



IBM MaaS360

&

Knox Platform for Enterprise

July 2022

Samsung R&D Centre UK
(SRUK)

Agenda

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

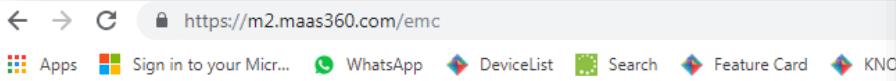
Trial Access:

<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>



IBM MaaS360

Log into IBM MaaS360

Username

Continue

Remember Me

Forgot Username or Password?

Not a customer?

Try For FREE

IBM MaaS360

Log into IBM MaaS360

i.dworkin@samsung.com

.....

Log In

Forgot Username or Password?

IBM MaaS360 | With Watson

HOME DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

Devices + 57

Users + 9

Apps + 7

Docs + 0

My Alert Center

Last Analyzed: Friday, May 24, 2019 9:59:24 AM BST

0 Recently Added	0 No Passcode	0 Jailbroken or Rooted
0 Out of Compliance	0 Roaming	0 Email/VPN/Wi-Fi Configuration Failure
57 Long Inactivity		

A Gmail account to map to MaaS360 for Managed Google Play

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

The image shows a composite of three screenshots illustrating the process of mapping a Gmail account to MaaS360 for Managed Google Play.

Screenshot 1: Google Play Work Profile Setup

This screenshot shows the "Google Play" interface with the "Work" profile selected. The sidebar on the left includes options like "My managed apps", "Shop", "Updates", and "Help Centre". The main area displays "Featured Work Apps" with icons for CamScanner, WPS Office + PDF, and Slack. Below this, the "Works With G Suite" section lists "Apps for making work easier" with icons for Google Sheets, Google Slides, and Google Docs.

Screenshot 2: Google Sign-in

This screenshot shows the "Sign in" screen for Google. A user has entered their email address, "leighdworkin.maas360@gmail.com", into the "Email or phone" field. Below the field is a link "Forgot email?". Further down, there is a note "Not your computer? Use Guest mode to sign in privately." and a "Create account" button. To the right of the sign-in form is a "Next" button.

Screenshot 3: MaaS360 Managed App List

This screenshot shows the "My managed apps" section of the MaaS360 interface. It lists several apps that have been approved for management:

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

Configure Android Enterprise

- Log into Maas360 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

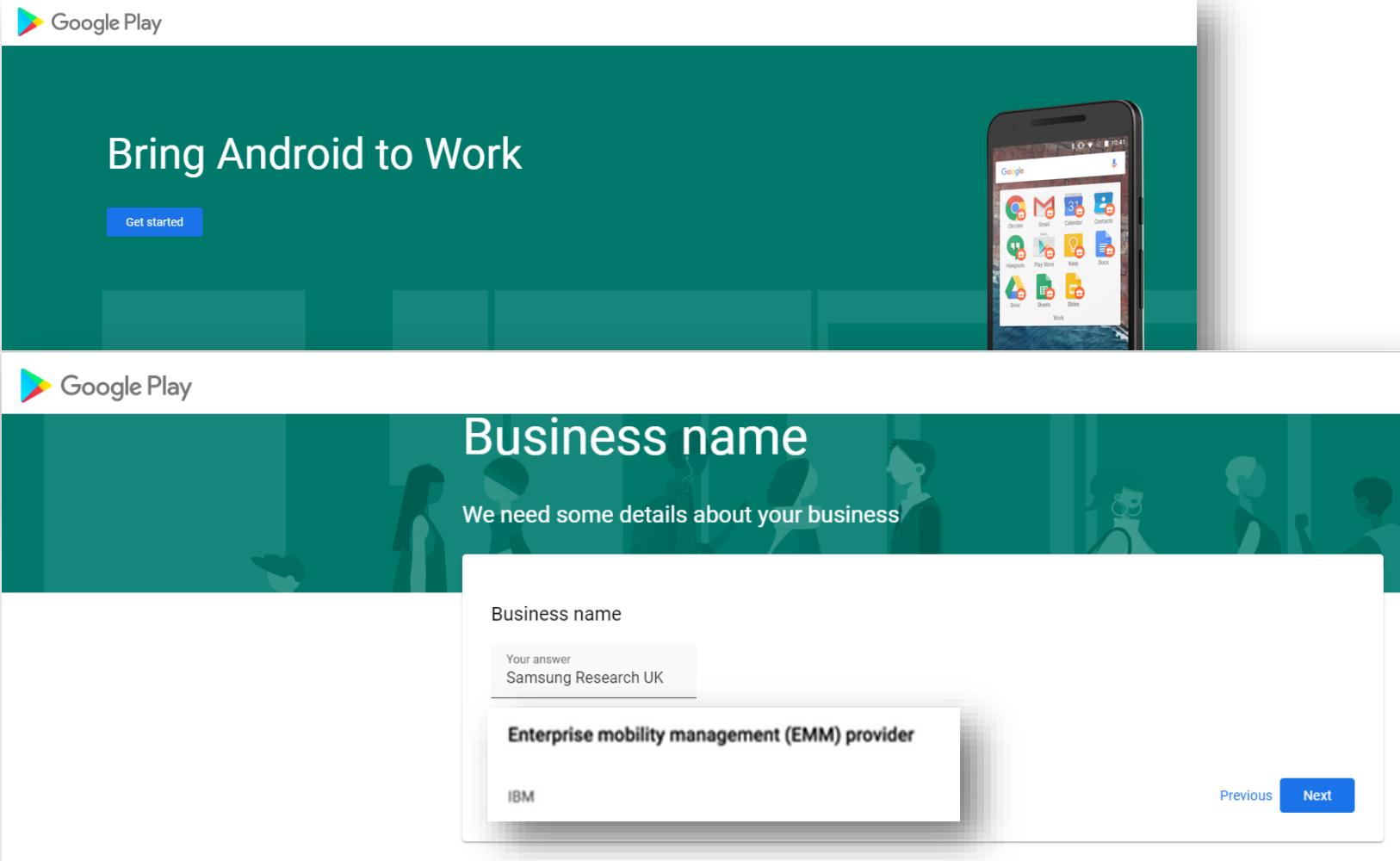
Import apps tied to your Android Enterprise account once approved on Google console. If you want to skip import now, uncheck the option and enable it later from [Apps > App Catalog > More > App Catalog Settings > Android Enterprise Settings](#).

Enable

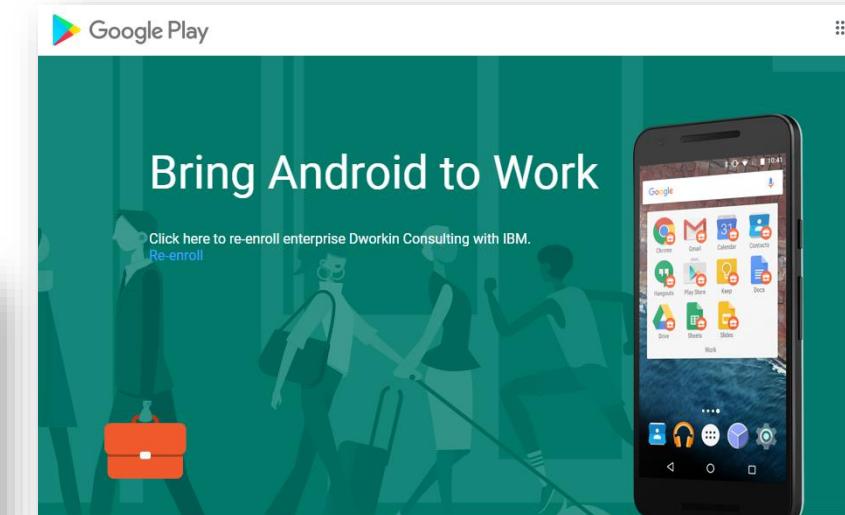
Configure Android Enterprise

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

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.

The image displays two screenshots of the Google Play Admin interface. The left screenshot shows the 'Contact details' page, which asks for contact information about key contacts. It includes fields for a Data Protection Officer (Name, Email, Phone) and an EU Representative (Name, Email, Phone). A note states that Google must maintain contact details for a customer data protection officer and an EU representative. The right screenshot shows a 'Set up complete' confirmation screen with a 'Complete Registration' button.

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 Confirm

Google Play

Set up complete

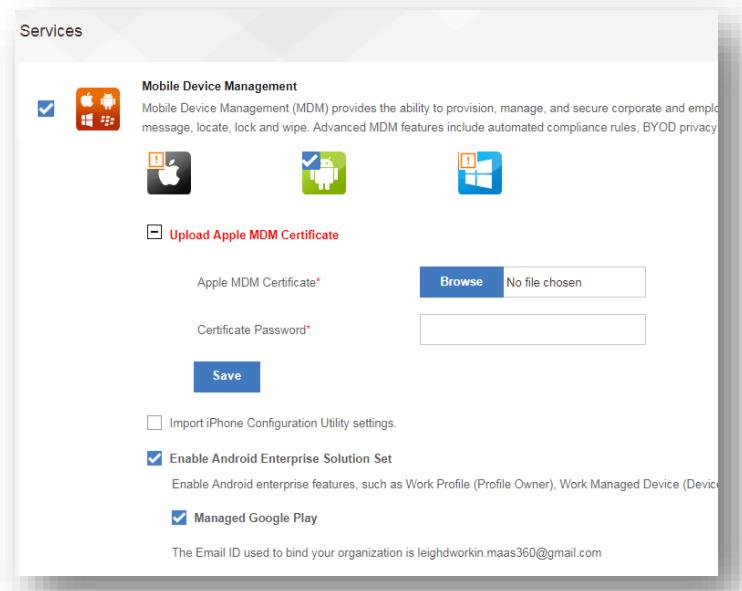
Thanks for choosing Android enterprise.

