

VMware Workspace ONE UEM 1907 & Knox Platform for Enterprise

May 2020
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
 - 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

Knowledge Base:

<https://support.air-watch.com/>

<https://air-watch.com/>

<https://www.air-watch.com/en/resources/webinars/>

VMWare AirWatch Solution:

<https://www.youtube.com/channel/UCZTvfJMhQ5Oc5TFw465tcJQ>

Trial Access:

<https://www.air-watch.com/lp/free-trial/>

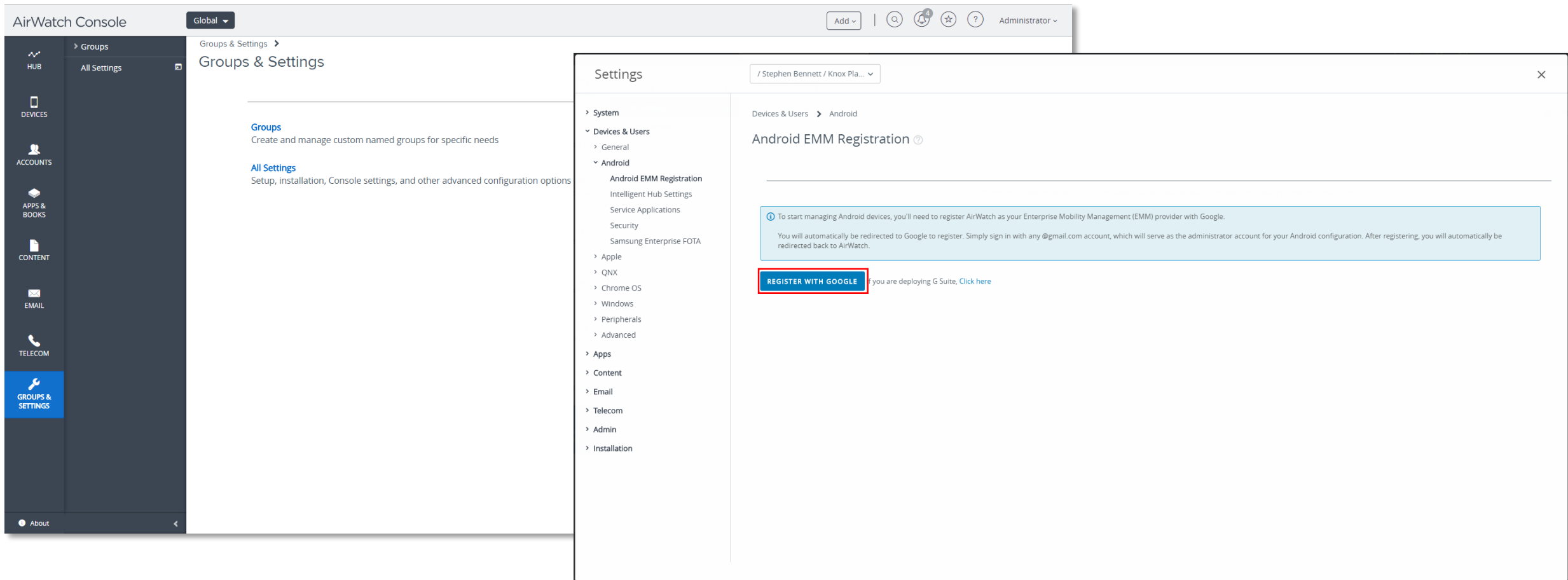
Pre-Requisites for Knox Platform for Enterprise

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

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.

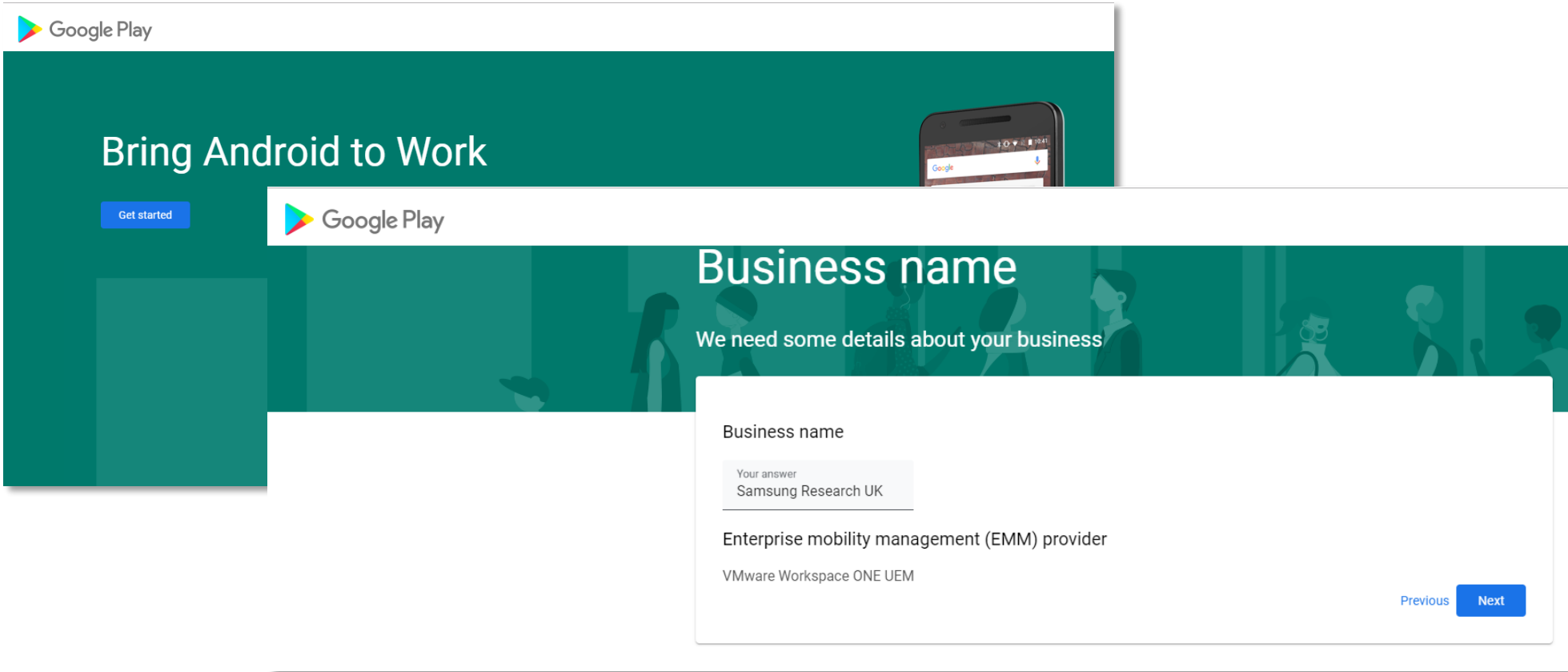


The screenshot displays the AirWatch Console interface. On the left is a dark sidebar with navigation icons for HUB, DEVICES, ACCOUNTS, APPS & BOOKS, CONTENT, EMAIL, TELECOM, and GROUPS & SETTINGS (highlighted in blue). The main area is titled 'Groups & Settings' and contains two sections: 'Groups' (Create and manage custom named groups for specific needs) and 'All Settings' (Setup, installation, Console settings, and other advanced configuration options). A 'Settings' modal window is open, showing a left-hand menu with categories like System, Devices & Users, and Apps. Under 'Devices & Users', the 'Android' section is expanded, listing 'Android EMM Registration' as the first item. The main content of the modal is titled 'Android EMM Registration' and includes an information box stating: '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 button labeled 'REGISTER WITH GOOGLE' with a red rectangular highlight. To the right of the button is a link: 'If you are deploying G Suite, [Click here](#)'.

Configure Android Enterprise

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.



