

IBM Maas360

&

Knox Platform for Enterprise

July 2022

Samsung R&D Centre UK
(SRUK)

1. How to gain access to IBM MaaS360
2. Pre-requisites for Knox Platform for Enterprise
3. Configure Android Enterprise
4. Android Enterprise Deployment Modes
 - BYOD
 - Work Profile
 - Company-owned Device
 - Fully Managed Device
 - Work Profile on Company-owned Device (WPC, WPCO or WPCOD)
 - Dedicated Device
5. Managed Google Play [MGP] Configuration
6. AppConfig in IBM MaaS360
7. Configure Knox Platform for Enterprise : Standard Edition
8. Configure Knox Platform for Enterprise : Premium Edition
9. Configure Knox Service Plugin [KSP]
10. Document Info

Contacts:

sruk.product@samsung.com

Knowledge Base:

https://www.ibm.com/support/knowledgecenter/SS8H2S/com.ibm.mc.doc/mc_collateral/mc_landing.htm

<https://www.ibm.com/security/mobile/maas360>

<https://www.ibm.com/security/mobile/maas360/android-mdm>

IBM MaaS360 Solution:

https://www.youtube.com/watch?v=UeH_zGcJ-bM

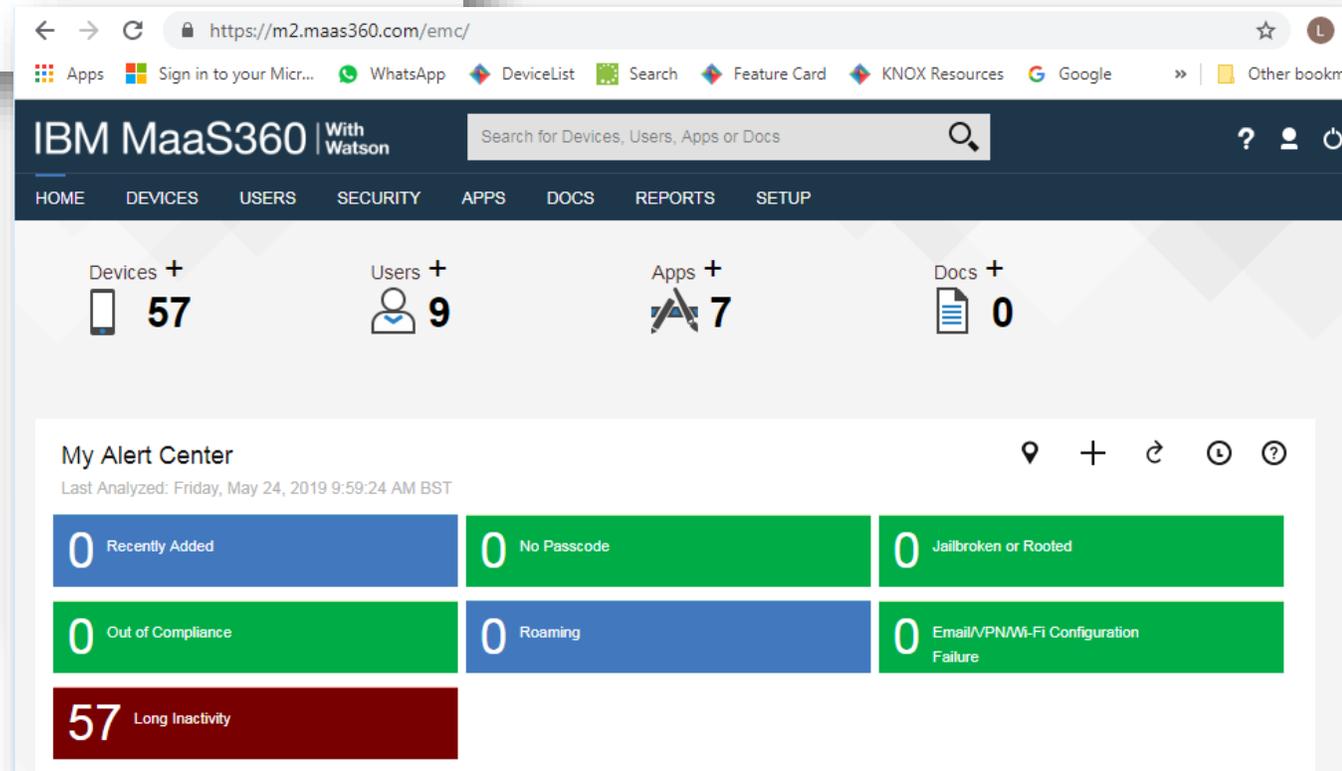
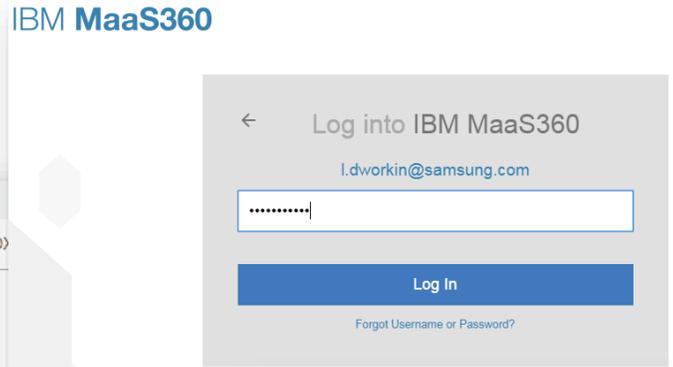
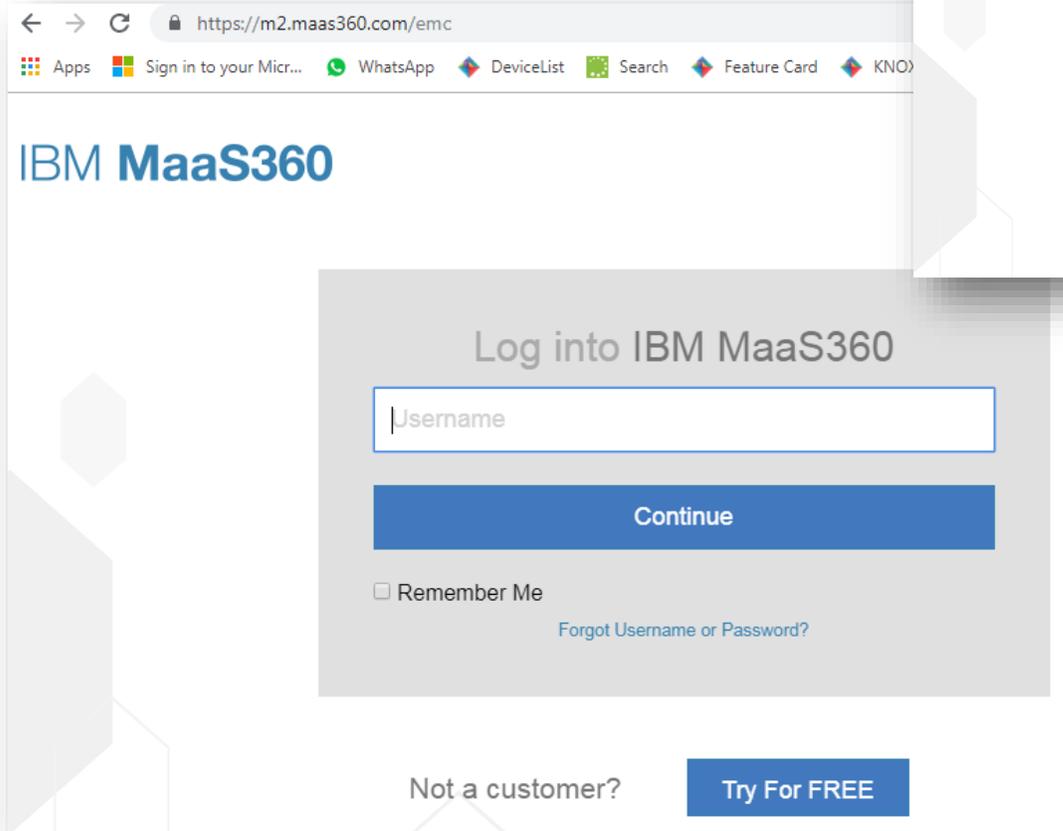
Trial Access:

<https://www.ibm.com/account/reg/us-en/signup?formid=urx-19907>

1. Obtain access to MaaS360 console
2. A Gmail account to map to MaaS360 for Managed Google Play
3. Consider what enrollment method to use:
 - Knox Mobile Enrollment (KME)
 - QR Code enrollment
 - Email enrollment
 - Server details enrollment
4. Obtain a Knox Platform for Enterprise Premium License

