

Windows 10 & 11 Hardened Services Guide

A role-based, testable approach to reducing endpoint attack surface

WINDOWS 10 & 11 EDITION

INTRODUCTION

The appendix principle

In the United States, appendicitis is responsible for roughly 300,000 hospital visits each year. Appendectomy remains one of the most familiar emergency operations, with published estimates generally placing the number performed annually at around 250,000 to 280,000. Those figures are substantial, but they are a long way from the 10 million cases sometimes repeated in older material.

For generations, the appendix was treated as a largely redundant piece of human equipment: a small organ with no obvious day-to-day role, but with an inconvenient ability to become inflamed. It would be tempting to conclude that everyone would be safer without one. Yet preventive removal of a healthy appendix is not normal practice. Surgery creates its own risk, the organ may have useful immune and microbiome functions, and most people will never develop appendicitis. A sensible clinician diagnoses the problem, weighs benefit against harm and intervenes when the evidence justifies it.

Windows services deserve the same discipline. A standard Windows installation includes a broad set of capabilities designed to support many devices, applications and working patterns. On a particular business PC, some of those services will be essential, some will be needed only occasionally and some may have no legitimate purpose at all. Every unnecessary service adds code, privilege, dependencies and potentially a network-facing route that an attacker might misuse.

That does not make indiscriminate disablement good security. Stopping the wrong service can interrupt updates, authentication, networking, endpoint protection or a business application. The objective is not to produce the shortest possible services list. It is to retain the minimum functionality needed by the endpoint's approved role—and to make every change through evidence, testing and rollback.

Diagnose before you operate

Treat each service as a risk decision, not an item on a generic disable list. Discover it, understand its function and dependencies, confirm whether the endpoint role needs it, test the proposed change and verify the result.

Figures are rounded estimates. Sources: [NCBI StatPearls, Appendicitis](#) (approximately 300,000 US hospital visits annually), the [AHRQ evidence review](#) (over 250,000 appendectomies annually) and a [National Hospital Discharge Survey analysis](#) (approximately 280,000 appendectomies annually).

01 — EXECUTIVE BRIEF

Purpose and scope

Windows services sit quietly in the background, but each one represents code, privileges, dependencies and—sometimes—a listening network interface. Reducing unnecessary functionality can shrink the attack surface. Doing it without evidence can also break updates, authentication, networking or line-of-business applications.

The operating principle

Preserve Windows defaults unless a service is demonstrably unnecessary for the endpoint role. Record the business reason, test the change, deploy in stages and verify the result.

This guide provides a practical baseline for Windows 10 22H2 and current Windows 11 Enterprise and Pro endpoints. It is a decision aid, not a universal disable list. Editions, feature updates, hardware, management tooling and installed applications alter the services present and their trigger behaviour.

The recommendations use five states: RETAIN, RETAIN IF REQUIRED, CANDIDATE, DEFAULT / TEST, and INVESTIGATE. A candidate is not an instruction to disable; it is an invitation to validate that the associated function has no approved business use.

Audience: endpoint engineering, security operations, IT support, auditors and SecureX7 administrators.
Scope: Windows 10 and Windows 11 desktop endpoints. Windows Server, kiosks, Azure Virtual Desktop and specialist OT/IoT images require separate role profiles.

Revision basis: Windows 10 and Windows 11 guidance and Microsoft documentation available in August 2026. Windows 10 entries refer to 22H2 unless stated otherwise. Revalidate this baseline for every feature release.

02 — ATTACK SURFACE

Why services matter

A service can be perfectly legitimate and still add risk. It may run with elevated rights, accept local or remote requests, load third-party modules, expose a protocol, or become useful to an attacker after compromise. Hardening therefore asks a simple question: does this endpoint need this capability?

Service control supports the wider goals of secure configuration management: minimise functionality, maintain an approved baseline, detect drift and preserve evidence of change. The security gain comes from the governance around the setting—not from chasing the smallest possible process count.

What has changed since 2019

- Windows 10 and 11 rely heavily on trigger-start services. A Manual service may start automatically when a feature invokes it.
- Many services are created per user at sign-in and carry a suffix such as `_443f50`. Manage the template, not a single temporary instance.
- Security baselines are versioned. A sound Windows 10 22H2 profile is not automatically suitable for Windows 11 24H2 or 25H2.
- Built-in security components are interdependent. Disabling BFE, Windows Defender Firewall, RPC or Event Log is a security regression, not hardening.

