

# VMware Workspace ONE UEM 2109

&

# Knox Platform for Enterprise

July 2021

Samsung R&D Centre UK  
(SRUK)

1. How to gain access to VMware Workspace ONE 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 a Company Owned Device
  - Dedicated Device
5. Managed Google Play [MGP] Configuration
6. AppConfig in Workspace ONE UEM
7. Configure Knox Platform for Enterprise : Standard Edition
8. Configure Knox Service Plugin [KSP]
9. Configure Knox Platform for Enterprise : Premium Edition

## Contacts:

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

## Knowledge Base:

<https://support.workspaceone.com/>

<https://www.vmware.com/products/workspace-one.html>

## VMWare Workspace ONE Solution:

<https://www.youtube.com/channel/UCZTvfJMhQ50c5TFw465tcJQ>

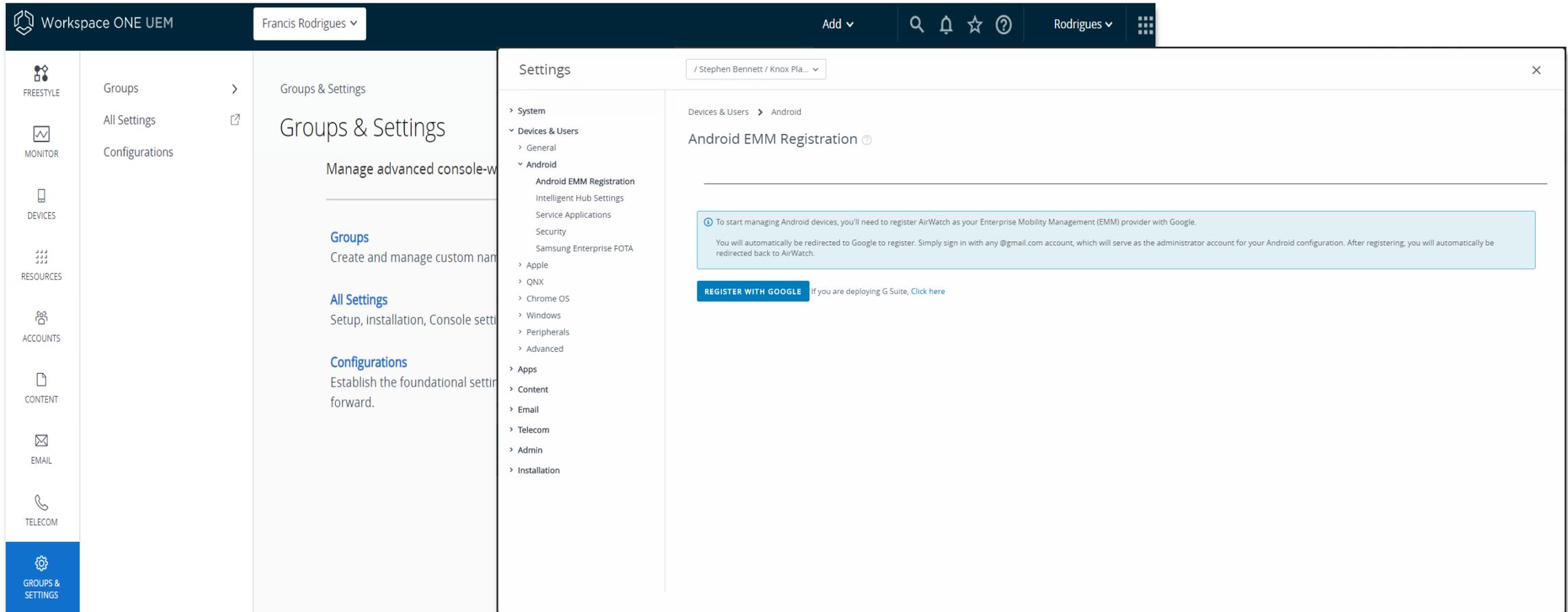
## Trial Access:

<https://www.vmware.com/workspace-one/free-trial.html>

1. Obtain access to VMware Workspace ONE UEM console
2. A Gmail account to map to Workspace ONE for Managed Google Play
3. Consider what enrollment method to use:
  - Knox Mobile Enrollment (KME)
  - QR Code enrollment
  - Email enrollment
  - Server details enrollment

## Configure Android Enterprise

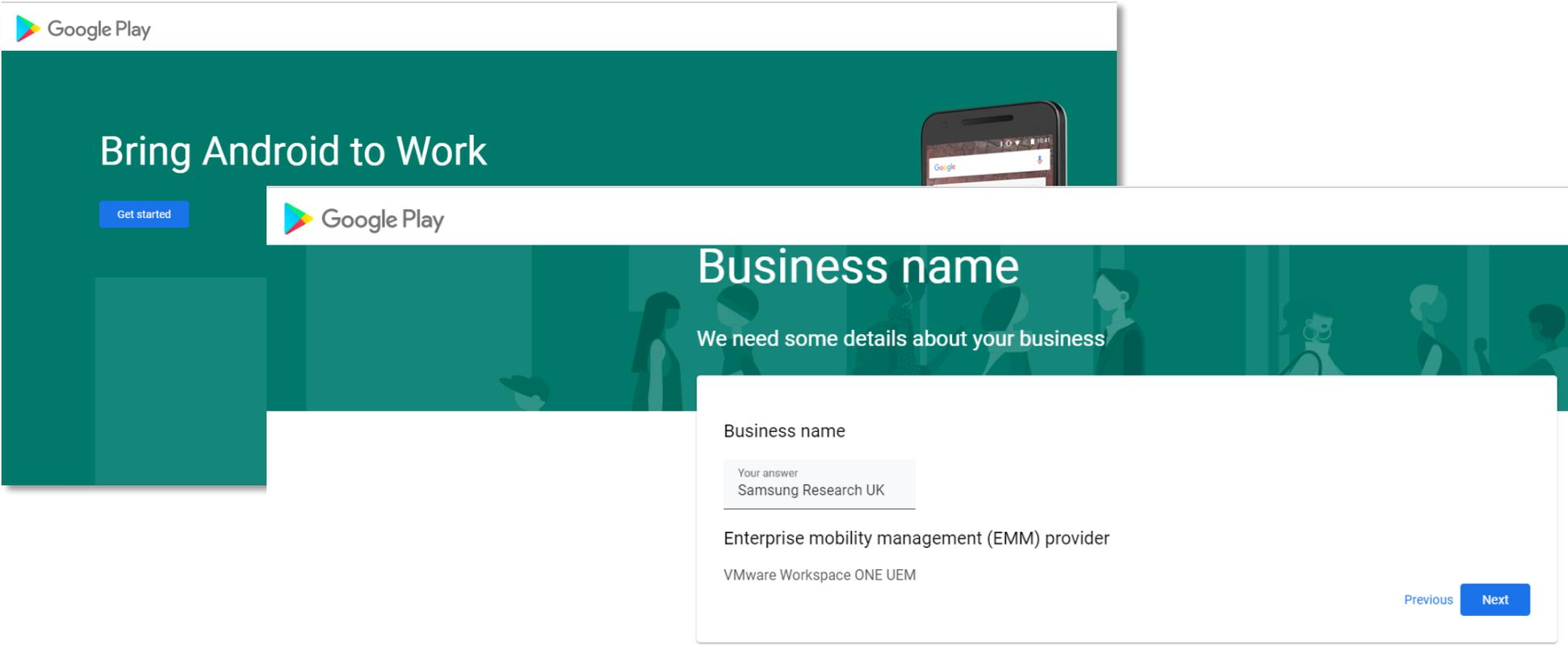
- Log into Workspace ONE UEM Console. Navigate to: GROUPS & SETTINGS -> All Settings -> Devices & Users -> Android -> Android EMM Registration.
- Select REGISTER WITH GOOGLE button.



The screenshot displays the Workspace ONE UEM console interface. The top navigation bar includes the Workspace ONE UEM logo, the user name 'Francis Rodrigues', and various utility icons. The left sidebar contains a navigation menu with categories like FREESTYLE, MONITOR, DEVICES, RESOURCES, ACCOUNTS, CONTENT, EMAIL, and TELECOM, with 'GROUPS & SETTINGS' highlighted at the bottom. The main content area is divided into three sections: a left sidebar for 'Groups & Settings' with options for 'Groups', 'All Settings', and 'Configurations'; a middle section titled 'Groups & Settings' with a description 'Manage advanced console-w...'; and a right section titled 'Settings' for 'Stephen Bennett / Knox Pla...'. The 'Settings' section is expanded to show 'Devices & Users > Android', with 'Android EMM Registration' selected. A light blue informational box states: 'To start managing Android devices, you'll need to register AirWatch as your Enterprise Mobility Management (EMM) provider with Google. You will automatically be redirected to Google to register. Simply sign in with any @gmail.com account, which will serve as the administrator account for your Android configuration. After registering, you will automatically be redirected back to AirWatch.' Below this box is a prominent blue 'REGISTER WITH GOOGLE' button, followed by a link: 'If you are deploying G Suite, [Click here](#)'.

