IBM MaaS360

&

Knox Platform for Enterprise

June 2019
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
     - Fully Managed Device with a Work Profile (Personally Enabled Work Device)
   - 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

IBM MaaS360 Collateral & Contacts

Contacts:

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/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

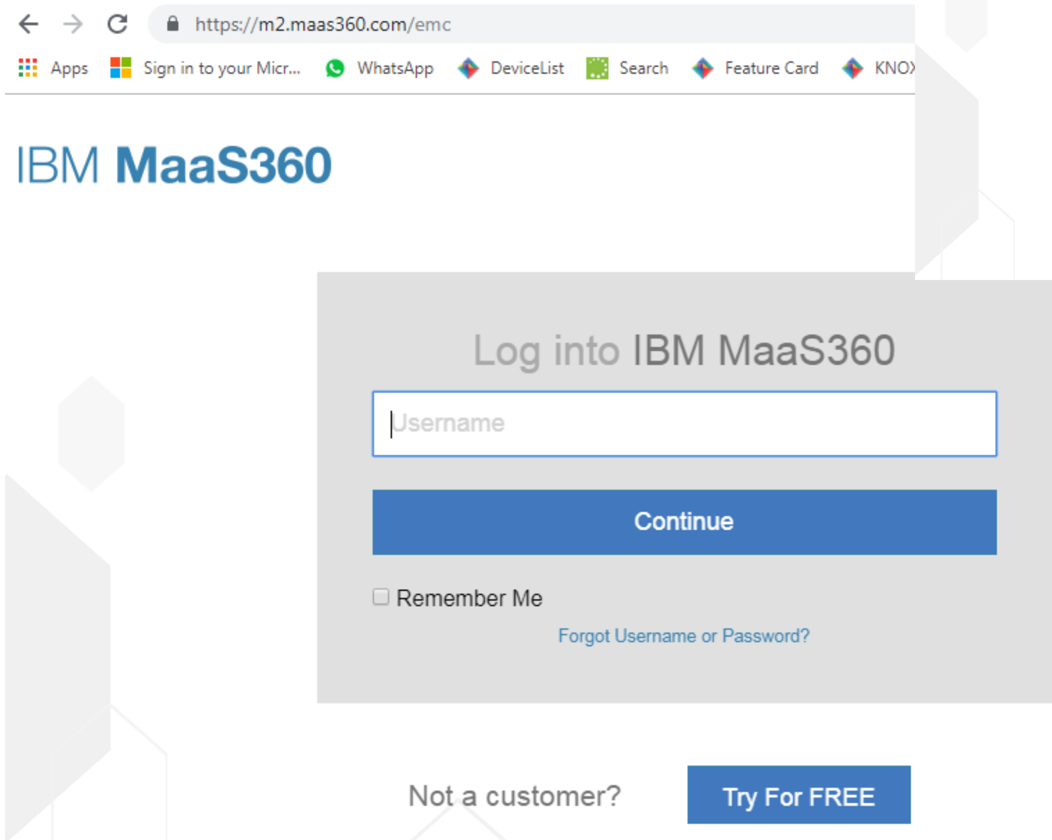
Pre-Requisites for Knox Platform for Enterprise

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

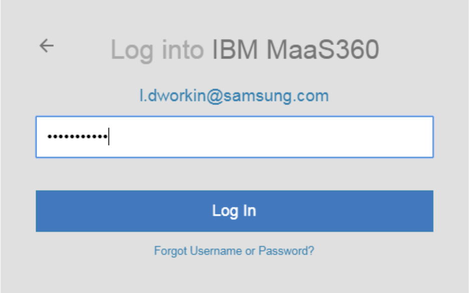
IBM MaaS360



Log into IBM MaaS360

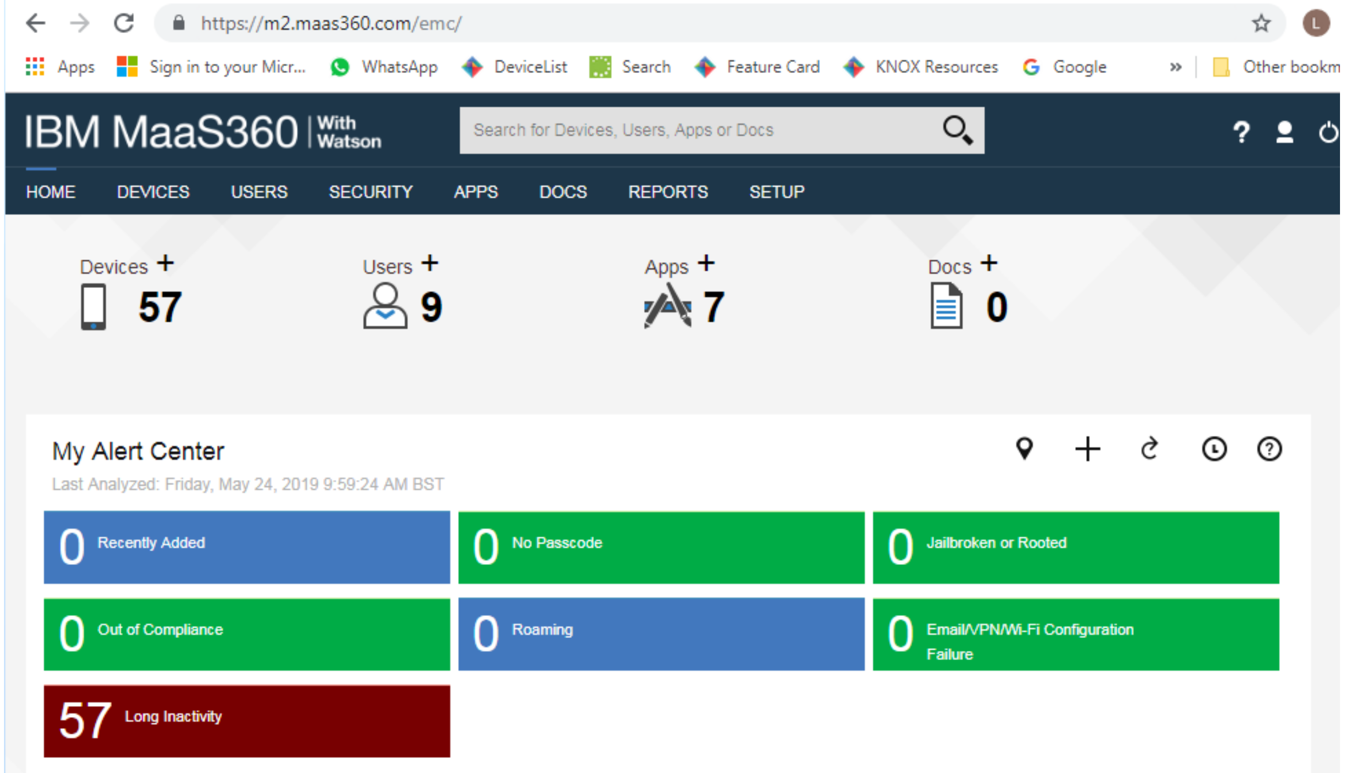
□ Remember Me

Not a customer?



Log into IBM MaaS360

l.dworkin@samsung.com



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

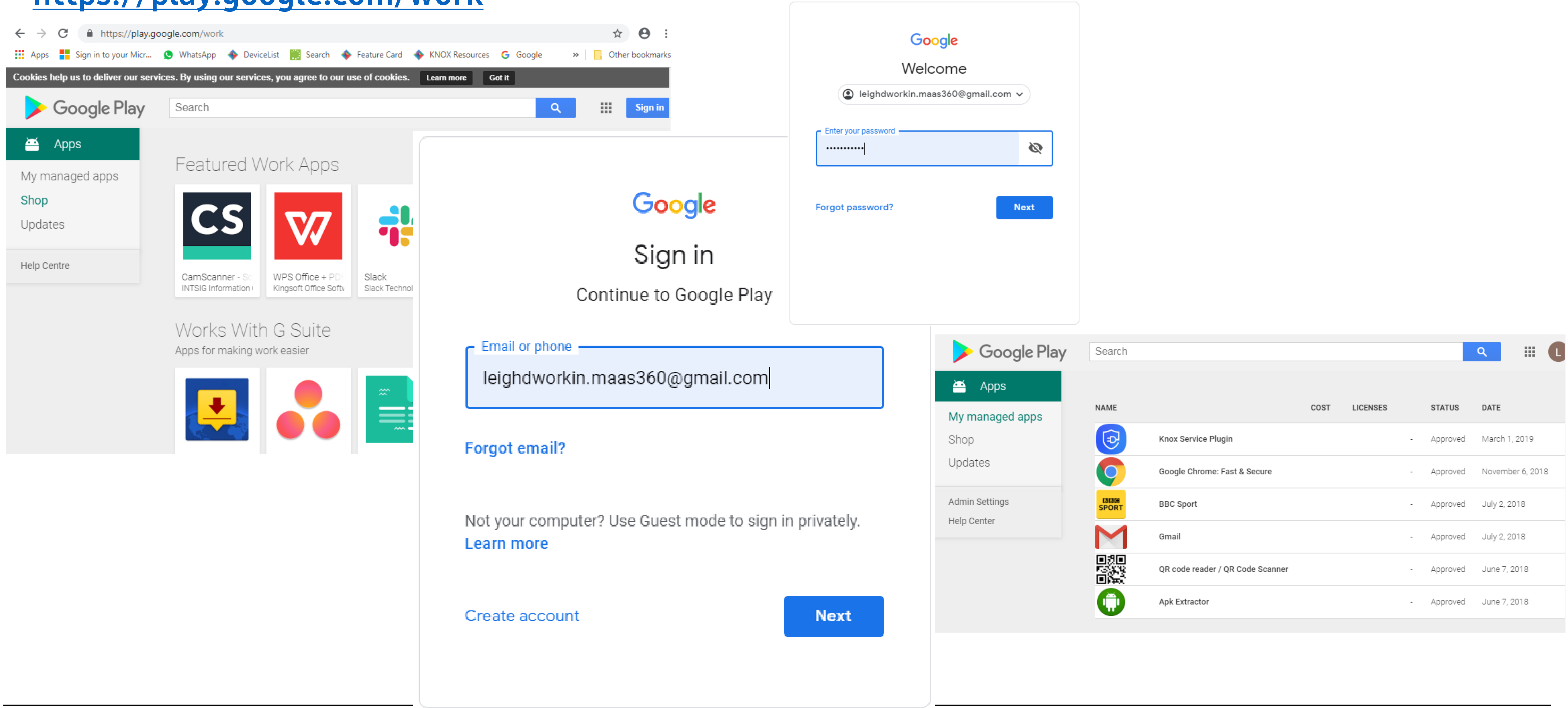
0 Roaming

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



https://play.google.com/work

Cookies help us to deliver our services. By using our services, you agree to our use of cookies. Learn more Got it

Google

Sign in

Continue to Google Play

Email or phone: leighdworkin.maas360@gmail.com

Forgot email?

Not your computer? Use Guest mode to sign in privately. Learn more

Create account Next

Google

Welcome

leighdworkin.maas360@gmail.com

Enter your password: ············

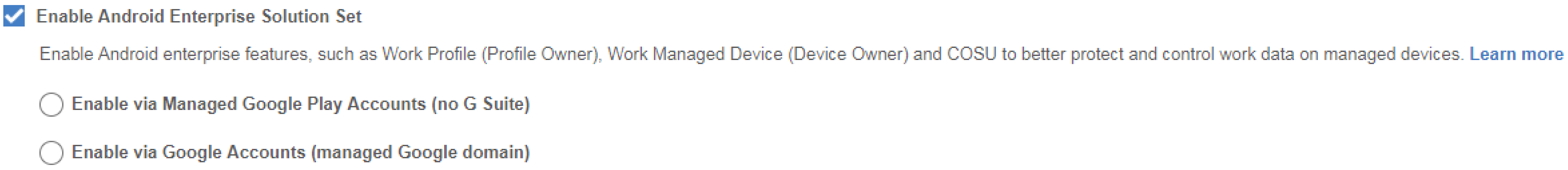
Forgot password? Next

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



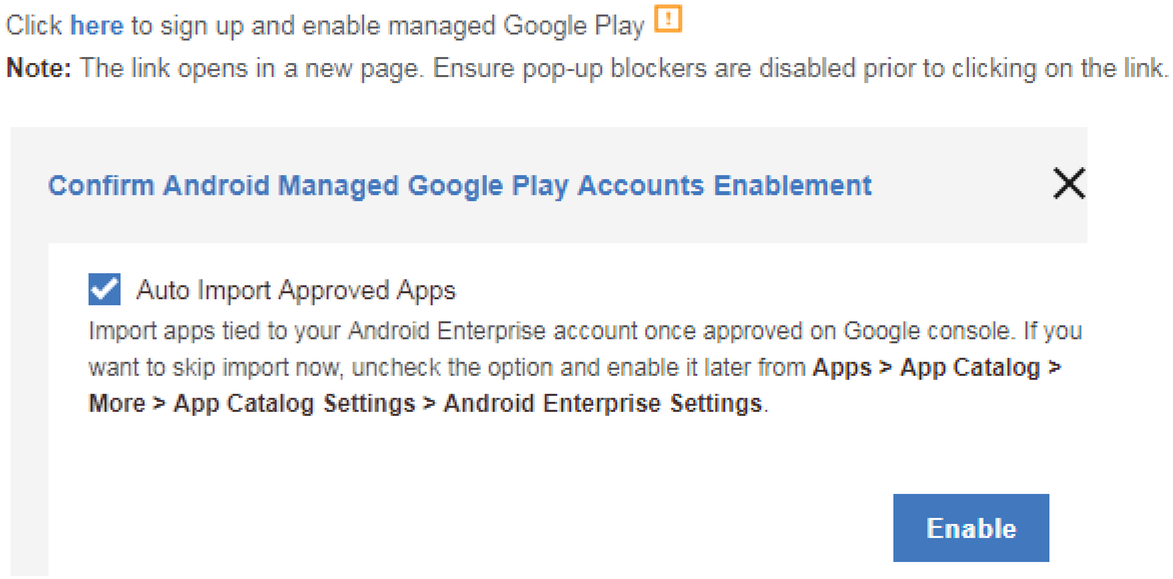
☑ **Enable Android Enterprise Solution Set**

