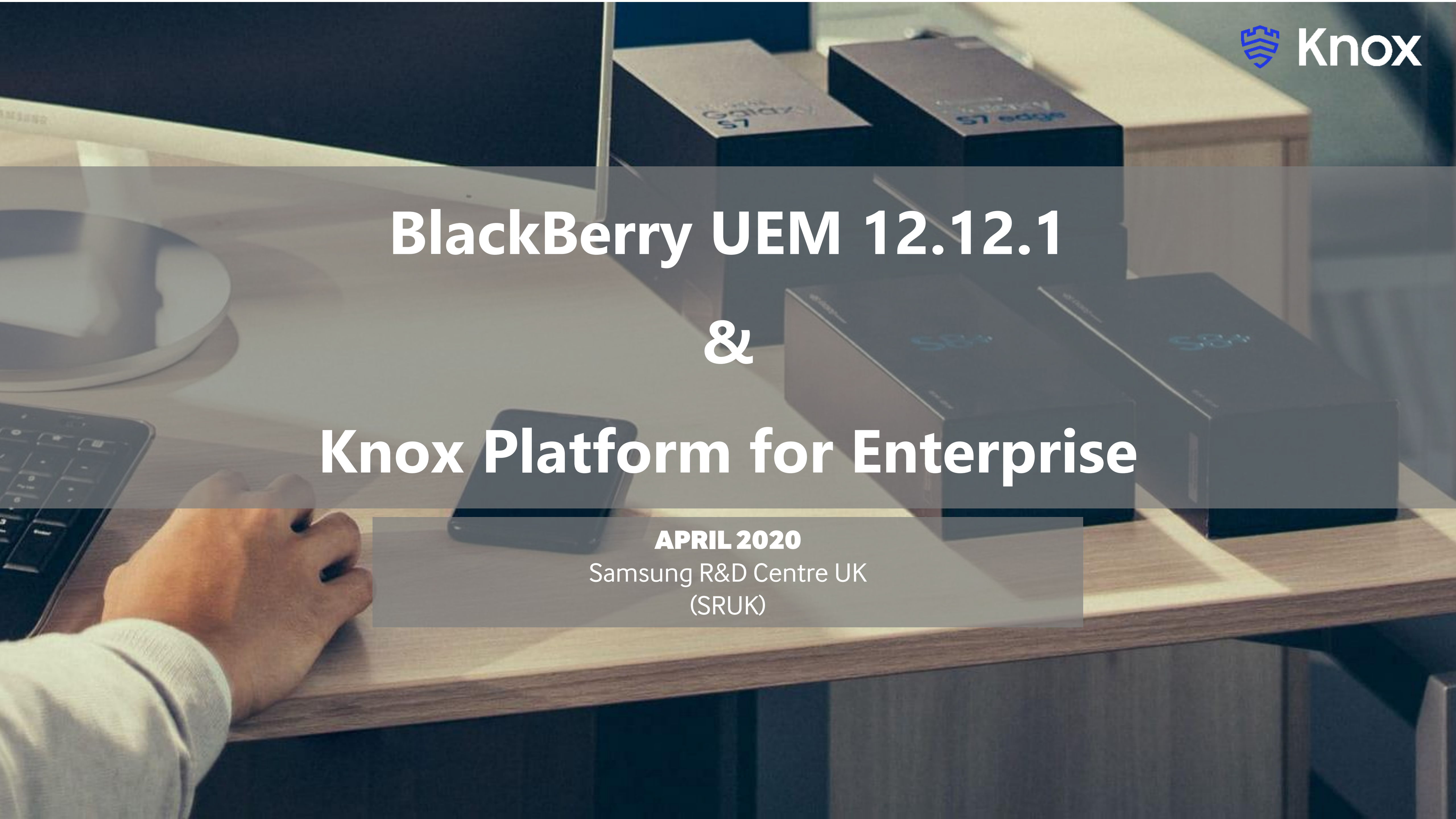


Knox

BlackBerry UEM 12.12.1

&

Knox Platform for Enterprise

APRIL 2020
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**
   - **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

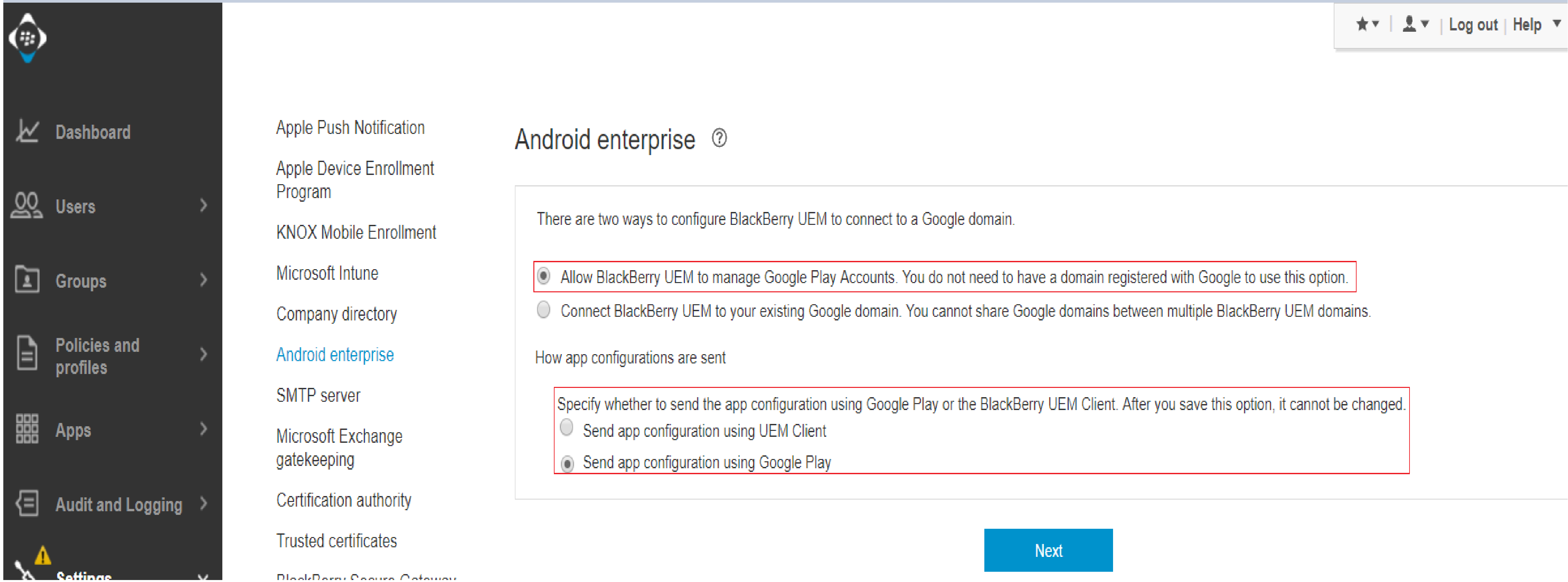
Pre-Requisites for Knox Platform for Enterprise

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

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.



Android enterprise

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.

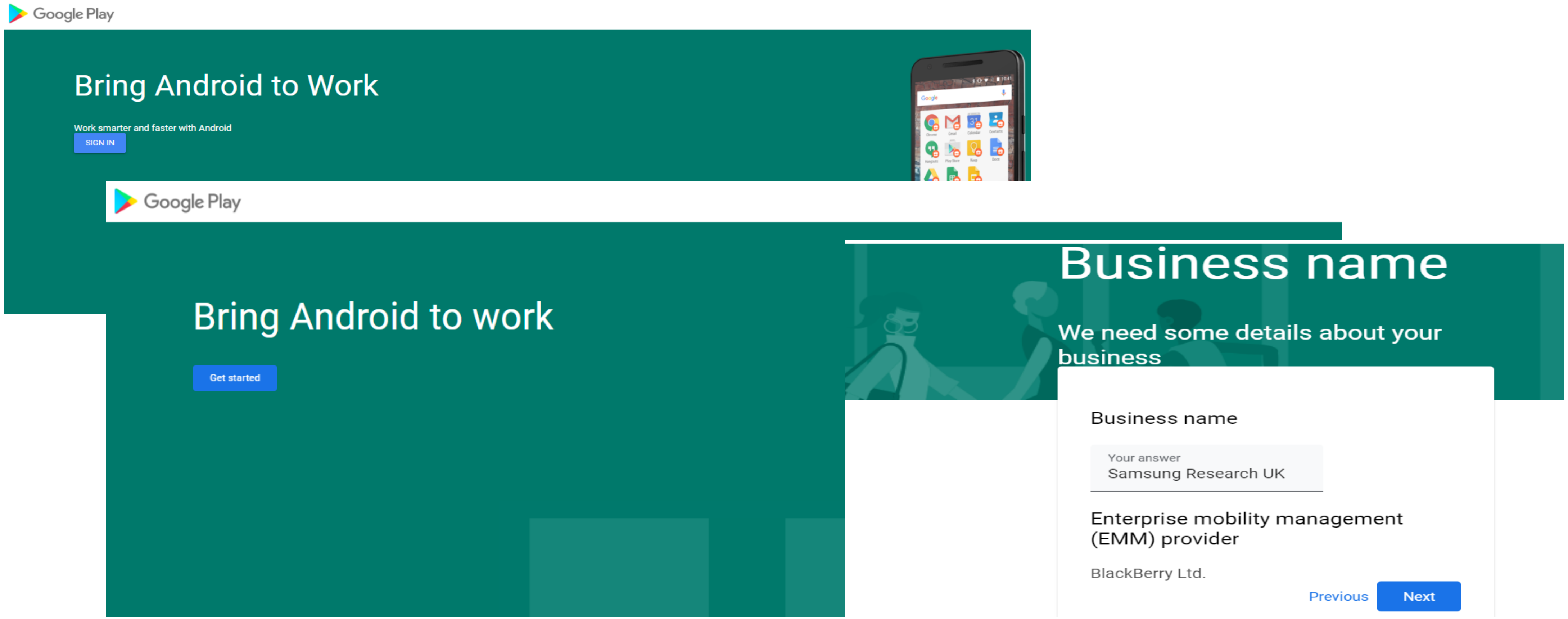
○ Send app configuration using UEM Client

● Send app configuration using Google Play

Configure Android Enterprise

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

Work smarter and faster with Android

Bring Android to work

Business name

We need some details about your business

Business name

Your answer
Samsung Research UK

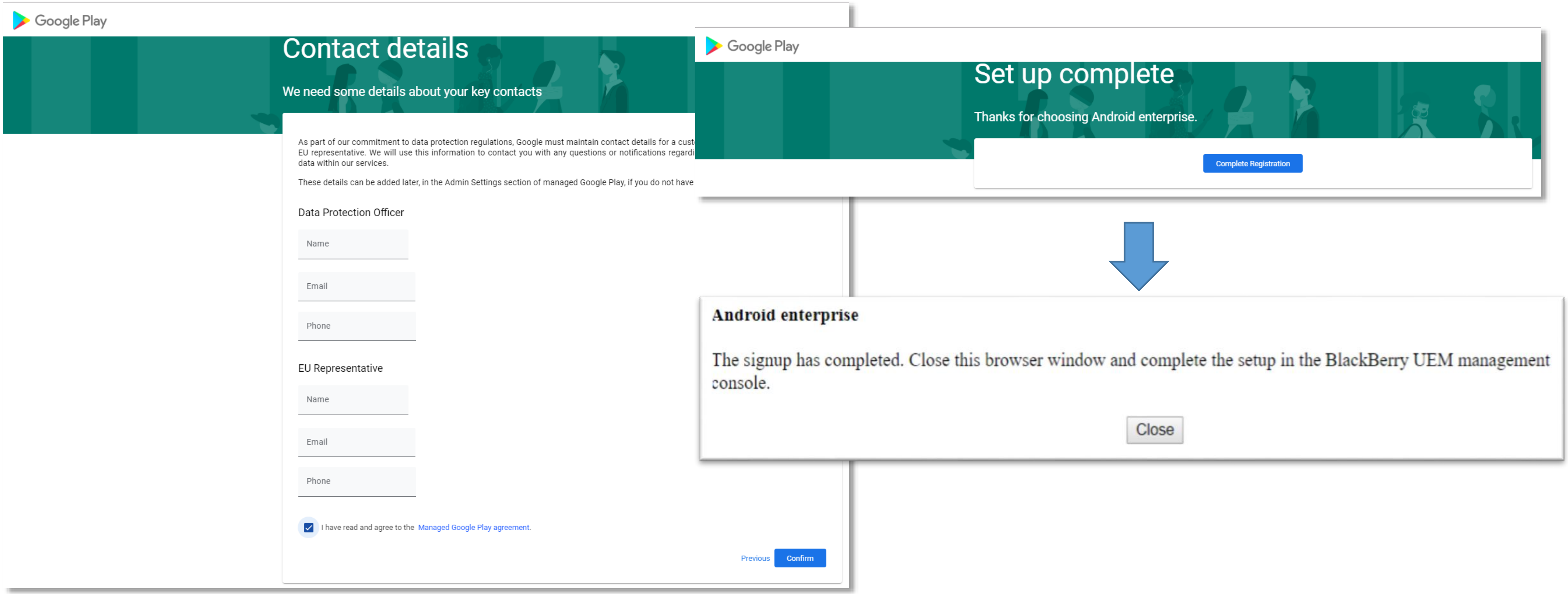
Enterprise mobility management (EMM) provider

BlackBerry Ltd.

Configure Android Enterprise

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 cust
EU representative. We will use this information to contact you with any questions or notifications regardi
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

EU Representative

☑ I have read and agree to the Managed Google Play agreement.

Set up complete

Thanks for choosing Android enterprise.

