



# IBM MaaS360

&

# Knox Platform for Enterprise

June 2021

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

**Knowledge Base:**

[https://www.ibm.com/support/knowledgecenter/SS8H2S/com.ibm.mc.doc/mc\\_collateral/mc\\_landing.htm](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](https://www.youtube.com/watch?v=UeH_zGcJ-bM)

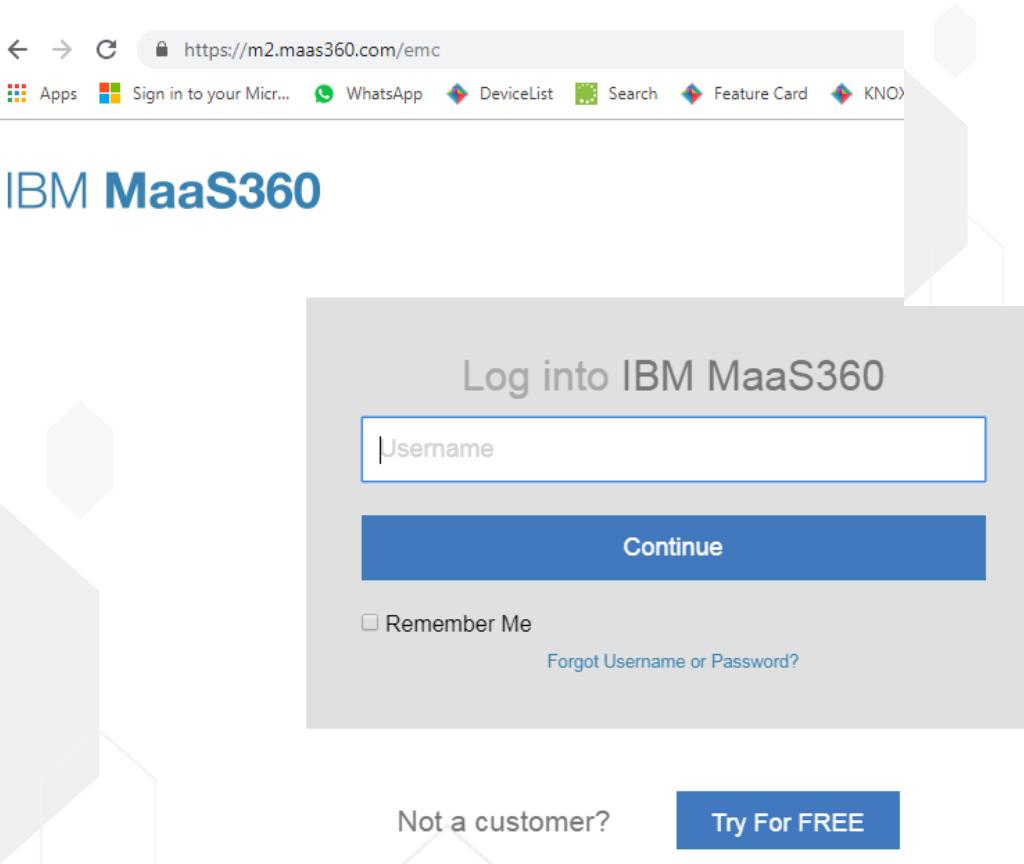
**Trial Access:**

<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

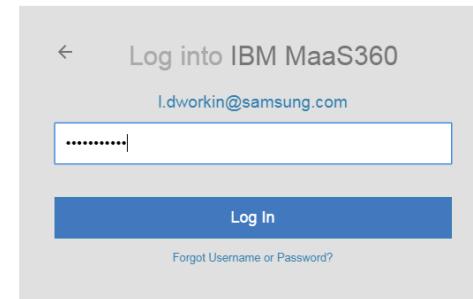
# Obtain access to MaaS360 console

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

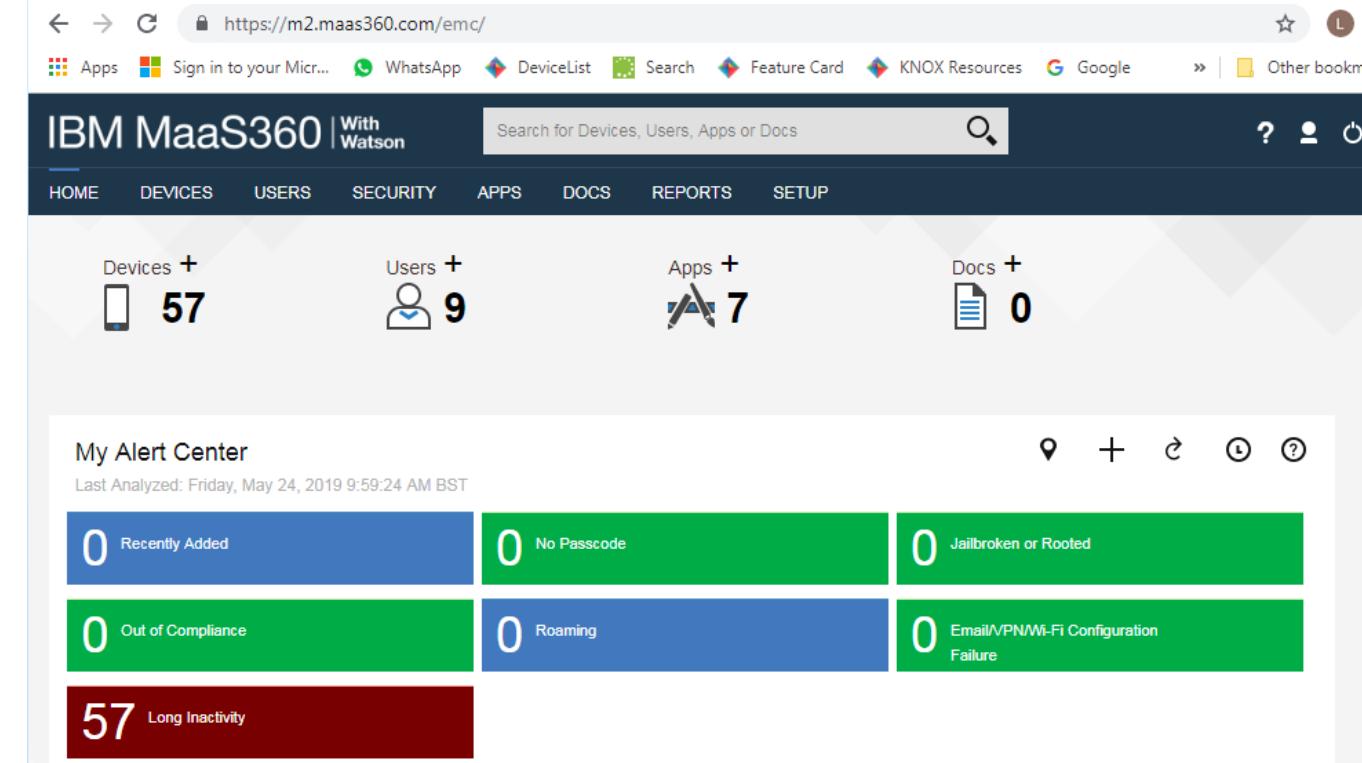


The screenshot shows the IBM MaaS360 login page. At the top, there's a navigation bar with links for Apps, Sign in to your Micr..., WhatsApp, DeviceList, Search, Feature Card, and KNOX Resources. Below the navigation is the IBM MaaS360 logo. The main area features a large "Log into IBM MaaS360" button. Below it is a "Username" input field, followed by a "Continue" button. There's also a "Remember Me" checkbox and a "Forgot Username or Password?" link. At the bottom left, there's a "Not a customer?" link and a "Try For FREE" button.

IBM MaaS360



A screenshot of a "Log into IBM MaaS360" dialog box. It shows a "Log in" form with a "Forgot Username or Password?" link below it.



The screenshot shows the IBM MaaS360 dashboard. At the top, there's a navigation bar with links for HOME, DEVICES, USERS, SECURITY, APPS, DOCS, REPORTS, and SETUP. The main area displays four summary cards: Devices (57), Users (9), Apps (7), and Docs (0). Below this is a section titled "My Alert Center" with a table showing six alert categories: Recently Added (0), No Passcode (0), Jailbroken or Rooted (0), Out of Compliance (0), Roaming (0), and Email/VPN/Wi-Fi Configuration Failure (0). At the bottom, there's a red banner with the number 57 and the text "Long Inactivity".

# A Gmail account to map to MaaS360 for Managed Google Play

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

The screenshot shows the Google Play Work section. On the left, a sidebar menu includes 'Apps', '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, a section titled 'Works With G Suite' shows icons for Google Sheets, Google Slides, and Google Docs. The central part of the page is a 'Sign in' form for Google Play. It has fields for 'Email or phone' (containing 'leighdworkin.maas360@gmail.com') and 'Password'. Below the password field are links for 'Forgot email?' and 'Not your computer? Use Guest mode to sign in privately.' There is also a 'Create account' button and a 'Next' button.

The screenshot shows a Google sign-in page titled 'Welcome'. It has a 'Sign in' button and a 'Forgot password?' link. A password input field contains '.....' and has a visibility toggle icon. A 'Next' button is located to the right of the password field.