Less is useful. Lowest is not the goal.

A hardened endpoint should provide the minimum approved business functionality while remaining supportable, observable and patchable.

03 — FROM INVENTORY TO ASSURANCE

A SecureX7 hardening workflow

1	Discover Identify Windows 10 and 11 assets, edition, build, role, owner and location.
2	Assess Compare observed service states with the approved role baseline.
3	Prioritise Combine exposure, privilege, vulnerability and business context.
4	Remediate Provide clear action, test, rollback and approval guidance.
5	Verify Rescan, confirm the service state and track compliance improvement.

SecureX7 terminology in this guide

Asset Discovery & Estate Visibility establishes what is present. Configuration Assessment tests the observed state. Security Posture Scoring and Risk-Based Prioritisation focus attention. AI-Assisted Analysis explains impact. Guided or Automated Configuration Remediation applies an approved correction. Verification of Completed Actions closes the loop and supports audit-ready reporting.

04 — OBSERVE BEFORE CHANGING

Build the inventory

Start from a representative donor device for each endpoint role. Capture service name, display name, state, start mode, service account, executable path and dependencies. A single list of service names is not enough.

```
Get-CimInstance Win32_Service | Select-Object Name, DisplayName, State, StartMode, StartName, PathName |  
Sort-Object DisplayName | Export-Csv .\services-before.csv -NoTypeInformation  
  
Get-CimInstance Win32_Service | Where-Object State -eq 'Running' | Select-Object Name, DisplayName,  
StartMode, StartName  
  
Get-NetTCPConnection -State Listen | Select-Object LocalAddress, LocalPort, OwningProcess | Sort-Object  
LocalPort  
  
Get-CimInstance Win32_Service | Where-Object PathName -match '^"?[^\"]*' | Select-Object Name, StartName,  
PathName
```

Record these contextual fields in SecureX7: endpoint role, device owner, business applications, network exposure, approved remote-management tools, security agents, printing needs, VPN/802.1X use, Windows Hello use and exception owner.

Watch the executable path

Unquoted service paths, writable service binaries and unexpected privileged accounts may be more urgent than an unnecessary optional service. Treat them as findings for risk-based prioritisation.

05 — EVIDENCE AND RISK

Decide what to change

Decision	Meaning	Required evidence
RETAIN	Core or security-critical service.	No change. Monitor for unexpected stop, disablement or binary change.
RETAIN IF REQUIRED	Supports a legitimate but role-dependent capability.	Named business function, owner and dependency.
CANDIDATE	Often unnecessary on a managed enterprise endpoint.	Confirmed absence of use, pilot test and rollback plan.
DEFAULT / TEST	No general security benefit from changing the default.	Change only for a specific, tested requirement.
INVESTIGATE	Unexpected, unsigned, vulnerable or policy-unknown service.	Publisher, binary hash, install source, privilege and exposure analysis.

SecureX7 risk context should increase priority where a service is internet-reachable, runs as LocalSystem, uses a vulnerable executable, appeared unexpectedly, has a weak path or permission, or sits on a high-sensitivity asset. A low-value optional service that is stopped and not exposed is usually less urgent.

06 — PILOT, DEPLOY, VERIFY

Change safely

The safest sequence is to stop first, observe, then disable. Where practical, retain the previous start mode and export a before-state so the change is reversible.

```
Get-Service -Name '' | Format-List Name, Status, StartType, DependentServices, ServicesDependedOn
Stop-Service -Name '' -WhatIf Stop-Service -Name '' Set-Service -Name '' -StartupType Disabled
```

To restore a service, set the recorded start type and start it only if that was its prior state. Do not assume every Manual service should be running.

```
Set-Service -Name '' -StartupType Manual Start-Service -Name ''
```

Deployment gates

- Lab: verify boot, sign-in, networking, updates, security tooling and role applications.
- Pilot: use a representative group across hardware models and user roles.
- Staged rollout: increase coverage only after error rates and support signals remain normal.
- Verification: SecureX7 reassesses the configuration and records the completed action.
- Rollback: restore the previous start mode when business impact or unexpected dependency appears.

Do not edit the registry by default

Use Services, PowerShell, policy, MDM or supported configuration management. Direct registry changes can bypass validation and are especially risky for per-user templates.