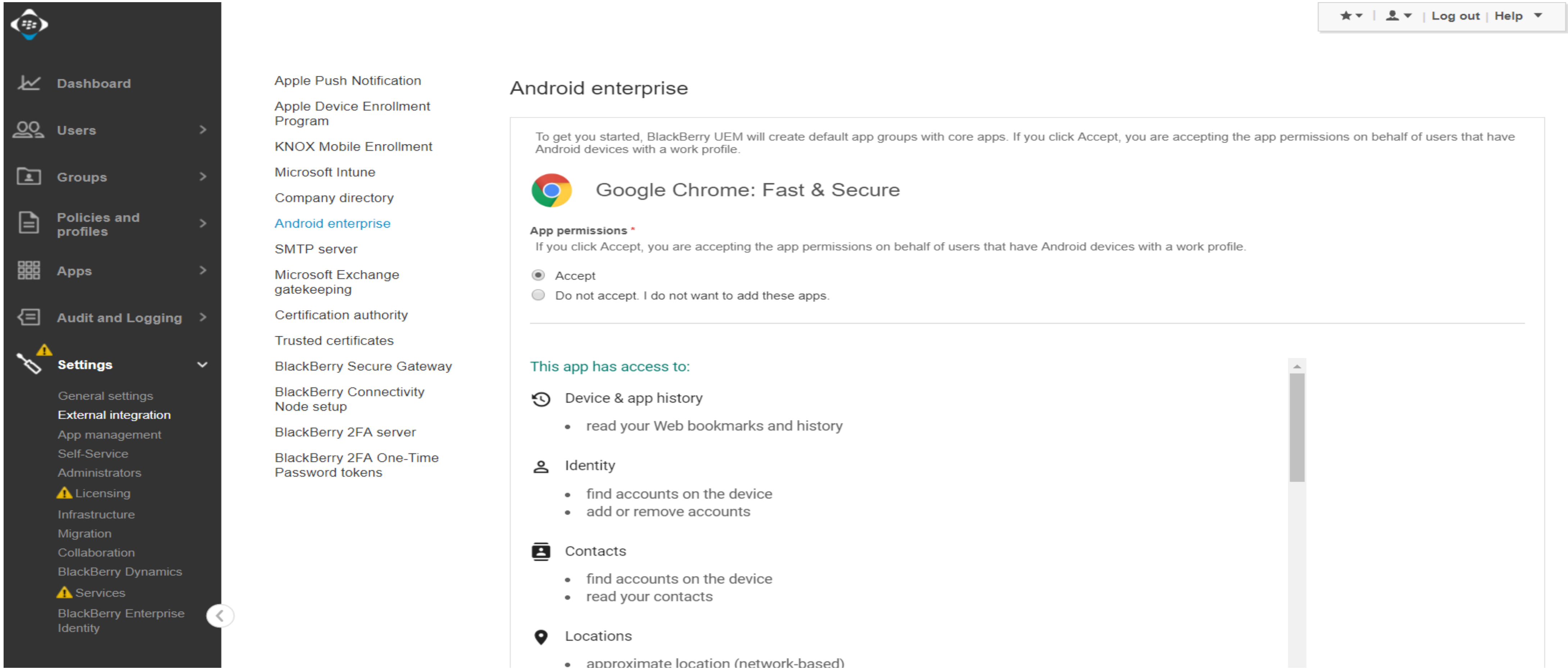
Android enterprise

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

Configure Android Enterprise

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.***



Android enterprise

To get you started, BlackBerry UEM will create default app groups with core apps. If you click Accept, you are accepting the app permissions on behalf of users that have Android devices with a work profile.

Google Chrome: Fast & Secure

App permissions *

If you click Accept, you are accepting the app permissions on behalf of users that have Android devices with a work profile.

● Accept

○ Do not accept. I do not want to add these apps.

This app has access to:

Device & app history
- read your Web bookmarks and history

Identity
- find accounts on the device
- add or remove accounts

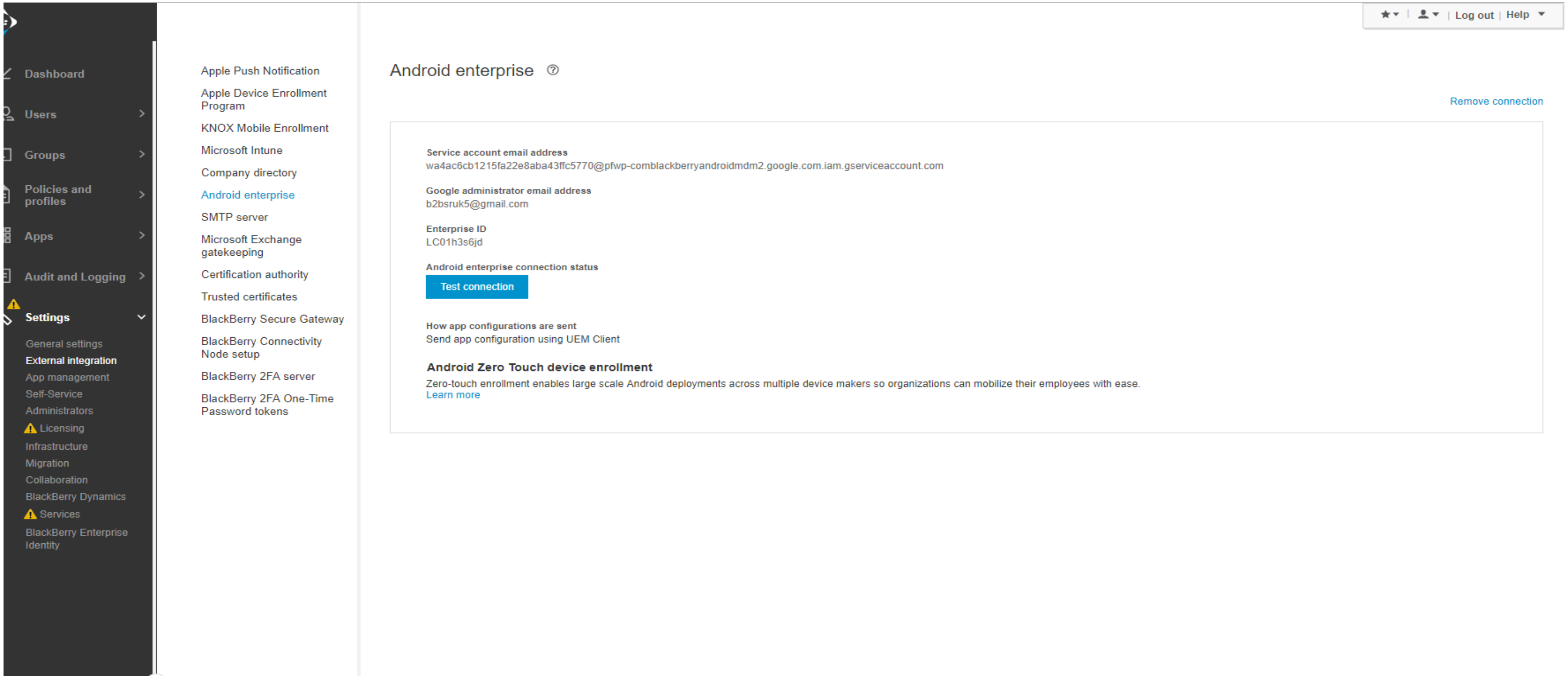
Contacts
- find accounts on the device
- read your contacts

Locations
- approximate location (network-based)

Configure Android Enterprise

CONFIGURE ANDROID ENTERPRISE

- Android Enterprise is now fully configured



Android enterprise

Service account email address
wa4ac6cb1215fa22e8aba43ffc5770@pfwp-comblackberryandroidmdm2.google.com.iam.gserviceaccount.com

Google administrator email address
b2bsruk5@gmail.com

Enterprise ID
LC01h3s6jd

Android enterprise connection status

How app configurations are sent
Send app configuration using UEM Client

Android Zero Touch device enrollment

Zero-touch enrollment enables large scale Android deployments across multiple device makers so organizations can mobilize their employees with ease.
Learn more

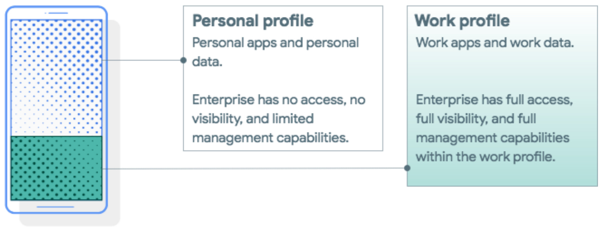
Android Enterprise Deployment Modes

DEPLOYMENT MODES

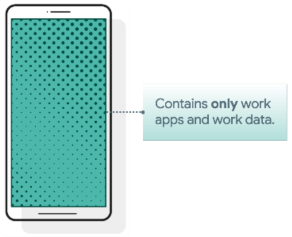
Android Enterprise can be deployed in the following 4 deployment modes

1. **BYOD** [*formerly known as Profile Owner*]
2. **Company-owned Device** [*formerly known as Device Owner*]
3. **Fully Managed device with a work profile** [*formerly known as COMP*]
4. **Dedicated device** [*formerly known as COSU*]

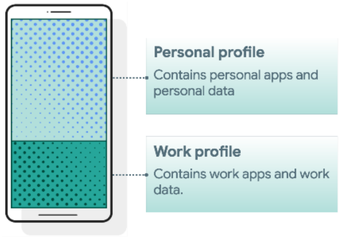
BlackBerry UEM can support 3 of these deployment modes. In this next section we will show you how to configure each of these 3 deployment modes in BlackBerry UEM for your device fleet.


Personal profile
Personal apps and personal data.
Enterprise has no access, no visibility, and limited management capabilities.
Work profile
Work apps and work data.
Enterprise has full access, full visibility, and full management capabilities within the work profile.

Bring Your Own Device [BYOD]



Company-owned Device


Personal profile
Contains personal apps and personal data
Work profile
Contains work apps and work data.

Fully Managed device with a Work Profile

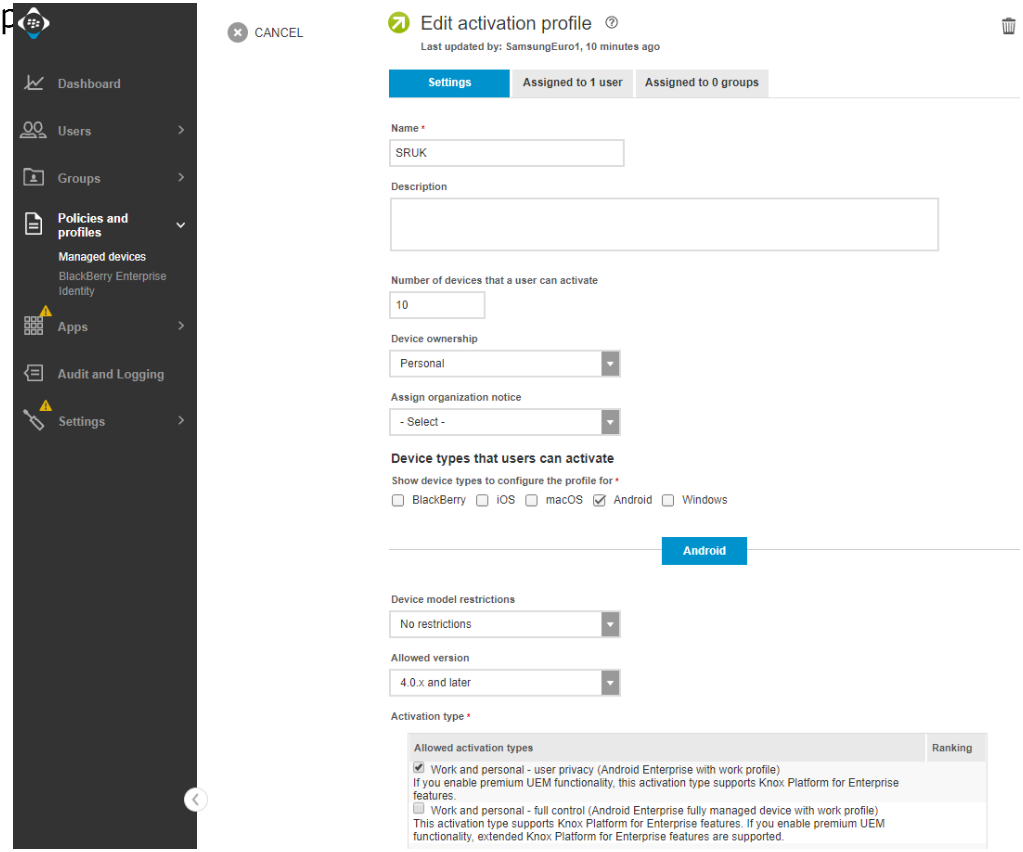
Android Enterprise: BYOD

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 typ



Edit activation profile

Last updated by: SamsungEuro1, 10 minutes ago

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

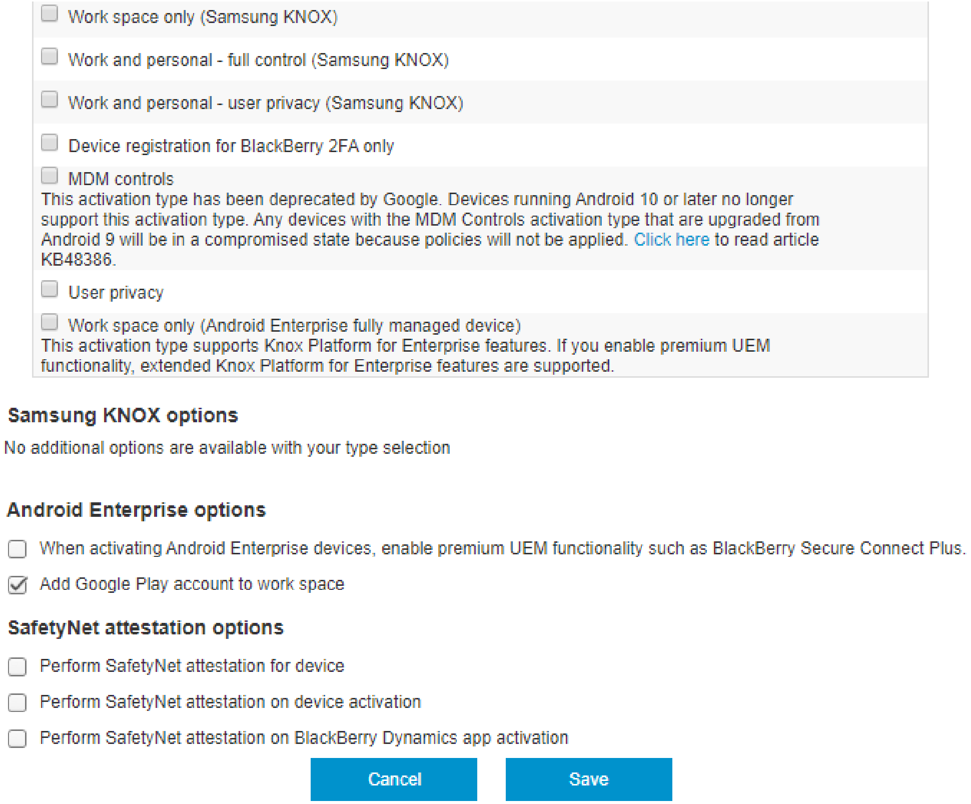
Show device types to configure the profile for *
□ BlackBerry □ iOS □ macOS ☑ Android □ Windows

Device model restrictions
No restrictions

Allowed version
4.0.x and later

Activation type *

Allowed activation types	Ranking
☑ 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.	
□ 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.	



□ 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

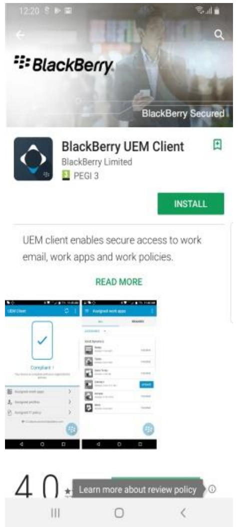
□ Perform SafetyNet attestation on BlackBerry Dynamics app activation

Android Enterprise: BYOD

ANDROID ENTERPRISE BYOD DEPLOYMENT

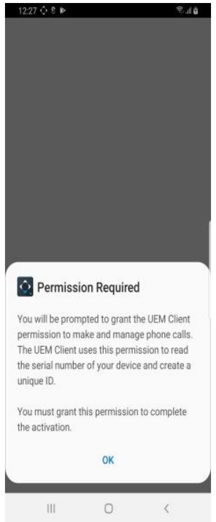
Now all you simply need to do is enroll your device by completing the following:

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



UEM client enables secure access to work email, work apps and work policies.

