Manage company owned Android devices - Checklist

MaaS360 Client Success | IBM Security MaaS360 with Watson | Oct 2020

IBM Security

Objective: Provide a checklist of simple deployment steps referencing training content and documentation focused on a company owned Android device deployment use case using MaaS360 integration with Android Enterprise. Note that when deploying Android Enterprise devices where you have full control over the device, this is considered a work device and is designated as Device Owner mode.
If you plan to manage devices where there is a separate work profile on a BYOD device without full control over the entire device, that is called Profile Owner .
Use Case Description: In this use case, devices can only be enrolled and managed from out of the box or by a factory reset. This use case provides several methods to choose from for device enrollment, with complete control over the device. These devices are typically purchased by your organization and provided to employees for work use.
Considerations: Maas360 has many features, settings and configuration options to meet your needs. This checklist's purpose is to get you started with common tasks. We recommend, you try this with a few devices and evaluate your configuration and alter as needed, then roll out to all your devices.
Prerequisites:

- Complete the MaaS360 Getting Started checklist
- Review the Comprehensive Guide to Android Enterprise Management
- Check that your devices are AE compatible. If you're unsure, check with your OEM and try enrollment of a test device.
- Choose a Device Owner enrollment method. Click each link for more information on each method and complete the prerequisites for each enrollment method.

Enrollment Workflow	Minimum OS version required	Description
NFC Bump	Android 5.1	An Admin sets up one device and bumps a target device to enroll it in AE Device Owner. NFC enabled devices must be tapped together to initiate enrollment.
MaaS360 Token	Android 6.0	Enter a token afw#maas360 in the Google Account to initiate the AE Device Owner enrollment.
QR Code	Android 7.0	Admin creates a QR code in MaaS360 portal and downloads it to enroll devices or provides it to users to enroll.
Zero Touch	Android 8.0	Devices must be purchased from a reseller who sets up the zero touch account and loads devices for your company. Provides bulk enrollment, devices are automatically enrolled when powered on. Note: Samsung devices not supported in ZT
Samsung KME	Android 8.0	Devices must be purchased from an authorized reseller partner and transmitted to the Samsung Knox portal that you create. Provides bulk enrollment, devices are automatically enrolled when powered on. Note: Non-Samsung devices not supported in KME portal.

**When possible, use the Guided Walkthroughs in the portal. They provide step by step instructions to complete tasks.

Task	Doc	Video	In - Portal Help  **	Best Practice
Integrate with Android Enterprise		 	Guided Walkthrough> iOS/Android Setup	When integrating with Android Enterprise using a Gmail account, make sure the Gmail account is accessible by your company.
Determine the type of users you will manage (Local, Corporate)		 Session 1	NA	Integrating with Corporate Directory requires the least management.
Add local users if applicable			Guided Walkthrough> Adding Users	If you have more than 10 or 15 local users, take advantage of the Bulk Add workflow using a CSV file. Consider using a separate email address for each user. Using one email address can result in too many notifications sent to one email. User passwords can be generated automatically, or you can set them manually, by configuring User Settings.
Integrate corporate users with Cloud Extender if applicable		 	Setup>Cloud Extender	In addition to using Cloud Extender or Azure AD cloud to cloud integration, for enrollment authentication, consider importing users into MaaS360 for group assignment of policy, and app and content distribution.
Configure Device Enrollment settings			Guided Walkthrough> Set up Deployment Settings	• Select Default User Authentication Mode Local user, Corporate User, One Time Passcode (OTP). • OTP is not recommended with KME or Zero Touch due to high maintenance. Note that if you have a mixed environment, you can select OTP in the Add Device workflow.
Configure User Settings			Guided Walkthrough> Set up Deployment Settings	The default User Password Setting for local users is to generate a password on admin request. If you are setting up all the devices, you might want to consider changing the default setting to manually set the password at user account creation so you only have to enter one password or if your users will be enrolling the device, automatically generate the password.

Task	Doc	Video	In - Portal Help **	Best Practice
Configure an Android Security policy			Guided Walkthrough> Editing and Publishing Policies	• Complete the Android Enterprise section of the security policy • Enable/disable native apps in the policy App compliance section • Best Practices Guide
Configure Mail			Guided Walkthrough> Configure Mail Settings	• Determine how your users will access mail: Secure Mail app, Security policy ActiveSync settings, or a third party mail App. Check with your CSM if needed. • The ActiveSync settings are pushed to the device Gmail app. • Note: You might need to distribute the Gmail app through the app catalog if not standard on device.
Build an App Catalog and Approve Apps				• Application Management Tips and Tricks • Introducing the Next Phase of Android App Management (blog)
Power up devices and complete the enrollment				• If the devices are cellular make sure you have wifi as backup. • The device enrollment differs based on the enrollment method you choose.
Manage devices in the portal				

If you want to learn more, the IBM Knowledge Center and the IBM Security Learning Academy have detailed MaaS360 product documentation and training.
Follow us on the MaaS360 Client Success Hub, where we will keep you updated on content and events in support of your MaaS360 service.