The screenshot shows the MaaS360 app management interface. The left sidebar includes 'Apps', 'My managed apps', 'Shop', 'Updates', 'Admin Settings', and 'Help Center'. The main area is a table listing installed apps:

| 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**

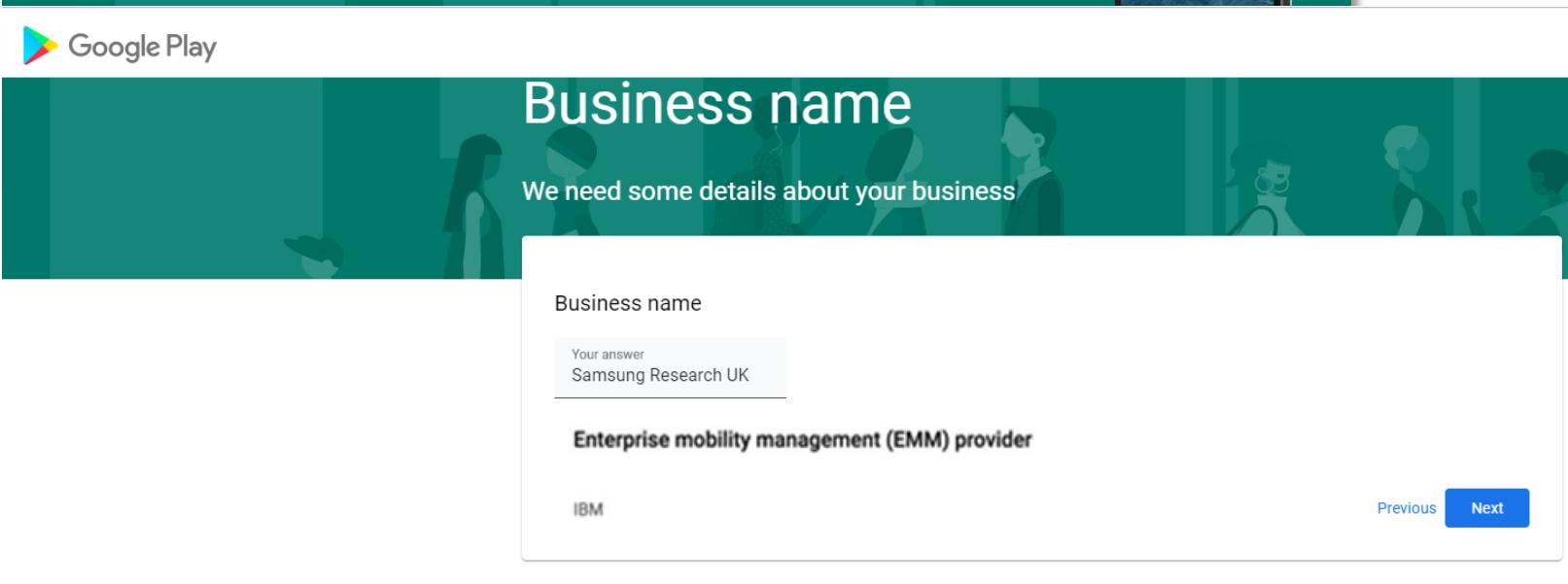
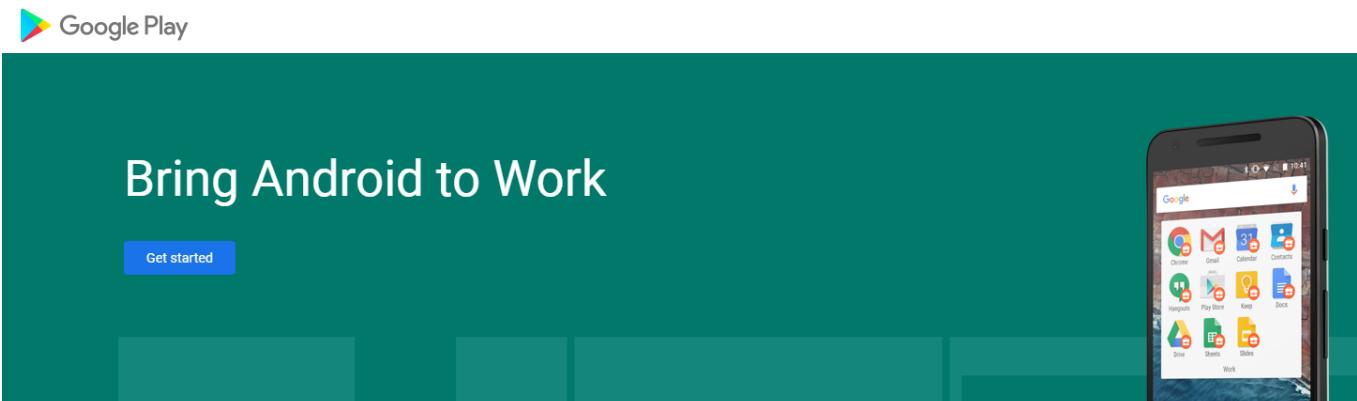
Import apps tied to your Android Enterprise account once approved on Google console. If you want to skip import now, uncheck the option and enable it later from [Apps > App Catalog > More > App Catalog Settings > Android Enterprise Settings](#).

**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.



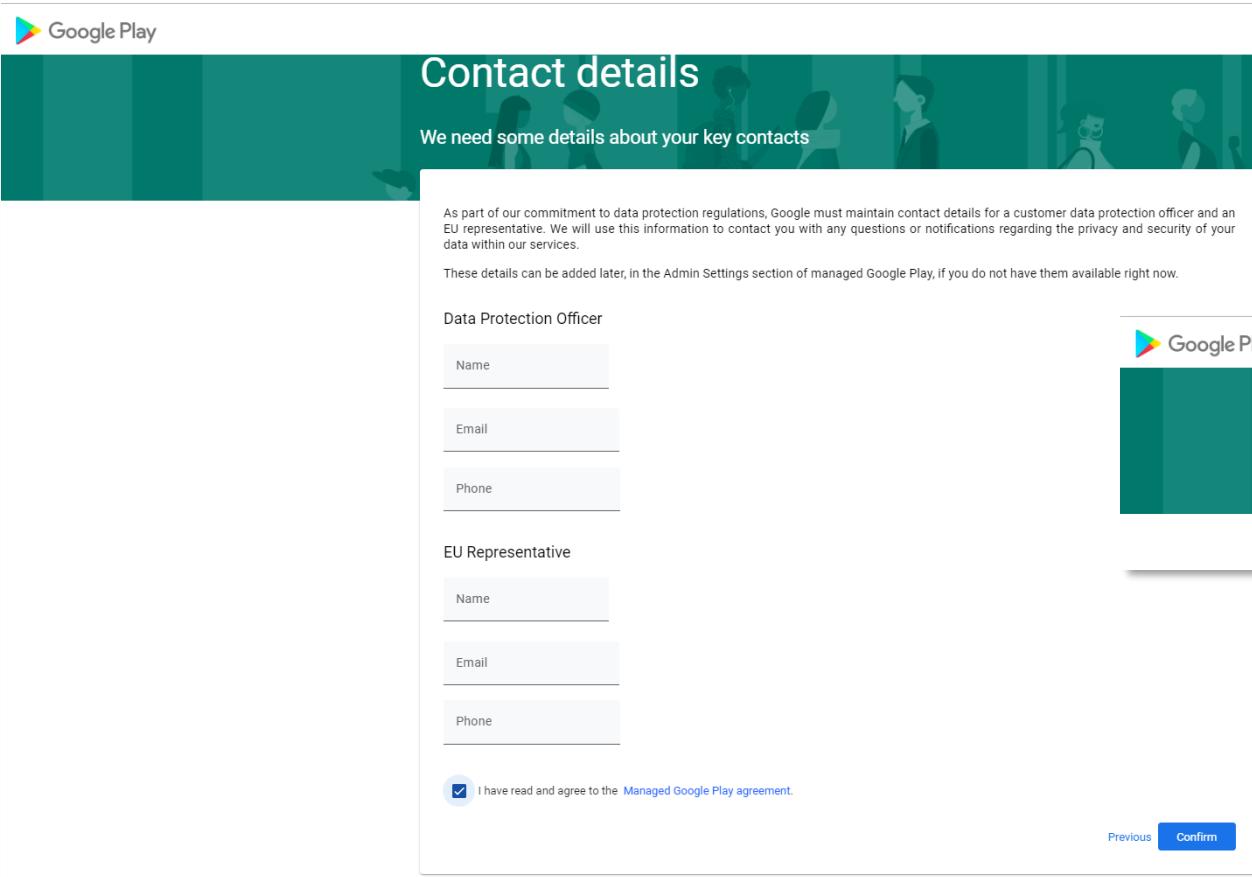
- (Note re-enrolling looks slightly different and there are fewer steps)
- Click Re-enroll)



# 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 screenshot shows the 'Contact details' step of the Google Play setup process. It includes a note about data protection regulations, fields for a Data Protection Officer (Name, Email, Phone) and an EU Representative (Name, Email, Phone), and a checkbox for accepting the Managed Google Play agreement. A 'Confirm' button is at the bottom.

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

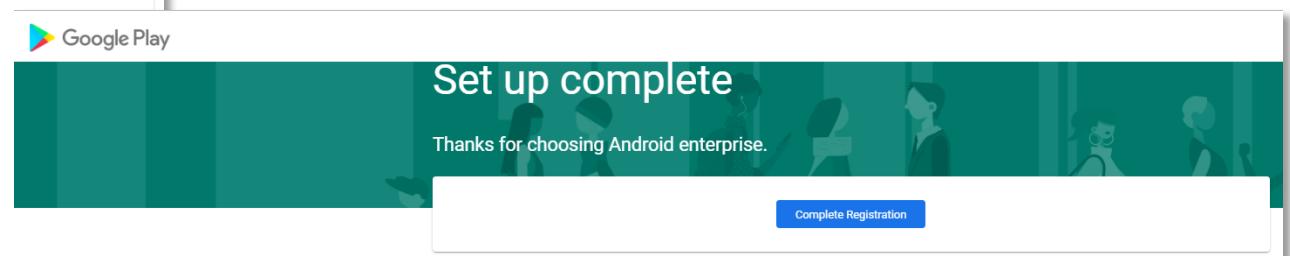
Name \_\_\_\_\_  
Email \_\_\_\_\_  
Phone \_\_\_\_\_

EU Representative

Name \_\_\_\_\_  
Email \_\_\_\_\_  
Phone \_\_\_\_\_

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

Previous **Confirm**



# 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.

The screenshot shows the 'Services' section of the IBM MaaS360 console. Under 'Mobile Device Management', the 'Enable Android Enterprise Solution Set' checkbox is checked. Other checkboxes shown are 'Import iPhone Configuration Utility settings.' and 'Managed Google Play'. A note at the bottom states: 'The Email ID used to bind your organization is leighdworkin.maas360@gmail.com'.