07 — LOCAL AND ENTERPRISE CONTROLS

Management options



Services console

Select Start, type `services.msc`, open Services, then inspect the service properties. Use this for diagnosis and a small pilot—not as the primary enterprise control.

PowerShell

Use `Get-Service` for status and `Get-CimInstance Win32_Service` for richer inventory. Use `Set-Service` only through an approved, logged change.

Group Policy

For domain-managed endpoints: Computer Configuration → Windows Settings → Security Settings → System Services. Link the policy to a test organisational unit first.

Intune and MDM

Use the current Microsoft security baseline for the target Windows release and a controlled configuration profile or remediation script for additional service decisions. Baseline upgrades are not automatic equivalents: review changes before moving profile versions.

SecureX7

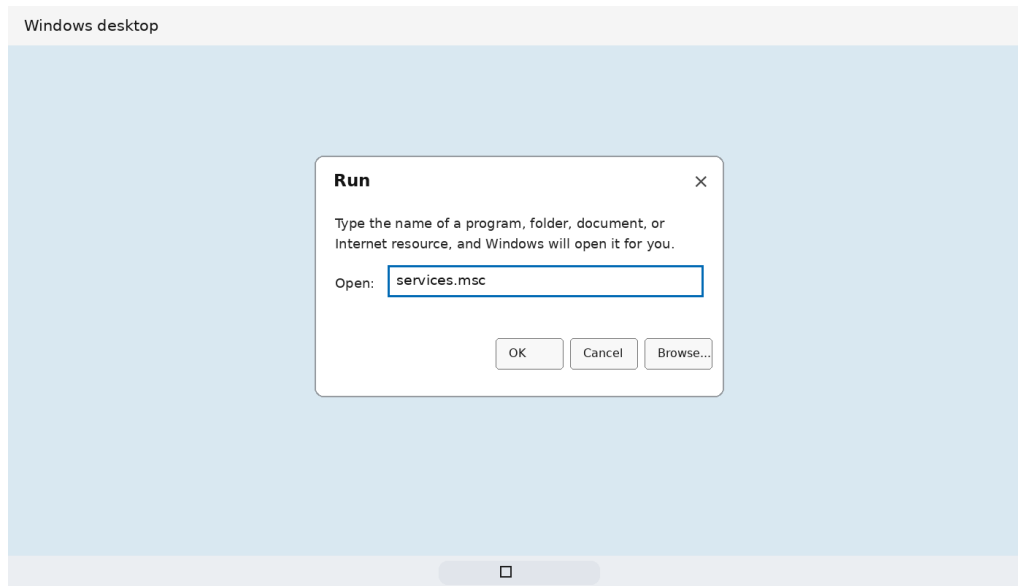
Use policy-based controls to associate a role baseline with the right assets, surface deviations, provide guided remediation and verify completed actions. Keep exceptions time-bounded, owned and visible in audit-ready reporting.

UI WALKTHROUGH — 1 OF 2

Open and inspect Services

These representative Windows 11 screens show the local graphical workflow. Windows 10 uses the same Services management console, although window styling and individual service states can differ.

1. Open the Services console



Press Windows key + R, enter `services.msc`, then select OK. Approve elevation if Windows requests administrative credentials.

