Microsoft HoloLens integration with MaaS360

MaaS360 has partnered with Microsoft to manage HoloLens devices alongside other endpoints in an enterprise from a single unified management solution. With this support, administrators can easily enroll a Microsoft HoloLens device into the MaaS360 Portal using the normal MDM enrollment workflow. MaaS360 also leverages Windows APIs to allow administrators to enforce security policies, compliance rules, perform device actions over-the-air as well as push applications to HoloLens devices.

The following features are supported with Microsoft HoloLens Integration:

Enrollment Support

MaaS360 supports the following enrollment options for HoloLens devices:

1. Windows Out of Box Enrollment (OOBE) [Recommended]

   The Windows Out of Box Experience (OOBE) allows administrators to automatically enroll Windows devices (Windows 10+ desktops, tablets, phones) into MaaS360® when the user boots the device and joins into Azure Active Directory. This is the most recommended and preferred enrollment for HoloLens devices.

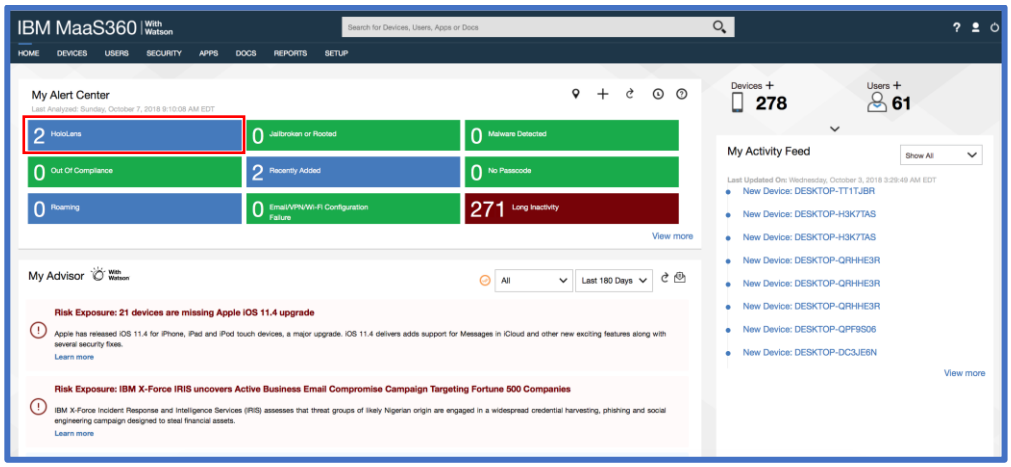
2. OTA native MDM enrollment

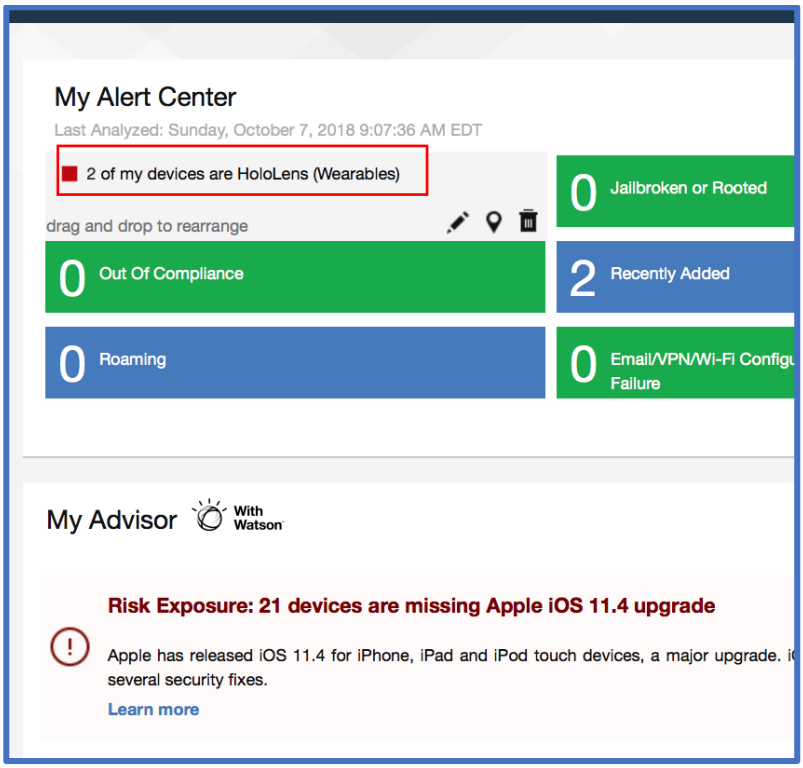
This is an enrollment process that can be achieved post device setup. All traditional Windows enrollment methods are supported such as passcode based enrollment, AD based enrollment (Azure), 2 Factor enrollment. Windows OOBE is the recommended enrollment method for HoloLens.

