Manage Corporate owned MacOS devices - 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 a corporate owned MacOS device deployment use case using MaaS360 integration with Apple Business Manager(ABM). Note that the Device Enrollment Program and Volume Purchase Program are now completely integrated in ABM.

Use Case Description: You purchased MacOS devices from Apple, an Apple Authorized Reseller or carrier and require complete control of the devices where you supervise the device and require the device to be enrolled in MaaS360. In this use case devices can only be enrolled and supervised in MaaS360 from out of the box or by a factory reset. This use case provides automated device enrollment, complete control over the device, with no separation of work and personal data on the device. These devices are typically purchased by your organization and provided to employees for work use.

Considerations: Maas360 has many features with a plethora of 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. Sign up for Apple Business Manager
    - **Note:** In certain cases, organizations might not be able to use Apple Business Manage for corporate owned devices; you have the option of using Apple Configurator, skip to 5b.
3. Work with your reseller/carrier to load your devices into the ABM portal by order number, serial number or csv file.
    - **Note:** If you purchased consumer devices from other sources, you can use Apple Configurator 2.5+ to add them to Apple Business Manager. Learn more here.
4. Add applications to ABM for Volume Purchase Program (VPP), this allows you to silently install applications as well as control license distribution for purchased apps
5. Review the following guide and video to get started:
    a) Getting Started with MaaS360 and Apple devices (1 hour video)

**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> MacOS 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 email address for each user. Using one email address

Task	Doc	Video	In - Portal Help **	Best Practice
				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 Local or Corporate Users. • One time passcode(OTP) cannot be used with ABM. Note that if you have a mixed environment with BYOD devices, you have the opportunity to 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. Note that you can set the DEP Profile to skip enrollment authentication and then have the Admin assign the User to a device in the portal after enrollment.
Configure an macOS 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 devices that you would like to have supervised that are not in ABM, you must manually supervise them through Apple configurator. • If you are supervising devices, use the settings in the Supervised section of the iOS policy.
Configure Mail			Guided Walkthrough> Configure Mail Settings	• Determine how your users will access mail. The MaaS360 Secure Mail container requires Deluxe, Premier, or Enterprise suite. If you have Essentials configure mail in the iOS Security policy or use a third party mail App and app config settings.

Task	Doc	Video	In - Portal Help **	Best Practice
				• Use the iOS Policy Guide for Activesync integration with Native Mail
Integrate MaaS360 with VPP if applicable			Guided Walkthrough> Configure Apple VPP	Use VPP to silently install both free and purchased Apps on Apple devices. Note that the device must be Supervised to take advantage of the silent install.
Build an App Catalog		Session 4		Included in Technical Intro series Session 4
Integrate MaaS360 with ABM			Guided Walkthrough> Integrate Apples Streamlined Enrollment	
Add tokens to MaaS360			Guided Walkthrough> Integrate Apples Streamlined Enrollment	Make sure ABM token names are unique and identifiable.
Configure and Assign DEP Profile			Guided Walkthrough> Integrate Apples Streamlined Enrollment	• Consider locking the MDM profile to the device if you do not want users to unenroll from MaaS360. If a user unenrolls, you will not have control over the device. • Consider disabling Authenticate User if an administrator is setting up the devices. The Admin can assign the user after the device enrollment is complete. • Consider whether you want to allow users to restore from back up.
Power up devices and complete the enrollment				If the devices are cellular make sure you have wifi as backup.
Assign Devices to users if applicable			Device Inventory >Assign User	Note: If the Authenticate User setting was enabled in the Profile, then this is not applicable.
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 Success Hub, where we will keep you updated on content and events in support of your MaaS360 service.