nerdio

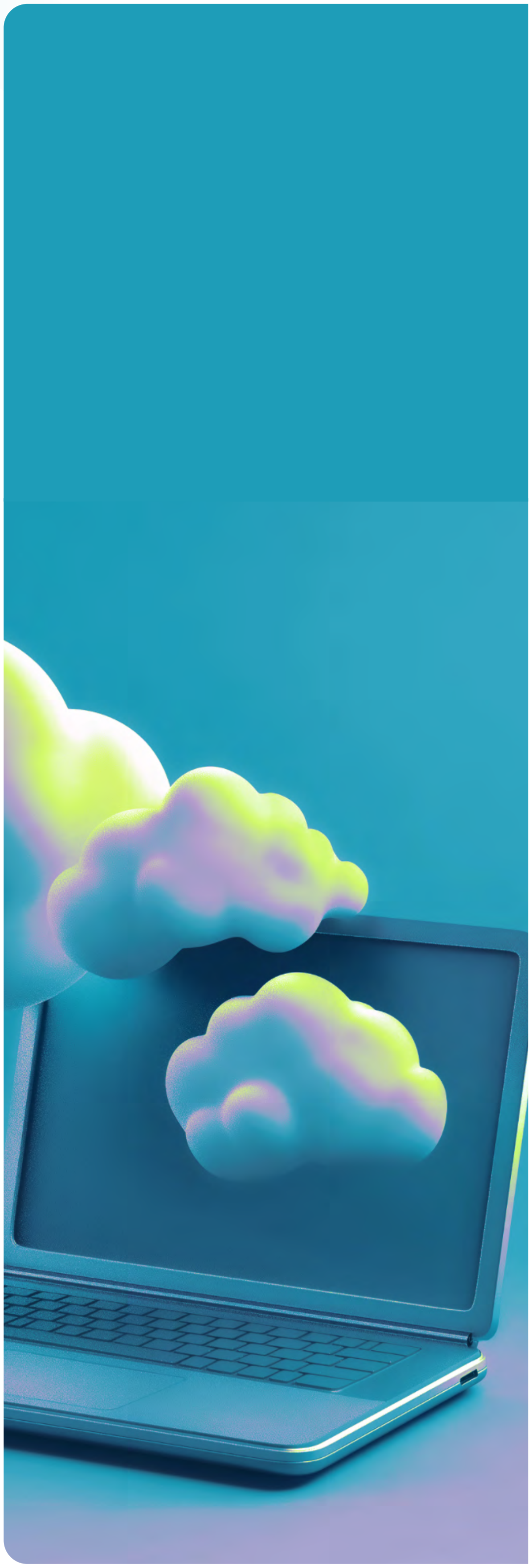
CIS Level 1 Intune policies for Windows 11 (3.0.1)

Full breakdown & MSP guide

Overview

The CIS (Center for Internet Security) Level 1 Baseline for Windows 11 is a robust security standard, widely recognized and trusted to reduce the attack surface and standardize controls for enterprise and SMB fleets.

When implemented through Microsoft Intune MDM templates, these settings provide a consistent, auditable way to enforce best practices across thousands of endpoints. Below, you'll find in-depth summaries, practical deployment notes, impact expectations for users and help desks, and a full reference table.



1 CIS L1 admin templates: system (Windows 11 Intune 3.0.1)

PURPOSE

Focuses on system-wide hardening—especially credential policies, boot time security, device driver management, and restricting legacy/remoted access features.

HIGHLIGHTS

- **Credential guard/delegation:** Tightens delegation, disables export of non-secure credentials, disables PIN & picture passwords to enforce strong authorization only.
- **Boot/driver controls:** Disables unverified boot drivers, enforces secure boot start driver policy, minimizes risk of rootkits and driver attacks.
- **Remote access & assistance:** Disables all unsolicited and solicited remote assistance. Only authenticated, authorized remote management is permitted.
- **Audit logging:** Command-line arguments for process creation are included in audit logs (important for deeper forensic capability).
- **Device/network restriction:** Device metadata pulling from network is blocked, making plug-and-play attack surfaces far smaller.

END-USER/HELP DESK IMPACT

Users can only use strong passwords; no easy PINs or picture logon. Some device/driver installs may fail if they come from untrusted sources. Remote help desk workflows are intentionally limited for security.

2 CIS L1 admin templates: Windows components (Windows 11 Intune 3.0.1)

PURPOSE

Targets hardening of built-in Windows features, core components, Windows Explorer, RDP, HomeGroup, event log management, and security interactions.