Complete Registration

Configure 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

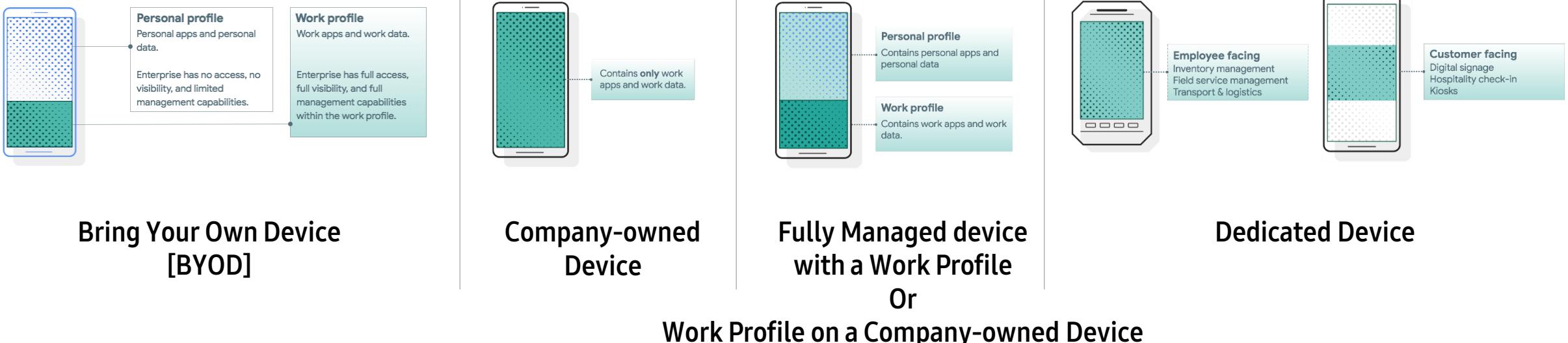
Deployment Modes

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*]

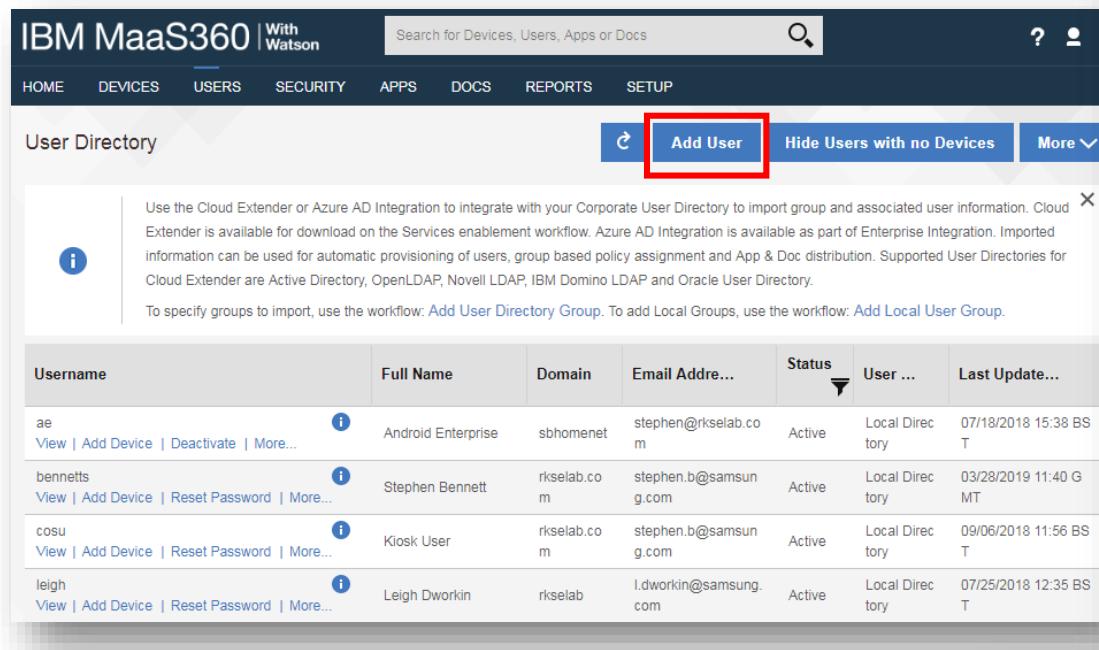
IBM MaaS360 can support 4 of these 5 of these deployment modes, all but COMP. In this next section we will show you how to configure each of these 4 supported deployment modes in IBM MaaS360 for your device fleet.



Create a User in MaaS360

Create a User in MaaS360

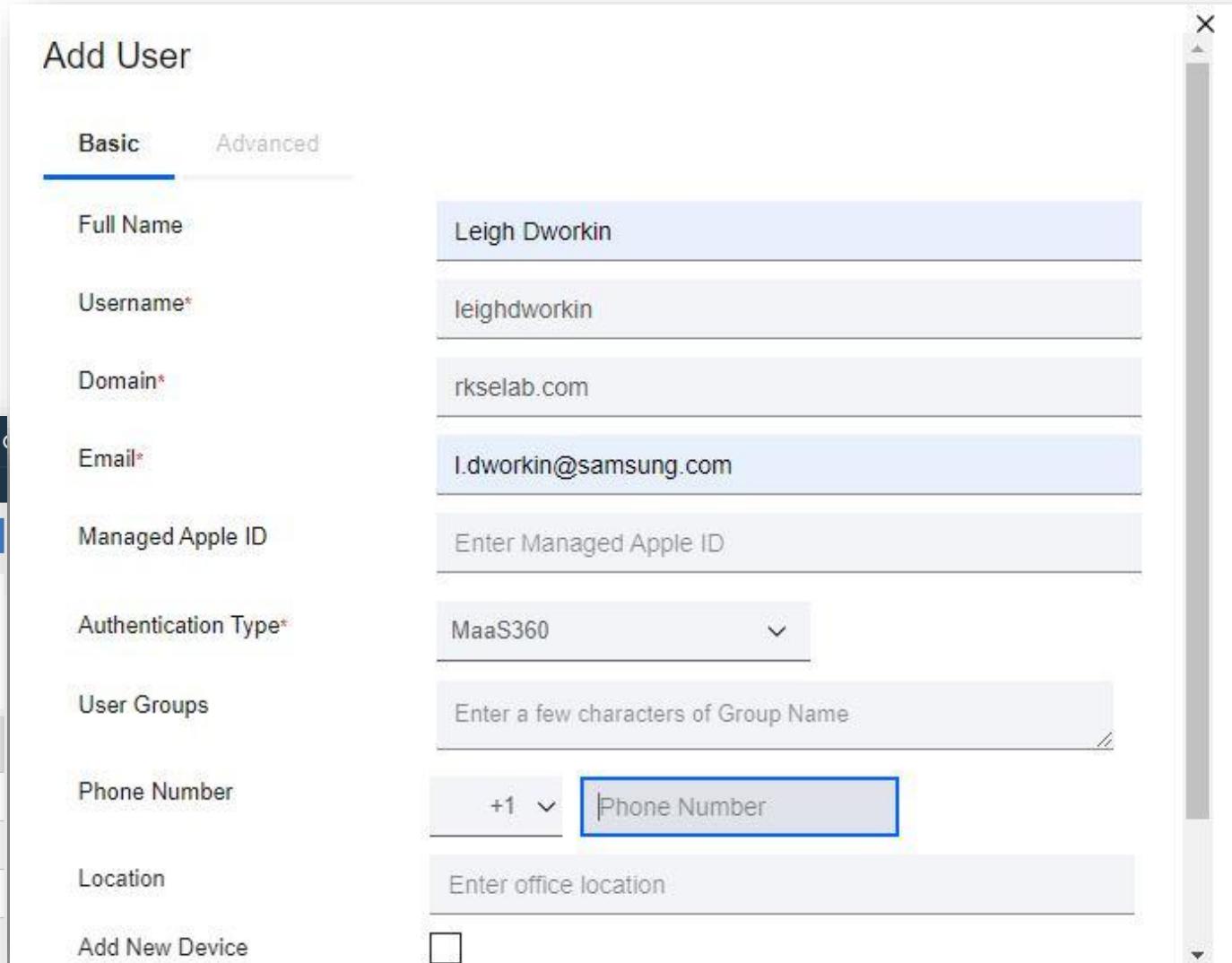
- Navigate to: **Users** and Click the **Add User** button
- Fill in all required fields and then click Save.



The screenshot shows the IBM MaaS360 interface. At the top, there's a navigation bar with links for HOME, DEVICES, USERS, SECURITY, APPS, DOCS, REPORTS, and SETUP. Below this is a search bar and a user profile icon. The main area is titled "User Directory". It features a table with columns: Username, Full Name, Domain, Email Address, Status, User ..., and Last Update... . There are four rows of data in the table. At the top of the table area, there are buttons for "Add User" (which is highlighted with a red box), "Hide Users with no Devices", and "More". A tooltip message about Cloud Extender and Azure AD Integration is displayed above the table. At the bottom of the table, there's a note about specifying groups to import.

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

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



The screenshot shows the "Add User" dialog box. It has two tabs: "Basic" (selected) and "Advanced". The "Basic" tab contains several input fields and dropdown menus:

- 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**:

 At the bottom of the dialog, there's a footer with links: "leigh.dworkin.ae", "View", "Add Device", "Reset Password" (which is highlighted with a red box), and "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

HOME DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

Groups

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

Search for Devices, Users, Apps or Docs

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

Jump To Page | Displaying 1 - 15 of 15 Records | Show 25 Records | Reset Filters | Customize Columns | CSV | Export

Add MaaS360 User Group

The User Group has been added successfully. You can manage this and issue Group Actions using the "Groups" workflow.

