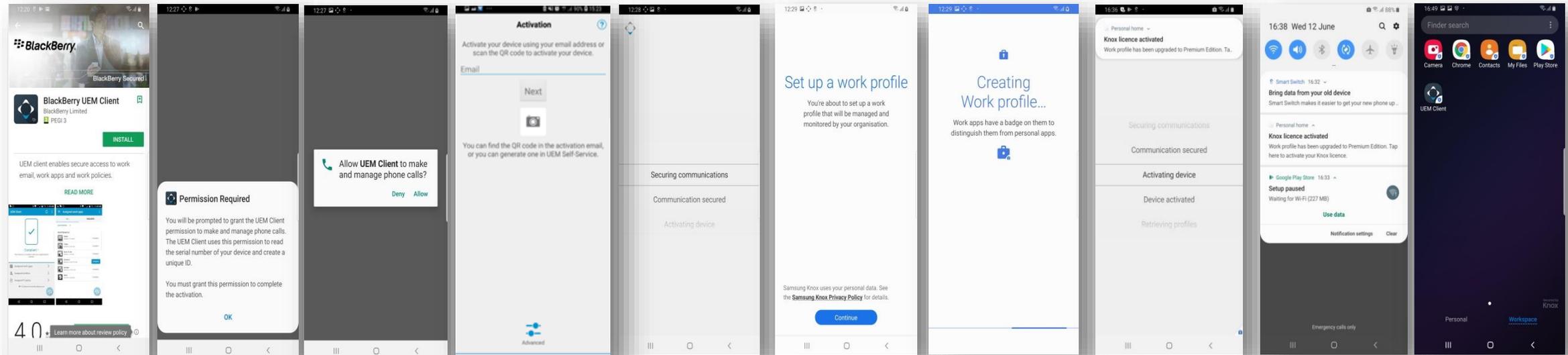
SafetyNet attestation options

- Perform SafetyNet attestation for device
- Perform SafetyNet attestation on device activation
- Perform SafetyNet attestation on BlackBerry Dynamics app activation

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*

The screenshot displays the Knox management console interface. On the left, a dark sidebar contains a navigation menu with items like Dashboard, Users, Groups, Policies and profiles, Apps, and Audit and Logging. The 'Apps' section is expanded, showing sub-options like App groups, Personal apps, and various app licenses. The main content area is titled 'Add Android apps' and features a search bar with 'knox service plugin' entered. Below the search bar, three app cards are displayed under the heading 'Apps':

- Knox Service Plugin** by Samsung Electronics C, with a 5-star rating.
- Knox Deployment** by Samsung Electronics C, with a 5-star rating.
- Samsung Knox Manager** by Samsung SDS INC, with a 5-star rating.

Approve etc...

Add Android apps

← Search 🔍







Knox Service Plugin

Samsung Electronics Co., Ltd.

★★★★★ 44 👤

 PEGI 3

⬇️ This app offers managed configuration

 This app is only available in certain countries

[Approve](#)

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*

Google Play

By Samsung Electronics Co.

App package ID
com.samsung.android.knox.kpu

App description

Screenshots (Up to 8)
[Add](#)

Send to
All Android devices

Automatically update app on Android Enterprise devices when update available

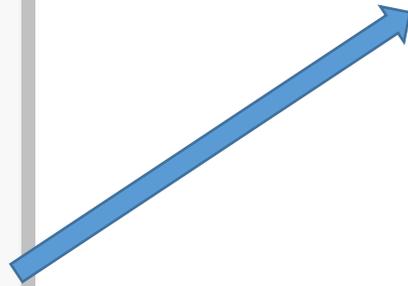
Name	Ranking	
	None defined	+

Category

App rating and review
Public mode

This app will be removed from the device when the device is removed from BlackBerry UEM.

[Cancel](#) [Add](#)



Knox Service Plugin

Name *
SRUK

Specify the configuration settings to use for this app.

Profile name
Knox profile

KPE Premium License key

Debug Mode

- ▶ Device-wide policies (Device Owner)
- ▶ Work profile policies (Profile Owner)
- ▶ DeX customization profile (Premium)
- ▶ Device and Settings customization profile (Premium)
- ▶ VPN profiles (Premium)
- ▶ Firewall configuration profile
- ▶ Manual Proxy configuration
- ▶ Proxy auto-config (PAC)
- ▶ APN configurations
- ▶ Certificates (Premium)
- ▶ UCM plugin configurations (Premium)
- ▶ NPA Data Points profile (Premium)
- ▶ RCP Data Sync profile Configurations (Premium)

▶ Allowed apps for reading private keys Configurations (Premium)

▶ Allowed USB devices for Applications Configurations

▶ Advanced Wi-Fi Configurations (Premium)

▶ Device Key Mapping to Launch & Exit application Configurations (Premium)

▶ Device Account Policy Configurations

[Cancel](#) [Save](#)

Configure App Configuration

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

Google Play [Google Play](#)

By Samsung Electronics Co.