HIGHLIGHTS

- **SmartScreen:** SmartScreen is forcibly enabled for Explorer—users are blocked from executing known-bad files and warned about unsigned executables.
- **HomeGroup/sharing disabled:** Classic HomeGroup and ad-hoc network sharing are turned off completely.
- **Credential UI:** Password reveal button is hidden; password reset questions are not presented to local users.
- **Powershell & script restrictions:** Enforces script block logging and PowerShell transcription—even invocation headers (with a default blank output directory) for security monitoring.
- **RDP security:** Disables password saving and drive redirection in Remote Desktop; enforces highest encryption mode and multi-factor for connections.
- **Event logging:** Expands max file sizes for security logs for robust auditing.

END-USER/HELP DESK IMPACT

Macro-based solutions and unsigned/legacy tools can break. Users can't disable Defender protections—even temporarily. False positives in legitimate business workflows could increase, but overall malware risk is greatly reduced.

3 CIS L1 auditing (Windows 11 Intune 3.0.1)

PURPOSE

Enables comprehensive, CIS-aligned, OS-level auditing across logon, account, object, privilege, and process events.

HIGHLIGHTS

- **Coverage:** Account logon, user credential validation, security group changes, logon/logoff, account lockout, and sensitive privilege use are all audited.
- **Object access:** File share and removable storage (USB, etc.) access is tracked.
- **Policy & system changes:** Changes to authentication, authorization, policy, group membership, system integrity, and special logons are captured.
- **Process auditing:** New process creation events (including CLI params) are auditable.

END-USER/HELP DESK IMPACT

Event log sizes increase sharply; auditing can occasionally reveal business process friction ("why can't I access this resource?"), but security and compliance posture is dramatically improved.

4 CIS L1 Defender (Windows 11 Intune 3.0.1)

PURPOSE

Drives Microsoft Defender configuration to the most secure enterprise baseline, with advanced attack surface reduction (ASR), antimalware, cloud protection, and real-time scanning enforced.

HIGHLIGHTS

- **ASR rules:** All critical ASR settings are on (block Office process spawning, execution of obfuscated scripts, Office injection, USB launch, etc).
- **Defender real-time protections:** Cannot be turned off; includes real-time behavior, email, removable drive, and script scanning.
- **SpyNet/cloud reporting:** Forced, cannot be altered locally.
- **PUA protection:** Detects/blocks potentially unwanted apps by default.

END-USER/HELP DESK IMPACT

Macro-based solutions and unsigned/legacy tools can break. Users can't disable Defender protections—even temporarily. False positives in legitimate business workflows could increase, but overall malware risk is greatly reduced.

5 CIS L1 device lock & WHFB (Windows 11 Intune 3.0.1)

PURPOSE

Enforces strict device lock, password, and Windows Hello for Business requirements—critical for Zero Trust environments.

HIGHLIGHTS

- **Password policy:** Minimum 14 characters, expires every 365 days, history of 24 remembered, complexity (at least 3 types), age minimum (1 day).
- **PIN policy (WHFB):** PIN minimum length of 6, must use security device (TPM, etc.).
- **Anti-spoof:** Enhanced anti-spoof enabled on biometric logon.
- **Alphanumeric required:**Picture passwords/patterns disabled.

END-USER/HELP DESK IMPACT

Users MUST set and remember strong passwords and PINs, frequent password changes, help desk workload increases (at least initially). Some older hardware may not support these requirements.

6 CIS L1 firewall (Windows 11 Intune 3.0.1)

PURPOSE

Activates and enforces strict host firewall rules for all network profiles.

HIGHLIGHTS

- **All profiles on:** Domain, private, and public firewalls enabled by default.
- **Inbound blocks:** Default inbound policy is blocked; outbound is allowed (standard).
- **Enhanced logging:** Firewalls log all dropped packets and successful connections, large max log files enabled.
- **Policy merge:** Local policy/app/user port merges allowed (except for public profile, which is most restrictive).
- **Notifications:** No inbound notification pop-ups (reduces social engineering risk).

END-USER/HELP DESK IMPACT

Legacy network shares, inbound services, and some app-to-app communications can break. Users will NOT see pop-ups for inbound blocks, reducing confusion and “silent” app breakage.

7 CIS L1 local policies security options (Windows 11 Intune 3.0.1)

PURPOSE

Focuses on account, logon, UAC, and SMB security options—locks down local accounts, guest access, NTLM, and user elevation.