## Configure Android Enterprise

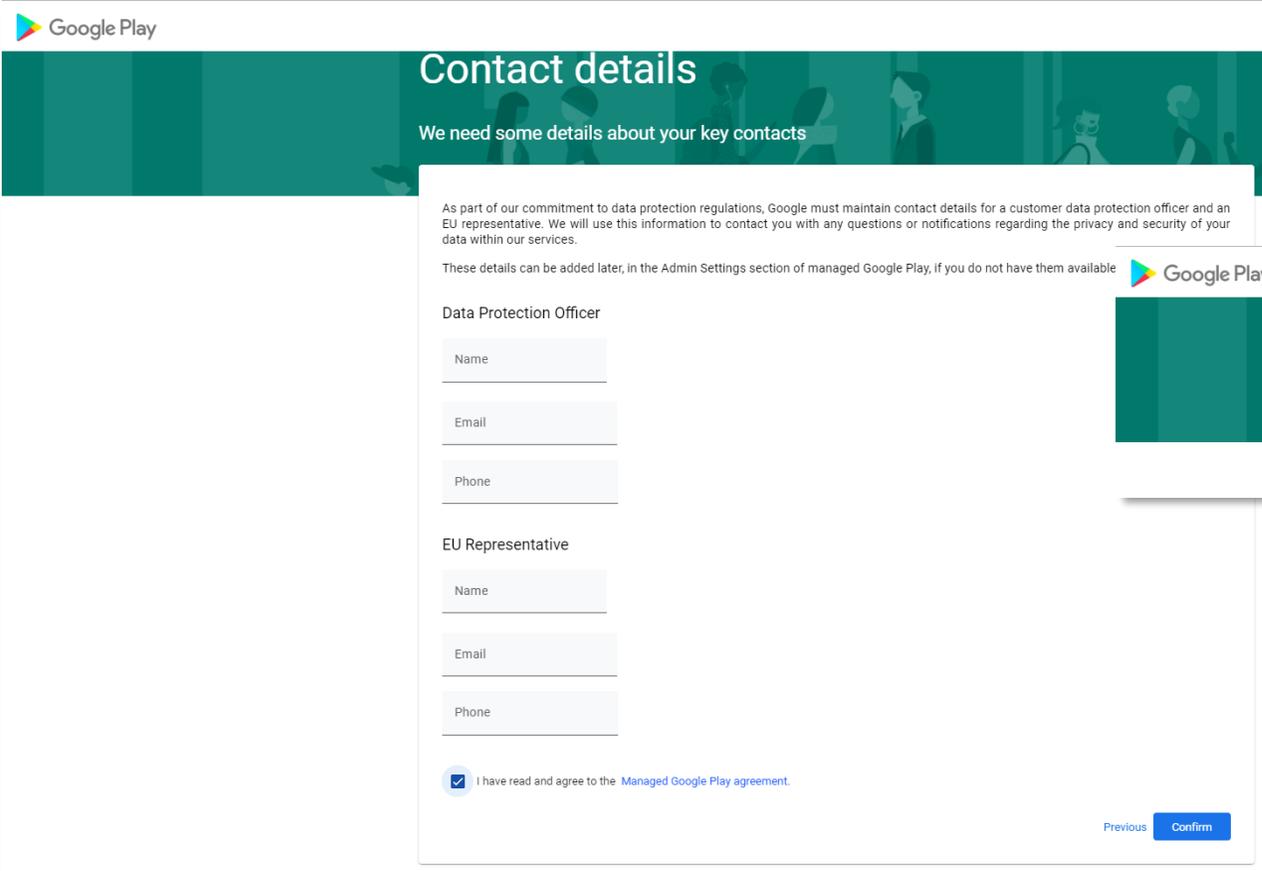
- You will then get redirected to a Google Play screen. Click Sign In. Once signed in with your Gmail account, you will be redirected again. Select Get started.
- Fill out your Business name and Select Next to allow VMware Workspace ONE UEM to be your EMM provider.



The screenshot displays the Google Play 'Bring Android to Work' setup interface. The main heading is 'Bring Android to Work' with a 'Get started' button. Below this, a 'Business name' section prompts the user to provide details about their business. The form shows 'Your answer' as 'Samsung Research UK'. The 'Enterprise mobility management (EMM) provider' is set to 'VMware Workspace ONE UEM'. Navigation buttons for 'Previous' and 'Next' are located at the bottom right of the form.

## 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 to complete the Android Enterprise configuration and return to VMware Workspace ONE UEM Console.



Google Play

## 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 data protection officer and an EU representative. We will use this information to contact you with any questions or notifications regarding the privacy and security of your data within our services.

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

**Data Protection Officer**

Name

Email

Phone

**EU Representative**

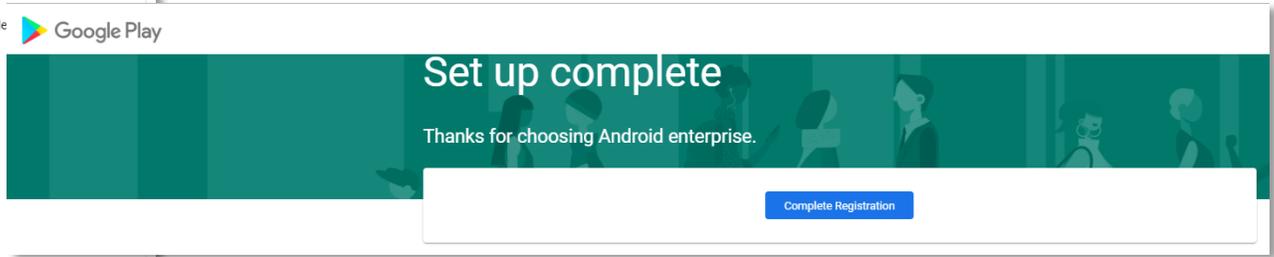
Name

Email

Phone

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

Previous Confirm



Google Play

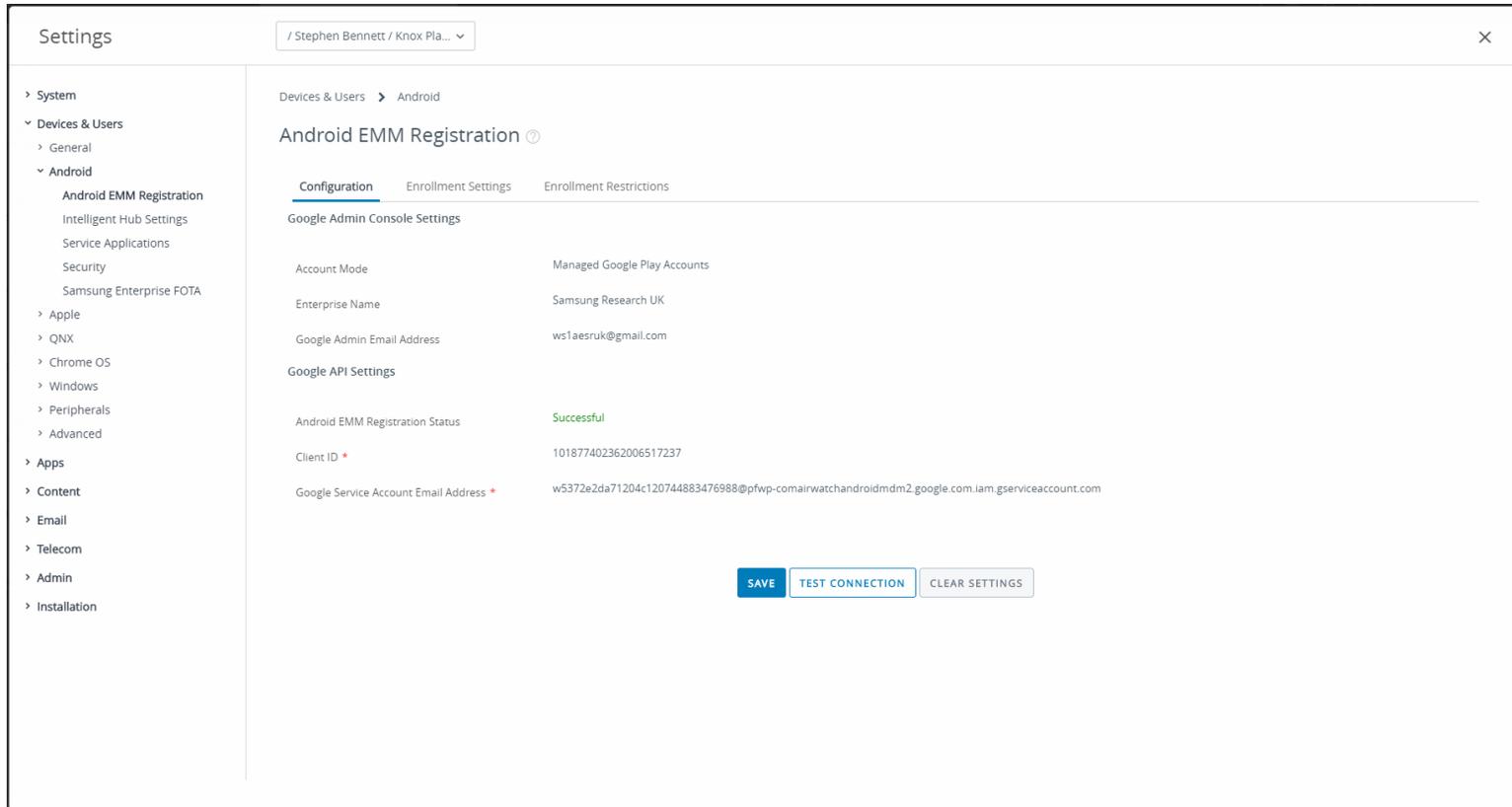
## Set up complete

Thanks for choosing Android enterprise.

Complete Registration

## Configure Android Enterprise

- You should now have been redirected back to the Android EMM Registration page and the configuration should now be completed and look similar to the below.
- Your Workspace ONE UEM tenant is now configured and ready to deploy Android Enterprise and Knox Platform for Enterprise: Standard Edition.



The screenshot shows the 'Settings' application interface. At the top, the user is identified as 'Stephen Bennett / Knox Pla...'. The left sidebar contains a navigation menu with categories like System, Devices & Users, and Apps. The 'Android' section is expanded, showing 'Android EMM Registration' as the selected option. The main content area is titled 'Android EMM Registration' and has three tabs: 'Configuration', 'Enrollment Settings', and 'Enrollment Restrictions'. The 'Configuration' tab is active, displaying 'Google Admin Console Settings' with fields for 'Account Mode' (Managed Google Play Accounts), 'Enterprise Name' (Samsung Research UK), and 'Google Admin Email Address' (ws1aesruk@gmail.com). Below this is the 'Google API Settings' section, which shows the 'Android EMM Registration Status' as 'Successful' in green text. Other fields include 'Client ID' (101877402362006517237) and 'Google Service Account Email Address' (w5372e2da71204c120744883476988@pfwp-comairwatchandroidmdm2.google.com.lam.gserviceaccount.com). At the bottom of the configuration area, there are three buttons: 'SAVE', 'TEST CONNECTION', and 'CLEAR SETTINGS'.

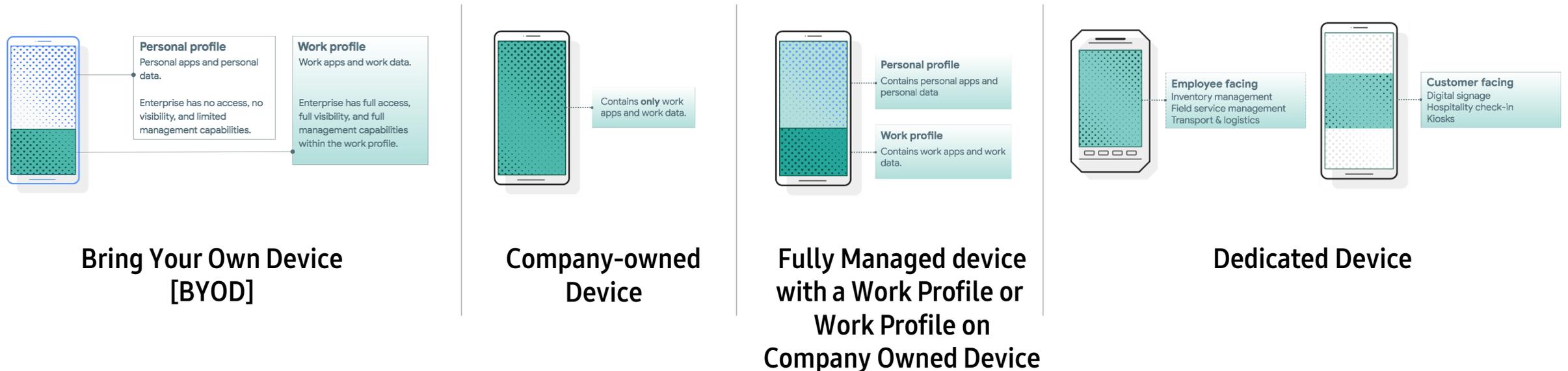
# Android Enterprise Deployment Modes

## Deployment Modes

Android Enterprise can be deployed in the following 5 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, up to Android 10*]
4. Work Profile On Company owned Device [*WPC, Android 11 or after*]
5. Dedicated device [*formerly known as COSU*]

VMware Workspace ONE UEM can support **all** 5 of these deployment modes. In this next section we will show you how to configure each of these 5 deployment modes in VMware Workspace ONE UEM for your device fleet.



