Basic iOS device management - Checklist

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

IBM **Security**

Objective: Provide a checklist of simple deployment steps referencing training content and documentation focused on basic iOS device management. Basic iOS device management is for companies who do not require advanced management capabilities. Devices are either owned by the end user and not taking advantage of iOS User Enrollment, or they are company owned and are not supervised using Apple Business Manager(ABM) or Apple Configurator2 (AC2). There is no separation of work and personal content in this use case without the addition of the MaaS360 Secure Productivity Suite.

Use Case Description: Your employees have personally owned devices, or you are providing them company owned devices. In this use case the end user or administrator must interact with the device to install the management profile. Devices do not need to be factory reset in order to be managed but you cannot restrict the end user from removing the management profile once installed. Basic management is geared more towards the user owned device than company owned device which translates to less policy options and limits the amount of control you will have over the device.

Considerations: Maas360 has many features with many 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:

1. Complete the MaaS360 Getting Started checklist
2. Review the following guide to get started:
    a) Maas360 and iOS Guide
3. Choose a device enrollment method
    a) 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)
    b) Unique Enrollment Request: Initiate a unique enrollment request that is sent to the user via email or sms text, this is accompanied with an OTP
    c) Bulk Add: Generate multiple enrollment requests that are sent to multiple users, typically this is accompanied with an OTP, but corporate and local user authentication can be used also

**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**
Create an APNS certificate	📚	🎥	Guided Walkthrough> iOS Setup	Use a company Apple ID instead of a personal Apple ID. Create an Apple ID just for this purpose, using an email that can be shared in your organization.
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

Task	Doc	Video	In - Portal Help ❓ **	Best Practice
				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 based on whether you are using One Time Passcode, Local or Corporate Users.
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 iOS Security policy	📚	🎥 🎥	Guided Walkthrough> Editing and Publishing Policies	• Determine if you will allow your users to have access to the App Store and iCloud features. • For Standard Management, you must use the Device Settings and Advanced Settings of the policy. Supervised settings do not apply.
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. • Use the iOS Policy Guide for ActiveSync integration with Native Mail
Build an App Catalog	📚			Application Management Tips and Tricks Note: Silent/Instant install is only available on Supervised Devices
Provide Self Service Enrollment				Publish the Self-service enrollment URL to your users. The enrollment URL is found in

Task	**Doc**	**Video**	**In - Portal Help** ❓ **	**Best Practice**
URL if application				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	📚			A Safari browser is required for enrollment.
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.