# Manage BYOD 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 personally-owned BYOD Android device deployment use case using MaaS360 integration with Android Enterprise. Note that when deploying Android Enterprise devices where a work profile is set up on a personally-owned device to store work apps and data in a separate container, this is called Profile Owner mode.

**Use Case Description:** In this use case, existing devices that are already in use can be enrolled and managed in MaaS360; a factory reset or out of the box state is not required. MaaS360 has complete control over the work profile on the device, but does not have visibility and control over personal apps, data, and activities. When an employee leaves your organization, you can wipe corporate apps and data, leaving personal apps and data intact.

**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 enrollment method
  - Self Service URL: Publish a general self service URL for all users to enroll where they use their corporate or local user credentials to authenticate (OTP not supported)
  - Unique Enrollment Request: Initiate a unique enrollment request that is sent to the user via email or sms text, this is accompanied with a OTP
  - Bulk Add: Generate multiple enrollment requests that are sent to multiple users, typically this is accompanied with a OTP, but corporate and local user authentication can be used also
- Recommended:
  - Complete this tutorial to enroll a device using a OTP to give you an understanding of the end to end process.

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

| Task | Doc | Video | In - Portal Help<br>❓ ** | Best Practice |
|---|---|---|---|---|
| Integrate with Android Enterprise | 📚 | 🎥<br>🎥 | 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) | 📚 | 🎥<br>Session 1 | NA | Integrating with Corporate Directory requires the least management. |

| Task | Doc | Video | In - Portal Help<br>❓ ** | Best Practice |
|---|---|---|---|---|
| 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 | 📚 | 🎥<br>🎥 | 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). |
| 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. |
| Configure an Android Security policy | 📚 | 🎥 | Guided Walkthrough> Editing and Publishing Policies | • Complete the Android Enterprise section of the security policy<br>• Enable/disable native apps in the policy App compliance section<br>• Best Practices Guide<br>Note: Review settings to ensure they are applicable to Profile Owner (PO) |
| 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.<br>• The ActiveSync settings are pushed to the device Gmail app.<br>• Note: You might need to distribute the Gmail app through the app catalog if not standard on device. |

| **Task** | **Doc** | **Video** | **In - Portal Help**<br>❓ ** | **Best Practice** |
|---|---|---|---|---|
| Build an App Catalog and Approve Apps | 📚<br>📚 | 🎥 | | - Application Management Tips and Tricks<br>- Introducing the Next Phase of Android App Management ( blog) |
| Provide Self Service Enrollment URL if applicable | | | | - Publish the Self-service enrollment URL to your users. The enrollment URL is found in Settings> Default User Authentication Mode (Local User or Corporate ) |
| Generate enrollment request(s) if applicable | 📚 | | Guided Walkthrough> Adding Devices | - To generate multiple enrollment requests to send to users, use the Settings>Enrollment Programs> Bulk Add csv file |
| Users enroll devices | 📚 | | | Note: The download of the MaaS360 App is initiated when the user types the enrollment URL in the browser or via the QR Code from the enrollment request. |
| 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.