Google Play

Bring Android to Work

Get started

Google Play

Business name

We need some details about your business

Business name

Your answer
Samsung Research UK

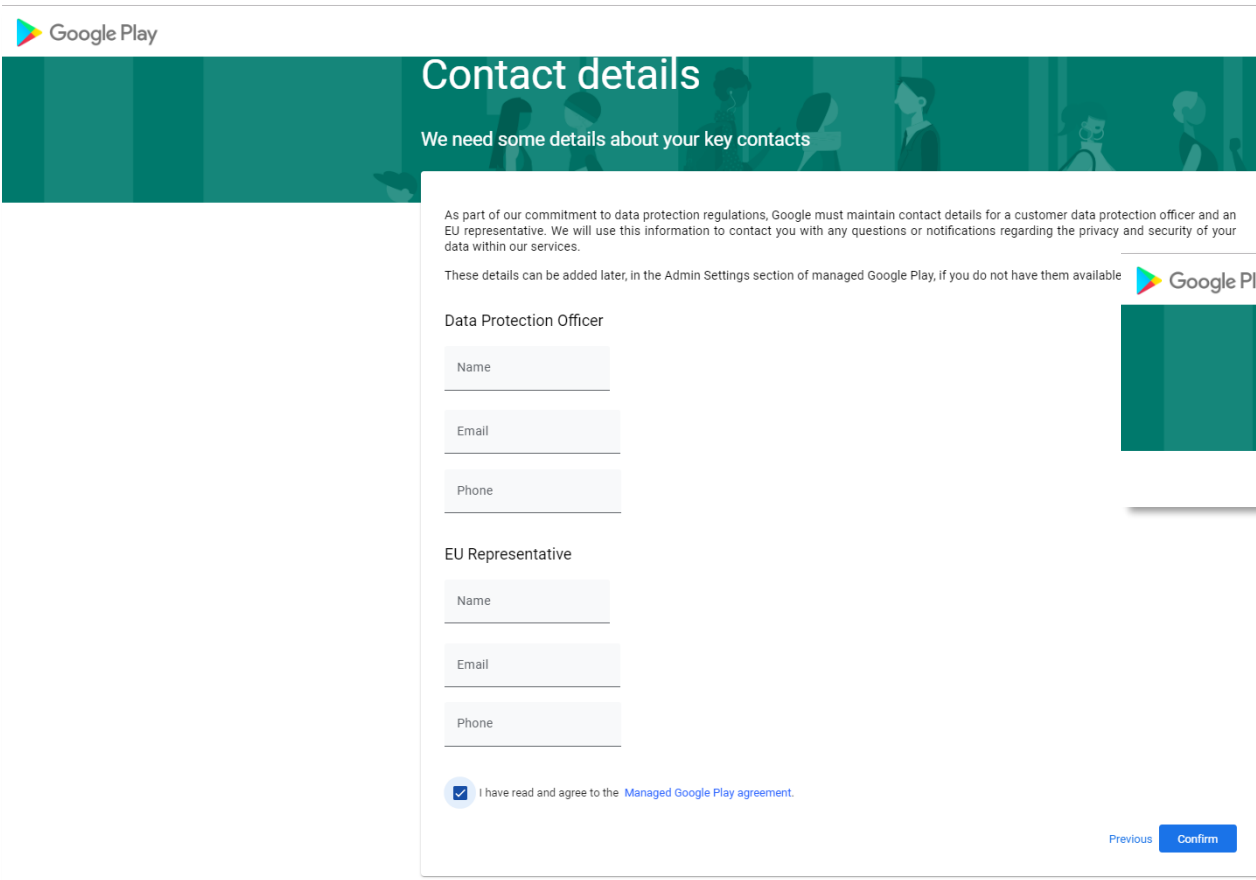
Enterprise mobility management (EMM) provider

VMware Workspace ONE UEM

Previous Next

Configure Android Enterprise

- Fill out the Contact details page, tick the Managed Google Play agreement page and then select Confirm. These text fields are not mandatory, so you can alternatively leave them blank and just tick the Managed Google Play agreement and then select Confirm.
- Click Complete Registration 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

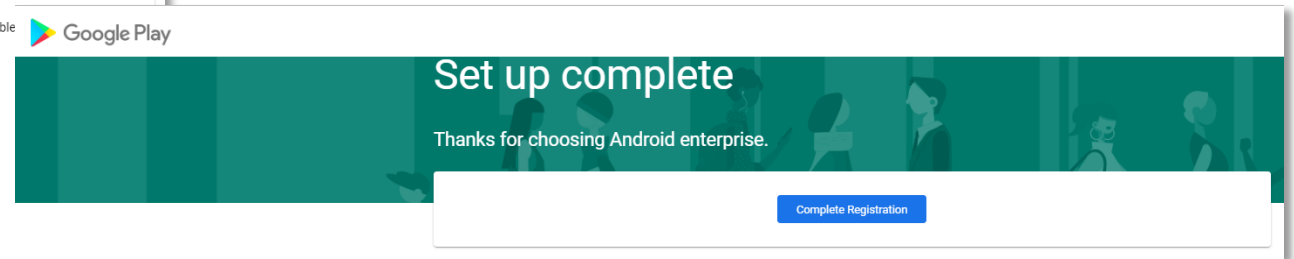
Name

Email

Phone

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

[Previous](#) [Confirm](#)



Google Play

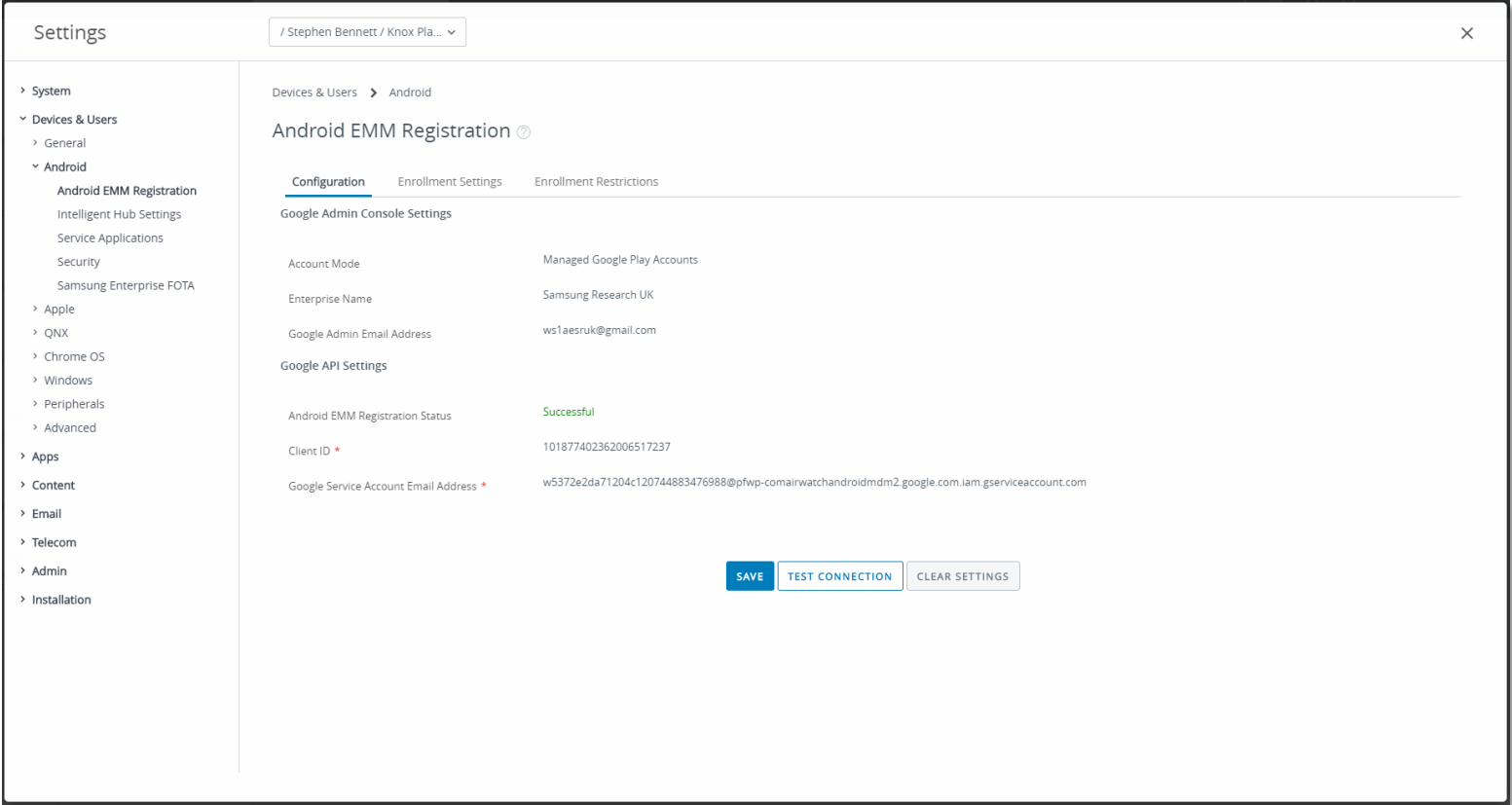
Set up complete

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.