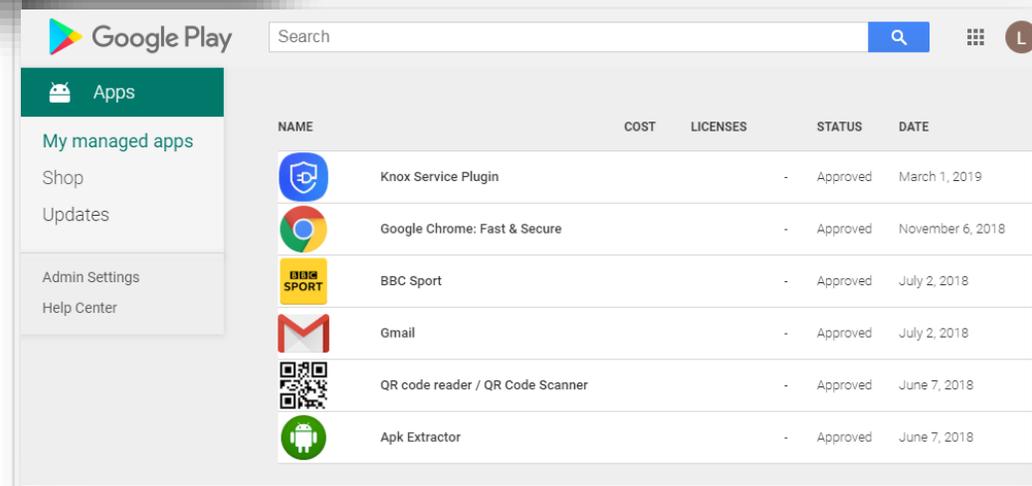
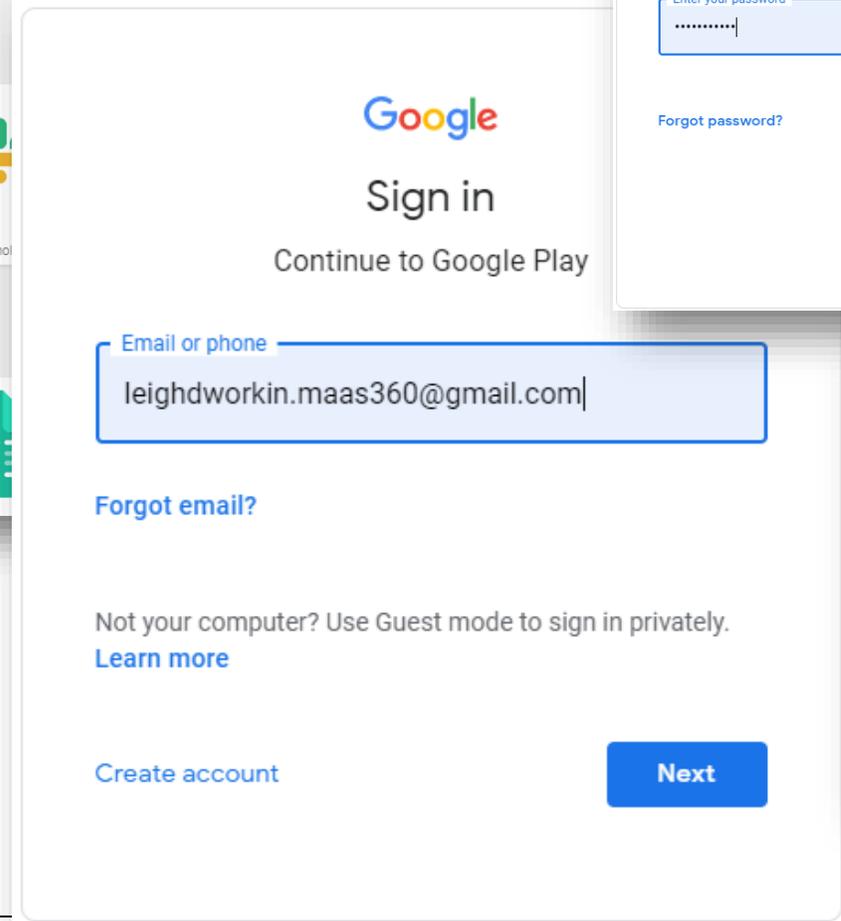
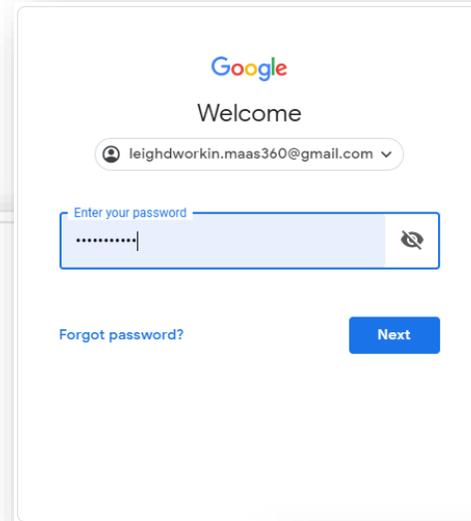
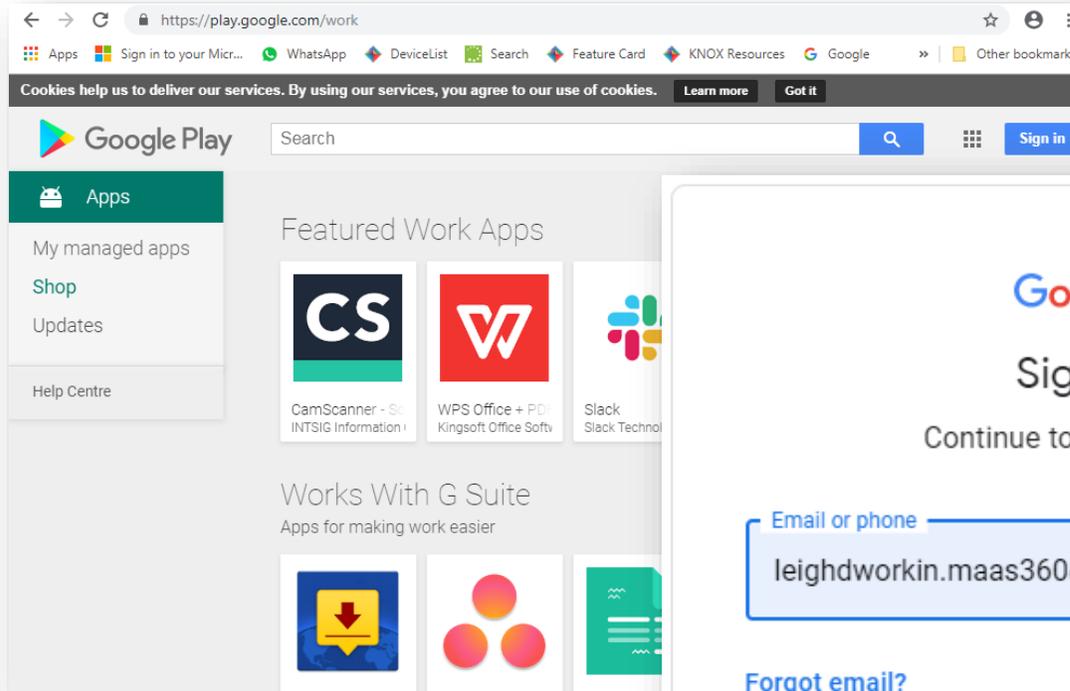
Obtain access to MaaS360 console

<https://m2.maas360.com/emc>



A Gmail account to map to MaaS360 for Managed Google Play

<https://play.google.com/work>



NAME	COST	LICENSES	STATUS	DATE
 Knox Service Plugin	-	-	Approved	March 1, 2019
 Google Chrome: Fast & Secure	-	-	Approved	November 6, 2018
 BBC Sport	-	-	Approved	July 2, 2018
 Gmail	-	-	Approved	July 2, 2018
 QR code reader / QR Code Scanner	-	-	Approved	June 7, 2018
 Apk Extractor	-	-	Approved	June 7, 2018

Configure Android Enterprise

- Log into MaasS360 Console. Navigate to: **Setup -> Services -> Mobile Device Management**
- Click **more...** next to **Mobile Device Management**
- Select **Enable Android Enterprise Solution Set**
- Select **Enable via Managed Google Play (no G Suite)**

Enable Android Enterprise Solution Set

Enable Android enterprise features, such as Work Profile (Profile Owner), Work Managed Device (Device Owner) and COSU to better protect and control work data on managed devices. [Learn more](#)

Enable via Managed Google Play Accounts (no G Suite)

Enable via Google Accounts (managed Google domain)

- Click **here** to sign up and enable managed Google Play
- Then Click **Enable** to Auto Import Approved Apps

Click [here](#) to sign up and enable managed Google Play 

Note: The link opens in a new page. Ensure pop-up blockers are disabled prior to clicking on the link.

Confirm Android Managed Google Play Accounts Enablement ✕

Auto Import Approved Apps

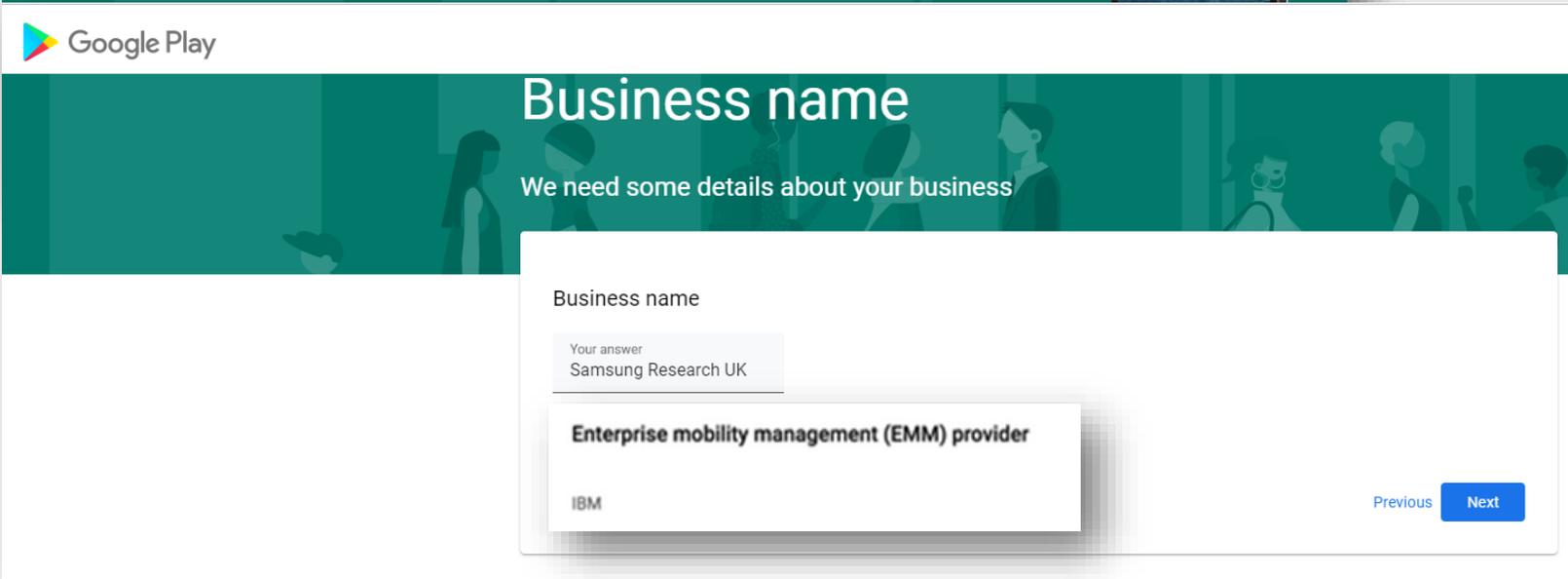
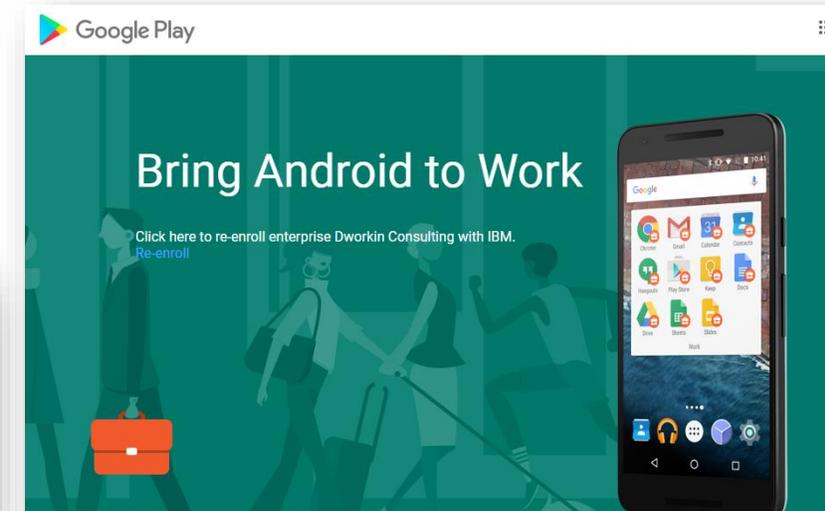
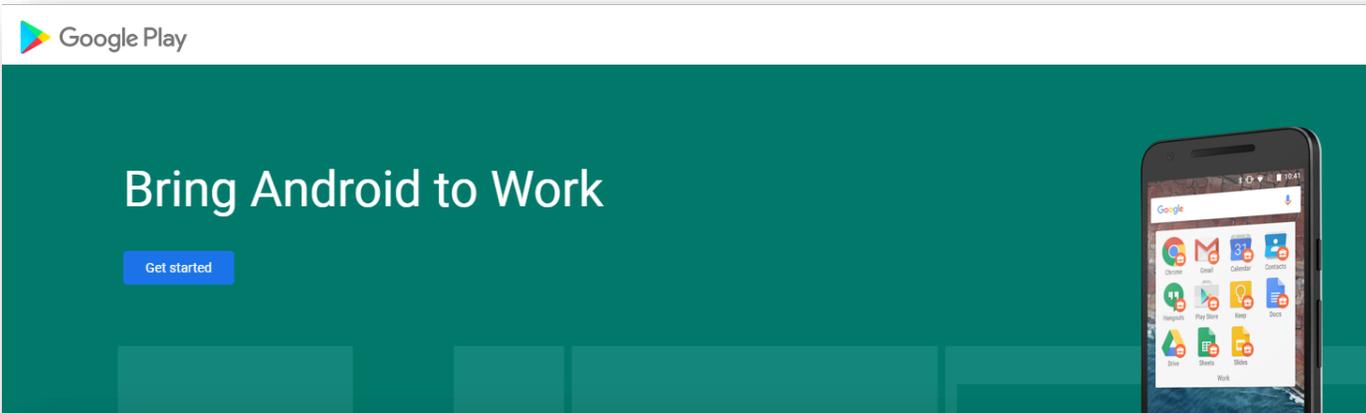
Import apps tied to your Android Enterprise account once approved on Google console. If you want to skip import now, uncheck the option and enable it later from **Apps > App Catalog > More > App Catalog Settings > Android Enterprise Settings**.

