NIST SP 800-171 Security Requirement Mapping

Windows Hardening Baseline

Mapping of the curated Windows configuration baseline to the security requirements of NIST SP 800-171, the requirements CMMC Level 2 assesses.

Project	briangeis/windows-hardening
Framework	NIST SP 800-171 Revision 2, with SP 800-171A
Derived From	NIST SP 800-53 Control Mapping: Windows Hardening Baseline
Baseline	Policy-Windows-Base.psd1 and Policy-Windows-NoStoreApps.psd1
Target	Windows 11 25H2, standalone and not joined to a domain
Settings	134 (112 base, 22 layer)
Author	Brian Geis, briangeis.com/samples
Version	1.0
Reviewed	2026-09-23

Contents

1. Executive Summary....3
2. Purpose, Scope, and Claims....4
    2.1 Purpose....4
    2.2 Scope....4
    2.3 Claims and Limitations....4
    2.4 Method....5
3. System Description....6
    3.1 Target System....6
    3.2 Enforcement Mechanism....6
    3.3 Artifact-Level Contributions....7
4. Requirement Mapping....8
    4.1 Access Control....9
    4.2 Configuration Management....10
    4.3 Identification and Authentication....12
    4.4 Media Protection....12
    4.5 System and Communications Protection....13

4.6 System and Information Integrity....14
5. Coverage Analysis....14
5.1 What Carried from SP 800-53....14
5.2 Channels That Can Carry CUI....15
5.3 Scoping Considerations....17
5.4 Requirements Not Addressed....17
6. Where the Baseline Works Against a Requirement....18
6.1 Defender Cloud Protection and Sample Submission....19
6.2 Find My Device....19
6.3 Cases Unchanged from SP 800-53....19
7. Settings the Baseline Declines....20
7.1 Windows Update....20
7.2 Time Synchronization and Trust Anchors....21
8. Notes for Assessors....21
9. Setting Index....22
10. Traceability....27
11. References....27
12. Revision History....28

1. Executive Summary

The curated Windows baseline applies 134 configuration settings to a standalone Windows device: 112 in the base profile and 22 in the optional No Store Apps layer. This document maps each to the security requirements of NIST SP 800-171 Revision 2, which CMMC Level 2 assesses. It is a companion to the baseline's NIST SP 800-53 control mapping, from which its assignments are derived, and it records what changes when the same configuration is read against 800-171. Five findings bear on how the result should be read.

Much of the baseline was chosen for privacy, and 800-171 has no privacy objective, yet those settings still count. 50 of the 134 settings rest in the SP 800-53 mapping on a control that NIST never carried into 800-171, and for 49 of them that control concerns privacy or retention. 800-171's assessment objectives do not ask why a function was disabled, only whether the organization has defined it as nonessential and whether its use is restricted. So 26 of those 50 are credited under nonessential functionality (3.4.7) exactly as the baseline's least-functionality settings are, and the rest find requirements of their own. Section 5.1 traces every setting.

34 settings close, narrow, or withhold a channel that can carry Controlled Unclassified Information (CUI), and 32 of them take effect on a current Windows 11 device. These are the settings whose value to a device processing CUI goes beyond the wording of a requirement. Section 5.2 lists them, so that each can be examined rather than a count taken on trust.

The settings reach 19 of the 53 assessment objectives in the requirements they are first assigned to, and the other 34 remain the organization's to supply. Most of those ask the organization to define, identify, or verify something, such as which functions are essential or where the system boundary lies, and a configuration can carry out those decisions but cannot make them. No requirement is MET on the strength of this baseline. Section 4 reports the split requirement by requirement.

Enforcement differs by Windows edition, and 3.4.2 makes enforcement an assessment objective. On Pro and higher, 123 of the 134 settings are written to Local Group Policy and re-applied at every policy refresh. On Home, and for 11 settings outside the policy branches on any edition, nothing re-asserts them after they are applied. Section 3.2 sets out the difference.

Six settings work against a requirement, and 28 catalog settings are declined. The costs fall on 3.14.1, 3.14.2, and 3.14.6. Three verdicts differ from the SP 800-53 mapping: Defender cloud protection becomes the organization's decision while sample submission stays disabled, Find My

Device becomes the organization's decision, and the tension in declining automatic updates moves from flaw remediation into change control. Section 6 and Section 7 record each with a verdict.

Taken together, the baseline is a device-layer contribution to a CMMC program rather than a substitute for one. It carries out least-functionality and external-connection decisions that the organization still has to adopt as its own, and records where the device's part ends.

2. Purpose, Scope, and Claims

2.1 Purpose

This document maps each setting in the curated Windows configuration baseline to the NIST SP 800-171 security requirements it advances, so that an organization seeking assessment, or an assessor, can see which requirements and assessment objectives the baseline supports, which remain the organization's, and which the baseline affects adversely.

The baseline's NIST SP 800-53 control mapping maps the same settings to SP 800-53 Revision 5 and is the fuller treatment of what each setting does. This document is its companion, organized by requirement as an assessment against 800-171 is, and covers what 800-171 changes. Where the reasoning is the same, it cites that mapping rather than repeating it.

2.2 Scope

In scope are the 134 settings carried by the two curated profiles: 112 in the base and 22 in the No Store Apps layer. Only the profiles are mapped, because nothing in a definitions file is applied until a profile applies it.

Four things are out of scope. The settings cataloged in the definitions files but not curated into either profile appear in Section 7 as declined rather than as coverage. The Microsoft Edge target is hardened separately. Windows services and preinstalled package removal are the concern of other components. And any requirement or assessment objective met by organizational policy, procedure, or practice rather than device configuration falls outside what this document can address at all.

2.3 Claims and Limitations

This document asserts that applying a given setting advances the stated requirement on the target device, identifies the assessment objective it reaches, and identifies where a setting advances only part of a requirement or advances it incidentally.

It does not assert that the baseline satisfies any requirement, that a device applying it complies with 800-171 or is ready for a CMMC assessment, or that this mapping is an assessment. It issues no findings and records no requirement as MET or NOT MET, which under CMMC requires all applicable assessment objectives to be satisfied based on evidence.

The verb throughout is **supports**. A configuration setting contributes to a requirement and does not satisfy one. The word *satisfies* appears in this document only in explicit negation or in quoting NIST's and CMMC's own definitions.