OK

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 * BYOD Work Profile

Usernames (or Email Addresses) leighdworkin (l.dworkin@samsung.com),

Description BYOD Work Profile or PO setup

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

Username	Full Name
ae	Android Ente
bennetts	Stephen Ben
cosu	Kiosk User
leigh	Leigh Dwork
leigh.ae	Leigh Dwork
leigh.dworkin.ae	Leigh Dworkin

Add Device

Basic Advanced

Device Addition Mode

Enroll using Android enterprise

Managed Google Play Account Type Device Account i User Account i

Account type once chosen cannot be changed later.

Username	leighdworkin
Domain	rkselab.com
Email	l.dworkin@samsung.com
Phone Number	+1 <input type="text"/> Phone Number
Notify User	<input checked="" type="checkbox"/> Email <input type="checkbox"/> SMS
Copy Email	<input type="checkbox"/> Me <input type="text"/> Enter comma separated email

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>

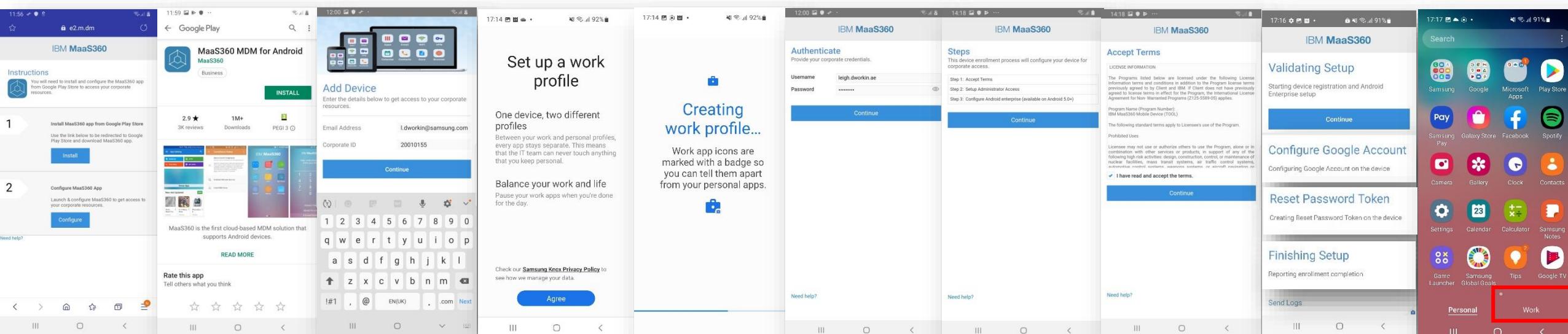
OK

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.
Install MaaS360 agent from Google Play Store
Click Install

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

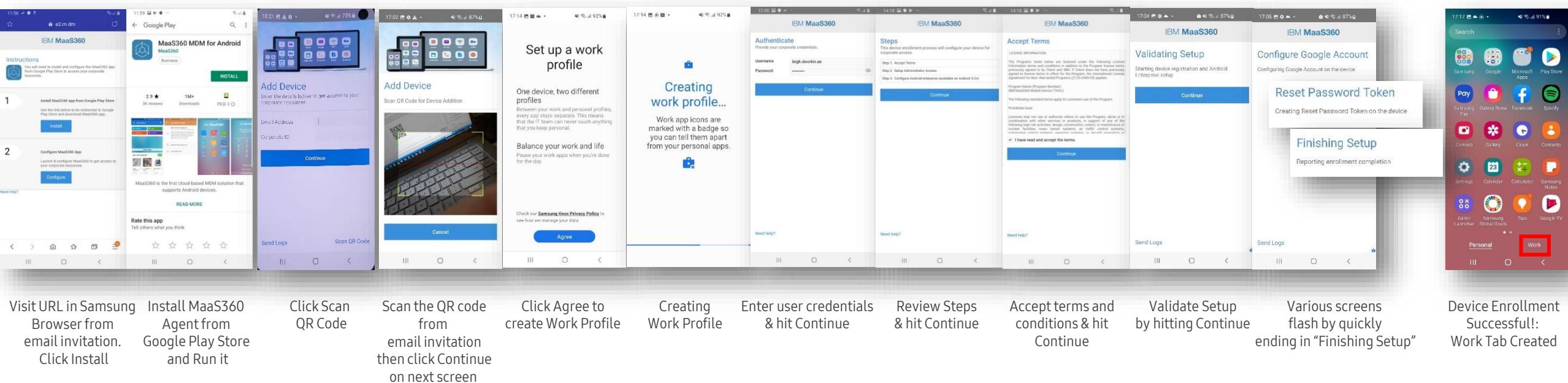
*You can also enroll your device using the alternative IBM MaaS360 methods. For example QR Code – see next slide.

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

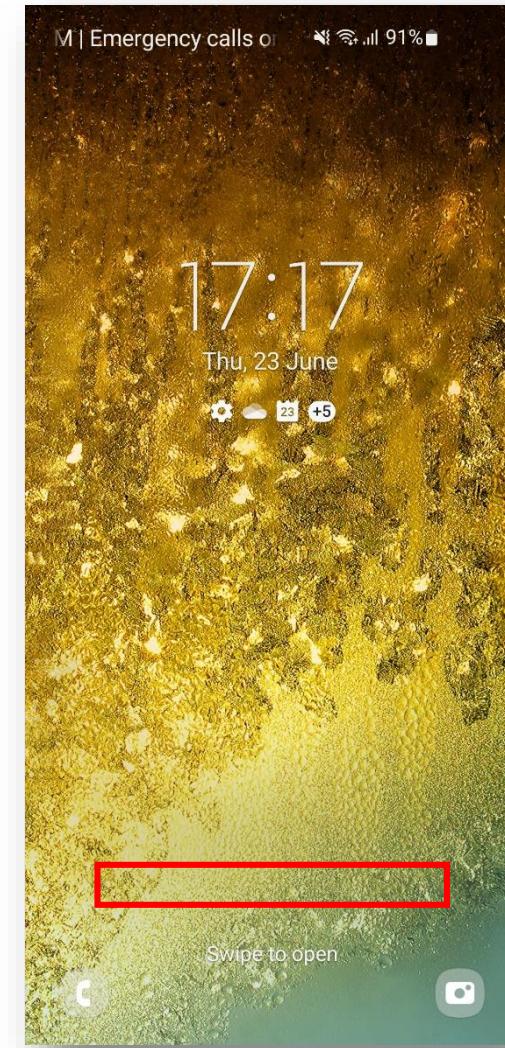
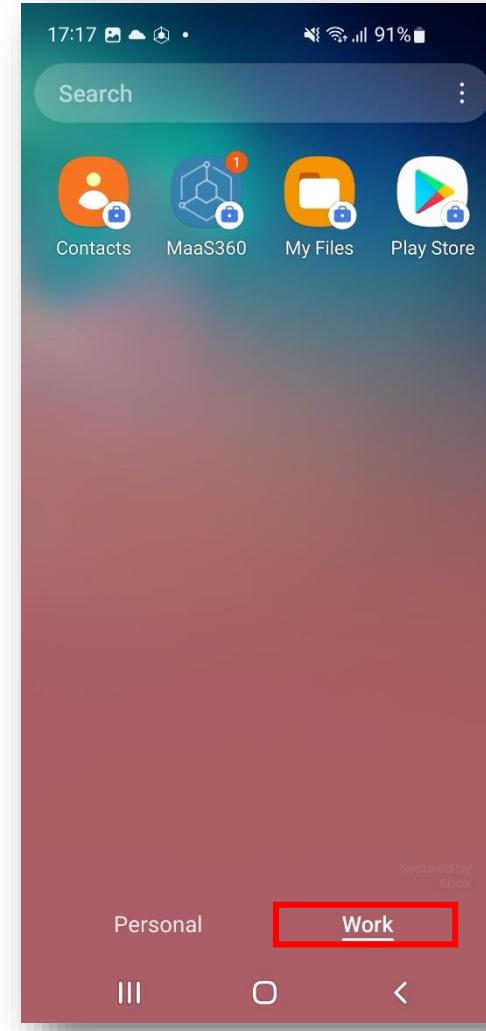
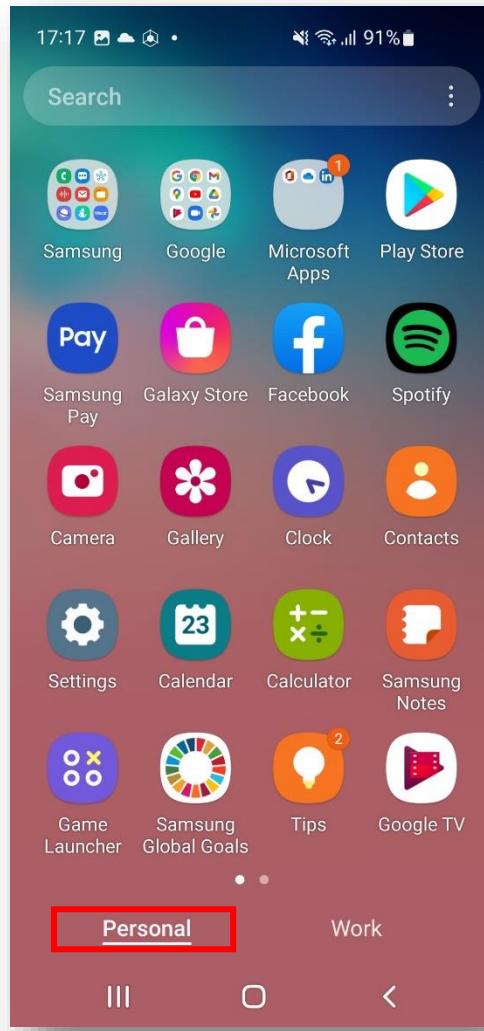
Validate Setup by hitting Continue

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:



No mention of device belonging
to your organization
on lock screen

Android Enterprise: Company-owned Device – DPC identifier

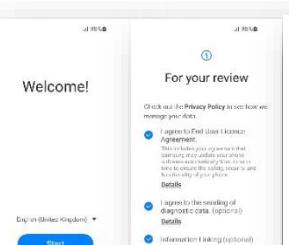
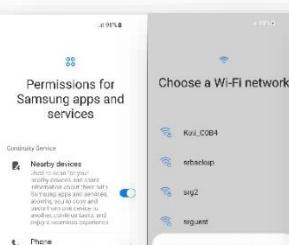
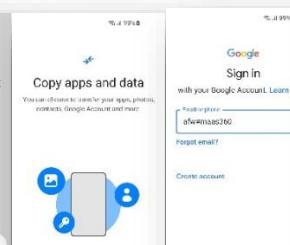
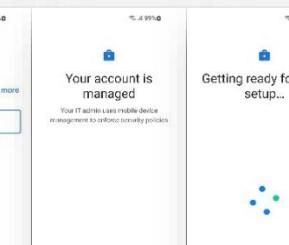
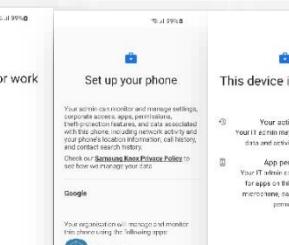
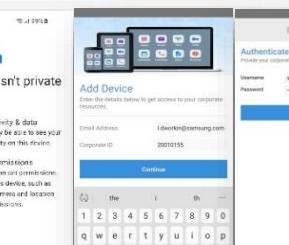
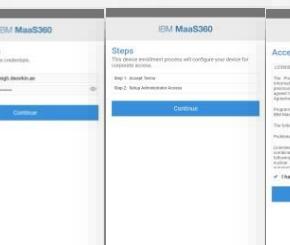
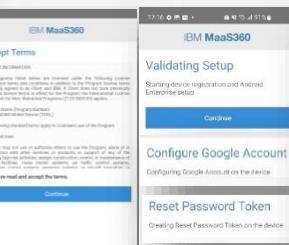


Android Enterprise Company-owned Device Deployment

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:

														
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 awf#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 Successful!

Android Enterprise: Company-owned Device - QR code

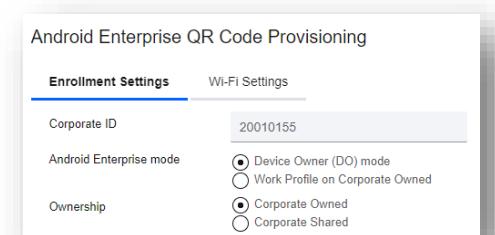
Android Enterprise Company-owned Device Deployment

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**

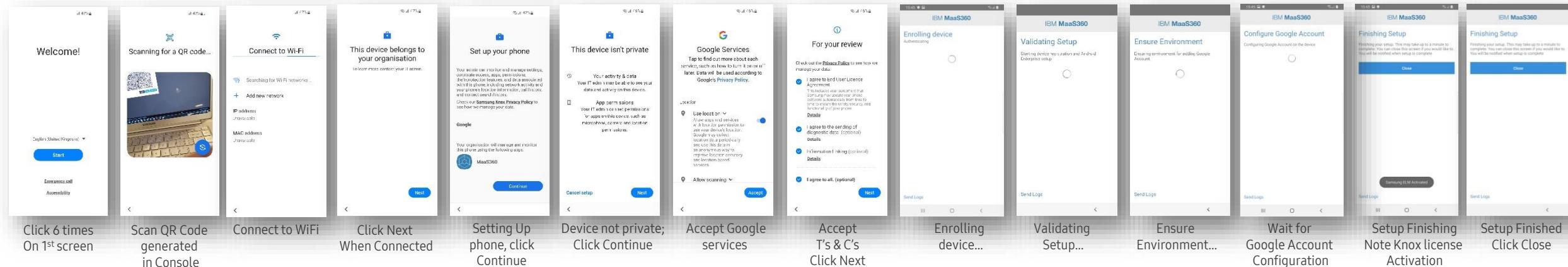
2. QR Code Enrollment / NFC Enrollment –

- 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 - KME

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 –

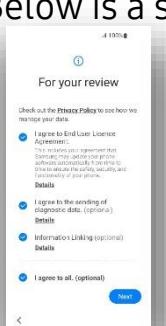
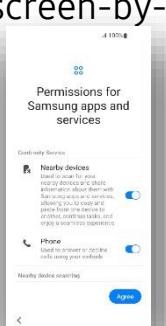
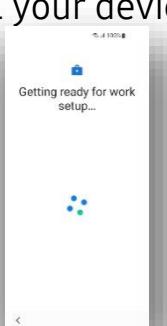
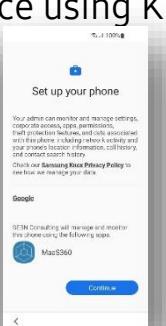
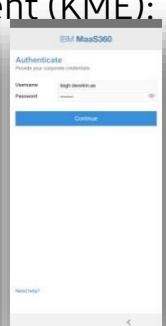
- scan QR code (MaaS360 Portal -> Devices -> Enrollments -> Other Enrollment Options -> Android Enterprise QR Code Provisioning)

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 -

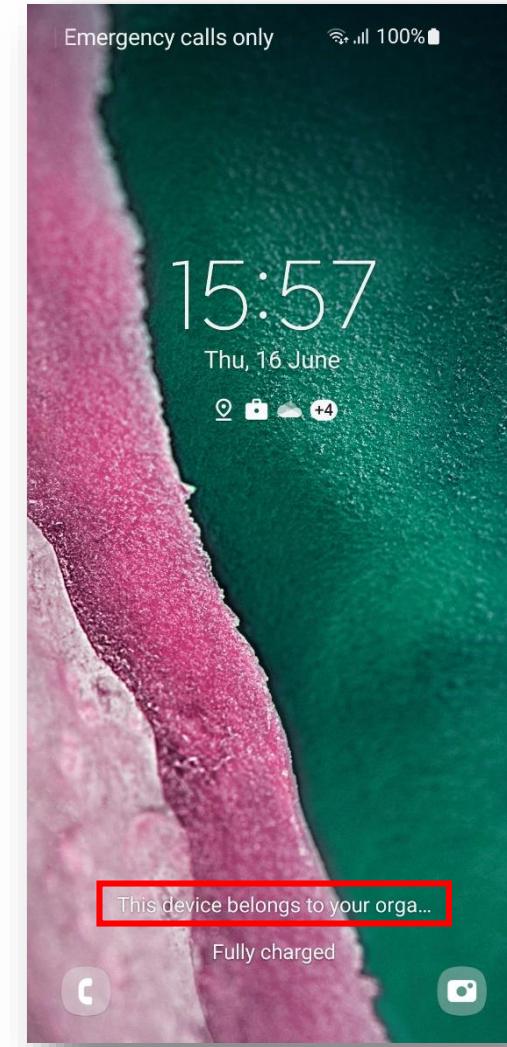
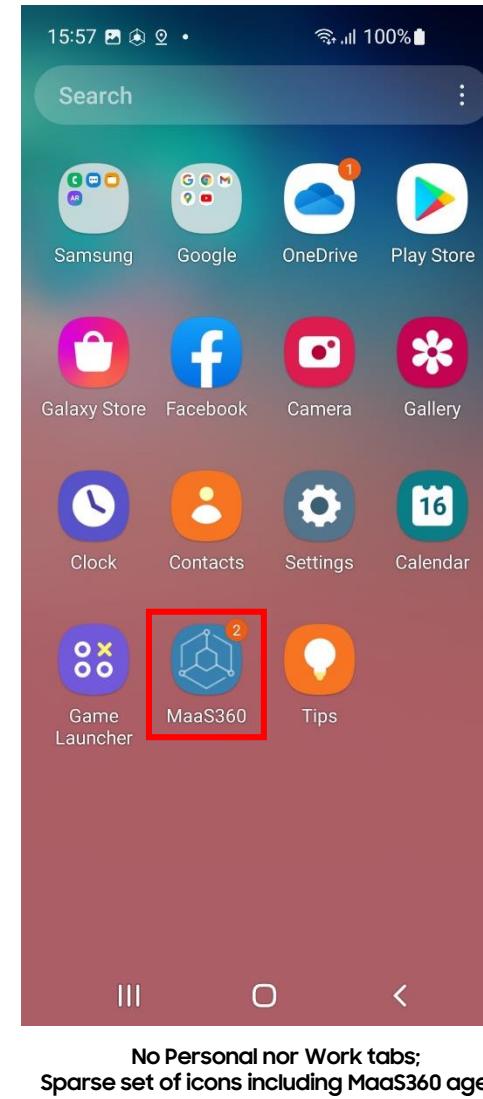
```
{"prompt_for_asset_tag":false,"disallow_enrollment_skipping":true,"enrollment_corp_id":"XXXXXXXX","enrollment_account_type":"userAccount","prompt_for_device_name":false,"ae_container_type":"WORK_ACTIVE_DEVICE","enrollment_username":"a.b@cccc.com","ae_enrollment_flow":"KME_ENROLLMENT","enrollment_email":"a.b@cccc.com","enrollment_ownership":"Corporate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

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

									
Click Start	Accept T's & C's Click Next	Agree to permissions for Samsung apps	Connect to Wi-Fi	Wait while KME updates	Get ready for work setup	Install MaaS360 MDM app by Clicking Continue	Device not private; Click Next	Enter email and Corporate ID	Enter Credentials

Android Enterprise: Fully Managed Device Enrollment

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



Android Enterprise: Fully Managed Device with a Work Profile

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)



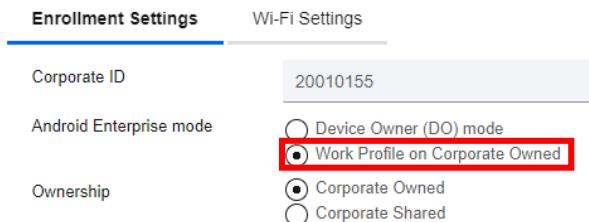
Android Enterprise Work Profile on a Company-owned Device Deployment

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:

Click 6 times On 1 st screen	Scan QR Code Generated in Console	Connect to Wi-Fi	Device is your organization's. Click Next	Setting Up Work Device	Set up Work Profile Click Agree	Creating Work Profile	Configure Google Account – Click Next	Skip personal Google Account setup	Google Services selection. More then Accept	Getting your phone ready...	Accept T's & C's, click Next

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 –

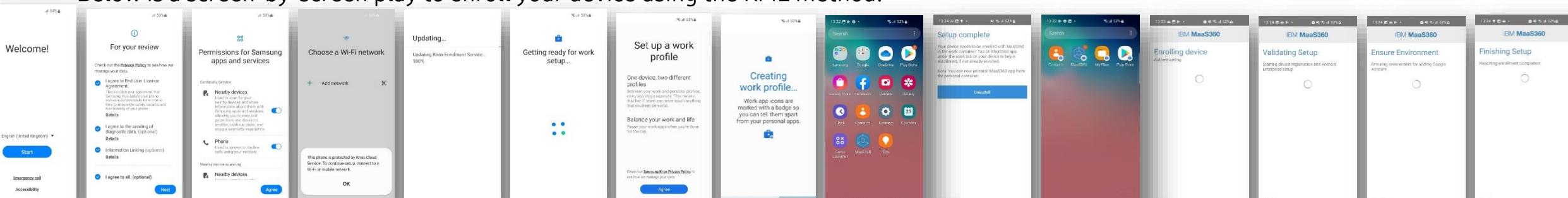
- scan QR code (MaaS360 Portal -> Devices -> Enrollments -> Other Enrollment Options -> Android Enterprise QR Code Provisioning)

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":"XXXXXXXXXX","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"}
```