2. Select and examine the service

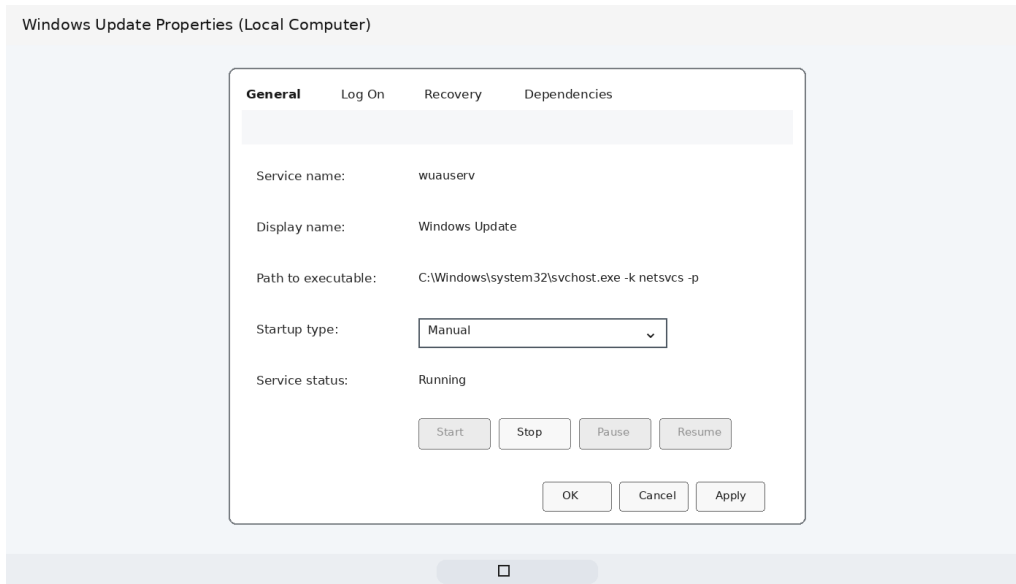
Services				
Services (Local)	Name	Description	Status	Startup Type
	Task Scheduler	Runs scheduled system tasks	Running	Automatic
	Windows Defender Firewall	Protects the computer from network access	Running	Automatic
	Windows Event Log	Manages events and event logs	Running	Automatic
	Windows Search	Provides content indexing	Running	Automatic (Delayed Start)
	Windows Time	Maintains date and time synchronisation	Running	Manual
	Windows Update	Enables detection and installation of updates	Running	Manual
	Windows Update Enables the detection, download and installation of updates for Windows and other programs.			

Sort by Name, Status or Startup Type. Read the description, then double-click the service to open its properties. Record the original state before making any change.

UI WALKTHROUGH — 2 OF 2

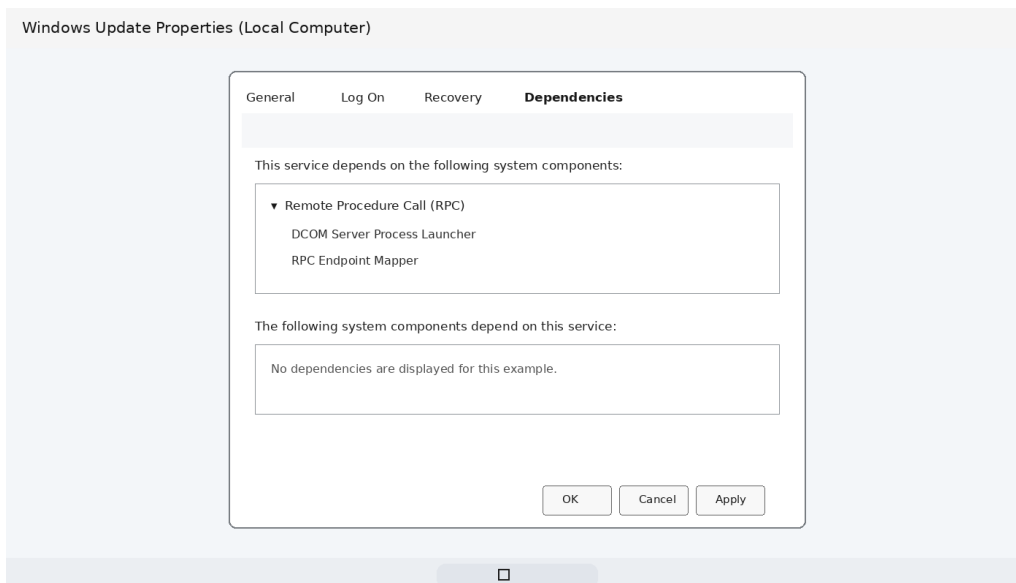
Reconfigure and verify

3. Review the current configuration



On the General tab, record the service name, executable path, startup type and status. For a candidate service, stop it first and complete the agreed observation period before setting Startup type to Disabled. Select Apply only within an approved change.

4. Check dependencies before changing anything



Use the Dependencies tab to identify components the service needs and components that rely on it. The view is useful but not exhaustive: applications can depend on a service without declaring a formal Service Control Manager dependency.

08 — HOW TO READ THE TABLES

Windows 10 and 11 baseline

The following tables deliberately separate core services from role-dependent and optional services. They do not prescribe a universal startup type because Windows uses automatic, delayed, manual, trigger-started and per-user patterns that vary by release and installed features.

Baseline rule

For RETAIN and DEFAULT / TEST rows, preserve the Windows or Microsoft baseline setting. For RETAIN IF REQUIRED and CANDIDATE rows, document the role decision. Any service not listed is INVESTIGATE—not automatically disable.