**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

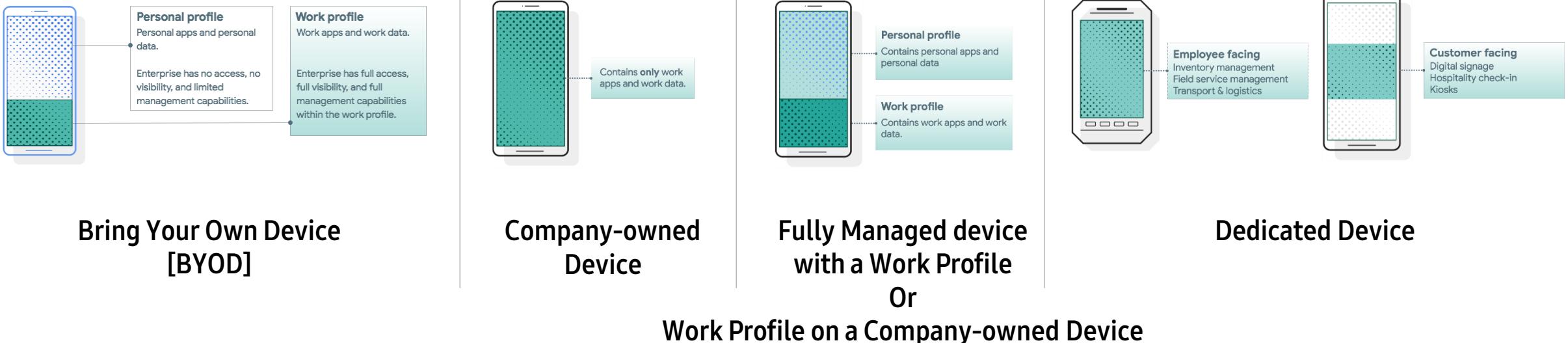
## Deployment Modes

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*]

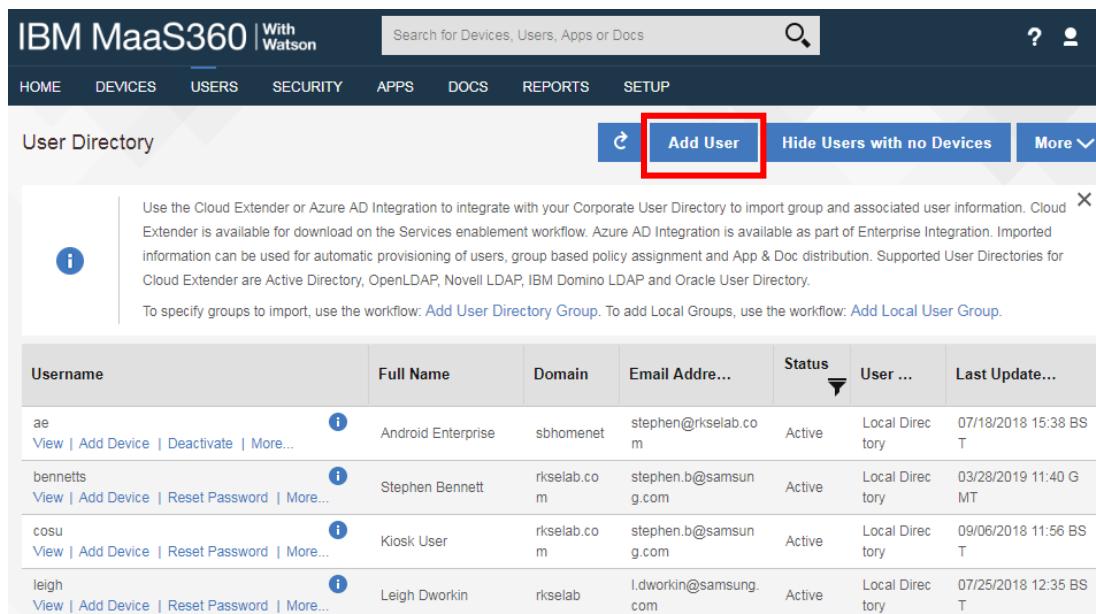
IBM MaaS360 can support 4 of these 5 of these deployment modes, all but COMP. In this next section we will show you how to configure each of these 4 supported deployment modes in IBM MaaS360 for your device fleet.



# Create a User in MaaS360

## Create a User in MaaS360

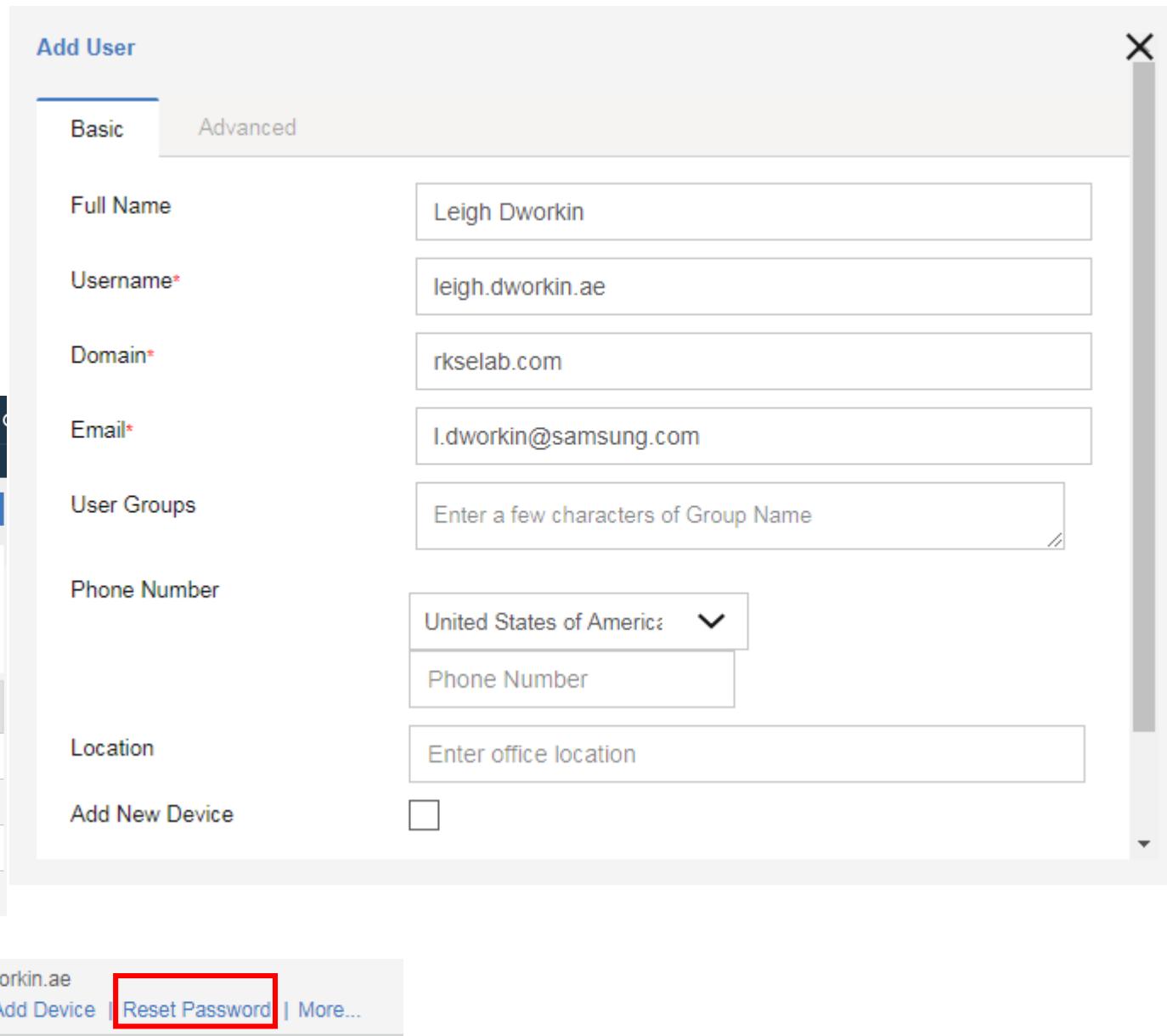
- Navigate to: **Users** and Click the **Add User** button
- Fill in all required fields and then click Save.



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". A callout box provides information about integrating with Corporate User Directories using Cloud Extender or Azure AD Integration. Below the callout is a table listing users with columns for Username, Full Name, Domain, Email Address, Status, User ID, and Last Update. The "Add User" button at the top right is highlighted with a red box.

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

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



The screenshot shows the "Add User" dialog box. It has tabs for "Basic" and "Advanced", with "Basic" selected. The form includes fields for Full Name (Leigh Dworkin), Username (leigh.dworkin.ae), Domain (rkselab.com), and Email (l.dworkin@samsung.com). There are sections for User Groups (with a placeholder "Enter a few characters of Group Name"), Phone Number (with a dropdown for United States of America and a field for Phone Number), and Location (with a placeholder "Enter office location"). Below these is an "Add New Device" section with a checkbox. At the bottom, there are buttons for "View | Add Device | Reset Password | More..." next to the username "leigh.dworkin.ae". The "Reset Password" button is highlighted with a red box.

# Add User to a Group in MaaS360

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

The screenshot illustrates the steps to add a user to a group in the IBM MaaS360 platform. It shows the main navigation bar with tabs like HOME, DEVICES, USERS, SECURITY, APPS, and DOCS. The USERS tab is selected. Below it, a sub-menu for 'Groups' is open, showing options like 'Directory' and 'Groups'. A red box highlights this area. On the right, there's a search bar and some administrative icons. Further down, a table lists various device categories such as 'Android Enterprise', 'Corporate Owned Devices', 'Devices Not Reported in Last 7 days', etc., each with edit and delete buttons. Another red box highlights the 'Add' button in the top right corner of the main content area. To the right, a modal window titled 'Add Local User Group' is open. It contains a note about user groups, fields for 'Name' (set to 'AE Work Profile'), 'Usernames (or Email Addresses)' (containing 'leigh.dworkin.ae'), 'Description' ('BYOD Work Profile or PO setup'), and checkboxes for distribution rights. The 'Save' button at the bottom right is highlighted with a red box. A success message in a separate window says 'The User Group has been added successfully.' with an 'OK' button.