Once the enrollment process is completed using either of the above methods, the IBM MaaS360 agent can be viewed on the device. The options in the Device menu are: App Catalog, Messages, and Settings.

Homepage Alert Center

- Enrollments alerts are presented on the My Alert Center section of the Home page the same way as any other device that is managed by the MaaS360 platform.



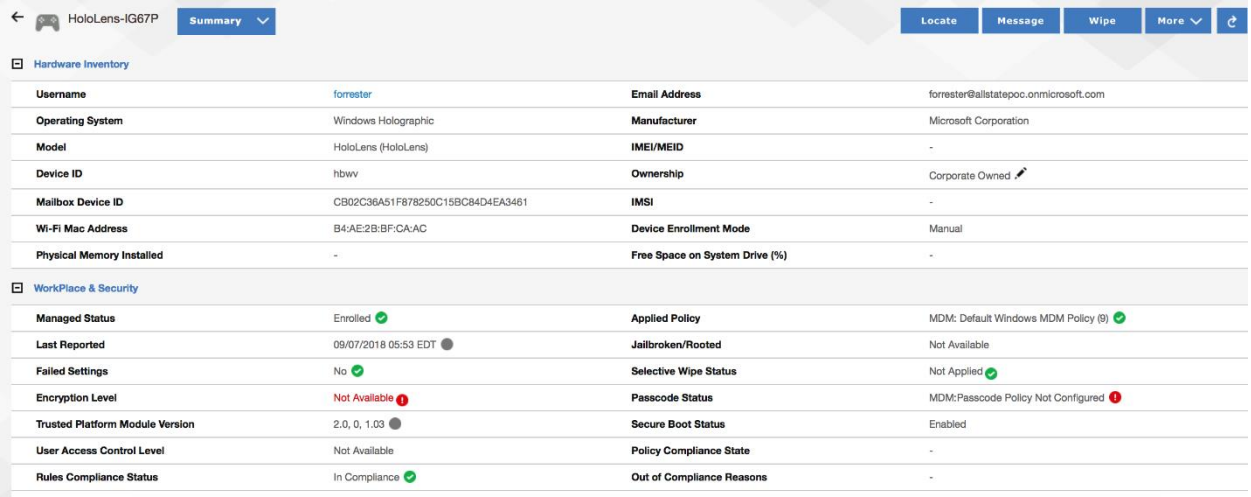


Managing the Microsoft HoloLens Device within MaaS360 Device Inventory

The Device Inventory page in the MaaS360® Portal lists all the devices that are managed. A managed Microsoft HoloLens device is listed along with all other managed devices in this page. This page also lists managed devices that are enrolled or not enrolled in the MaaS360® Portal, managed devices where the user removed control of the device or the devices that are pending a control removal, and managed devices that are active or inactive.

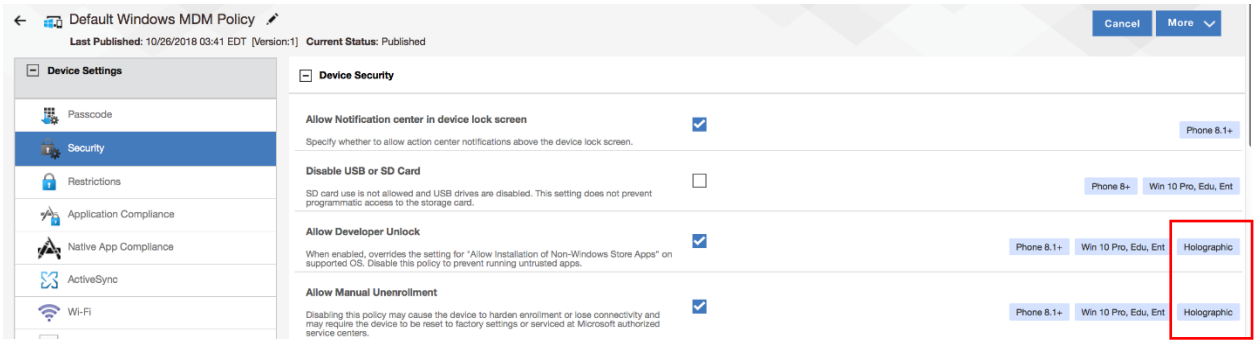
The following actions can be taken on the HoloLens Device managed by the MaaS360® Portal:

- Locate
- Send Message
- Change Policy/Rule Sets
- Selective Wipe of Corporate settings (WiFi, VPN, App Catalog)
- Wipe
- Reboot Device
- Update License to Business edition OTA
- Hide
- Distribute App
- Remove Control on-demand



MDM Policies for HoloLens Devices within the MaaS360 Portal

There are Windows MDM policies that can be configured for HoloLens devices in the MaaS360® Portal under the MDM policies. The policies that can be applied to HoloLens devices are designated by the tag '*Holographic'* against the Windows policies section.