Minimum acceptance tests

- Cold boot and restart complete without material errors.
- Interactive and remote sign-in work as designed.
- DNS, DHCP, wired/Wi-Fi, VPN and 802.1X work where required.
- Windows Update, Microsoft Defender and endpoint management remain healthy.
- BitLocker, Windows Hello, printing, Bluetooth and smart card work where in scope.
- Business applications, backup, monitoring and remote support remain operational.
- Event collection and SecureX7 verification provide evidence of the final state.

Core services - retain (1 of 2)

Display name	Service	Applies to	Baseline decision	Operational note
Base Filtering Engine	BFE	All versions	RETAIN	Required for firewall and IPsec policy processing.
COM+ Event System	EventSystem	All versions	RETAIN	Supports system event notification and dependent components.
CoreMessaging	CoreMessagingRegistrar	All versions	RETAIN	Core communication between Windows components.
Cryptographic Services	CryptSvc	All versions	RETAIN	Signatures, catalog database and trusted root processing.
DCOM Server Process Launcher	DcomLaunch	All versions	RETAIN	Core COM/DCOM activation; disabling destabilises Windows.
DHCP Client	Dhcp	All versions	RETAIN	Addressing and DNS registration in typical managed networks.
DNS Client	Dnscache	All versions	RETAIN	Name resolution cache and computer-name registration.
Group Policy Client	gpsvc	All versions	RETAIN	Applies computer and user policy.
Local Session Manager	LSM	All versions	RETAIN	Core local user-session management.
Network Location Awareness	NlaSvc	All versions	RETAIN	Network identity and change notification.
Network Store Interface	nsi	All versions	RETAIN	Core network notifications for user-mode clients.
Plug and Play	PlugPlay	All versions	RETAIN	Hardware recognition and device lifecycle.
Power	Power	All versions	RETAIN	Power policy and notifications.

Core services - retain (2 of 2)

Display name	Service	Applies to	Baseline decision	Operational note
Remote Procedure Call	RpcSs	All versions	RETAIN	Fundamental Windows inter-process communication.
RPC Endpoint Mapper	RpcEptMapper	All versions	RETAIN	Maps RPC interfaces to endpoints.
Security Accounts Manager	SamSs	All versions	RETAIN	Local account and security database.
System Event Notification	SENS	All versions	RETAIN	Publishes system events to subscribing components.
Task Scheduler	Schedule	All versions	RETAIN	Runs Windows and enterprise maintenance tasks.
User Manager	UserManager	All versions	RETAIN	Multi-user interaction and app operation.
Windows Defender Firewall	mpssvc	All versions	RETAIN	Host firewall control; do not disable.
Windows Event Log	EventLog	All versions	RETAIN	Security, audit and operational event recording.
Windows Management Instrumentation	Winmgmt	All versions	RETAIN	Management and inventory dependencies.
Windows Update	wuauerv	All versions	RETAIN	Update detection and installation; may be trigger-started.
Windows Modules Installer	TrustedInstaller	All versions	RETAIN	Required for Windows updates and optional component servicing.
Windows Security Service	SecurityHealthService	All versions	RETAIN	Provides unified device protection and health information.
Windows Update Medic Service	WaaSMedicSvc	All versions	RETAIN	Repairs and protects Windows Update components.

Role-dependent services (1 of 3)

Display name	Service	Applies to	Baseline decision	Operational note
App Readiness	AppReadiness	All versions	RETAIN IF REQUIRED	Needed when preparing Store apps at first sign-in or app addition.
Application Identity	AppIDSvc	All versions	RETAIN IF REQUIRED	Required to enforce AppLocker policies.
Background Intelligent Transfer	BITS	All versions	RETAIN IF REQUIRED	Used by Windows Update and many management agents.
BitLocker Drive Encryption	BDESVC	All versions	RETAIN IF REQUIRED	Supports BitLocker operations and status.
Bluetooth Support	bthserv	All versions	RETAIN IF REQUIRED	Keep where Bluetooth peripherals are approved.
Credential Manager	VaultSvc	All versions	RETAIN IF REQUIRED	Stores credentials for users and applications.
Device Association	DeviceAssociation Service	All versions	RETAIN IF REQUIRED	Pairs wired and wireless devices.
Encrypting File System	EFS	All versions	RETAIN IF REQUIRED	Keep only where EFS is part of the data protection design.
Extensible Authentication Protocol	EapHost	All versions	RETAIN IF REQUIRED	Required for 802.1X, VPN and some Wi-Fi authentication.
Function Discovery Provider Host	fdPHost	All versions	RETAIN IF REQUIRED	Network discovery of devices and resources.
Function Discovery Resource Publication	FDResPub	All versions	RETAIN IF REQUIRED	Publishes the computer and attached resources.

