inforcer

Intune Security Essentials Checklist

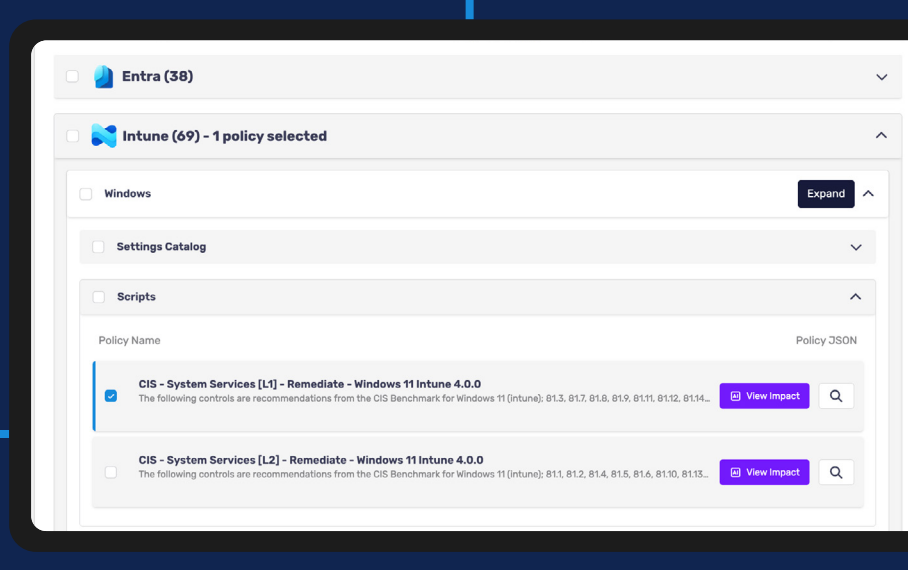
As an MSP, ensuring the security of your customer devices is essential. Use our checklist to ensure you are configuring and managing Microsoft Intune according to best practices.