## Android Enterprise BYOD Deployment

To enroll a device in the Android Enterprise BYOD deployment type, the final pre requisite is you need to ensure that the legacy Android container options are disabled. To do this:

- Go to *GROUPS & SETTINGS* -> *All Settings* -> *Devices & Users* -> *Android* -> *Intelligent Hub Settings*
- About half way down you will see a Samsung KNOX section. Set Enable Containers to DISABLED and ensure the Knox License Key field is blank. Then scroll all the way to the bottom and click Save.



The screenshot shows the Samsung KNOX settings interface. It includes a text input field for the Knox License Key, which is currently blank, and a 'Show Characters' toggle. Below this are two toggle switches: 'Enable Containers' is set to 'DISABLED' (indicated by a blue bar), and 'Enable Audit Logging' is set to 'ENABLED' (indicated by a white bar).

## 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 VMware Intelligent Hub, and enroll your device into your tenant.



Install Intelligent Hub from Google Play Store



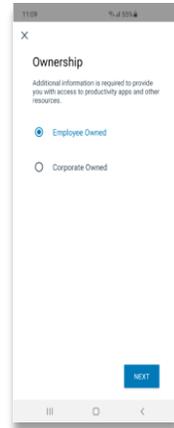
Enter server URL & hit NEXT



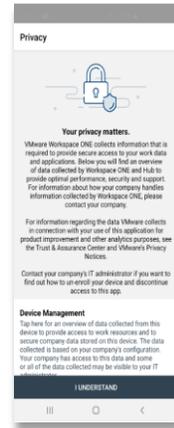
Enter Group ID & hit NEXT



Enter credentials & hit NEXT



Select Employee Owned



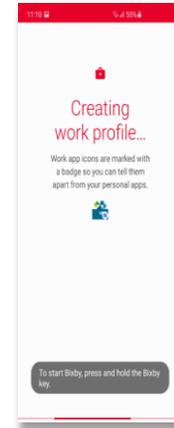
Accept privacy permissions



Agree to Data Sharing



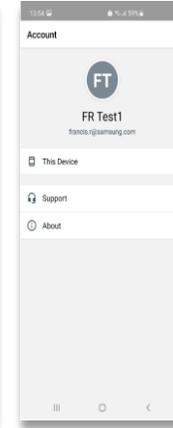
Click Agree to create Work Profile



Creating Work Profile



Create a Passcode



Successful Enrollment



Note: Work and Personal tabs plus icon Badges in Personal Profile

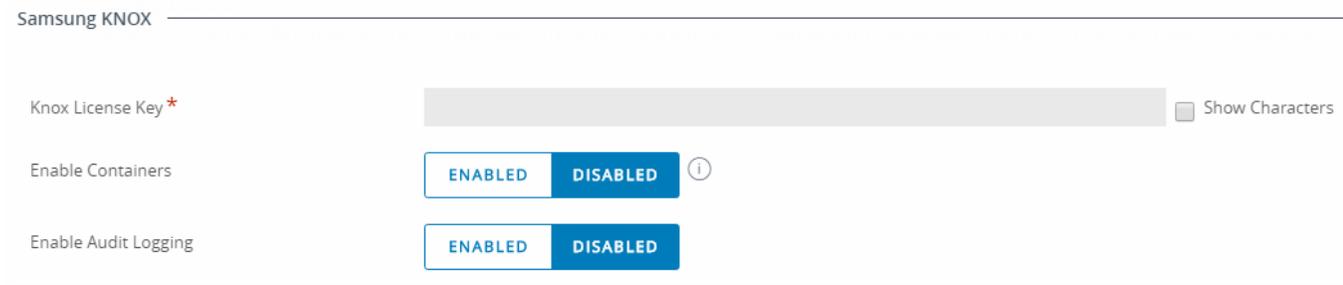
\*You can also enroll your device using the alternative Workspace ONE UEM methods. For example QR Code.

\*\*Knox Mobile Enrollment is not a compatible enrollment method for this deployment type

## Android Enterprise Company-owned Device Deployment

To enroll a device in the Android Enterprise Company-owned Device deployment type, the final pre requisites are you need to ensure that the legacy Android container options are disabled and that the Android EMM Registration Enrollment Settings are set correctly. To do this:

- Go to *GROUPS & SETTINGS -> All Settings -> Devices & Users -> Android -> Intelligent Hub Settings*
- About half way down you will see a Samsung KNOX section. Set Enable Containers to DISABLED and ensure the Knox License Key field is blank. Then scroll all the way to the bottom and click Save.

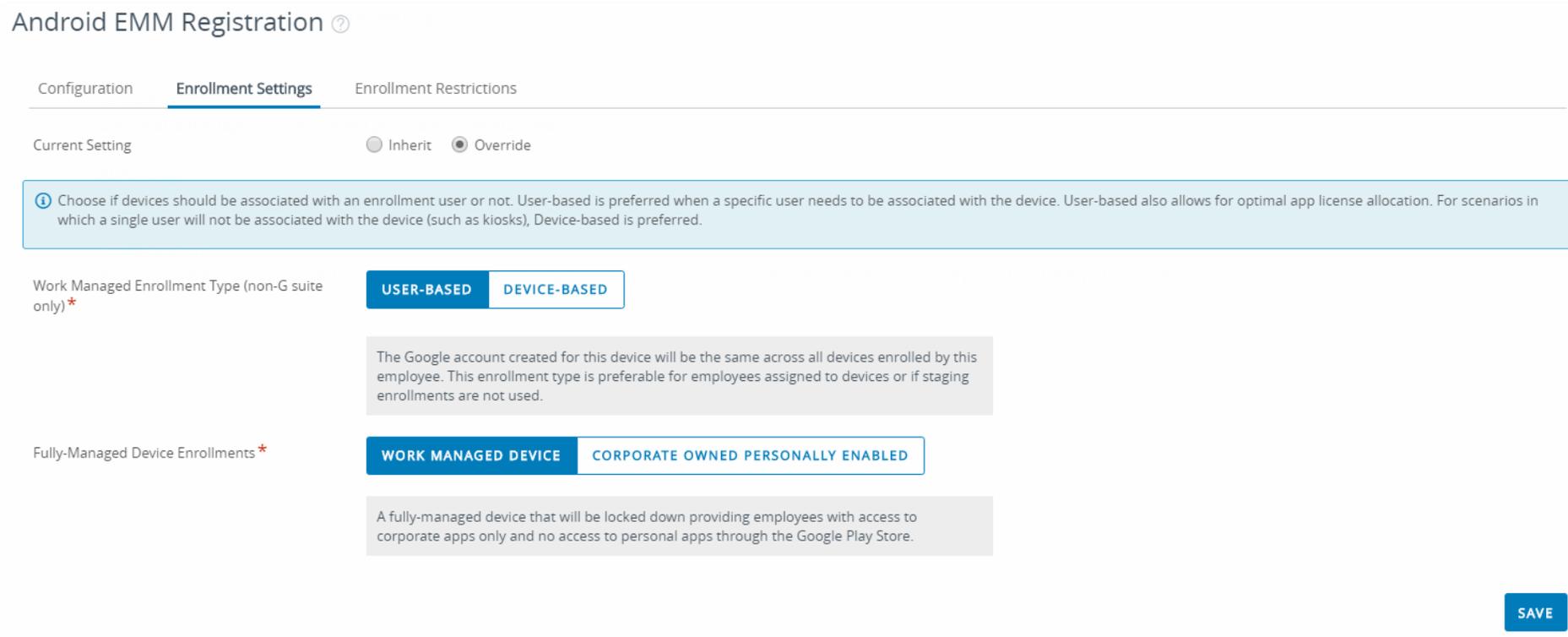


The screenshot shows the Samsung KNOX settings interface. It includes a text input field for the Knox License Key, which is currently blank, and a 'Show Characters' toggle. Below this are two toggle switches: 'Enable Containers' and 'Enable Audit Logging'. Both are currently set to 'ENABLED', but the 'ENABLED' button for 'Enable Containers' is highlighted in blue, indicating it is the selected state. An information icon is visible next to the 'Enable Containers' toggle.

## Android Enterprise Company-owned Device Deployment

To ensure that the Android EMM Registration Enrollment Settings are set correctly.

- Go to *Groups & Settings* -> *All Settings* -> *Devices & Users* -> *Android* -> *Android EMM Registration* -> *Enrollment Settings*
- Ensure **Work Managed Enrollment Type** is set to **USER-BASED** and **Fully-Managed Device Enrollments** is set to **WORK MANAGED DEVICE**.



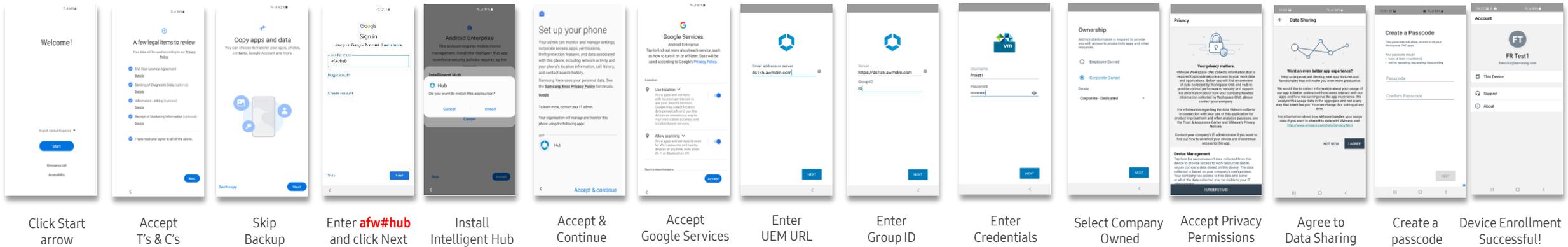
The screenshot shows the 'Android EMM Registration' configuration page, specifically the 'Enrollment Settings' tab. At the top, there are three tabs: 'Configuration', 'Enrollment Settings' (which is selected), and 'Enrollment Restrictions'. Below the tabs, there is a 'Current Setting' section with two radio buttons: 'Inherit' and 'Override', with 'Override' being selected. A blue information box contains the following text: 'Choose if devices should be associated with an enrollment user or not. User-based is preferred when a specific user needs to be associated with the device. User-based also allows for optimal app license allocation. For scenarios in which a single user will not be associated with the device (such as kiosks), Device-based is preferred.' Below this, there are two main settings. The first is 'Work Managed Enrollment Type (non-G suite only)\*', which has two buttons: 'USER-BASED' (selected) and 'DEVICE-BASED'. A grey text box below it explains: 'The Google account created for this device will be the same across all devices enrolled by this employee. This enrollment type is preferable for employees assigned to devices or if staging enrollments are not used.' The second setting is 'Fully-Managed Device Enrollments\*', which has two buttons: 'WORK MANAGED DEVICE' (selected) and 'CORPORATE OWNED PERSONALLY ENABLED'. A grey text box below it explains: 'A fully-managed device that will be locked down providing employees with access to corporate apps only and no access to personal apps through the Google Play Store.' At the bottom right of the page, there is a blue 'SAVE' button.