Role-dependent services (2 of 3)

Display name	Service	Applies to	Baseline decision	Operational note
IKE and AuthIP IPsec Keying Modules	IKEEXT	All versions	RETAIN IF REQUIRED	Required for IPsec and some VPN scenarios.
Microsoft Account Sign-in Assistant	wlidsvc	All versions	RETAIN IF REQUIRED	Required for Microsoft account sign-in scenarios.
Microsoft Defender Antivirus	WinDefend	All versions	RETAIN IF REQUIRED	Keep unless a supported security product owns the antivirus role.
Microsoft iSCSI Initiator	MSiSCSI	All versions	RETAIN IF REQUIRED	Required only for iSCSI storage.
Netlogon	Netlogon	All versions	RETAIN IF REQUIRED	Required for domain authentication and secure channel.
Remote Access Connection Manager	RasMan	All versions	RETAIN IF REQUIRED	Required for VPN and dial-up connections.
Remote Desktop Services	TermService	All versions	RETAIN IF REQUIRED	Keep only where approved remote desktop access is needed.
Smart Card	SCardSvr	All versions	RETAIN IF REQUIRED	Required for smart-card authentication.
Storage Service	StorSvc	All versions	RETAIN IF REQUIRED	Storage settings and notifications; test before changing.
SysMain	SysMain	All versions	DEFAULT / TEST	Performance optimisation; not normally a security hardening target.
Windows Search	WSearch	All versions	DEFAULT / TEST	Indexing service; disable only for a documented role or privacy need.

Role-dependent services (3 of 3)

Display name	Service	Applies to	Baseline decision	Operational note
Windows Time	W32Time	All versions	RETAIN IF REQUIRED	Accurate time is essential for logs and domain authentication.
WLAN AutoConfig	WlanSvc	All versions	RETAIN IF REQUIRED	Required on endpoints using Wi-Fi.
AppX Deployment Service	AppXSVC	All versions	RETAIN IF REQUIRED	Required for deployment and servicing of Microsoft Store applications.
Client License Service	ClipSVC	All versions	RETAIN IF REQUIRED	Supports Microsoft Store licensing and acquired applications.
Delivery Optimization	DoSvc	All versions	RETAIN IF REQUIRED	Supports controlled peer and cloud delivery of Microsoft content.
Microsoft Passport	NgcSvc	All versions	RETAIN IF REQUIRED	Supports Windows Hello and identity-provider key isolation.
Microsoft Passport Container	NgcCtnrSvc	All versions	RETAIN IF REQUIRED	Manages Windows Hello identity keys and TPM virtual smart cards.
Microsoft Store Install Service	InstallService	All versions	RETAIN IF REQUIRED	Required for Microsoft Store application installation.
Windows Remote Management	WinRM	All versions	RETAIN IF REQUIRED	Required for approved remote management and event collection.
Cloud Backup and Restore Service	CloudBackupRestoreSvc	Windows 11	RETAIN IF REQUIRED	Supports Windows Backup of settings and application state.

Candidate services - validate before disabling (1 of 3)

Display name	Service	Applies to	Baseline decision	Operational note
ActiveX Installer	AxInstSV	All versions	CANDIDATE	Disable if legacy ActiveX deployment is not used.
AllJoyn Router	AJRouter	All versions	CANDIDATE	Disable where no AllJoyn applications are approved.
Downloaded Maps Manager	MapsBroker	All versions	CANDIDATE	Disable if offline maps are not used.
Fax	Fax	All versions	CANDIDATE	Disable if fax devices and services are absent.
Geolocation Service	lfsvc	All versions	CANDIDATE	Disable if location-aware apps are prohibited or unnecessary.
Internet Connection Sharing	SharedAccess	All versions	CANDIDATE	Disable unless the endpoint is intentionally sharing connectivity.
Microsoft Windows SMS Router	SmsRouter	All versions	CANDIDATE	Disable on devices without SMS/mobile broadband use.
Net.Tcp Port Sharing	NetTcpPortSharing	All versions	CANDIDATE	Disable unless an approved application requires shared net.tcp ports.
Offline Files	CscService	All versions	CANDIDATE	Disable if enterprise Offline Files is not used.
Phone Service	PhoneSvc	All versions	CANDIDATE	Disable where telephony integrations are not used.
Print Spooler	Spooler	All versions	CANDIDATE	Disable on endpoints that never print; assess application dependencies.
Remote Desktop Configuration	SessionEnv	All versions	CANDIDATE	Disable with RDP services if remote desktop is prohibited.