Install BlackBerry UEM Client from Google Play Store

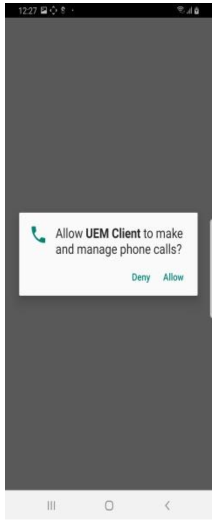


Permission Required

You will be prompted to grant the UEM Client permission to make and manage phone calls. The UEM Client uses this permission to read the serial number of your device and create a unique ID.

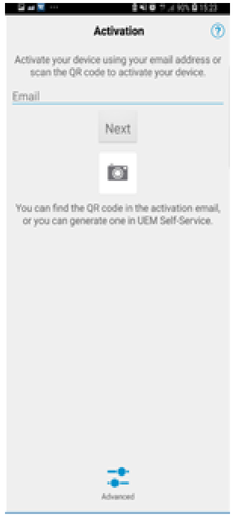
You must grant this permission to complete the activation.

Accept the permission request



Allow **UEM Client** to make and manage phone calls?

Allow UEM Client to …



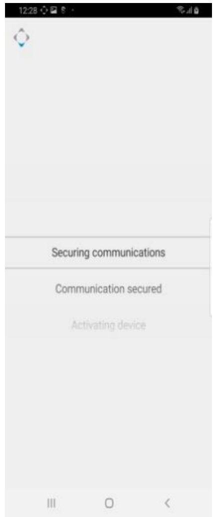
Activation

Activate your device using your email address or scan the QR code to activate your device.

Email

You can find the QR code in the activation email, or you can generate one in UEM Self-Service.

Enter Credentials

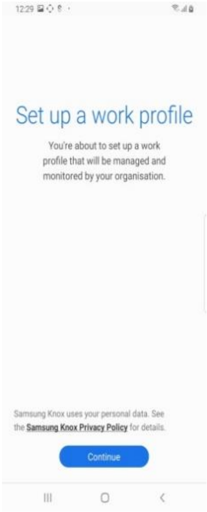


Securing communications

Communication secured

Activating device

Start of the Enrollment

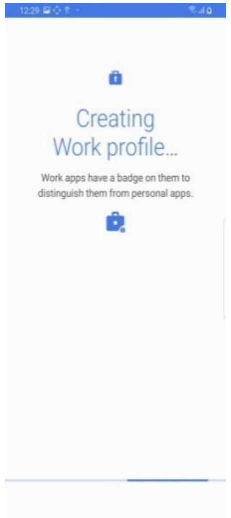


Set up a work profile

You're about to set up a work profile that will be managed and monitored by your organisation.

Samsung Knox uses your personal data. See the **Samsung Knox Privacy Policy** for details.

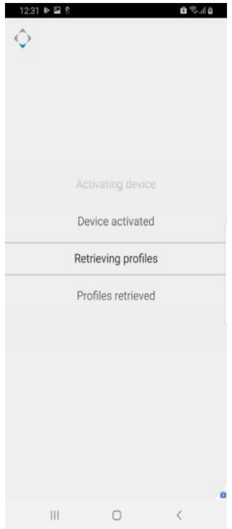
Click Continue to Set up a Work Profile



Creating Work profile...

Work apps have a badge on them to distinguish them from personal apps.

Creating Work Profile



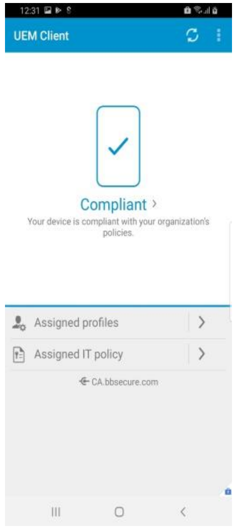
Activating device

Device activated

Retrieving profiles

Profiles retrieved

Profiles being Retrieved



Compliant ›

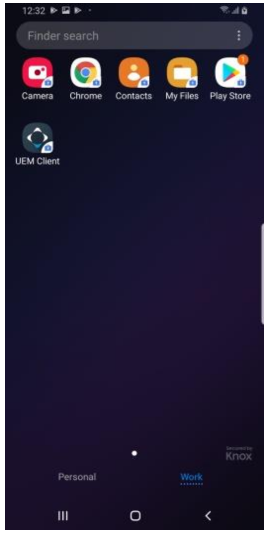
Your device is compliant with your organization's policies.

Assigned profiles

Assigned IT policy

CA.bbsecure.com

Device Enrollment Successful!



Inside the Work Profile

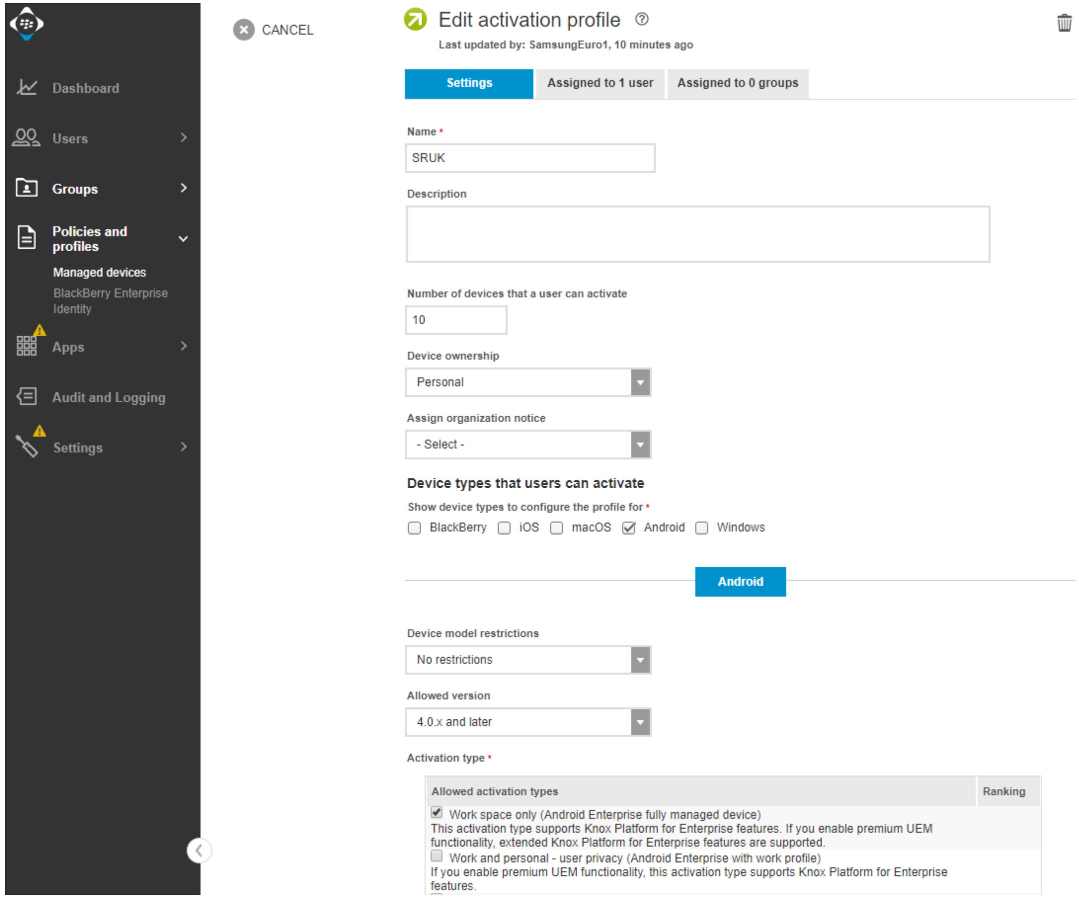
Android Enterprise: Company-owned Device

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.



Edit activation profile

Last updated by: SamsungEuro1, 10 minutes ago

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 *

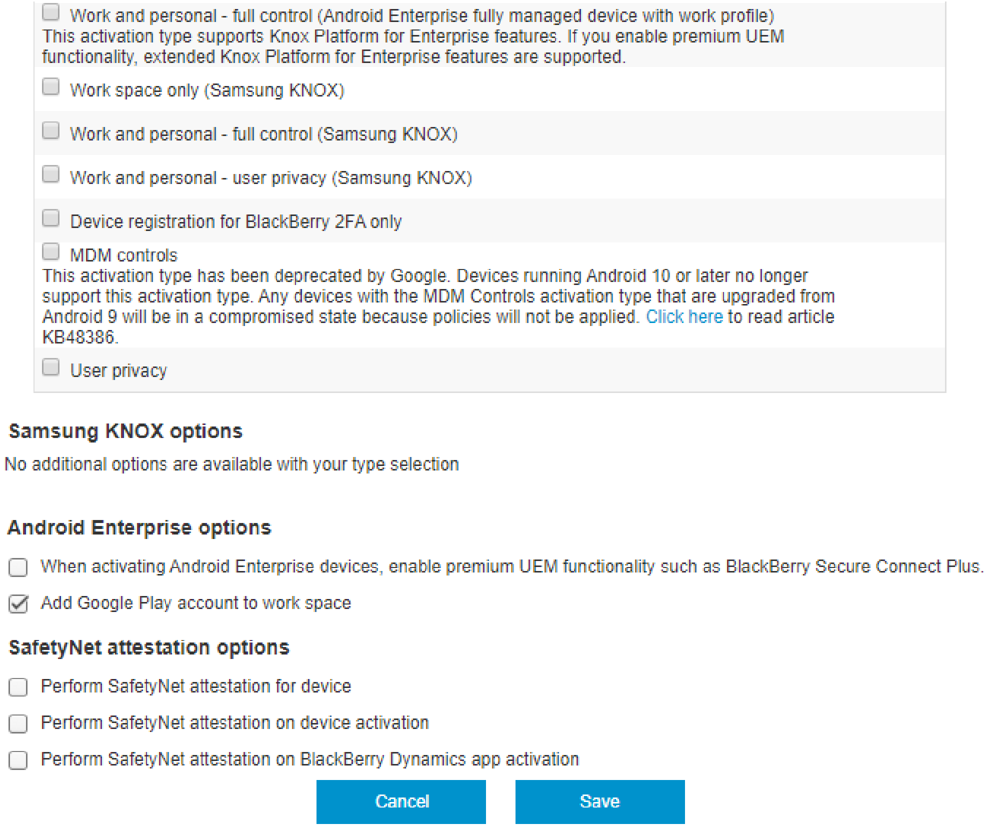
□ BlackBerry □ iOS □ macOS ☑ Android □ Windows

Device model restrictions: No restrictions

Allowed version: 4.0.x and later

Activation type *

Allowed activation types	Ranking
☑ 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.	



□ 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.

□ 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

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

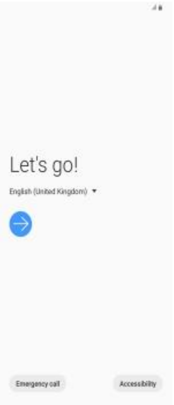
Android Enterprise: Company-owned Device

ANDROID ENTERPRISE COMPANY-OWNED DEVICE DEPLOYMENT

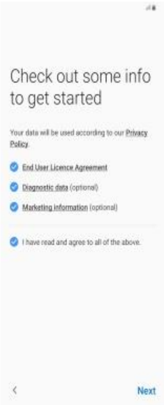
To enroll your device as an Android Enterprise Company-owned device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 4 ways you can enroll your device into BlackBerry UEM as an Android Enterprise Company-owned device.

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.


Let's go!

Click Start arrow

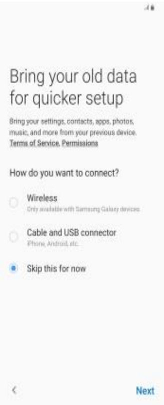

Check out some info to get started

Your data will be used according to our Privacy Policy.

☑ End User Licence Agreement
☑ Diagnostic data (optional)
☑ Marketing information (optional)

☑ I have read and agree to all of the above.

Accept T's & C's

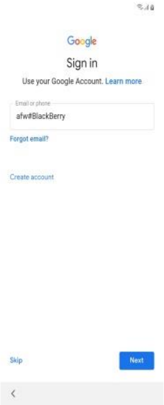

Bring your old data for quicker setup

Bring your settings, contacts, apps, photos, music, and more from your previous device. Terms of Service, Permissions

How do you want to connect?

○ Wireless
Only available with Samsung Galaxy devices
○ Cable and USB connector
iPhone, Android, etc.
● Skip this for now

Skip Backup

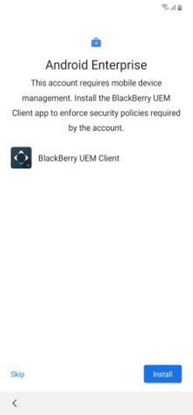

Google

Sign in

Use your Google Account. Learn more

Email or phone: afw#BlackBerry

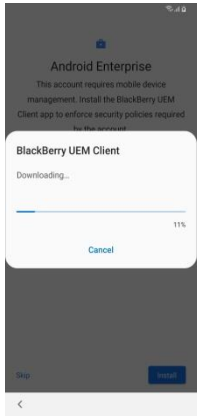
Enter **afw#BlackBerry** and click next


Android Enterprise

This account requires mobile device management. Install the BlackBerry UEM Client app to enforce security policies required by the account.

BlackBerry UEM Client

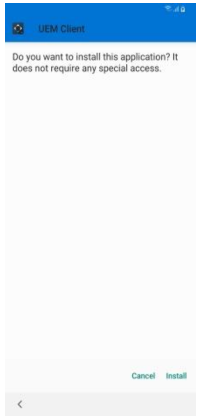
Select Install


BlackBerry UEM Client

Downloading...

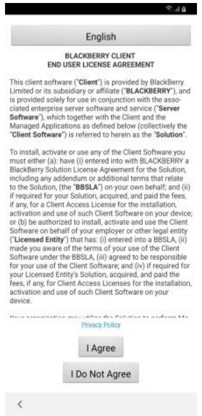
11%

UEM client being downloaded


UEM Client

Do you want to install this application? It does not require any special access.

Click Install

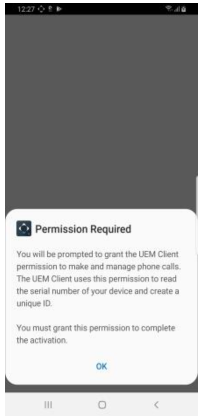

English

BLACKBERRY CLIENT
END USER LICENSE AGREEMENT

This client software ("**Client**") is provided by BlackBerry Limited or its subsidiary or affiliate ("**BLACKBERRY**"), and is provided solely for use in conjunction with the associated enterprise server software and service ("**Server Software**"), which together with the Client and the Managed Applications as defined below (collectively the "**Client Software**") is referred to herein as the "**Solution**".

To install, activate or use any of the Client Software you must either (a): have (i) entered into with BLACKBERRY a BlackBerry Solution License Agreement for the Solution, including any addendum or additional terms that relate to the Solution, (the "**BBSLA**") on your own behalf; and (ii) if required for your Solution, acquired, and paid the fees, if any, for a Client Access License for the installation, activation and use of such Client Software on your device; or (b) be authorized to install, activate and use the Client Software on behalf of your employer or other legal entity ("**Licensed Entity**") that has: (i) entered into a BBSLA, (ii) made you aware of the terms of your use of the Client Software under the BBSLA, (iii) agreed to be responsible for your use of the Client Software; and (iv) if required for your Licensed Entity's Solution, acquired, and paid the fees, if any, for Client Access Licenses for the installation, activation and use of such Client Software on your device.