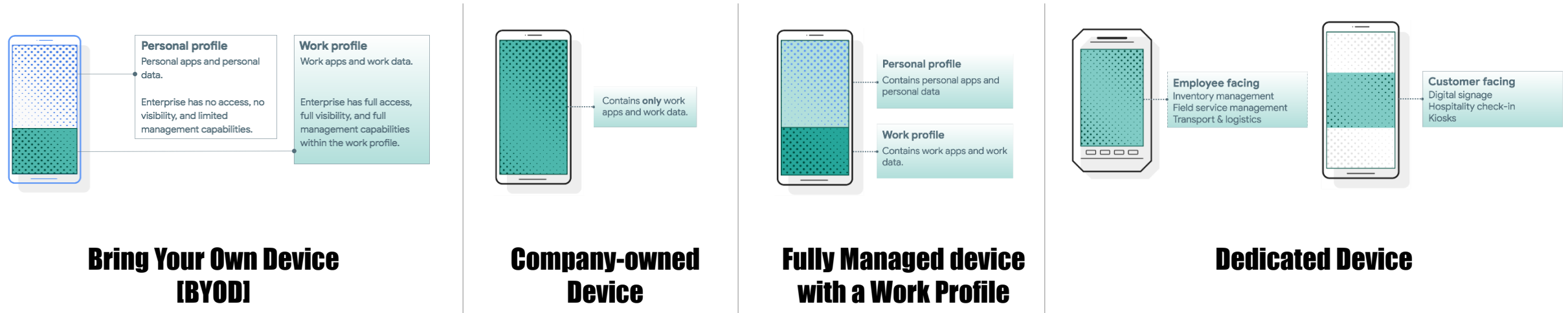
Android Enterprise Deployment Modes

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*]

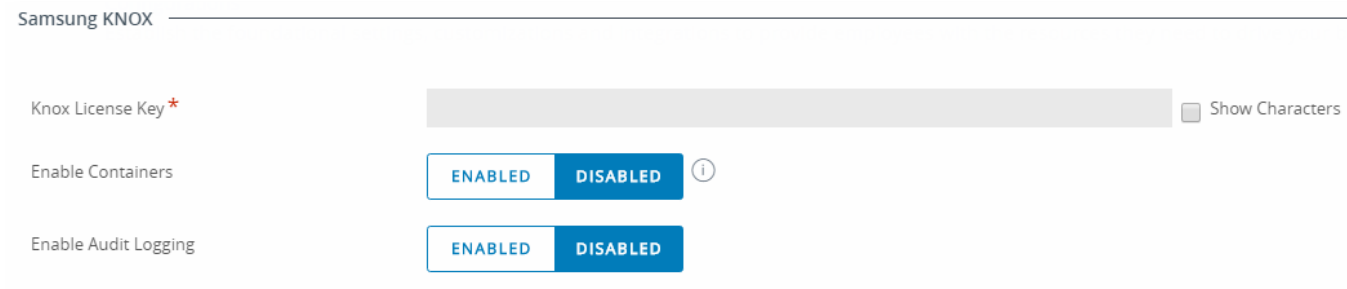
VMware Workspace ONE UEM can support **all** 4 of these deployment modes. In this next section we will show you how to configure each of these 4 deployment modes in VMware Workspace ONE UEM for your device fleet.



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.



Samsung KNOX

Knox License Key * ☐ Show Characters

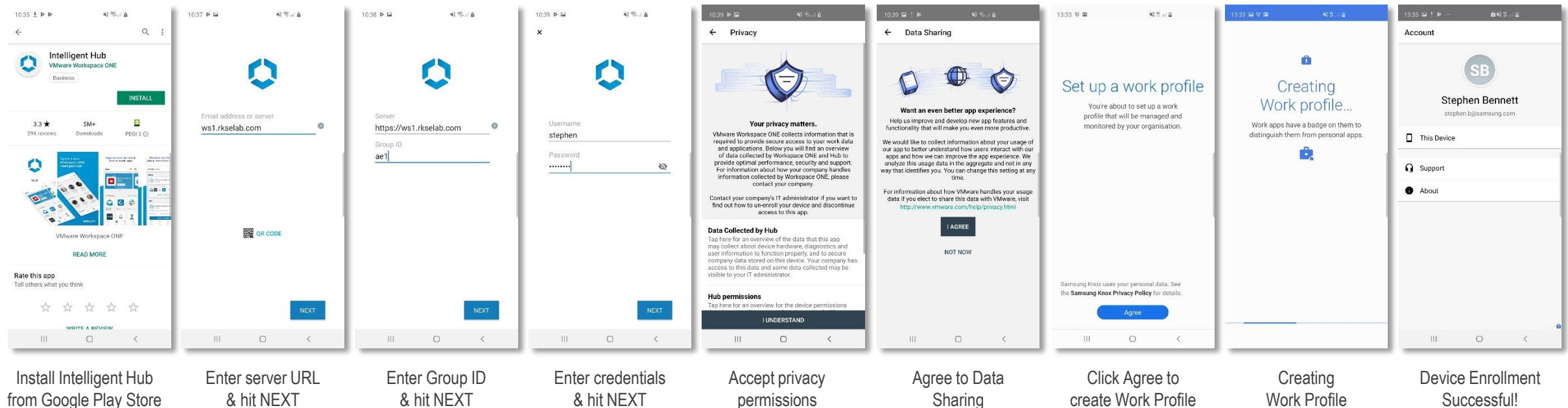
Enable Containers ENABLED DISABLED ⓘ

Enable Audit Logging ENABLED DISABLED

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.



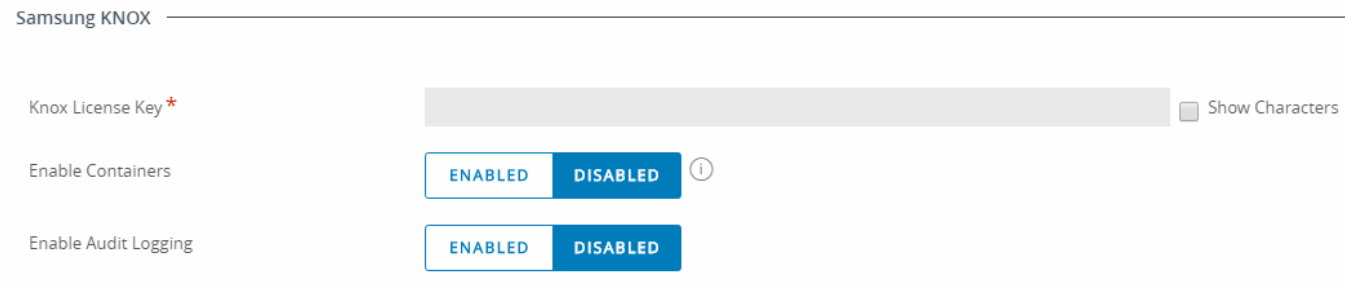
*You can also enroll your device using the alternative Workspace ONE UEM methods. For example QR Code.

**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.



Samsung KNOX

Knox License Key ^{*} ☐ Show Characters

Enable Containers ENABLED DISABLED ⓘ

Enable Audit Logging ENABLED DISABLED

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**.

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

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.