Enable

Configure Android Enterprise

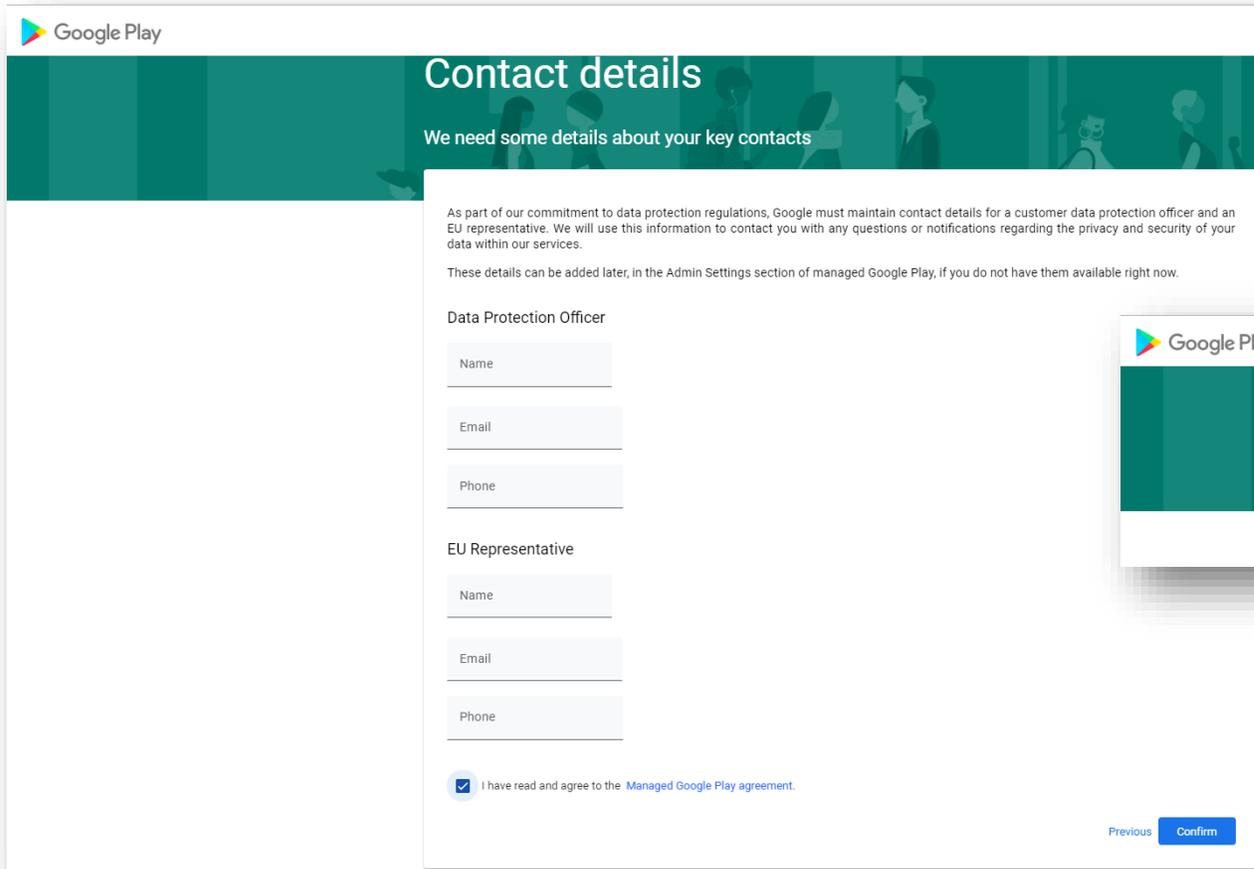
- You will then get redirected to a Google Play screen. Click Get started.
- Fill out your Business name and Select Next to allow IBM MaaS360 to be your EMM provider.

- (Note re-enrolling looks slightly different and there are fewer steps)
- Click Re-enroll)



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 IBM MaaS360 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 right now.

Data Protection Officer

Name

Email

Phone

EU Representative

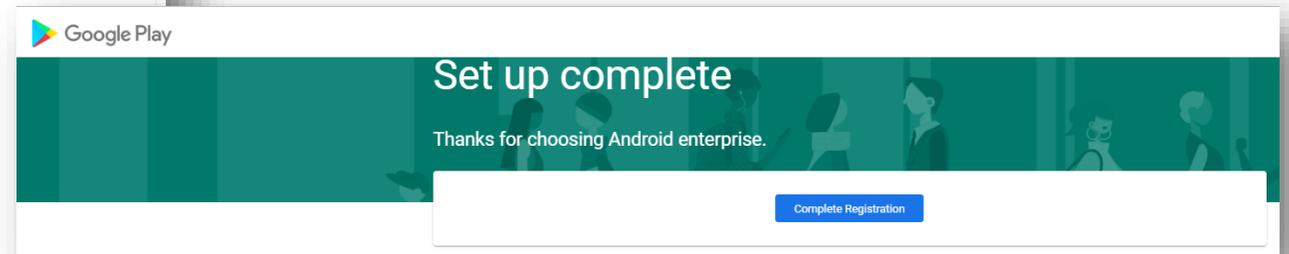
Name

Email

Phone

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

Previous



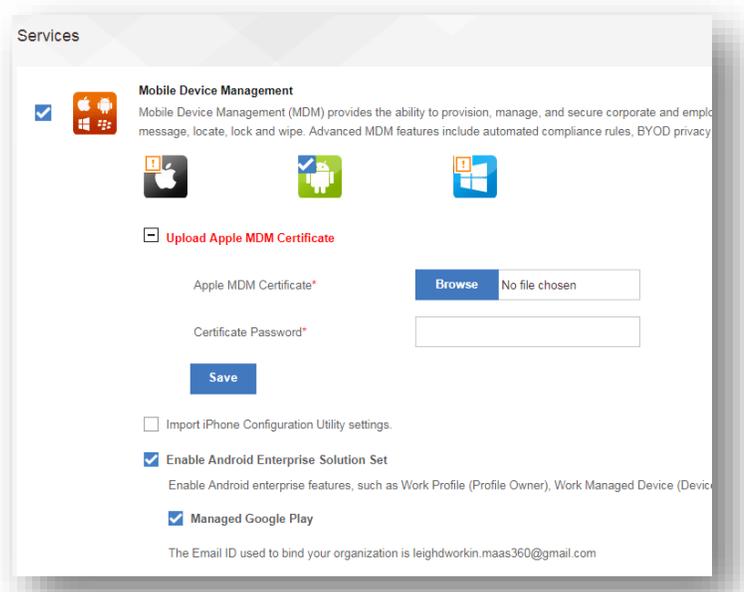
Google Play

Set up complete

Thanks for choosing Android enterprise.

Configure Android Enterprise

- You should now have been redirected back to the IBM MaaS360 console
- The Mobile Device Management configuration should now be completed and look similar to the below.
- You may check by visiting **Setup -> Services -> Mobile Device Management** again
- Your IBM MaaS360 tenant is now configured and ready to deploy Android Enterprise and Knox Platform for Enterprise: Standard Edition.



Enable Android Enterprise Solution Set

Enable Android enterprise features, such as Work Profile (Profile Owner), Work Managed Device (Device Owner) and COSU to better protect and control work data on managed devices. [Learn more](#)

Managed Google Play

The Email ID used to bind your organization is leighdworkin.maas360@gmail.com

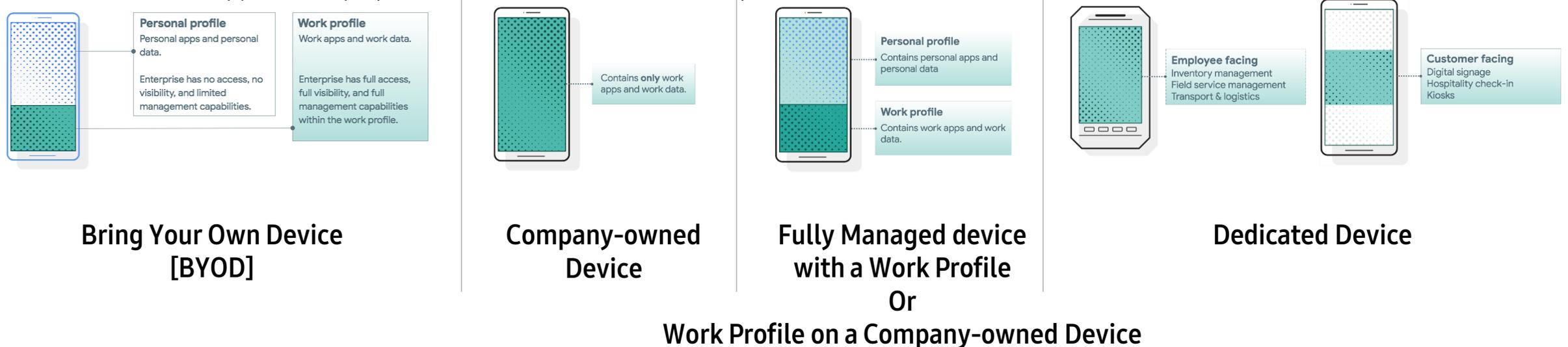
Android Enterprise Deployment Modes

Deployment Modes

Android Enterprise can be deployed in the following 5 deployment modes

1. BYOD
 - Work Profile [*formerly known as Profile Owner or PO*]
2. Company-owned Device
 - Fully Managed Device [*formerly known as Device Owner or DO*]
 - Fully Managed Device with a Work Profile [*formerly known as COMP, on Android 10 or before*]
 - Work Profile on a Company-owned Device [*WPC, only on Android 11 or later*]
3. Dedicated device [*formerly known as Corporate Owned Single Use or COSU*]

IBM MaaS360 can support 4 of these 5 of these deployment modes, all but COMP. In this next section we will show you how to configure each of these 4 supported deployment modes in IBM MaaS360 for your device fleet.



Create a User in MaaS360

Create a User in MaaS360

- Navigate to: **Users** and Click the **Add User** button
- Fill in all required fields and then click Save.