App package ID
com.samsung.android.knox.kpu

App description

Screenshots (Up to 8)
[Add](#)

Send to
All Android devices

Automatically update app on Android Enterprise devices when update available

App configuration

Name	Ranking	
SRUK		+
		x

Category

App rating and review
Public mode

This app will be removed from the device when the device is removed from BlackBerry UEM.

[Cancel](#) [Add](#)

No filters selected							
<input type="checkbox"/>	App name	Vendor	OS	Applied users	Installed	App rating	Source
<input type="checkbox"/>	Knox Service Plugin Version 1.1.99	Samsung Electr...		0	3	☆☆☆☆☆ 0	Google Play

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**

The screenshot shows the Knox Admin console interface. On the left is a navigation sidebar with options like Dashboard, Users, Groups, Policies and profiles, Apps, Audit and Logging, and Settings. The main content area is for user 'SamsungEuro2'. It includes sections for 'MANAGED DEVICES' (5 devices), 'ENTERPRISE IDENTITY', and 'IT policy and profiles'. A table lists various profiles such as 'Default IT policies', 'SRUK Activation', 'Default BlackBerry Dynamics', 'Default Enterprise Management Agent', 'Default Compliance', 'Default Device SR requirements', 'Trial01 Gatekeeping Gatekeeping', 'Default Enterprise connectivity', 'Default BlackBerry Dynamics connectivity', and 'Default Factory reset protection'. At the bottom, there is an 'Apps' section with a table header: Name, OS, Disposition, Per-app VPN, App configuration, Assignment, and a plus sign (+). The table currently shows 'None assigned'.

The 'Assign apps' dialog box is shown, featuring a search bar for 'App name, vendor, or OS'. Below the search bar is a table with columns: App name, OS, Disposition, Per-app VPN, and App configuration. One app is listed: 'Knox Service Plugin Google Play app' with OS 'Android', Disposition 'Required', and App configuration 'SRUK'. Below the table, there are two buttons: 'Back' and 'Assign'. A note at the bottom states: 'Required app dispositions cannot be enforced on devices that are activated with Work and personal - user privacy. App groups that have been enabled for Android work profiles will have a disposition of required.'

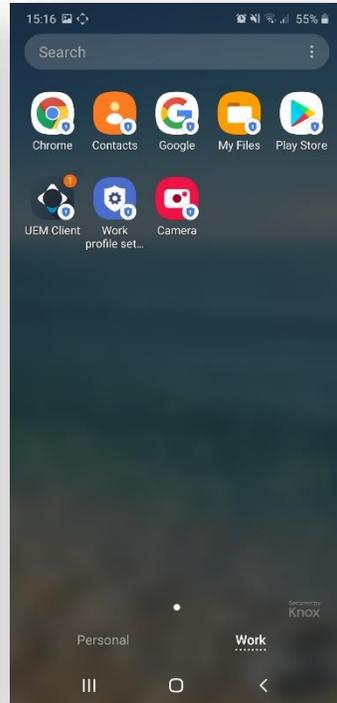
Knox Service Plugin [KSP]

KSP deployment on the device

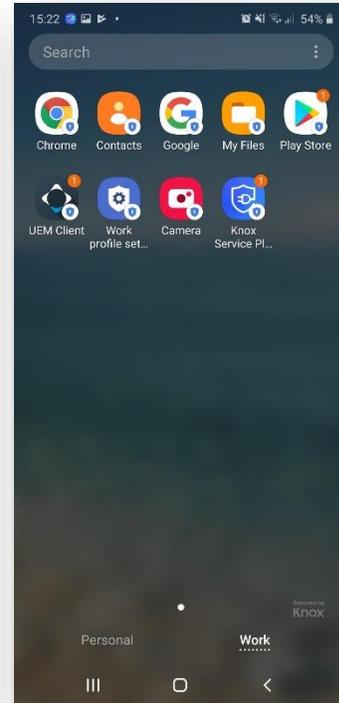
The below screen captures provide a view of the KSP app inside the Work Profile



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 in KSP configuration through managed app configuration

Document Information

This is version 2.3 of this document.

Thank you!