Candidate services - validate before disabling (2 of 3)

Display name	Service	Applies to	Baseline decision	Operational note
Remote Desktop Services UserMode Port Redirector	UmRdpService	All versions	CANDIDATE	Disable when RDP redirection is unnecessary.
Remote Registry	RemoteRegistry	All versions	CANDIDATE	Keep disabled unless a controlled management dependency is documented.
Retail Demo	RetailDemo	All versions	CANDIDATE	Disable on enterprise endpoints.
Routing and Remote Access	RemoteAccess	All versions	CANDIDATE	Disable unless the device is an authorised router or VPN server.
Secondary Logon	seclogon	All versions	ASSESS CAREFULLY	Disabling affects Run as different user and some administration workflows.
Sensor Data Service	SensorDataService	All versions	CANDIDATE	Disable on hardware without an approved sensor scenario.
Sensor Monitoring Service	SensrSvc	All versions	CANDIDATE	Disable when sensor-based display or device behaviour is unused.
SNMP Trap	SNMPTRAP	All versions	CANDIDATE	Disable unless legacy SNMP trap reception is required.
Touch Keyboard and Handwriting Panel	TabletInputService	All versions	CANDIDATE	Disable only on non-touch devices with no handwriting requirement.
WalletService	WalletService	All versions	CANDIDATE	Disable where digital wallet functionality is not used.
Windows Biometric Service	WbioSrv	All versions	CANDIDATE	Retain for Windows Hello biometrics; otherwise a candidate.
Windows Insider Service	wisvc	All versions	CANDIDATE	Disable on production systems not enrolled in Insider builds.

Candidate services - validate before disabling (3 of 3)

Display name	Service	Applies to	Baseline decision	Operational note
Windows Media Player Network Sharing	WMPNetworkSvc	All versions	CANDIDATE	Disable when media-library sharing is not approved.
Xbox Accessory Management	XboxGipSvc	All versions	CANDIDATE	Disable where Xbox accessories are not business-required.
Xbox Live Auth Manager	XblAuthManager	All versions	CANDIDATE	Disable on managed enterprise endpoints without Xbox use.
Xbox Live Game Save	XblGameSave	All versions	CANDIDATE	Disable where Xbox gaming is not approved.
Xbox Live Networking	XboxNetApiSvc	All versions	CANDIDATE	Disable where Xbox networking is not approved.
Internet Explorer ETW Collector	IEEtwCollectorService	Windows 10	CANDIDATE	Legacy Internet Explorer diagnostic collection; absent from standard Windows 11 builds.
Peer Name Resolution Protocol	PNRPsvc	Windows 10	CANDIDATE	Legacy peer-to-peer name resolution; disable when no approved peer application requires it.
Peer Networking Identity Manager	p2pimsvc	Windows 10	CANDIDATE	Legacy peer identity service; validate dependencies before disabling.
PNRP Machine Name Publication	PNRPAutoReg	Windows 10	CANDIDATE	Publishes computer names through peer name resolution; rarely required on managed endpoints.
Windows Perception Service	spectrum	Windows 10	CANDIDATE	Supports legacy Windows Mixed Reality spatial perception scenarios.
Windows Perception Simulation	perceptionsimulation	Windows 10	CANDIDATE	Supports legacy Windows Mixed Reality simulation and virtual camera scenarios.