IBM MaaS360 | With Watson

Search for Devices, Users, Apps or Docs

HOME DEVICES **USERS** SECURITY APPS DOCS REPORTS SETUP

User Directory ↻ **Add User** Hide Users with no Devices More ▾

Use the Cloud Extender or Azure AD Integration to integrate with your Corporate User Directory to import group and associated user information. Cloud Extender is available for download on the Services enablement workflow. Azure AD Integration is available as part of Enterprise Integration. Imported information can be used for automatic provisioning of users, group based policy assignment and App & Doc distribution. Supported User Directories for Cloud Extender are Active Directory, OpenLDAP, Novell LDAP, IBM Domino LDAP and Oracle User Directory.

To specify groups to import, use the workflow: [Add User Directory Group](#). To add Local Groups, use the workflow: [Add Local User Group](#).

Username	Full Name	Domain	Email Address	Status	User ...	Last Update...
ae View Add Device Deactivate More...	Android Enterprise	sbhomenet	stephen@rkselab.com	Active	Local Directory	07/18/2018 15:38 BST
bennetts View Add Device Reset Password More...	Stephen Bennett	rkselab.com	stephen.b@samsung.com	Active	Local Directory	03/28/2019 11:40 GMT
cosu View Add Device Reset Password More...	Kiosk User	rkselab.com	stephen.b@samsung.com	Active	Local Directory	09/06/2018 11:56 BST
leigh View Add Device Reset Password More...	Leigh Dworkin	rkselab	l.dworkin@samsung.com	Active	Local Directory	07/25/2018 12:35 BST

Add User

Basic | Advanced

Full Name: Leigh Dworkin

Username*: leighdworkin

Domain*: rkselab.com

Email*: l.dworkin@samsung.com

Managed Apple ID: Enter Managed Apple ID

Authentication Type*: MaaS360

User Groups: Enter a few characters of Group Name

Phone Number: +1 [Phone Number]

Location: Enter office location

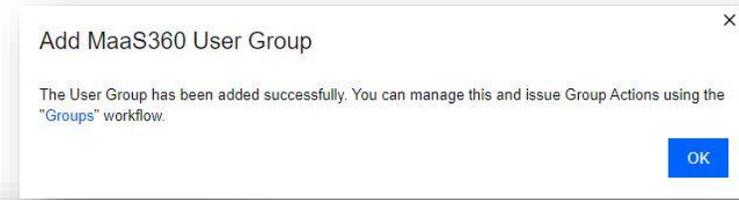
Add New Device:

- Note, you may need to Reset the Password for the new user:

leigh.dworkin.ae
[View](#) | [Add Device](#) | **Reset Password** | [More...](#)

Add User to a Group in MaaS360

- Navigate to: Users -> Groups -> Add -> MaaS360 User Group.
- Fill in the required fields and add the email address of the user to "Usernames" field. Then click Save.
- Click OK



IBM MaaS360 With Watson

Search for Devices, Users, Apps or Docs

HOME DEVICES **USERS** SECURITY APPS DOCS REPORTS SETUP

Groups

Directory
Groups

Show Private Groups Bulk Delete User Groups Bulk Import Groups **Add**

Name	Type	Policies	Rule Sets	Apps	Docs	Updated by
Android Enterprise Users Edit Delete More...	👤	📱 AfW		📧 Gmail 📺 BBC Sport		stephen.b@samsung.com
Test Devices Devices Refresh Edit More...	📱					System Administrator
Corporate Owned Devices Devices Refresh Edit More...	📱					System Administrator
Devices Not Reported in Last 7 days Devices Refresh Edit More...	📱					System Administrator
Devices with Passcode Out-of-Compliance Devices Refresh Edit More...	📱					System Administrator
Roaming Devices Devices Refresh Edit More...	📱					System Administrator
All Devices Devices Refresh Edit More...	📱					System Administrator
Smartphones Devices Refresh Edit More...	📱					System Administrator
Tablets Devices Refresh Edit More...	📱					System Administrator
iPads Devices Refresh Edit More...	📱					System Administrator
iPhones Devices Refresh Edit More...	📱					System Administrator
iOS Devices Devices Refresh Edit More...	📱					System Administrator
Android Devices Devices Refresh Edit More...	📱					System Administrator
Employee Owned Devices Devices Refresh Edit More...	📱					System Administrator
Windows Phone Devices Devices Refresh Edit More...	📱					System Administrator

Jump To Page: Displaying 1 - 15 of 15 Records | Show 25 Records

Add MaaS360 User Group

Note:
User Groups can be used for assigning policies and distributing Apps & Docs. To manage Groups and take actions on these, use the "Groups" workflow

Name *

Usernames (or Email Addresses)

Description

User group to be available for

- Security (Policies, Compliance Rules, Locations and Privacy Settings)
- App distribution
- Doc distribution

Cancel Save

Add a device for the newly created user

- In the User directory click Add Device for the relevant user
- Click Send Request
- Click OK

User Directory



Use the Cloud Extender or Azure AD Integration to integrate with your Corporate User Directory to import groups for automatic provisioning of users, group based policy assignment and App & Doc distribution. Supported User Directory integrations include Active Directory, Azure AD, and Okta. To specify groups to import, use the workflow: [Add User Directory Group](#). To add Local Groups, use the workflow: [Add Local Group](#).

Username	Full Name
ae View Add Device Deactivate More...	Android Enterprise
bennetts View Add Device Reset Password More...	Stephen Bennett
cosu View Add Device Reset Password More...	Kiosk User
leigh View Add Device Reset Password More...	Leigh Dworkin
leigh.ae View Add Device Reset Password More...	Leigh Dworkin
leigh.dworkin.ae View Add Device Reset Password More...	Leigh Dworkin

Add Device

Basic Advanced

Device Addition Mode

Enroll using Android enterprise

Managed Google Play Account Type Device Account User Account

Account type once chosen cannot be changed later.

Username: leighdworkin

Domain: rksselab.com

Email: l.dworkin@samsung.com

Phone Number: +1 Phone Number

Notify User* Email SMS

Copy Email Me

[Cancel](#) [Send Request](#)

Enrollment request sent successfully.



An enrollment request and registration instructions have been sent to l.dworkin@samsung.com. The device can also be registered by accessing the below URL from the device.

Corporate Identifier: 20010155

URL: <https://m.dm/20010155/7578805>

QR Code for Enrollment URL
[Download](#)

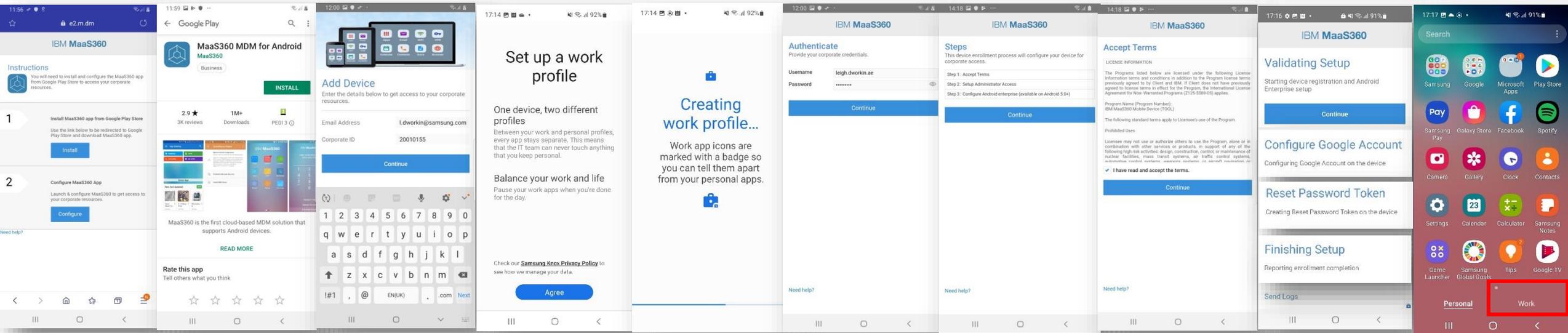
OK

Android Enterprise: Work Profile (BYOD)

Android Enterprise Work Profile 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 IBM MaaS360 agent, and enroll your device into your tenant.
- Alternatively, in a browser on the device, visit the URL from the Email invitation for the device:



Visit URL in Samsung Browser from Email invitation. Click Install

Install MaaS360 agent from Google Play Store

Check email and hit Continue

Click Agree to create Work Profile

Creating Work Profile

Enter user credentials & hit Continue

Review Steps & hit Continue

Accept terms and conditions & hit Continue

Validate Setup by hitting Continue; various screens then flash past ending in Finishing Setup

Device Enrollment Successful!: Work Tab Created

*You can also enroll your device using the alternative IBM MaaS360 methods. For example QR Code – see next slide.

Android Enterprise: Work Profile (BYOD) - QR code

Android Enterprise Work Profile Deployment with QR code

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 IBM MaaS360 agent, and enroll your device into your tenant.
- Alternatively, in a browser on the device, visit the URL from the Email invitation for the device:

Visit URL in Samsung Browser from email invitation. Click Install

Install MaaS360 Agent from Google Play Store and Run it

Click Scan QR Code

Scan the QR code from email invitation then click Continue on next screen

Click Agree to create Work Profile

Creating Work Profile

Enter user credentials & hit Continue

Review Steps & hit Continue

Accept terms and conditions & hit Continue

Validate Setup by hitting Continue

Various screens flash by quickly ending in "Finishing Setup"

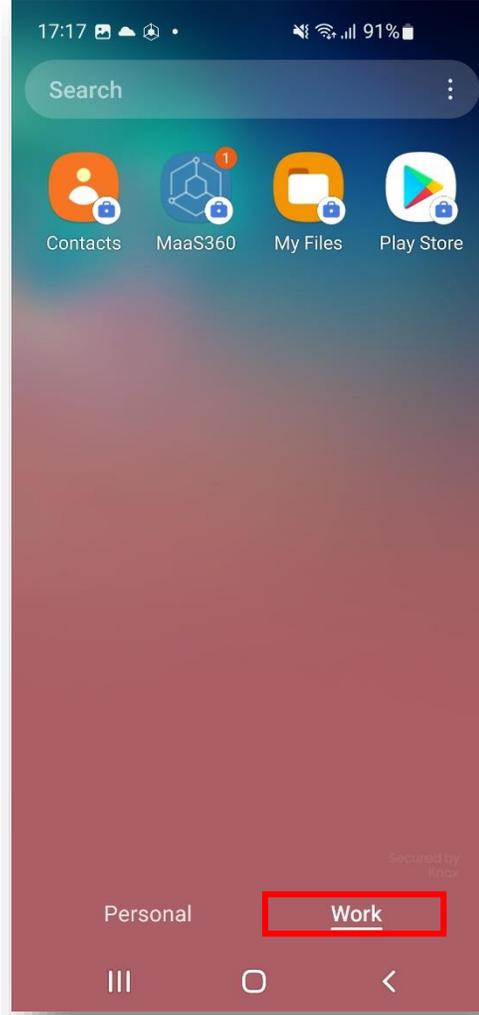
Device Enrollment Successful!: Work Tab Created

Android Enterprise: Work Profile Enrollment

How to tell that Work Profile has been successfully set up:



Personal Tab



Work Tab



No mention of device belonging to your organization on lock screen

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#maas360**
2. QR Code Enrollment / NFC Enrollment –
 - scan QR code (MaaS360 Portal -> Devices -> Enrollments -> Other Enrollment Options -> Android Enterprise QR Code Provisioning)
3. Knox Mobile Enrollment (MaaS360 Portal -> Devices -> Enrollments -> Other Enrollment Options -> Android Enterprise KME enrollment)

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

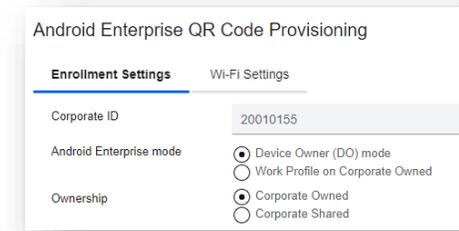
<p>Welcome!</p>	<p>For your review</p>	<p>Permissions for Samsung apps and services</p>	<p>Choose a Wi-Fi network</p>	<p>Copy apps and data</p>	<p>Google Sign in with your Google Account. Learn more</p>	<p>Your account is managed</p>	<p>Getting ready for work setup...</p>	<p>Set up your phone</p>	<p>This device isn't private</p>	<p>Add Device</p>	<p>Authenticate</p>	<p>Steps</p>	<p>Accept Terms</p>	<p>Validating Setup</p>	<p>Finishing Setup</p>
Click Start	Accept T's & C's and click Next	Agree to permissions for Samsung apps	Connect to WiFi if needed	Don't copy apps & data	Enter afw#maas360 and click Next	Note your account is managed & click Next	Get ready for work setup...	Install MaaS360 by hitting Continue	Note device isn't private & hit Next	Enter email and Corporate ID	Enter Credentials	Review Steps And Continue	Accept Terms and Continue	Validate Setup by hitting Continue; Device Enrollment various screens then flash past ending in Finishing Setup	Click Close Successful!

Android Enterprise: Company-owned Device - QR code

Android Enterprise Company-owned Device Deployment

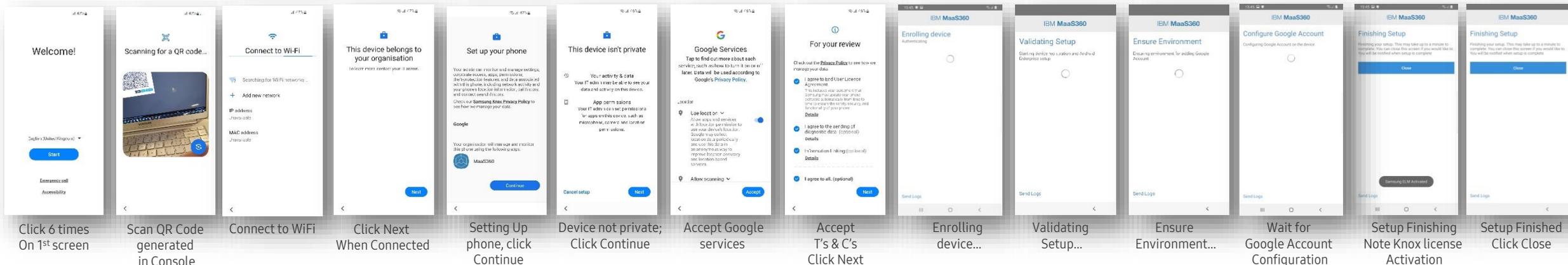
To enroll your device as an Android Enterprise Company-owned device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 3 ways you can enroll your device into Workspace ONE UEM as an Android Enterprise Company-owned device.

1. DPC Identifier [Also known as the hashtag method] **afw#maas360**
2. QR Code Enrollment / NFC Enrollment –
 - scan QR code (MaaS360 Portal -> Devices -> Enrollments -> Other Enrollment Options -> Android Enterprise QR Code Provisioning)
 - Select Device Owner (DO) mode and Corporate Owned:



3. Knox Mobile Enrollment (MaaS360 Portal -> Devices -> Enrollments -> Other Enrollment Options -> Android Enterprise KME enrollment)

- Below is a screen-by-screen play to enroll your device using the QR code method:



Android Enterprise Company-owned Device Deployment

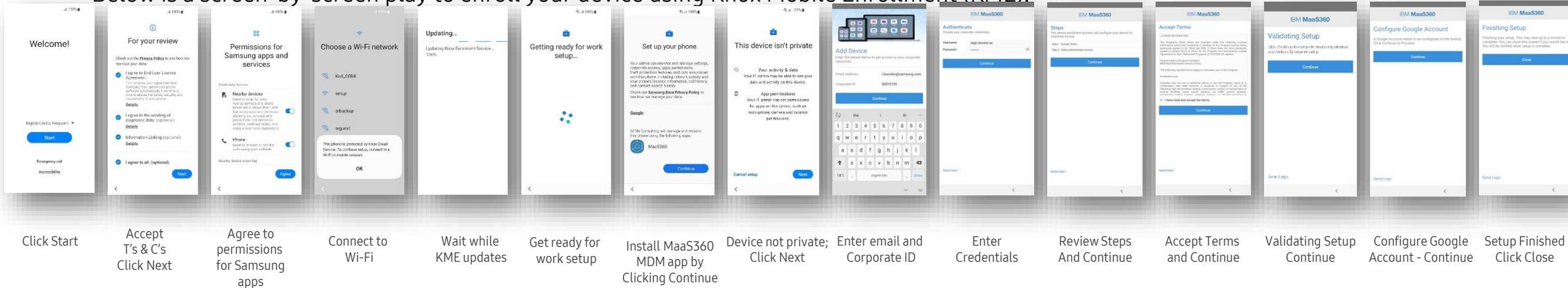
To enroll your device as an Android Enterprise Company-owned device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 3 ways you can enroll your device into Workspace ONE UEM as an Android Enterprise Company-owned device.

1. DPC Identifier [Also known as the hashtag method] **afw#maas360**
2. QR Code Enrollment / NFC Enrollment –
 - scan QR code (MaaS360 Portal -> Devices -> Enrollments -> Other Enrollment Options -> Android Enterprise QR Code Provisioning)
3. Knox Mobile Enrollment (MaaS360 Portal -> Devices -> Enrollments -> Other Enrollment Options -> Android Enterprise KME enrollment)

This generates a JSON string for your KME profile in the KME console, similar to the one below, which may be customized -

```
{\"prompt_for_asset_tag\":false,\"disallow_enrollment_skipping\":true,\"enrollment_corp_id\":\"XXXXXXXX,\"enrollment_account_type\":\"userAccount\",\"prompt_for_device_name\":false,\"ae_container_type\":\"WORK_NATIVE_DEVICE\",\"enrollment_username\":\"a.b@cccc.com\",\"ae_enrollment_flow\":\"KME_ENROLLMENT\",\"enrollment_email\":\" a.b@cccc.com \",\"enrollment_ownership\":\"Corporate Owned\",\"enrollment_password\":\"*****\",\"android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME\":\"com.fiberlink.maas360.android.control/com.fiberlink.maas360.android.control.receivers.Maas360DeviceAdminReceiver\"}
```

• Below is a screen-by-screen play to enroll your device using Knox Mobile Enrollment (KME):

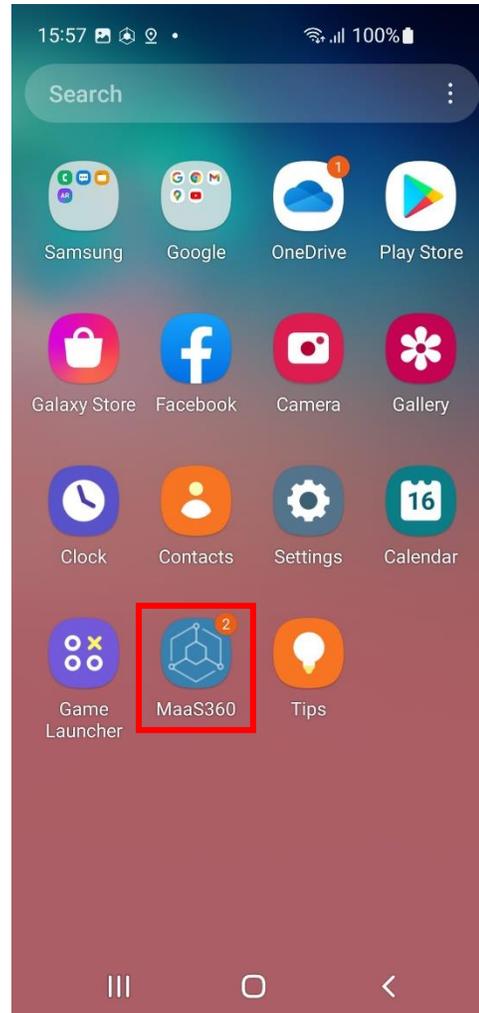


Android Enterprise: Fully Managed Device Enrollment

How to tell that Fully Managed Device has been successfully set up:



Sparse set of icons on home screen



No Personal nor Work tabs;
Sparse set of icons including MaaS360 agent



Mention of device belonging to your organization on lock screen

Android Enterprise Fully Managed Device with a Work Profile Deployment

This is not currently supported by IBM MaaS360.

Attempts to enroll into Fully Managed Device with a Work Profile on Android 10 will result in a Fully Managed Device.

However, on Android 11 or later a very similar deployment mode – Work Profile on Company-owned Device – is supported. See next page.

Android Enterprise: Work Profile on a Company-owned Device (QR CODE)

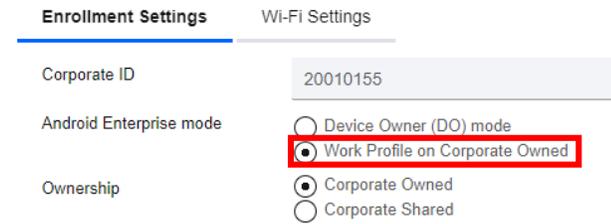
Android Enterprise Work Profile on a Company-owned Device Deployment

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 2 ways you can enroll your device into Workspace ONE UEM as an Android Enterprise Company-owned device with a Work Profile.

1. QR Code Enrollment / NFC Enrollment –

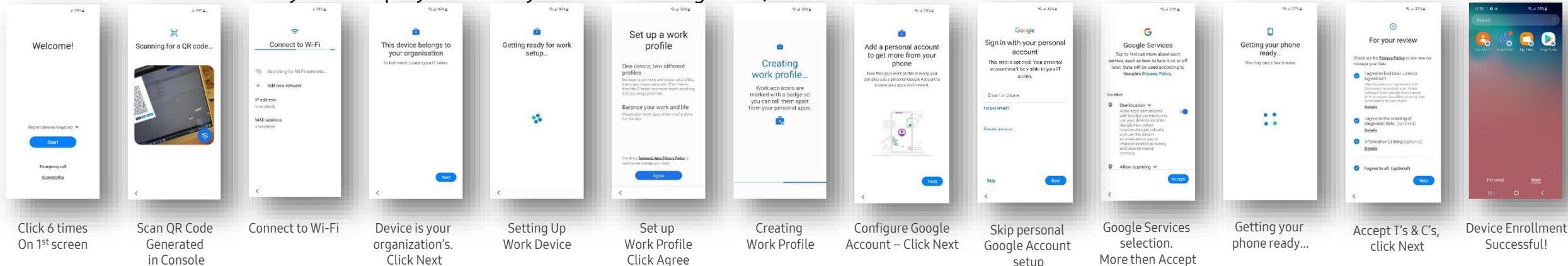
- scan QR code (MaaS360 Portal -> Devices -> Enrollments -> Other Enrollment Options -> Android Enterprise QR Code Provisioning)
- Select Work Profile on Corporate Owned and Corporate Owned:

Android Enterprise QR Code Provisioning



2. Knox Mobile Enrollment (MaaS360 Portal -> Devices -> Enrollments -> Other Enrollment Options -> Android Enterprise KME enrollment)

- Below is a screen-by-screen play to enroll your device using the QR code method:



Android Enterprise: Work Profile on a Company-owned Device (KME)



Android Enterprise Work Profile on a 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 2 ways you can enroll your device into Workspace ONE UEM as an Android Enterprise Company-owned device with a Work Profile.