HIGHLIGHTS

- **Microsoft accounts blocked:** Users cannot use MS accounts for OS logon.
- **Guest disabled/renamed:** Guest account renamed to "Gtest" or similar, disabled.
- **UAC/tokens:** UAC is highly restricted, approval is required for all admin actions, only elevation for secure locations.
- **900s inactivity timeout:** Workstation auto-locks after 15 minutes of inactivity.
- **Custom banner:** TEST TEST TEST: must be customized.

END-USER/HELP DESK IMPACT

No consumer logons, login screens display "TEST" placeholder, must be changed to org-compliant message. More prompt for elevation, stricter controls on account behaviors.

8 CIS L1 section 1-3.9.1.1 (Windows 11 Intune 3.0.1)

PURPOSE

Implements a wide array of baseline controls: Disables lock screen features (camera/Cortana/slideshow), legacy networking, and hardens protocols.

HIGHLIGHTS

- **Lock screen hardening:** No camera, Cortana, or slideshow allowed above lock.
- **Legacy protocols:** SMBv1, NetBIOS, ICMP redirects disabled.
- **AutoAdmin disabled:** Automatic admin sign on forbidden.
- **UNC paths:** Hardened with require-integrity/mutual auth.
- **Default policy:** Safe DLL search order, faster lockout, restricted router discovery.

END-USER/HELP DESK IMPACT

Most consumer-facing lock screen items gone, legacy systems may stop working. Network admins must support new, modern file share methods.

9 CIS L1 section 22-80 (Windows 11 Intune 3.0.1)

PURPOSE

Tightens privacy and cloud options: Blocks telemetry, Cortana, feedback notifications, news/interests, non-private Windows Store.

HIGHLIGHTS

- **No Cortana, Spotlight, Ink Workspace, feedback:** All consumer/telemetry features blocked organization-wide.
- **App control:** Only private store allowed, GameDVR off.
- **Web protection:** Defender browser integration locked, exploit protection override disallowed.
- **Telemetry:** Minimal, none if possible; only required data sent.
- **No news/interests feed:** Taskbar remains “businesslike.”

END-USER/HELP DESK IMPACT

Users lose almost all consumer/ personalization and cloud “added value” features. Gamers and power users may notice, but business productivity is unaffected (and privacy much improved).

10 CIS L1 system services (Windows 11 Intune 3.0.1)

PURPOSE

Disables non-essential Windows system services used for gaming/Xbox integration.

HIGHLIGHTS

- **All Xbox-related services:** Disabled, including accessory management, live auth, game save, and networking.
- **Startup mode set to disabled:** No background Xbox/ gaming services allowed to run.

END-USER/HELP DESK IMPACT

Gaming, streaming, and Xbox apps/ features will not function, but no impact on productivity or business software.

11 CIS L1 user rights (Windows 11 Intune 3.0.1)

PURPOSE

Granularly restricts high-privilege operations, specifying exactly which group or SID gets each user right.

HIGHLIGHTS

- **Admins only:** Nearly all privileged actions (shutdown, backup, debug, restore, install drivers, etc.) set to local administrators (SID: S-1-5-32-544).
- **Explicit "no one" for sensitive rights:** Many rights left blank (using empty CDATA), making them unassignable.
- **Network access:** Only admins or power users allowed, denied for guests and local service accounts.
- **Impersonation/delegation:** Only highly trusted/ privileged accounts permitted.

END-USER/HELP DESK IMPACT

Legacy apps needing privileged OS rights may break. Most users see no direct difference, but fewer vectors for privilege escalation and lateral movement.

12 CIS L1 virtualization based technology (Windows 11 Intune 3.0.1)

PURPOSE

Leverages VBS (virtualization-based security), device guard, LSA protection, secure boot, and HVCI for next-level credential and kernel isolation.

HIGHLIGHTS

- **System guard, credential guard, HVCI:** All enabled. Mitigates kernel-level exploits, scripting attacks, credential dumping.
- **UEFI requirements:** Requires UEFI memory attributes table for maximum protection.
- **Platform security:** Blocks unsigned or legacy drivers completely.

END-USER/HELP DESK IMPACT

Some legacy software and drivers will not run (especially unsigned or non-UEFI). Slight boot time increases. Most impactful on non-Enterprise SKUs or modernizing legacy environments.