Per-user service templates

Display name	Service	Applies to	Baseline decision	Operational note
Agent Activation Runtime	AarSvc_*	All versions	DEFAULT / TEST	Conversational-agent activation; per-user instance.
Bluetooth User Support	BluetoothUserService_*	All versions	RETAIN IF REQUIRED	Supports Bluetooth features for each signed-in user.
OneCore Capture	CaptureService_*	All versions	RETAIN IF REQUIRED	Application screen-capture API support.
Clipboard User Service	cbdhsvc_*	All versions	RETAIN IF REQUIRED	Clipboard history and cross-device clipboard scenarios.
Cloud Backup and Restore	CloudBackupRestoreSvc_*	Windows 11	RETAIN IF REQUIRED	Cloud backup and restore of settings and application state.
Connected Devices Platform User	CDPUserService_*	All versions	RETAIN IF REQUIRED	Cross-device and connected-device experiences.
Contact Data	PimIndexMaintenanceSvc_*	All versions	RETAIN IF REQUIRED	Indexes contact data for user applications.
Game DVR and Broadcast User	BcastDVRUserService_*	All versions	CANDIDATE	Disable template where game recording is prohibited.
Messaging Service	MessagingService_*	All versions	CANDIDATE	Disable where SMS and related messaging are not used.
Sync Host	OneSyncSvc_*	All versions	RETAIN IF REQUIRED	Synchronises mail, contacts, calendar and user data.
User Data Access	UserDataSvc_*	All versions	RETAIN IF REQUIRED	Broker access to structured user data.
User Data Storage	UnistoreSvc_*	All versions	RETAIN IF REQUIRED	Stores structured user data for apps.
Windows Push Notifications User	WpnUserService_*	All versions	RETAIN IF REQUIRED	Push and local notification support.

The asterisk represents the locally unique suffix added to each user instance. Manage the underlying template and test the effect on dependent apps. Microsoft notes that some templates cannot be managed through ordinary security templates and may require Group Policy Preferences or a script.

11 — MAINTAIN THE BASELINE

References and limitations

- Microsoft Learn — Guidance on configuring system services (Windows 10 and 11 IoT Enterprise): classification model for Don't disable, OK to disable, already disabled and no guidance.
- Microsoft Learn — Per-user services in Windows: templates, LUID-suffixed instances, dependencies and supported management approaches.
- Microsoft Learn — Security Compliance Toolkit: versioned Windows 11 baselines, Policy Analyzer and LGPO tooling.
- Microsoft Learn — Windows security baselines: deployment through Group Policy, Configuration Manager or Intune.
- Microsoft PowerShell documentation — Get-Service, Stop-Service and Set-Service.
- NCBI Bookshelf — StatPearls: Appendicitis: approximately 300,000 appendicitis-related hospital visits annually in the United States.
- AHRQ/NCBI Bookshelf — Diagnosis of suspected acute appendicitis: over 250,000 appendectomies annually in the United States.
- National Hospital Discharge Survey analysis — Trends in appendicitis and appendectomy: approximately 280,000 appendectomies annually in the United States.
- SecureX7 — Asset Discovery & Estate Visibility; Security & Compliance Assessment; Risk Prioritisation; Automated Configuration Remediation; AI Security Assistant; Reporting & Assurance.

Limitations

Microsoft's detailed service-disablement table cited above covers Windows 10 and Windows 11 IoT Enterprise and fixed-function devices. This guide uses its decision model but does not present that table as a universal desktop prescription. 'All versions' means the service is ordinarily present in both Windows 10 22H2 and supported Windows 11 releases; it does not imply every edition or installation. Service availability and defaults vary by release, edition, installed capabilities, hardware and applications. Microsoft security baselines do not necessarily prescribe every service in this guide.

Review cadence

Review after each Windows feature release, material application change, management-agent change or security incident, and at least annually. The baseline owner should record the Windows build tested and the date of approval.

Prepared August 2026. Links: [Windows service guidance](#) · [Per-user services](#) · [Security Compliance Toolkit](#) · [SecureX7](#)

See your estate. Prioritise risk. Remediate with confidence.



SecureX7 brings asset visibility, configuration assessment, contextual risk prioritisation, clear remediation guidance and verification into one practical cybersecurity posture platform.

Turn a hardening document into an operating control

Use SecureX7 to associate the right Windows 10 or Windows 11 service baseline with the right endpoint role, identify deviations and demonstrate measurable improvement over time.

[Start a free trial](#) · [Request a demo](#) · [Contact SecureX7](#)



SEE YOUR ESTATE. PRIORITIZE RISK. ACT WITH CONFIDENCE.

SecureX7 is a natively built, AI-driven cyber security platform that helps organizations understand their environment, identify the risks that matter most, and take clear action to improve security and compliance.

FROM ASSESSMENT TO ACTION - WITHOUT COMPLEXITY

Discover assets • Assess posture • Prioritize exposure • Guide remediation

[START YOUR FREE TRIAL](#)[REQUEST A FREE DEMO](#)