ROMY
Romy Dar | Organizational Development Consultant

Windows Hardening Checklist

Windows 11 and Windows 10 Workstations and Windows Server

Version 1.1 | Updated November 25, 2026

Important: test in a test environment before production

This is a generic checklist. It is not tailored to any specific organization, its applications or its infrastructure.

Test every setting first in a test environment or a representative pilot group, and only then move it to production.

Adjust as needed. Some settings may break legacy applications, NAS devices, printers, management tools and remote connections.

Back up and prepare a rollback path before every change.

How to Use This Checklist

- **W11, W10 and Server columns:** V means the check applies, a hyphen means it does not apply, and "If needed" means it depends on the device role.
- **Verification column:** A PowerShell command or manual check that confirms the state. Run the commands in an elevated PowerShell window. The commands only read information and do not change settings.
- **Status column:** V OK, X not OK, N/A not applicable, E approved exception, ? not checked or error. A check that was not run is not a passing result.
- **Evidence column:** A reference to the evidence: screenshot, output file, report or record. Record the checker name, date and devices checked at the top of the checklist.
- **One command is not always enough:** When a check has several parts, such as limiting users and sources, verify each part and keep evidence for each.
- **Sources:** The checklist is based on the Microsoft security baselines, the CIS Benchmarks and Microsoft Learn documentation, as of November 2026. Defaults and support dates change, so check against the current source.

Review Details

Checker name	
Date	
Devices or group checked	
Checklist version	1.1

1 Before You Start

Check	W11	W10	Server	Verification	Status	Evidence
An up-to-date inventory exists for all workstations and servers: OS, version, edition, servicing channel, end-of-support date, role and owner	V	V	V	`Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion' | Select-Object EditionID, DisplayVersion, CurrentBuild`		
A test environment or representative pilot group is in place, and every change is tested there before rollout to production	V	V	V	Pilot records and results		
A backup of the data and the system exists, and a restore from it was tested	V	V	V	Restore test report		
The current security settings were exported before the change. The export does not replace a backup	V	V	V	`secedit /export /cfg C:\Hardening\before.inf`		
Every change goes through change management and is documented, including a rollback path	V	V	V	Change record		
An exceptions register is open: setting not applied, reason, compensating control, owner and review date	V	V	V	Exceptions register		
An emergency access and recovery procedure exists: who is authorized, how to reach the console, where recovery keys are, and what to do when a hardening change blocks access or management	V	V	V	Approved procedure and drill		

2 Updates and Supported Versions

Check	W11	W10	Server	Verification	Status	Evidence
The version and edition are supported. Support depends on the edition: Windows 11 24H2 Home and Pro reached end of support on October 13, 2026, and Enterprise and Education are supported until October 12, 2027	V	-	V	Inventory compared with the Microsoft supported versions table		
Windows 10 22H2 is covered by ESU for the current year. LTSC and IoT editions have a separate support lifecycle	-	V	-	`slmgr /dlv`		

Check	W11	W10	Server	Verification	Status	Evidence
Monthly security updates are installed within the organization target, for example 14 days	V	V	V	`Get-HotFix | Sort-Object InstalledOn -Descending`		
Third-party software is up to date: browsers, PDF readers, archivers and meeting tools	V	V	V	`winget upgrade`		
Firmware, BIOS or UEFI, and drivers are updated per the manufacturer	V	V	V	Manufacturer update tool		
The 2023 Secure Boot certificate update is complete: UEFICA2023Status is Updated and UEFICA2023Error is 0. The 2011 certificates expired during 2026	V	V	V	`Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing' | Select-Object UEFICA2023Status, UEFICA2023Error`		

3 Security Baseline

Check	W11	W10	Server	Verification	Status	Evidence
The Microsoft security baseline for the matching version is applied via GPO, Intune, or OSConfig on Windows Server 2025	V	V	V	PolicyAnalyzer, Intune report or OSConfig		
Settings were compared with the CIS Benchmark Level 1, and gaps were fixed or recorded as exceptions	V	V	V	Comparison report		
Exceptions are applied in a separate GPO, without editing the baseline object itself	V	V	V	`gpresult /h C:\Hardening\gp.html`		

4 Accounts and Privileges

Check	W11	W10	Server	Verification	Status	Evidence
Standard users work without local administrator rights	V	V	V	`Get-LocalGroupMember -Group Administrators`		
IT staff use a separate admin account that is not used for email or browsing	V	V	V	Account review		
Privileged group membership is minimal and reviewed quarterly	V	V	V	`Get-ADGroupMember 'Domain Admins' -Recursive`		
Windows LAPS manages a unique local admin password on every device. Windows Server 2016 requires Legacy LAPS	V	V	V	`Get-LapsADPassword -Identity <PC>`		