2.4 Method

Framework. The requirements are those of NIST SP 800-171 Revision 2 and the assessment objectives those of NIST SP 800-171A, taken from NIST's machine-readable files. NIST has withdrawn both in favor of their third revisions, and 32 CFR 170 still incorporates both by reference, so they remain the edition CMMC Level 2 assesses.

Identifiers. Requirements are cited by their 800-171 identifiers and objectives by letter, as in 3.4.7[f]. CMMC cites the same requirement as CM.L2-3.4.7, and the titles used here are the CMMC Assessment Guide's.

Derivation. Each setting starts from its SP 800-53 assignment. Where NIST carried that control into 800-171, the setting takes a requirement 800-171 maps it to. Where NIST did not, the setting is read against the requirements directly, by what it does, and assigned where an assessor would look for it. Section 5.1 sets out both.

Relationship. This is a **supportive relationship mapping** in the sense of NIST IR 8278A Rev. 1: it records how a supporting concept, a configuration setting, helps achieve a supported concept, a requirement. The set-theory relationships of the OLIR program do not apply, because a registry setting is not a subset, superset, or equivalent of a requirement. The strength scale is the SP 800-53 mapping's:

Relationship	Meaning
Supports	Advances the requirement directly and materially
Partially supports	Advances one element of a multi-element requirement
Incidental	Advances the requirement as a side effect of a different primary purpose

Responsibility. 800-171 publishes no designation of which requirements an organization implements and which a system implements, so the split is read from the 800-171A assessment objectives. An objective that something is defined, identified, or verified asks the organization for a

decision, and one that use is restricted, controlled, or enforced asks for a mechanism. That classification is this document's reading of NIST's wording.

The mapping follows the six mapping principles in the compliance mappings overview. An assignment would be invalidated by a change in a setting's behavior in a later Windows feature update, or by DoD adopting a later revision of 800-171 for CMMC.

3. System Description

3.1 Target System

The baseline targets a standalone device: locally administered, not joined to an Active Directory domain, and receiving no centrally managed policy. A standalone device inherits nothing, so every requirement is met on the device or not at all.

Under CMMC, a device that processes, stores, or transmits CUI is a CUI Asset, documented in the asset inventory and the system security plan and assessed against all Level 2 security requirements. This document places the device in no assessment scope, which is the organization's decision. It is written for the case in which the device is a CUI Asset.

An organization seeking assessment typically manages its devices through a domain or a cloud management service, and domain policy supersedes Local Group Policy. For such a device the settings transfer, since each carries its registry value and, where one exists, its Group Policy path in the definitions files. The enforcement analysis below does not transfer, because enforcement and its evidence then belong to the managing service. `Disable MDM Enrollment` should be excluded from a device the organization intends to manage.

3.2 Enforcement Mechanism

3.4.2 requires that security configuration settings be established, [a], and enforced, [b]. The first is what a curated profile is. The second depends on the Windows edition.

On Home edition, where Local Group Policy is unavailable, the toolkit writes registry values directly. On Pro, Enterprise, Education, and LTSC editions it writes through `LGPO.exe` into Local Group Policy, and the Group Policy engine re-applies the settings at every policy refresh, by default at startup and roughly every 90 minutes, restoring any value a local administrator changes manually.

Registry location	Settings	Behavior after application
Under a `\Policies\` key	123	Managed by Group Policy and re-applied at every refresh on non-Home editions
Outside the `\Policies\` keys	11	Written once and not re-asserted on any edition

For 3.4.2[b], the 123 policy-managed settings on non-Home editions are enforced. On Home, and for the 11 exceptions everywhere, a setting is applied and not enforced: any local administrator can change it and nothing restores it. The 11 are listed in Section 3.3 of the SP 800-53 mapping. Domain policy supersedes Local Group Policy, so this holds for the standalone case and not for a device later joined to a domain.

3.3 Artifact-Level Contributions

Some requirements are supported by the toolkit's artifacts rather than by any individual setting. These are reported separately and are **not** counted among the 134 setting assignments.

Requirement	Artifact and contribution
3.4.1 System Baselining	The curated profile is a documented, version-controlled baseline configuration for the device's security settings. Supports 3.4.1[a], and [c] in part. The profile covers software configuration only, not the hardware, firmware, and documentation 3.4.1[b] names, and the inventory objectives, [d] through [f], are not addressed
3.4.2 Security Configuration Enforcement	All 134 settings are established in the profile, which supports 3.4.2[a]. Enforcement, [b], depends on the edition, as Section 3.2 sets out
3.4.3 System Change Management	Snapshot comparison provides the record against which configuration change can be identified. Incidental to 3.4.3[a], and detection is manual
3.4.6 Least Functionality	The baseline as a whole configures the device to provide a reduced set of capabilities. Supports 3.4.6[b] against the essential capabilities the organization defines under 3.4.6[a]

Two artifact-level contributions in the SP 800-53 mapping do not carry. Retaining the prior configuration, which Snapshot Mode does, supports CM-2(3), which NIST did not carry into 800-171. And the 28 documented deviations from the catalog support CM-6c, which has no counterpart objective in 3.4.2.

4. Requirement Mapping

The requirements the settings support, in 800-171 order. `First` counts settings assigned to a requirement first, and `All` adds settings that support it as a second requirement. `Reached` gives the assessment objectives the settings reach, out of the total in `Of`. Every setting's assignment is in Section 9.

Requirement	Title	First	All	Reached	Of
3.1.1	Authorized Access Control	0	1	-	-
3.1.2	Transaction & Function Control	10	10	[b]	2
3.1.10	Session Lock	2	3	[b], [c]	3
3.1.20	External Connections	17	22	[e], [f]	6
3.4.2	Security Configuration Enforcement	4	6	[a], [b]	2
3.4.3	System Change Management	3	3	[c]	4
3.4.7	Nonessential Functionality	64	74	[c], [f], [l], [o]	15
3.4.8	Application Execution Policy	0	1	-	-
3.4.9	User-Installed Software	1	1	[b]	3
3.5.2	Authentication	2	2	[a]	3
3.8.7	Removable Media	3	3	In part	1
3.13.1	Boundary Protection	21	24	[e]	8
3.13.7	Split Tunneling	0	1	-	-
3.13.12	Collaborative Device Control	3	4	[c]	3
3.13.13	Mobile Code	1	1	[a]	2
3.13.16	Data at Rest	3	9	In part	1
3.14.2	Malicious Code Protection	0	3	-	-
Total		134	168	19	53

Of the 34 objectives not reached, 20 ask the organization to define, identify, or verify something. Three ask for change-control process: tracking, reviewing, and logging changes. The other 11 ask for mechanisms the baseline does not configure, such as monitoring at the boundary, port restrictions, and an indication that a camera is in use. Under CMMC every applicable objective must be satisfied for a requirement to be MET, so a requirement the baseline reaches at one objective of eight, as it does 3.13.1, is a long way from MET on the baseline's strength.

