Microsoft 365 Device Management (Intune) Best Practices Checklist

By Alex Fields, ITProMentor.com

Updated July 15, 2019

	Checklist item	Description	End user impact	Where to change this	Importance
☐	Create security groups for deployment rings	Define pilot group for testing updates and changes; additional rings up to your discretion	No impact simply by creating securtiy groups	Groups blade	Recommended
☐	Setup Windows 10 Software Update Rings	Define Windows 10 update rings to apply automatic updates; also defer updates for sensitive users	Updates will be less likely to negatively impact end users in defered update groups	Software Updates blade > Windows 10 Update Rings	Recommended
☐	Setup automatic deployment of the Office apps on Windows 10	Office 365 apps auto-installed on enrolled Windows 10 devices; also define servicing branches	End users (or IT) will not have to manually download and install basic productivity software	Client Apps blade > Apps	Recommended
☐	Setup App protection policies (MAM)	MAM enables BYOD scenarios with application-based management, rather than device-based (MDM)	Users must stick to approved mobile apps, and will be prompted to meet the conditions (e.g. PIN, etc.)	Client Apps blade > App protection policies	Recommended
☐	Customize Company Portal	Configure branding, privacy URL, and define the support contact displayed in the Company portal	The Company Portal app will display the defined settings and customizations to end users	Client Apps blade > Branding and customization	Optional
☐	Create the Company terms and conditions	This is the Organization's place to communicate terms of use to the end users (example provided)	End users will view and accept the terms and conditions in the Intune Company portal app	Device Enrollment blade > Terms and conditions	Optional
☐	Configure Device enrollment restrictions	Blocks unsupported devices from enrolling, and limits the number of devices per user	Users will not be able to enroll certain device types, nor will they be able to enroll too many devices	Device Enrollment blade > Enrollment restrictions	Critical
☐	Configure Windows 10 automatic enrollment	Windows devices joined to Azure AD will be auto-enrolled into the Intune service also	End users who join devices using corporate credentials will not have to enroll separaetly for Intune	Device enrollment > Windows enrollment > Automatic Enrollment	Critical
☐	Configure Windows Hello for Business	Hello is 2FA built-in to Windows 10; many devices also support fingerprint or face recognition	Users will be required to setup PIN and optional biometric for Windows	Device Enrollment > Windows Enrollment > Windows Hello for Business	Recommended
☐	Configure Apple MDM push certificate	If managing iOS devices via MDM: you must setup a certificate through Apple (renewed annually)	End-users with mobile devices under MDM will be required to enroll via the Company portal app	Device Enrollment > Apple enrollment > Apple MDM Push certificate	Optional
☐	Configure device cleanup	Delete devices based on the last check-in date, e.g. 90-180 days	Devices that have not checked in will need to be re-enrolled into the service if past this date	Devices blade > Device cleanup rules	Recommended
☐	Configure the default compliance policy settings	Devices without an assigned compliance policy should be marked as non-compliant	Non-compliant devices will be denied access to resources (once Conditional access is in place)	Device Compliance blade > Compliance policy settings	Critical
☐	Configure Device compliance policies	Each type of device that you intend to manage should have a compliance policy for use with Conditional access	End users will be required to enroll their devices and meet the requirements of compliance (e.g. PIN, encryption, etc.)	Device Compliance blade > Policies	Critical
☐	Enroll devices	Devices must be enrolled for management or none of the policies and profiles will apply	Devices that are not enrolled will not have access to resources (once Conditional access is enabled)	Use the Company Portal app, or automatic enrollment	Critical
☐	Verify compliance	Do not skip this step. Review compliance for any non-compliant devices, and remediate	Non-compliant devices will be denied access to resources (once Conditional access is in place)	Device Compliance blade > Device compliance	Critical
☐	Enable Conditional Access	See my Conditional Access policy design and guide for more details	Users must enroll devices and/or use managed applications, according to the rules defined.	Conditional Access blade > Policies	Critical
☐	Setup Device configuration profiles	Recommended profiles for Windows 10 are discussed in the guide. Others up to your discretion.	Devices in scope of the profiles will receive settings from Intune; users will not be able to change the admin-defined settings	Device Configuration blade > Profiles	Optional