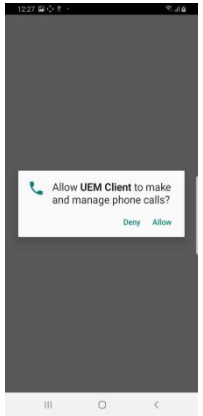
Agree to the license agreement


Permission Required

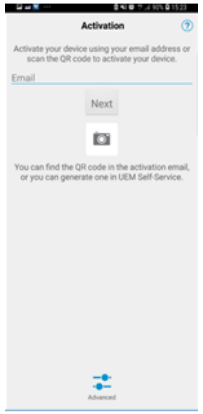
You will be prompted to grant the UEM Client permission to make and manage phone calls. The UEM Client uses this permission to read the serial number of your device and create a unique ID.

You must grant this permission to complete the activation.

Accept the Permission


Allow **UEM Client** to make and manage phone calls?

Allow UEM Client to .....


Activation

Activate your device using your email address or scan the QR code to activate your device.

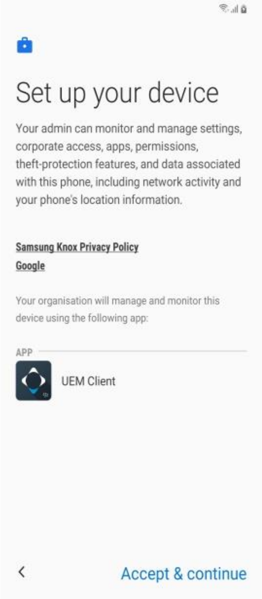
Email

You can find the QR code in the activation email, or you can generate one in UEM Self-Service.

Enter Credential for the enrollment

Android Enterprise: Company-owned Device

ANDROID ENTERPRISE COMPANY-OWNED DEVICE DEPLOYMENT



Set up your device

Your admin can monitor and manage settings, corporate access, apps, permissions, theft-protection features, and data associated with this phone, including network activity and your phone's location information.

Samsung Knox Privacy Policy

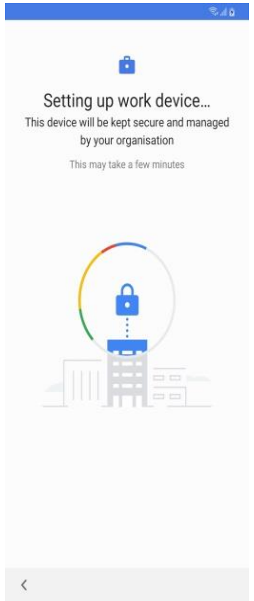
Google

Your organisation will manage and monitor this device using the following app:

APP

UEM Client

Accept & Continue

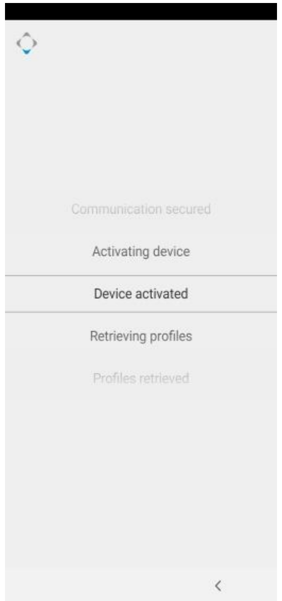


Setting up work device...

This device will be kept secure and managed by your organisation

This may take a few minutes

Setting up Work device



Communication secured

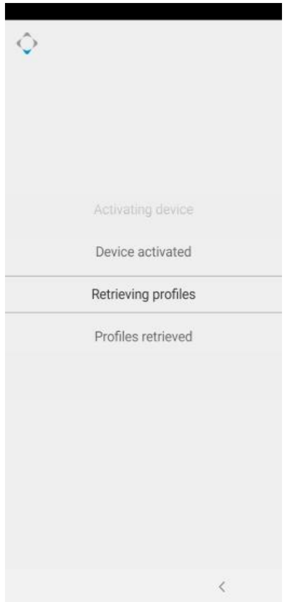
Activating device

Device activated

Retrieving profiles

Profiles retrieved

Device activated



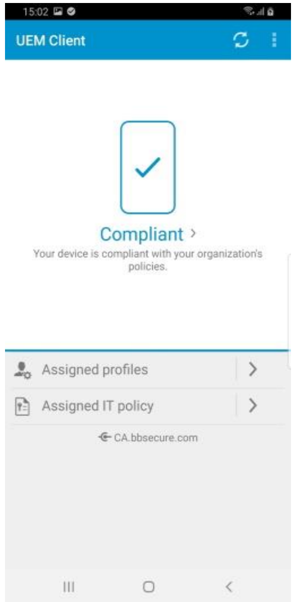
Activating device

Device activated

Retrieving profiles

Profiles retrieved

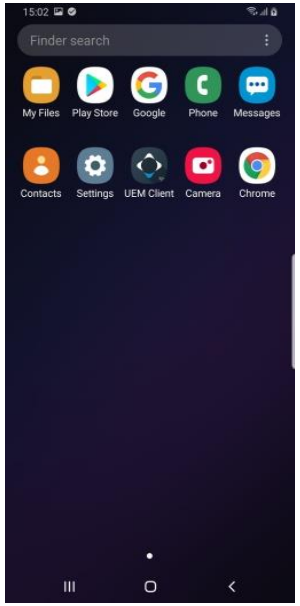
Profiles being retrieved



Compliant ›

Your device is compliant with your organization's policies.

Device Enrollment Successful!



Device Area

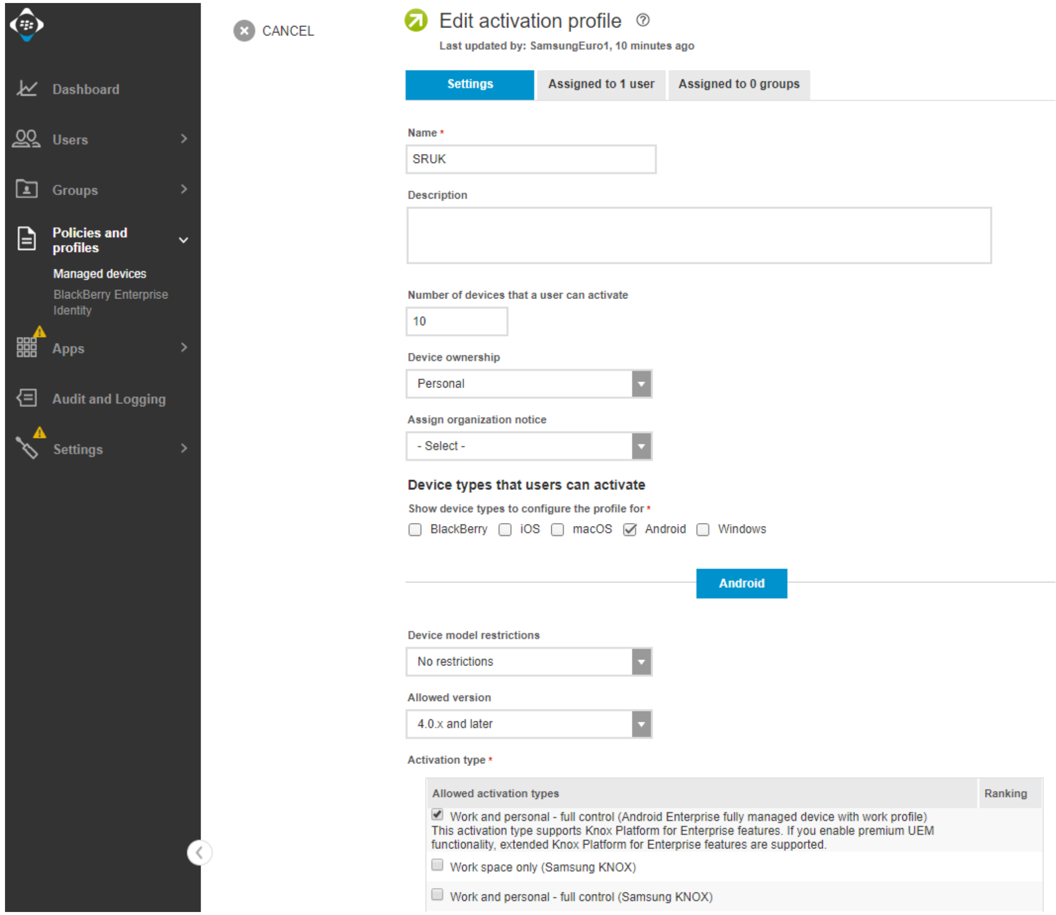
Android Enterprise: Fully Managed Device with a Work Profile

ANDROID ENTERPRISE FULLY MANAGED DEVICE WITH A WORK PROFILE

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

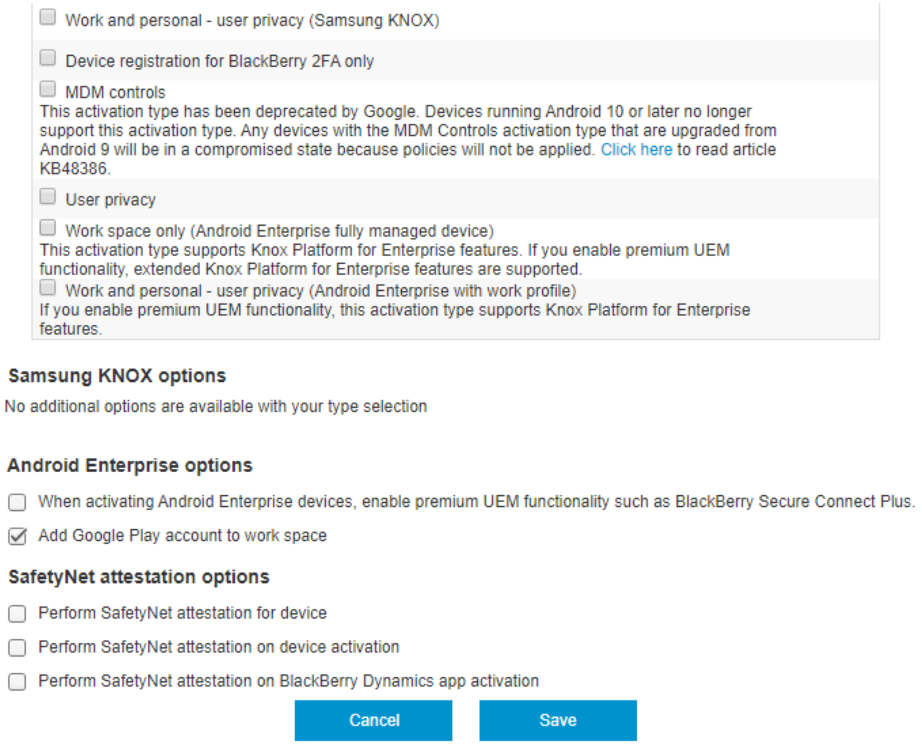
Android

Device model restrictions: No restrictions

Allowed version: 4.0.x and later

Activation type *

Allowed activation types	Ranking
☑ 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.	
□ 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.

□ 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

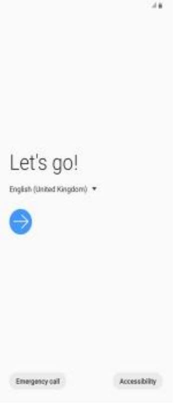
Android Enterprise: Fully Managed Device with a Work Profile

ANDROID ENTERPRISE FULLY MANAGED DEVICE WITH A WORK PROFILE

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

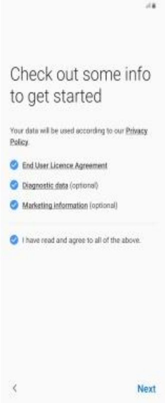
- Below is a screen-by-screen play to enroll your device using the DPC Identifier method.



Let's go!

English (United Kingdom) ▾

Click Start arrow



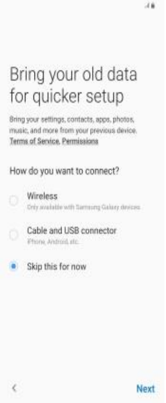
Check out some info to get started

Your data will be used according to our Privacy Policy.

☑ End User Licence Agreement
☑ Diagnostic data (optional)
☑ Marketing information (optional)

☑ I have read and agree to all of the above.

Accept T's & C's



Bring your old data for quicker setup

Bring your settings, contacts, apps, photos, music, and more from your previous device. Terms of Service, Permissions

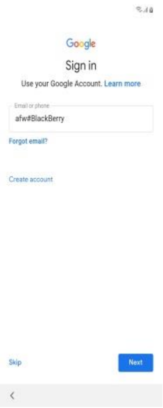
How do you want to connect?

○ Wireless
Only available with Samsung Galaxy devices

○ Cable and USB connector
iPhone, Android, etc.

● Skip this for now

Skip Backup



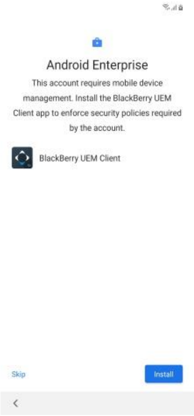
Google

Sign in

Use your Google Account. Learn more

Email or phone: afw#BlackBerry

Enter **afw#BlackBerry** and click next

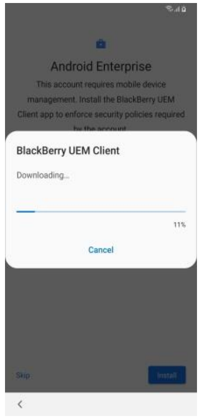


Android Enterprise

This account requires mobile device management. Install the BlackBerry UEM Client app to enforce security policies required by the account.

BlackBerry UEM Client

Select Install

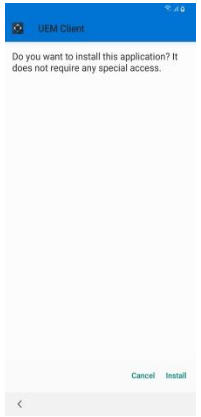


BlackBerry UEM Client

Downloading...

11%

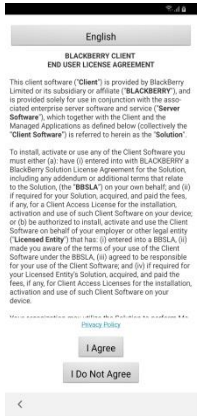
UEM client being downloaded



UEM Client

Do you want to install this application? It does not require any special access.

Click Install



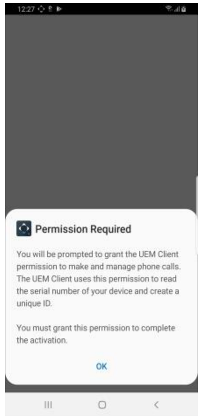
English

BLACKBERRY CLIENT
END USER LICENSE AGREEMENT

This client software ("**Client**") is provided by BlackBerry Limited or its subsidiary or affiliate ("**BLACKBERRY**"), and is provided solely for use in conjunction with the associated enterprise server software and service ("**Server Software**"), which together with the Client and the Managed Applications as defined below (collectively the "**Client Software**") is referred to herein as the "**Solution**".