✓	Checklist Item	Rationale	End User Impact	How to Change This	Subscription
☐	Ensure MDM enrollment when adding a work or school account on Windows is blocked	Accidental enrollment of unwanted devices can lead to: inadvertant management of personal devices; more devices than you are licensed to manage; increased difficulty in hardware lifecycles.	This will prevent Intune enrollment when a user, for example, signs into Microsoft 365 desktop apps on non-managed device	Intune > Devices > Enrollment > Automatic Enrollment > Disable MDM enrollment when adding work or school account on Windows (YES)	Intune Plan 1
☐	Ensure App Protection Policies are configured for Android and iOS when accessing M365 applications	App Protection Policies ensure that business data can be controlled on personally owned mobile devices.	Depending on the OS used, end-users will need to either install Company Portal (Android) or MS Authenticator (iOS) for the app encryption fo function. Follow MS Guidance for more details.	Intune > Apps > Protection > Create Policies	Intune Plan 1 & Entra ID P1 to enforce via CA Policy
☐	Ensure devices are marked as “not compliant” when no compliance policy is assigned.	To make compliance policies effective, it is wise to adjust this default setting to highlight devices which are not in-scope of a desired compliance policy	If devices meet the compliance policy rules you set, no impact.	Intune > Devices > Compliance > Compliance settings > Mark devices with no compliance policy assigned as (Not compliant)	Intune Plan 1
☐	Ensure a compliance policy is configured and targeted for each OS type in use within your business	Compliance policies help admins maintain minimum security and client health standards; device compliance can be a requirement to access resources when linked with an Entra Conditional Access policy	If devices meet the compliance policy rules you set, no impact.	Intune > Devices > Compliance > Create Compliance Policy	Intune Plan 1 & Entra ID P1 to create the CA Policy
☐	Ensure number of web browers used in the business is known, limited, and the ones in use have a patching strategy	An increasing amount of time is spent within the web browser; unapproved browsers could be considered both shadow IT and shadow AI depending on how they are used.	Agree and communicate the expectations to the business so everyone is aware what they can use	Various methods; App Control for Business, uninstall scripts/remediations, or written guidance.	Intune P1 (Windows Enterprise needed for remediation scripts)
☐	Ensure browser extension use is limited	Illegitimate browser extensions are becoming a popular route of compromise for browsers and business data; you should consider making installation by request only	End-users who need additional extensions should request them.	“Intune > Devices > Configuration > Create Settings Catalog Policies OR M365 Admin Center > Settings > Microsoft Edge”	Intune P1
☐	Ensure third-party browser sync services are disabled	Business data and credentials can leave corporate devices if personal account sync is permitted in browsers; for example, a user could sign into Chrome and sync passwords and data back to a personal device which could then be compromised.	Communication to end-users that sync is only permitted using the corporate account in the approved browser	“Intune > Devices > Configuration > Create Settings Catalog Policies OR M365 Admin Center > Settings > Microsoft Edge”	Intune P1
☐	Ensure OneDrive sync is restricted to approved tenants	By default, end-users can sign in and link OneDrive to multiple M365 tenants or accounts. By limiting this to a single tenant ID, we reduce the liklihood of data loss.	End-user expectations should be set that the corporate device is for corporate data only.	Configure Intune Settings Catalog item: Allow syncing OneDrive accounts for only specific organizations	Intune P1
☐	Ensure deployed applications are relevant and use up-to-date packages	Unpatched third-party software presents operational risk to a business and should be updated as soon as possible.	Minimal impact if updates are applied considerately; more potential impact if an app stops working due to incompatibility	Intune > Apps > Deploy required app packages	Intune P1
☐	Ensure hard drive encryption is enabled on all business devices (BitLocker/FileVault)	Hard drive encryption is a necessary step to reduce the likelihood of unauthorised data access if a corporate device is lost or stolen.	None if configured silently. End-users may need to be aware of how they obtain their recovery keys	Configure Intune Settings Catalog items for hard drive encryption	Intune P1
☐	Ensure end-users are not operating as local admins.	End users having local administrator rights at all times significantly increases risk and decreases the effectiveness of company-managed security controls.	End-users who need elevation will either need the assistance of IT, or by using Endpoint Privilege Management	Various methods; for new devices ensure Windows Autopilot profile sets standard user and for macOS ADE enrollment set local primary account type to Standard	Intune P1
☐	Ensure device compliance is integrated with Conditional Access to gate access to company data	Restricting access to corporate data from corporate-owned devices only is one of the highest-impact security controls for reducing phishing success and data exfiltration.	High-impact. This will require careful communications and an adjustment of expectations if people frequently sign in from personal devices	Ensure all company devices are Intune enrolled, and block enrolment of personal devices. Then create an Entra Conditional Access policy to require device compliance	Intune P1 & Entra ID P1
☐	Ensure Windows Hello for Business is configured for PIN or biometric use, with TPM required	Windows Hello for Business is a valid MFA method that simplifies the user experience compared to repeated password entry. Requiring TPM ties authentication to the physical device.	Depending on current log-in method, this could see users switching from a password to a PIN/Biometric	Dependant on existing setup. WHfB can be configured using policies in the Intune Settings Catalog	Intune P1
☐	Ensure a lock screen policy is set for all devices	Configuring the lock screen timeout helps protect sensitive data by preventing unauthorised access to the device when it is unattended.	Login will be required after the specified time of inactivity	Configure Intune Settings Catalog items for screen lock.	Intune P1
☐	Ensure all devices have checked in within the last 90 days	Keeping the device inventory current prevents reaching licence limits and improves overall compliance scores. Devices reported as lost should be removed promptly.	None	Configure Intune device cleanup rules for each operating system	Intune P1

An easier way to manage Intune across multiple tenants

Configuring all these settings and policies manually is extremely time-consuming and resource-heavy. Save time, reduce effort, and eliminate human error by using inforcer for multi-tenant Intune management.

Book a demo



inforcer