SAVE

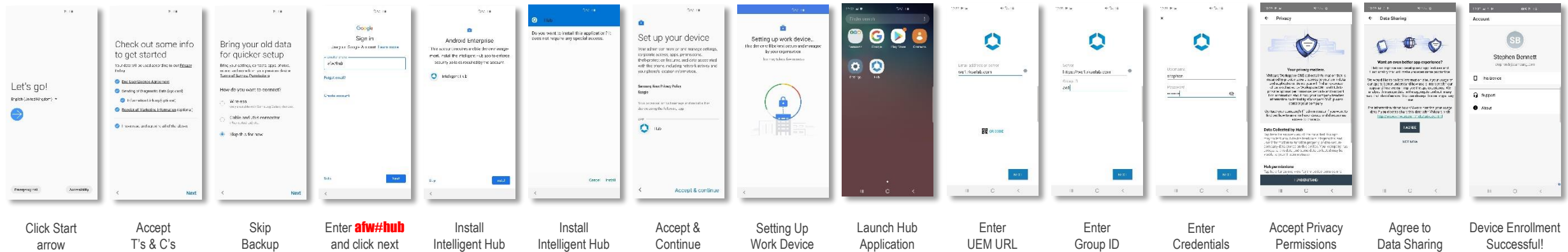
Android Enterprise: Company-owned Device

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 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

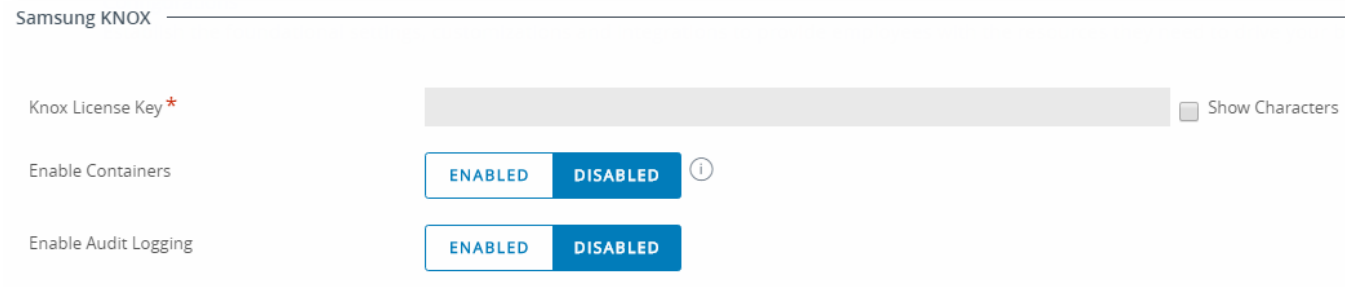
- Below is a screen-by-screen play to enroll your device using the DPC Identifier method.



Android Enterprise Fully Managed Device with a Work Profile Deployment

To enroll a device in the Android Enterprise Fully Managed Device with a Work Profile 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 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 **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

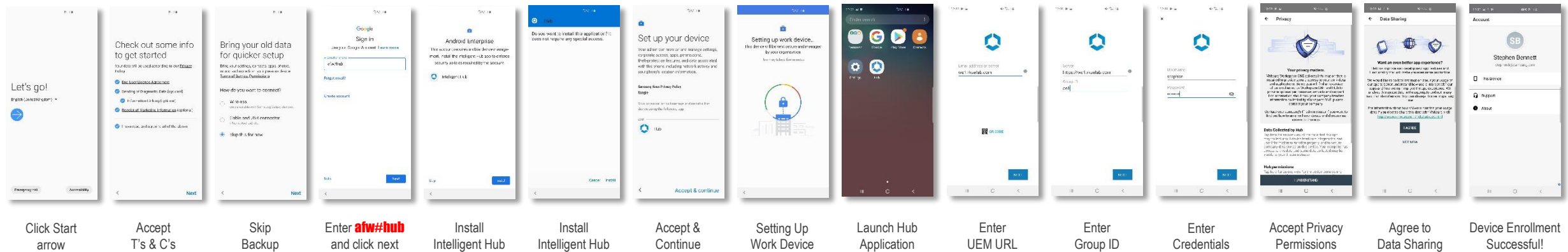
Android Enterprise: Fully Managed Device with a Work Profile

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 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

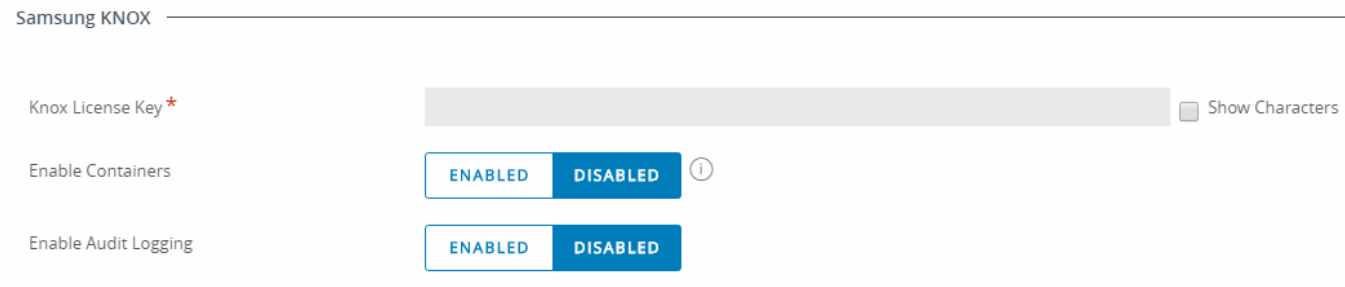
- Below is a screen-by-screen play to enroll your device using the DPC Identifier method.



Android Enterprise 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

?

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 generated Google account on the device is unique to each device enrolled by the same enrollment user. Ideal for staging and single-use scenarios.

Fully-Managed Device Enrollments *


WORK MANAGED DEVICE

CORPORATE OWNED PERSONALLY ENABLED

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.

SAVE

19



Android Enterprise Dedicated Device Deployment

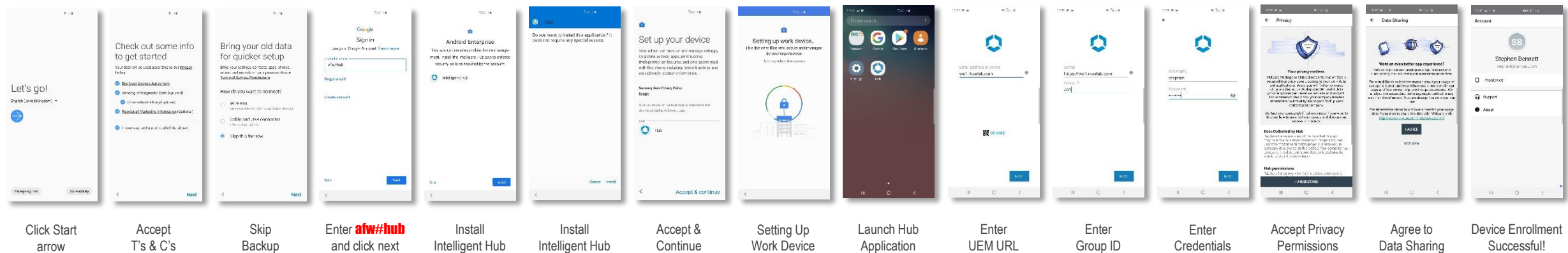
The Android Enterprise Dedicated Device deployment type has been integrated into the VMware Launcher profile. So you need to ensure that your Launcher profile has been created and assigned to your device prior to enrolling. You can create this profile by going to:

- *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

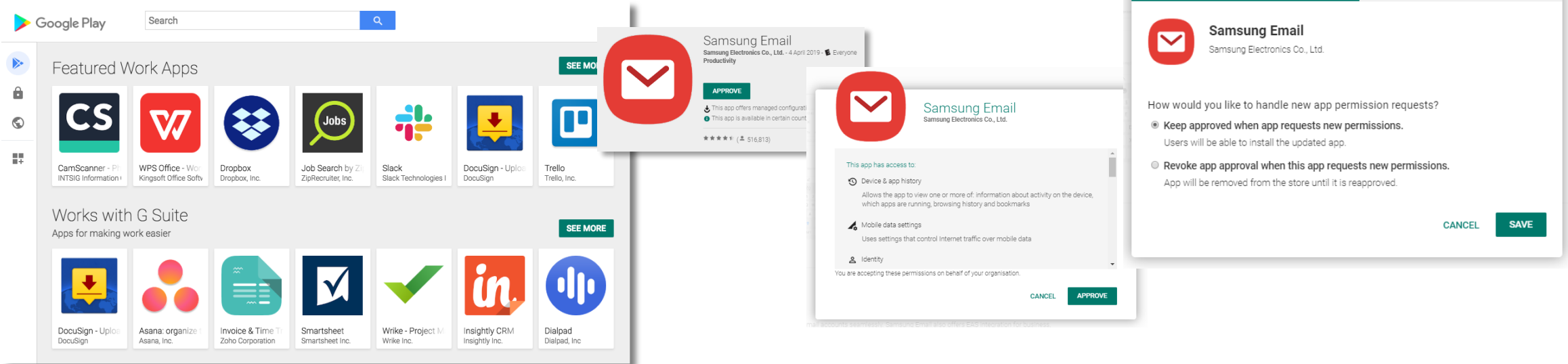
- Below is a screen-by-screen play to enroll your device using the DPC Identifier method.



