Intune device baseline checklist

Conditional Access can only trust a device as far as Intune checks it. This checklist is what a sensible device baseline looks like before you let “require compliant device” make access decisions.

Use it for a New Zealand mid-market or public-sector Microsoft 365 tenant. Tick only what is enforced, not “planned”. Work top-down: tenant-wide compliance settings first, then compliance policies per platform, then encryption and local admin, then Defender, updates and baselines, then enrolment, BYOD and Conditional Access.

Do not change the tenant compliance default or switch on a “require compliant device” policy until every platform you allow has a compliance policy assigned. Use report-only mode first and keep break-glass accounts excluded. Most Intune settings default to “Not configured”, which means they are not evaluated. Document what you changed and why. That matters under Privacy Act 2020 when you need to show reasonable safeguards for devices that hold personal information.

BEFORE YOU START

- [ ] You know which licences you have (Intune, Entra ID P1 / P2, Defender for Endpoint, Windows Autopatch eligibility) so you only tick what you can enforce
- [ ] You have a device inventory by platform and OS version, including every remaining Windows 10 device
- [ ] At least one break-glass account exists and is excluded from Conditional Access policies that could lock out all admins
- [ ] A pilot device group exists for each platform you manage

TENANT-WIDE COMPLIANCE SETTINGS

- [ ] The Devices without compliance policy report has been reviewed and every device in it has an owner or a policy
- [ ] Mark devices with no compliance policy assigned as is set to Not compliant (the default is Compliant)
- [ ] Compliance status validity period is a deliberate choice (default 30 days, range 1–120) — devices that do not report within it become noncompliant
- [ ] Actions for noncompliance are set on purpose (for example, email the user, then a grace period) rather than left at the default

COMPLIANCE POLICIES PER PLATFORM

- [ ] Windows: a compliance policy is assigned to every managed Windows device, requiring BitLocker, Secure Boot, code integrity, firewall, antivirus and Microsoft Defender Antimalware with real-time protection
- [ ] Windows: a minimum OS version or valid operating system build ranges set a patch floor for each Windows release you allow
- [ ] Windows: if Defender for Endpoint is connected, the policy requires the device to be at or under your chosen machine risk score
- [ ] iOS/iPadOS: minimum OS version, passcode required and jailbroken devices blocked
- [ ] Android Enterprise: minimum OS version, password required, rooted devices blocked and a Play Integrity verdict required

Intune device baseline checklist

- ☐ macOS: minimum OS version, password required, encryption of data storage required, firewall enabled and System Integrity Protection required
- ☐ Every platform you allow to enrol has a compliance policy; platforms you do not support are blocked at enrolment

WINDOWS 10 AND WINDOWS 11

- ☐ Every remaining Windows 10 device has a decision: Windows 11 upgrade date, replacement, or ESU Year 2 with a named owner and exit date
- ☐ ESU devices run Windows 10 22H2 with the ESU prerequisite updates (KB5066791 and the licensing preparation package KB5072653) installed
- ☐ The Year 2 ESU key is installed and activated, and slmgr.vbs /dlv shows the Year 2 programme as Licensed
- ☐ Windows 10 devices relying on Windows 365 for ESU are Entra joined or hybrid joined and receive the EnableESUSubscriptionCheck policy
- ☐ Windows 11 upgrades are driven by an Intune feature update policy or Windows Autopatch, using the Windows feature update device readiness report to find devices that need replacing

ENCRYPTION AND LOCAL ADMIN

- ☐ BitLocker is enforced with an endpoint security disk encryption policy
- ☐ Require device to back up recovery information to Microsoft Entra is set to Yes, so encryption does not complete without a stored recovery key
- ☐ Windows LAPS is configured with an endpoint security account protection (LAPS) policy, backing up to Microsoft Entra ID or Active Directory to match the device join type
- ☐ LAPS is enabled in Microsoft Entra device settings for Entra-joined devices
- ☐ Each device receives one LAPS configuration — conflicting LAPS policies can stop the password being backed up

DEFENDER, ANTIVIRUS AND FIREWALL

- ☐ Intune is connected to Microsoft Defender for Endpoint (Tenant administration > Connectors and tokens)
- ☐ Windows devices are onboarded through an endpoint detection and response (EDR) policy, and the onboarded count matches your Intune Windows device count
- ☐ Microsoft Defender Antivirus is managed with an endpoint security antivirus policy
- ☐ Windows Firewall is managed with an endpoint security firewall policy, and conflicting Group Policy settings are removed

UPDATES

- ☐ Windows update rings exist for test, pilot and production, assigned to device groups
- ☐ If you use Windows Autopatch, custom update rings are not assigned to Autopatch-managed devices
- ☐ A feature update policy (or Autopatch) holds devices on the Windows version you have chosen
- ☐ Pausing a ring is an emergency brake (up to 35 days), not a standing setting
- ☐ Windows diagnostic data is enabled for Intune, so feature update and readiness reports actually populate
- ☐ Update and compatibility reports are reviewed after each monthly security release

SECURITY BASELINES

- ☐ The Security Baseline for Windows 10 and later is deployed, piloted before broad assignment, and on a current version
- ☐ The Microsoft Defender for Endpoint, Microsoft Edge and Microsoft 365 Apps baselines are considered where you license and use those products

Intune device baseline checklist

- ☐ Baselines are checked for conflicts with each other and with other configuration profiles; per-setting status is reviewed
- ☐ Preview baselines are not used in production

ENROLMENT

- ☐ Device platform restrictions block platforms and OS versions you do not support
- ☐ Personally owned Windows enrolment is blocked if corporate devices should be the only managed Windows devices
- ☐ A device limit restriction is set to what users actually need (1–15)
- ☐ Enrolment restrictions are treated as a best-effort barrier, not a security control — compliance and Conditional Access do the enforcing

BYOD AND APP PROTECTION

- ☐ App protection policies cover iOS/iPadOS and Android for the Microsoft 365 apps people use on personal devices
- ☐ Policies follow Microsoft's data protection framework (Level 2 enhanced protection suits most users with sensitive data)
- ☐ Conditional Access for unenrolled mobile devices requires an approved client app or app protection policy

CONDITIONAL ACCESS

- ☐ A "require device to be marked as compliant" policy exists, with break-glass accounts and directory synchronisation accounts excluded
- ☐ The policy ran in report-only mode and the impact was reviewed before it was switched on
- ☐ If you are not ready for all users, administrators at least require a compliant or Entra hybrid joined device
- ☐ Unknown or unsupported device platforms are blocked

REPORTING AND OPERATING RHYTHM

- ☐ The device compliance dashboard is reviewed on a set cadence, with Not compliant, In grace period and Not evaluated devices followed up
- ☐ Defender onboarding, BitLocker and LAPS coverage are checked against the Intune device count
- ☐ The Windows 10 tail is tracked down to zero, with ESU renewals decided well before each October
- ☐ Changes are recorded: what was switched on, who approved it, and why

What good looks like: a device with no compliance policy cannot pass Conditional Access. Every platform has a policy that checks real settings. BitLocker keys and LAPS passwords are backed up, Defender is onboarded everywhere, and updates flow through rings you can explain. And your Windows 10 tail is a short list with names and dates — not a surprise each October.

zenaossolutions.co.nz contact@zenaossolutions.co.nz