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

○ **Enable via Managed Google Play Accounts (no G Suite)**

○ **Enable via Google Accounts (managed Google domain)**

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



Click **here** to sign up and enable managed Google Play

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

Confirm Android Managed Google Play Accounts Enablement

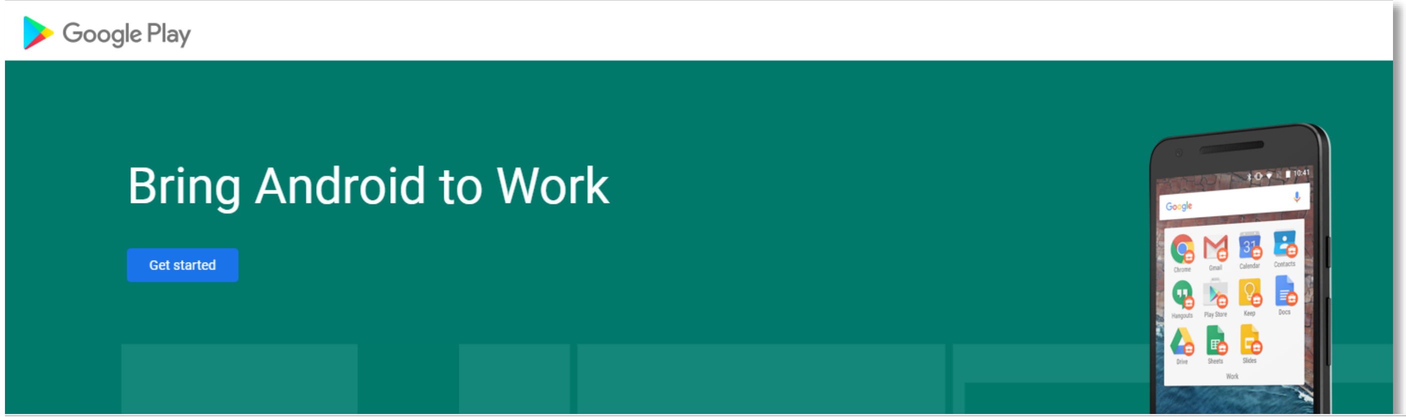
☑ Auto Import Approved Apps

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

Configure Android Enterprise

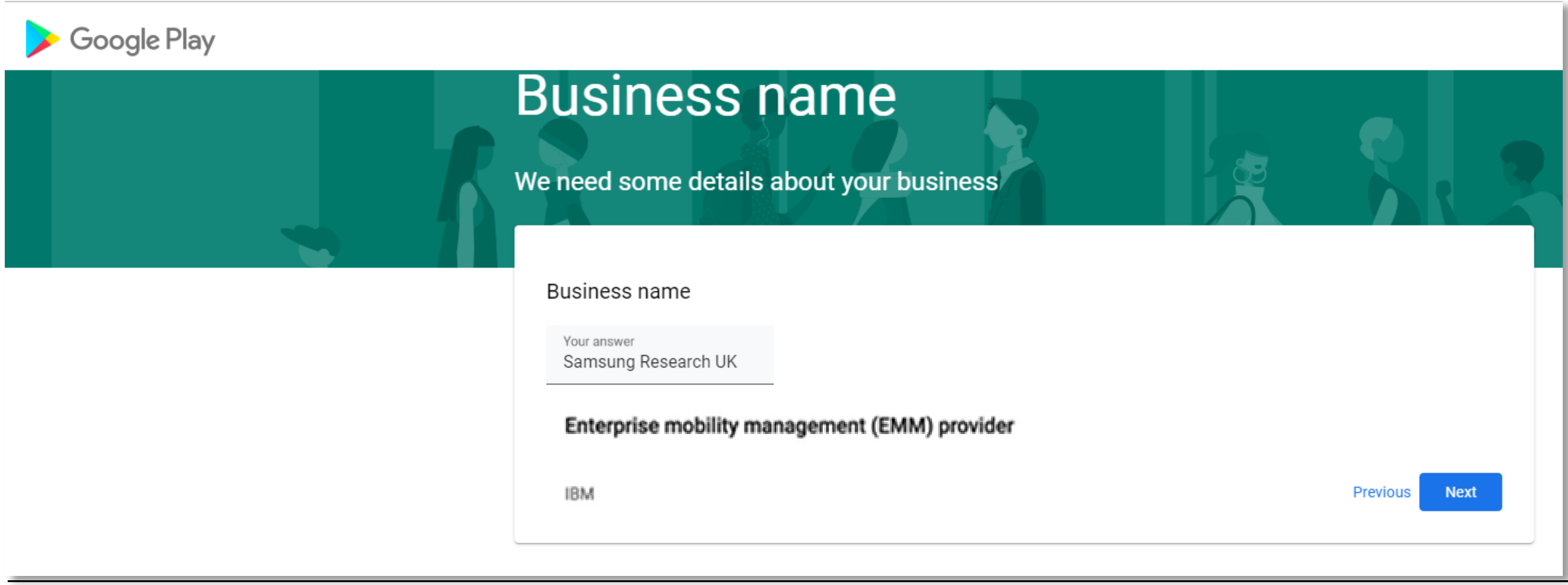
Configure Android Enterprise

- 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.



Google Play

Bring Android to Work



Google Play

Business name

We need some details about your business

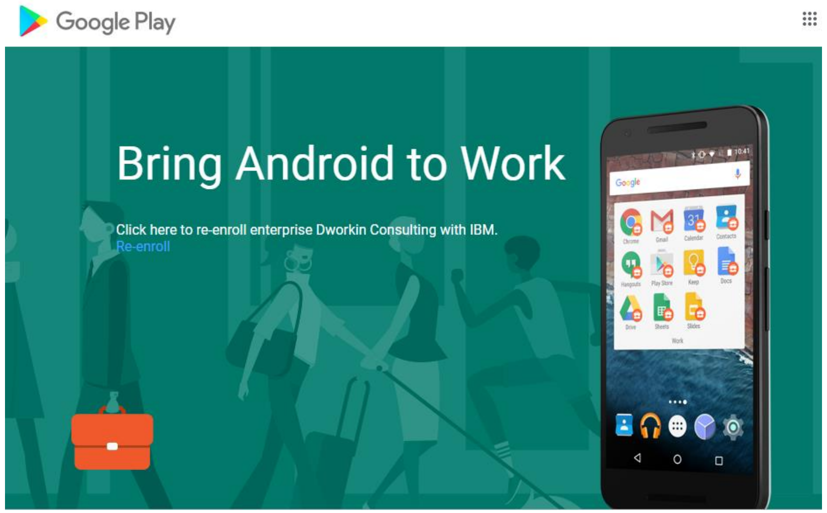
Business name

Your answer
Samsung Research UK

Enterprise mobility management (EMM) provider

IBM

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



Google Play

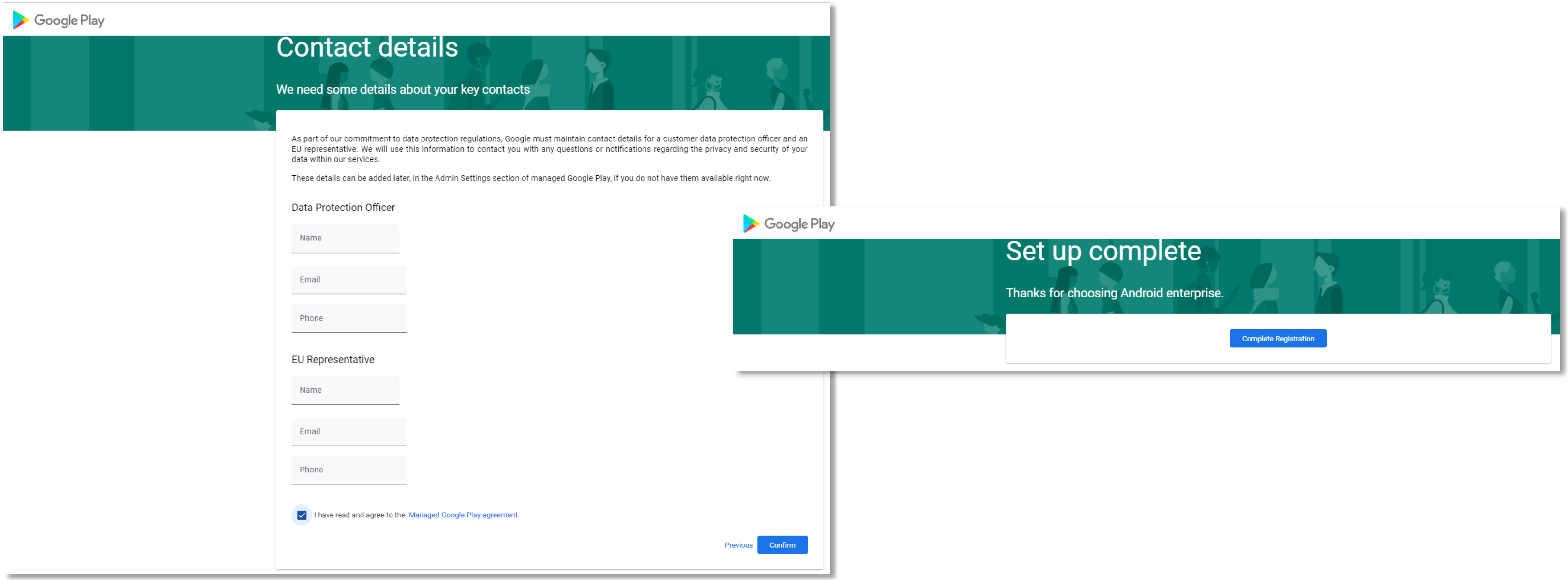
Bring Android to Work

Click here to re-enroll enterprise Dworkin Consulting with IBM.
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.



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.

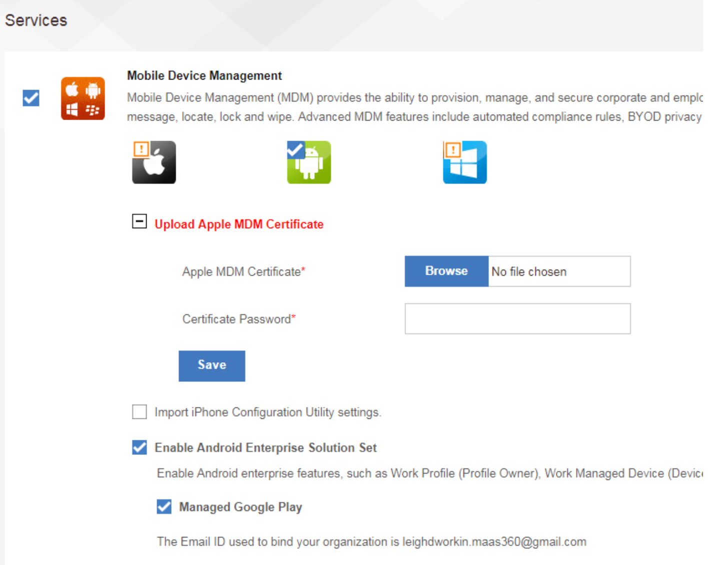
Set up complete

Thanks for choosing Android enterprise.

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.



Services

☑ **Mobile Device Management**

Mobile Device Management (MDM) provides the ability to provision, manage, and secure corporate and emplc message, locate, lock and wipe. Advanced MDM features include automated compliance rules, BYOD privacy

⊟ Upload Apple MDM Certificate

Apple MDM Certificate* Browse No file chosen

Certificate Password*

Save

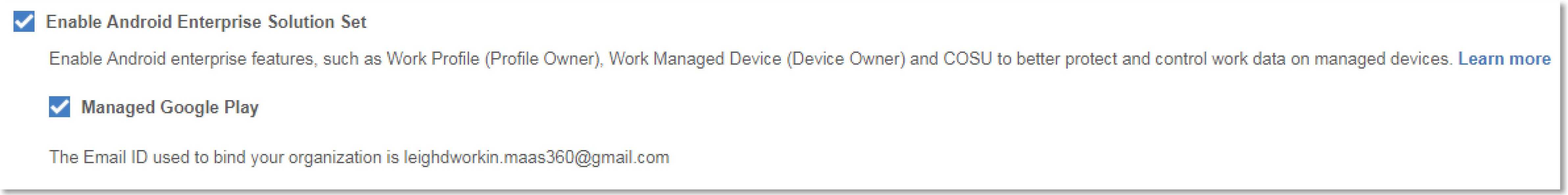
☐ Import iPhone Configuration Utility settings.

☑ Enable Android Enterprise Solution Set

Enable Android enterprise features, such as Work Profile (Profile Owner), Work Managed Device (Devic

☑ Managed Google Play

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

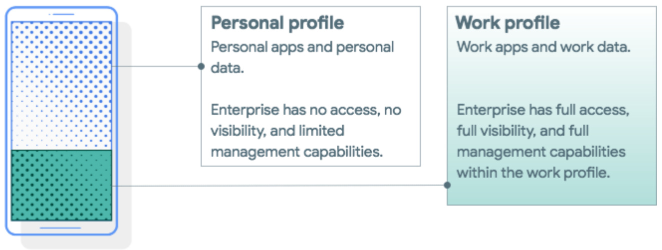
Android Enterprise Deployment Modes

Deployment Modes

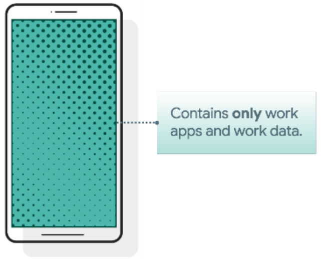
Android Enterprise can be deployed in the following 4 deployment modes

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*]
3. **Dedicated device** [*formerly known as Corporate Owned Single Use or COSU*]

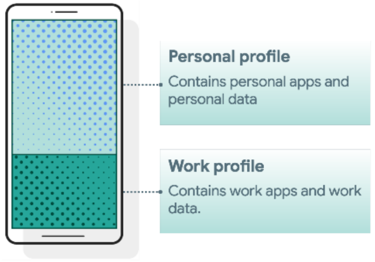
IBM MaaS360 can support **all** 4 of these deployment modes. In this next section we will show you how to configure each of these 4 deployment modes in IBM MaaS360 for your device fleet.


Personal profile
Personal apps and personal data.
Enterprise has no access, no visibility, and limited management capabilities.
Work profile
Work apps and work data.
Enterprise has full access, full visibility, and full management capabilities within the work profile.

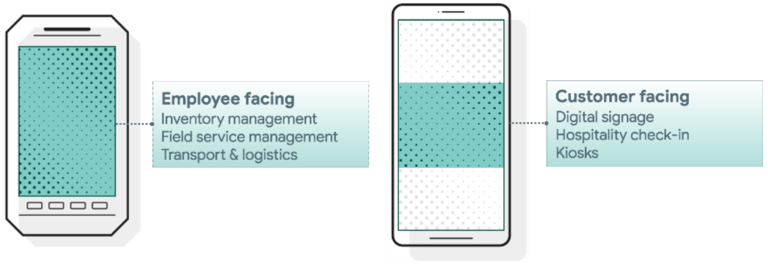
Bring Your Own Device [BYOD]



Company-owned Device


Personal profile
Contains personal apps and personal data
Work profile
Contains work apps and work data.