To install, activate or use any of the Client Software you must either (a): have (i) entered into with BLACKBERRY a BlackBerry Solution License Agreement for the Solution, including any addendum or additional terms that relate to the Solution, (the "**BBSLA**") on your own behalf; and (ii) if required for your Solution, acquired, and paid the fees, if any, for a Client Access License for the installation, activation and use of such Client Software on your device; or (b) be authorized to install, activate and use the Client Software on behalf of your employer or other legal entity ("**Licensed Entity**") that has: (i) entered into a BBSLA, (ii) made you aware of the terms of your use of the Client Software under the BBSLA, (iii) agreed to be responsible for your use of the Client Software; and (iv) if required for your Licensed Entity's Solution, acquired, and paid the fees, if any, for Client Access Licenses for the installation, activation and use of such Client Software on your device.

Agree to the license agreement

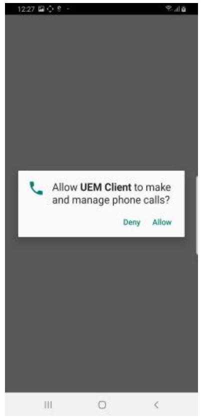


Permission Required

You will be prompted to grant the UEM Client permission to make and manage phone calls. The UEM Client uses this permission to read the serial number of your device and create a unique ID.

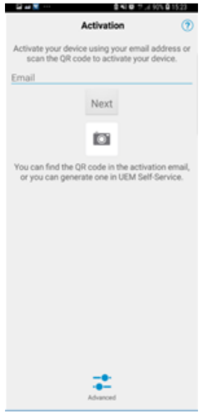
You must grant this permission to complete the activation.

Accept the Permission



Allow **UEM Client** to make and manage phone calls?

Allow UEM Client to .....



Activation

Activate your device using your email address or scan the QR code to activate your device.

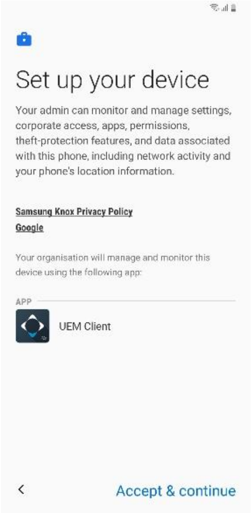
Email

You can find the QR code in the activation email, or you can generate one in UEM Self-Service.

Enter Credential for the enrollment

Android Enterprise: Fully Managed Device with a Work Profile

ANDROID ENTERPRISE FULLY MANAGED DEVICE WITH A WORK PROFILE



Set up your device

Your admin can monitor and manage settings, corporate access, apps, permissions, theft-protection features, and data associated with this phone, including network activity and your phone's location information.

Samsung Knox Privacy Policy

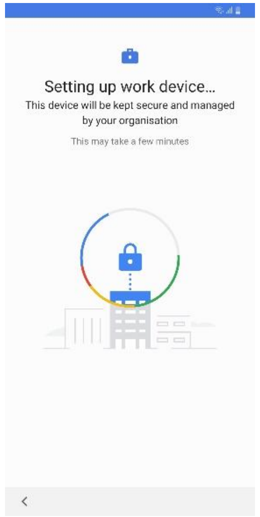
Google

Your organisation will manage and monitor this device using the following app:

APP

UEM Client

Accept & Continue

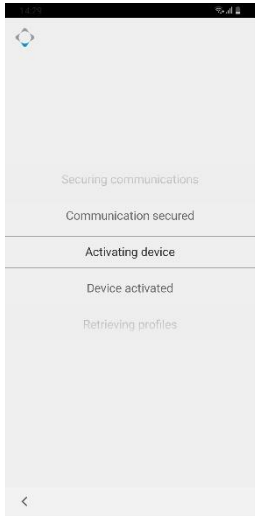


Setting up work device...

This device will be kept secure and managed by your organisation

This may take a few minutes

Setting up Work device



Securing communications

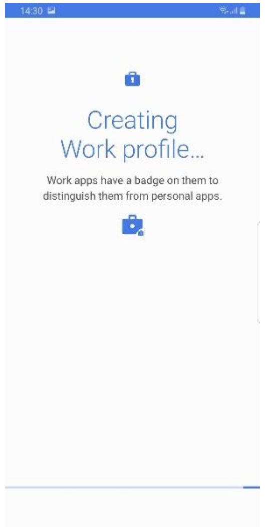
Communication secured

Activating device

Device activated

Retrieving profiles

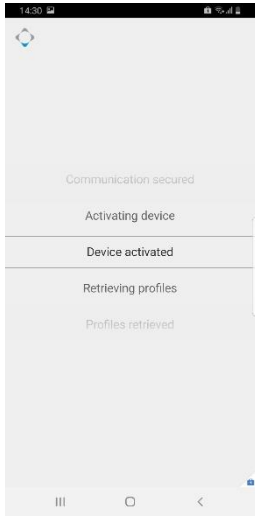
Activating device



Creating Work profile...

Work apps have a badge on them to distinguish them from personal apps.

Profiles being retrieved



Communication secured

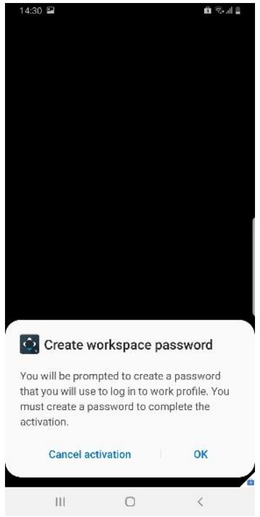
Activating device

Device activated

Retrieving profiles

Profiles retrieved

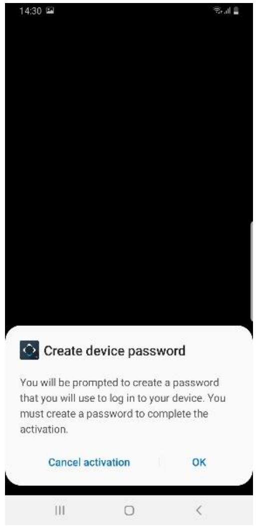
Device Enrollment Successful!



Create workspace password

You will be prompted to create a password that you will use to log in to work profile. You must create a password to complete the activation.

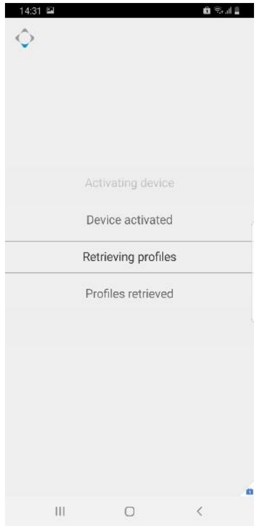
Work Profile password creation



Create device password

You will be prompted to create a password that you will use to log in to your device. You must create a password to complete the activation.

Device Password Creation



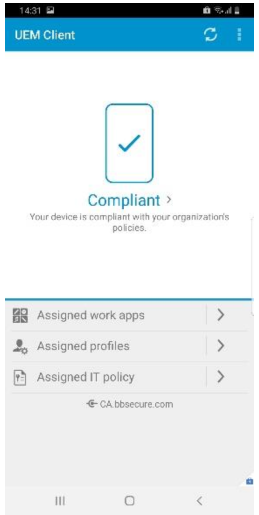
Activating device

Device activated

Retrieving profiles

Profiles retrieved

Profile Assignment



UEM Client

Compliant ›

Your device is compliant with your organization's policies.

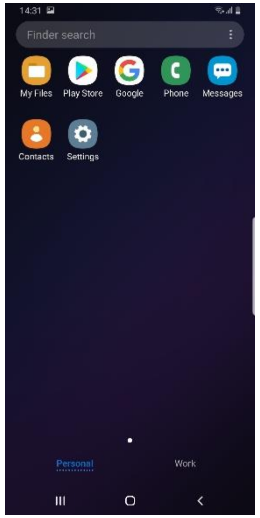
Assigned work apps

Assigned profiles

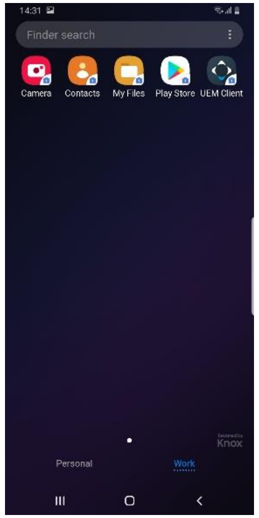
Assigned IT policy

CA.bbsecure.com

Device Enrollment Successful!



Device Area



Inside the Work Profile

Android Enterprise: **DEDICATED DEVICE**

ANDROID ENTERPRISE DEDICATED DEVICE DEPLOYMENT

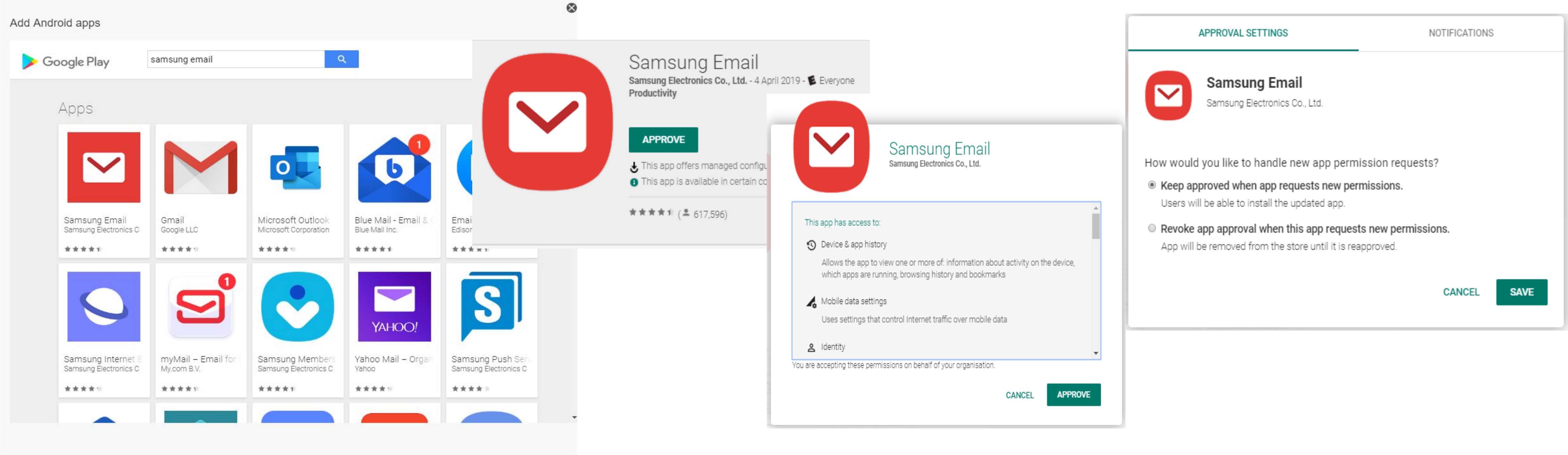
BLACKBERRY UEM 12.11 MR1 DOES NOT SUPPORT DEDICATED DEVICE.
WHEN IT IS SUPPORTED, THIS GUIDE WILL BE UPDATED TO INCLUDE STEPS ON HOW TO CONFIGURE IT.

Managed Google Play Configuration

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**



Add Android apps

Google Play samsung email

Apps

Samsung Email Samsung Electronics C
Gmail Google LLC
Microsoft Outlook Microsoft Corporation
Blue Mail - Email & C Blue Mail Inc.
Emai Edisor
Samsung Internet B Samsung Electronics C
myMail – Email for My.com B.V.
Samsung Members Samsung Electronics C
Yahoo Mail – Organ Yahoo
Samsung Push Ser Samsung Electronics C

Samsung Email
Samsung Electronics Co., Ltd. - 4 April 2019 - Everyone
Productivity
APPROVE
This app offers managed configu
This app is available in certain co
★★★★ (617,596)

Samsung Email
Samsung Electronics Co., Ltd.

This app has access to:

Device & app history
Allows the app to view one or more of: information about activity on the device, which apps are running, browsing history and bookmarks

Mobile data settings
Uses settings that control Internet traffic over mobile data

Identity

You are accepting these permissions on behalf of your organisation.

CANCEL APPROVE

APPROVAL SETTINGS NOTIFICATIONS

Samsung Email
Samsung Electronics Co., Ltd.

How would you like to handle new app permission requests?

● Keep approved when app requests new permissions.
Users will be able to install the updated app.

○ Revoke app approval when this app requests new permissions.
App will be removed from the store until it is reapproved.

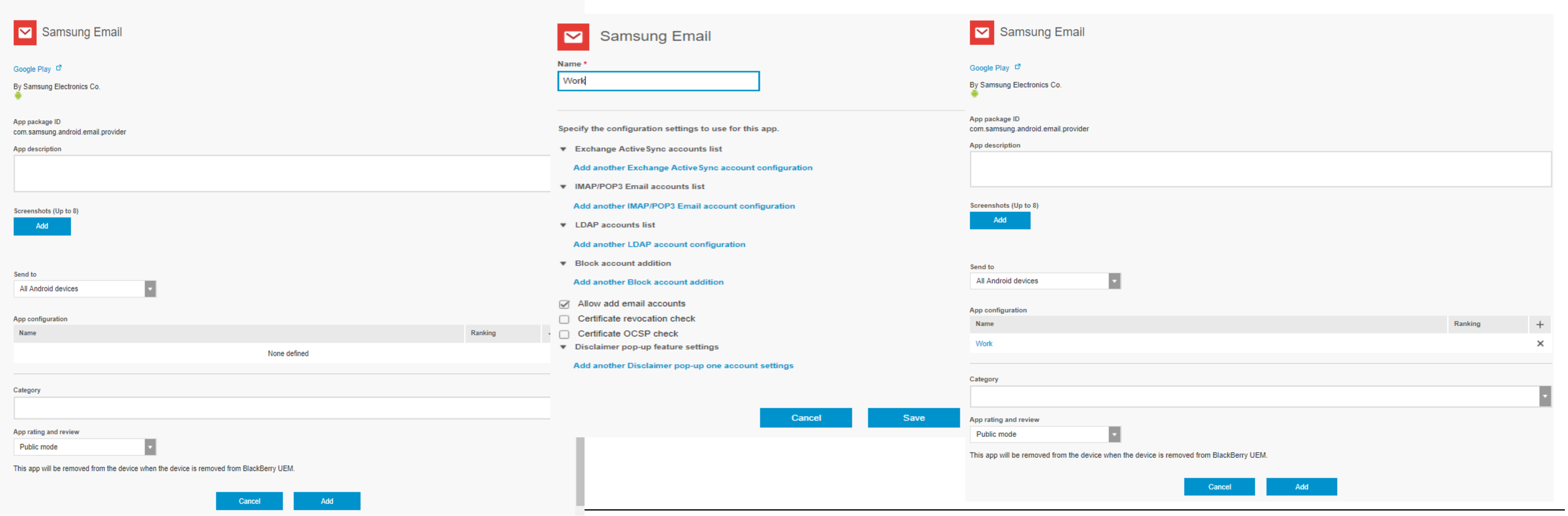
CANCEL SAVE

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.



Samsung Email

Google Play

By Samsung Electronics Co.

App package ID
com.samsung.android.email.provider

App description

Screenshots (Up to 8)
Add

Send to
All Android devices

App configuration

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

Samsung Email

Name *
Work

Specify the configuration settings to use for this app.