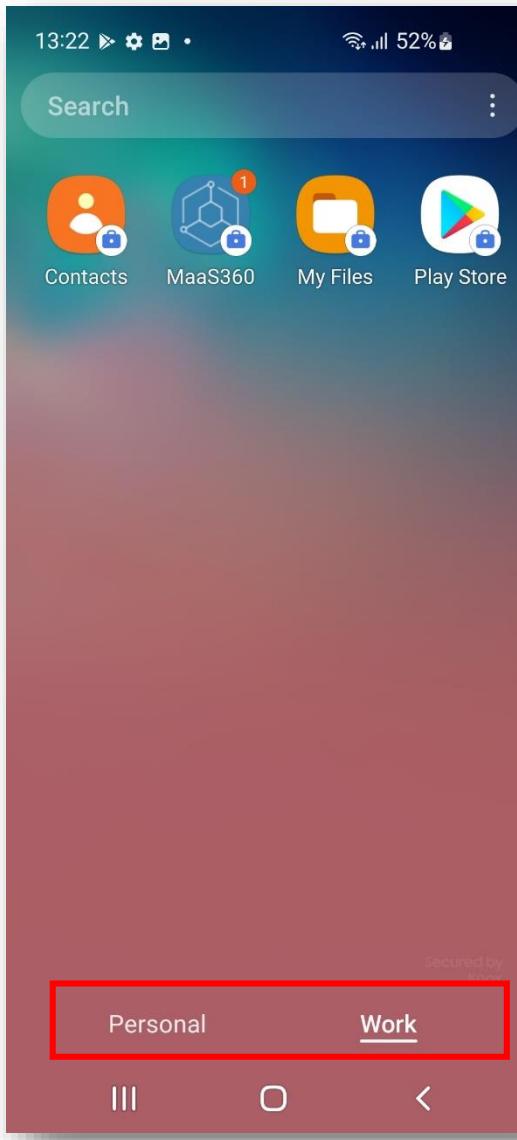
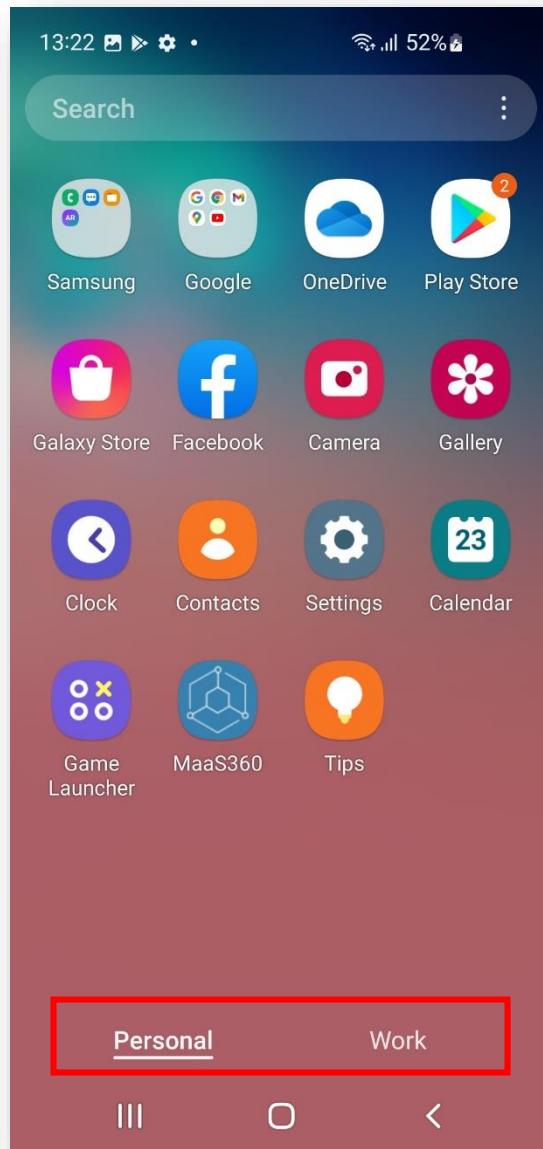
- Below is a screen-by-screen play to enroll your device using the KME method:



Click Start	Accept T's & C's, click Next	Agree to permissions for Samsung apps	Connect to WiFi	Wait while KME updates	Getting ready For work setup	Set up work profile; Click Agree	Creating Work Profile	Open MaaS360 agent in Personal profile	Uninstall MaaS360 in Personal profile	Open MaaS360 agent in Work profile	Enrolling Device...	Validating Setup...	Ensure Environment...	Finishing Setup!
-------------	------------------------------	---------------------------------------	-----------------	------------------------	------------------------------	----------------------------------	-----------------------	--	---------------------------------------	------------------------------------	---------------------	---------------------	-----------------------	------------------

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



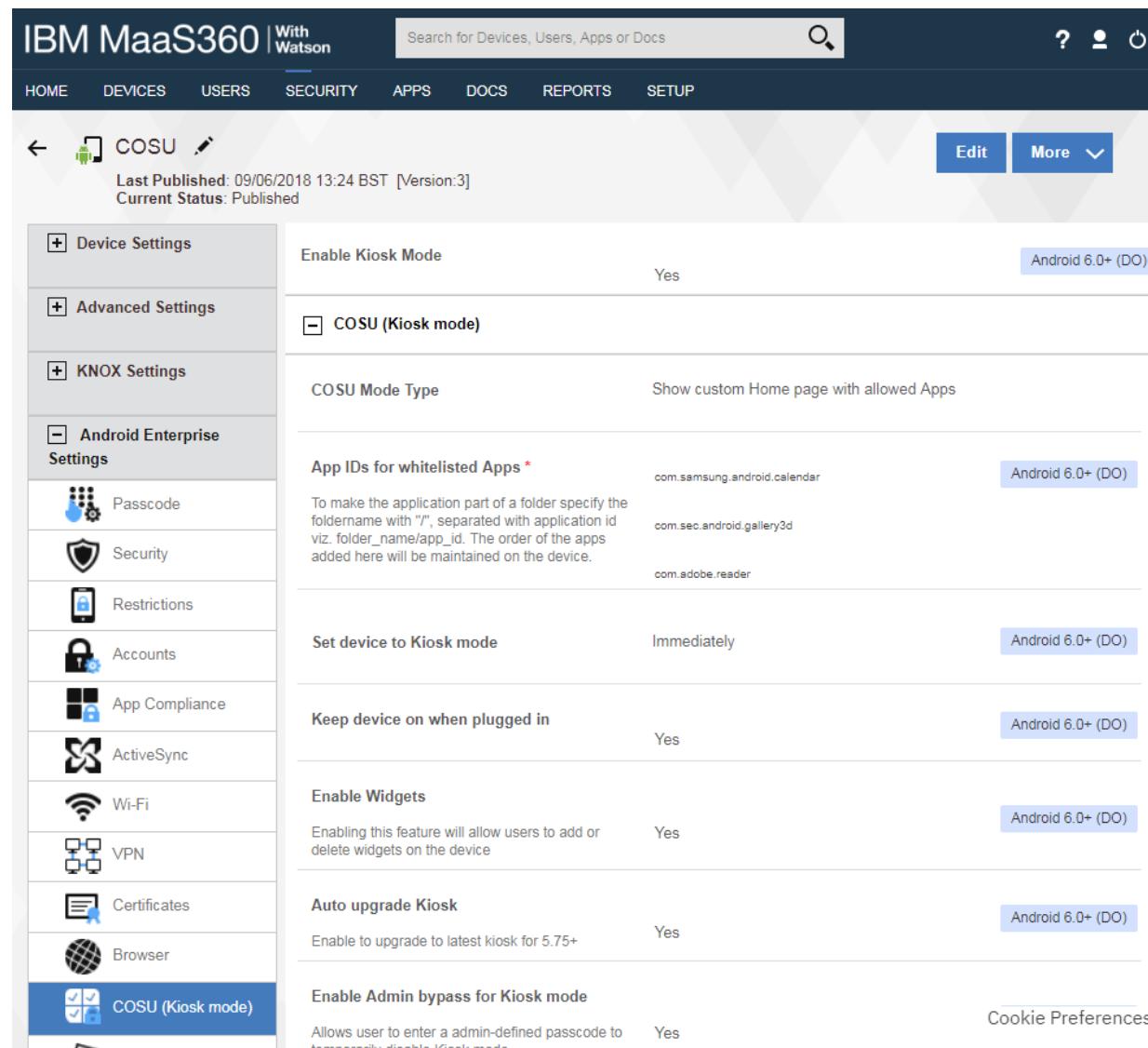
Android Enterprise Dedicated Device Deployment