Check	W11	W10	Server	Verification	Status	Evidence
Who may decrypt encrypted LAPS passwords is defined, and an authorized support user can retrieve a password while an unauthorized user cannot. Encryption in AD requires domain functional level 2016 or later	-	-	V	ADPasswordEncryptionPrincipal and a retrieval test		
The Guest account is disabled	V	V	V	`Get-LocalUser -Name Guest`		
Local administrator accounts are denied network and RDP logon via the group Local account and member of Administrators group	V	V	V	User Rights Assignment in GPO		
Password and account lockout policies match the baseline	V	V	V	`net accounts`		
UAC is enabled	V	V	V	`(Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System).EnableLUA`		
Administrator protection status is checked and the decision documented. It is on by default since the October 2026 update, and Microsoft advises not to enable it on LAPS-managed devices, on devices that require Hyper-V, or with apps that share files across profiles	V	-	-	Windows Security, Account protection, and the documented decision		
Multifactor authentication for all remote access and admin accounts	V	V	V	Identity provider settings		
Domain admin accounts are members of Protected Users	-	-	V	`Get-ADGroupMember 'Protected Users'`		

5 Credential Protection

Check	W11	W10	Server	Verification	Status	Evidence
Credential Guard is running. Supported on Enterprise and Education editions and on servers, not on domain controllers	V	V	V	`(Get-CimInstance Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard).SecurityServicesRunning`		
LSA protection is enabled. Start in audit mode	V	V	V	`(Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Control\Lsa).RunAsPPL`		
WDigest does not cache passwords: UseLogonCredential is 0 or not set	V	V	V	`Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest`		
LAN Manager authentication level is NTLMv2 only, value 5	V	V	V	`(Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Control\Lsa).LmCompatibilityLevel`		

Check	W11	W10	Server	Verification	Status	Evidence
NTLM usage is audited, and a reduction plan exists	V	V	V	NTLM logs in Event Viewer		

6 Network and Protocols

Check	W11	W10	Server	Verification	Status	Evidence
The firewall is on in all profiles, inbound traffic is blocked by default, and dropped packets are logged. The effective policy was checked, including whether local rules are merged	V	V	V	`Get-NetFirewallProfile -PolicyStore ActiveStore | Format-Table Name, Enabled, DefaultInboundAction, LogBlocked, AllowLocalFirewallRules`		
SMBv1 components are removed, on both the client and server sides	V	V	V	`Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol`		
SMB signing is required on both server and client sides	V	V	V	`(Get-SmbServerConfiguration).RequireSecuritySignature ; (Get-SmbClientConfiguration).RequireSecuritySignature`		
Insecure SMB guest logons are blocked	V	V	V	`(Get-SmbClientConfiguration).EnableInsecureGuestLogons`		
LLMNR is disabled	V	V	V	`(Get-ItemProperty 'HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient').EnableMulticast`		
NetBIOS over TCP/IP is disabled, value 2	V	V	V	`Get-CimInstance Win32_NetworkAdapterConfiguration -Filter 'IPEnabled=TRUE' | Select-Object Description, TcpipNetbiosOptions`		
RDP is disabled where not needed and is never exposed to the internet	V	V	V	`(Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server').fDenyTSConnections`		
RDP requires NLA: UserAuthentication is 1	V	V	V	`(Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp').UserAuthentication`		
RDP access is limited to a dedicated group and defined source addresses, and a connection was tested from an allowed source and from a source that should be blocked	V	V	V	`Get-LocalGroupMember 'Remote Desktop Users' ; Get-NetFirewallRule -DisplayGroup 'Remote Desktop' | Get-NetFirewallAddressFilter`		
WinRM is limited to the management network, with no Basic authentication and no unencrypted traffic	If needed	If needed	V	`Get-Item WSMan:\localhost\Service\Auth\Basic ; Get-Item WSMan:\localhost\Service\AllowUnencrypted ; Get-ChildItem WSMan:\localhost\Listener`		
OpenSSH Server is installed only when needed, with key-based authentication only	If needed	If needed	If needed	`C:\ProgramData\ssh\sshd_config`		
TLS 1.0 and TLS 1.1 are disabled	V	V	V	`HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols`		