▾ Exchange ActiveSync accounts list
Add another Exchange ActiveSync account configuration
▾ IMAP/POP3 Email accounts list
Add another IMAP/POP3 Email account configuration
▾ LDAP accounts list
Add another LDAP account configuration
▾ Block account addition
Add another Block account addition
☑ Allow add email accounts
□ Certificate revocation check
□ Certificate OCSP check
▾ Disclaimer pop-up feature settings
Add another Disclaimer pop-up one account settings

Cancel Save

Samsung Email

Google Play

By Samsung Electronics Co.

App package ID
com.samsung.android.email.provider

App description

Screenshots (Up to 8)
Add

Send to
All Android devices

App configuration

Name	Ranking
Work	

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

Configure Knox Platform for Enterprise : Standard Edition

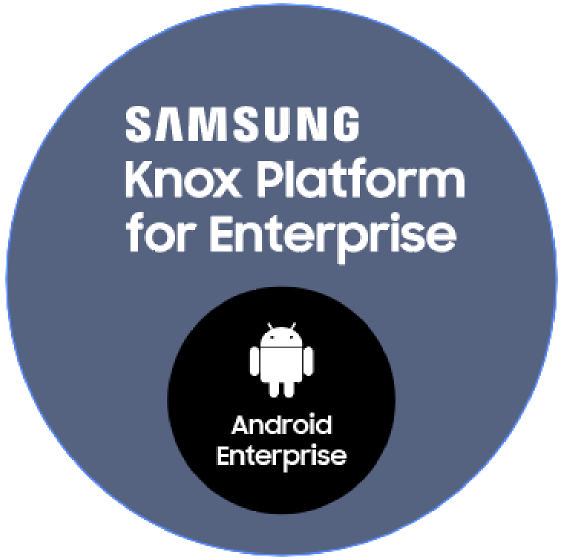
KNOX PLATFORM FOR ENTERPRISE : STANDARD EDITION

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 [$]

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.

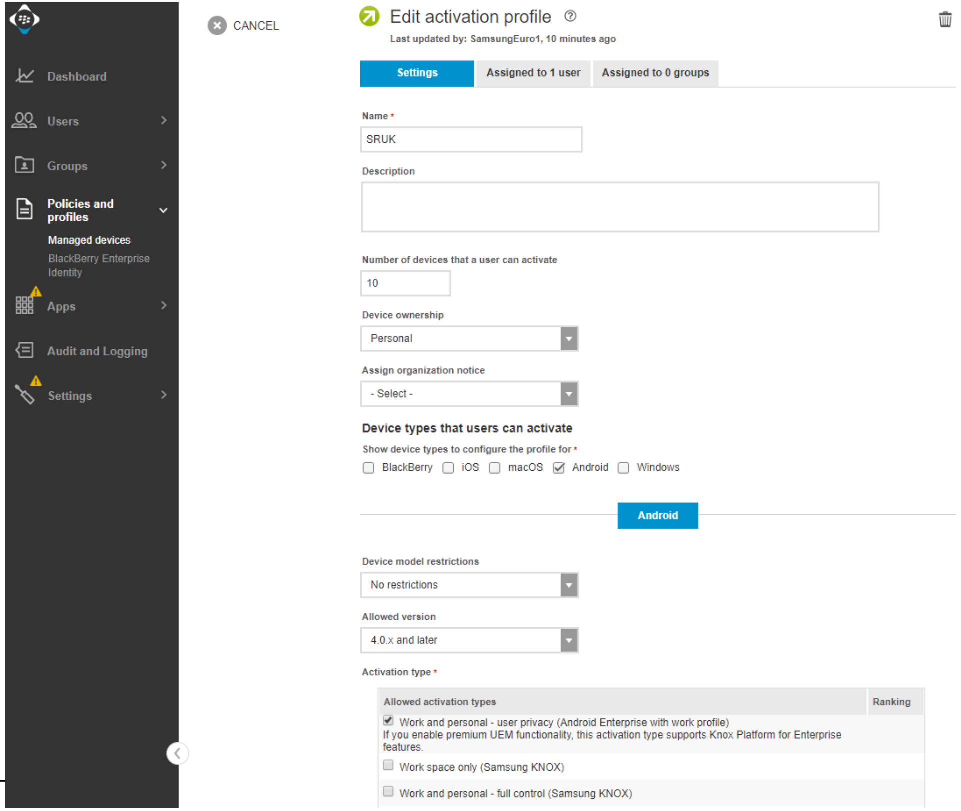


Configure Knox Platform for Enterprise : Standard Edition

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 - 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 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

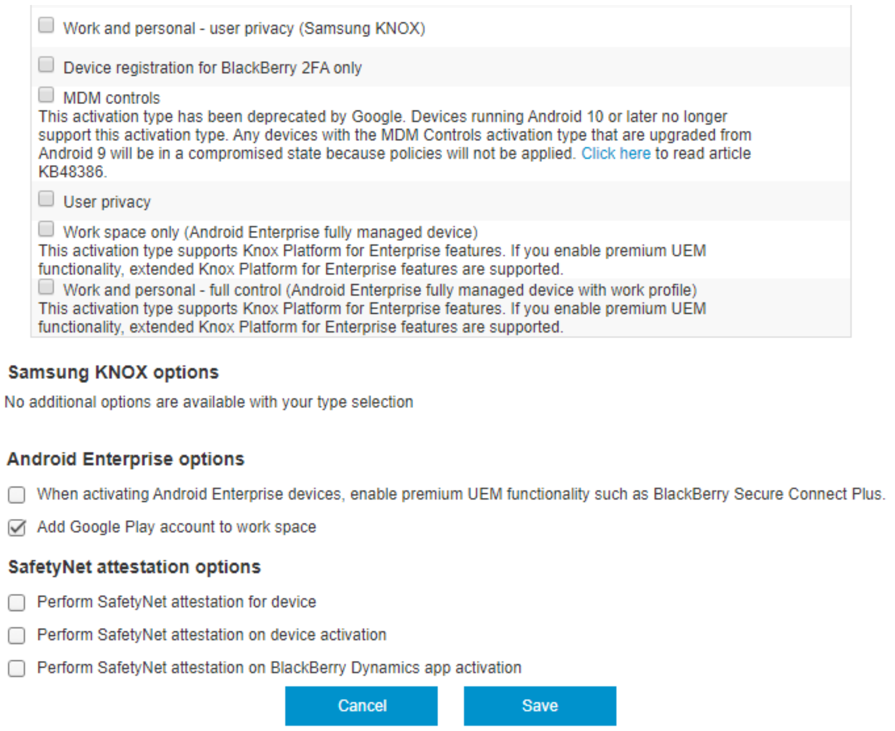
Android

Device model restrictions: No restrictions

Allowed version: 4.0.x and later

Activation type *

Allowed activation types	Ranking
☑ 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.	
□ 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.

□ 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

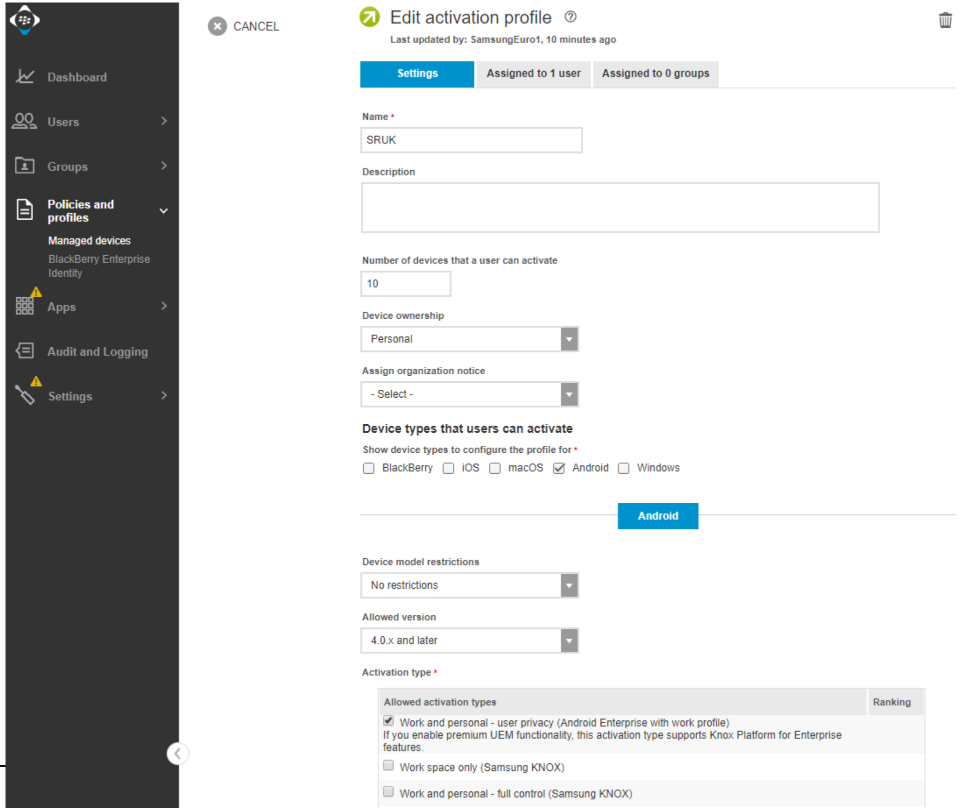
□ Perform SafetyNet attestation on BlackBerry Dynamics app activation

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 - 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 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

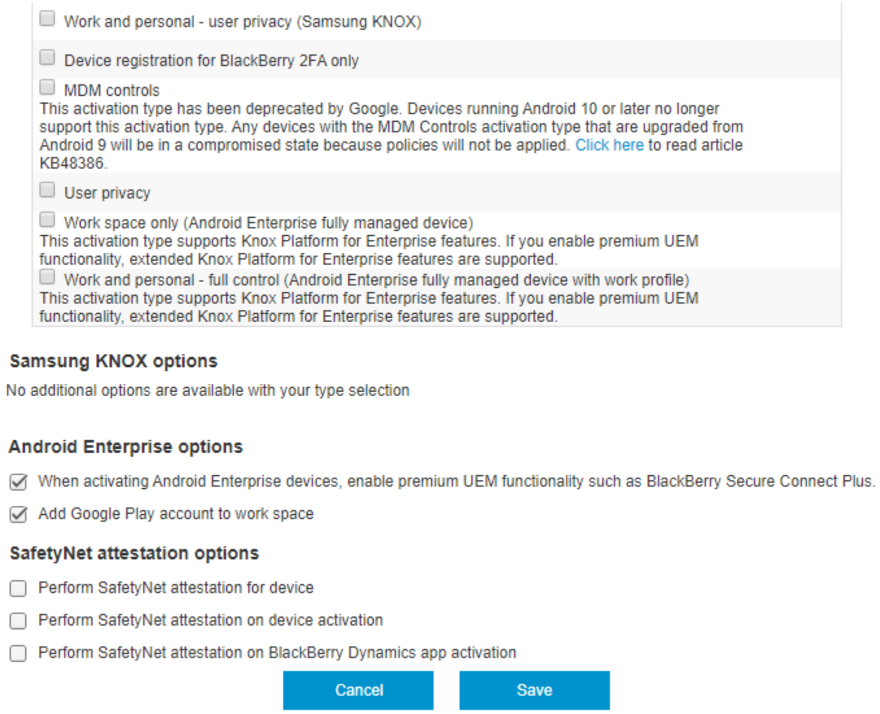
Android

Device model restrictions: No restrictions

Allowed version: 4.0.x and later

Activation type *

Allowed activation types	Ranking
☑ 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.	
□ 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.

□ 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

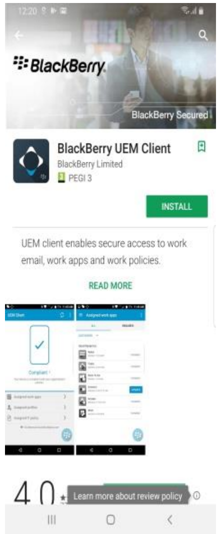
□ Perform SafetyNet attestation on BlackBerry Dynamics app activation

Knox Platform for Enterprise : Premium Edition

ANDROID ENTERPRISE BYOD DEPLOYMENT, WORK PROFILE UPGRADE TO KPE PREMIUM

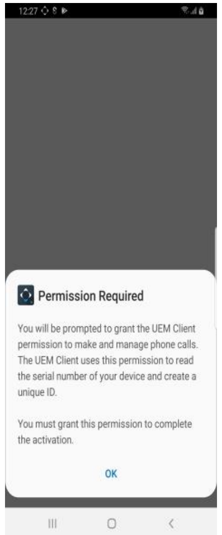
Now all you simply need to do is enroll your device by completing the following:

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



UEM client enables secure access to work email, work apps and work policies.

Install BlackBerry UEM Client from Google Play Store

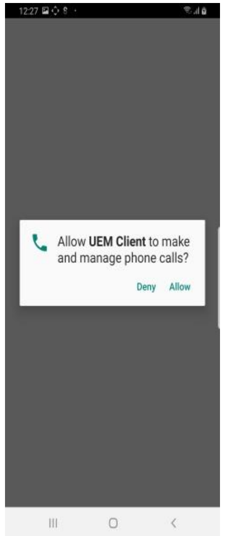


Permission Required

You will be prompted to grant the UEM Client permission to make and manage phone calls. The UEM Client uses this permission to read the serial number of your device and create a unique ID.

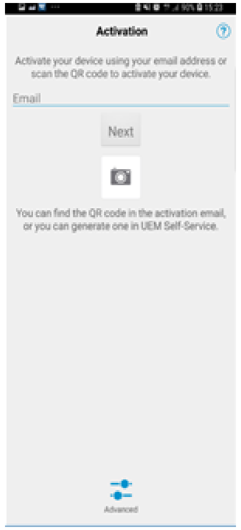
You must grant this permission to complete the activation.

Accept the permission request



Allow **UEM Client** to make and manage phone calls?

Allow UEM client to …

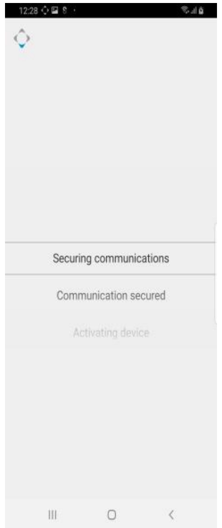


Activation

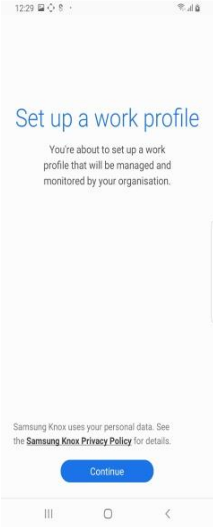
Activate your device using your email address or scan the QR code to activate your device.

You can find the QR code in the activation email, or you can generate one in UEM Self-Service.

Enter Credentials



Start of the Enrollment

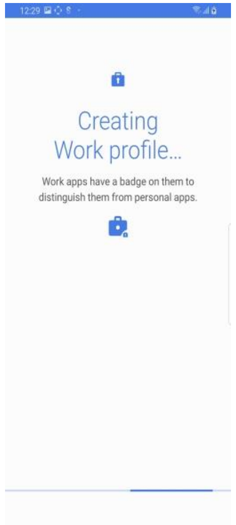


Set up a work profile

You're about to set up a work profile that will be managed and monitored by your organisation.