Fully Managed device with a Work Profile

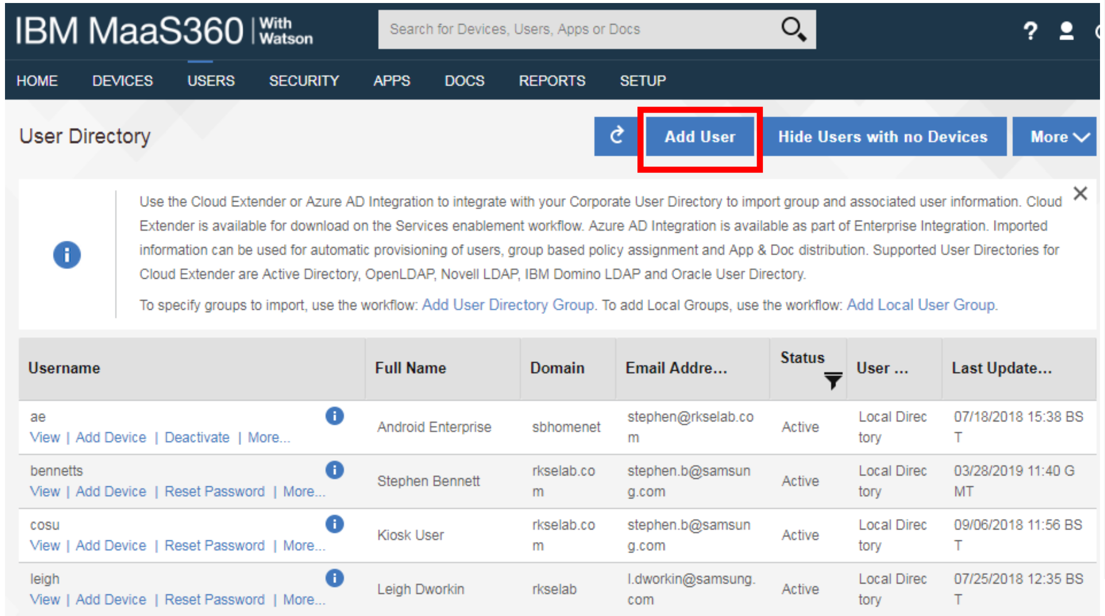


Dedicated Device

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.

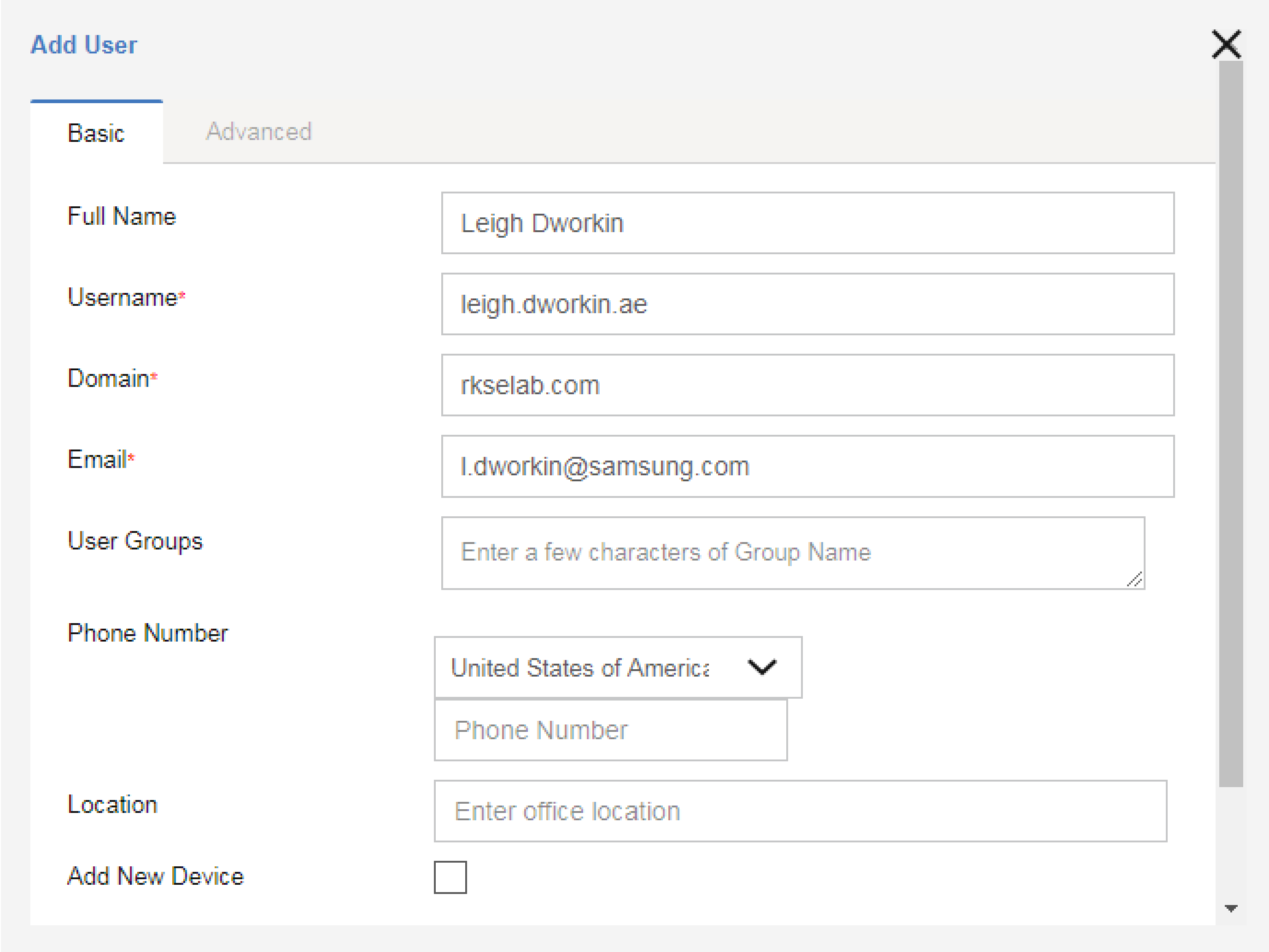


User Directory

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

To specify groups to import, use the workflow: Add User Directory Group. To add Local Groups, use the workflow: Add Local User Group.

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



Full Name: Leigh Dworkin

Username*: leigh.dworkin.ae

Domain*: rkselab.com

Email*: l.dworkin@samsung.com

User Groups: Enter a few characters of Group Name

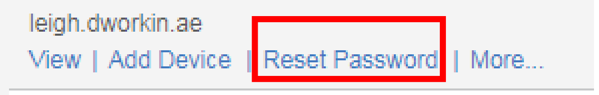
Phone Number: United States of America

Phone Number

Location: Enter office location

Add New Device □

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

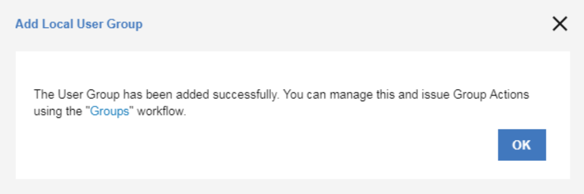


leigh.dworkin.ae

View | Add Device | Reset Password | More...

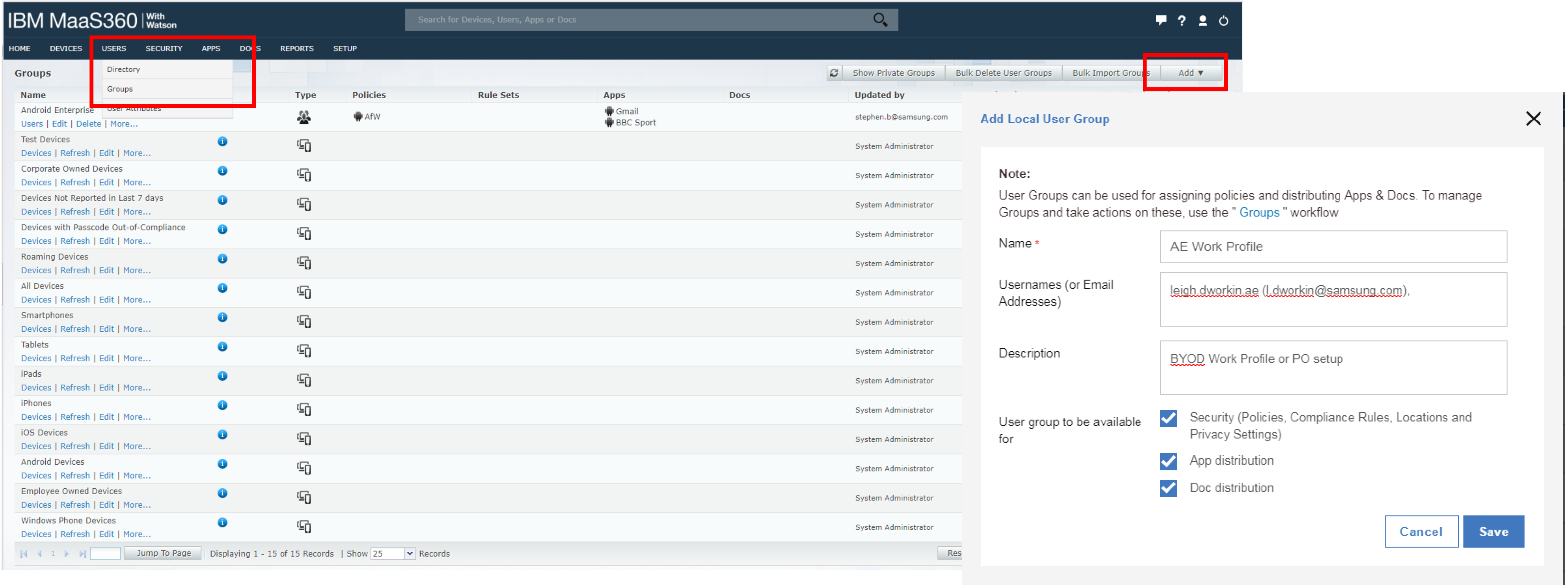
Add User to a Group in MaaS360

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



Add Local User Group

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



Groups

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

Add Local 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

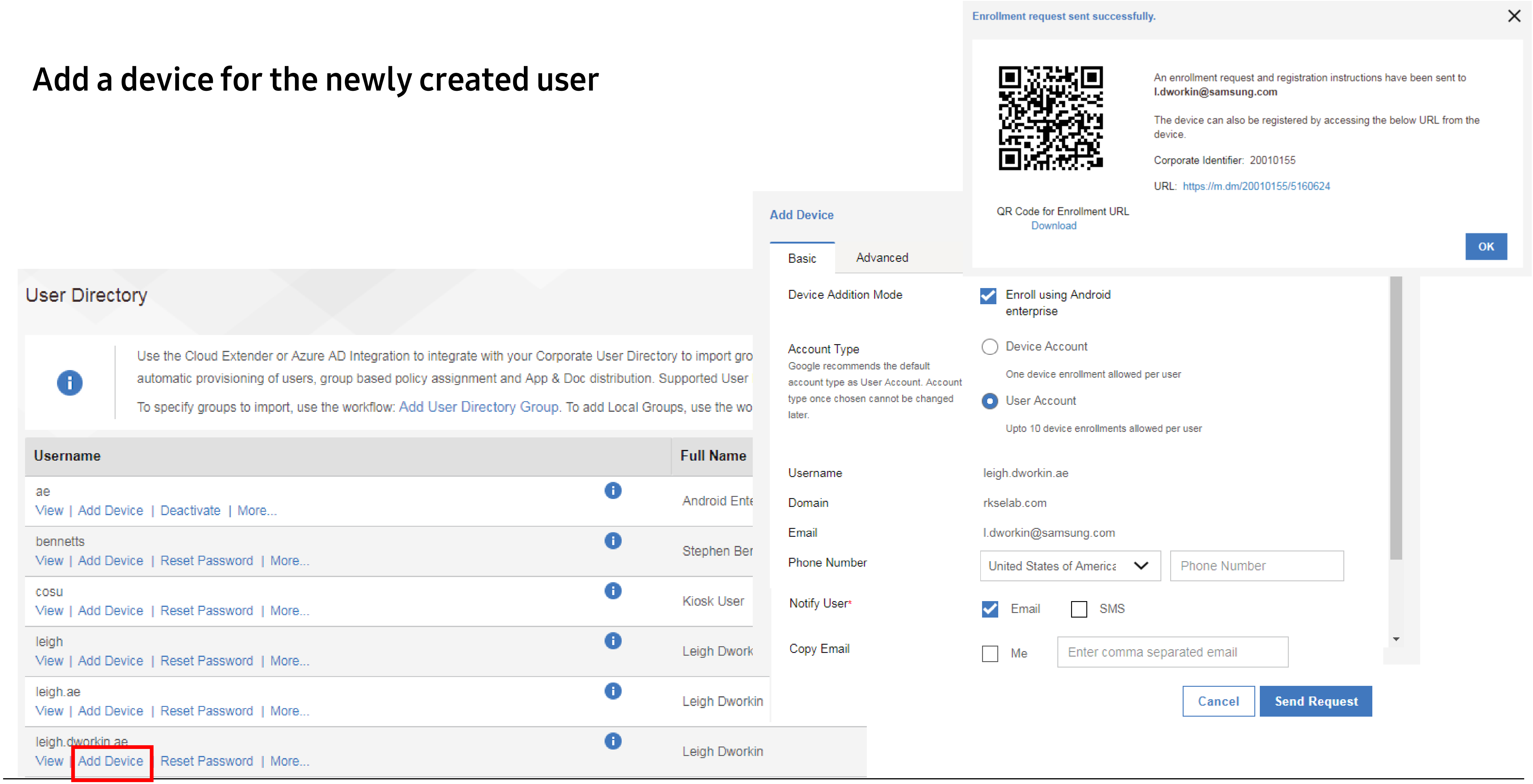
Name *: AE Work Profile

Usernames (or Email Addresses): leigh.dworkin.ae (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

Add a device for the newly created user



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

QR Code for Enrollment URL
Download

Add Device

Device Addition Mode: ☑ Enroll using Android enterprise

Account Type
Google recommends the default account type as User Account. Account type once chosen cannot be changed later.

○ 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 Americ‹ | Phone Number

Notify User*: ☑ Email □ SMS

Copy Email: □ Me | Enter comma separated email

User Directory

Use the Cloud Extender or Azure AD Integration to integrate with your Corporate User Directory to import gro
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

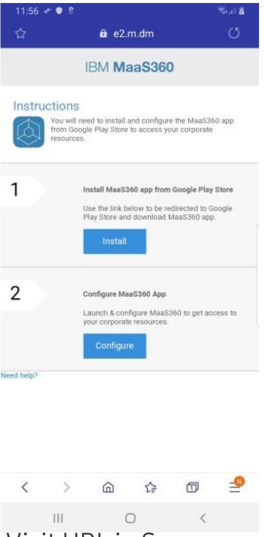
Username	Full Name
ae View | Add Device | Deactivate | More...	Android Ente
bennetts View | Add Device | Reset Password | More...	Stephen Ber
cosu View | Add Device | Reset Password | More...	Kiosk User
leigh View | Add Device | Reset Password | More...	Leigh Dwork
leigh.ae View | Add Device | Reset Password | More...	Leigh Dworkin
leigh.dworkin.ae View | Add Device | Reset Password | More...	Leigh Dworkin

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:


e2.m.dm

IBM MaaS360

Instructions

You will need to install and configure the MaaS360 app from Google Play Store to access your corporate resources.