7 Malware Protection and Application Control

Check	W11	W10	Server	Verification	Status	Evidence
Microsoft Defender or an alternative product is active, with real-time protection and current signatures. On Windows Server, an alternative product does not switch Defender to passive mode automatically. With an alternative product, collect the evidence from that product	V	V	V	`Get-MpComputerStatus | Select-Object AMRunningMode, RealTimeProtectionEnabled, AntivirusSignatureLastUpdated`		
Tamper Protection is on	V	V	V	`(Get-MpComputerStatus).IsTamperProtected`		
Cloud protection, PUA blocking and Network Protection are on	V	V	V	`Get-MpPreference | Select-Object MAPSReporting, PUAProtection, EnableNetworkProtection`		
The three standard protection ASR rules are in block mode. Other rules move from audit to block after testing. ASR requires Defender as the active antivirus	V	V	V	`Get-MpPreference | Select-Object AttackSurfaceReductionRules_Ids, AttackSurfaceReductionRules_Actions`		
Controlled Folder Access was evaluated	V	V	If needed	`(Get-MpPreference).EnableControlledFolderAccess`		
Application control is in place: App Control for Business or AppLocker, at minimum blocking execution from user-writable folders. Enforcement is verified for each technology	V	V	V	`Get-AppLockerPolicy -Effective ; CiTool.exe -lp`		
Office macros in files from the internet are blocked	V	V	If needed	Microsoft 365 Apps baseline		
The Microsoft Edge baseline is applied, and SmartScreen is on	V	V	If needed	`edge://policy`		

8 Encryption and Hardware

Check	W11	W10	Server	Verification	Status	Evidence
BitLocker encrypts the OS drive. On laptops the protector is TPM plus PIN, not TPM only	V	V	If needed	`(Get-BitLockerVolume -MountPoint C:).KeyProtector | Select-Object KeyProtectorType`		
BitLocker recovery keys are stored in Active Directory or Microsoft Entra ID, and an authorized support user was able to retrieve a key in a controlled test	V	V	If needed	Check in AD or Entra and a controlled retrieval test		
Secure Boot is on	V	V	V	`Confirm-SecureBootUEFI`		
TPM 2.0 is present and ready	V	V	V	`Get-Tpm`		

Check	W11	W10	Server	Verification	Status	Evidence
Memory integrity (HVCI) is on	V	V	V	`(Get-CimInstance Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard).SecurityServicesRunning`		
Writing to removable drives is blocked or controlled, and was tested with a write attempt	V	V	V	`(Get-ItemProperty 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}').Deny_Write`		
AutoPlay is off	V	V	V	`(Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer').NoDriveTypeAutoRun`		
A firmware password is set, and booting from external devices is blocked	V	V	V	BIOS or UEFI settings		

9 Operating System and Services

Check	W11	W10	Server	Verification	Status	Evidence
PowerShell 2.0 is removed. It is already removed in Windows 11 24H2 and later and in Windows Server 2025	V	V	V	`Get-WindowsOptionalFeature -Online | Where-Object FeatureName -like '*PowerShellV2*'`		
Script Block Logging is on in Windows PowerShell, and in PowerShell 7 if it is installed	V	V	V	`(Get-ItemProperty 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging').EnableScriptBlockLogging ; (Get-ItemProperty 'HKLM:\SOFTWARE\Policies\Microsoft\PowerShellCore\ScriptBlockLogging').EnableScriptBlockLogging`		
Print Spooler is disabled on every server that is not a print server, and on all domain controllers	If needed	If needed	V	`Get-Service Spooler | Select-Object Status, StartType`		
Unused features, roles and services are removed	V	V	V	`Get-WindowsOptionalFeature -Online | Where-Object State -eq 'Enabled'`		
The screen locks after at most 15 minutes of inactivity	V	V	V	`(Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System).InactivityTimeoutSecs`		
The clock is synchronized with a reliable time source	V	V	V	`w32tm /query /status`		

10 Logging and Monitoring

Check	W11	W10	Server	Verification	Status	Evidence
Advanced audit policy follows the Microsoft recommendations for the device role: workstation, member server or domain controller. The expected events were verified to be generated	V	V	V	`auditpol /get /category:*`		

Check	W11	W10	Server	Verification	Status	Evidence
The command line is recorded in process creation events, event 4688	V	V	V	`(Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit').ProcessCreationIncludeCmdLine_Enabled`		
The Security log size is at least 196608 KB	V	V	V	`wevtutil gl Security`		
Sysmon is installed with a configuration file. Built-in on Windows 11 and Windows Server 2025, standalone elsewhere	V	V	V	`Get-Service *sysmon*`		
Logs are forwarded to a central server via WEF or a SIEM. A recent event from every device and a test event reaching its destination were verified	V	V	V	Inventory compared with reporting devices, and a test event		
An alert exists for a device or source that stopped reporting, a stopped collection service and a log that is filling up	V	V	V	SIEM alert rules and a test event		
Alerts exist for critical events, including 1102, 4720, 4732, 4740, 7045 and 4104. Each alert has an owner, a response time and escalation criteria	V	V	V	SIEM alert rules and the handling procedure		