Examples of some of the policies that can be set:

Restrictions

- Controls such as Passcode settings
- Disable Cortana
- Disable location, telemetry, date time
- Disable Bluetooth, VPN

Configurations

- WiFi settings
- VPN Settings
- Edge Browser Settings
- Bluetooth Settings/Controls

Device Security Policies

- Enforce BitLocker Encryption

- Disable from un-enrollment
- Privacy Settings
- Disable Developer Unlock

Windows Holographic Windows MDM Policy Specifics

Navigation	Policy	
Device Settings > Security	Allow Developer Unlock	
	Allow Manual Unenrollment	
	Enforce Device Drive Encryption	
	Allow Fast Reconnect	
	Allow Installation of Non-Windows Store Apps	
	Allow Auto-Update of Windows Store Apps	
Passcode	Minimum Passcode Length (4-16 characters)	
	Allow Simple Passcode	
	Passcode Quality	Alphanumeric
		Numeric
	Minimum number of character sets	
	Allowed Idle Time (in minutes) Before Auto-Lock	
	Number of Unique Passcodes Required Before Reuse Allowed	
	Number of Failed Passcode Attempts Before All Data Is Erased	
	Allow Idle Return Without Passcode	
	Allow Screen Timeout configuration on lock screen	
	Screen Timeout duration on lock screen	
Restrictions	Allow Cortona	
	Allow Location	
	Allow Telemetry	
	Allow Microsoft Account Connection	
	Allow Search to use Location	
Application Compliance	Configure Restricted Universal Applications (App Blacklist)	
	Configure Allowed Universal Applications (App Whitelist)	
WiFI	Configure WiFi Profile	

VPN	Configure VPN Profile	
Update Management	Configure update settings	
Profile Management	Enable Profile Manager	Deletion Policy
		Storage capacity percentage threshold to start profile deletion (%)
		Storage capacity percentage threshold to stop profile deletion (%)
Advanced Setting	Privacy Restrictions	
	Network Restrictions	Allow Bluetooth
		Allow Bluetooth Discoverable Mode
		Allow Bluetooth Advertising
		Configure Bluetooth Device Name
	Browser Restrictions	Allow Send Do Not Track Requests
		Accept Cookies
		Allow search suggestion in address bar
		Enable Smart Screen Filter Warnings

Compliance Rules for HoloLens within the MaaS360 Portal

MaaS360® Portal uses rule sets to check for compliance on devices. If a device is out of compliance with the defined rule set or condition, MaaS360® takes appropriate enforcement actions against the device.

From the MaaS360 Portal Home page, select **Security**>**Compliance Rules**.

Example of compliance rules that can be set are: Enrollment, OS Version, Application Compliance.

For more information about configuring compliance rules, see https://www.ibm.com/support/knowledgecenter/SS8H2S/com.ibm.mc.doc/pag_source/tasks/pag_sec_apply_compliance_rules.htm.

App management within MaaS360 Portal

The MaaS360® Portal allows for App Management for HoloLens devices with the use of the MaaS360® App Catalog and Policies. The App Catalog allows for the administrator to distribute and manage applications on the device and then apply security policies around those apps. Specifically, the following can be utilized within an organization to manage apps on HoloLens devices.

App Management

- App Catalog
  - Add HoloLens apps to MaaS360 Portal
- Blacklist/whitelist HoloLens apps in App Compliance MDM Policies
- Distribute Applications
  - Distribute to specific HoloLens device, a specific group or all HoloLens devices.
  - Setting Mandatory applications
  - Configuring Apps that can be installed on demand

App Security MDM Policies

- Disable auto-update of Windows Store Apps
- Disable installation of non-Windows Store Apps
- Disable Developer Unlock/sideloading

Edge Browser Settings in MDM Policies

- Disable/Enable Pop-up
- Cookie policy – accept/block
- Allow search suggestion in address bar
- Prevent Send Do Not Track requests
- Enable Smart Screen Filters (Defender)

Reporting

The MaaS360® Portal reports include HoloLens device information.