## 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 3 ways you can enroll your device into Workspace ONE UEM as an Android Enterprise Company-owned device.

1. DPC Identifier [Also known as the hashtag method] **afw#hub**
2. QR Code Enrollment / NFC Enrollment
3. 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 or Work Profile on Company Owned Device [Android 11+]

## Android Enterprise Fully Managed Device with a Work Profile or Work Profile on Company Owned Device

To enroll a device in the Android Enterprise Fully Managed Device with a Work Profile or Work Profile on Company Owned Device (Android 11+) deployment type, the final pre requisites are you need to ensure that the legacy Android container options are disabled and that the Android EMM Registration Enrollment Settings are set correctly. To do this:

- Go to *GROUPS & SETTINGS* -> *All Settings* -> *Devices & Users* -> *Android* -> *Intelligent Hub Settings*
- About half way down you will see a Samsung KNOX section. Set Enable Containers to DISABLED and ensure the Knox License Key field is blank. Then scroll all the way to the bottom and click Save.

Samsung KNOX

Knox License Key \*   Show Characters

Enable Containers  ENABLED  DISABLED ⓘ

Enable Audit Logging  ENABLED  DISABLED

# Android Enterprise: Fully Managed Device with a Work Profile or Work Profile on Company Owned Device [Android 11+]

## Android Enterprise Fully Managed Device with a Work Profile Deployment & Work Profile on Company Owned Device

To ensure that the Android EMM Registration Enrollment Settings are set correctly.

- Go to *GROUPS & SETTINGS* -> *All Settings* -> *Devices & Users* -> *Android* -> *Android EMM Registration* -> *Enrollment Settings*
- Ensure **Work Managed Enrollment Type** is set to **USER-BASED** and **Fully-Managed Device Enrollments** is set to **CORPORATE OWNED PERSONALLY ENABLED**.

### Android EMM Registration ?

Configuration **Enrollment Settings** Enrollment Restrictions

Current Setting  Inherit  Override

? Choose if devices should be associated with an enrollment user or not. User-based is preferred when a specific user needs to be associated with the device. User-based also allows for optimal app license allocation. For scenarios in which a single user will not be associated with the device (such as kiosks), Device-based is preferred.

Work Managed Enrollment Type (non-G suite only)\* **USER-BASED** **DEVICE-BASED**

The Google account created for this device will be the same across all devices enrolled by this employee. This enrollment type is preferable for employees assigned to devices or if staging enrollments are not used.

Fully-Managed Device Enrollments\* **WORK MANAGED DEVICE** **CORPORATE OWNED PERSONALLY ENABLED**

Complete device management will remain intact. Employees will receive a Work Profile to access corporate apps and will still have access to their personal Google Play Store outside of the Work Profile. For Android versions 8.0 and later.

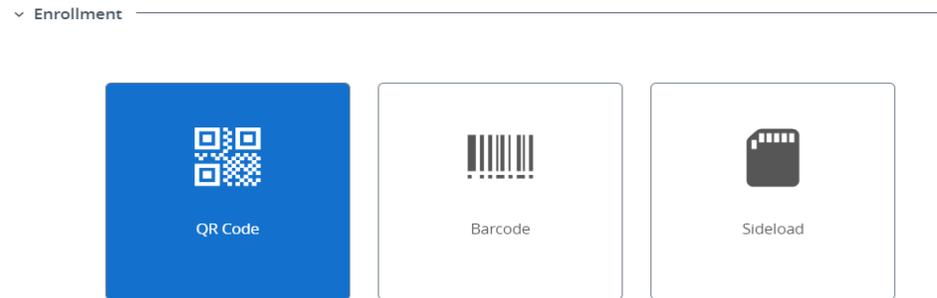
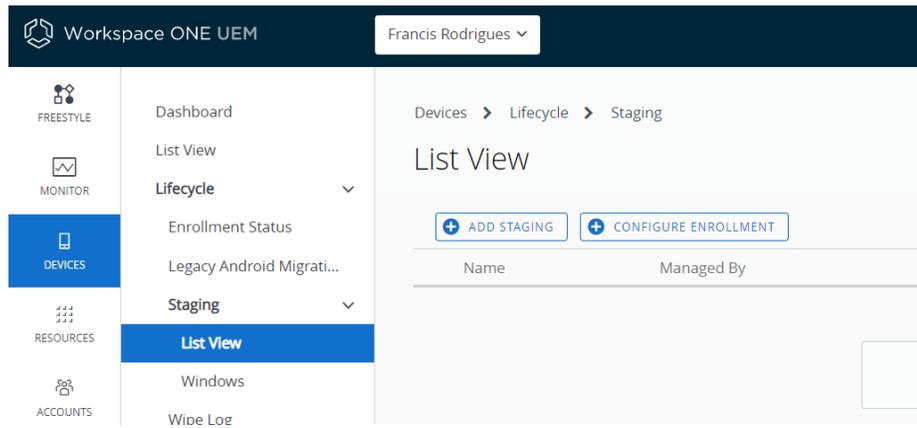
**SAVE**

# Android Enterprise: Fully Managed Device with a Work Profile or Work Profile on Company Owned Device [Android 11+]

## Android Enterprise Fully Managed Device with a Work Profile Deployment & Work Profile on Company Owned Device

To create the Workspace One UEM QR code for this type of enrollment, please do the following.

- Go to *DEVICES -> Lifecycle -> Staging -> List View -> + CONFIGURE ENROLLMENT*
- Choose *Android* (under Platform), -> *QR Code* (under Enrollment) -> *CONFIGURE*
- Configure the options for your environment and choose to *DOWNLOAD FILE* prior to closing. This file can be distributed accordingly.



### Enrollment Configuration Wizard

- 1 Wi-Fi
- 2 Hub
- 3 Enrollment Details
- 4 Summary**

Configuration is complete, and the QR code is available for download. The QR code is in plain text and can be interpreted by any QR reader/decoder. Please take necessary precautions to avoid leakage of any sensitive information.

Please choose to either download or view your PDF.

[DOWNLOAD FILE](#)

[VIEW PDF](#)

You configured the following components. Please note that this data is not saved, so make sure the configuration is correct before closing

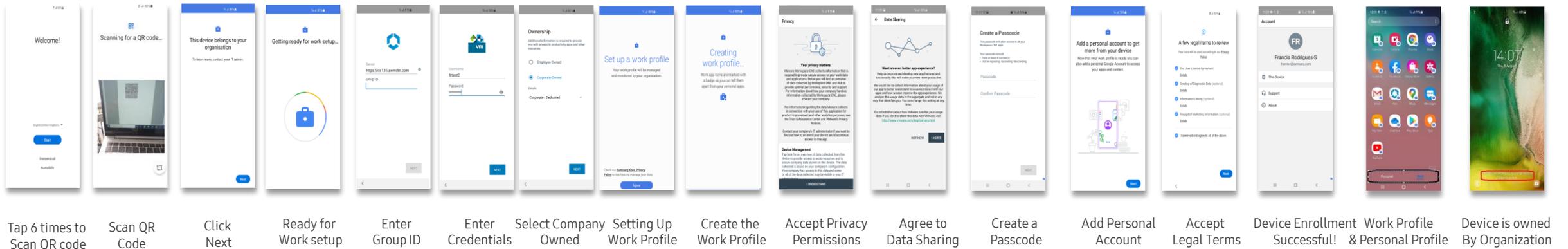
# Android Enterprise: Fully Managed Device with a Work Profile or Work Profile on Company Owned Device [Android 11+]

## Android Enterprise Fully Managed Device with a Work Profile Deployment

To enroll your device as an Android Enterprise Fully Managed Device with a Work Profile, you need to ensure the device is factory reset and at the welcome screen. From here, there are 2 ways you can enroll your device into Workspace ONE UEM as an Android Enterprise Company-owned device.

1. QR Code Enrollment / NFC Enrollment
2. Knox Mobile Enrollment

- Below is a screen-by-screen play to enroll your device using the QR code method. The QR Code is provided by your IT Admin



Tap 6 times to Scan QR code    Scan QR Code    Click Next    Ready for Work setup    Enter Group ID    Enter Credentials    Select Company Owned    Setting Up Work Profile    Create the Work Profile    Accept Privacy Permissions    Agree to Data Sharing    Create a Passcode    Add Personal Account    Accept Legal Terms    Device Enrollment Successful!    Work Profile & Personal Profile    Device is owned By Organization

## Android Enterprise Dedicated Device Deployment

To enroll a device in the Android Enterprise Dedicated Device deployment type, the final pre requisites are you need to ensure that the legacy Android container options are disabled and that the Android EMM Registration Enrollment Settings are set correctly. To do this:

- Go to *GROUPS & SETTINGS* -> *All Settings* -> *Devices & Users* -> *Android* -> *Intelligent Hub Settings*
- About half way down you will see a Samsung KNOX section. Set Enable Containers to DISABLED and ensure the Knox License Key field is blank. Then scroll all the way to the bottom and click Save.



Samsung KNOX

Knox License Key \*   Show Characters

Enable Containers   ⓘ

Enable Audit Logging

## Android Enterprise Dedicated Device Deployment

To ensure that the Android EMM Registration Enrollment Settings are set correctly.

- Go to *GROUPS & SETTINGS* -> *All Settings* -> *Devices & Users* -> *Android* -> *Android EMM Registration* -> *Enrollment Settings*
- Ensure **Work Managed Enrollment Type** is set to **DEVICE-BASED** and **Fully-Managed Device Enrollments** is set to **WORK MANAGED DEVICE**.

### Android EMM Registration ?

Configuration

**Enrollment Settings**

Enrollment Restrictions

Current Setting

Inherit  Override

Management Mode for Corporate Devices \*

**WORK MANAGED**

CORPORATE OWNED PERSONALLY ENABLED

A fully managed and locked-down device. Employees will only have access to corporate apps and no access to personal apps through the Google Play Store.

