TechSuit · Engineering blueprint

The Intune & Entra ID Configuration Blueprint

Automating CIS Controls v8.1 (IG1) and cross-border GRC controls in Microsoft Intune and Entra ID.

Why we build on CIS Controls v8.1, IG1

The CIS Critical Security Controls give small businesses a specific, testable baseline instead of a vague "be more secure" mandate. Implementation Group 1 (IG1) is the 56-safeguard floor CIS defines as essential cyber hygiene for every organisation, regardless of size. It's also the practical technical hub behind NIS2's Article 21 measures, Spain's ENS, and ISO 27001 Annex A - implement IG1 properly once, in Microsoft Intune and Entra ID, and the evidence for all three frameworks comes from the same configuration.

This is exactly how we deploy it for clients: real settings, real menu paths, in the Microsoft Intune admin center (**intune.microsoft.com**) and the Microsoft Entra admin center.

1. Hardware and software inventory automation

CIS Safeguard 1.1 - Establish and Maintain Detailed Enterprise Asset Inventory. Enrolling every Windows, macOS, iOS, and Android device into Intune MDM gives you a live inventory automatically - no spreadsheet, no annual audit. Every enrolled device reports its model, OS build, compliance state, and last check-in continuously under **Devices > All devices**.

CIS Safeguard 2.1 - Establish and Maintain a Software Inventory. Microsoft Defender for Endpoint's **Vulnerability management > Inventories** view gives you a continuously updated list of installed software and browser extensions across every enrolled device, cross-referenced against known CVEs. Combined with Intune's **Apps > Discovered apps** report, you get software discovery without asking anyone to fill out a form.

Two related safeguards worth knowing: automated software-inventory tooling (Safeguard 2.4) and audited application allow-listing sit in IG2, one step above this baseline. If IG1 is your floor, Defender's discovered-apps view already gets you most of the way there for free.

2. Endpoint hardening and asset protection

CIS Safeguard 4.3 - Configure Automatic Session Locking. CIS's own IG1 baseline calls for locking within 15 minutes on general-purpose devices and 2 minutes on mobile. We set clients tighter than that by default, because the stricter standards they're often also trying to satisfy expect it:

Standard	General-purpose OS	Mobile
CIS Controls v8.1 IG1 baseline	15 minutes	2 minutes
ISO 27001 (Control 7.7) / Spain's ENS (mp.eq.1, mp.eq.2)	5 minutes	2 minutes

Configuration path: Intune admin center > Devices > Configuration > Create > New policy > Platform: Windows 10 and later > Profile type: **Settings catalog** > search "Device lock" and set the inactivity timeout in seconds (300 for 5 minutes). Repeat with the equivalent screen-lock setting under the macOS and iOS/Android configuration profiles.

CIS Safeguard 4.4 and 4.5 - Firewall on servers and end-user devices. Build an **Endpoint security > Firewall** policy in Intune targeting Windows Defender Firewall. Set "Block all inbound connections that don't match a rule" explicitly to **Yes** rather than leaving it unconfigured - this enforces default-deny for unsolicited inbound traffic instead of relying on the client's implicit default.

CIS Safeguard 10.3 - Disable Autorun and Autoplay for removable media. One important 2026 change: Intune retired the standalone "Administrative Templates" device-configuration profile type in December 2024. The setting still exists, but you now reach it through **Settings catalog > browse by category > Administrative Templates > Windows Components > AutoPlay Policies**, and set "Turn off Autoplay" to **Enabled: All drives**. If you're following an older guide that says to create an "Administrative Templates" profile directly, that path no longer exists in the portal.

3. Sensitive data encryption and backups

CIS Safeguard 3.6 - Encrypt Data on End-User Devices. Build a disk-encryption profile under **Endpoint security > Disk encryption**. For Windows, set "Store recovery information in Microsoft Entra ID before enabling BitLocker" to **Required** - this silently escrows the recovery key to Entra ID and blocks encryption from completing until the key is confirmed stored, so you never end up with an encrypted device and no recovery key on file. For macOS, the equivalent FileVault profile escrows the personal recovery key to Intune, retrievable from the admin centre or self-service through Company Portal.

CIS Safeguard 9.2 - Use DNS Filtering Services. Push a custom Settings Catalog profile under **Administrative Templates > Network > DNS Client** to point managed Windows devices at a trusted DNS-over-HTTPS resolver such as Quad9 (9.9.9.9, DoH endpoint dns.quad9.net). Confirm the exact setting label in your tenant's Settings Catalog picker before deploying at scale - Microsoft has moved this setting between menus more than once.