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:

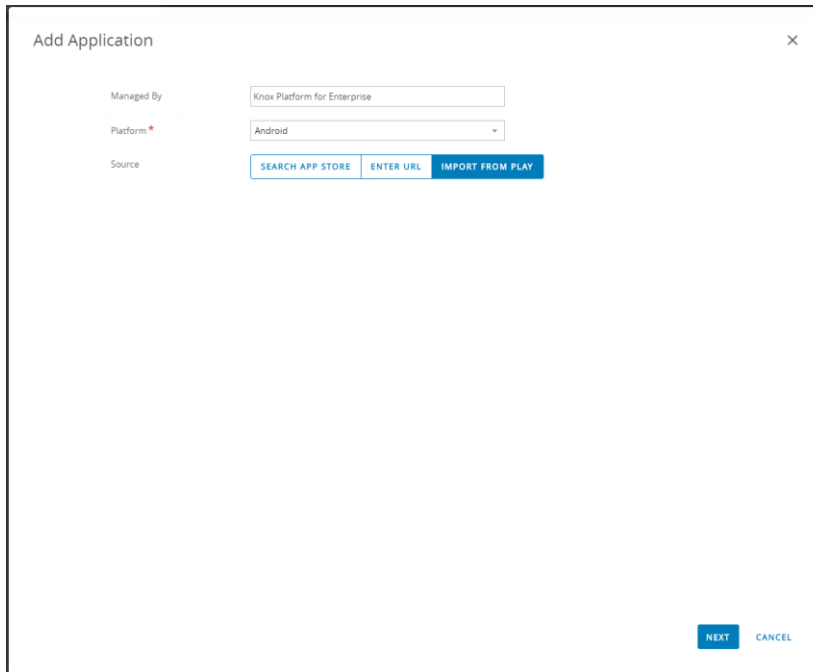
- Navigate to <https://play.google.com/work> and log in with the Gmail account you bound to Workspace ONE UEM in the Configuring Android Enterprise Section.
- Search for the App you want to distribute. For example; Samsung Email
- Click the APPROVE button.
- APPROVE the App Permission request
- Choose 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



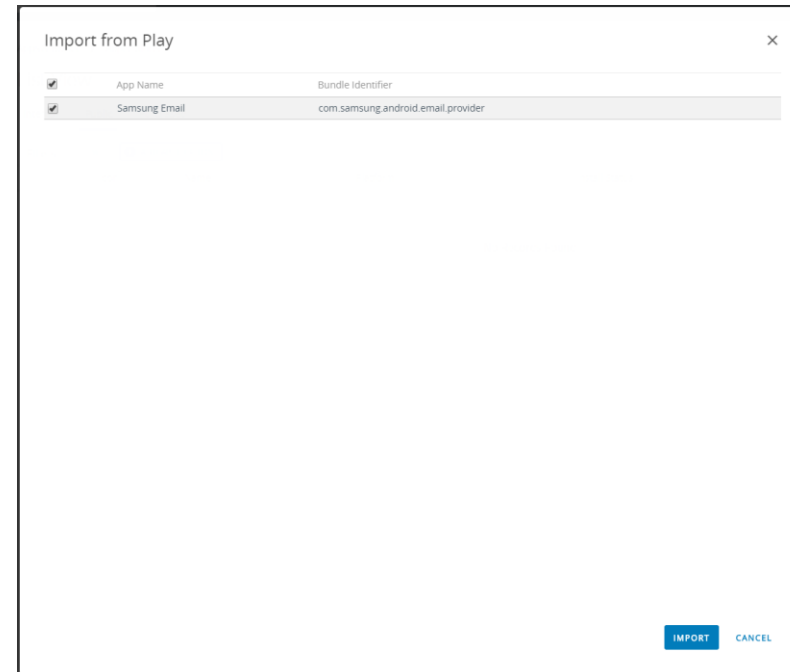
Managed Google Play Configuration

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.



The 'Add Application' dialog box shows the configuration for adding a new application. It includes fields for 'Managed By' (Knox Platform for Enterprise), 'Platform' (Android), and 'Source' (SEARCH APP STORE, ENTER URL, IMPORT FROM PLAY). The 'IMPORT FROM PLAY' button is highlighted in blue. At the bottom right, there are 'NEXT' and 'CANCEL' buttons.

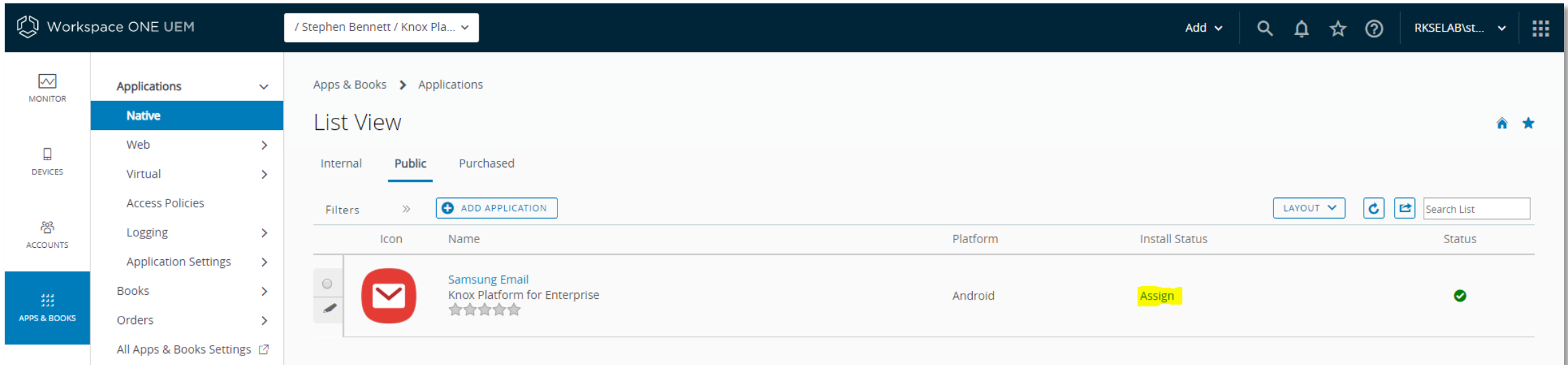


The 'Import from Play' dialog box displays a table of applications available for import. The 'Samsung Email' app is selected with a checkmark. At the bottom right, there are 'IMPORT' and 'CANCEL' buttons.

App Name	Bundle Identifier
Samsung Email	com.samsung.android.email.provider

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 displays 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 various utility icons (Add, Search, Notifications, Favorites, Help) along with a dropdown menu for RKSELAB\st... and a grid icon.

The left sidebar contains navigation options: MONITOR, DEVICES, ACCOUNTS, and APPS & BOOKS (highlighted). Under APPS & BOOKS, the 'Applications' menu is expanded, showing options like Native (selected), Web, Virtual, Access Policies, Logging, Application Settings, Books, Orders, and All Apps & Books Settings.

The main content area shows the 'List View' of applications under the 'Public' category. The breadcrumb path is 'Apps & Books > Applications'. The view includes tabs for Internal, Public (selected), and Purchased. A 'Filters' section with an 'ADD APPLICATION' button is present. The application list table has columns for Icon, Name, Platform, Install Status, and Status.

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.

Samsung Email - Update Assignment

×

AssignmentsExclusions

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).

+

ADD ASSIGNMENT

+

Name	Priority	App Delivery Method	Managed Access	VPN Access	Send Configuration	Pre-release Version
No Records Found						

SAVE AND PUBLISH

CANCEL

Samsung Email - Add Assignment

×

Select Assignment Groups

Knox Platform for Enterprise (Knox Platform for Enterprise)

Start typing to add a group


App Delivery Method*

AUTO

ON DEMAND


1

Policies



Adaptive Management Level: Open Access

Apply policies that give users open access to apps with minimal administrative management.