CIS Intune policies table (Windows 11–L1)

Policy name	What it does/focus	Key settings/user impact	Enterprise-only?	Any placeholders?	Day-to-day impact
CIS L1 admin templates system	System hardening: audit, credentials, device, lock/logon, power	• Command-line audit in events • Disables PIN, picture password • Disables device metadata download • Restricts credentials & driver policies • No remote assistance	Some features require Enterprise for full protection	**X** None	Passwords only, some device/ driver installs may break, no remote help
CIS L1 admin templates Windows components	Hardens Windows features: Explorer, credentials, RDP, logging, SmartScreen	SmartScreen, disables HomeGroup, toughens RDP/security log, disables legacy password help	PowerShell logging is best in Enterprise/EDU	PowerShell transcription output directory is blank	No HomeGroup, RDP restrictions, more security prompts
CIS L1 auditing	Expands Windows audit logging	All events (logon, policy, privilege, USB, etc.) are tracked	No	**X** None	Large logs, all system actions tracked
CIS L1 Defender	Hardens Defender, ASR, anti-tampering	All core Defender/ASR are enabled, cannot be turned off, stricter macro/script control	ASR/full requires Defender for Endpoint	**X** None	Macros/scripts break, Defender always on
CIS L1 device lock & WHFB	Device lock & Hello for Business	Passwords (min 14 chars) and complex PINs, anti-spoofing enforced	Full WHFB requires Enterprise	{tenantid} (template, not a real placeholder)	Users must follow strong password policy, some devices not supported
CIS L1 firewall	Strict firewall enforcement	Domain/Private/Public all enabled, dropped packets logged	No	**X** None	Legacy inbound communication breaks
CIS L1 local policy security options	Local/account logon security	MS accounts blocked, guest/ adm renamed, 15-min idle lock, UAC strict, banner is TEST (need to change)	No	"TEST TEST TEST" login text (replace in production)	No MS accounts, more prompts, custom banner shown
CIS L1 section 1-3.9.1.1	Baseline for lock screen, net, UAC, protocols	Disables camera/Cortana on lock, disables legacy protocols, hardens networking	Some advanced parts need Enterprise	**X** None	No camera on lock, legacy file shares may break
CIS L1 Section 22-80	Restricts cloud, telemetry, privacy, feedback	No Cortana/Spotlight/Ink/ Feedback, telemetry lowest	Enterprise recommended for some privacy options	**X** None	No personalization or "news" features
CIS L1 system services	Disables Xbox-related services	All Xbox/gaming services disabled	No	**X** None	Gaming/Xbox not available
CIS L1 user rights	Tight OS user right restrictions	• Only admin group can backup, shutdown, debug, etc. • Many rights unassigned for max hardening	No	Many CDATA blanks ("no one")	Legacy admin-needed apps may break
CIS L1 virtualization-based technology	Enables VBS, device/ credential guard, secure boot	HVCI, LSA, platform security all ON, UEFI required	Enterprise/EDU required for some options	**X** None	Old drivers/apps may not work, requires modern hardware

Guidance & practical advice

- **Before rollout:** Ensure all endpoints run a compatible SKU (Enterprise is ideal for advanced protections). Test legacy peripherals/drivers for compatibility.
- **Initial deployment:** Pilot to a group of power users/admins. Watch event logs, application failures, help desk tickets.
- **Customizations needed:** CHANGE all placeholder login banners ("TEST TEST TEST") to your company's compliance/consent message.
- **Communicate:** Notify users of removed features (HomeGroup, PIN, personalization, Office macros), and explain the intent behind new prompts and logon behaviors.
- **Ongoing:** Review Intune and Defender logs for spikes/errors, adjust macros/loosen as necessary for LOB apps, and validate new hardware against VBS/Device Guard/HVCI requirements.

In summary, deploying these CIS Intune Baselines rapidly improves security, audit readiness, and incident response, but demands user education, careful legacy analysis, and customization of banners and communications. Consider this your blueprint for a secure, supportable, and well-documented Windows 11 security posture!

About Nerdio

Nerdio is a leading provider of powerful, simplified cloud management solutions for businesses of all sizes. Trusted by managed service providers (MSPs) and enterprise IT departments alike, Nerdio equips organizations with seamless, cost-effective management tools for Azure Virtual Desktop (AVD), Windows 365, and comprehensive Modern Work solutions.

With thousands of customers worldwide, Nerdio accelerates cloud adoption, enabling companies to thrive in an era of hybrid work by providing modern, future-proof technology that adapts to evolving workplace needs.

For more information, please visit **www.getnerdio.com**.

nerdio

WEB www.getnerdio.com
EMAIL hello@getnerdio.com