1 Install MaaS360 app from Google Play Store

Use the link below to be redirected to Google Play Store and download MaaS360 app.

Install

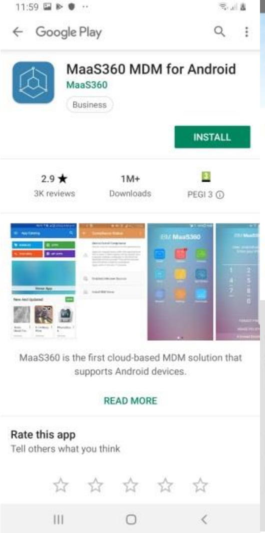
2 Configure MaaS360 App

Launch & configure MaaS360 to get access to your corporate resources.

Configure

Need help?

Visit URL in Samsung Browser from Email invitation. Click Install


Google Play

MaaS360 MDM for Android

MaaS360

Business

INSTALL

2.9 ★ 3K reviews | 1M+ Downloads | PEGI 3

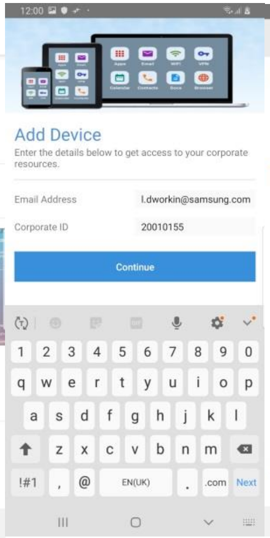
MaaS360 is the first cloud-based MDM solution that supports Android devices.

READ MORE

Rate this app

Tell others what you think

Install MaaS360 agent from Google Play Store


Add Device

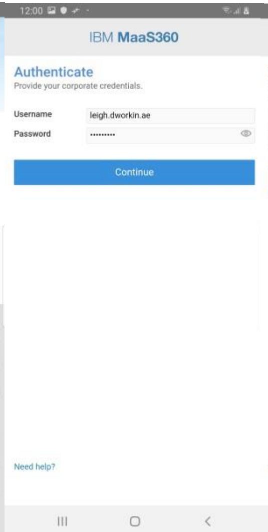
Enter the details below to get access to your corporate resources.

Email Address: l.dworkin@samsung.com

Corporate ID: 20010155

Continue

Check email and hit Continue


IBM MaaS360

Authenticate

Provide your corporate credentials.

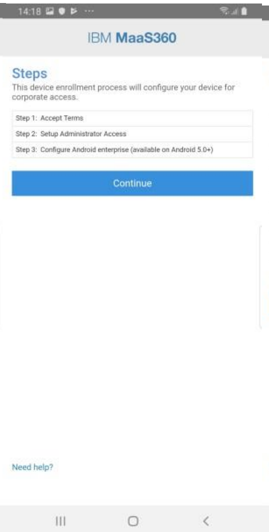
Username: leigh.dworkin.ae

Password: ••••••••••

Continue

Need help?

Enter user credentials & hit Continue


IBM MaaS360

Steps

This device enrollment process will configure your device for corporate access.

Step 1: Accept Terms

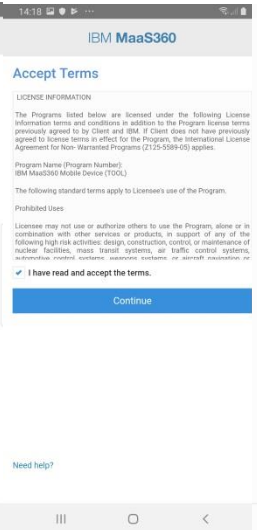
Step 2: Setup Administrator Access

Step 3: Configure Android enterprise (available on Android 5.0+)

Continue

Need help?

Review Steps & hit Continue


IBM MaaS360

Accept Terms

LICENSE INFORMATION

The Programs listed below are licensed under the following License Information terms and conditions in addition to the Program license terms previously agreed to by Client and IBM. If Client does not have previously agreed to license terms in effect for the Program, the International License Agreement for Non- Warranted Programs (Z125-5589-05) applies.

Program Name (Program Number):
IBM MaaS360 Mobile Device (TOOL)

The following standard terms apply to Licensee's use of the Program.

Prohibited Uses

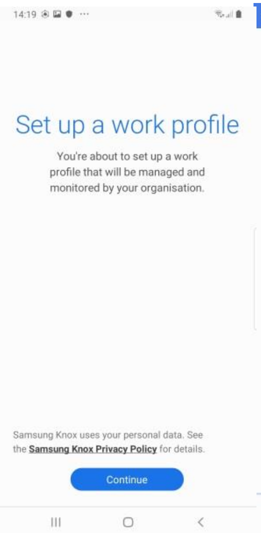
Licensee may not use or authorize others to use the Program, alone or in combination with other services or products, in support of any of the following high risk activities: design, construction, control, or maintenance of nuclear facilities, mass transit systems, air traffic control systems, automotive control systems, weapons systems, or aircraft navigation or

☑ I have read and accept the terms.

Continue

Need help?

Accept terms and conditions

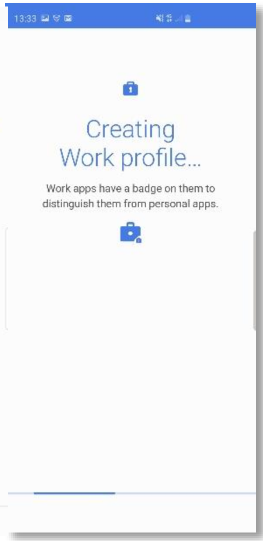

Set up a work profile

You're about to set up a work profile that will be managed and monitored by your organisation.

Samsung Knox uses your personal data. See the **Samsung Knox Privacy Policy** for details.

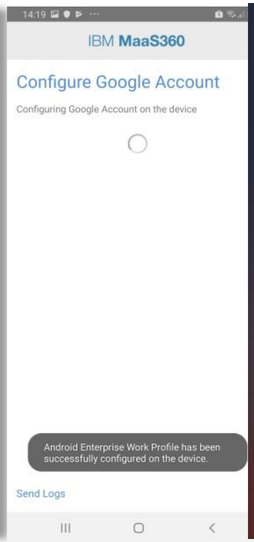
Continue

Click Continue to create Work Profile


Creating Work profile...

Work apps have a badge on them to distinguish them from personal apps.

Creating Work Profile


IBM MaaS360

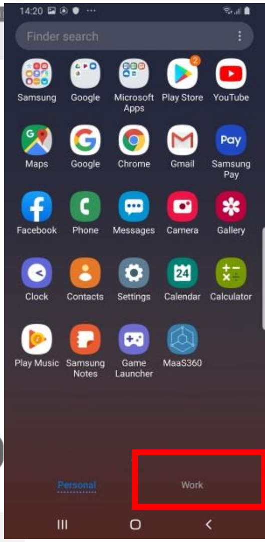
Configure Google Account

Configuring Google Account on the device

Android Enterprise Work Profile has been successfully configured on the device.

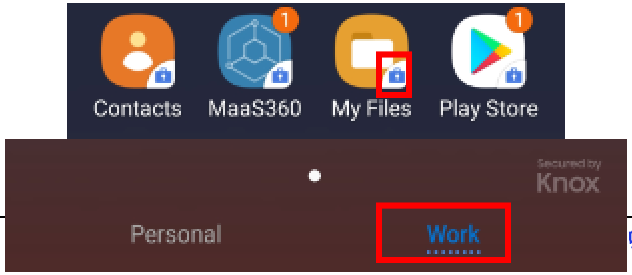
Send Logs

Device Enrollment Successful!



Work Tab Created

<span style="color:red">*You can also enroll your device using the alternative IBM MaaS360 methods. For example QR Code.</span>



What to look out for in the Work Tab

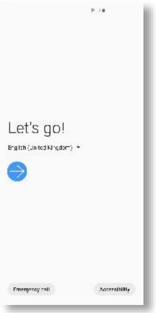
Android Enterprise: Company-owned Device

Android Enterprise Company-owned Device Deployment

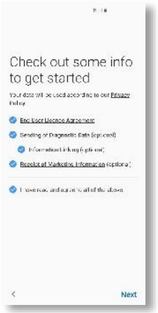
To enroll your device as an Android Enterprise Company-owned device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 3 ways you can enroll your device into Workspace ONE UEM as an Android Enterprise Company-owned device.

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 -> QR Code for Android Enterprise DO Provisioning)`
3. Knox Mobile Enrollment `(MaaS360 Portal -> Devices -> Enrollments -> Other Enrollment Options -> KNOX Mobile Enrollment)`

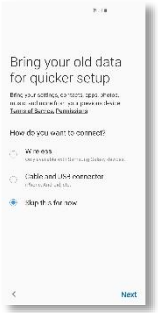
- Below is a screen-by-screen play to enroll your device using the DPC Identifier method:



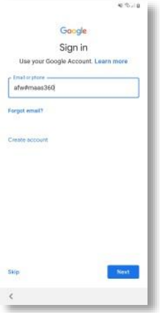
Click Start arrow



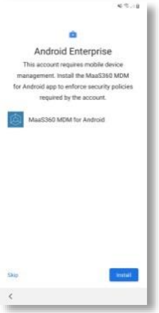
Accept T's & C's



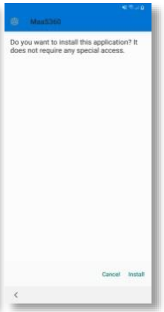
Skip Import of Old Data



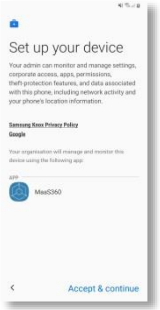
Enter afw#maas360 and click next



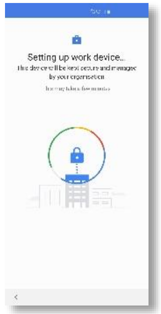
Install MaaS360 MDM app



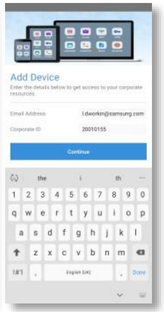
Install MaaS360 MDM app



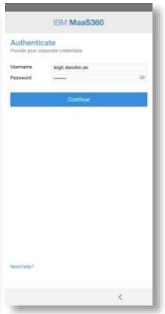
Accept & Continue



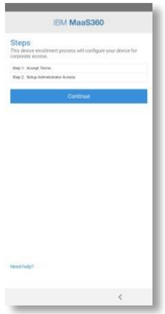
Setting Up Work Device



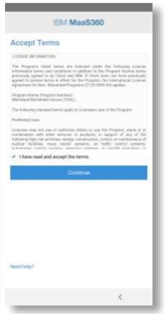
Enter email and Corporate ID



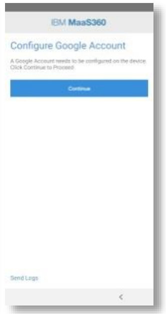
Enter Credentials



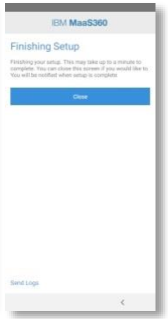
Review Steps And Continue



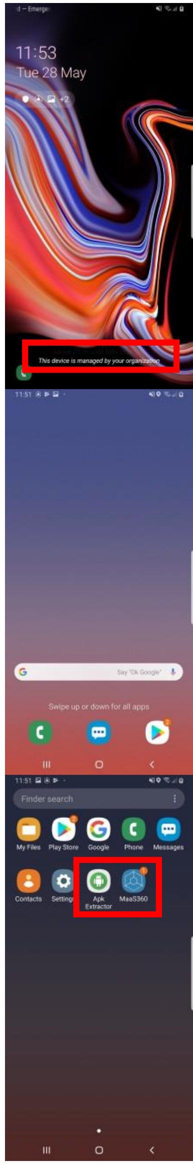
Accept Terms and Continue



Configure Google Account - Continue



Setup Finished Click Close



Device Enrollment Successful!

Android Enterprise: Company-owned Device

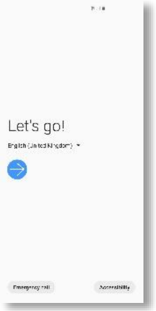
Knox

Android Enterprise Company-owned Device Deployment

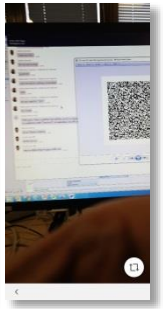
To enroll your device as an Android Enterprise Company-owned device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 3 ways you can enroll your device into Workspace ONE UEM as an Android Enterprise Company-owned device.

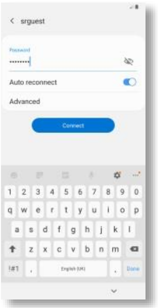
1. DPC Identifier [Also known as the hashtag method] afw#maas360
2. QR Code Enrollment / NFC Enrollment –
   - `scan QR code (MaaS360 Portal -> Devices -> Enrollments -> Other Enrollment Options -> QR Code for Android Enterprise DO Provisioning)`
3. Knox Mobile Enrollment `(MaaS360 Portal -> Devices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

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

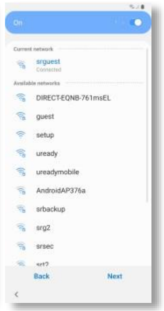

Let's go!

Click 6 times On 1st screen

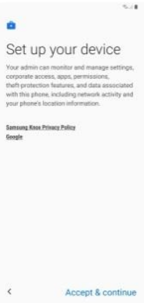

Scan QR Code Generated in Console



Connect to WiFi

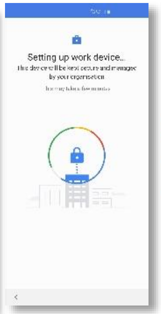


Click Next When Connected

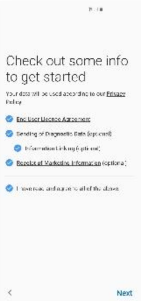

Set up your device

Accept & continue

Accept & Continue

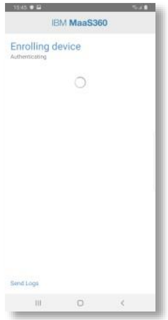

Setting up work device...