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 interface with the title "IBM MaaS360 | With Watson". The navigation bar includes HOME, DEVICES, USERS, SECURITY, APPS, DOCS, REPORTS, and SETUP. A search bar at the top right contains the placeholder "Search for Devices, Users, Apps or Docs". On the left, a sidebar lists various settings under "Android Enterprise Settings", including Device Settings, Advanced Settings, KNOX Settings, and a expanded section for "Android Enterprise Settings" which includes Passcode, Security, Restrictions, Accounts, App Compliance, ActiveSync, Wi-Fi, VPN, Certificates, Browser, and COSU (Kiosk mode). The main content area displays the "cosu" policy, last published on 09/06/2018 at 13:24 BST [Version:3] and currently Published. It includes the following configuration options:

Setting	Value	Notes
Enable Kiosk Mode	Yes	Android 6.0+ (DO)
COSU Mode Type	Show custom Home page with allowed Apps	
App IDs for whitelisted Apps *	com.samsung.android.calendar com.sec.android.gallery3d com.adobe.reader	Android 6.0+ (DO)
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)
Auto upgrade Kiosk	Yes	Android 6.0+ (DO)
Enable Admin bypass for Kiosk mode	Yes	Cookie Preferences

Android Enterprise: Dedicated Device (COSU)

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.

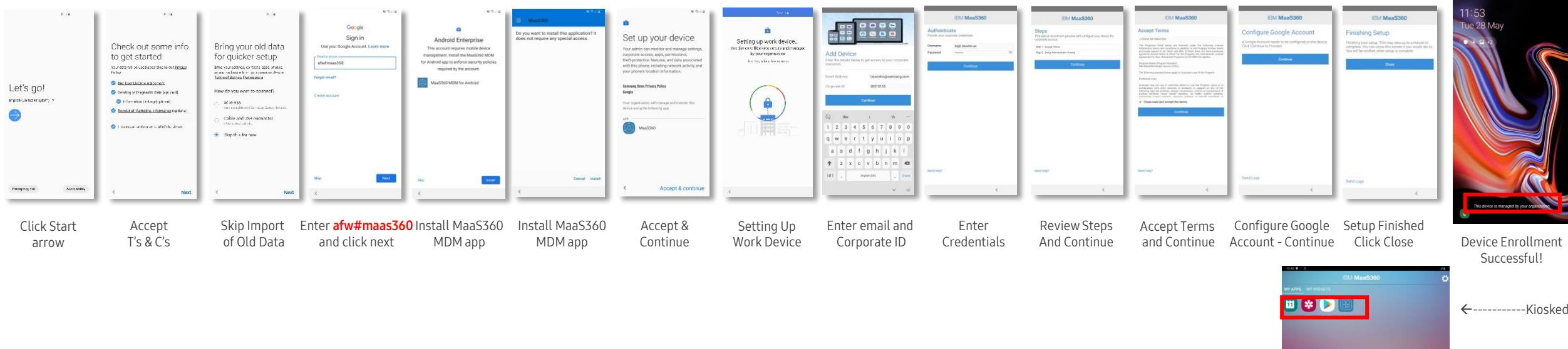
1. DPC Identifier [Also known as the hashtag method] **afw#maas360**

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:

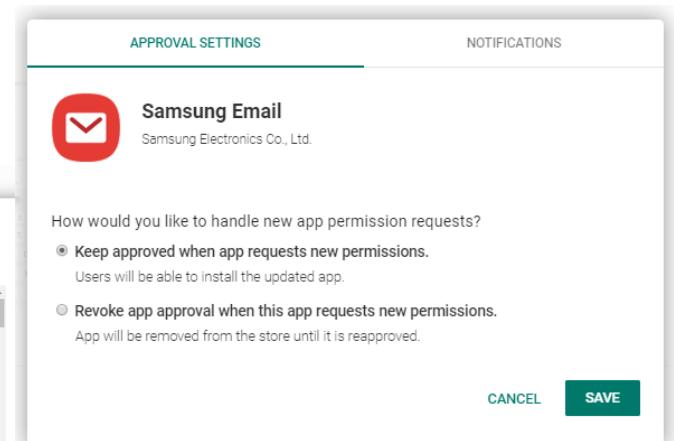
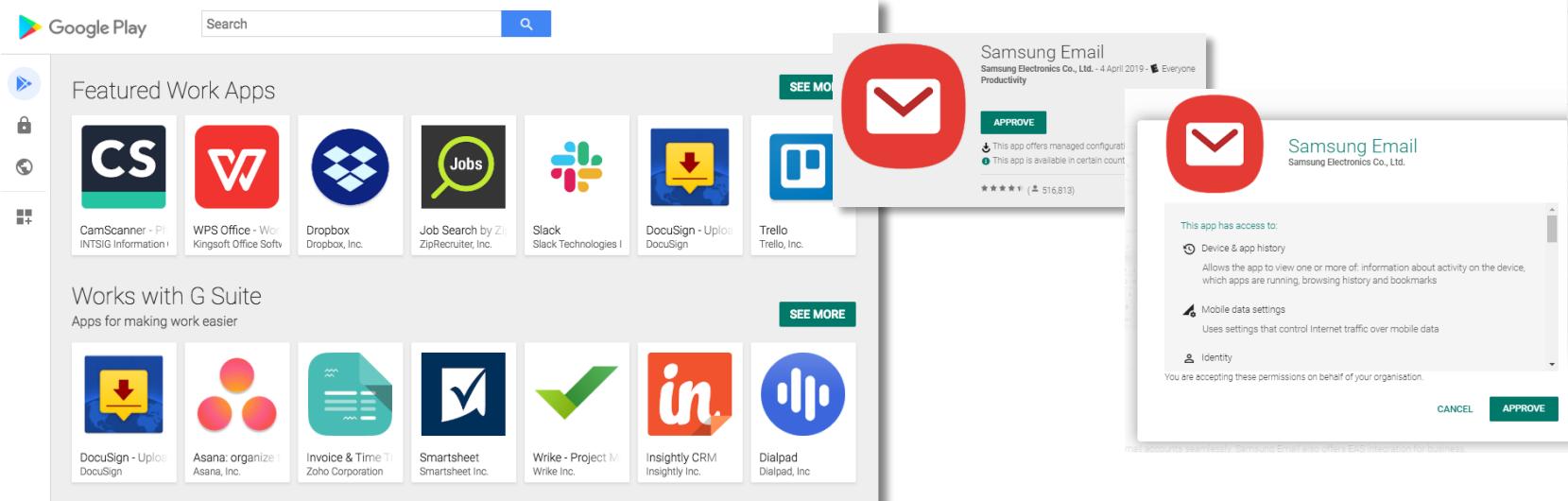


Managed Google Play Configuration

Managed Google Play Configuration

In the Configuring Android Enterprise section of this document, we completed the majority of the work needed to configure applications to be used for Managed Google Play. All we have left to do is the following:

- 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

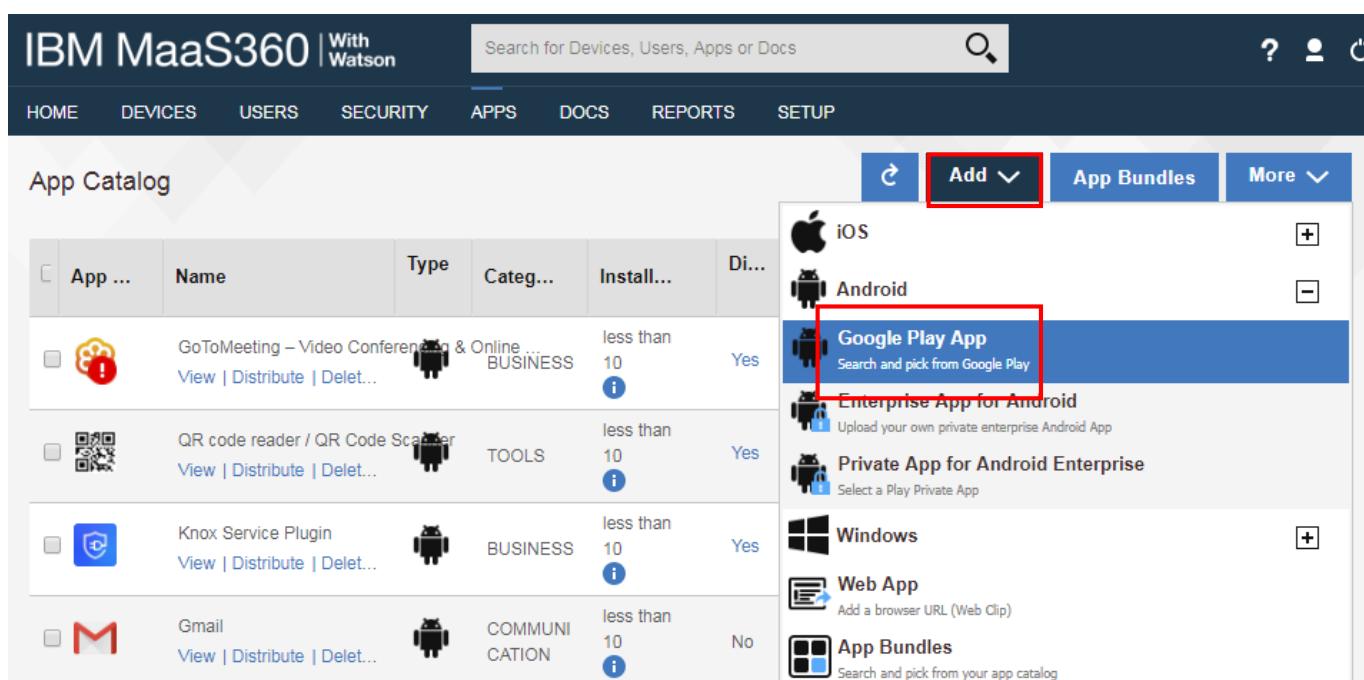


Managed Google Play Configuration

Managed Google Play Configuration

Now we have approved an application we would like to distribute in IBM MaaS360.