Google Account Generation for Corporate Devices \*

**DEVICE-BASED**

USER-BASED

AOSP / CLOSED NETWORK

The generated Google account on the device is unique to each device enrolled by the same enrollment user. Ideal for staging and dedicated devices.

## Android Enterprise Dedicated Device Deployment

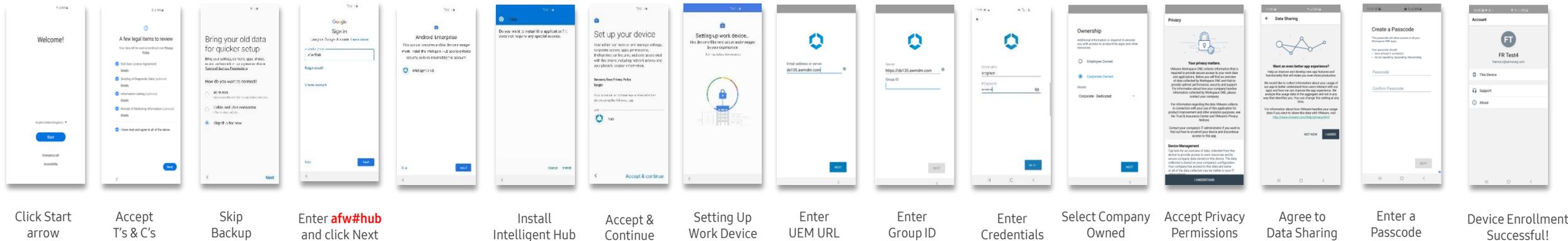
The Android Enterprise Dedicated Device deployment type has been integrated into the VMware Launcher profile. So you need to ensure that your Launcher profile has been created and assigned to your device prior to enrolling. You can create this profile by going to:

- *Devices -> Profiles & Resources -> Profiles -> ADD -> Android -> Launcher*

Once you have done this you then enroll your device. To enroll your device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 3 ways you can enroll your device into Workspace ONE UEM as an Android Enterprise Dedicated device.

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

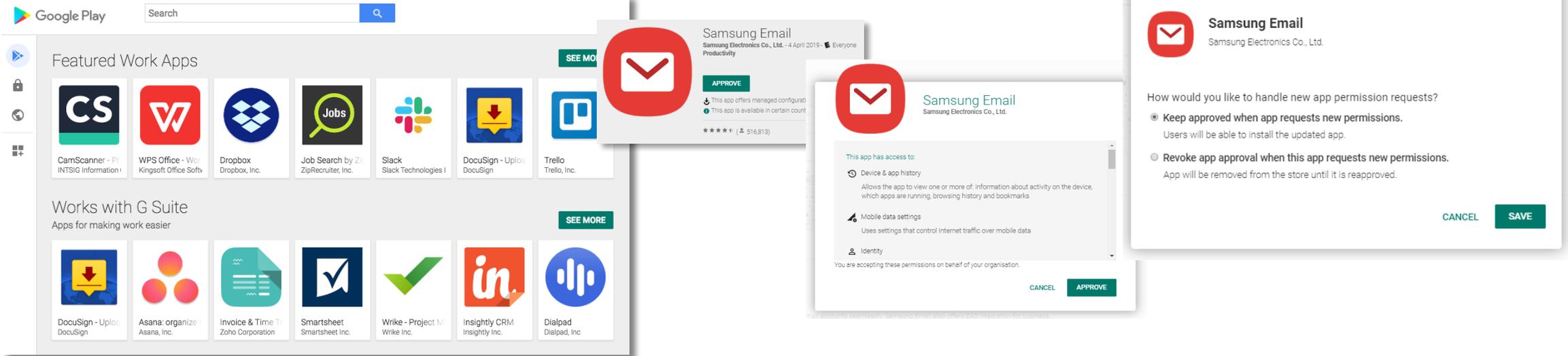
- Below is a screen-by-screen play to enroll your device using the DPC Identifier method.



## 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:

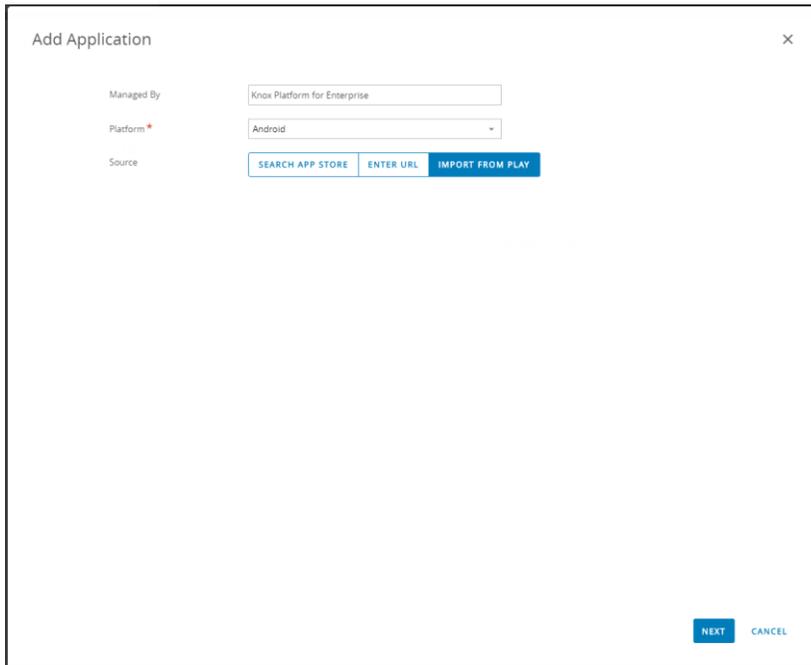
- Navigate to <https://play.google.com/work> and log in with the Gmail account you bound to Workspace ONE UEM in the Configuring Android Enterprise Section.
- Search for the App you want to distribute. For example; Samsung Email
- Click the APPROVE button.
- APPROVE the App Permission request
- Choose how you would like to handle new app permission requests and then click SAVE
- You will now see your app lists in your My managed apps page



## Managed Google Play Configuration

Now we have approved an application we would like to distribute in Workspace ONE UEM.

- Log in to your Workspace ONE UEM Console and navigate to the tenant you have configured Android Enterprise
- Navigate to **APPS & BOOKS -> Applications -> Native -> Public** and click ADD APPLICATION
- Select Android from the Platform drop down list
- Then select the IMPORT FROM PLAY option and click NEXT
- You should then see the Samsung Email app we approved in our Managed Google Play Store.
- Ensure the app is ticked and then click IMPORT.



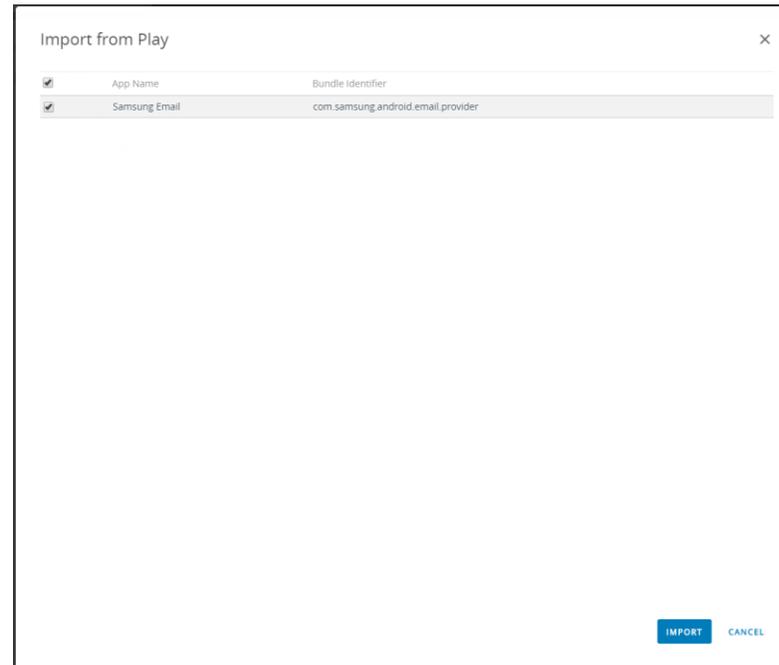
Add Application

Managed By: Knox Platform for Enterprise

Platform: Android

Source: SEARCH APP STORE | ENTER URL | **IMPORT FROM PLAY**

NEXT CANCEL



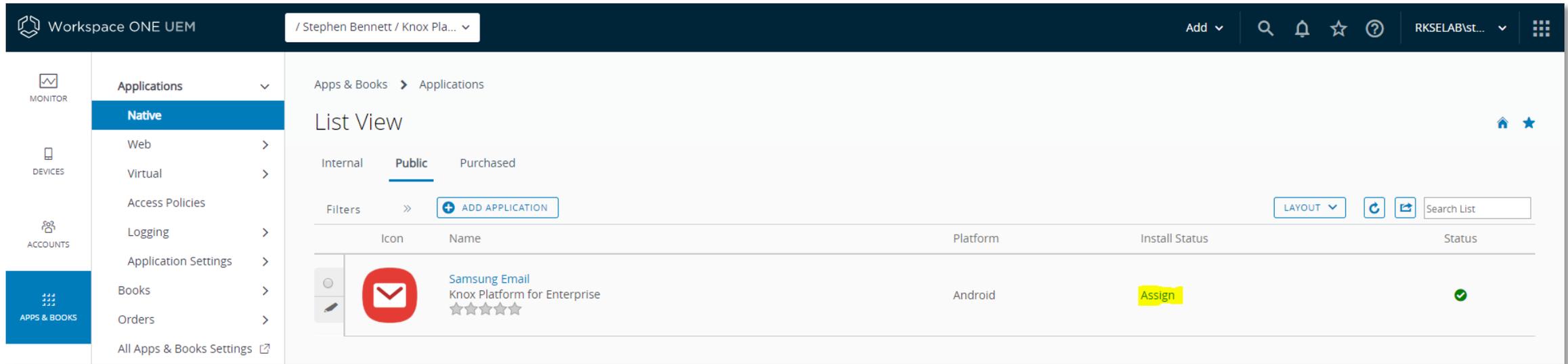
Import from Play

App Name	Bundle Identifier
<input checked="" type="checkbox"/> Samsung Email	com.samsung.android.email.provider

IMPORT CANCEL

## Managed Google Play Configuration

- You will now see the apps you approved imported into the Public list.
- Now we have imported the app, next we need to assign it to our users.
- Select the Assign button under the Install Status column for the app you wish to distribute.