Setting Up Work Device


Check out some info to get started

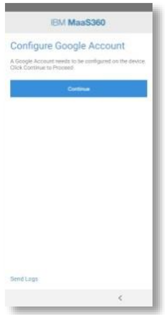
Next

Accept T's & C's


IBM MaaS360

Enrolling device

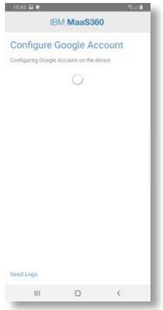
Wait for Enrollment


IBM MaaS360

Configure Google Account

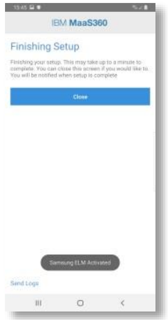
Continue

Configure Google Account - Continue


IBM MaaS360

Configure Google Account

Wait for Google Account Configuration

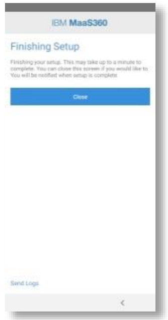

IBM MaaS360

Finishing Setup

Close

Samsung ELM Activated

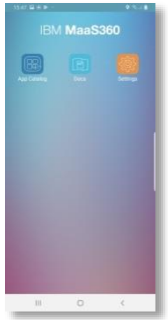
Setup Finishing Note ELM Activation


IBM MaaS360

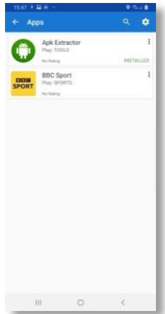
Finishing Setup

Close

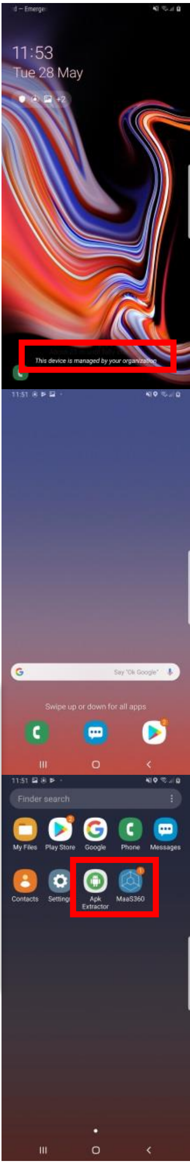
Setup Finished Click Close


IBM MaaS360

Open App Catalog



Note apps Installed



Device Enrollment Successful!

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 IMB MaaS360.

It should be supported before the end of H1 2019 (TBC).

Android Enterprise: Dedicated Device

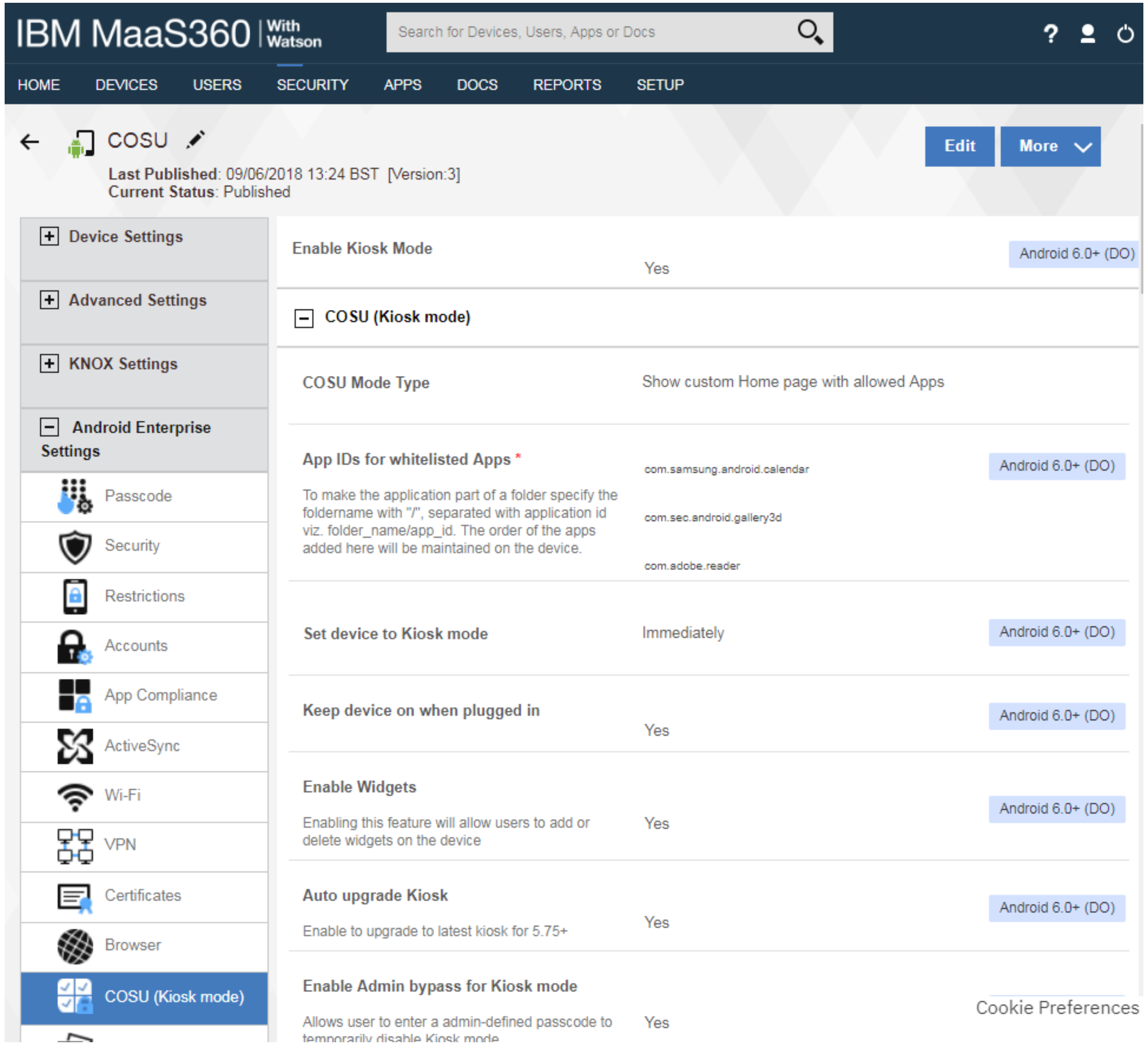
Android Enterprise Dedicated Device Deployment

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



COSU

Last Published: 09/06/2018 13:24 BST [Version:3]
Current Status: Published

Enable Kiosk Mode — Yes — Android 6.0+ (DO)

COSU (Kiosk mode)

COSU Mode Type — Show custom Home page with allowed Apps

App IDs for whitelisted Apps * — Android 6.0+ (DO)
To make the application part of a folder specify the foldername with "/", separated with application id viz. folder_name/app_id. The order of the apps added here will be maintained on the device.
com.samsung.android.calendar
com.sec.android.gallery3d
com.adobe.reader

Set device to Kiosk mode — Immediately — Android 6.0+ (DO)

Keep device on when plugged in — Yes — Android 6.0+ (DO)

Enable Widgets — Yes — Android 6.0+ (DO)
Enabling this feature will allow users to add or delete widgets on the device

Auto upgrade Kiosk — Yes — Android 6.0+ (DO)
Enable to upgrade to latest kiosk for 5.75+

Enable Admin bypass for Kiosk mode — Yes
Allows user to enter a admin-defined passcode to temporarily disable Kiosk mode

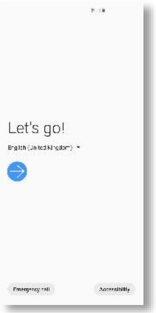
Android Enterprise: Dedicated Device (COSU)

Android Enterprise Company-owned Device Deployment

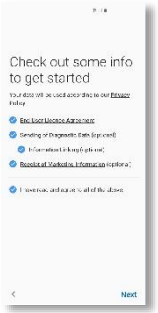
To enroll your device as an Android Enterprise Company-owned device, you need to ensure the device is factory reset and at the welcome screen. From here, there are 3 ways you can enroll your device into Workspace ONE UEM as an Android Enterprise Company-owned device.

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)

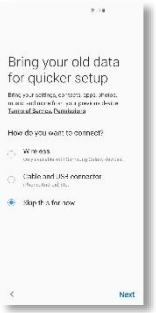
- Below is a screen-by-screen play to enroll your device using the DPC Identifier method:



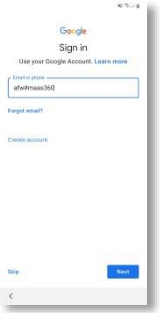
Click Start arrow



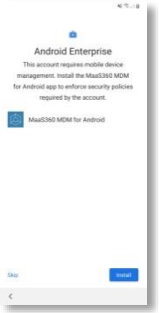
Accept T's & C's



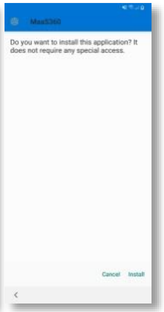
Skip Import of Old Data



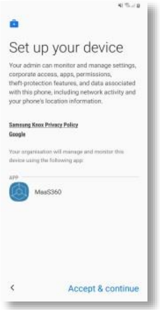
Enter afw#maas360 and click next



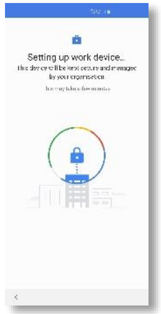
Install MaaS360 MDM app



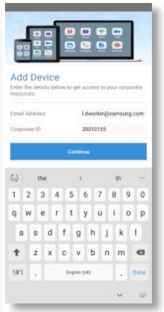
Install MaaS360 MDM app



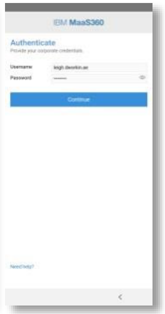
Accept & Continue



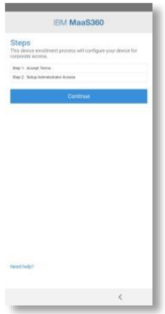
Setting Up Work Device



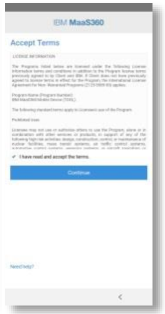
Enter email and Corporate ID



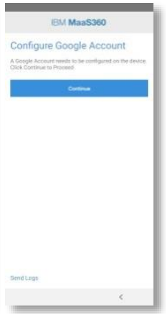
Enter Credentials



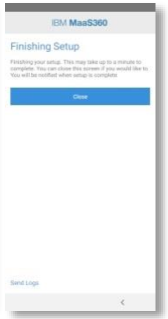
Review Steps And Continue



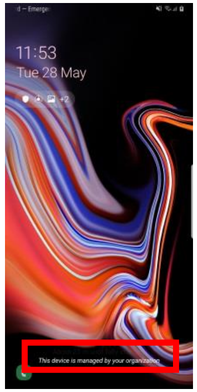
Accept Terms and Continue



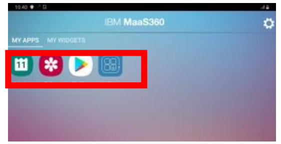
Configure Google Account - Continue



Setup Finished Click Close



Device Enrollment Successful!



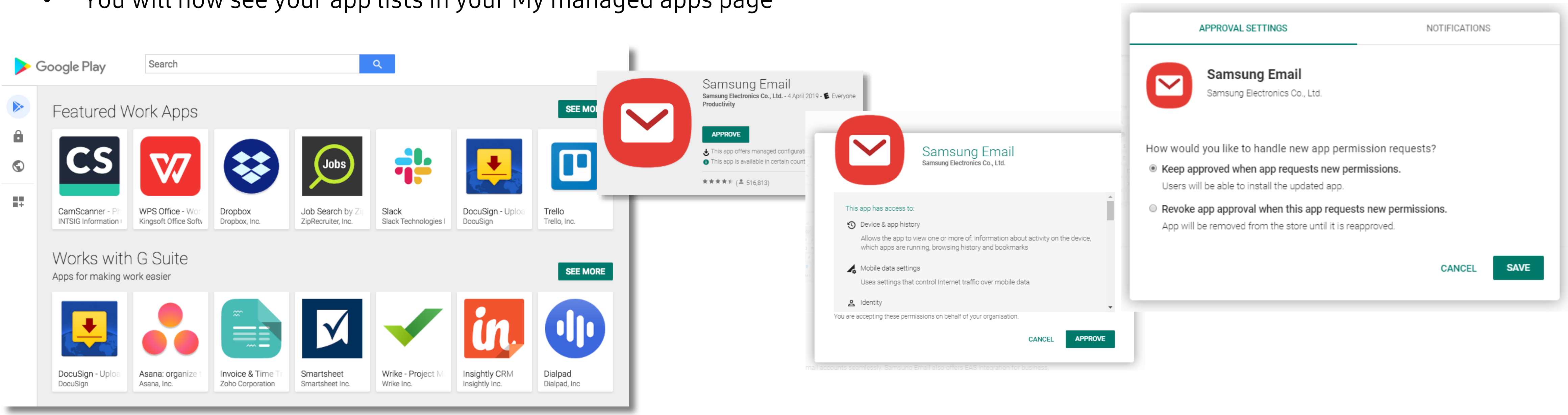
←-----------Kiosked

Managed Google Play Configuration

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



Samsung Email
Samsung Electronics Co., Ltd. - 4 April 2019 - Everyone
Productivity

APPROVE

This app offers managed configurati
This app is available in certain count
★★★★½ (516,813)

Samsung Email
Samsung Electronics Co., Ltd.

This app has access to:

Device & app history
Allows the app to view one or more of: information about activity on the device, which apps are running, browsing history and bookmarks

Mobile data settings
Uses settings that control Internet traffic over mobile data

Identity

You are accepting these permissions on behalf of your organisation.

CANCEL APPROVE

APPROVAL SETTINGS NOTIFICATIONS

Samsung Email
Samsung Electronics Co., Ltd.

How would you like to handle new app permission requests?

● Keep approved when app requests new permissions.
Users will be able to install the updated app.

○ Revoke app approval when this app requests new permissions.
App will be removed from the store until it is reapproved.