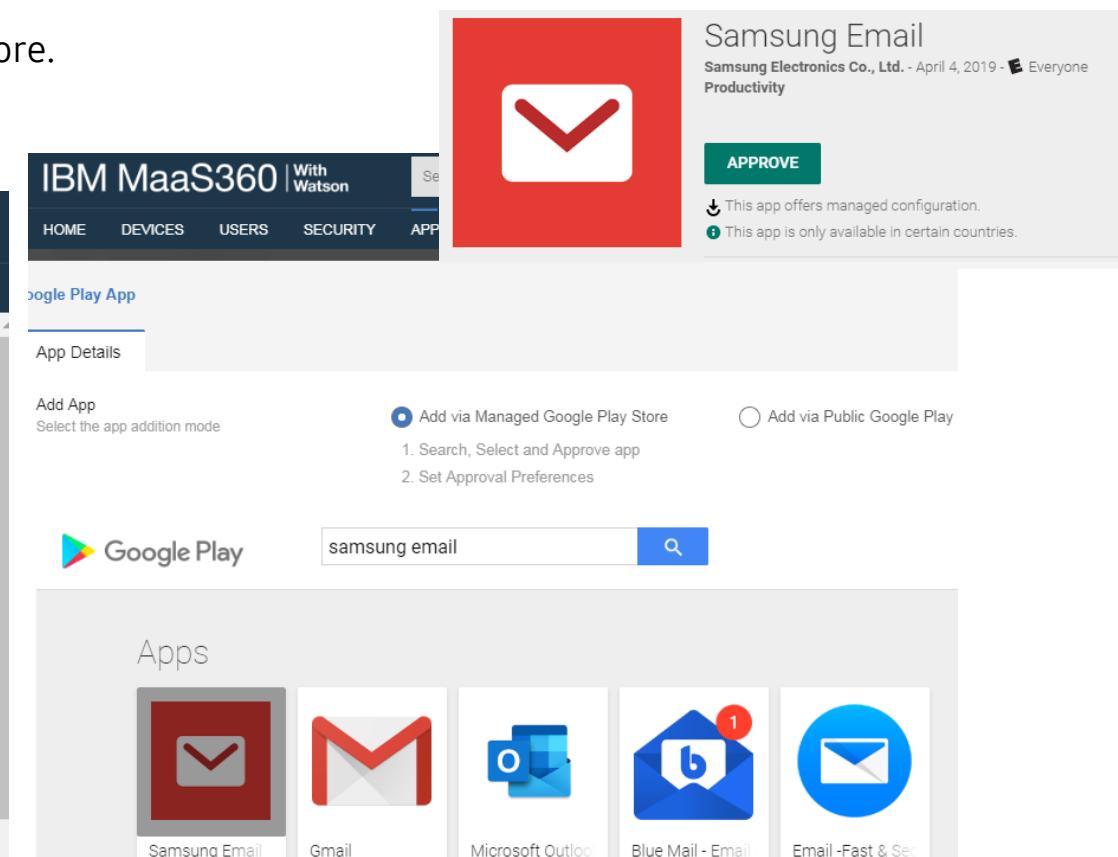
- Log in to your IBM MaaS360 Console and navigate to the tenant you have configured Android Enterprise
- Navigate to APPS->Catalog and click Add->Android->Google Play App
- Click Add via Managed Google Play Store
- Select the Samsung Email app we approved in our Managed Google Play Store.
- Click APPROVE



The screenshot shows the IBM MaaS360 console interface. At the top, there's a navigation bar with links for HOME, DEVICES, USERS, SECURITY, APPS (which is currently selected), DOCS, REPORTS, and SETUP. Below this is a search bar labeled "Search for Devices, Users, Apps or Docs". The main area is titled "App Catalog" and contains a table with columns for App, Name, Type, Category, Install..., and Di... (partially visible). There are four rows of apps listed:

App	Name	Type	Category	Install...	Di...
	GoToMeeting – Video Conferencing & Online...	ANDROID	BUSINESS	less than 10	Yes
	QR code reader / QR Code Scanner	ANDROID	TOOLS	less than 10	Yes
	Knox Service Plugin	ANDROID	BUSINESS	less than 10	Yes
	Gmail	ANDROID	COMMUNICATION	less than 10	No

In the center, there's a dropdown menu with options: iOS, Android, Google Play App (which is highlighted with a red box), Enterprise App for Android, Private App for Android Enterprise, Windows, Web App, and App Bundles. Above this dropdown is a large blue button labeled "Add" with a dropdown arrow, also highlighted with a red box.



The screenshots show the IBM MaaS360 configuration and the Google Play Store interface.

IBM MaaS360 Configuration:

- The left panel shows the "Google Play App" section with the "Add App" step selected.
- The right panel shows the "App Details" section where the "Add via Managed Google Play Store" option is selected.
- Below these are two informational notes: "This app offers managed configuration" and "This app is only available in certain countries".

Google Play Store:

- The top part shows the "Google Play" logo and a search bar containing "samsung email".
- The bottom part shows a grid of five app icons: Samsung Email (red), Gmail (white), Microsoft Outlook (blue), Blue Mail - Email (blue with a red notification badge), and Email - Fast & Secure (blue).

Managed Google Play Configuration

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 with the following details:

IBM MaaS360 | With Watson - Top navigation bar

Search for Devices, Users, Apps or Docs - Search bar

HOME DEVICES USERS SECURITY APPS DOCS - Main menu

Distribute App: Samsung Email - Dialog title

Target - Target dropdown set to "Group" and "AE Work Profile".

Send Notification and **Send Email** checkboxes are available.

Cancel and **Distribute** buttons at the bottom right of the dialog.

App Catalog table:

App ...	Name	Type	Categ...	Instal...
<input type="checkbox"/>	Samsung Email		PRODUCTIVITY	less than 10
<input type="checkbox"/>	GoToMeeting – Video Conferencing & Online...		BUSINESS	less than 10
<input type="checkbox"/>	QR code reader / QR Code Scanner		TOOLS	less than 10
<input type="checkbox"/>	Knox Service Plugin		BUSINESS	less than 10

AppConfig on IBM MaaS360

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. On the left, the 'App Catalog' page lists several apps: Samsung Email, GoToMeeting – Video, QR code reader / QR, Knox Service Plugin, and Gmail. The 'Samsung Email' row has a red box around the 'Edit App Configurations' link under the 'Actions' column. A modal window titled 'App Configurations - Samsung Email' is open over the catalog. The modal contains notes about device compatibility and configuration types, and a note that native applications like Gmail or Chrome will override certain policies. It includes 'Cancel', 'Check for Settings', and 'Save' buttons. Below the modal, another smaller window titled 'App Configurations - Samsung Email' shows configuration fields for Exchange ActiveSync accounts, including fields for Email address, User name, Account password, and EAS domain, with 'Cancel' and 'Save' buttons at the bottom.

Configure Knox Platform for Enterprise : Standard Edition

Knox Platform for Enterprise : Standard Edition

The Knox Platform for Enterprise solution provides a robust set of features on top of the core Android Enterprise platform, to fill security and management gaps and meet the strict requirements of highly regulated industries.

The Knox Platform for Enterprise solution comes in a two tiered offering:

- Knox Platform for Enterprise : Standard Edition [FREE]
- Knox Platform for Enterprise : Premium Edition [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 Knox Platform for Enterprise : Standard Edition

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

The screenshot shows the 'Leigh AE Policy' configuration page. In the left sidebar, under 'OEM Settings', the 'Samsung License Management' option is selected. A sub-section titled 'Samsung License Management' is displayed. Within this section, there is a 'KNOX License Key' field containing the value 'KLM03-MDGDJ-D1BPJ-WF71N-11Zv'. Below this field, it says 'Requires MaaS360 app version 6.50+'. At the bottom of the page are buttons for 'Cancel', 'Save', 'Save And Publish', and 'More'.

The screenshot shows the 'Groups' page. Under the 'Groups' heading, there is a table listing several groups: 'AE Work Profile', 'SIDI Group', 'COSU Group', and 'Knox CL'. The 'AE Work Profile' row is expanded, showing its members ('Leigh A...'), associated policies ('Policies'), rule sets ('Rule Sets'), apps ('Apps'), and documents ('Docs'). A 'Devices' tab is also visible. A modal window titled 'Change Policy - AE Work Profile' is open over the table. Inside the modal, there are fields for 'iOS Policy' (with a dropdown menu), 'Android Policy' (set to 'Leigh AE Policy'), 'Windows MDM Policy' (with a dropdown menu), and an 'Auto assign to new users' checkbox which is checked. At the bottom right of the modal are 'Cancel' and 'Submit' buttons. The 'Change Policy' button in the modal is highlighted with a red box.