4.1 Access Control

3.1.1 Authorized Access Control

No first assignments, 1 citation. Basic requirement.

`Disable MDM Enrollment` partially supports limiting system access to authorized devices and systems, [f], by closing an enrollment path through which an external management service could take control of the device.

3.1.2 Transaction & Function Control

10 settings. Basic requirement.

Ten settings deny UWP applications access to another application's data: account information, contacts, calendar, email, messages, phone calls, call history, tasks, notifications, and diagnostic information about other applications. They limit the functions a process acting on a user's behalf can perform, [b], against the functions the organization defines under [a]. All ten apply to UWP applications only, and Win32 applications are outside their reach.

3.1.10 Session Lock

2 settings and 3 citations. Derived requirement.

`Disable Lock Screen App Notifications` supports concealing information behind the pattern-hiding display, [c]. The objective's wording concerns previously visible information, which a notification arriving after the lock is not, and the SP 800-53 mapping held the setting at a partial relationship for that reason. 3.1.10's discussion adds the caveat that "none of the images convey controlled unclassified information", and notification content on a locked display, a sender, a subject line, the opening of a message, is what that caveat excludes, so the fit holds here where it did not there. `Deny Voice Activation Above Lock` supports [b] by preventing microphone interaction with a locked device, and `Disable Automatic Sign-In After Restart` partially supports it. The inactivity period, [a], is the organization's to set, and the baseline configures no lock timeout.

3.1.20 External Connections

17 settings and 22 citations. Derived requirement.

3.1.20's discussion reaches this baseline directly: the requirement "addresses the use of external systems for the processing, storage, or transmission of CUI, including accessing cloud services." Every Microsoft service a Windows component reaches out to is an external system in that sense.

The settings control or limit connections to them, [e], and their use, [f]: OneDrive file storage, cloud clipboard, settings synchronization, cross-device experiences, Phone Link, online speech recognition, inking and typing data, optional diagnostic data, Windows Error Reporting, and Defender sample submission. Identifying and verifying external connections and uses, [a] through [d], is the organization's.

Where Windows asks the user before sending content, as Defender does before sending a file likely to contain personal data, the prompt hands a decision 3.1.20 gives the organization to whoever is at the keyboard. Closing the channel returns it to the organization as a mechanism an assessor can examine.

Settings the SP 800-53 mapping assigns to boundary protection, such as web search, keep that assignment under 3.13.1 and carry 3.1.20 as a second requirement where the channel carries content.

4.2 Configuration Management

3.4.2 Security Configuration Enforcement

4 settings and 6 citations. Basic requirement.

`Disable Settings Sync User Override`, `Lock IE Home Page Setting`, and `Disable Compatibility View Editing` prevent a user overriding an applied setting, which supports [b]. `Set IE Home Page to Blank` establishes one, [a]. Three of the four do not take effect on Windows 11, where the setting-level contribution reduces to `Disable Settings Sync User Override`. The larger contribution is the profile itself and its enforcement, in Section 3.

3.4.3 System Change Management

3 settings. Derived requirement.

`Disable Services Configuration` prevents Microsoft pushing configuration changes to Windows components without review, which supports approval of change, [c]. `Disable Insider Preview Builds` keeps the device off a pre-release channel, and `Disable Auto Download and Install of Updates`, in the layer, makes Store application updates administrator-initiated. Tracking, reviewing, and logging changes, [a], [b], and [d], are the organization's process.

3.4.7 Nonessential Functionality

64 settings and 74 citations, the largest grouping in the baseline. Derived requirement.

3.4.7 has 15 assessment objectives, three for each of programs, functions, ports, protocols, and services: that the essential ones are defined, that the use of the rest is defined, and that the use of the rest is restricted as defined. The settings reach four of the third kind. They restrict programs, [c], through `Disable All Store Apps`, functions, [f], through most of the baseline, a protocol, [l], through `Disable Multicast Name Resolution`, and services, [o], through the location and license manager services. They reach no port objective, since the baseline configures no firewall, and none of the ten definitions.

Those definitions are the organization's, and the baseline proposes values for them: that a standalone device does not need Microsoft consumer content, AI assistants, cross-device linking, or diagnostic reporting beyond the minimum. An organization whose users depend on Phone Link or Copilot will define those as essential, and the layered profile design exists for that case.

The SP 800-53 mapping assigns 26 of these settings first to privacy and retention controls that 800-171 does not carry. 3.4.7 credits them as fully as the rest, since its assessment objectives ask whether a function is nonessential, not why it was disabled, so under 800-171 a privacy setting and a least-functionality setting look the same. Its discussion does expect the organization's decision on what is restricted to be "security-based", and that basis is the organization's to state when it adopts the definitions. What sets some apart for a device processing CUI is whether they close a channel that can carry it, in Section 5.2.

800-171's own discussion names three behaviors the baseline disables: auto-execute, stopped by `Disable AutoRun Command Execution`, peer-to-peer networking, stopped by `Disable Peer-to-Peer Update Sharing`, and tunneling, named in 3.4.6's discussion and stopped by `Disable Teredo`.

3.4.8 Application Execution Policy

No first assignments, 1 citation. Derived requirement.

`Disable All Store Apps`, in the layer, denies one class of software, which partially supports implementing a deny-by-exception policy, [c]. The baseline implements no allowlisting, and the choice of policy, [a], and the software it names, [b], are the organization's.

3.4.9 User-Installed Software

1 setting. Derived requirement.

`Disable Push To Install Service` closes a channel through which applications can be installed on the device remotely and silently, which supports controlling installation, [b]. The installation policy, [a], and monitoring, [c], are the organization's, and the baseline does not configure account rights.

4.3 Identification and Authentication

3.5.2 Authentication

2 settings. Basic requirement.

`Disable Local Account Security Questions` supports authenticating users before access, [a], by removing a recovery mechanism weaker than the password it recovers. `Disable Automatic Sign-In After Restart` partially supports it by preventing Windows signing the user back in with stored credentials after an update restart. Its SP 800-53 control, re-authentication, was in none of the baselines 800-171 derives from, so it is read against 3.5.2 directly. The baseline configures no password policy, lockout threshold, or multifactor authentication, which are 3.5.7, 3.1.8, and 3.5.3.

