

Deploy Windows 10 devices using manual enrollments - Checklist



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

Objective: Provide a checklist of simple deployment steps referencing training content and documentation focused on managing Windows 10 (Professional, Enterprise, Education, Home) devices with MaaS360 using manual enrollment methods.

- Note: Windows 10 Home devices are enrolled in the MaaS360 Portal in DTM mode, which uses traditional agent-based management that is normally used for Windows 7, while Windows 10 (Education, Enterprise, Professional) devices are enrolled in MDM mode, which uses modern management capabilities built on the Windows 10 MDM APIs.

Use Case Description: You have existing Windows 10 devices in an out of the box state or that are already in circulation. You will rely on an administrator or end user to enter a MaaS360 self-service enrollment URL, or a one time enrollment request URL. You do not plan on using streamlined enrollment methods such as Windows Out of the Box Enrollment, Windows 10 Autopilot, or Windows 10 Bulk provisioning tools. This use case provides device enrollment and control over the devices through Windows policy with no containerized separation of work and personal data on the device, though MaaS360 does support Windows Information Protection settings through the Windows security policy. These devices are typically purchase by your organization, but BYOD devices are supported also.

Prerequisites:

- Complete the MaaS360 Getting Started [checklist](#)
- Review the following video to get started:
 - [Introduction to Windows 10 Management \(1 hour video\)](#)

****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/Additional Instructions
Enable Windows/Laptop Service				In Setup> Services, enable Laptop and Desktop Management and select Windows Desktop and Laptop Management.
Determine the type of users you will manage (Local, Corporate)		 Session 1	NA	Integrating with your 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		 	Setup>Cloud Extender	In addition to using Cloud Extender or Azure AD cloud to cloud integration , for enrollment authentication, consider importing users into

Task	Doc	Video	In - Portal Help  **	Best Practice/Additional Instructions
Extender if applicable				MaaS360 for group assignment of policy, and app and content distribution.
Configure Device Enrollment settings			Guided Walkthrough> Set up Deployment Settings	- If you plan to provide a self-service enrollment URL to your end users, set the corporate identifier to your company name or shortened company name. The identifier must be unique across MaaS360 instances. - A self-service url enables the end user or MaaS360 admin to type the MaaS360 generated URL into the Edge browser to launch enrollment. - Select Default User Authentication Mode based on whether you are using Local, Corporate Users or One Time Passcode. - If you are not leveraging integration with your corporate directory, consider using One Time Passcodes for enrollment.
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 a Windows Security policy			Guided Walkthrough> Editing and Publishing Policies	- Enable Bitlocker - Enable Passcode settings - Configure Wifi/VPN - Enable Anti-virus and Firewall settings (Windows Defender only) - Configure Update Management Note: MaaS360 and Windows 10 also supports Kiosk mode in Advanced settings.
Send Enrollment Request if applicable			Guided Walkthrough> Adding Devices	- You have the option of sending the enrollment request to the end user or publishing a self service URL as noted above in the Device Enrollment Settings. - If you select Self Service using corporate directory, you also can still use OTP by selecting the Advanced Tab>Override Authentication and enabling Passcode for the request. - If you want to send a large number of enrollment requests to your end users,

Task	Doc	Video	In - Portal Help  **	Best Practice/Additional Instructions
				consider using a csv upload with Setup>Device Enrollment Settings>Enrollment Programs>Others> Bulk Add.
Build an App Catalog				
Enroll Windows 10 in MaaS360				• In order to enroll in MaaS360 using a OTP or self service URL, the end user or MaaS360 admin must log into the Windows 10 device as a Windows administrator. • The end user will be prompted for the email address associated with the OTP enrollment request sent in an email by the MaaS360 Admin, or the end user will enter their email associated with their corporate directory credentials or MaaS360 local credentials based on the default authentication method selected in the Device Enrollment Settings.
Manage devices in the portal		 		• Use Device Inventory > Summary>Endpoint Security to review Anti-virus, Anti-Spyware, Firewall, Encryption, and Backup and Recovery status. • Ensure Antivirus and Firewall software is running by setting an alert on the home page and or creating a group based compliance rule.

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.