1. QR Code Enrollment / NFC Enrollment –

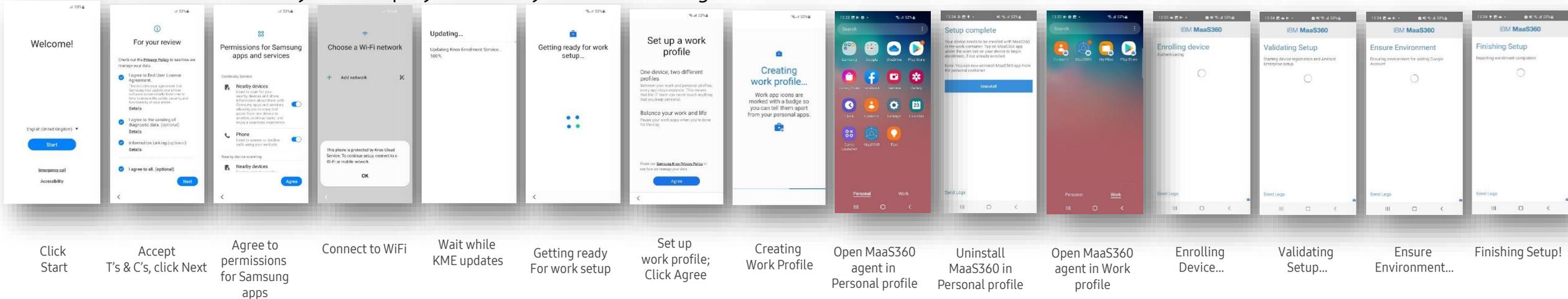
- scan QR code (MaaS360 Portal -> Devices -> Enrollments -> Other Enrollment Options -> Android Enterprise QR Code Provisioning)

2. Knox Mobile Enrollment (MaaS360 Portal -> Devices -> Enrollments -> Other Enrollment Options -> Android Enterprise KME enrollment)

This generates a JSON string for your KME profile in the KME console, similar to the one below, which may be customized

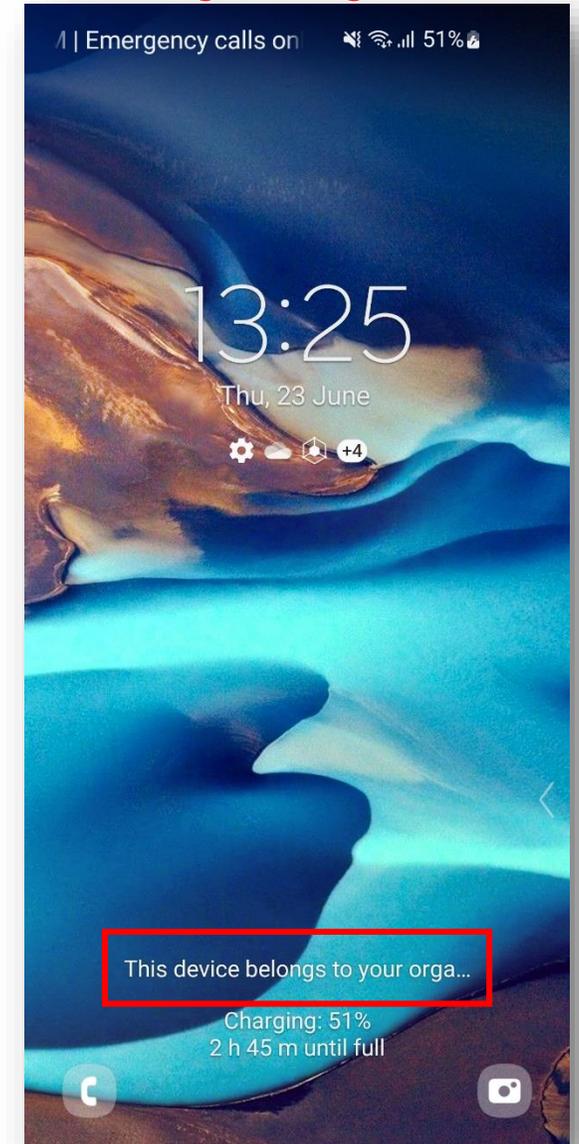
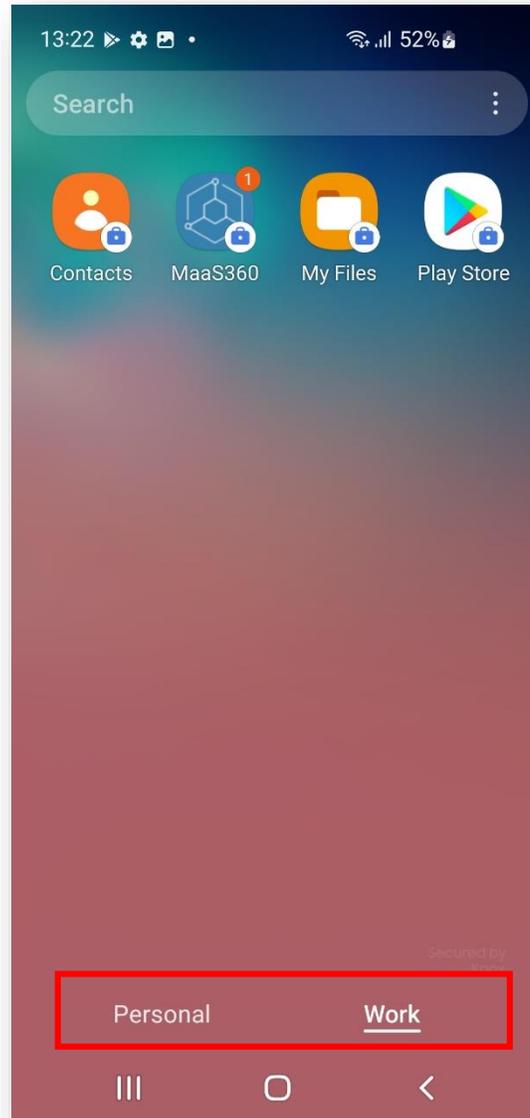
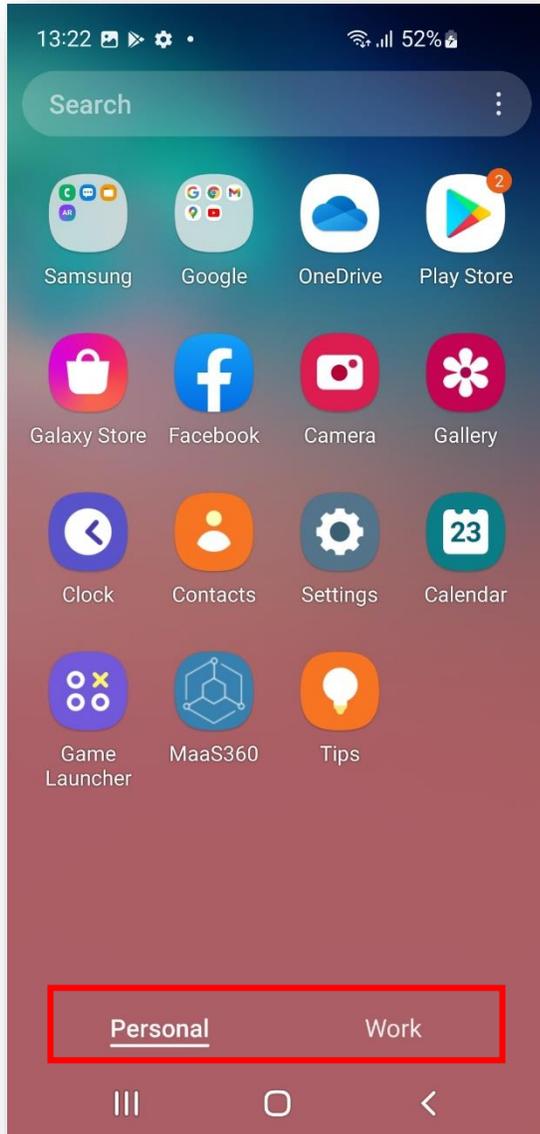
```
{ "prompt_for_asset_tag": false, "enrollment_corp_id": "XXXXXXXX", "enrollment_account_type": "userAccount", "prompt_for_device_name": false, "ae_container_type": "WORK_NATIVE_PROFILE", "enrollment_domain": "cccccccc.com", "enrollment_username": "a.bbbb@cccccccc.com", "ae_enrollment_flow": "KME_ENROLLMENT", "enrollment_email": "a.bbbb@cccccccc.com", "enrollment_ownership": "Corporate Owned", "enrollment_password": "*****", "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.fiberlink.maas360.android.control/com.fiberlink.maas360.android.control.receivers.Maas360DeviceAdminReceiver" }
```

- Below is a screen-by-screen play to enroll your device using the KME method:



Android Enterprise: Work Profile on a Company-owned Device (WPC or WPCO)

How to tell on the device that you are in WPC mode – **Personal and Work Tabs + Device Belongs to Organisation**



Android Enterprise Dedicated Device Deployment

This should be possible and will be documented when time permits.