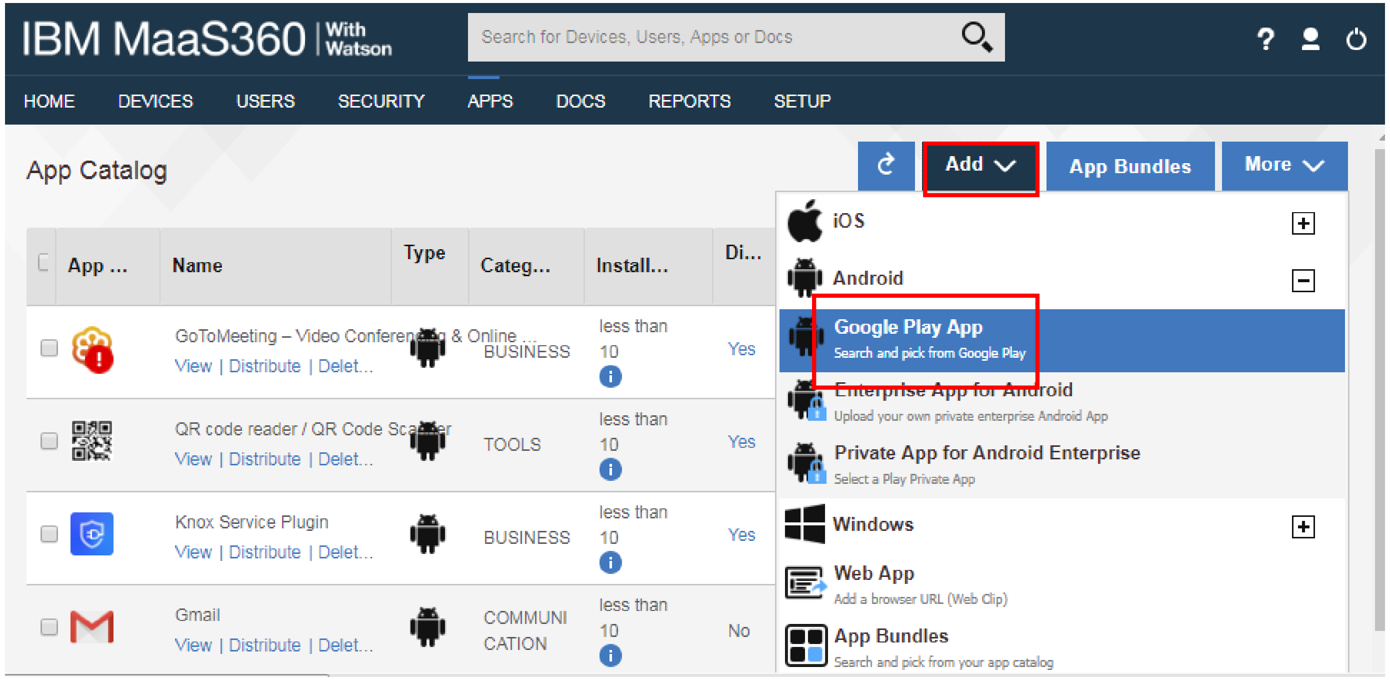
CANCEL SAVE

Managed Google Play Configuration

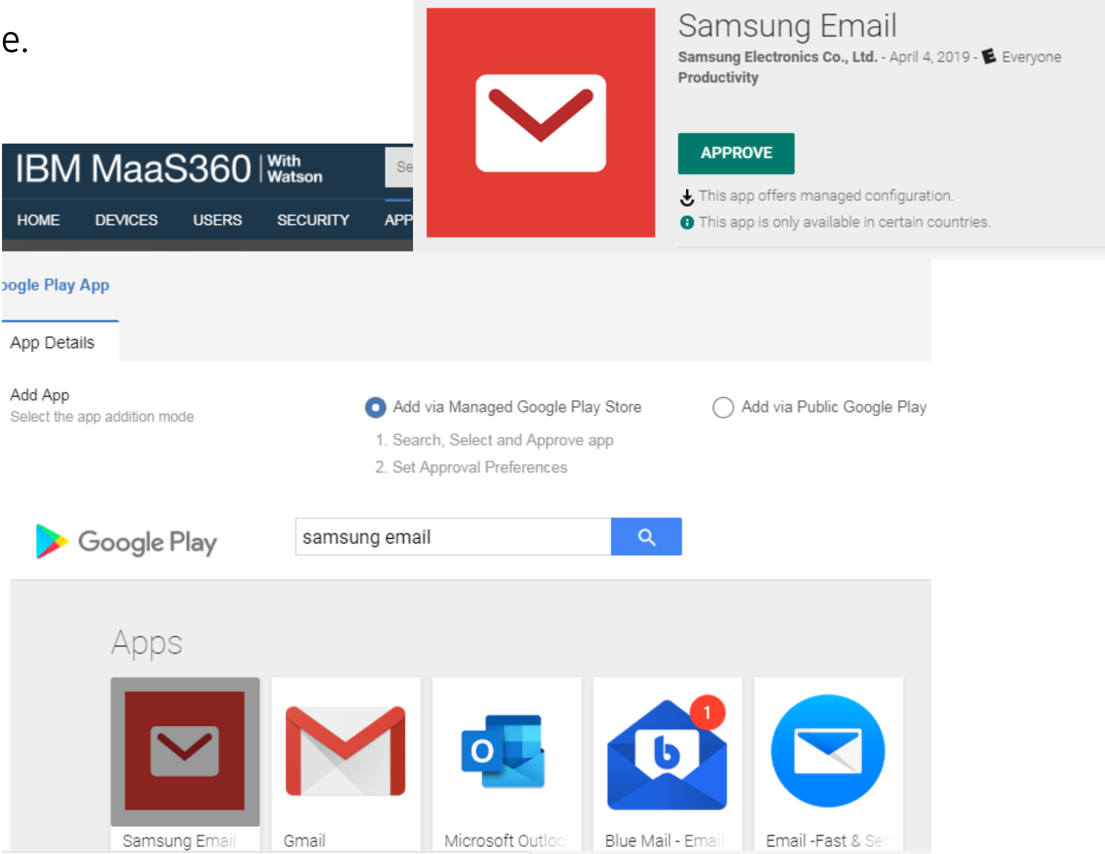
Managed Google Play Configuration

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**


IBM MaaS360 With Watson
Search for Devices, Users, Apps or Docs
HOME
DEVICES
USERS
SECURITY
APPS
DOCS
REPORTS
SETUP
App Catalog
Add
App Bundles
More
iOS
Android
Google Play App
Search and pick from Google Play
Enterprise App for Android
Upload your own private enterprise Android App
Private App for Android Enterprise
Select a Play Private App
Windows
Web App
Add a browser URL (Web Clip)
App Bundles
Search and pick from your app catalog

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



Samsung Email

Samsung Electronics Co., Ltd. - April 4, 2019 - Everyone

Productivity

This app offers managed configuration.

This app is only available in certain countries.

Add App

Select the app addition mode

● Add via Managed Google Play Store ○ Add via Public Google Play

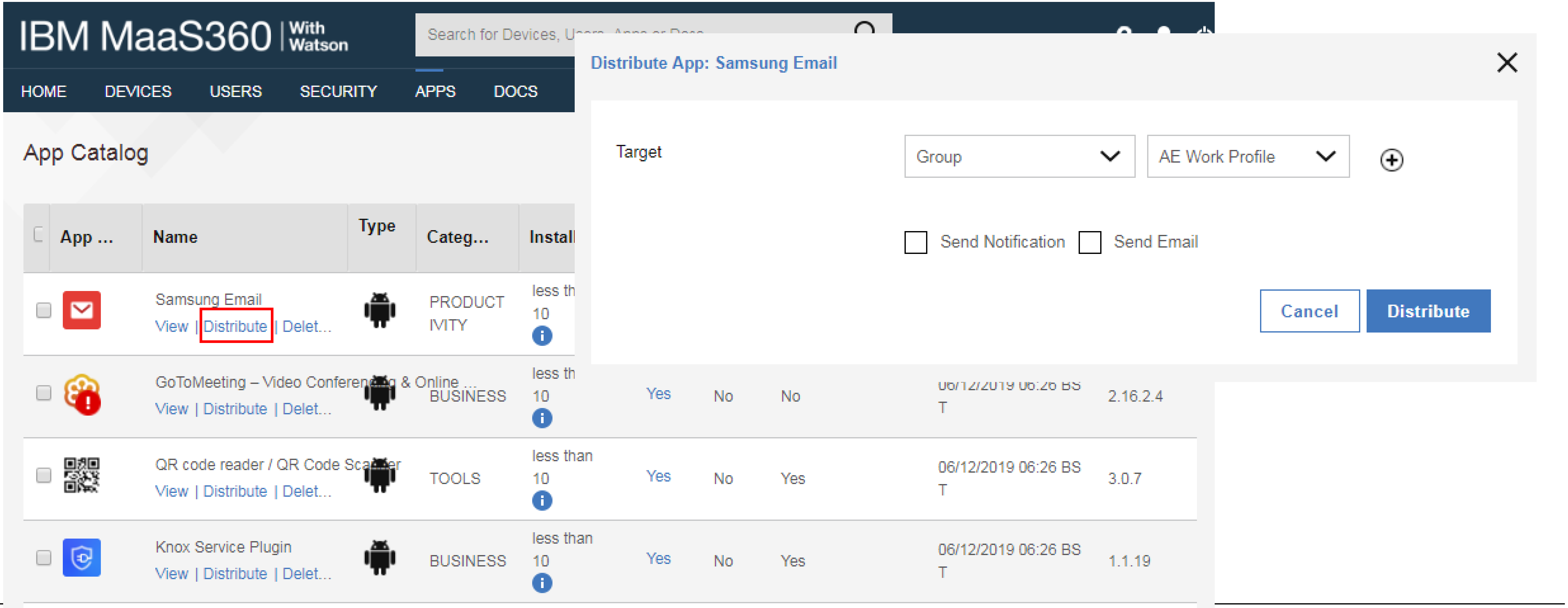
1. Search, Select and Approve app
2. Set Approval Preferences

samsung email

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**.



App Catalog

☐	App ...	Name	Type	Categ...	Install					
☐		Samsung Email View | Distribute | Delet...		PRODUCTIVITY	less th 10					
☐		GoToMeeting – Video Conferencing & Online ... View | Distribute | Delet...		BUSINESS	less th 10	Yes	No	No	06/12/2019 06:26 BST	2.16.2.4
☐		QR code reader / QR Code Scanner View | Distribute | Delet...		TOOLS	less than 10	Yes	No	Yes	06/12/2019 06:26 BST	3.0.7
☐		Knox Service Plugin View | Distribute | Delet...		BUSINESS	less than 10	Yes	No	Yes	06/12/2019 06:26 BST	1.1.19

Distribute App: Samsung Email

Target: Group, AE Work Profile

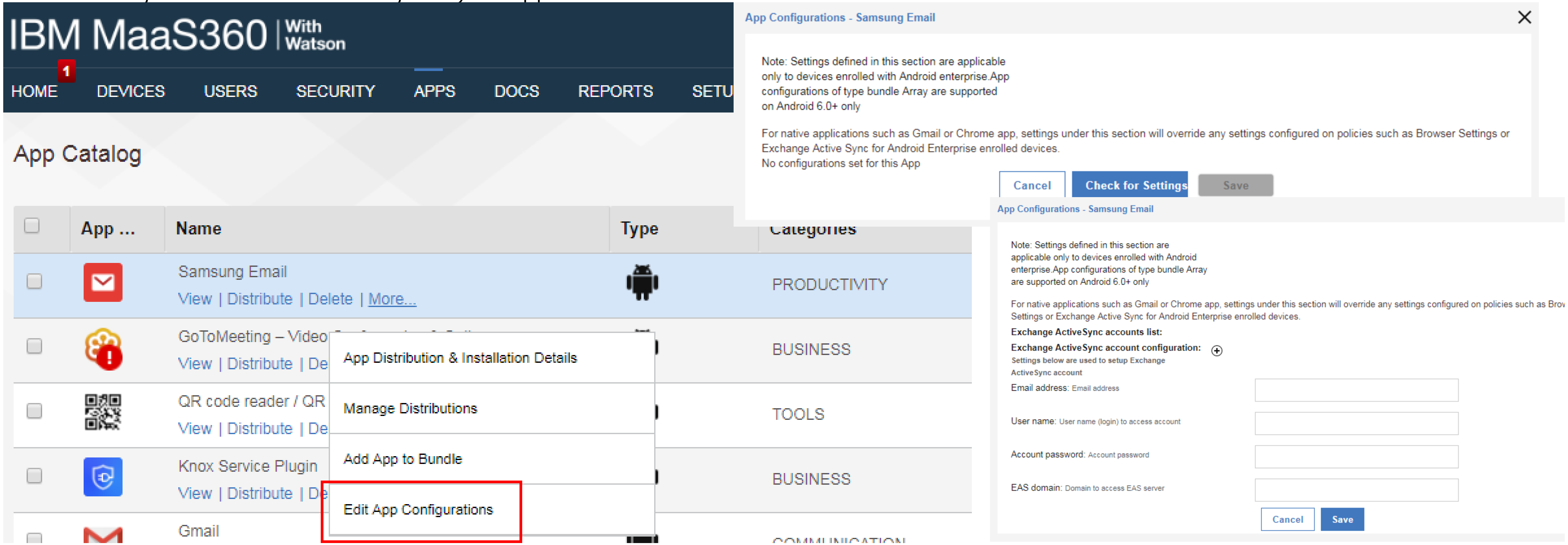
☐ Send Notification ☐ Send Email

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



App Catalog

□	App ...	Name	Type	Categories
□		Samsung Email View | Distribute | Delete | More...		PRODUCTIVITY
□		GoToMeeting – Video View | Distribute | De		BUSINESS
□		QR code reader / QR View | Distribute | De		TOOLS
□		Knox Service Plugin View | Distribute | De		BUSINESS
□		Gmail		COMMUNICATION

App Configurations - Samsung Email

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.
No configurations set for this App

App Configurations - Samsung Email

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 Brov Settings or Exchange Active Sync for Android Enterprise enrolled devices.

Exchange ActiveSync accounts list:

Exchange ActiveSync account configuration: ⊕
Settings below are used to setup Exchange ActiveSync account

Email address: Email address

User name: User name (login) to access account

Account password: Account password

EAS domain: Domain to access EAS server

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 [$]

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.