11 Servers and Domain Controllers

Check	W11	W10	Server	Verification	Status	Evidence
Minimal installation, Server Core where possible, with only the required roles	-	-	V	`Get-WindowsFeature | Where-Object Installed`		
Administration is done from a dedicated admin workstation, with no browsing or email on the server	-	-	V	Policy and manual review		
Tiering model: accounts that manage domain controllers do not log on to other servers or workstations	-	-	V	User Rights Assignment in GPO		
LDAP signing and LDAP channel binding are enforced on domain controllers	-	-	V	`Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters | Select-Object LDAPServerIntegrity, LdapEnforceChannelBinding`		
The krbtgt password is reset twice, after a replication health check, waiting at least 10 hours between resets, or longer if the Kerberos ticket lifetime was changed. Suggested frequency: yearly, per organizational policy	-	-	V	`Get-ADUser krbtgt -Properties PasswordLastSet ; repadmin /replsummary`		

Check	W11	W10	Server	Verification	Status	Evidence
Active Directory Recycle Bin is enabled	-	-	V	`Get-ADOptionalFeature -Filter 'Name -like "Recycle Bin Feature"' | Select-Object EnabledScopes`		
On Windows Server 2025, SMB signing is required for inbound connections too, not only outbound	-	-	V	`(Get-SmbServerConfiguration).RequireSecuritySignature`		
Backups follow the 3-2-1 rule, with an offline or immutable copy, and a restore test every quarter	-	-	V	Restore test report		
Windows Server 2016 machines are replaced before end of support on January 12, 2027, or covered by ESU	-	-	V	`Get-ComputerInfo | Select-Object OsName`		

12 Ongoing Maintenance

Check	W11	W10	Server	Verification	Status	Evidence
Monthly: security updates, compliance reports and a periodic review of the handled alerts	V	V	V	Maintenance log		
Quarterly: privileged group review, Defender and firewall exclusions review, and a restore test	V	V	V	Maintenance log		
With every new Windows version: new baseline, comparison, pilot and rollout	V	V	V	PolicyAnalyzer		
Yearly: full review against this checklist and an incident response exercise	V	V	V	Review report		

Disclaimer

This checklist is provided as is, without warranty of any kind. It does not replace professional advice, a review of your specific environment, or vendor guidance.

Responsibility for applying the settings and for the results lies with the implementer.

Open License

This checklist is licensed under Creative Commons Attribution 4.0 International, CC BY 4.0.

You may copy, distribute, adapt and use it, including for commercial purposes, provided you credit the source: Romy Dar, ROMY, romy.co.il.

https://creativecommons.org/licenses/by/4.0/

Sources

Links to the official documentation, for checking and updating the settings. Click a source name to open it.

Microsoft Security Compliance Toolkit
Microsoft security baselines and the PolicyAnalyzer tool

CIS Benchmarks
CIS baselines for workstations and servers

Microsoft Learn - Supported versions of Windows client
Versions, editions and end-of-support dates

Microsoft Support - Secure Boot registry key updates, KB5068202
Checking the Secure Boot certificate update status

Microsoft Support - Secure Boot certificate expiration, KB5062710
Expiration of the 2011 certificates and the update to 2023

Microsoft Learn - Windows LAPS with Active Directory
Password encryption and read and decrypt permissions

Microsoft Learn - Administrator protection
Scenarios where the feature should not be enabled

Microsoft Learn - Windows Firewall rules
Effective rules and local rule merging

Microsoft Learn - Detect, enable and disable SMBv1, SMBv2 and SMBv3
Checking and removing SMBv1 components

Microsoft Learn - Installation and configuration for WinRM
Authentication methods, encryption and listeners

Microsoft Learn - Microsoft Defender Antivirus compatibility
Running alongside another security product and passive mode

Microsoft Learn - Attack surface reduction rules
ASR rules and audit and block modes

Microsoft Learn - Get-AppLockerPolicy
Scope of the AppLocker verification command

Microsoft Learn - Enable-BitLocker
Enabling encryption and protector types

Microsoft Learn - Audit policy recommendations
Audit recommendations for workstations, servers and domain controllers

Microsoft Learn - PowerShell logging on Windows
Logging in Windows PowerShell and PowerShell 7

Microsoft Learn - Sysmon configuration files
Filtering logic and collection rules

Microsoft Learn - Reset the krbtgt password
Two resets and waiting per the Kerberos ticket lifetime

NCSC - Logging and monitoring
Collection health and end-to-end testing

For questions and support with hardening and information security: romy@romy.co.il | +972-52-3375029 | romy.co.il