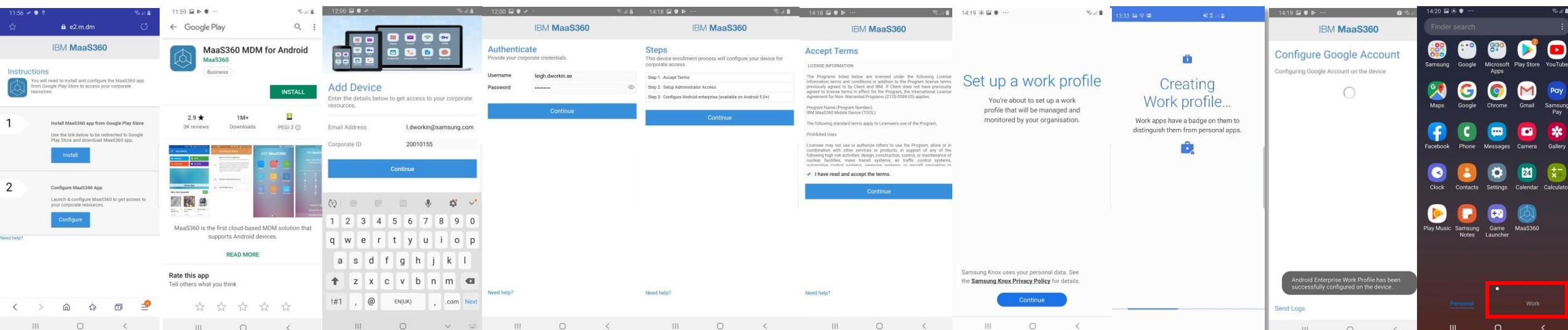
- Then in Users->Groups choose More... and assign the new Policy to the group

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. Install MaaS360 agent from Google Play Store Click Install

Check email and hit Continue

Enter user credentials & hit Continue

Review Steps & hit Continue

Accept terms and conditions

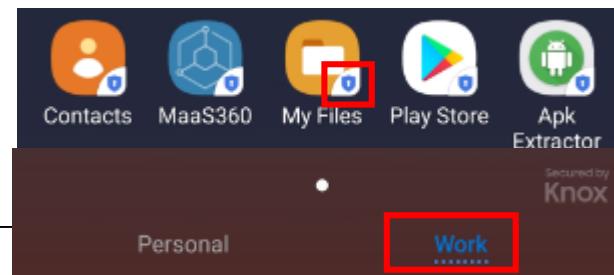
Click Continue to create Work Profile

Creating Work Profile

Device Enrollment Successful!

Work Tab Created

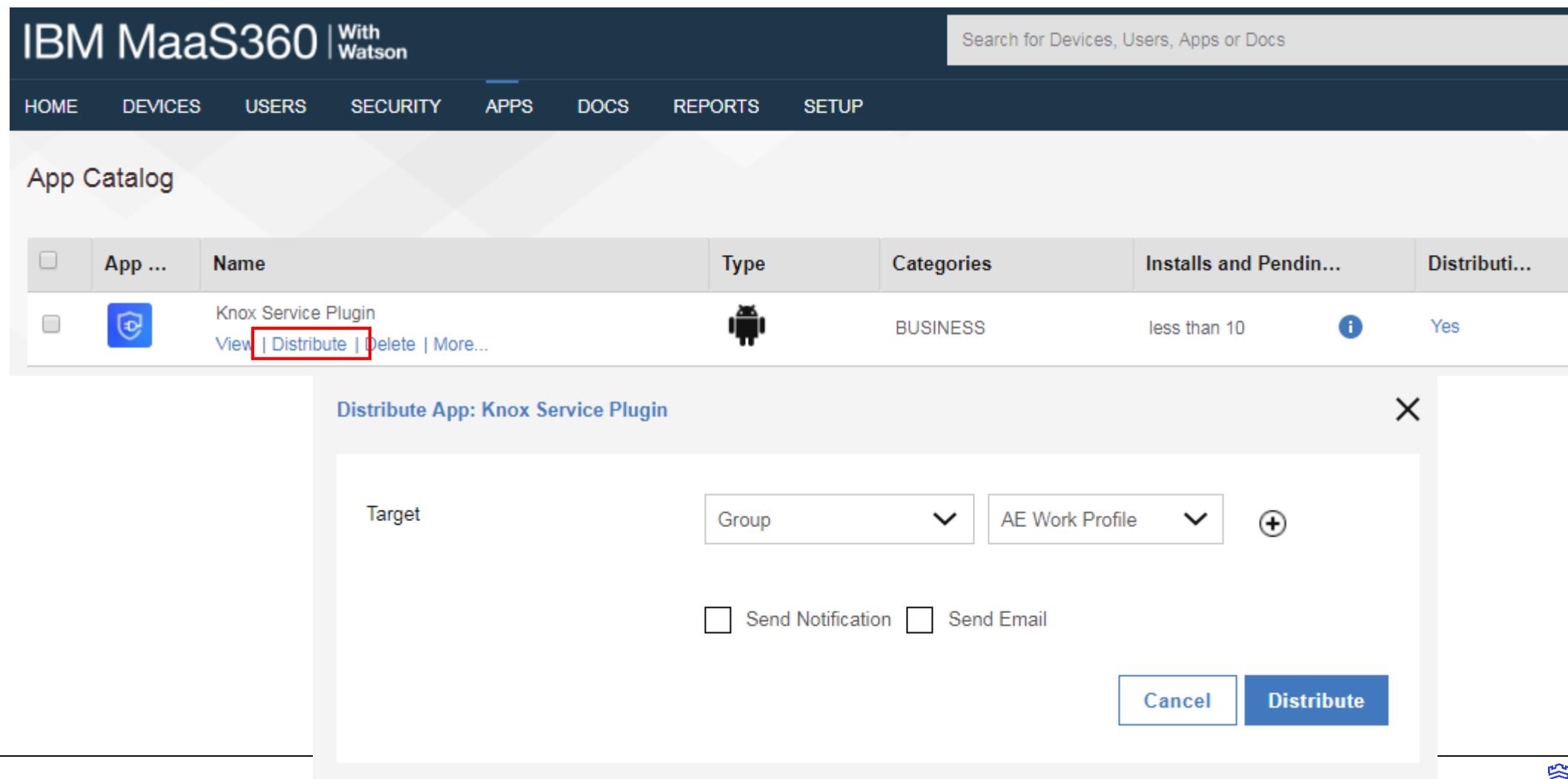
*You can also enroll your device using the alternative IBM MaaS360 methods. For example QR Code.



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 Pending...	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

Knox Service Plugin [KSP]

IBM MaaS360 fully supports Knox Service Plugin.

The screenshot shows the IBM MaaS360 interface with the "Knox Service Plugin" selected in the App Catalog. A modal dialog titled "App Configurations - Knox Service Plugin" is open, containing configuration options for the selected app.

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: (This field is partially visible at the bottom of the dialog.)

Buttons at the bottom of the dialog: Cancel, Reset to Defaults, Check for Settings, Save.

App Catalog Table:

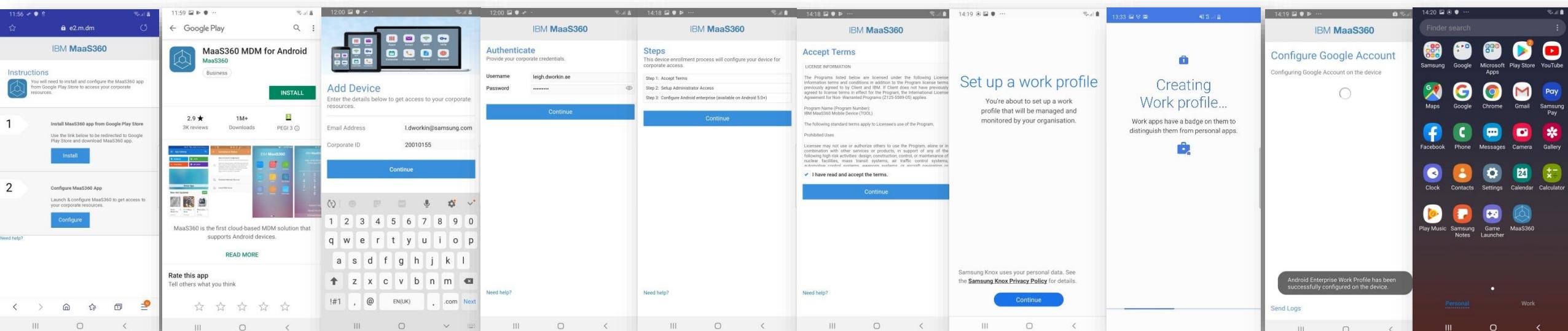
<input type="checkbox"/>	App ...	Name
<input type="checkbox"/>		Knox Service Plugin View Distribute Delete More...
<input type="checkbox"/>		GoToMeeting – Video View Distribute De
<input type="checkbox"/>		QR code reader / QR View Distribute De
<input type="checkbox"/>		Gmail View Distribute De
<input type="checkbox"/>		Apk Extractor Edit App Configurations

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.
Install MaaS360 agent from Google Play Store
Click Install

Check email and hit Continue

Enter user credentials & hit Continue

Review Steps & hit Continue

Accept terms and conditions

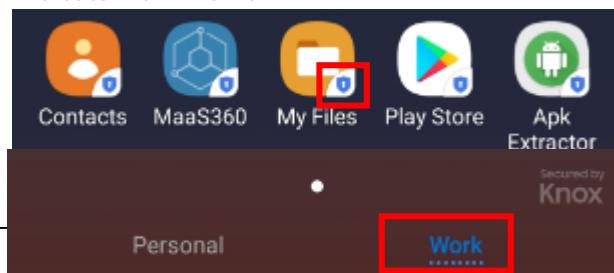
Click Continue to create Work Profile

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

This is version 3.0 of this document.

Thank you!