Would you like to enable Data Loss Prevention (DLP)?
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

CONFIGURE

Managed Access

ENABLED

DISABLED

1

App Tunneling

ENABLED

DISABLED

1

Android 5.0+

Pre-release Version*

NONE

ALPHA

BETA

1

Application Configuration

ENABLED

DISABLED

1

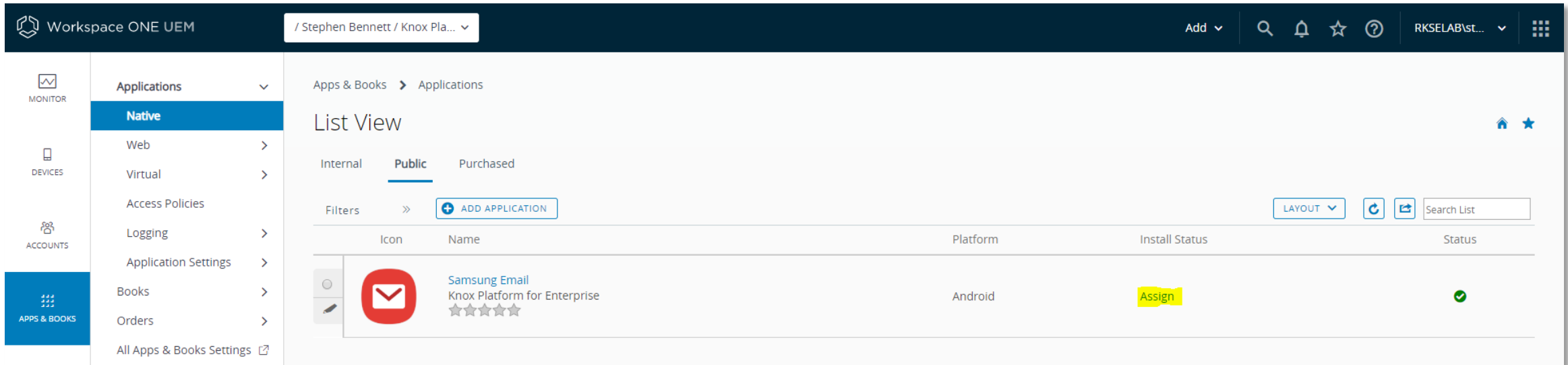
ADD

CANCEL


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.

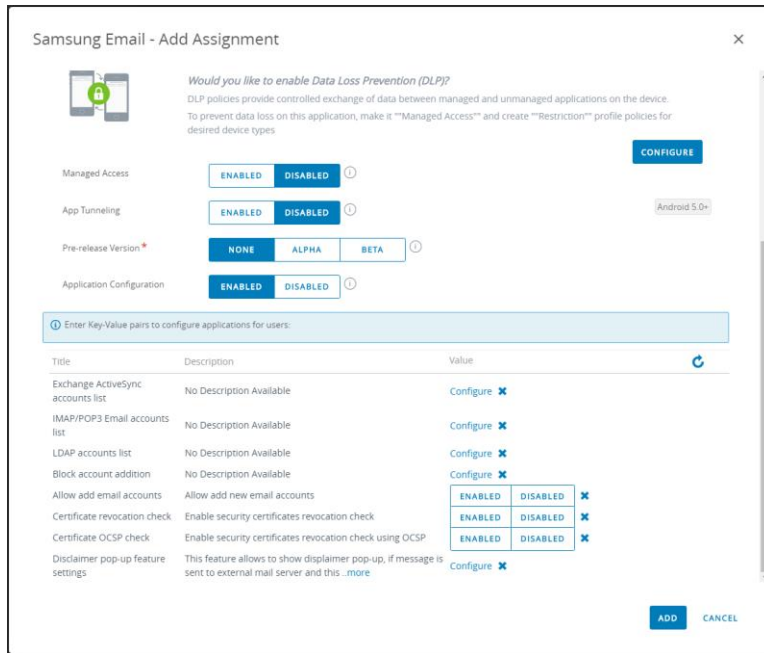


The screenshot shows the Workspace ONE UEM console interface. The left sidebar contains navigation options: MONITOR, DEVICES, ACCOUNTS, and APPS & BOOKS. The APPS & BOOKS section is expanded, showing a list of categories: Applications, Native, Web, Virtual, Access Policies, Logging, Application Settings, Books, Orders, and All Apps & Books Settings. The main content area displays the 'List View' for 'Public' applications. A table lists the applications, with the first entry being 'Samsung Email' (Knox Platform for Enterprise) for the 'Android' platform. The 'Install Status' column shows 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	✓

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.



Samsung Email - Add Assignment

Would you like to enable Data Loss Prevention (DLP)?
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: **ENABLED** **DISABLED** ⓘ

App Tunneling: **ENABLED** **DISABLED** ⓘ

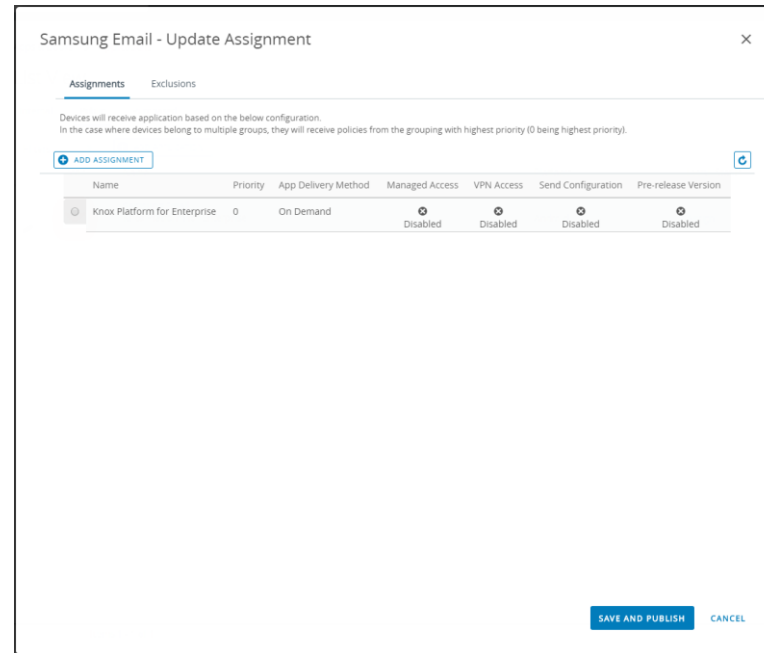
Pre-release Version: **NONE** **ALPHA** **BETA** ⓘ

Application Configuration: **ENABLED** **DISABLED** ⓘ

Enter Key-Value pairs to configure applications for users:

Title	Description	Value
Exchange ActiveSync accounts list	No Description Available	Configure ⓘ
IMAP/POP3 Email accounts list	No Description Available	Configure ⓘ
LDAP accounts list	No Description Available	Configure ⓘ
Block account addition	No Description Available	Configure ⓘ
Allow add email accounts	Allow add new email accounts	ENABLED DISABLED ⓘ
Certificate revocation check	Enable security certificates revocation check	ENABLED DISABLED ⓘ
Certificate OCSP check	Enable security certificates revocation check using OCSP	ENABLED DISABLED ⓘ
Disclaimer pop-up feature settings	This feature allows to show disclaimer pop-up, if message is sent to external mail server and this ...more	Configure ⓘ

ADD **CANCEL**



Samsung Email - Update Assignment

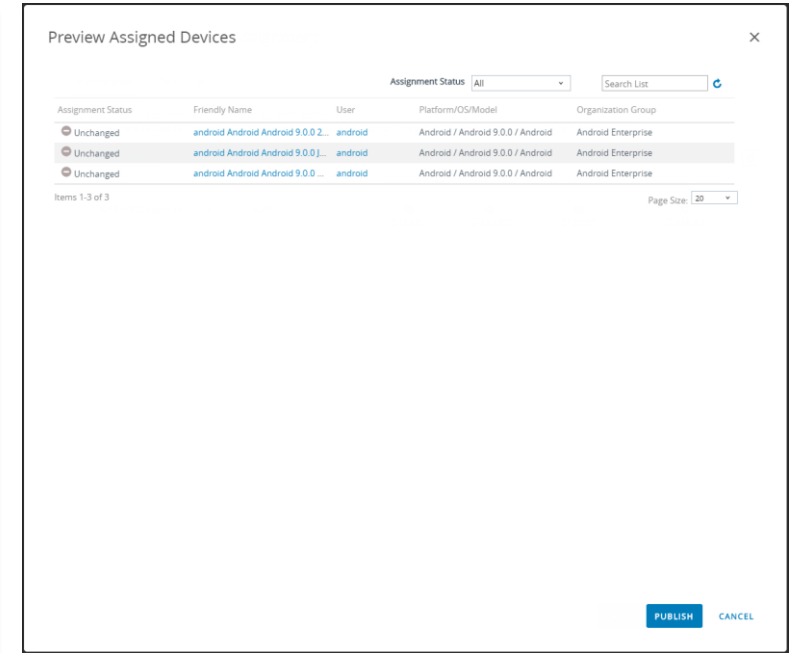
Assignments Exclusions

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).