4.4 Media Protection

3.8.7 Removable Media

3 settings. Derived requirement.

`Disable AutoPlay`, `Disallow AutoPlay for Non-Volume Devices`, and `Disable AutoRun Command Execution` act together, and any subset leaves a gap, as the SP 800-53 mapping sets out. An assessor should confirm all three. They control what happens automatically once media is connected, not whether media can be connected, so they support the requirement's single objective in part. Each also partially supports 3.14.2.

4.5 System and Communications Protection

3.13.1 Boundary Protection

21 settings and 24 citations. Basic requirement.

Most of these settings close outbound connections initiated by Windows components: web results and cloud search, media and device metadata retrieval, font streaming, map data, push notifications, and DRM license acquisition. They control communications at the device's external boundary, [e], by reducing its unsolicited outbound destinations. They neither monitor nor protect communications and are no substitute for firewall policy, which the baseline does not configure. Defining the boundary, [a] and [b], is the organization's. `Disable Teredo` is the cleanest assignment: Teredo tunnels IPv6 through an IPv4 NAT, a boundary traversal a host firewall does not necessarily observe.

3.13.7 Split Tunneling

No first assignments, 1 citation. Derived requirement.

`Disable Smart Multi-Homed Name Resolution` stops Windows sending DNS queries over every active interface at once, which can leak them outside a VPN tunnel. It partially supports preventing split tunneling, for name resolution only.

3.13.12 Collaborative Device Control

3 settings and 4 citations. Derived requirement.

`Deny App Access to Camera`, `Deny App Access to Microphone`, and `Deny Voice Activation` partially support prohibiting remote activation, [c], since each applies to UWP applications only. `Deny Voice Activation Above Lock` adds a fourth citation. The indication that a device is in use, [b], is Windows' own, and the baseline neither establishes nor verifies it. Under 800-171 these settings protect CUI directly: a conversation or a whiteboard in view of an active camera is content.

3.13.13 Mobile Code

1 setting. Derived requirement.

`Disable ActiveX VersionList Download` supports controlling mobile code, [a], for ActiveX, which runs on Windows 11 only within Edge's IE mode. Where IE mode is not configured, the contribution is absent, as Section 5.3 notes.

3.13.16 Data at Rest

3 settings and 9 citations. Derived requirement.

`Limit Dump Collection`, `Disable Indexing of Encrypted Files`, and `Disable Fast Startup` reduce what is written to disk in the clear. Six more settings, among them clipboard history, Recall, and the search histories, are incidental: disabling them removes places where copies of CUI would otherwise accumulate, and protects none of what remains. The baseline configures no encryption, and it declines `Disable Hibernation`, so the hibernation write path stays open. An organization relying on this baseline for the confidentiality of memory images at rest without full-disk encryption relies on something it does not provide.

4.6 System and Information Integrity

3.14.2 Malicious Code Protection

No first assignments, 3 citations. Basic requirement.

The three AutoPlay and AutoRun settings partially support it by closing automatic execution from media. Four settings work against it, as Section 6 records.

5. Coverage Analysis

5.1 What Carried from SP 800-53

800-171 derives from the SP 800-53 Revision 4 moderate baseline. Appendix E of 800-171 Revision 2 records NIST's tailoring action for each control in it: `CUI` for a control reflected in a requirement, `NCO` for one not directly related to protecting the confidentiality of CUI, `FED` for one uniquely federal, and `NFO` for one expected to be routinely satisfied without specification. Appendix D maps each requirement to the controls it derives from. A control absent from Appendix E was not in the moderate baseline at all.

SP 800-53 control	Appendix E	Settings	Carried	Promoted	Re-read
PT-3	absent	38	0	14	24
CM-7	CUI	38	38	0	0
SC-7	CUI	19	19	0	0
SI-12	FED	10	0	0	10
AC-20	CUI	8	8	0	0
CM-6	CUI	4	4	0	0
CM-3, MP-7, SC-28	CUI	9	9	0	0
AC-3, AC-11, AC-11(1), CM-11, IA-5, SC-18	CUI	6	6	0	0
IA-11, SI-19	absent	2	0	0	2
Total		134	84	14	36

`Settings` counts settings by their first SP 800-53 control. A setting is **carried** when that control is marked `CUI`, and takes the requirement Appendix D maps it to. It is **promoted** when its first control did not carry and its second did. It is **re-read** otherwise, and is assigned by what it does: 25 disable a function and take 3.4.7, 6 stop content leaving the device and take 3.1.20, 2 limit application access and take 3.1.2, 2 trim what is sent and take 3.1.20 at a reduced relationship, and 1 is an authentication setting whose control was never baselined. With `Disable Application Telemetry`, promoted through its CM-7 second, 26 of the 50 reach 3.4.7.

PT-3 and SI-19 are privacy controls new in SP 800-53 Revision 5, IA-11 was in no Revision 4 baseline, and SI-12 is marked `FED`.

5.2 Channels That Can Carry CUI

The settings below close, narrow, or withhold a channel that carries content, meaning material whose substance a user created or received: files, memory images, typed, spoken, or inked text, captured screens, audio, and video, copied items, messages, calendar and task entries, notifications, and search queries. On a device that processes CUI, any such channel can carry CUI. Channels carrying only identifiers, configuration, usage data, locations, file paths, or records about people are not listed, however sensitive that data is as personal information.

Microsoft's documentation, listed in Section 11, settled the cases that were not obvious. Optional diagnostic data can include the memory state of the device at a crash, which may contain parts of a file that was open. Defender cloud protection sends file metadata with filenames hashed, while sample submission sends the files themselves.