SAMSUNG
Knox Platform
for Enterprise
Android
Enterprise

Configure Knox Platform for Enterprise : Standard Edition

Configure KPE : Standard Edition on IBM MaaS360

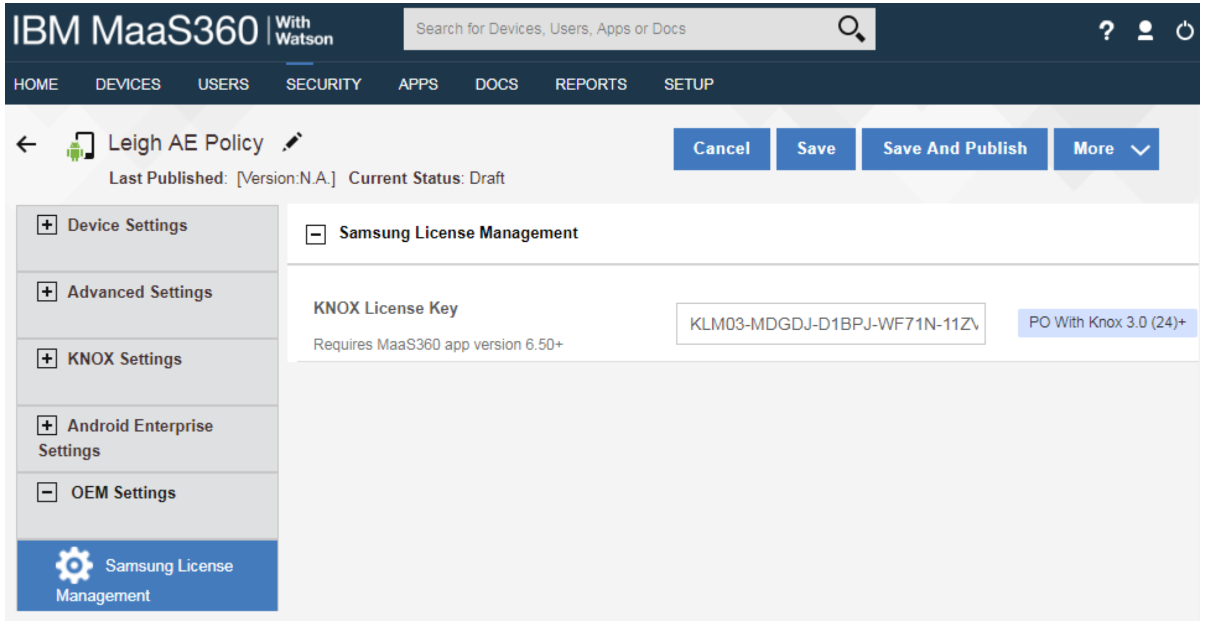
- This is on by default with Android Enterprise on a Samsung Device

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



Leigh AE Policy

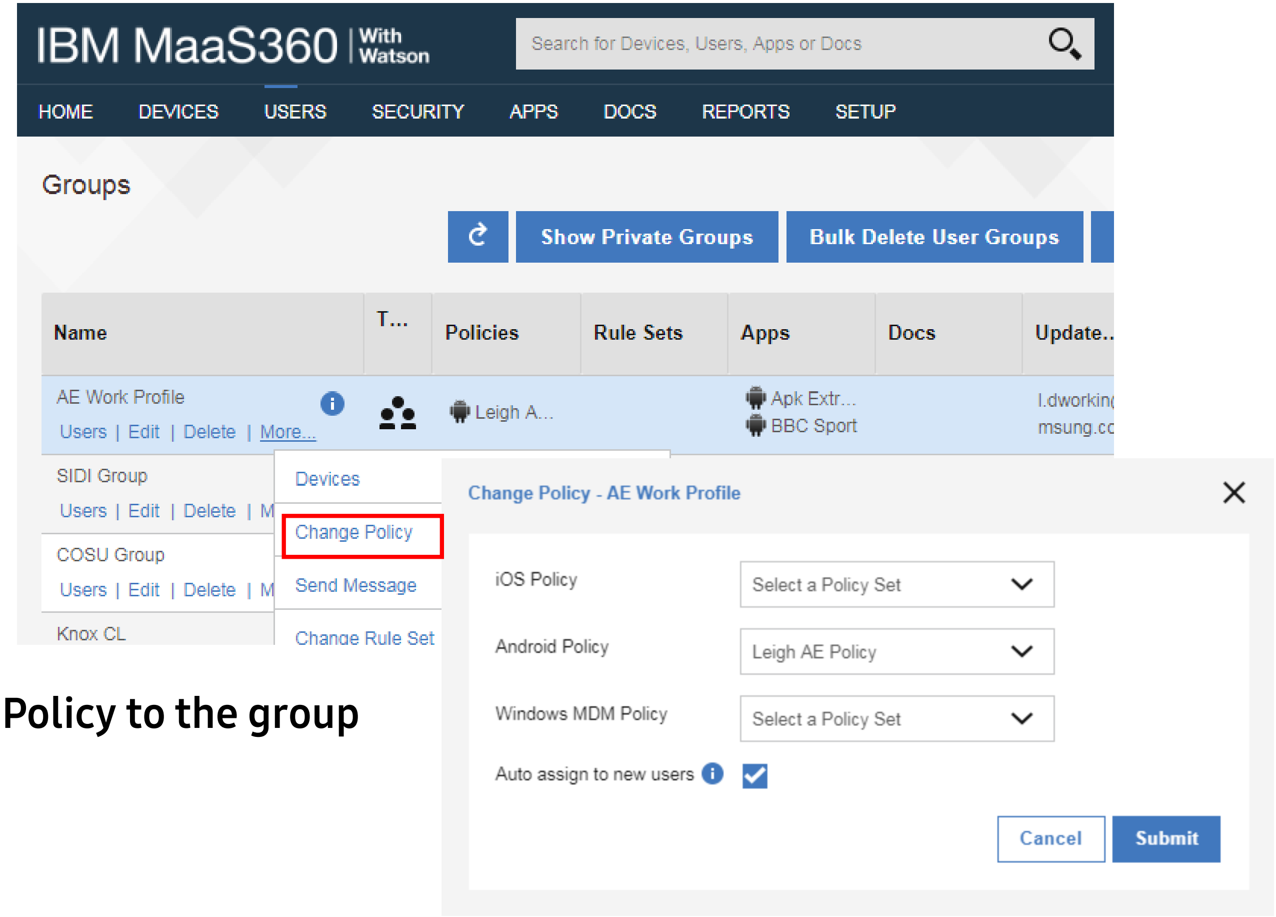
Last Published: [Version:N.A.] Current Status: Draft

Samsung License Management

KNOX License Key: KLM03-MDGDJ-D1BPJ-WF71N-11ZV

Requires MaaS360 app version 6.50+

PO With Knox 3.0 (24)+



Groups

Name	T...	Policies	Rule Sets	Apps	Docs	Update..
AE Work Profile Users | Edit | Delete | More...		Leigh A...		Apk Extr... BBC Sport		l.dworkin msung.cc
SIDI Group Users | Edit | Delete | M						
COSU Group Users | Edit | Delete | M						
Knox CL						

Change Policy - AE Work Profile

iOS Policy: Select a Policy Set

Android Policy: Leigh AE Policy

Windows MDM Policy: Select a Policy Set

Auto assign to new users ☑

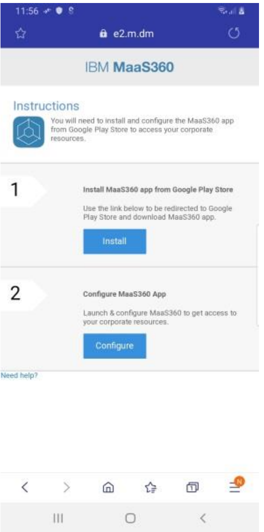
- Then in Users->Groups choose More… and assign the new Policy to the group

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:



e2.m.dm

IBM MaaS360

Instructions

You will need to install and configure the MaaS360 app from Google Play Store to access your corporate resources.

1 Install MaaS360 app from Google Play Store

Use the link below to be redirected to Google Play Store and download MaaS360 app.

Install

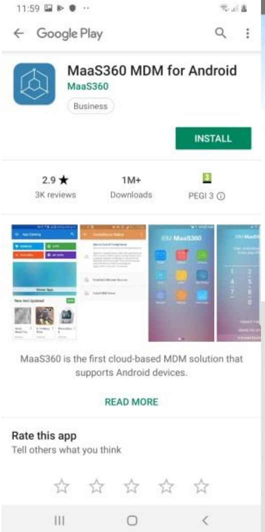
2 Configure MaaS360 App

Launch & configure MaaS360 to get access to your corporate resources.

Configure

Need help?

Visit URL in Samsung Browser from Email invitation. Click Install



Google Play

MaaS360 MDM for Android

MaaS360

Business

INSTALL

2.9 ★ 3K reviews | 1M+ Downloads | PEGI 3

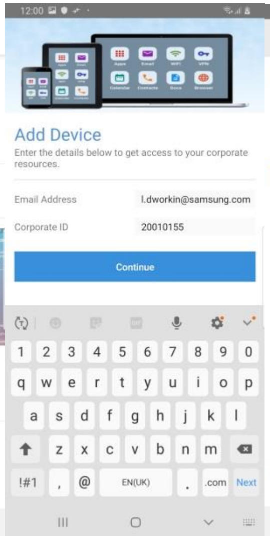
MaaS360 is the first cloud-based MDM solution that supports Android devices.

READ MORE

Rate this app

Tell others what you think

Install MaaS360 agent from Google Play Store



Add Device

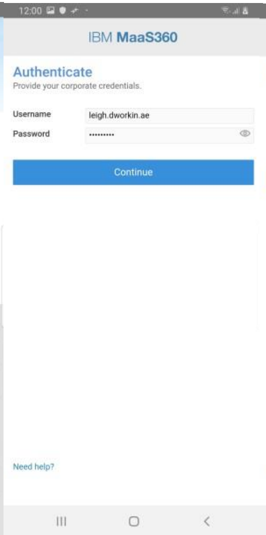
Enter the details below to get access to your corporate resources.

Email Address: l.dworkin@samsung.com

Corporate ID: 20010155

Continue

Check email and hit Continue



IBM MaaS360

Authenticate

Provide your corporate credentials.

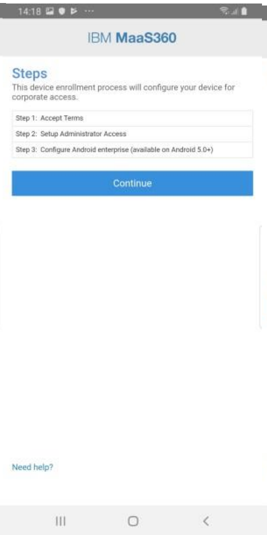
Username: leigh.dworkin.ae

Password: ••••••••••

Continue

Need help?

Enter user credentials & hit Continue



IBM MaaS360

Steps

This device enrollment process will configure your device for corporate access.

Step 1: Accept Terms

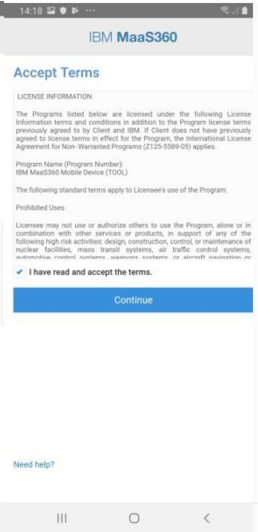
Step 2: Setup Administrator Access

Step 3: Configure Android enterprise (available on Android 5.0+)

Continue

Need help?

Review Steps & hit Continue



IBM MaaS360

Accept Terms

LICENSE INFORMATION

The Programs listed below are licensed under the following License Information terms and conditions in addition to the Program license terms previously agreed to by Client and IBM. If Client does not have previously agreed to license terms in effect for the Program, the International License Agreement for Non- Warranted Programs (Z125-5589-05) applies.

Program Name (Program Number):
IBM MaaS360 Mobile Device (TOOL)

The following standard terms apply to Licensee's use of the Program.

Prohibited Uses

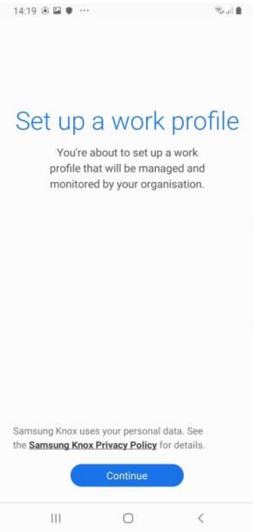
Licensee may not use or authorize others to use the Program, alone or in combination with other services or products, in support of any of the following high risk activities: design, construction, control, or maintenance of nuclear facilities, mass transit systems, air traffic control systems, automotive control systems, weapons systems, or aircraft navigation or

☑ I have read and accept the terms.

Continue

Need help?

Accept terms and conditions



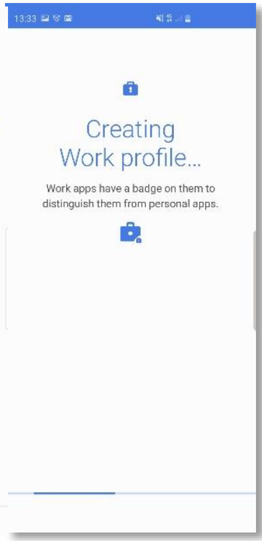
Set up a work profile

You're about to set up a work profile that will be managed and monitored by your organisation.

Samsung Knox uses your personal data. See the **Samsung Knox Privacy Policy** for details.

Continue

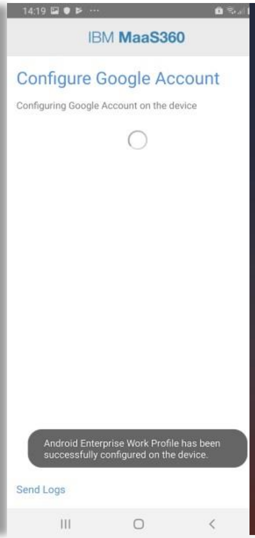
Click Continue to create Work Profile



Creating Work profile...

Work apps have a badge on them to distinguish them from personal apps.

Creating Work Profile



IBM MaaS360

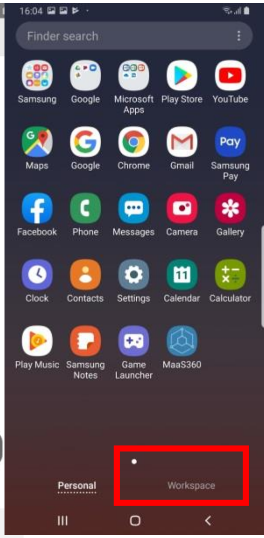
Configure Google Account

Configuring Google Account on the device

Android Enterprise Work Profile has been successfully configured on the device.

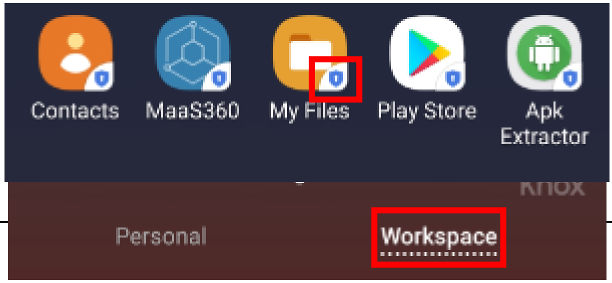
Send Logs

Device Enrollment Successful!