# Add a device for the newly created user

## User Directory



Use the Cloud Extender or Azure AD Integration to integrate with your Corporate User Directory to import groups, automatic provisioning of users, group based policy assignment and App & Doc distribution. Supported User

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

### Username

ae

[View](#) | [Add Device](#) | [Deactivate](#) | [More...](#)

bennetts

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

cosu

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

leigh

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

leigh.ae

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

leigh.dworkin.ae

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

### Full Name



Android Ente



Stephen Ber



Kiosk User



Leigh Dwork



Leigh Dworkin



Leigh Dworkin

### Add Device

#### Basic

#### Advanced

#### Device Addition Mode

 Enroll using Android enterprise

 Device Account

One device enrollment allowed per user

 User Account

Upto 10 device enrollments allowed per user

#### Username

leigh.dworkin.ae

#### Domain

rkselab.com

#### Email

l.dworkin@samsung.com

#### Phone Number

United States of America

Phone Number

#### Notify User\*

 Email  SMS

#### Copy Email

 Me Enter comma separated email
**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

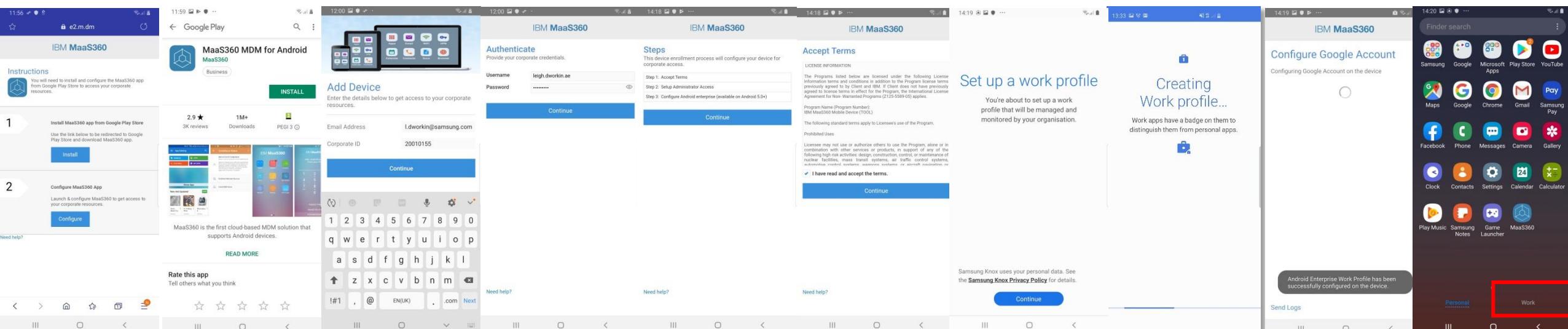
URL: <https://m.dm/20010155/5160624>**OK**

# Android Enterprise: BYOD

## Android Enterprise BYOD Deployment

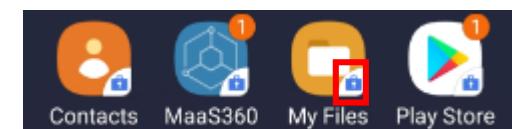
Now all you simply need to do is enroll your device by completing the following:

- On your device, go to the Google Play Store, download the 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!

\*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



 Secured by Knox

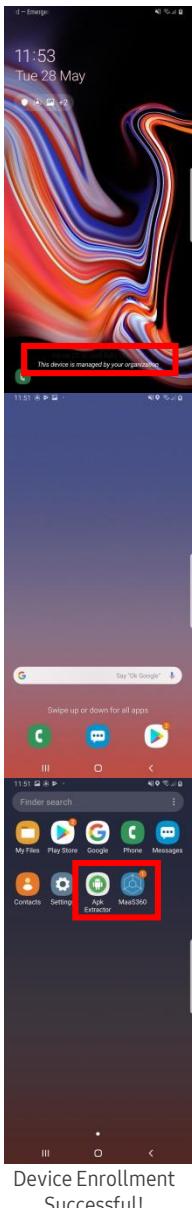
# Android Enterprise: Company-owned Device

## Android Enterprise Company-owned Device Deployment

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

1. DPC Identifier [Also known as the hashtag method] **afw#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 arrow | Accept T's & C's | Skip Import of Old Data | Enter <b>afw#maas360</b> and click next | Install MaaS360 MDM app | Install MaaS360 MDM app | Accept & Continue | Setting Up Work Device | Enter email and Corporate ID | Enter Credentials |



Device Enrollment Successful!

# Android Enterprise: Company-owned Device

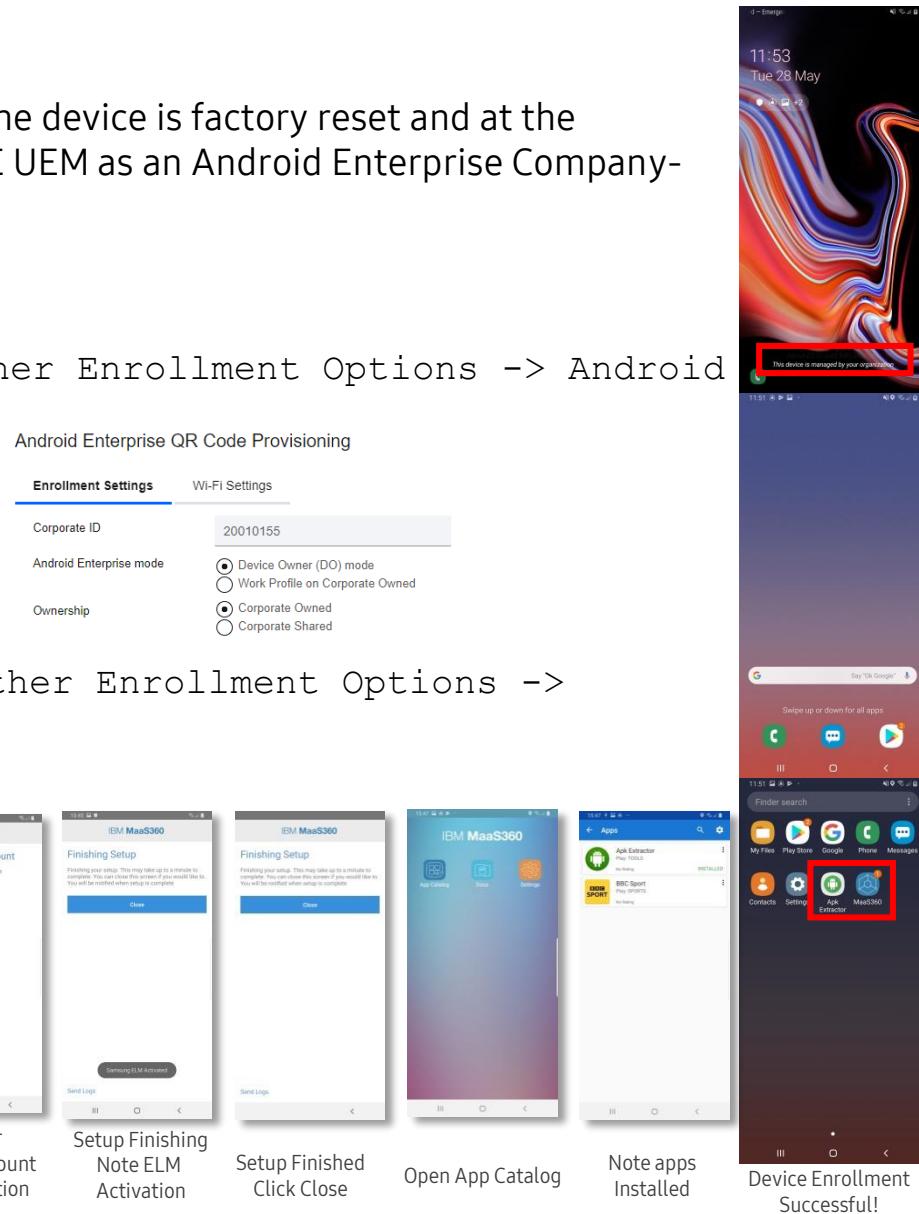
## Android Enterprise Company-owned Device Deployment

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

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

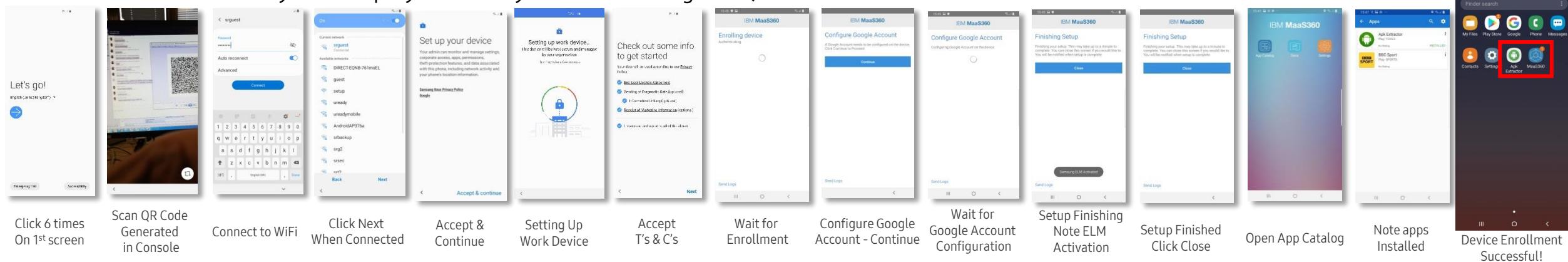
2. QR Code Enrollment / NFC Enrollment –

- 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 Fully Managed Device with a Work Profile Deployment

This is not currently supported by IBM MaaS360.

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 (WPC or WPCO)



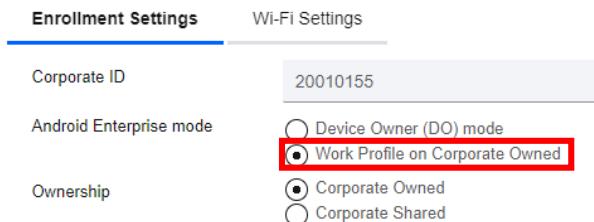
## Android Enterprise Work Profile on a Company-owned Device Deployment

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 –

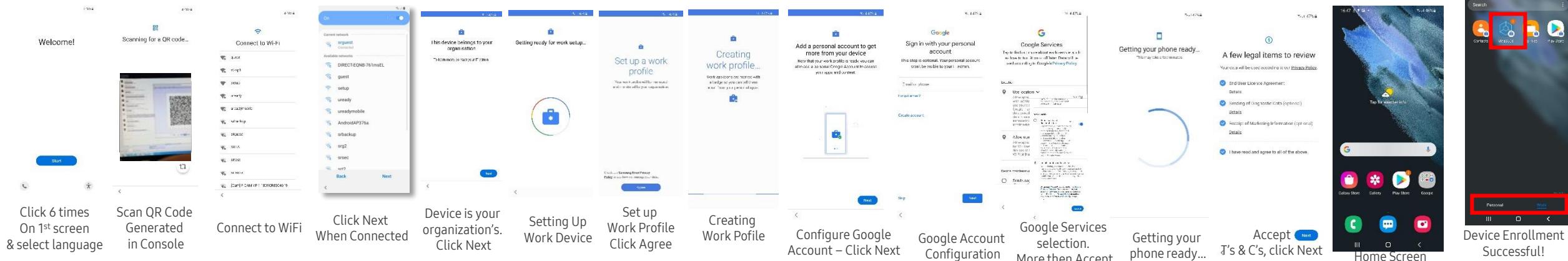
- scan QR code (MaaS360 Portal -> Devices -> Enrollments -> Other Enrollment Options -> Android Enterprise QR Code Provisioning)
- Select Work Profile on Corporate Owned and Corporate Owned:

Android Enterprise QR Code Provisioning



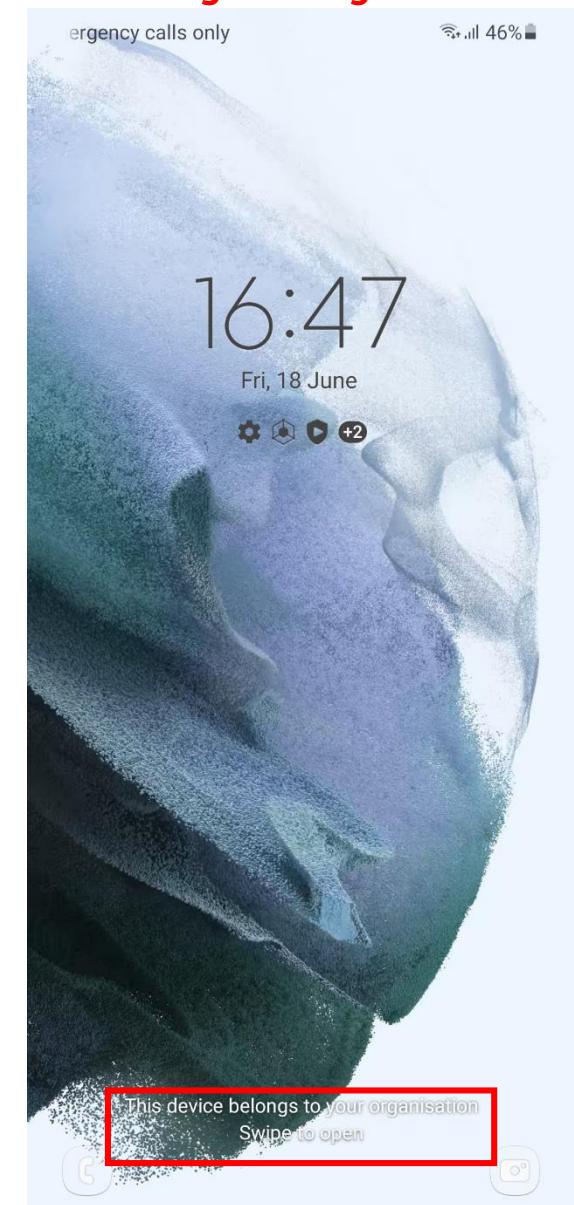
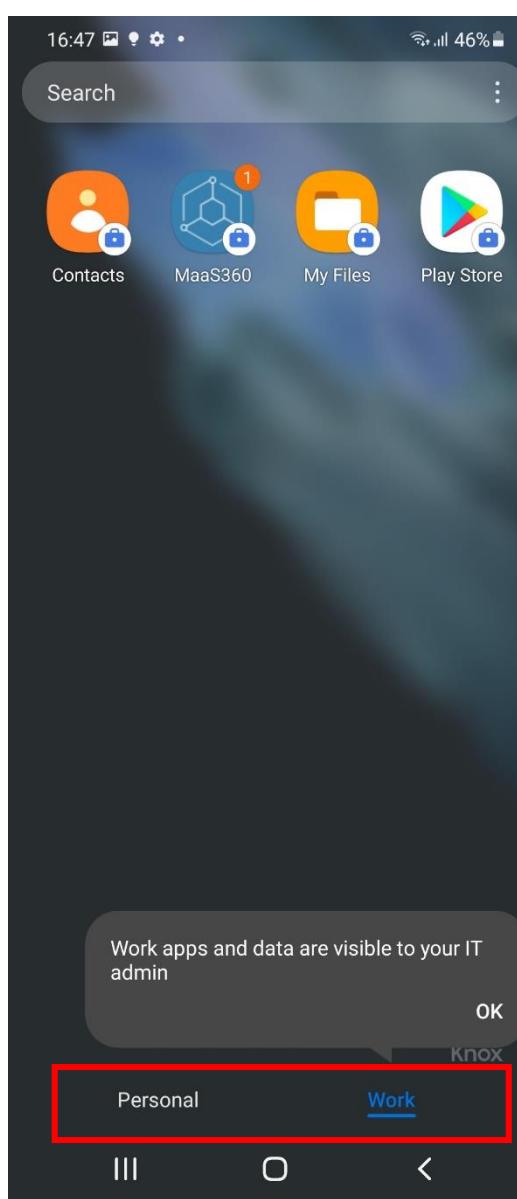
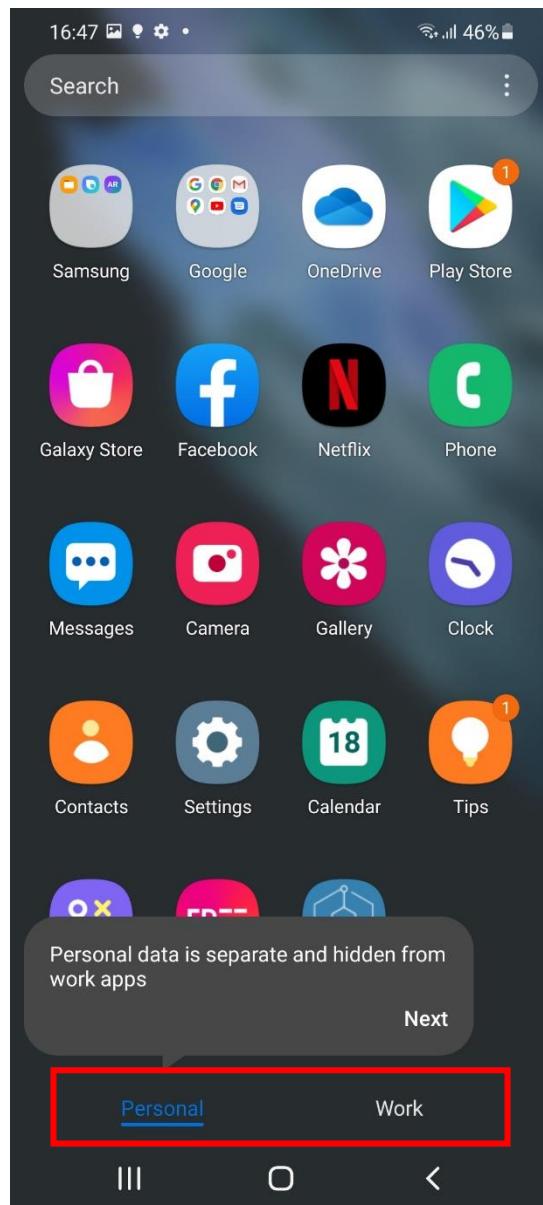
### 2. Knox Mobile Enrollment (MaaS360 Portal -> Devices -> Enrollments -> Other Enrollment Options -> Android Enterprise KME enrollment)

- 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 (WPC or WPCO)

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



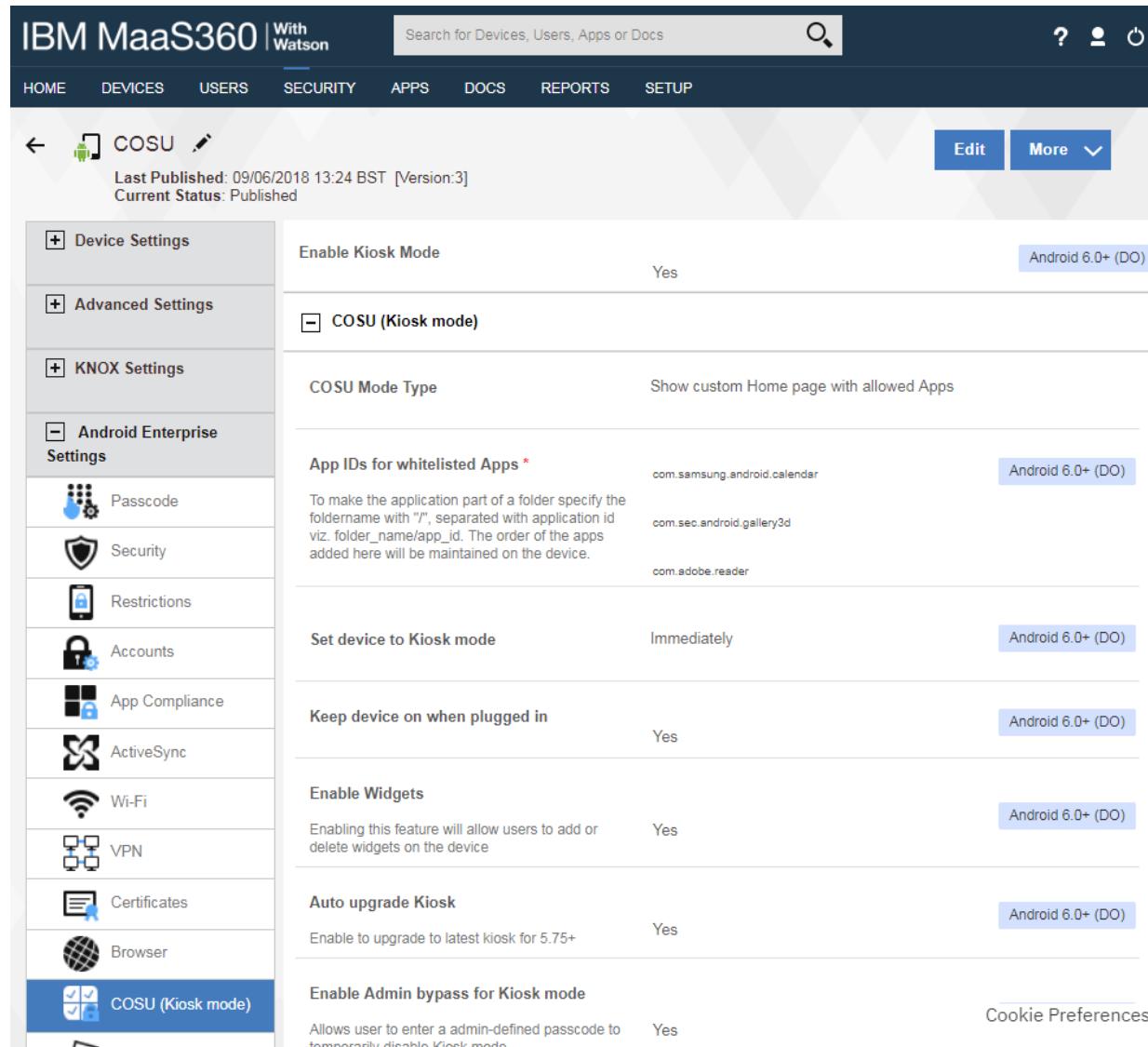
## Android Enterprise Dedicated Device Deployment

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 links for 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, there is a sidebar with sections like Device Settings, Advanced Settings, KNOX Settings, and a expanded "Android Enterprise Settings" section. Under "Android Enterprise Settings", there are icons for 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 settings for "Enable Kiosk Mode" (set to Yes), "COSU Mode Type" (set to Show custom Home page with allowed Apps), and a list of "App IDs for whitelisted Apps" which includes com.samsung.android.calendar, com.sec.android.gallery3d, and com.adobe.reader. Other settings shown include "Set device to Kiosk mode" (set to Immediately), "Keep device on when plugged in" (set to Yes), "Enable Widgets" (set to Yes), "Auto upgrade Kiosk" (set to Yes), and "Enable Admin bypass for Kiosk mode" (set to Yes). A "Cookie Preferences" link is also visible at the bottom right.