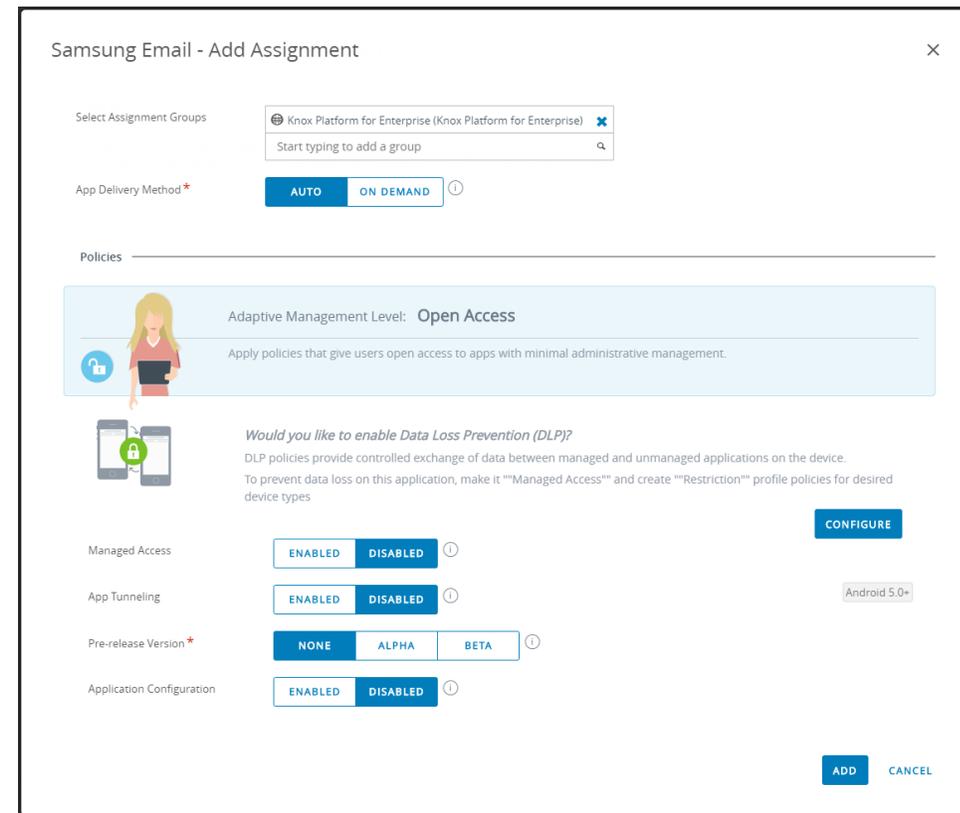
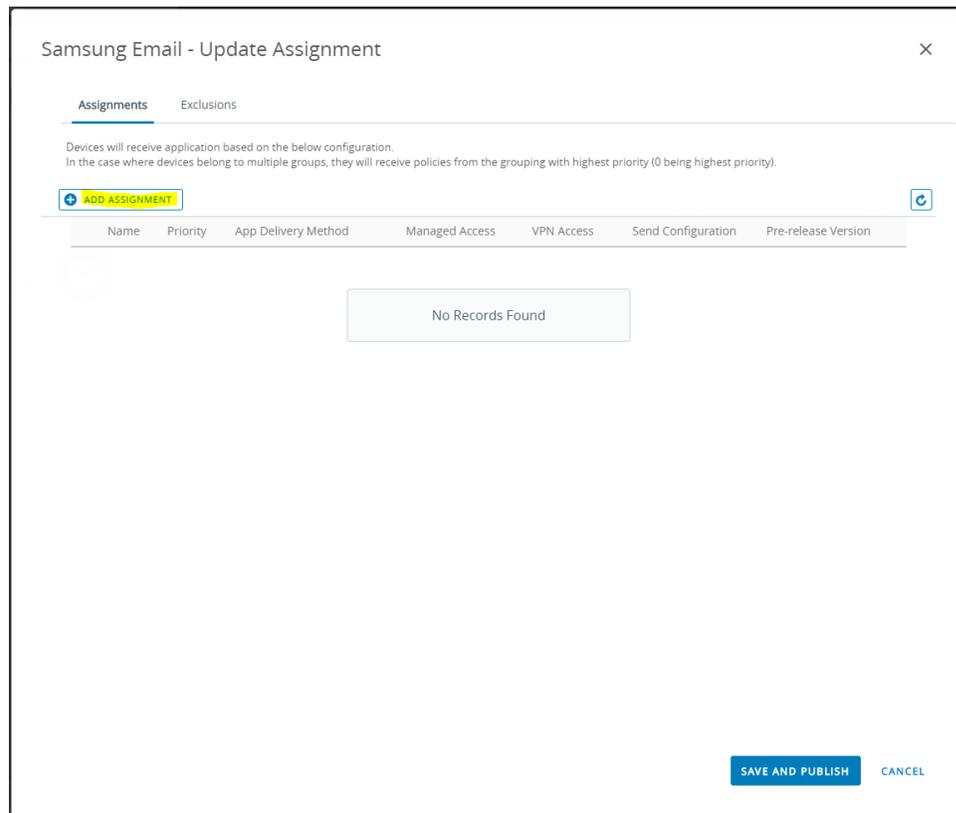
The screenshot shows the Workspace ONE UEM console interface. The top navigation bar includes the Workspace ONE UEM logo, a user profile dropdown for Stephen Bennett / Knox Pla..., and utility icons for Add, Search, Notifications, Favorites, Help, and a user-specific dropdown for RKSELAB\st... The left sidebar contains navigation categories: MONITOR, DEVICES, ACCOUNTS, and APPS & BOOKS. The 'APPS & BOOKS' section is expanded to show 'Applications' > 'Native'. The main content area displays a 'List View' of applications under the 'Public' tab. A table lists the applications with columns for Icon, Name, Platform, Install Status, and Status. The 'Samsung Email' app is listed with a red envelope icon, the name 'Samsung Email Knox Platform for Enterprise', a 5-star rating, and the platform 'Android'. The 'Install Status' column for this app contains a yellow 'Assign' button, and the 'Status' column shows a green checkmark.

Icon	Name	Platform	Install Status	Status
	Samsung Email Knox Platform for Enterprise ★★★★★	Android	Assign	✓

## Managed Google Play Configuration

- Select ADD ASSIGNMENT from the pop up window that appears
- Next select the Assignment groups you wish to distribute this app too, along with the delivery method.

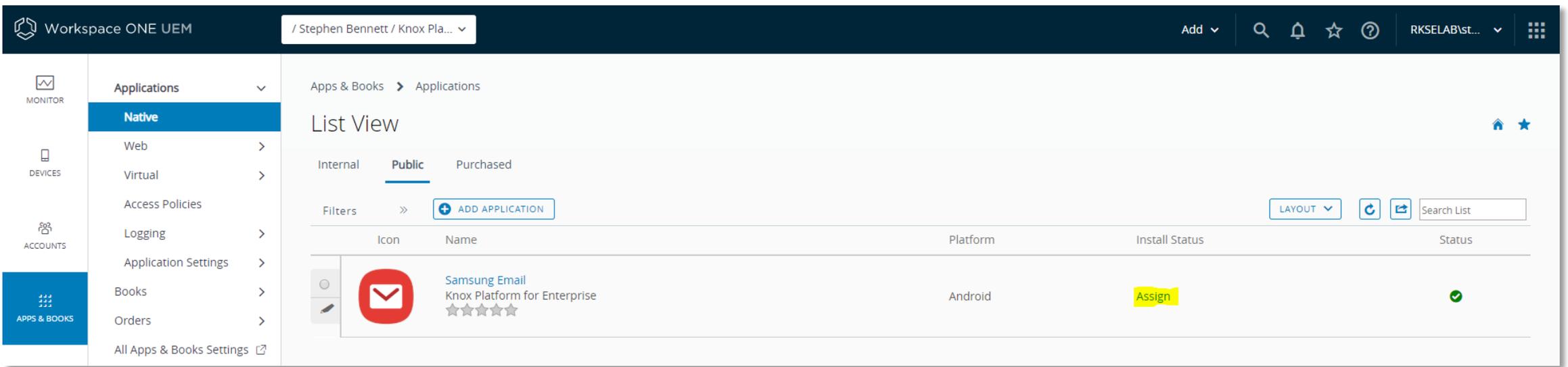
If you wish to send down an AppConfig profile along with your application, follow the instructions in the next section on how to do this. If you don't want to send down an AppConfig profile, or the app you are trying to deploy doesn't support AppConfig, simply click ADD to complete the deployment of your application.