Workspace Tab Created

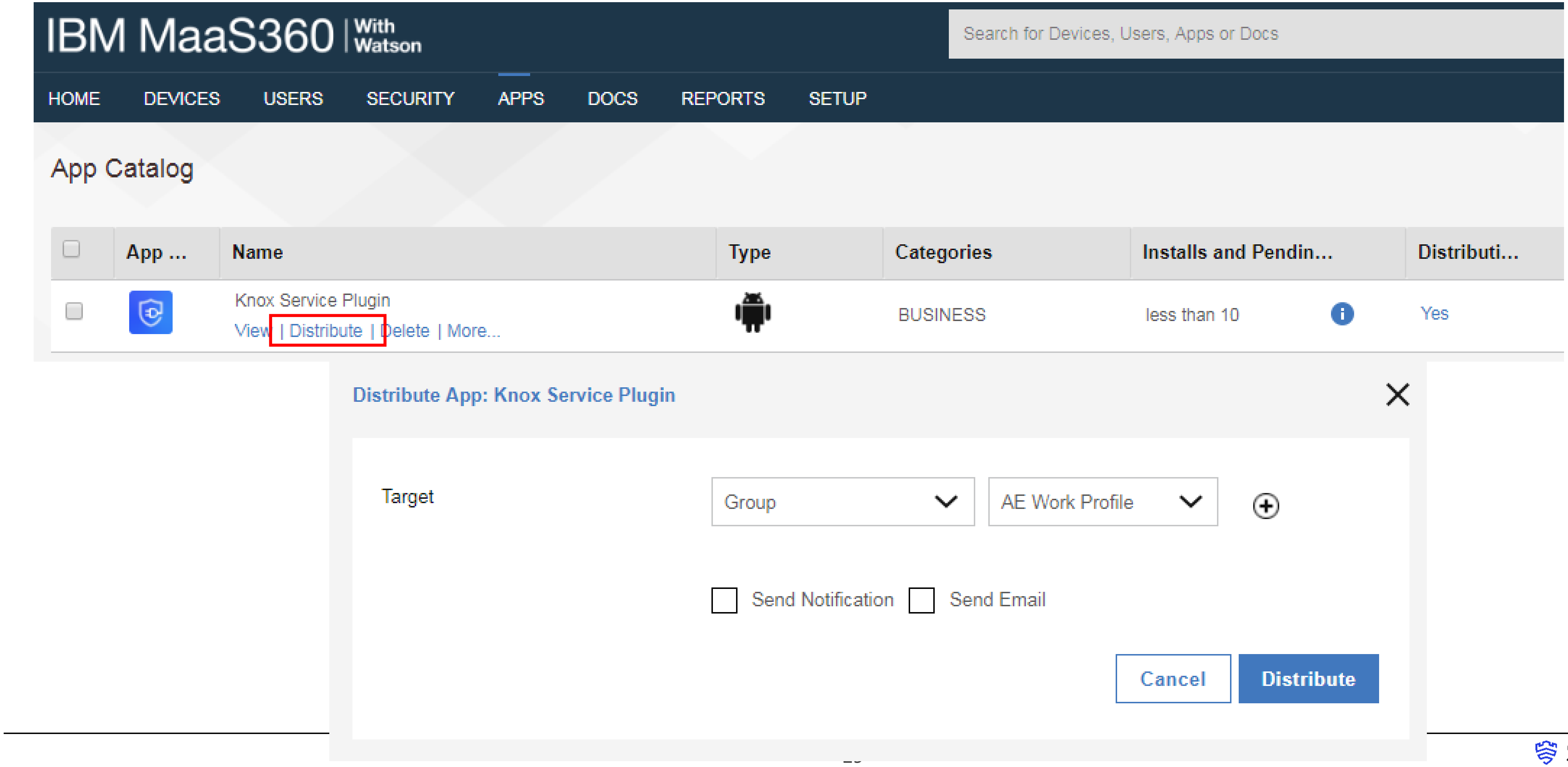
*You can also enroll your device using the alternative IBM MaaS360 methods. For example QR Code.



What to look out for in the Workspace 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

□	App ...	Name	Type	Categories	Installs and Pendin...	Distributi...
□		Knox Service Plugin View | Distribute | Delete | More...		BUSINESS	less than 10	Yes

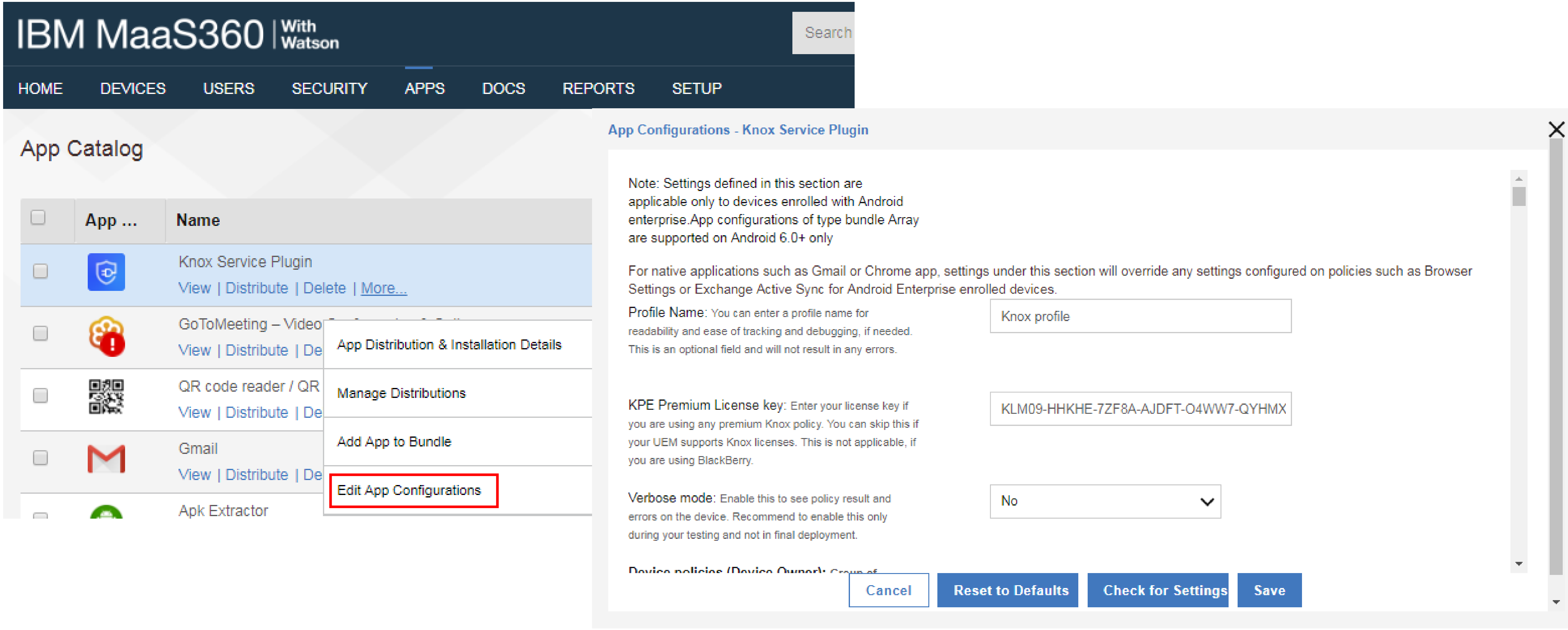
Distribute App: Knox Service Plugin

Target: Group; AE Work Profile

□ Send Notification □ Send Email

Knox Service Plugin [KSP]

IBM MaaS360 fully supports Knox Service Plugin.



App Configurations - Knox Service Plugin

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

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

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

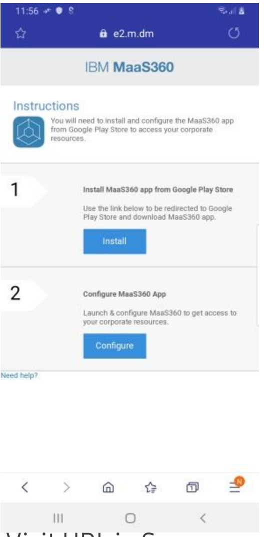
Device policies (Device Owner): Group of

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:



Instructions

You will need to install and configure the MaaS360 app from Google Play Store to access your corporate resources.

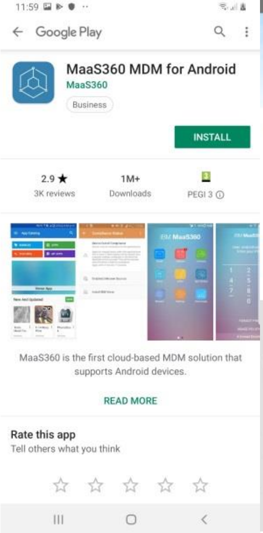
1 Install MaaS360 app from Google Play Store

Use the link below to be redirected to Google Play Store and download MaaS360 app.

2 Configure MaaS360 App

Launch & configure MaaS360 to get access to your corporate resources.

Visit URL in Samsung Browser from Email invitation. Click Install

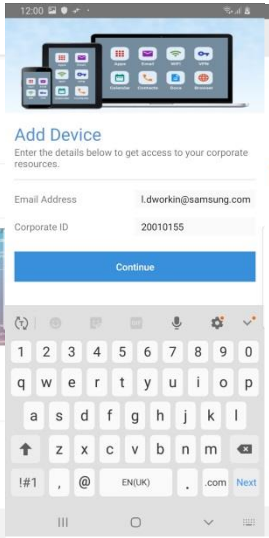


MaaS360 MDM for Android

MaaS360

MaaS360 is the first cloud-based MDM solution that supports Android devices.

Install MaaS360 agent from Google Play Store



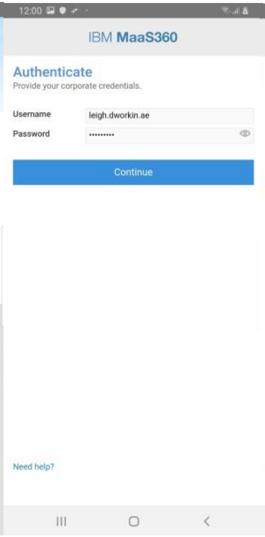
Add Device

Enter the details below to get access to your corporate resources.

Email Address: l.dworkin@samsung.com

Corporate ID: 20010155

Check email and hit Continue



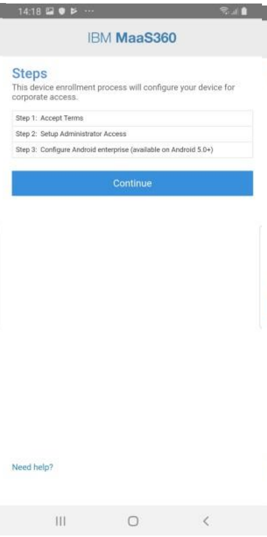
Authenticate

Provide your corporate credentials.

Username: leigh.dworkin.ae

Password: •••••••••

Enter user credentials & hit Continue



Steps

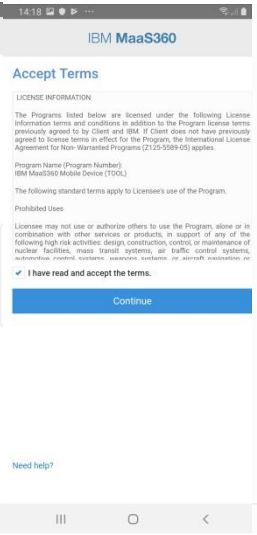
This device enrollment process will configure your device for corporate access.

Step 1: Accept Terms

Step 2: Setup Administrator Access

Step 3: Configure Android enterprise (available on Android 5.0+)

Review Steps & hit Continue



Accept Terms

LICENSE INFORMATION

The Programs listed below are licensed under the following License Information terms and conditions in addition to the Program license terms previously agreed to by Client and IBM. If Client does not have previously agreed to license terms in effect for the Program, the International License Agreement for Non- Warranted Programs (Z125-5589-05) applies.

Program Name (Program Number):
IBM MaaS360 Mobile Device (TOOL)

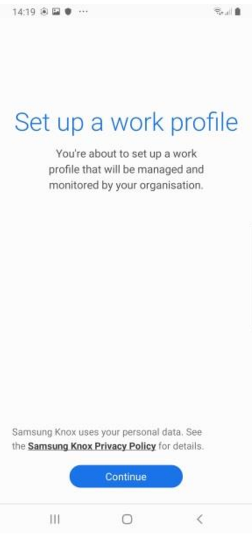
The following standard terms apply to Licensee's use of the Program.

Prohibited Uses

Licensee may not use or authorize others to use the Program, alone or in combination with other services or products, in support of any of the following high risk activities: design, construction, control, or maintenance of nuclear facilities, mass transit systems, air traffic control systems, automotive control systems, weapons systems, or aircraft navigation or

☑ I have read and accept the terms.

Accept terms and conditions

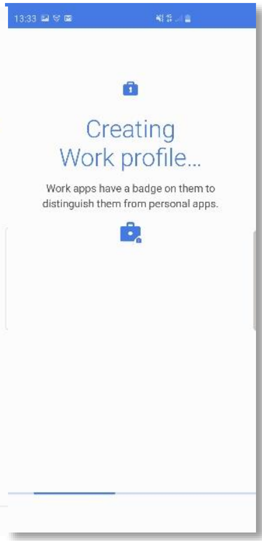


Set up a work profile

You're about to set up a work profile that will be managed and monitored by your organisation.

Samsung Knox uses your personal data. See the Samsung Knox Privacy Policy for details.

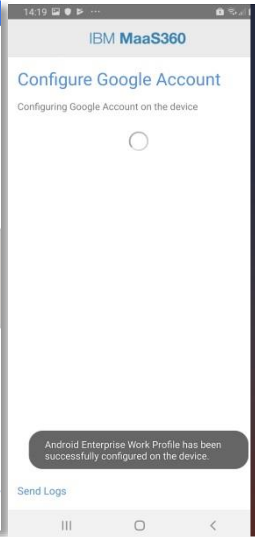
Click Continue to create Work Profile



Creating Work profile...

Work apps have a badge on them to distinguish them from personal apps.

Creating Work Profile

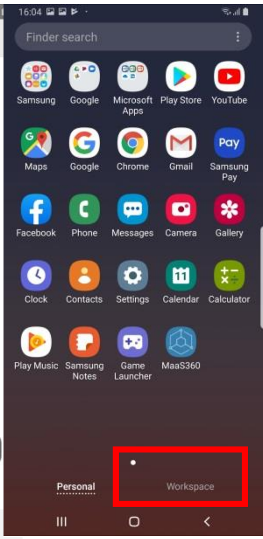


Configure Google Account

Configuring Google Account on the device

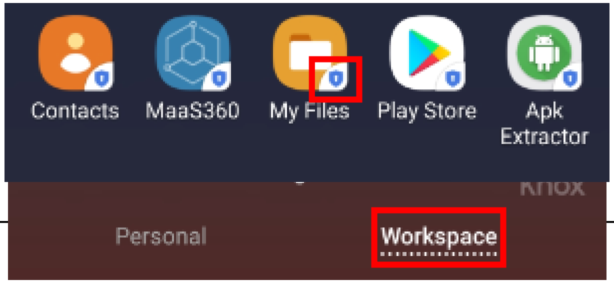
Android Enterprise Work Profile has been successfully configured on the device.

Device Enrollment Successful!



Workspace 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 Workspace Tab

Document Information

This is version 2 of this document.

Thank you!

Knox