# 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.

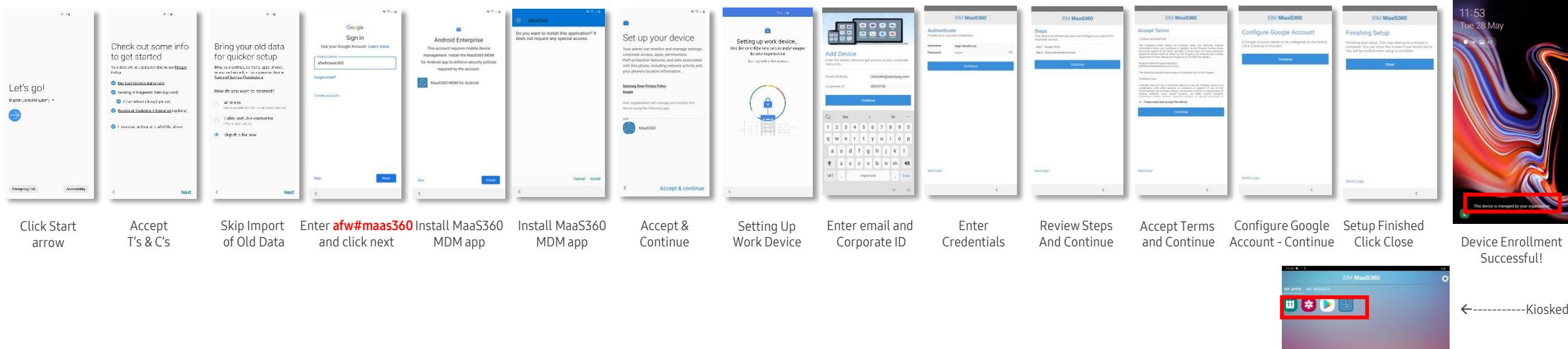
1. DPC Identifier [Also known as the hashtag method] **afw#maas360**

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:

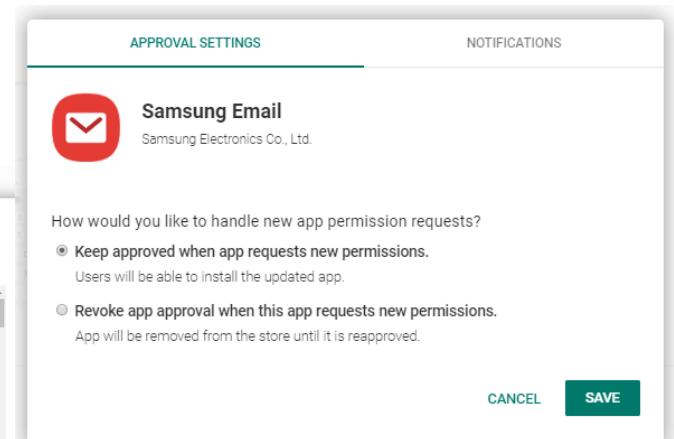
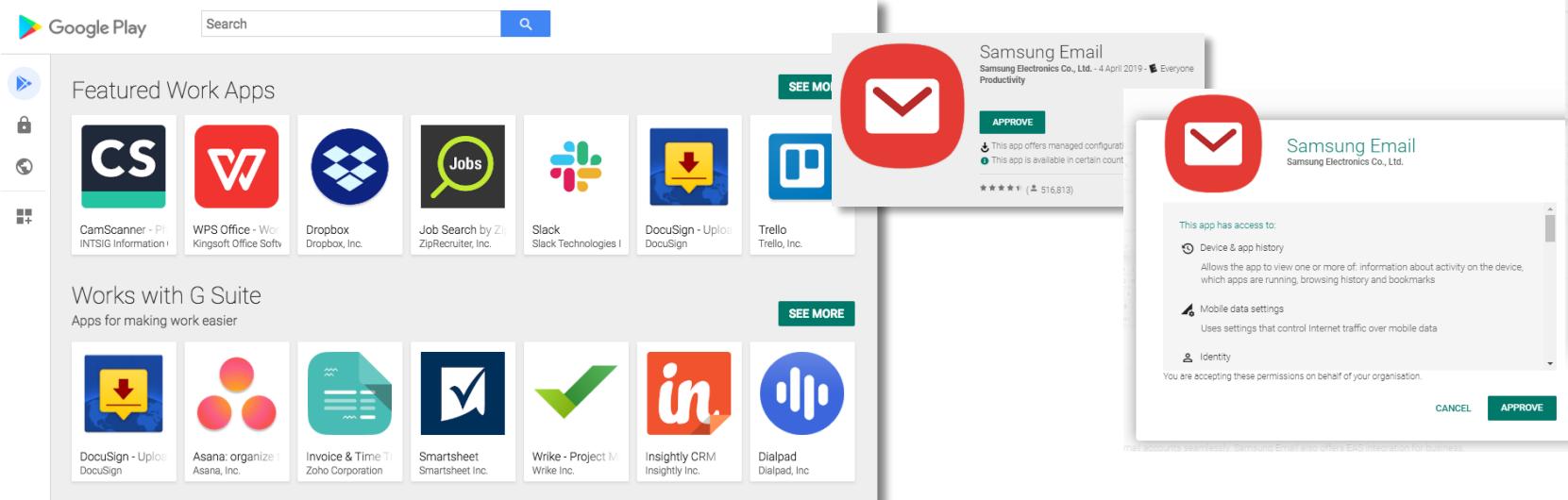