Samsung Knox uses your personal data. See the **Samsung Knox Privacy Policy** for details.

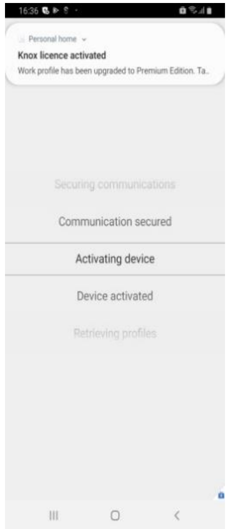
Click Continue to
Set up a Work Profile



Creating Work profile...

Work apps have a badge on them to distinguish them from personal apps.

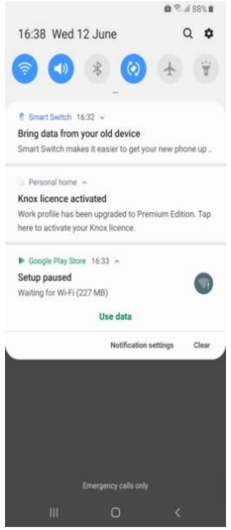
Creating Work Profile



Knox licence activated

Work profile has been upgraded to Premium Edition. Ta..

KPE Premium Edition License activation request

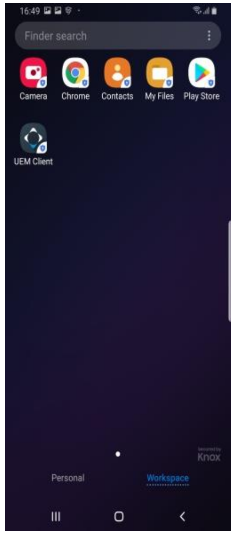


Bring data from your old device
Smart Switch makes it easier to get your new phone up ..

Knox licence activated
Work profile has been upgraded to Premium Edition. Tap here to activate your Knox licence.

Setup paused
Waiting for Wi-Fi (227 MB)

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

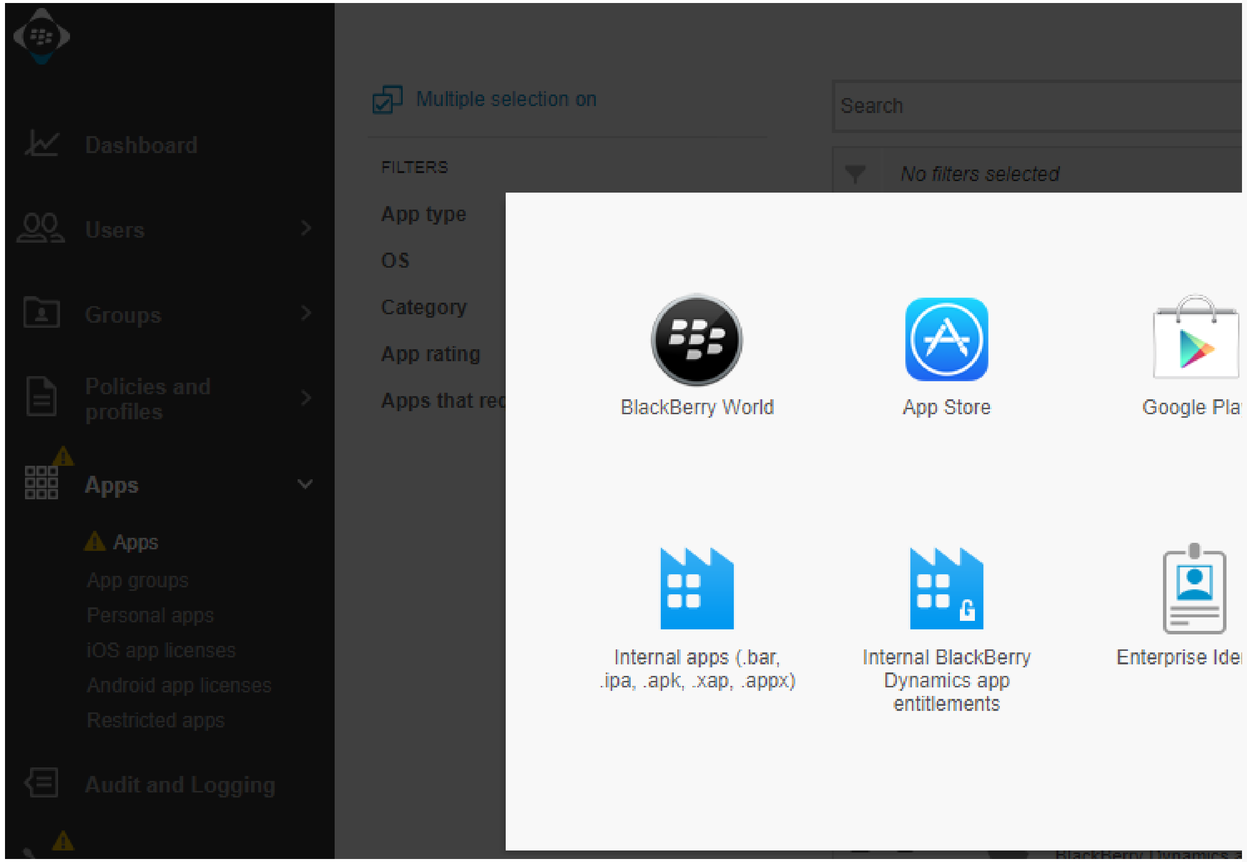


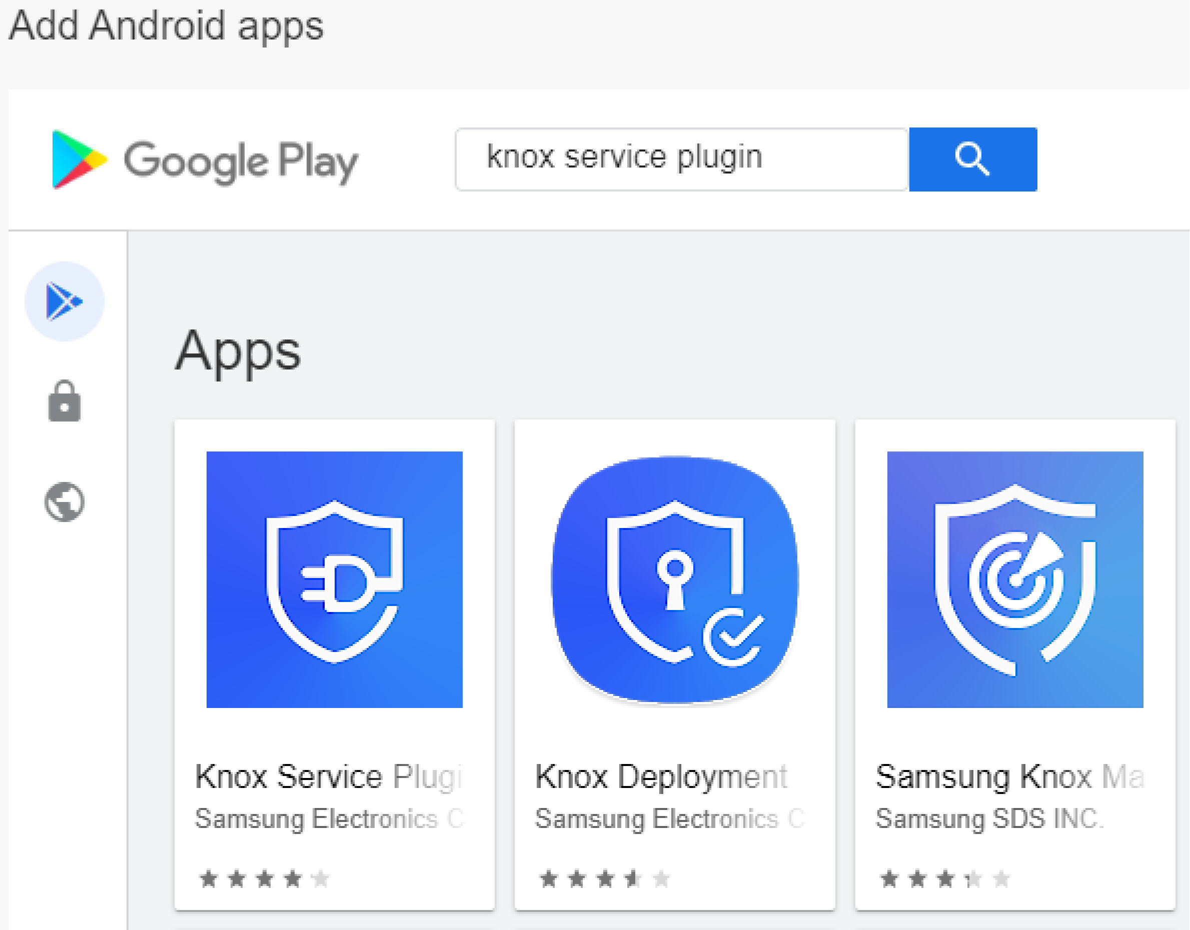
Work Profile device activated and
Work Profile upgraded to KPE Premium

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.

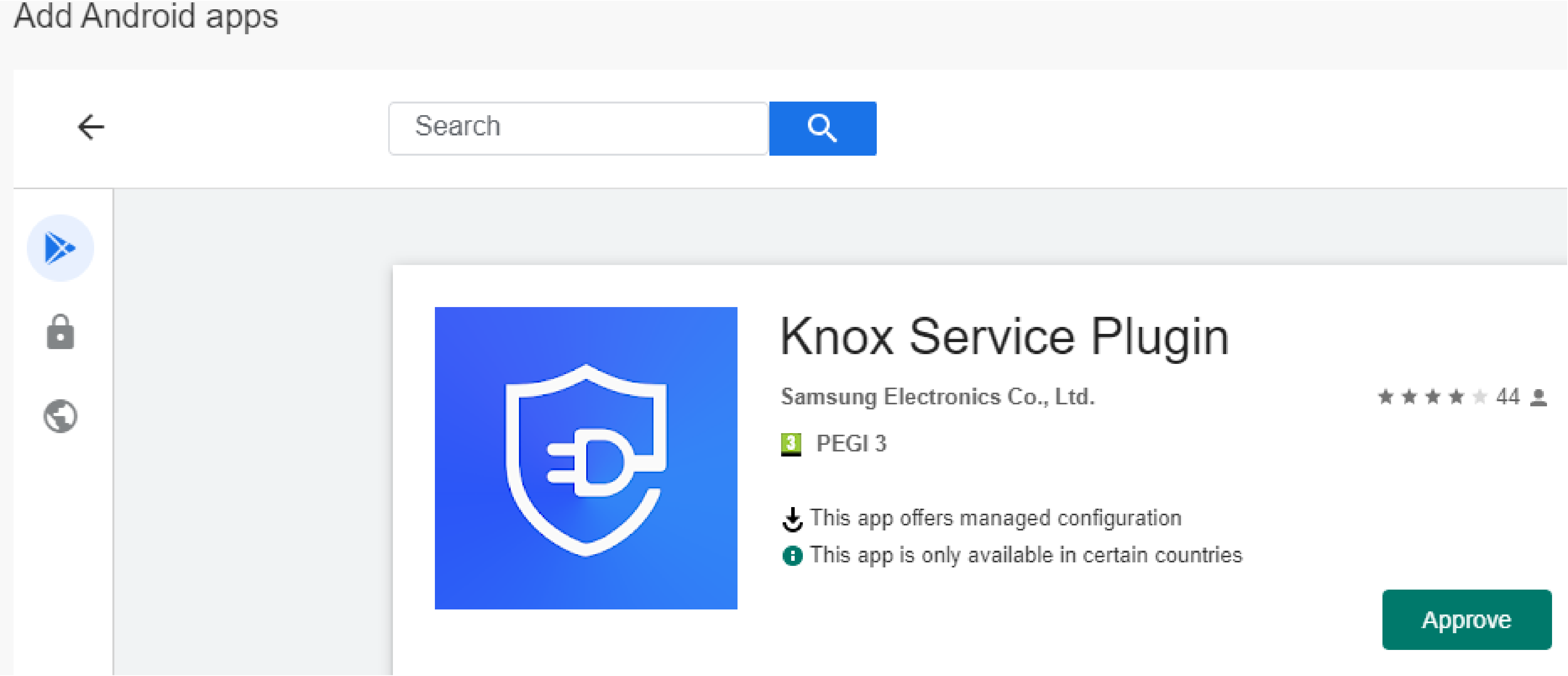
Navigate to *Apps* -> ▦ *to add an app -> Google Play -> Search for Knox Service Plugin*





Knox Service Plugin [KSP]

Approve etc…



Add Android apps

Knox Service Plugin

Samsung Electronics Co., Ltd.

PEGI 3

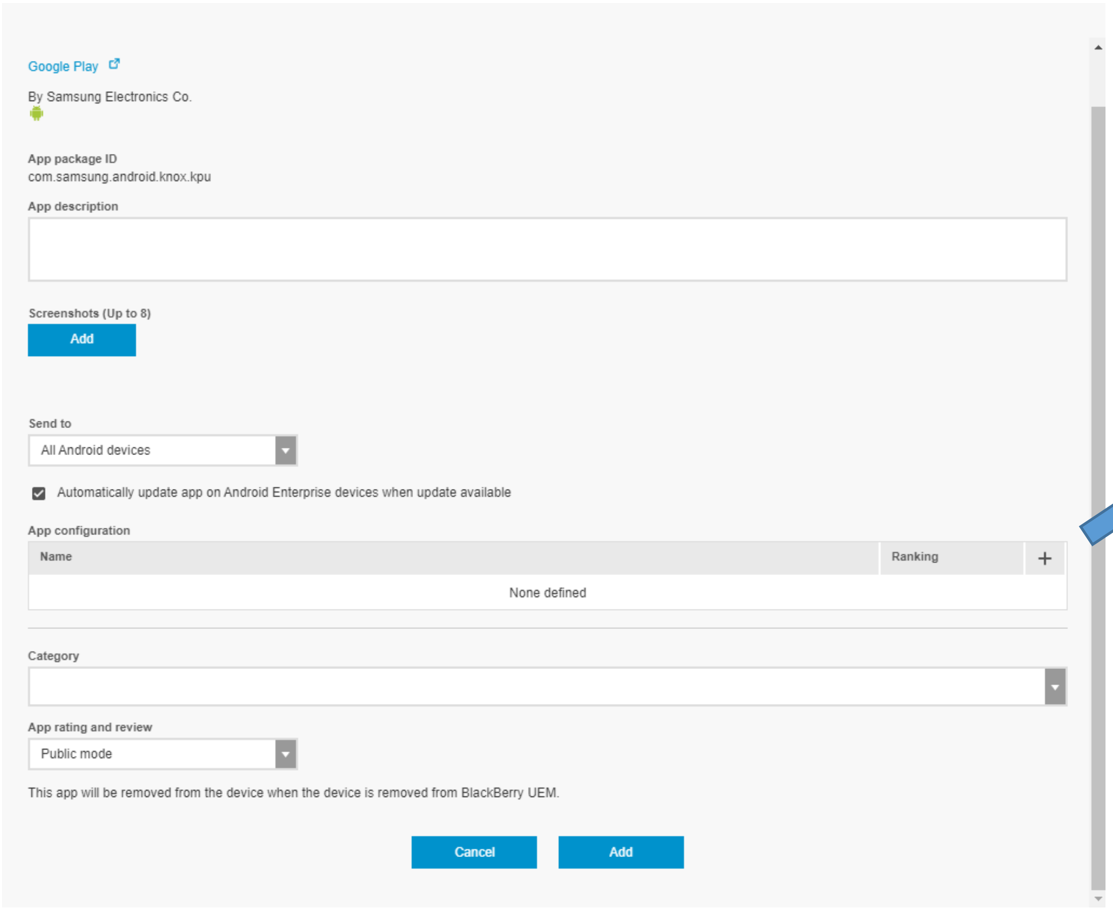
This app offers managed configuration

This app is only available in certain countries

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)