Setting	Channel	Content
`Set Diagnostic Data to Minimum`	Optional diagnostic data: memory state, browsing history, search terms	Leaving
`Disable Sample Submission`	Files sent for cloud analysis	Leaving
`Disable Windows Error Reporting`	Crash reports and dumps	Leaving
`Disable Inking and Typing Data Collection`	Inking and typing samples	Leaving
`Disable Online Speech Recognition`	Voice	Leaving
`Disable Enhanced Suggestions*`	Address bar keystrokes	Leaving
`Disable Web Search`	Search queries	Leaving
`Disable Web Results in Search`	Search queries	Leaving
`Disable Cloud Search`	Search queries against cloud content	Leaving
`Disable OneDrive File Storage`	Files	Leaving
`Disable Cloud Clipboard`	Copied items	Leaving
`Disable Cross-Device Experiences`	Files through Nearby Sharing, app state	Leaving
`Disable Phone-PC Linking`	Messages, photos, and notifications between phone and device	Leaving
`Restrict Implicit Text Collection`	Typed text in a personalization store	Retained
`Restrict Implicit Ink Collection`	Ink in a personalization store	Retained
`Disable File Explorer Search History`	Typed queries	Retained
`Disable Search History`	Typed queries	Retained
`Disable Clipboard History`	Copied items	Retained
`Disable Recall*`	Screen snapshots	Retained
`Disable Game Recording and Broadcasting`	Screen recordings	Retained
`Limit Dump Collection`	Memory images, narrowed to triage dumps	Retained
`Disable Fast Startup`	Kernel session image written at shutdown	Retained
`Disable Indexing of Encrypted Files`	Decrypted file content in the search index	Retained
`Deny App Access to Camera`	Video	Exposed
`Deny App Access to Microphone`	Audio	Exposed
`Deny Voice Activation`	Audio, continuously	Exposed
`Deny Voice Activation Above Lock`	Audio on a locked device	Exposed
`Deny App Access to Email`	Message bodies	Exposed
`Deny App Access to Messaging`	Message bodies	Exposed

Setting	Channel	Content
`Deny App Access to Calendar`	Calendar entries	Exposed
`Deny App Access to Tasks`	Task entries	Exposed
`Deny App Access to Notifications`	Notification text	Exposed
`Disable Lock Screen App Notifications`	Notification text on a locked display	Exposed
`Disable Click to Do`	Screen content passed to AI actions	Exposed

`Leaving` is content sent to a Microsoft service or another device. `Retained` is content kept or written on the device beyond what the user asked for. `Exposed` is content made available to applications or to anyone near the device.

34 settings, 26 in the base and 8 in the layer. Two are subject to a scoping consideration, so 32 take effect on a current Windows 11 device. File paths in document history are left off, though on a device where a file name can itself reveal what a CUI document concerns, `Disable Recently Opened Document History` belongs on the list.

5.3 Scoping Considerations

21 of the 112 base settings do not take effect on a standard, retail-licensed Windows 11 25H2 device. They are the same settings under the same conditions as in the SP 800-53 mapping, whose Section 6.2 enumerates them, and they are marked with an asterisk in Section 9. Coverage should be read against the settings effective on the configuration being assessed, not against the count applied.

Requirement	Applied	Conditional	Unconditional on target
3.4.7	64	10	54
3.13.1	21	5	16
3.1.20	17	2	15
3.4.2	4	3	1
3.13.13	1	1	0

3.13.13 is the sharpest case. Its single assignment is effective only where Edge's IE mode is configured, and an assessor crediting it should confirm that IE mode is present.

5.4 Requirements Not Addressed

The settings support 17 of the 110 requirements, in 6 of the 14 families, and the artifacts add 3.4.1 and 3.4.6.

Family	Requirements	Supported by the settings
Access Control	22	4
Awareness and Training	3	0
Audit and Accountability	9	0
Configuration Management	9	5
Identification and Authentication	11	1
Incident Response	3	0
Maintenance	6	0
Media Protection	9	1
Personnel Security	2	0
Physical Protection	6	0
Risk Assessment	3	0
Security Assessment	4	0
System and Communications Protection	16	5
System and Information Integrity	7	1
Total	110	17

The baseline does not address, and should not be credited toward, **3.13.11, FIPS-validated cryptography**, since it configures no cryptography. Nor does it address 3.5.3, multifactor authentication, 3.3.1 and 3.3.2, audit logging and accountability, 3.1.5, least privilege, 3.13.6, deny network traffic by default, or 3.14.6, system monitoring. Of the eight families with no supported requirement, Audit and Accountability turns on audit logging the baseline does not configure, and the other seven are programs of people and process that no device configuration reaches.

6. Where the Baseline Works Against a Requirement

Nine settings carry a cost alongside their benefit. Six fall on a requirement: 3.14.1, 3.14.2, or 3.14.6. Three fall on a capability no requirement covers: `Disable Find My Device`, `Disable Windows Error Reporting`, and `Disable Disk Health Model Updates`. The two cases whose reading changes under 800-171 are treated below, and the rest in Section 6.3. All are deliberate, and all should reach a system owner before the baseline is applied.

6.1 Defender Cloud Protection and Sample Submission

`Disable MAPS Reporting` turns off Defender cloud protection, and `Disable Sample Submission` stops Defender sending files to Microsoft for analysis. Both work against 3.14.2: cloud protection responds fastest to threats no signature covers yet, and block at first sight, which holds a new file until the cloud returns a verdict, depends on samples.

The two settings are separable. Cloud protection sends metadata in which filenames are hashed, and requests a file sample only when metadata cannot settle a verdict. With sample submission set to never send, no file leaves the device whether cloud protection is on or off, and metadata verdicts keep working while it is on. The protection that matters for CUI sits in sample submission.

Verdict: sample submission stays disabled, and cloud protection is the organization's decision. A file that may contain CUI does not leave the device, and the loss of block at first sight is the price. The baseline also disables cloud protection, for a reason its profile reference records: file hashes reveal which known files a device holds. 800-171 has no requirement that weighs that reason. An organization that relies on cloud-assisted detection can exclude `Disable MAPS Reporting` alone and keep every CUI protection the baseline provides.

6.2 Find My Device

`Disable Find My Device` disables a function, which supports 3.4.7[f], at the cost of device recovery after loss or theft. In the SP 800-53 mapping the gain was closing a continuous, high-sensitivity location stream, and neither of the controls it rested on reaches 800-171.

Verdict: under 800-171 this is a least-functionality decision the organization owns. Whether device recovery is essential is the organization's definition to make under 3.4.7[e]. The baseline makes it for a device with no recovery need, and an organization with portable devices processing CUI should make it deliberately rather than inherit it.

6.3 Cases Unchanged from SP 800-53

The SP 800-53 mapping's verdicts stand for the rest. The base keeps system-wide SmartScreen and drops the narrow filters for Store app content and Internet Explorer, `Disable SmartScreen for Store Apps` and `Disable IE SmartScreen`, which work against 3.14.2. `Disable Auto Download and Install of Updates` works against 3.14.1 and costs nothing in context, since the same layer disables Store applications entirely. `Disable Enhanced Notifications` reduces Defender alerting to the user, a small 3.14.6 cost. Disabling Windows Error Reporting forgoes Microsoft's analysis of

crash reports, and disabling disk health model updates forgoes failure prediction, capabilities no requirement covers.