# Managed Google Play Configuration

## 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

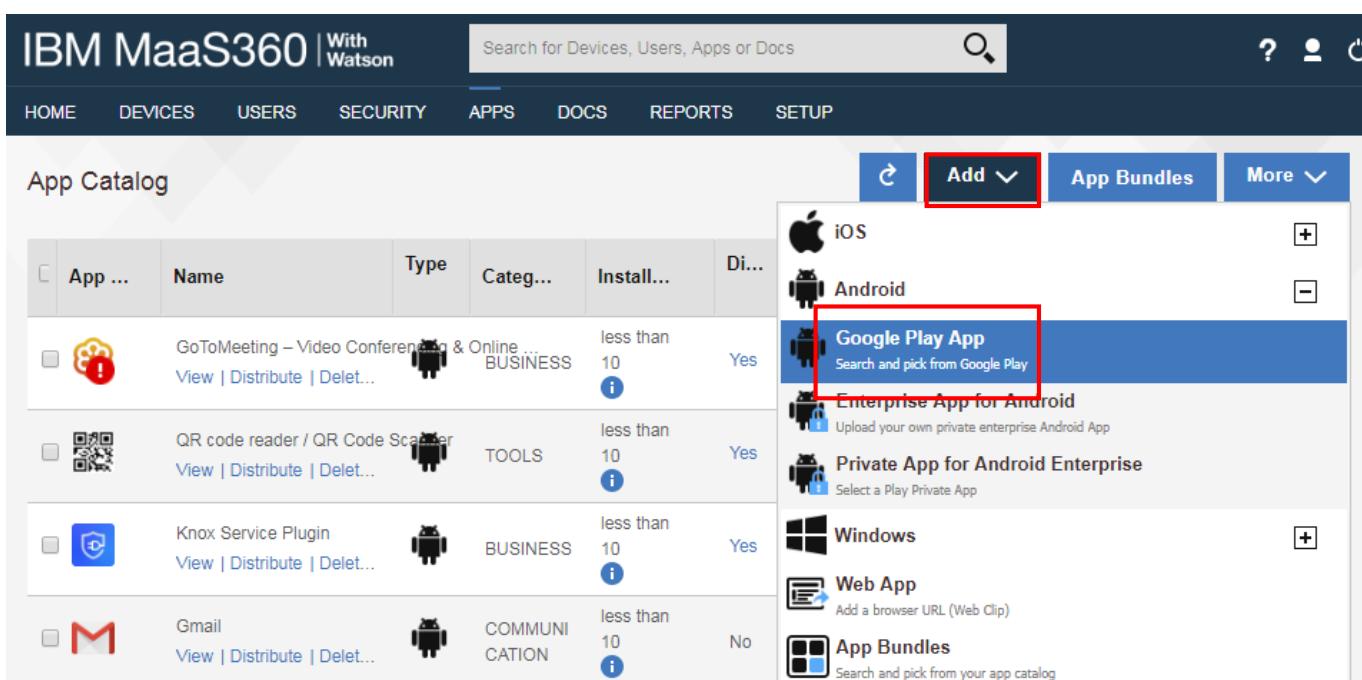


# Managed Google Play Configuration

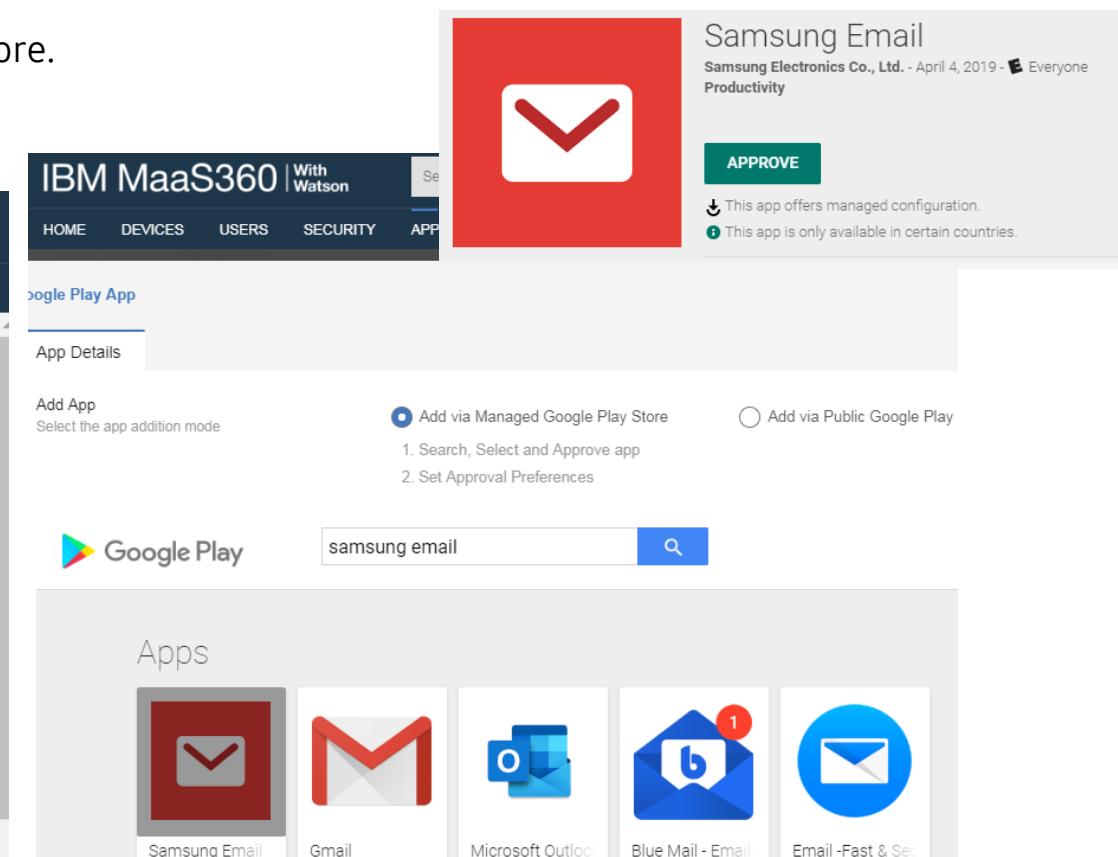
## Managed Google Play Configuration

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 App Catalog page. At the top, there's a search bar and a navigation menu with links for HOME, DEVICES, USERS, SECURITY, APPS (which is currently selected), DOCS, REPORTS, and SETUP. Below the menu is a table titled 'App Catalog' with columns for App, Name, Type, Category, Install..., and Di... (partially visible). The table lists several apps: GoToMeeting – Video Conferencing & Online BUSINESS, QR code reader / QR Code Scanner TOOLS, Knox Service Plugin BUSINESS, and Gmail COMMUNICATION. To the right of the table is a dropdown menu with options for iOS, Android, Google Play App, Enterprise App for Android, Private App for Android Enterprise, Windows, Web App, and App Bundles. The 'Google Play App' option is highlighted with a red box. A large red box also highlights the 'Add' button in the top navigation bar.



The screenshots illustrate the app approval process:

- IBM MaaS360 Catalog:** Shows the 'Add' button highlighted in the top navigation bar and the 'Google Play App' option highlighted in the dropdown menu.
- App Details Page:** Shows the 'Add via Managed Google Play Store' option selected. It includes instructions: 'Select the app addition mode' (radio buttons for 'Add via Managed Google Play Store' and 'Add via Public Google Play'), '1. Search, Select and Approve app', and '2. Set Approval Preferences'. It also shows a preview of the Samsung Email app.
- Google Play Store Search Results:** Shows the search term 'samsung email' entered in the search bar. The results include 'Samsung Email', 'Gmail', 'Microsoft Outlook', 'Blue Mail - Email', and 'Email - Fast & Secure'.

# 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 (unchecked)

**Cancel** and **Distribute** buttons

**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 |

The "Samsung Email" row has its "Distribute" button highlighted with a red box.

# 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 section for setting up Exchange ActiveSync accounts. It includes fields for 'Email address', 'User name', 'Account password', and 'EAS domain'. At the bottom of the modal are 'Cancel', 'Check for Settings', and 'Save' buttons.

# 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 KPE : Standard Edition on IBM MaaS360

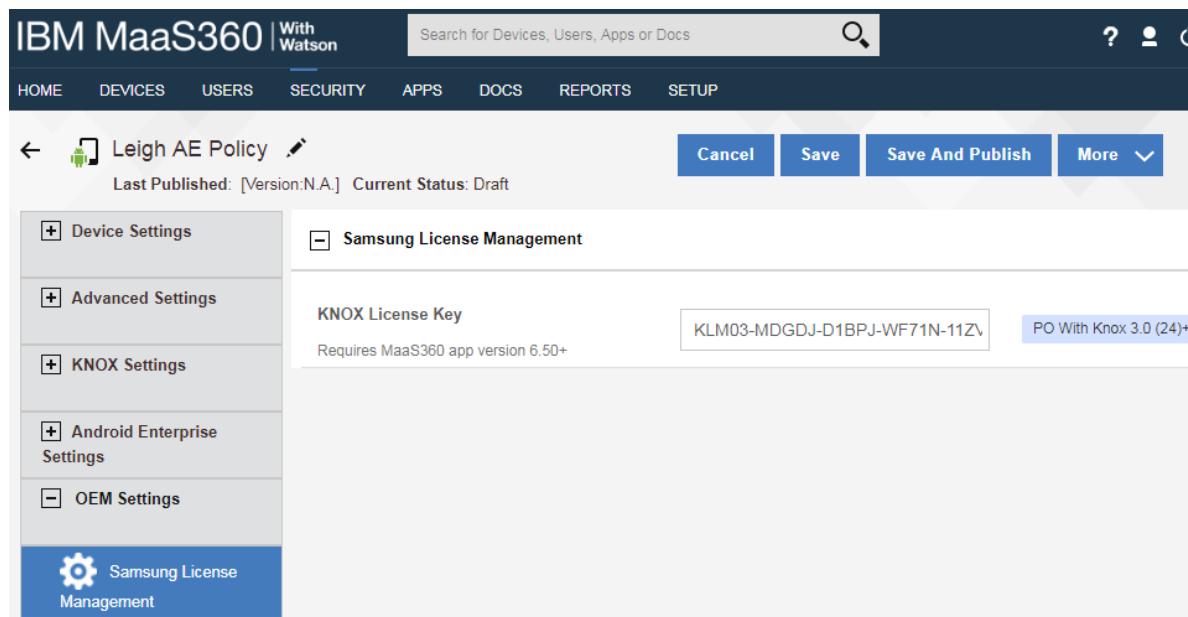
- This is on by default with Android Enterprise on a Samsung Device

# Knox Platform for Enterprise : Premium Edition

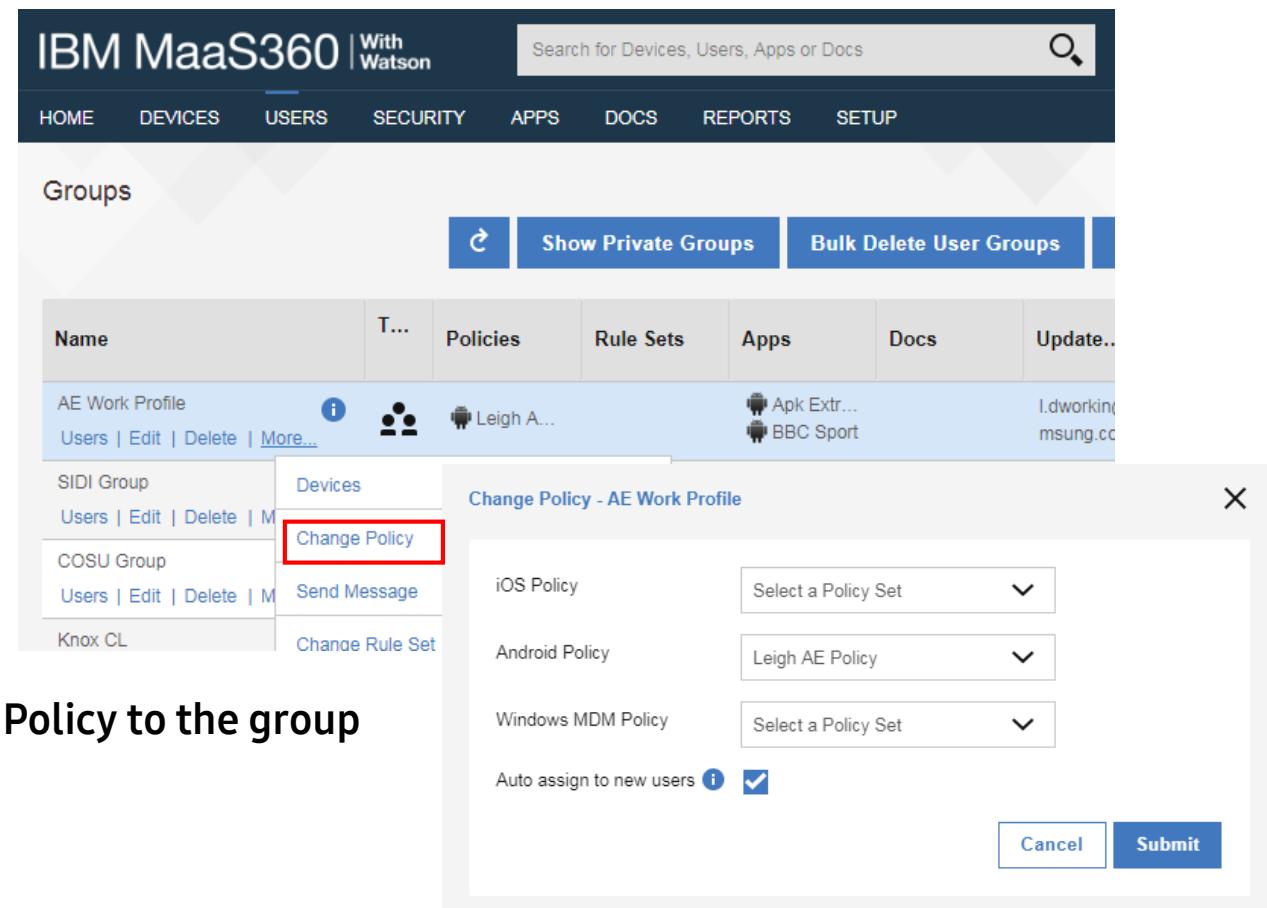
IBM MaaS360 fully supports Knox Platform for Enterprise Premium Edition.