Send to: All Android devices

☑ Automatically update app on Android Enterprise devices when update available

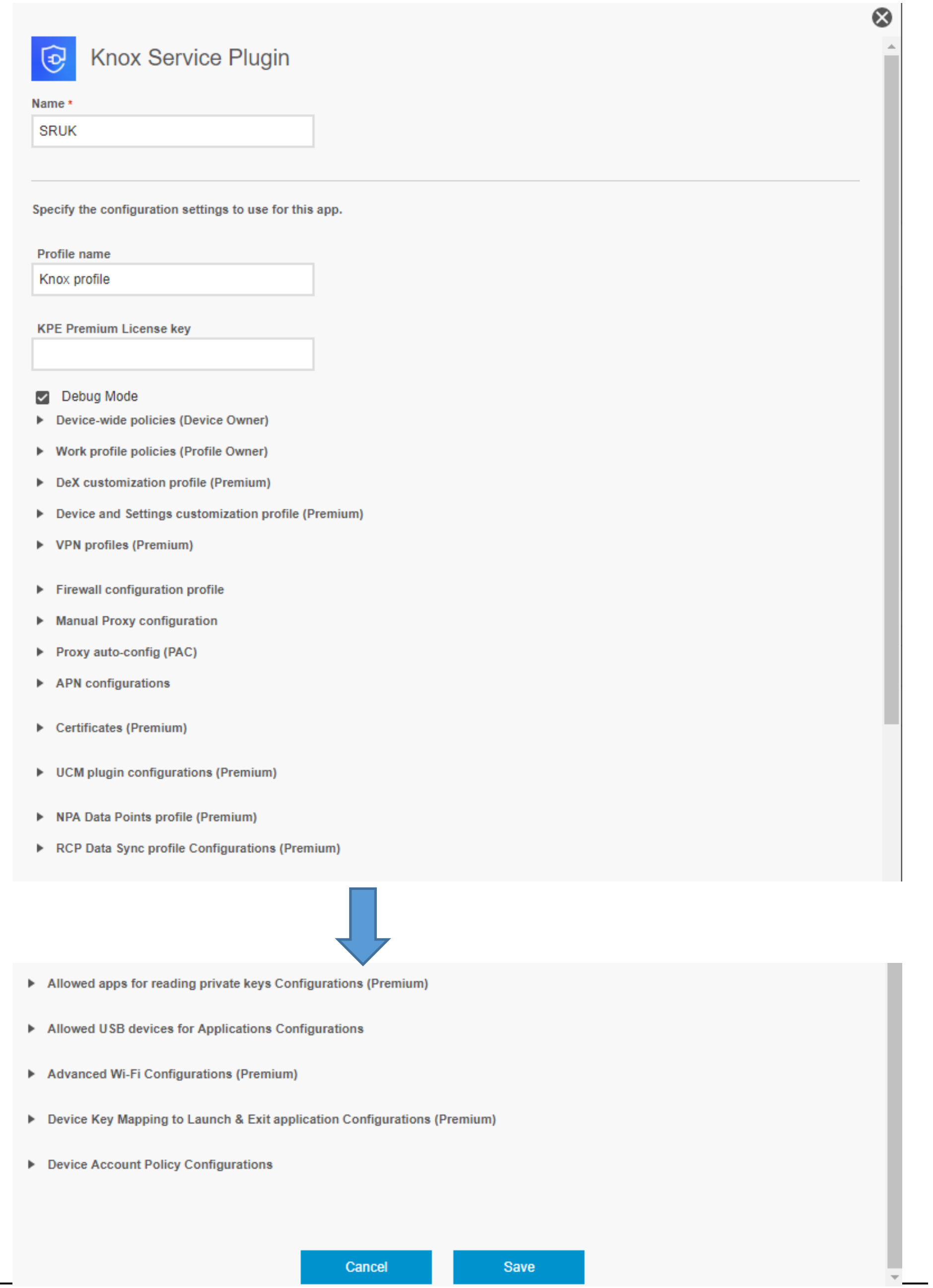
App configuration

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.



Knox Service Plugin

Name *: SRUK

Specify the configuration settings to use for this app.

Profile name: Knox profile

KPE Premium License key

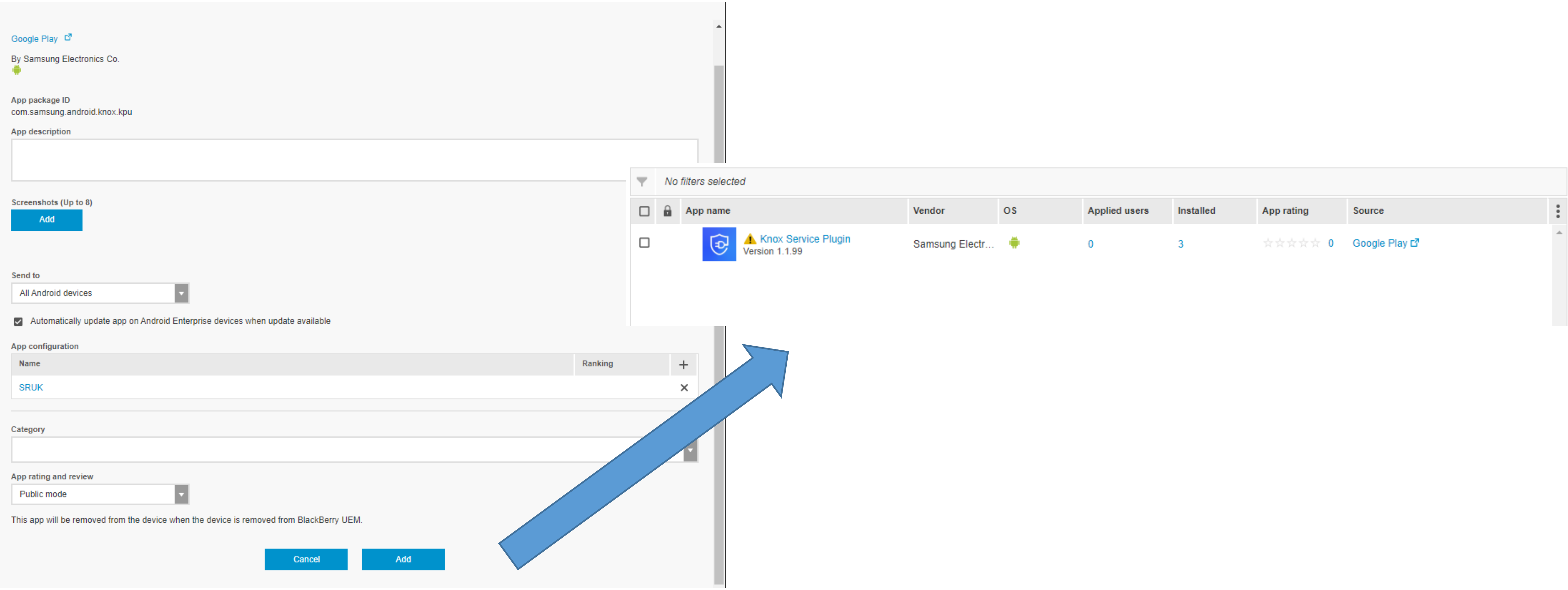
☑ Debug Mode

- 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

Knox Service Plugin [KSP]

CONFIGURE APP CONFIGURATION

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



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	

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

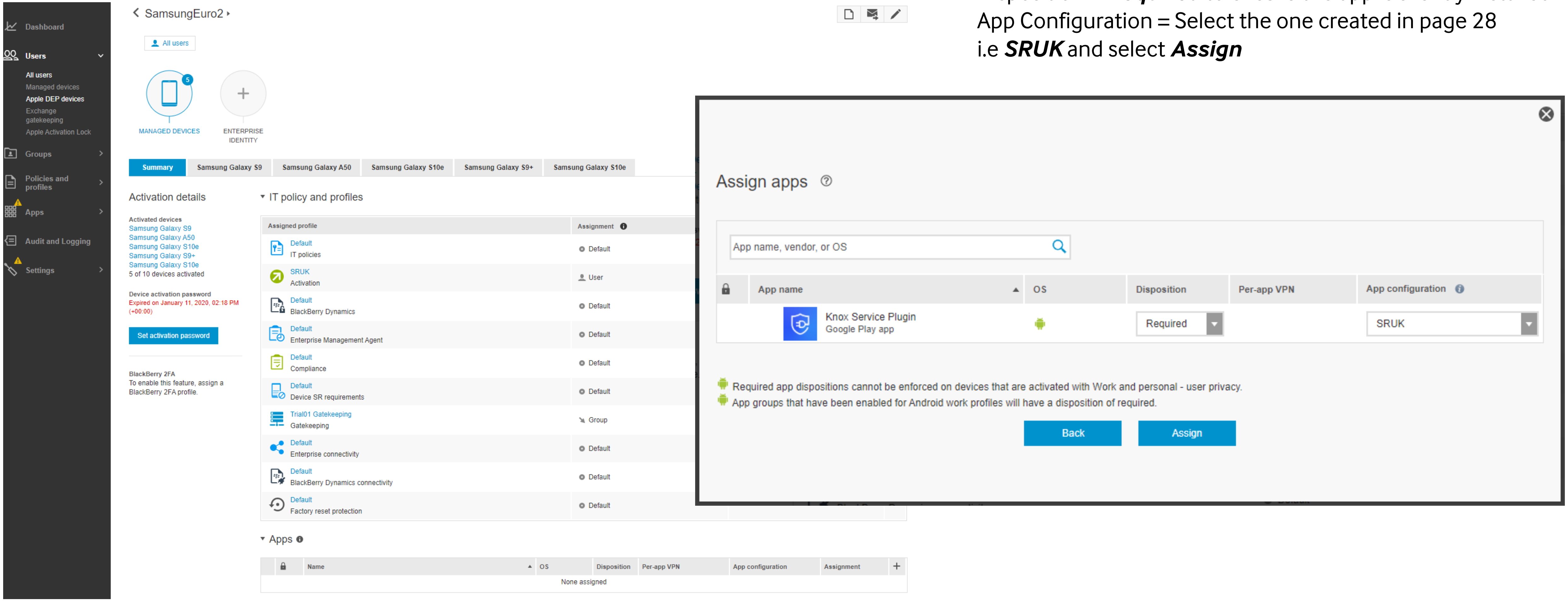
□	App name	Vendor	OS	Applied users	Installed	App rating	Source
□	⚠ Knox Service Plugin Version 1.1.99	Samsung Electr…		0	3	☆☆☆☆☆ 0	Google Play

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***



Activation details

Activated devices
Samsung Galaxy S9
Samsung Galaxy A50
Samsung Galaxy S10e
Samsung Galaxy S9+
Samsung Galaxy S10e
5 of 10 devices activated

Device activation password
Expired on January 11, 2020, 02:18 PM (+00:00)

Set activation password

BlackBerry 2FA
To enable this feature, assign a BlackBerry 2FA profile.

IT policy and profiles

Assigned profile	Assignment
Default IT policies	Default
SRUK Activation	User
Default BlackBerry Dynamics	Default
Default Enterprise Management Agent	Default
Default Compliance	Default
Default Device SR requirements	Default
Trial01 Gatekeeping Gatekeeping	Group
Default Enterprise connectivity	Default
Default BlackBerry Dynamics connectivity	Default
Default Factory reset protection	Default

Apps

	Name	OS	Disposition	Per-app VPN	App configuration	Assignment	+
	None assigned						

Assign apps

App name, vendor, or OS

	App name	OS	Disposition	Per-app VPN	App configuration
	Knox Service Plugin Google Play app		Required		SRUK

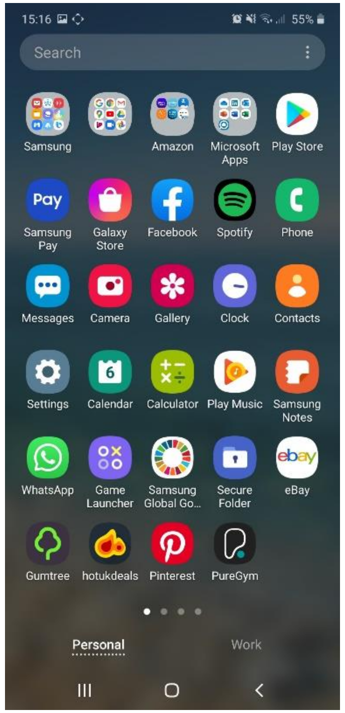
Required app dispositions cannot be enforced on devices that are activated with Work and personal - user privacy.
App groups that have been enabled for Android work profiles will have a disposition of required.

Back Assign

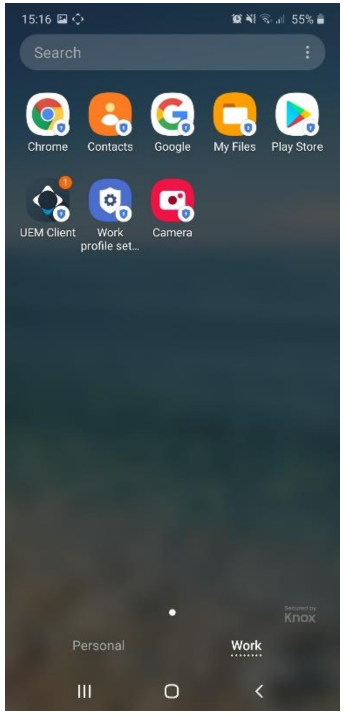
Knox Service Plugin [KSP]

KSP DEPLOYMENT ON THE DEVICE

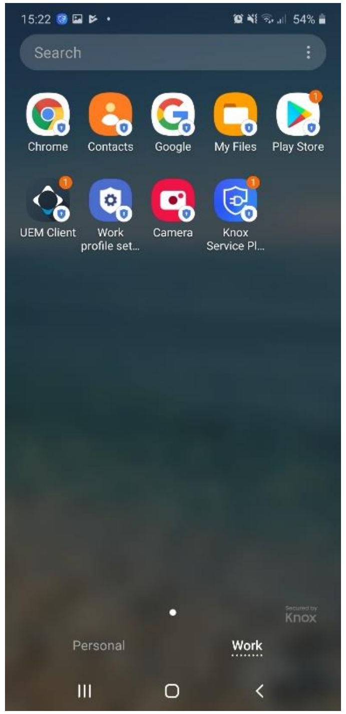
The below screen captures provide a view of the KSP app inside the Work Profile



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 in KSP configuration through managed app configuration

Document Information

THIS IS VERSION 2.2 OF THIS DOCUMENT.

Thank you!

Knox