## AppConfig

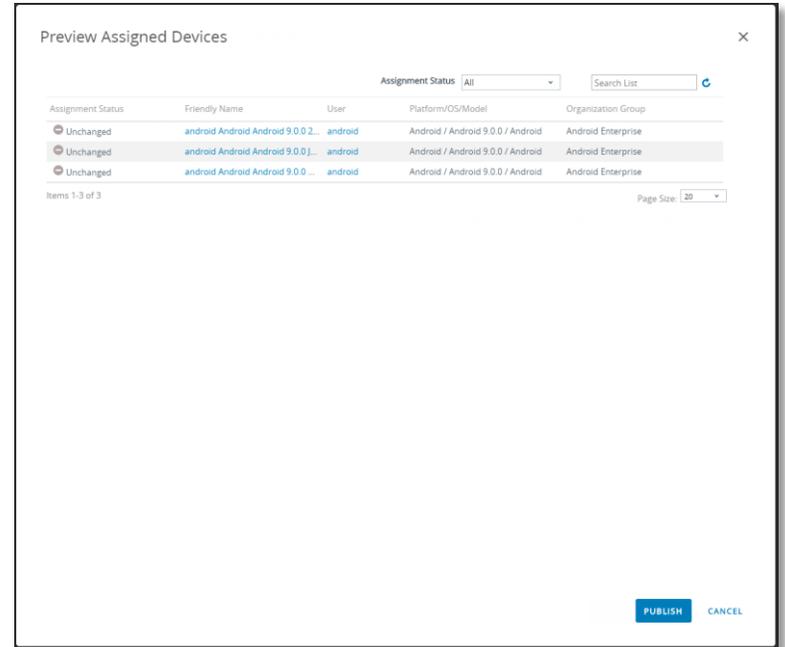
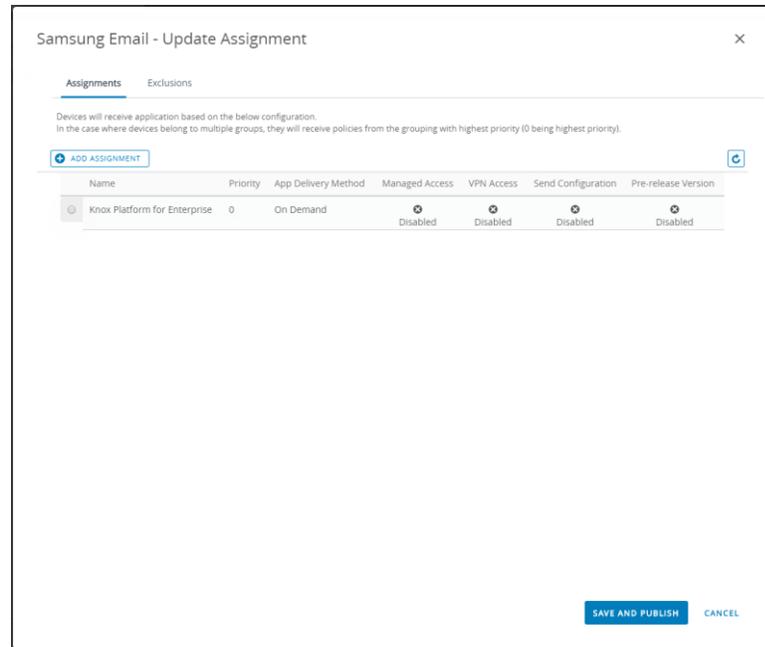
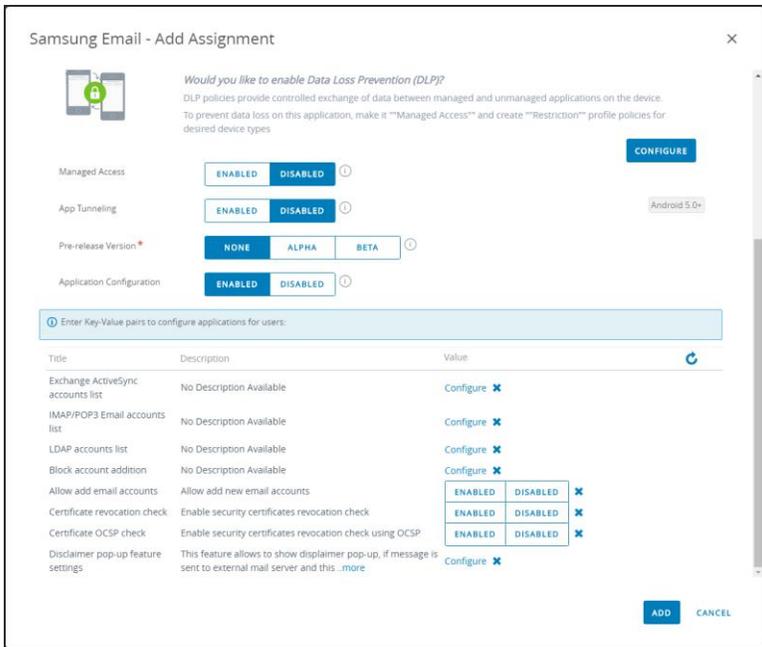
AppConfig enables you to send down application configuration profiles along with your managed apps when you distribute them through your Managed Google Play Store. This saves on having to have the UEM implement the required APIs for the app you are using so you can remotely configure it. To use AppConfig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

- Navigate to **Apps & Books -> Applications -> Native -> Public** and assign an app to the group you wish.



## AppConfig

- Before hitting the ADD button, scroll down to the Application Configuration section and select ENABLED. If the app has been developed in accordance to the AppConfig community, then you will see a list of variables you can configure below. Like in the below screenshot for the Samsung Native Email client.
- Configure the various options you wish and then when you are finished, click the ADD button.
- Confirm the assignment by clicking SAVE AND PUBLISH and then PUBLISH on the final screen. You have now used AppConfig to distribute a Managed Play app with a config profile.



## 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 some special options such as Dual DAR]

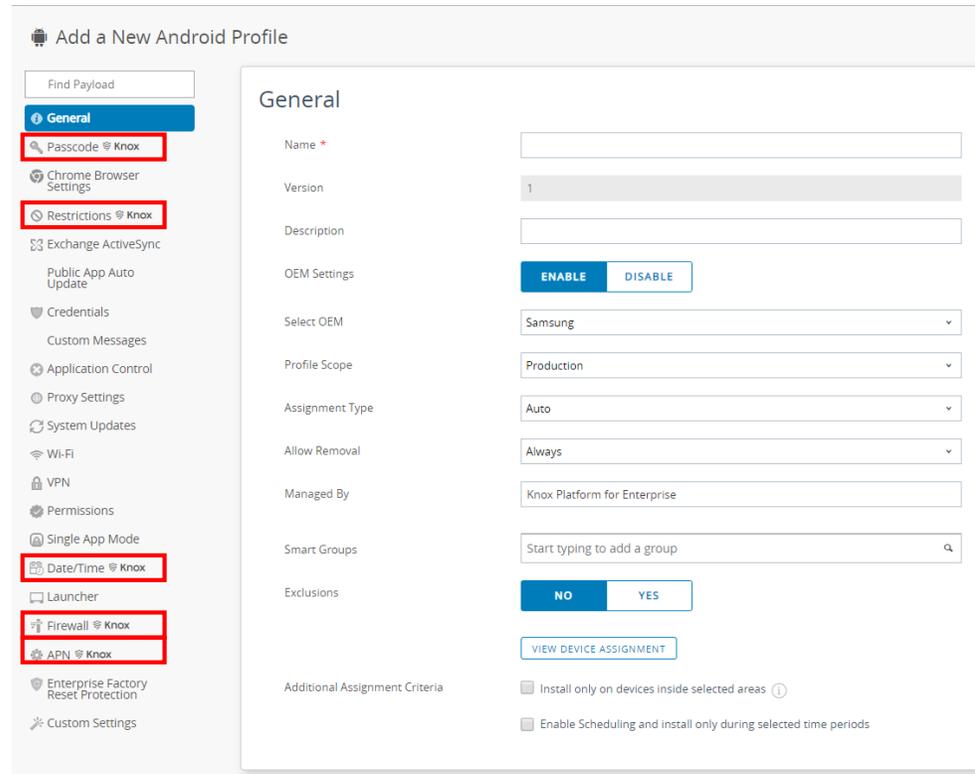
Knox Platform for Enterprise : Standard Edition offers free additional policies you can use to provide enhanced security, manageability and usability over your Samsung device fleet, running Android Enterprise 8 or above.



## Configure KPE : Standard Edition on VMware Workspace ONE UEM

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

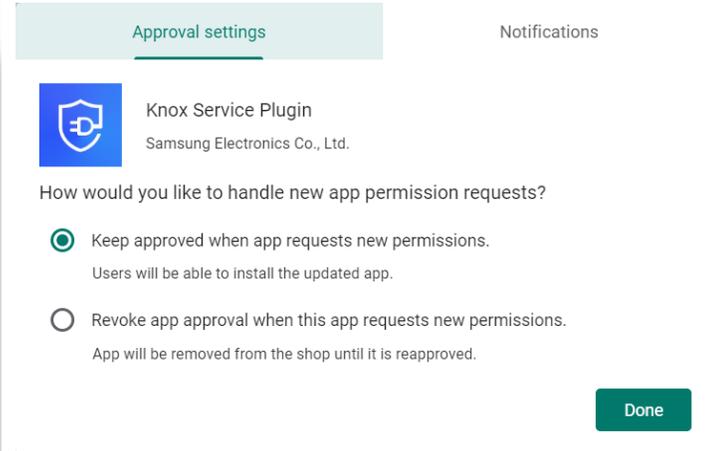
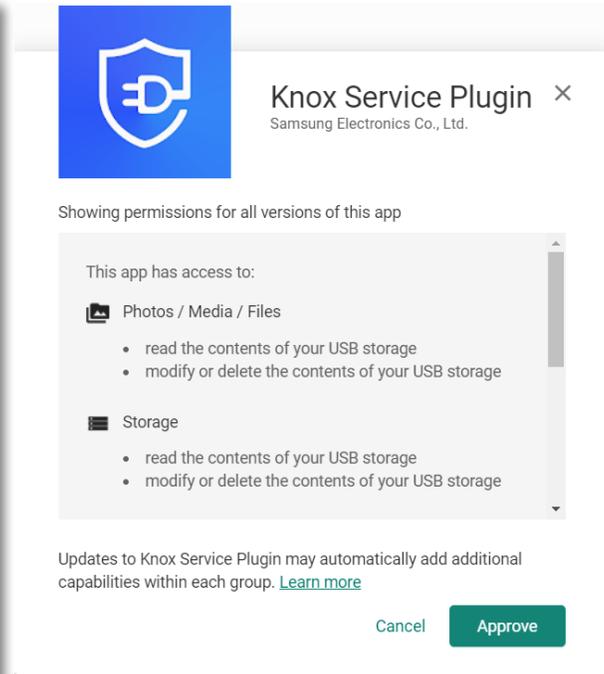
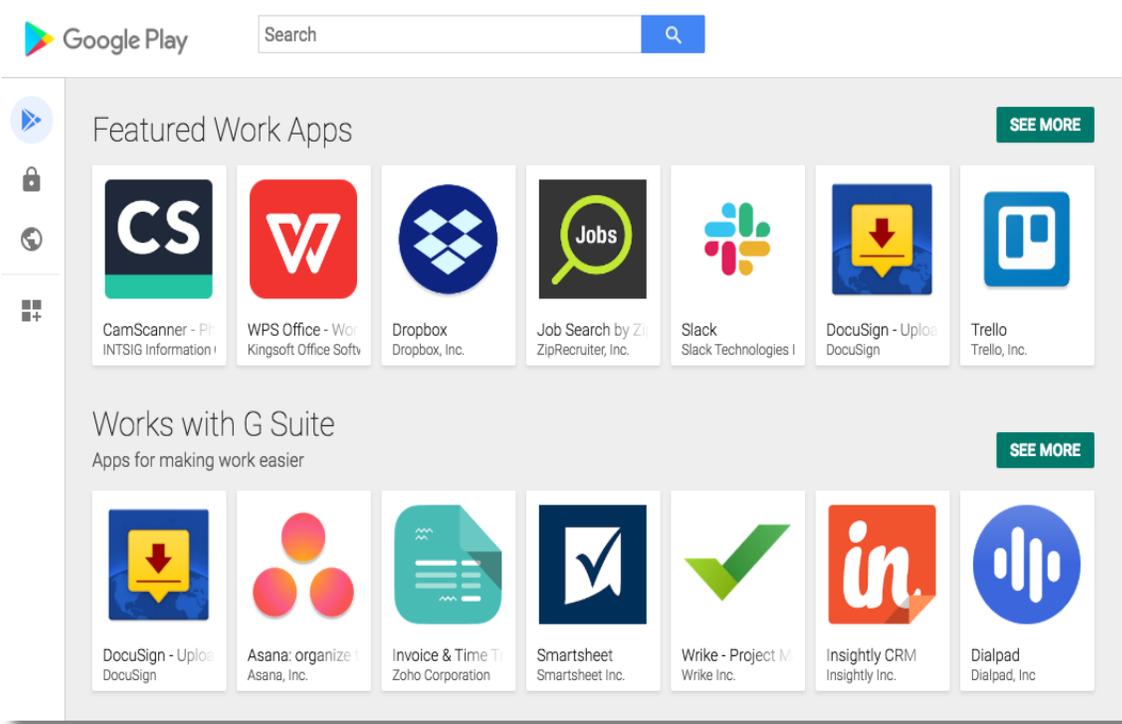
- Navigate to **Devices -> Profiles & Resources -> Profiles**
- Select **Add -> Add Profile -> Android**
- On the General payload screen, select the **ENABLE** button for OEM Settings, then select Samsung from the drop down
- You have now enabled all the additional KPE Standard APIs available to you in your payload. These have been highlighted for you using the Samsung Knox logo. You are now free to select those payloads and take advantage of the free additional APIs found in KPE Standard Edition!