7. Settings the Baseline Declines

The definitions files catalog 162 settings, and the curated profiles carry 134. The 28 the baseline declines are as much a part of its design as the 134 it applies, and each is declined to protect a requirement or because it falls outside this target's scope.

Declined setting or group	Count	Objective protected	Requirement
Windows Update settings	8	The device continues to receive and install security updates without administrative action	3.14.1
Microsoft Edge and Edge Update	14	Not a protection. Scope boundary, deferred to the Edge target	None
Set Time Sync to NoSync, Disable NTP Client	2	Internal clocks stay synchronized with an authoritative source, on which audit timestamps and certificate validity both depend	3.3.7, 3.13.15
Disable Automatic Root Certificate Updates	1	Certificate path validation continues to work as trust anchors change	3.13.15
Disable SmartScreen (system-wide)	1	Broad malware and phishing protection for files and applications	3.14.2
Disable NCSI Active Tests	1	Connectivity detection that applications and services depend on	Availability
Disable Hibernation	1	Hibernation remains available. The data-at-rest gain applies only to an unencrypted disk	Functionality

7.1 Windows Update

The SP 800-53 mapping treats the decline of automatic updates as a trade inside a single control, because SP 800-53 asks both for testing updates before installation and for installing them within a defined period. 800-171 separates the two. 3.14.1's six assessment objectives ask that time frames to identify, report, and correct flaws be specified, [a], [c], and [e], and that flaws be identified, reported, and corrected within them, [b], [d], and [f]. None concerns testing. Testing sits in 3.4.3, whose discussion names the testing of changes and changes to remediate vulnerabilities, and whose objective [c] asks that changes be approved or disapproved. The trade is between two requirements rather than inside one, and the organization reconciles them by approving automatic security updates in advance, as a class of change.

On an unattended standalone device, automatic installation is what keeps 3.14.1[f] from depending on an operator who may not exist. Four of the eight declined settings would also blank or redirect the update source.

Verdict: security patching is not traded away. The decline costs 3.4.3 nothing once the organization approves automatic security updates as a class, and specifying the time frames remains the organization's.

7.2 Time Synchronization and Trust Anchors

`Set Time Sync to NoSync` and `Disable NTP Client` would stop the device synchronizing its clock, which 3.3.7[c] requires: "internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source." Clock drift also breaks TLS certificate validation, because validity windows are evaluated against local time.

`Disable Automatic Root Certificate Updates` would stop the device acquiring new trust anchors. SP 800-53 protects trust anchors through SC-17, which NIST marked uniquely federal and did not carry into 800-171. The objective survives through 3.13.15, the authenticity of communications sessions, which TLS certificate validation underpins, though the fit is looser than SC-17's.

Verdict: time, certificate, and update integrity are never traded for privacy. They are declined without qualification.

8. Notes for Assessors

MET, and the system security plan. An organization can cite this baseline as the mechanism for the objectives it reaches, in Section 4, and as a documented baseline configuration for 3.4.1[a] and 3.4.2[a]. It must supply every other objective itself. For 3.4.7 in particular, the baseline proposes the definitions of nonessential functions under [b] and [e], and the system security plan has to adopt them as the organization's own. An assessor looks for the definition before the mechanism.

What the evidence demonstrates. Snapshot Mode captures current system state as a profile for comparison against the applied baseline. That is point-in-time evidence: it shows a setting was configured when the snapshot ran, not that it held across a period. On non-Home editions the Local Group Policy entry is the authoritative record for the 123 policy-managed settings, because a registry read cannot distinguish a managed value from one set manually. On Home, and for the 11

settings outside the policy branches, the registry is the only record, and drift is found only by comparing snapshots.

Assessment methods. The objectives this baseline reaches are met by mechanisms, so the applicable methods are examine, for the configuration or policy state, and test, for the snapshot comparison. The objectives it leaves are established by examining the organization's documentation and the mechanisms it supplies, and by interview.

Changes the organization makes. Section 6 records two settings an organization may reasonably exclude. An organization that excludes them has changed its baseline configuration, and should record the change.

Verification details. The settings that have no Group Policy equivalent, and one Group Policy whose name inverts its effect, are set out in Section 9 of the SP 800-53 mapping. The baseline carries no Common Configuration Enumeration identifiers and is not SCAP content, so an automated tool consuming XCCDF or OVAL cannot evaluate it directly.

Scoping. Before crediting any requirement, confirm which settings take effect on the device being assessed, Section 5.3, and whether the device is managed by a domain or a cloud management service, Section 3.1.

9. Setting Index

Every setting, in definitions order, with the assessment objective it reaches, or the requirement alone where it has a single objective. An asterisk marks a setting subject to a scoping consideration.

Setting	Profile	Requirement	Relationship	Also Supports
Set Diagnostic Data to Minimum	Base	3.1.20[f]	Supports	-
Disable Tailored Experiences	Base	3.4.7[f]	Supports	-
Disable Consumer Experiences	Base	3.4.7[f]	Supports	-
Disable Feedback Notifications	Base	3.4.7[f]	Supports	-
Set Feedback Period to Zero	Base	3.4.7[f]	Partially supports	-
Set Feedback Count to Zero	Base	3.4.7[f]	Partially supports	-
Disable Advertising ID (Feature)	Base	3.4.7[f]	Supports	-
Disable Advertising ID (Policy)	Base	3.4.7[f]	Supports	3.4.2 (partially supports)
Disable Language List Access	Base	3.4.7[f]	Supports	-
Disable MAPS Reporting	Base	3.4.7[f]	Supports	-