ADD ASSIGNMENT ⓘ

Name	Priority	App Delivery Method	Managed Access	VPN Access	Send Configuration	Pre-release Version
Knox Platform for Enterprise	0	On Demand	DISABLED	DISABLED	DISABLED	DISABLED

SAVE AND PUBLISH **CANCEL**



Preview Assigned Devices

Assignment Status: **All** Search List ⓘ

Assignment Status	Friendly Name	User	Platform/OS/Model	Organization Group
Unchanged	android Android Android 9.0.0.2...	android	Android / Android 9.0.0 / Android	Android Enterprise
Unchanged	android Android Android 9.0.0.1...	android	Android / Android 9.0.0 / Android	Android Enterprise
Unchanged	android Android Android 9.0.0...	android	Android / Android 9.0.0 / Android	Android Enterprise

Items 1-3 of 3 Page Size: **20**

PUBLISH **CANCEL**

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.

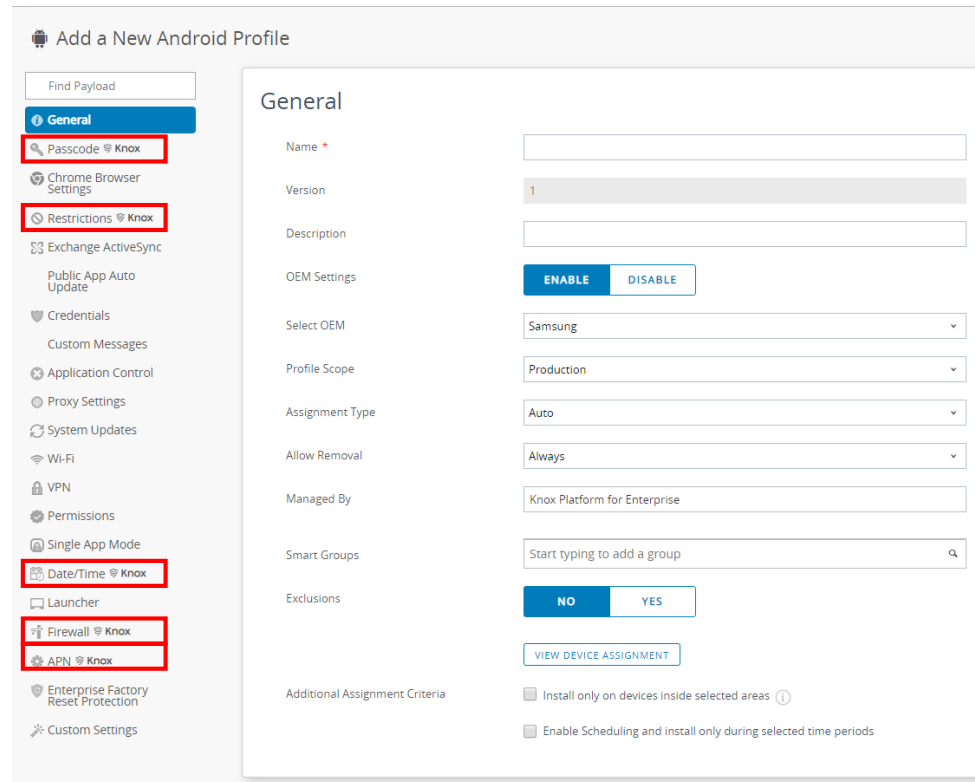


Configure Knox Platform for Enterprise : Standard Edition

Configure KPE : Standard Edition on 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
- 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




Featured Work Apps




CamScanner - P
INTSIG Information




WPS Office - Wor
Kingsoft Office Softv




Dropbox
Dropbox, Inc.




Job Search by Zi
ZipRecruiter, Inc.



Slack
Slack Technologies I



DocuSign - Uploa
DocuSign




Trello
Trello, Inc.


SEE MORE

Works with G Suite


Apps for making work easier




DocuSign - Uploa
DocuSign




Asana: organize t
Asana, Inc.




Invoice & Time T
Zoho Corporation




Smartsheet
Smartsheet Inc.



Wrike - Project M
Wrike Inc.




Insightly CRM
Insightly Inc.



Dialpad
Dialpad, Inc

SEE MORE




Knox Service Plugin

Samsung Electronics Co., Ltd.


Showing permissions for all versions of this app

This app has access to:



Photos / Media / Files

- read the contents of your USB storage
- modify or delete the contents of your USB storage



Storage

- read the contents of your USB storage
- modify or delete the contents of your USB storage


Updates to Knox Service Plugin may automatically add additional capabilities within each group. [Learn more](#)

Cancel

Approve

Approval settings

Notifications



Knox Service Plugin

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.

☐

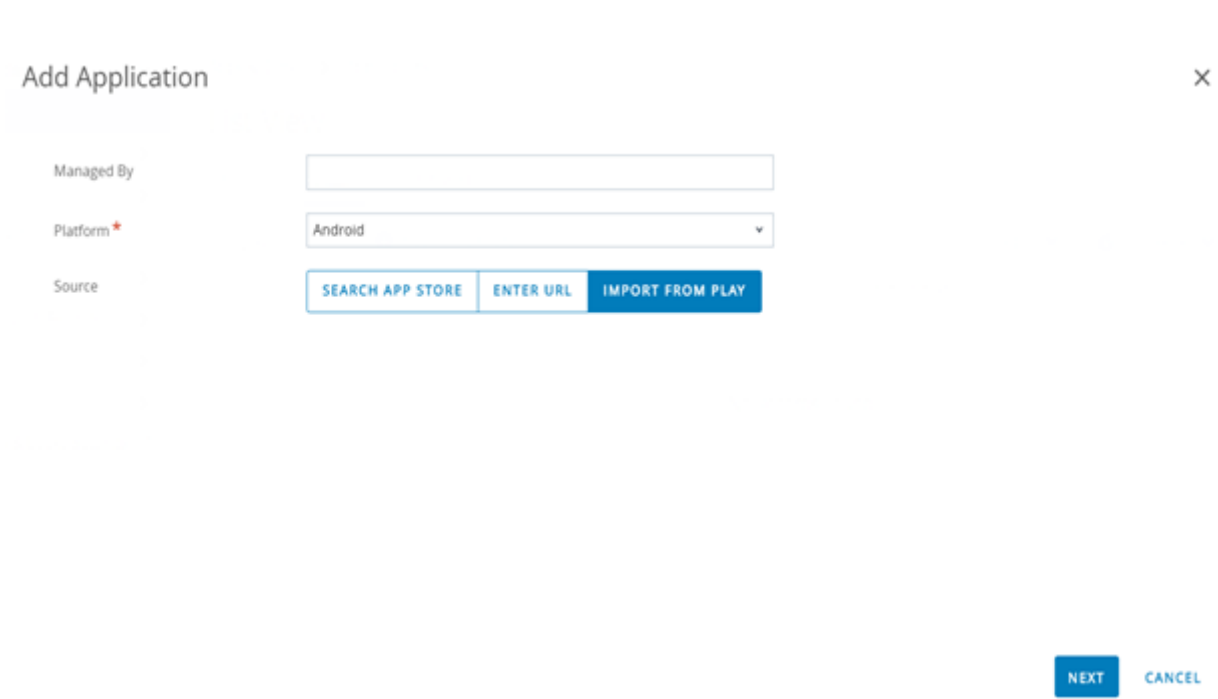
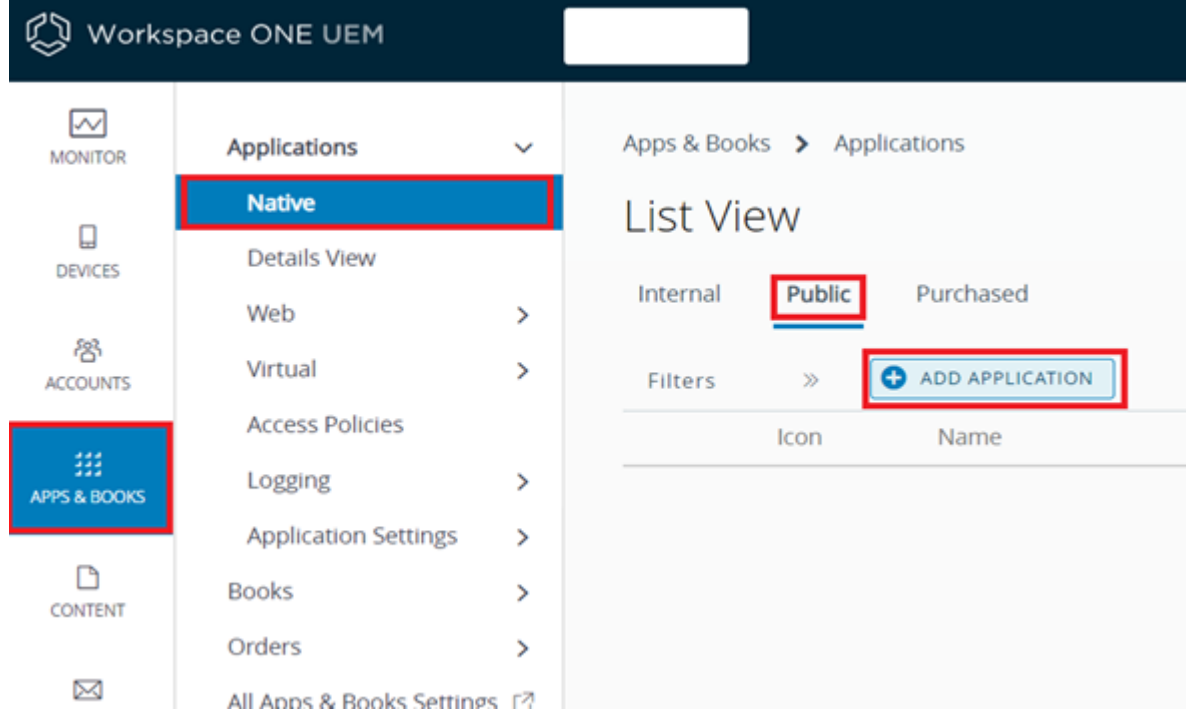
Revoke app approval when this app requests new permissions.