Note: When you apply a KPE Standard Policy to your device, you will notice the Android Enterprise briefcase icon change to a Knox Shield. This is how you will know you are now using Knox Platform for Enterprise.

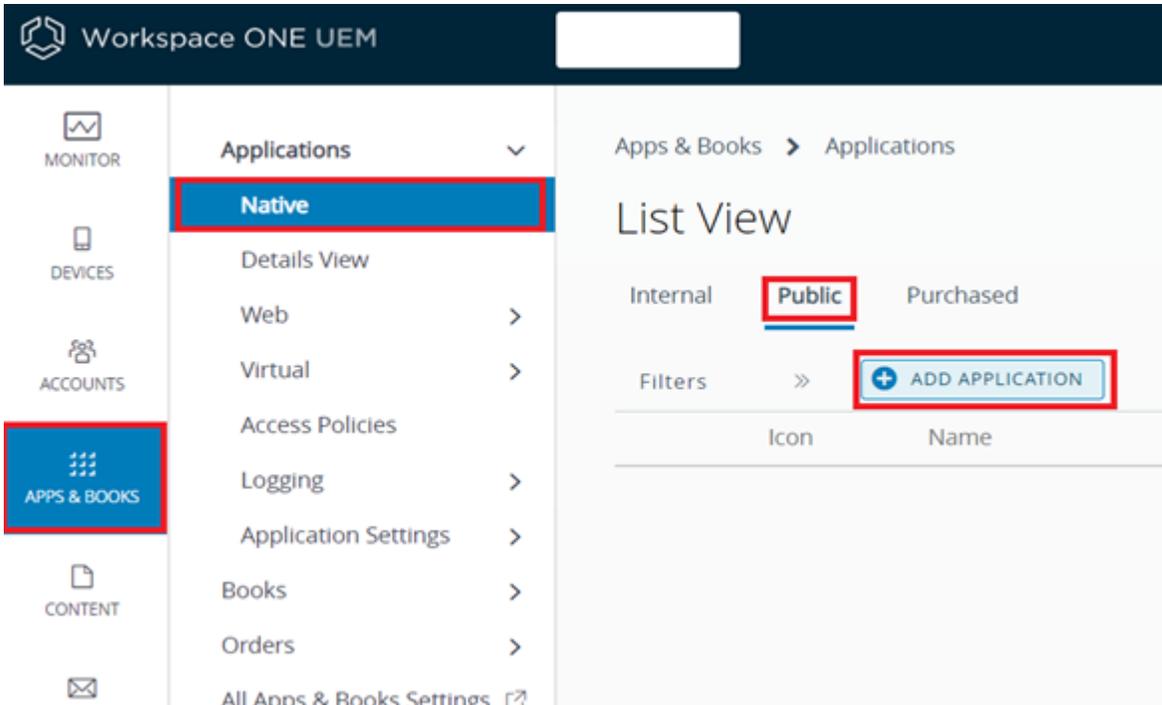
# Knox Service Plugin [KSP]

- Navigate to: [https://play.google.com/work?hl=en\\_GB](https://play.google.com/work?hl=en_GB)
- Search for and approve the Knox Service Plugin Application.
- Choose how you would like to handle new app permission requests and then click Done.
- You will now see KSP in your My managed apps page



# Knox Service Plugin [KSP]

- In the Workspace One UEM console, navigate to: Apps and Books > Applications > Native
- Select Public and then Add Application
- In the Add Application window, select the platform as “Android” and then the source to “Import from Play”.
- Select Next and then Import.



## Add Application

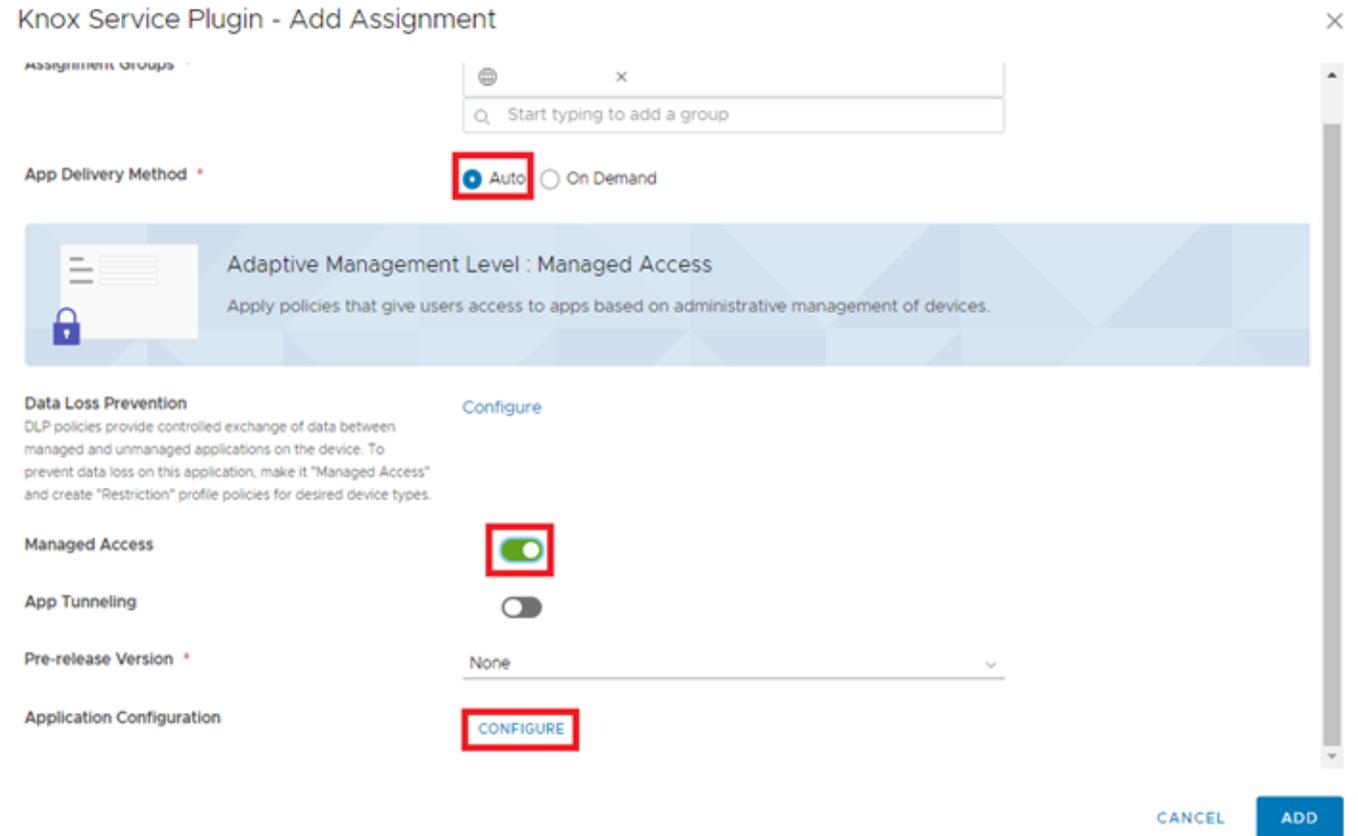
Managed By

Platform \*

Source

# Knox Platform for Enterprise : Premium Edition

- In the application list, find the Knox Service Plugin and select assign.
- Select Add Assignment and select your chosen assignment group.
- Set the App Delivery Method to Auto.
- Turn on Managed Access.
- Select Configure next to Application Configuration.



- Enter a profile name of your choice.
- Copy and Paste your KPE Premium License Key from your Samsung Knox Portal.
- To configure the KPE premium settings, scroll down and select configure against the desired configuration option.
- Select Add and then Save.

## Knox Service Plugin - Application Configuration

Profile name	Knox profile		
KPE Premium License key	KLMII-AVFVP		
Debug Mode	Disable		
Device-wide policies (Device Owner)	<b>CONFIGURE</b>		

DEX policy, VPN policy (Premium), Firewall and Proxy policy, Call and Messaging control, Device Restrictions, Advanced Restriction policies (Premium), Firmware update (FOTA) policy, Device Settings (Premium), Password Policy, Application management policies, Device Admin whitelisting, Device customization controls (Premium), Device Controls, Device Key Mapping (Premium), Enterprise Billing policy (Premium), Universal Credential Manager policy (Premium), Certificate management policies (Premium), Network Platform Analytics (NPA) (Premium), Audit Log (Premium), Date Time Change, Device

CANCEL SAVE

## Device-wide policies (Device Owner)

### < APPLICATION CONFIGURATION

> Device Restrictions

▼ Advanced Restriction policies (Premium)

Enable Advanced Restrictions controls	Disable	
Allow wi-fi scanning	Enable	
Allow bluetooth scanning	Enable	
Allow remote control	Enable	
Enable Common Criteria (CC) mode	Select	
	Enable	
	Disable	
Allow dual SIM operation	Enable	

ADD

- Select Add.
- Select Save and Publish.
- Review the list of assigned devices/users and select Publish.

Knox Service Plugin - Edit assignment

Management Group:

App Delivery Method:  Auto  On Demand

Adaptive Management Level: Managed Access  
Apply policies that give users access to apps based on administrative management of devices.

Data Loss Prevention:  Configure  
DLP policies provide controlled exchange of data between managed and unmanaged applications on the device. To prevent data loss on this application, make it "Managed Access" and create "Restriction" profile policies for desired device types.

Managed Access:

App Tunneling:

Pre-release Version: None

Application Configuration:

Knox Service Plugin - Update Assignment

Assignments Exclusions

Devices will receive application based on the below configuration. In the case where devices belong to multiple groups, they will receive policies from the grouping with highest priority (0 being highest priority).

	Name	Priority	App Delivery Method	Managed Access	VPN Access	Send Configuration	Pre-release Version
<input type="checkbox"/>	▼	0	On Demand	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled

Knox Service Plugin - Preview Assigned Devices

Assignment Status: All Search List

Assignment Status	Friendly Name	User	Platform	Organization Group
Added				

Page Size: 20 Items 1 - 1 of 1

# Document Information

This is version 2.2 of this document.

**Thank you!**