A COSU policy should be selected within the Android Enterprise Settings

Key policies are

1. Enable Kiosk Mode
2. Enable Admin Bypass for Kiosk mode
3. App package names should be added to the whitelist

The screenshot shows the IBM MaaS360 console interface. The top navigation bar includes 'HOME', 'DEVICES', 'USERS', 'SECURITY', 'APPS', 'DOCS', 'REPORTS', and 'SETUP'. A search bar is present on the right. The main content area is titled 'COSU' and shows the following settings:

- Device Settings**
 - Enable Kiosk Mode: Yes (Android 6.0+ (DO))
- Advanced Settings**
- KNOX Settings**
- Android Enterprise Settings**
 - Passcode
 - Security
 - Restrictions
 - Accounts
 - App Compliance
 - ActiveSync
 - Wi-Fi
 - VPN
 - Certificates
 - Browser
 - COSU (Kiosk mode)**
 - COSU Mode Type**: Show custom Home page with allowed Apps
 - App IDs for whitelisted Apps ***
 - com.samsung.android.calendar (Android 6.0+ (DO))
 - com.sec.android.gallery3d
 - com.adobe.reader
 - Set device to Kiosk mode**: Immediately (Android 6.0+ (DO))
 - Keep device on when plugged in**: Yes (Android 6.0+ (DO))
 - Enable Widgets**: Yes (Android 6.0+ (DO))
Enabling this feature will allow users to add or delete widgets on the device
 - Auto upgrade Kiosk**: Yes (Android 6.0+ (DO))
Enable to upgrade to latest kiosk for 5.75+
 - Enable Admin bypass for Kiosk mode**: Yes
Allows user to enter an admin-defined passcode to temporarily disable Kiosk mode

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#maas360**
2. QR Code Enrollment / NFC Enrollment –
 - scan QR code (MaaS360 Portal -> Devices -> Enrollments -> Other Enrollment Options -> QR Code for Android Enterprise DO Provisioning)
3. Knox Mobile Enrollment (MaaS360 Portal -> Devices -> Enrollments -> Other Enrollment Options -> KNOX Mobile Enrollment)

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

Click Start arrow

Accept T's & C's

Skip Import of Old Data

Enter **afw#maas360** and click next

Install MaaS360 MDM app

Install MaaS360 MDM app

Accept & Continue

Setting Up Work Device

Enter email and Corporate ID

Enter Credentials

Review Steps And Continue

Accept Terms and Continue

Configure Google Account - Continue

Setup Finished Click Close

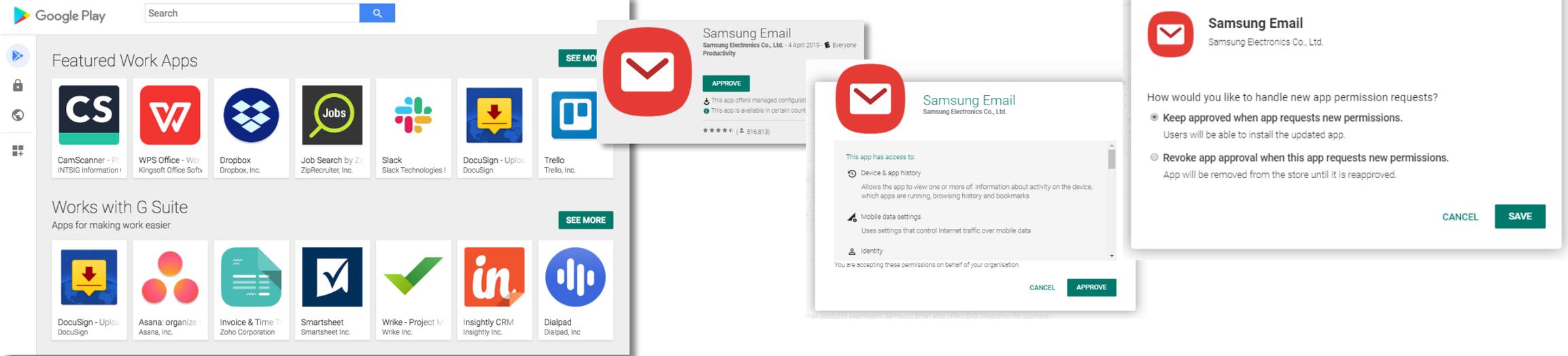
Device Enrollment Successful!

←-----Kiosked

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 IBM MaaS360 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 IBM MaaS360.

- Log in to your IBM MaaS360 Console and navigate to the tenant you have configured Android Enterprise
- Navigate to **APPS->Catalog** and click **Add->Android->Google Play App**
- Click **Add via Managed Google Play Store**
- Select the Samsung Email app we approved in our Managed Google Play Store.
- Click **APPROVE**

The screenshot shows the IBM MaaS360 console interface. At the top, there is a search bar and navigation tabs for HOME, DEVICES, USERS, SECURITY, APPS, DOCS, REPORTS, and SETUP. The 'APPS' tab is active, displaying the 'App Catalog' table. The table has columns for App Name, Type, Category, Install count, and Distribution status. Below the table, the 'Add' dropdown menu is open, showing options for iOS, Android, and Windows. Under the Android section, 'Google Play App' is highlighted with a red box. Other options include 'Enterprise App for Android' and 'Private App for Android Enterprise'.

The screenshot shows the Google Play Store interface for the Samsung Email app. The app details page is displayed, showing the app name 'Samsung Email', the developer 'Samsung Electronics Co., Ltd.', and the release date 'April 4, 2019'. The app is categorized as 'Productivity'. A prominent red 'APPROVE' button is visible. Below the button, there are two informational icons: a download icon indicating 'This app offers managed configuration' and an information icon indicating 'This app is only available in certain countries'. The 'Add App' section shows two options: 'Add via Managed Google Play Store' (selected) and 'Add via Public Google Play'. Below this, a search bar contains the text 'samsung email'. At the bottom, a row of app icons is shown, including Samsung Email, Gmail, Microsoft Outlook, Blue Mail - Email, and Email - Fast & Secure.

Managed Google Play Configuration

- You will now see the apps you approved imported into the App Catalog.
- Now we have imported the app, next we need to assign it to our users.
- Select the Distribute button under the app you wish to distribute and select a relevant group of users and Click **Distribute**.

The screenshot shows the IBM MaaS360 interface. At the top, there's a navigation bar with 'HOME', 'DEVICES', 'USERS', 'SECURITY', 'APPS', and 'DOCS'. Below this is the 'App Catalog' section with a table of apps. The 'Samsung Email' app is highlighted, and a 'Distribute App: Samsung Email' dialog box is open over it. The dialog box has a 'Target' section with two dropdown menus: 'Group' and 'AE Work Profile'. Below that are checkboxes for 'Send Notification' and 'Send Email'. At the bottom of the dialog are 'Cancel' and 'Distribute' buttons.

App ...	Name	Type	Categ...	Instal
	Samsung Email View Distribute Delet...		PRODUCTIVITY	less than 10
	GoToMeeting – Video Conferencing & Online... View Distribute Delet...		BUSINESS	less than 10
	QR code reader / QR Code Scanner View Distribute Delet...		TOOLS	less than 10
	Knox Service Plugin View Distribute Delet...		BUSINESS	less than 10

Yes	No	No	06/12/2019 06:26 BS T	2.16.2.4
Yes	No	Yes <td>06/12/2019 06:26 BS T<td>3.0.7</td></td>	06/12/2019 06:26 BS T <td>3.0.7</td>	3.0.7
Yes	No	Yes <td>06/12/2019 06:26 BS T<td>1.1.19</td></td>	06/12/2019 06:26 BS T <td>1.1.19</td>	1.1.19

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 IBM MaaS360, follow the below instructions.

- Navigate to **Apps Catalog** and choose **More->Edit App Configurations** for the app you wish to send down a configuration for.
- Configure the relevant settings for your app

The screenshot shows the IBM MaaS360 interface. At the top, there is a navigation bar with 'HOME', 'DEVICES', 'USERS', 'SECURITY', 'APPS', 'DOCS', 'REPORTS', and 'SETUP'. Below this is the 'App Catalog' section. A table lists several apps: Samsung Email, GoToMeeting - Video, QR code reader / QR, Knox Service Plugin, and Gmail. The 'Samsung Email' app is selected, and a context menu is open over it. The menu items are: 'App Distribution & Installation Details', 'Manage Distributions', 'Add App to Bundle', and 'Edit App Configurations'. The 'Edit App Configurations' option is highlighted with a red box. To the right, a modal window titled 'App Configurations - Samsung Email' is open. It contains a note: 'Note: Settings defined in this section are applicable only to devices enrolled with Android enterprise. App configurations of type bundle Array are supported on Android 6.0+ only'. Below the note, there is a section for 'Exchange ActiveSync accounts list' with a plus icon. Underneath, there are four input fields: 'Email address: Email address', 'User name: User name (login) to access account', 'Account password: Account password', and 'EAS domain: Domain to access EAS server'. At the bottom of the modal, there are 'Cancel' and 'Save' buttons.

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 advanced options such as Dual DAR)]

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



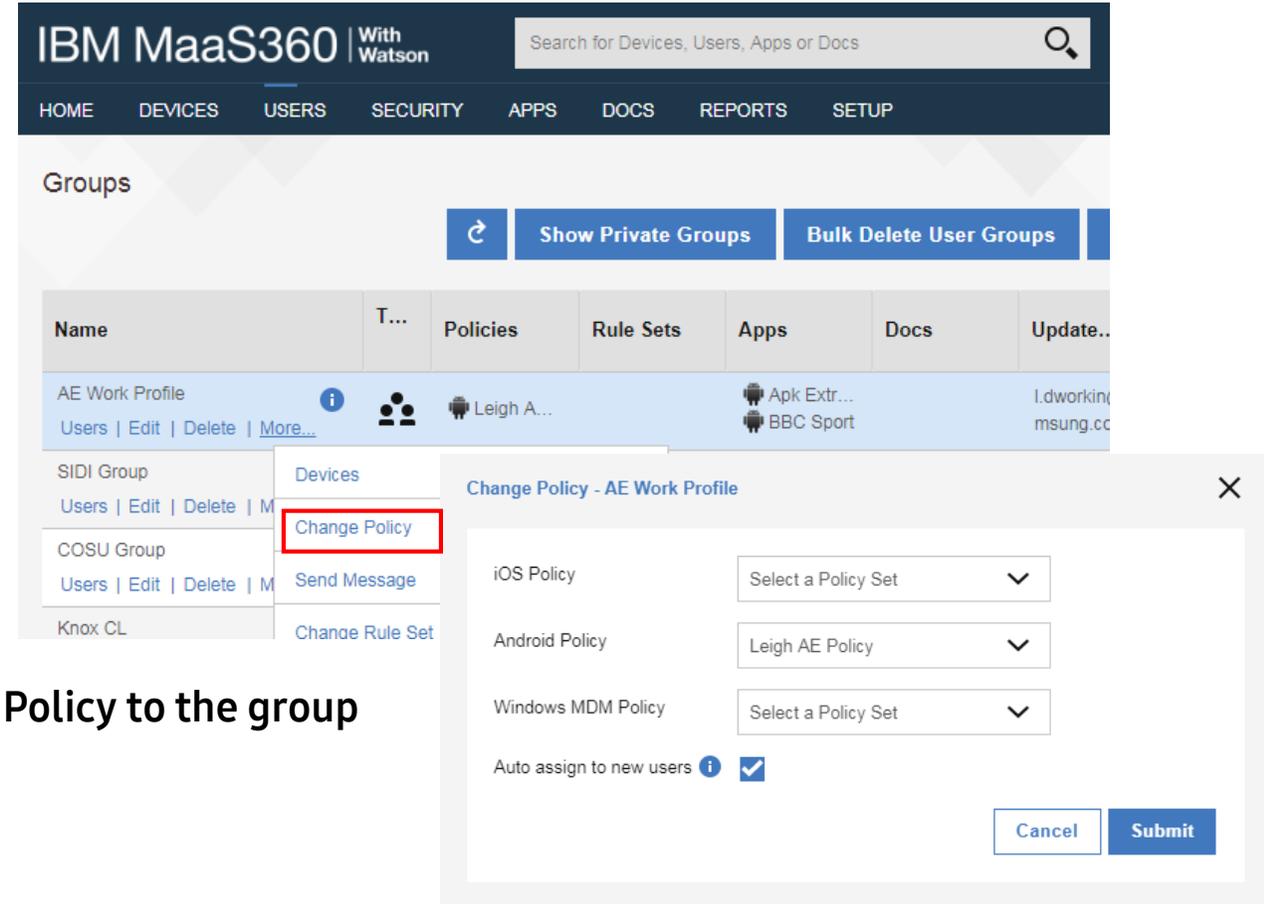
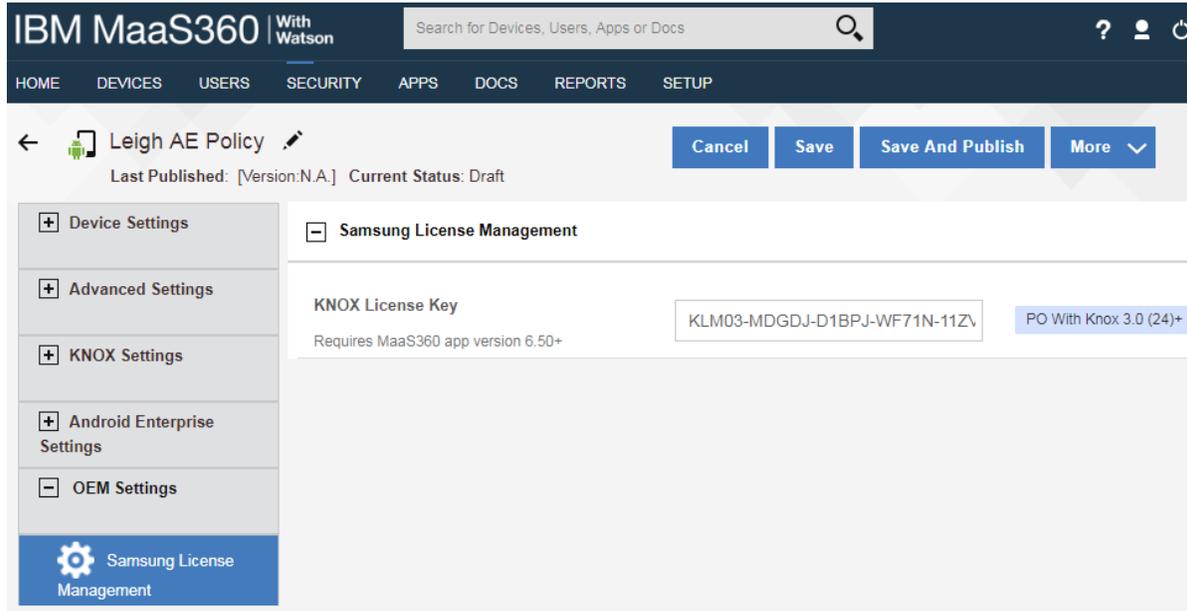
Configure KPE : Standard Edition on IBM MaaS360