CIS Safeguards 11.2 through 11.4 - Automated, isolated backups. Use Intune's OneDrive ADMX-backed policy (Settings Catalog > OneDrive category) to silently enforce **Known Folder Move**, redirecting Desktop, Documents, and Pictures into OneDrive without asking the user. That satisfies **automated backups (11.2)** and, because OneDrive keeps version history and a recycle bin genuinely separate from the local disk, contributes to **protecting recovery data (11.3)** and **maintaining an isolated instance of recovery data (11.4)** - a ransomware event that encrypts the local drive doesn't touch the cloud-side versions.

4. Identity, access, and administrative hygiene

This is the section most CIS SME-level guides gloss over, because it needs Entra ID configuration, not just a device policy.

CIS Safeguards 6.3 and 6.4 - MFA for externally-exposed applications and remote access. Build a Conditional Access policy requiring MFA for all users, all cloud apps, when accessing from outside your trusted network. This is IG1 baseline - every client should have this on day one.

Phishing-resistant MFA for admin accounts. Standard MFA is the IG1 floor; requiring **phishing-resistant** MFA specifically for privileged roles is a step above it, and it's the one control most SMB tenants skip because it needs Conditional Access **Authentication Strengths**, not just a basic MFA toggle. Configure a policy scoped to your privileged directory roles (Global Administrator, Security Administrator, Exchange Administrator, Conditional Access Administrator, at minimum) requiring the built-in **Phishing-resistant MFA** authentication strength - FIDO2 security keys, Windows Hello for Business, or certificate-based authentication. Microsoft ships a ready-made policy template for exactly this ("Require phishing-resistant multifactor authentication for Microsoft Entra administrator roles"). Always exclude one break-glass account, stored offline, so a misconfiguration can't lock you out of your own tenant.

CIS Safeguard 4.7 - Manage default accounts. Rename or disable the built-in local administrator account on Windows devices via the Settings Catalog "Local Administrator Password Solution" (Windows LAPS) profile, which also rotates the local admin password automatically - closing the single most common lateral-movement path in a small-business breach.

CIS Safeguard 5.3 - Disable dormant accounts. We recommend disabling accounts after 45 days of inactivity as a working threshold. Be aware of a real gap here: **base Entra ID has no native "auto-disable after N days" toggle.** Reaching that automatically requires **Microsoft Entra ID Governance** (a licensed add-on) using Lifecycle Workflows or Access Reviews scoped to sign-in inactivity. Without that licence, this has to run as a scheduled script against the Microsoft Graph API, checking the **lastSignInDateTime** field and disabling anything past the threshold. Most SMB tenants don't hold Entra ID Governance, so budget for either the licence or the script - don't assume the portal will do this for you out of the box.

5. Continuous GRC telemetry and audit correlation

CIS Safeguards 8.1 and 8.2 - Audit log management and collection. Microsoft 365 audit logging now lives in the **Microsoft Purview compliance portal**, under **Audit**. Standard licensing retains 180 days of activity; Audit (Premium), included with E5 or as an add-on, extends default retention to a year and can go out to ten with the long-term retention add-on. Turn on unified audit logging for every workload (Exchange, SharePoint, Entra ID sign-ins, Teams) so PowerShell command-line-level actions are captured, not just UI clicks.

Turning telemetry into standing evidence, not a one-off screenshot. The point of all this configuration isn't the settings themselves - it's that they produce continuous, timestamped evidence you can hand to an auditor without a scramble. Feed Intune compliance state, Defender alerts, and Purview audit exports into a continuous monitoring layer, and the same telemetry maps cleanly onto:

- **NIST CSF 2.0** - PR.PS-01 (configuration management) and PR.DS-11 (data backup availability)
- **ISO 27001 Annex A** - the access-control, cryptography, and logging control families
- **Spain's ENS** - op.mon.3 (automatic event correlation), which specifically expects continuous, correlated monitoring rather than periodic manual review

That's the actual deliverable of a CIS IG1 build-out: not a one-time checklist, but a compliance posture that keeps producing its own evidence every day.

Book a free 30-minute call and we'll map your current Intune and Entra ID tenant against this exact blueprint - what's already covered, what's missing, and what it takes to close the gap.