Setting	Profile	Requirement	Relationship	Also Supports
Disable Sample Submission	Base	3.1.20[f]	Supports	-
Disable MSRT Diagnostic Data	Base	3.4.7[f]	Supports	-
Disable Enhanced Notifications	Base	3.4.7[f]	Supports	-
Restrict Implicit Text Collection	Base	3.4.7[f]	Supports	3.13.16 (incidental)
Restrict Implicit Ink Collection	Base	3.4.7[f]	Supports	3.13.16 (incidental)
Disable OneDrive File Storage	Layer	3.1.20[f]	Supports	3.4.7 (partially supports)
Disable OneDrive Network Traffic Before Sign-In	Layer	3.13.1[e]	Supports	-
Disable Microsoft Account Sign-In Assistant	Layer	3.1.20[e]	Supports	3.4.7 (partially supports)
Disable Web Results in Search	Base	3.13.1[e]	Supports	3.1.20 (partially supports)
Disable Web Search	Base	3.13.1[e]	Supports	3.1.20 (partially supports)
Disable Search Location	Base	3.4.7[f]	Supports	-
Disable Cortana *	Base	3.4.7[f]	Supports	-
Disable Cross-Device Experiences	Layer	3.1.20[f]	Supports	3.4.7 (partially supports)
Disable Settings Sync	Base	3.1.20[f]	Supports	-
Disable Settings Sync User Override	Base	3.4.2[b]	Supports	-
Disable Cloud Clipboard	Base	3.1.20[f]	Supports	-
Disable Find My Device	Base	3.4.7[f]	Supports	-
Disable Location Services	Layer	3.4.7[o]	Supports	-
Deny App Access to Location	Layer	3.4.7[f]	Supports	-
Deny App Access to Camera	Layer	3.13.12[c]	Partially supports	-
Deny App Access to Microphone	Layer	3.13.12[c]	Partially supports	-
Deny App Access to Radios	Base	3.4.7[f]	Supports	-
Deny App Access to Motion	Base	3.4.7[f]	Supports	-
Deny Sync with Unpaired Devices	Base	3.1.20[e]	Supports	-
Deny App Access to Trusted Devices	Layer	3.1.20[e]	Supports	-
Deny App Access to Account Info	Layer	3.1.2[b]	Partially supports	-
Deny App Access to Contacts	Layer	3.1.2[b]	Partially supports	-
Deny App Access to Calendar	Layer	3.1.2[b]	Partially supports	-
Deny App Access to Email	Layer	3.1.2[b]	Partially supports	-
Deny App Access to Messaging	Layer	3.1.2[b]	Partially supports	-
Deny App Access to Phone Calls	Layer	3.1.2[b]	Partially supports	-
Deny App Access to Call History	Layer	3.1.2[b]	Partially supports	-

Setting	Profile	Requirement	Relationship	Also Supports
Deny Background App Execution	Layer	3.4.7[f]	Supports	-
Deny App Access to Notifications	Base	3.1.2[b]	Partially supports	-
Deny Voice Activation	Base	3.13.12[c]	Partially supports	-
Deny Voice Activation Above Lock	Base	3.1.10[b]	Supports	3.13.12 (supports)
Deny App Access to Tasks	Base	3.1.2[b]	Partially supports	-
Deny App Access to Diagnostics	Base	3.1.2[b]	Supports	3.4.7 (partially supports)
Disable All Store Apps	Layer	3.4.7[c]	Supports	3.4.8 (partially supports)
Disable Auto Download and Install of Updates	Layer	3.4.3[c]	Supports	-
Suppress Store App Recommendations (Policy)	Base	3.4.7[f]	Supports	-
Suppress Store App Recommendations (Source)	Base	3.4.7[f]	Supports	-
Disable SmartScreen for Store Apps	Base	3.13.1[e]	Partially supports	-
Disable All Spotlight Features	Base	3.4.7[f]	Supports	-
Disable Cloud Optimized Content	Base	3.4.7[f]	Supports	-
Disable Widgets	Base	3.4.7[f]	Supports	-
Disable News and Interests *	Base	3.4.7[f]	Supports	-
Disable Recommendations	Base	3.4.7[f]	Supports	-
Disable App Launch Tracking	Base	3.4.7[f]	Supports	-
Disable Online Speech Recognition	Base	3.1.20[f]	Supports	3.13.1 (partially supports)
Disable Speech Model Updates	Base	3.13.1[e]	Partially supports	-
Disable Notification Network Traffic	Layer	3.13.1[e]	Supports	-
Disable Online Tips	Base	3.4.7[f]	Supports	3.13.1 (partially supports)
Disable App URI Handlers	Base	3.4.7[f]	Supports	-
Disable Auto Download Map Data	Base	3.4.7[f]	Supports	3.13.1 (partially supports)
Disable Unsolicited Map Network Traffic	Base	3.13.1[e]	Supports	-
Disable Activity Feed *	Base	3.4.7[f]	Supports	-
Disable Publish User Activities *	Base	3.4.7[f]	Supports	-
Disable Upload User Activities *	Base	3.1.20[f]	Partially supports	-
Disable Insider Preview Builds	Base	3.4.3[c]	Supports	-
Disable Peer-to-Peer Update Sharing	Base	3.13.1[e]	Supports	3.4.7 (supports)
Disable Disk Health Model Updates	Base	3.4.7[f]	Partially supports	-
Disable Services Configuration	Base	3.4.3[c]	Supports	3.4.2 (supports)
Disable Suggested Sites *	Base	3.13.1[e]	Partially supports	-

Setting	Profile	Requirement	Relationship	Also Supports
Disable Enhanced Suggestions *	Base	3.1.20[f]	Partially supports	-
Disable Browser Geolocation *	Base	3.4.7[f]	Supports	-
Disable AutoComplete for Web Addresses *	Base	3.4.7[f]	Supports	-
Disable Feed Background Sync *	Base	3.13.1[e]	Supports	3.4.7 (partially supports)
Disable IE SmartScreen *	Base	3.13.1[e]	Partially supports	-
Disable ActiveX VersionList Download *	Base	3.13.13[a]	Supports	-
Set IE Home Page to Blank *	Base	3.4.2[a]	Supports	-
Lock IE Home Page Setting *	Base	3.4.2[b]	Supports	-
Disable IE First Run Wizard *	Base	3.4.7[f]	Partially supports	-
Set IE New Tab to Blank *	Base	3.4.7[f]	Partially supports	-
Disable Compatibility View Editing *	Base	3.4.2[b]	Supports	-
Disable Flip Ahead *	Base	3.13.1[e]	Partially supports	-
Disable Device Metadata Retrieval	Base	3.13.1[e]	Supports	-
Disable Font Streaming	Base	3.13.1[e]	Supports	3.4.7 (partially supports)
Disable KMS Online Validation *	Base	3.13.1[e]	Supports	-
Disable Teredo	Base	3.13.1[e]	Supports	3.4.7 (supports)
Disable License Manager Service	Layer	3.4.7[o]	Supports	-
Exclude Device Name from Diagnostic Data	Base	3.1.20[f]	Incidental	-
Limit Diagnostic Log Collection	Base	3.1.20[f]	Partially supports	-
Limit Dump Collection	Base	3.13.16	Supports	3.1.20 (partially supports)
Disable Windows Error Reporting	Base	3.1.20[f]	Supports	-
Disable Application Telemetry	Base	3.4.7[f]	Supports	-
Disable Inventory Collector	Base	3.4.7[f]	Supports	-
Disable Inking and Typing Data Collection	Base	3.1.20[f]	Supports	-
Disallow AutoPlay for Non-Volume Devices	Base	3.8.7	Supports	3.14.2 (partially supports)
Disable AutoRun Command Execution	Base	3.8.7	Supports	3.14.2 (partially supports)
Disable AutoPlay	Base	3.8.7	Supports	3.14.2 (partially supports)
Disable Multicast Name Resolution	Base	3.4.7[l]	Supports	-
Disable Smart Multi-Homed Name Resolution	Base	3.13.1[e]	Supports	3.13.7 (partially supports)
Disable Lock Screen App Notifications	Base	3.1.10[c]	Supports	-
Disable Automatic Sign-In After Restart	Base	3.5.2[a]	Partially supports	3.1.10 (partially supports)
Disable Local Account Security Questions	Base	3.5.2[a]	Supports	-