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 IBM MaaS360. On the left, there's a sidebar with options like Device Settings, Advanced Settings, KNOX Settings, Android Enterprise Settings, OEM Settings, and Samsung License Management (which is currently selected). The main panel shows a 'Samsung License Management' section with a 'KNOX License Key' field containing 'KLM03-MDGDJ-D1BPJ-WF71N-11Zv'. Below it, a note says 'Requires MaaS360 app version 6.50+'. At the top right, there are buttons for Cancel, Save, Save And Publish, and More.



The screenshot shows the 'Groups' page in IBM MaaS360. It lists several groups: AE Work Profile, SIDI Group, COSU Group, and Knox CL. The 'AE Work Profile' group is selected. A modal window titled 'Change Policy - AE Work Profile' is open over the list. Inside the modal, under the 'Devices' tab, there's a 'Change Policy' button which is highlighted with a red box. The modal also contains 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. At the bottom right of the modal are 'Cancel' and 'Submit' buttons.

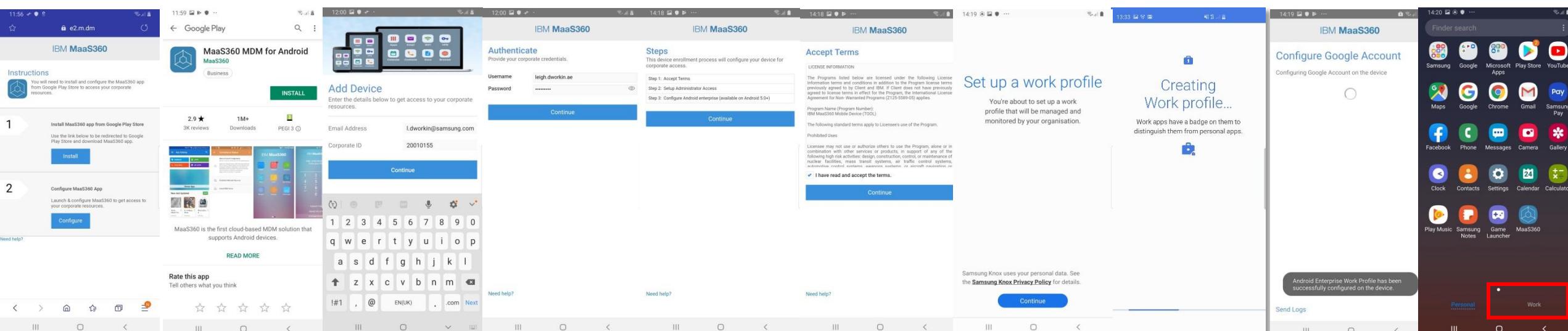
- Then in Users->Groups choose More... and assign the new Policy to the group

# 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

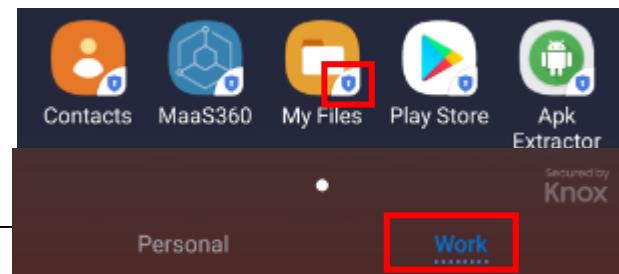
Click Continue to create Work Profile

Creating Work Profile

Device Enrollment Successful!

Work Tab Created

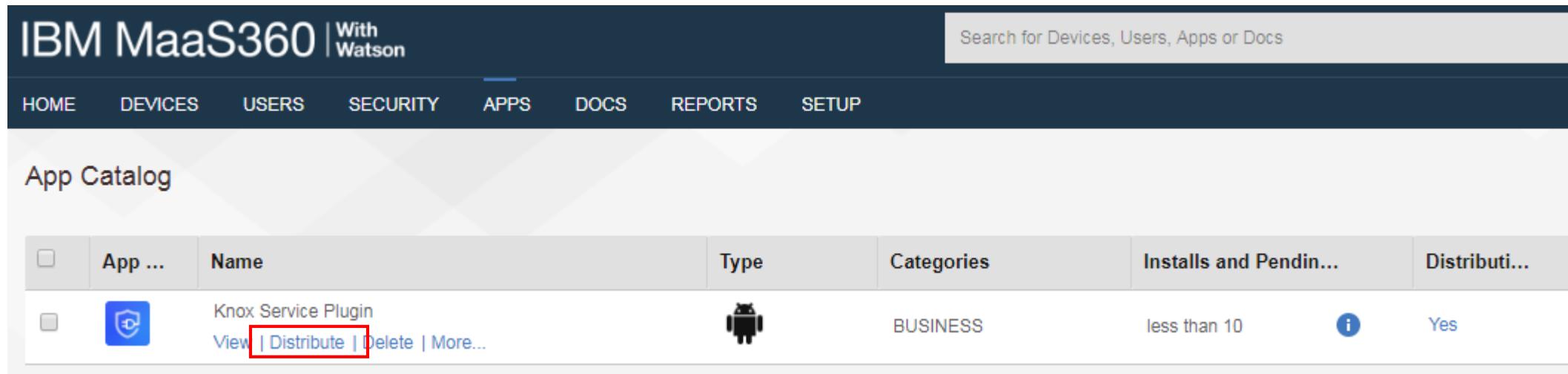
\*You can also enroll your device using the alternative IBM MaaS360 methods. For example QR Code.



What to look out for in the Work Tab

# Knox Service Plugin [KSP]

IBM MaaS360 fully supports Knox Service Plugin.



The screenshot shows the IBM MaaS360 interface with the "SECURITY" tab selected. In the "App Catalog" section, there is a table listing apps. One row for the "Knox Service Plugin" is shown, with the "Distribute" button highlighted by a red box. A modal window titled "Distribute App: Knox Service Plugin" is open, showing distribution settings: Target set to "Group" and "AE Work Profile", and checkboxes for "Send Notification" and "Send Email".

| <input type="checkbox"/> | App ...   | Name  | Type  | Categories | Installs and Pending... | Distributi...   |
|--------------------------|---|---|---|------------|-------------------------|---|
| <input type="checkbox"/> |  | Knox Service Plugin<br><a href="#">View</a>   <a href="#">Distribute</a>   <a href="#">Delete</a>   <a href="#">More...</a> |  | 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 "With Watson" logo. The top navigation bar includes links for HOME, DEVICES, USERS, SECURITY, APPS, DOCS, REPORTS, and SETUP. A search bar is also present. The main area is titled "App Catalog" and lists several apps: "Knox Service Plugin", "GoToMeeting – Video", "QR code reader / QR", "Gmail", and "Apk Extractor". The "Knox Service Plugin" row has a red box around the "Edit App Configurations" button. A modal window titled "App Configurations - Knox Service Plugin" is open over the catalog. It contains a note about device enrollment requirements and mentions that native app settings will override enterprise policies. It includes fields for "Profile Name" (with a placeholder "Knox profile") and "KPE Premium License key" (containing the value "KLM09-HHKHE-7ZF8A-AJDFT-O4WW7-QYHMX"). There are also sections for "Verbose mode" (set to "No") and "Device policies (Device Owner) Group of". At the bottom of the modal are buttons for "Cancel", "Reset to Defaults", "Check for Settings", and "Save".

IBM MaaS360 | With Watson

HOME DEVICES USERS SECURITY APPS DOCS REPORTS SETUP

Search

App Catalog

Knox Service Plugin

View | Distribute | Delete | More...

GoToMeeting – Video

View | Distribute | De

QR code reader / QR

View | Distribute | De

Gmail

View | Distribute | De

Apk Extractor

Edit App Configurations

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.

Knox profile

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.

KLM09-HHKHE-7ZF8A-AJDFT-O4WW7-QYHMX

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.

No

Device policies (Device Owner) Group of

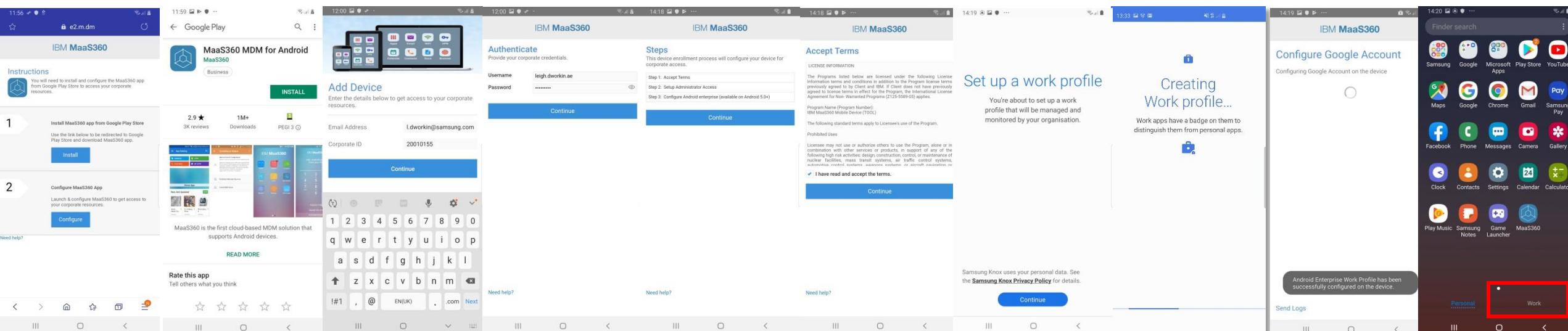
Cancel Reset to Defaults Check for Settings Save

# 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

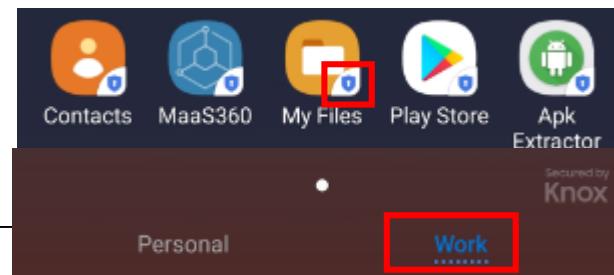
Click Continue to create Work Profile

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 2.1 of this document.

Thank you!