- This is on by default with Android Enterprise on a Samsung Device

Knox Platform for Enterprise : Premium Edition

IBM MaaS360 fully supports Knox Platform for Enterprise Premium Edition.
It does this by just adding in a Knox license key.

- Simply add the Knox license key to OEM Settings->Samsung License Management and Save



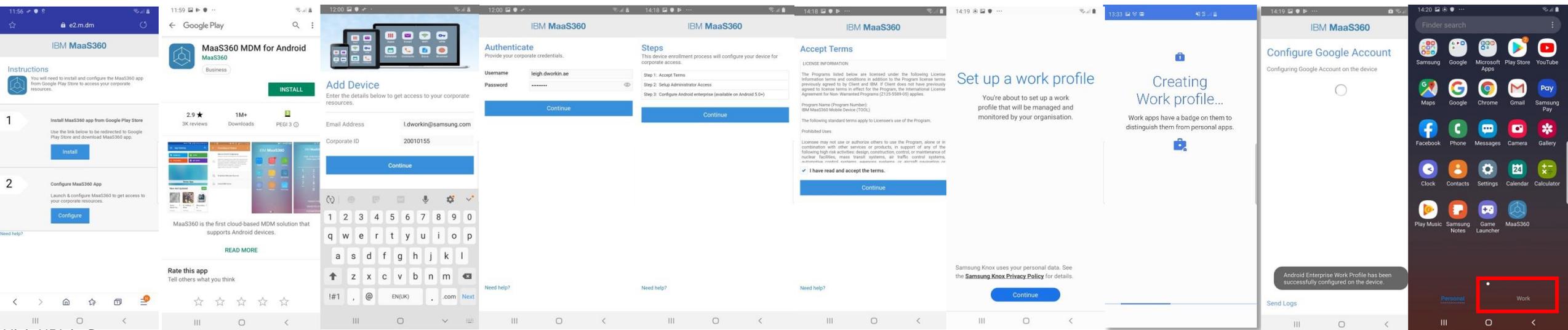
- Then in Users->Groups choose More... and assign the new Policy to the group

Knox Platform for Enterprise : Premium Edition

Android Enterprise BYOD Deployment with a KPE license key policy

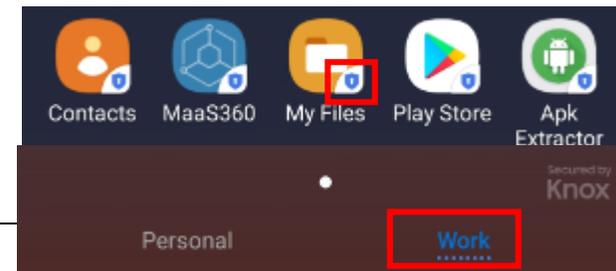
Now all you simply need to do is enroll your device by completing the following:

- On your device, go to the Google Play Store, download the IBM MaaS360 agent, and enroll your device into your tenant.
- Alternatively, in a browser on the device, visit the URL from the Email invitation for the device:



Visit URL in Samsung Browser from Email invitation. Click Install Install MaaS360 agent from Google Play Store Check email and hit Continue Enter user credentials & hit Continue Review Steps & hit Continue Accept terms and conditions Click Continue to create Work Profile Creating Work Profile Device Enrollment Successful! Work Tab Created

*You can also enroll your device using the alternative IBM MaaS360 methods. For example QR Code.



What to look out for in the Work Tab

Knox Service Plugin [KSP]

IBM MaaS360 fully supports Knox Service Plugin.

IBM MaaS360 | With Watson

Search for Devices, Users, Apps or Docs

HOME DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

App Catalog

<input type="checkbox"/>	App ...	Name	Type	Categories	Installs and Pendin...	Distributi...
<input type="checkbox"/>		Knox Service Plugin View Distribute Delete More...		BUSINESS	less than 10 	Yes

Distribute App: Knox Service Plugin

Target

Group AE Work Profile

Send Notification Send Email

Secured by Knox

IBM MaaS360 fully supports Knox Service Plugin.

The screenshot shows the IBM MaaS360 interface. At the top, there is a navigation bar with 'HOME', 'DEVICES', 'USERS', 'SECURITY', 'APPS', 'DOCS', 'REPORTS', and 'SETUP'. Below this is the 'App Catalog' section, which lists several applications. The 'Knox Service Plugin' is highlighted, and a context menu is open over it, with 'Edit App Configurations' selected and highlighted with a red box. To the right, a modal window titled 'App Configurations - Knox Service Plugin' is displayed. It contains a note about settings applicability, a 'Profile Name' field with the value 'Knox profile', a 'KPE Premium License key' field with the value 'KLM09-HHKHE-7ZF8A-AJDFT-O4WW7-QYHMX', and a 'Verbose mode' dropdown menu set to 'No'. At the bottom of the modal are buttons for 'Cancel', 'Reset to Defaults', 'Check for Settings', and 'Save'.

App ...	Name
	Knox Service Plugin View Distribute Delete More...
	GoToMeeting – Video View Distribute Delete
	QR code reader / QR View Distribute Delete
	Gmail View Distribute Delete
	Apk Extractor

App Configurations - Knox Service Plugin

Note: Settings defined in this section are applicable only to devices enrolled with Android enterprise. App configurations of type bundle Array are supported on Android 6.0+ only

For native applications such as Gmail or Chrome app, settings under this section will override any settings configured on policies such as Browser Settings or Exchange Active Sync for Android Enterprise enrolled devices.

Profile Name: You can enter a profile name for readability and ease of tracking and debugging, if needed. This is an optional field and will not result in any errors.

KPE Premium License key: Enter your license key if you are using any premium Knox policy. You can skip this if your UEM supports Knox licenses. This is not applicable, if you are using BlackBerry.

Verbose mode: Enable this to see policy result and errors on the device. Recommend to enable this only during your testing and not in final deployment.

Device policies (Device Owner): Group of

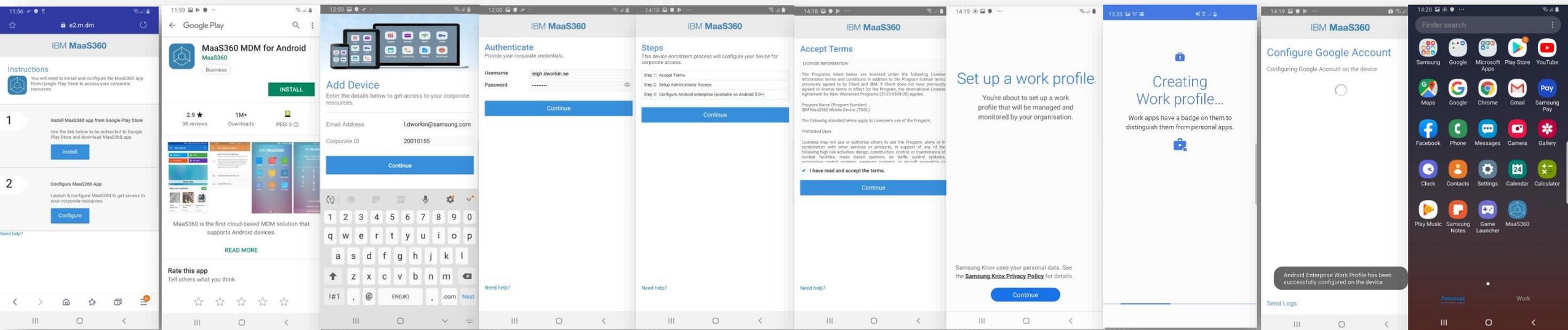
[Cancel](#) [Reset to Defaults](#) [Check for Settings](#) [Save](#)

Android Enterprise: KSP

Android Enterprise BYOD Deployment with Knox Service Plugin

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 IBM MaaS360 agent, and enroll your device into your tenant.
- Alternatively, in a browser on the device, visit the URL from the Email invitation for the device:



Visit URL in Samsung Browser from Email invitation. Click Install

Install MaaS360 agent from Google Play Store

Check email and hit Continue

Enter user credentials & hit Continue

Review Steps & hit Continue

Accept terms and conditions

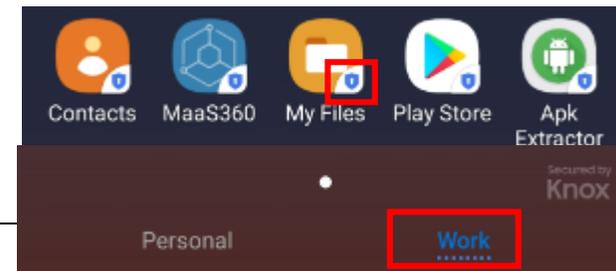
Click Continue to create Work Profile

Creating Work Profile

Device Enrollment Successful!

Work Tab Created

*You can also enroll your device using the alternative IBM MaaS360 methods. For example QR Code.



What to look out for in the Work Tab

Document Information

This is version 3.0 of this document.

Thank you!