Setting	Profile	Requirement	Relationship	Also Supports
Disable Fast Startup	Base	3.13.16	Partially supports	-
Disable Indexing of Encrypted Files	Base	3.13.16	Supports	-
Disable MDM Enrollment	Base	3.4.7[f]	Supports	3.1.1 (partially supports)
Disable Recently Opened Document History	Base	3.4.7[f]	Supports	-
Remove Recently Added List from Start Menu	Base	3.4.7[f]	Supports	-
Disable File Explorer Search History	Base	3.4.7[f]	Supports	3.13.16 (incidental)
Disable Search History	Base	3.4.7[f]	Supports	3.13.16 (incidental)
Disable File Explorer Account Insights	Base	3.4.7[f]	Supports	3.1.20 (partially supports)
Disable Clipboard History	Base	3.4.7[f]	Supports	3.13.16 (incidental)
Disable Windows Tips	Base	3.4.7[f]	Supports	-
Disable Consumer Account State Content	Base	3.4.7[f]	Supports	-
Disable Spotlight Collection on Desktop	Base	3.4.7[f]	Supports	-
Disable Windows Welcome Experience	Base	3.4.7[f]	Supports	-
Disable Spotlight on Action Center	Base	3.4.7[f]	Supports	-
Disable Spotlight on Settings	Base	3.4.7[f]	Supports	-
Disable Search Highlights	Base	3.4.7[f]	Supports	-
Disable Cloud Search	Base	3.13.1[e]	Supports	3.1.20 (partially supports)
Disable Push To Install Service	Base	3.4.9[b]	Supports	3.4.7 (partially supports)
Disable Account Notifications in Start	Base	3.4.7[f]	Supports	-
Disable Windows Copilot *	Base	3.4.7[f]	Supports	-
Disable Recall *	Base	3.4.7[f]	Supports	3.13.16 (incidental)
Disable Click to Do	Base	3.4.7[f]	Supports	-
Disable Settings Agentic Search	Base	3.4.7[f]	Supports	-
Disable Phone-PC Linking	Layer	3.1.20[e]	Supports	3.4.7 (partially supports)
Disable Game Recording and Broadcasting	Base	3.4.7[f]	Supports	-
Disable Windows Media DRM Internet Access	Base	3.13.1[e]	Supports	-
Disable CD and DVD Media Information Retrieval	Base	3.13.1[e]	Supports	-
Disable Music File Media Information Retrieval	Base	3.13.1[e]	Supports	-

10. Traceability

Every setting in this mapping traces to its entry in a curated profile, Policy-Windows-Base.psd1 or Policy-Windows-NoStoreApps.psd1, to its definition in Policy-MicrosoftPrivacyConnections.psd1 or Policy-WindowsPrivacyDefaults.psd1 and the reference documents under definitions/reference/, to the curation decision in profiles/reference/Policy-Windows.md, and to its SP 800-53 assignment in Policy-Windows-NIST-800-53.md, from which this assignment is derived.

Requirement text and assessment objectives are drawn from NIST's machine-readable files for 800-171 Revision 2 and 800-171A. The tailoring actions and the requirement-to-control mapping are drawn from Appendix E and Appendix D of the Revision 2 publication, which have no machine-readable form. Requirement titles are the CMMC Assessment Guide's, with one correction: the guide spells 3.8.7's title "Removeable Media".

11. References

NIST SP 800-171 Revision 2, February 2020 (includes updates as of January 28, 2021). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.* Requirement text and discussion, and the Appendix D mapping and Appendix E tailoring actions. Withdrawn by NIST on 2024-05-14 and superseded by Revision 3, and incorporated by reference in 32 CFR 170, which is why it is the edition used.

NIST SP 800-171A, June 2018. *Assessing Security Requirements for Controlled Unclassified Information.* Assessment objectives and methods. Withdrawn and incorporated on the same terms as Revision 2.

32 CFR Part 170. *Cybersecurity Maturity Model Certification (CMMC) Program.* Incorporates 800-171 Revision 2 and 800-171A, and defines the asset categories cited here.

CMMC Assessment Guide, Level 2, Version 2.13, September 2024. Requirement titles and the definition of MET. Guidance under 32 CFR 170, which prevails where the two differ.

NIST SP 800-53 Revision 5, Release 5.2.0. *Security and Privacy Controls for Information Systems and Organizations.* The framework of the mapping this document derives from. NIST's Revision 4 to Revision 5 comparison workbook bridges it to the Revision 4 controls that 800-171 Appendix D and E cite.

NIST IR 8278 Revision 1 and NIST IR 8278A Revision 1. *National Online Informative References (OLIR) Program.* The relationship types used to classify a mapping, and the supportive relationship mapping this document performs.

Microsoft. *Configure Windows diagnostic data in your organization.* What each diagnostic data level sends, cited in Section 5.2.

Microsoft. *Cloud protection and sample submission at Microsoft Defender Antivirus.* What cloud protection and sample submission send and when the user is prompted, cited in Section 4.1, Section 5.2, and Section 6.1.

12. Revision History

Version	Date	Change
1.0	2026-09-23	Initial issue