App will be removed from the shop until it is reapproved.

Done

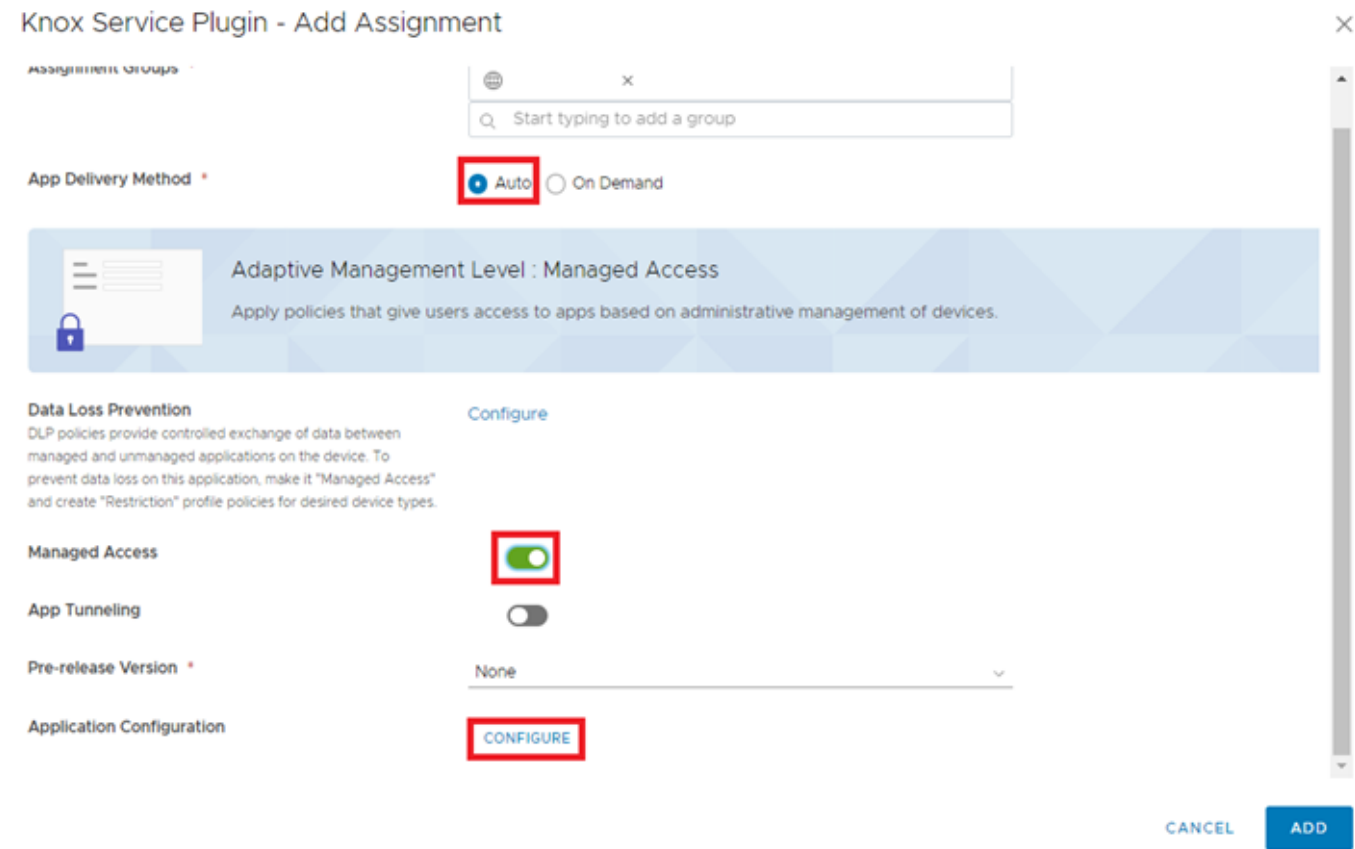
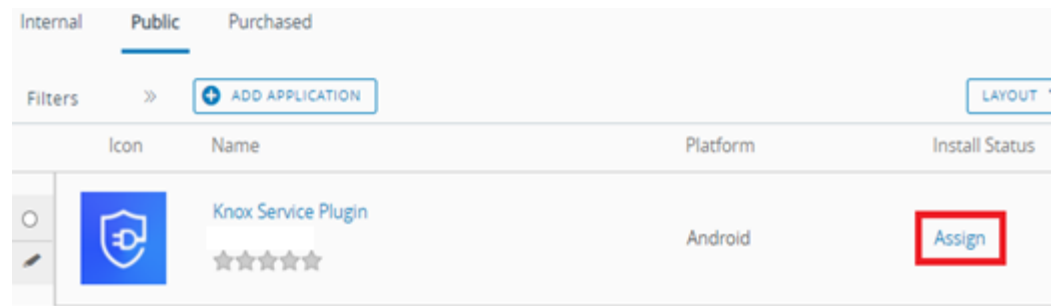
Knox Service Plugin [KSP]

- In the WorkspaceOne 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.



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.



Knox Platform for Enterprise : Premium Edition

- 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)

CONFIGURE

DeX policy, VPN policy (Premium), Firewall and Proxy policy, Call and Messaging control, Device Restrictions, Advanced Restriction policies (Premium), Firmware update (OTA) 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

Allow dual SIM operation

Enable

ADD

Knox Platform for Enterprise : Premium Edition

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

Knox Service Plugin - Edit assignment

management groups

Start typing to add a 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 in this application, make it "Managed Access" and create "Restriction" profile policies for desired device types.

Managed Access

On

App Tunneling

Off

Pre-release Version *

None

Application Configuration

EDIT

DELETE

CANCEL

ADD

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).

ADD ASSIGNMENT

EDIT

DELETE

MOVE UP

MOVE DOWN

	Name	Priority	App Delivery Method	Managed Access	VPN Access	Send Configuration	Pre-release Version
<div><div></div><div></div></div>		0	On Demand	<div>Enabled</div>	<div>Disabled</div>	<div>Enabled</div>	<div>Disabled</div>

CANCEL

SAVE AND PUBLISH

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

CANCEL

PUBLISH

Document Information

This is version 2.1 of this document.

Thank you!

