

Microsoft is pleased to announce the **June 2025 Revision (v2506)** of the security baseline package for **Windows Server 2025**! You can download the baseline package from the [Microsoft Security Compliance Toolkit](#), test the recommended configurations in your environment, and customize / implement them as appropriate.

Starting with this release, we plan to revise the **Windows Server baseline more frequently** to keep pace with evolving threats, new Windows features, and community feedback.

Summary of Changes in This Release (v2506)

This release includes several changes made since the last release of the [security baseline for Windows Server 2025 in January 2025](#) to further assist in the security of enterprise customers along with better aligning with the latest standards. The changes include what is now depicted in the table below.

Security Policy	Change Summary
Deny log on through Remote Desktop Services	Allow remote logon for non-admin local accounts on MS and add “BUILTIN\Guests” to both DC and MS.
WDigest Authentication	Remove from the baseline
Allow Windows Ink Workspace	Remove from the baseline
Audit Authorization Policy Change	Set to “Success” in both DC and MS
Include command line in process creation events	Enable in both DC and MS
Control whether exclusions are visible to local users	Moved to Not Configured as it is overridden by the parent setting.

Deny log on through Remote Desktop Services

We updated **SeDenyRemoteInteractiveLogonRight** on member servers to use S-1-5-114(Local account and member of Administrators group) instead of S-1-5-113(all local accounts) to strike a better balance between security and operational flexibility. This change continues to block remote RDP access for high-risk local admin accounts—our primary threat vector—while enabling legitimate use cases for non-admin local accounts, such as remote troubleshooting and maintenance during failover or domain unavailability. By allowing non-admin local accounts to log on interactively, we preserve a secure recovery path without weakening protection for privileged accounts.

In addition, to strengthen the Remote Desktop Services (RDS) posture on both Windows Server 2025 Domain Controllers and Member Servers, we added the **Guests group** to the **"Deny log on through Remote Desktop Services"** policy. While the Guest account is disabled by default, explicitly denying its RDP access adds a defense-in-depth measure that helps prevent misuse if the group is ever enabled or misconfigured. This complements the existing restriction on Local Account logon for DCs and helps ensure a consistent security posture across server roles.

WDigest Authentication

We removed the policy **"WDigest Authentication (disabling may require KB2871997)"** from the security baseline because it is no longer necessary for Windows Server 2025. This policy was originally enforced to prevent **WDigest** from storing users plaintext passwords in memory, which posed a serious credential theft risk. However, starting with 24H2 update ([KB5041160](#)) for **Windows Server 2022** and continuing into **Windows Server 2025**, the engineering teams have deprecated this policy. As a result, there is no longer a need to explicitly enforce this setting, and the policy has been removed from the baseline to reflect the current default behavior.

Allow Windows Ink Workspace

We removed the policy **"Allow Windows Ink Workspace"** from the Windows Server 2025 security baseline. This policy applies only to Windows client editions and is not available on Windows Server. Including it in the baseline caused confusion removing an unnecessary setting from the baseline reduces GPO processing time and helps ensure all recommended settings are applicable for the Windows Server environment.

Audit Authorization Policy Change

We set **Audit Authorization Policy Change (Success)** on the baseline for both **Domain Controllers** and **Member Servers** to ensure visibility into any changes that affect the system's security posture, including modifications to user rights and audit policies. These changes directly impact how access is granted and how activity is monitored, making them critical to detect for both security and compliance purposes. Logging successful changes helps identify misconfigurations, unauthorized privilege assignments, or malicious tampering — especially in cases of lateral movement or privilege escalation. Because these events occur infrequently, they generate minimal log volume while offering high forensic and operational value.

While **Failure** auditing is not set, it is available as an optional setting on both Domain Controllers and Member Servers for organizations that have the monitoring capability to interpret and act on failed attempts to modify security policies. This provides an added layer of visibility in high-assurance or tightly controlled environments.

Include command line in process creation events

We added **Include command line in process creation events** in the baseline to improve visibility into how processes are executed across the system. Capturing command-line arguments allows defenders to detect and investigate malicious activity that may otherwise appear legitimate, such as abuse of scripting engines, credential theft tools, or obfuscated payloads using native binaries. This setting supports modern threat detection techniques with minimal performance overhead and is widely recommended.

Visibility of Microsoft Defender Antivirus Exclusions

We updated the configuration for the policy "**Control whether exclusions are visible to local users**" (Computer Configuration\Windows Components\Microsoft Defender Antivirus) to **Not Configured** in this release.

This change was made because the parent policy "**Control whether or not exclusions are visible to Local Admins**" is already set to **Enabled**, which takes precedence and effectively overrides the behavior of the former setting. As a result, explicitly configuring the child policy is unnecessary and may introduce confusion without impacting actual behavior.

You can continue to manage exclusion visibility through the parent policy, which provides the intended control over whether local administrators can view exclusion lists.

UEFI Lock and Virtualization-Based Protections

In Windows, some security features are protected by Secure Boot and the TPM. When combined with firmware protections that lock UEFI configuration variables, these protections become tamper-resistant: Windows can detect and respond to unauthorized hardware changes or tamper attempts, making it significantly harder for attackers to disable key security features after deployment.

In the Windows Server 2025 security baseline, two policy categories are configured to take advantage of UEFI lock:

- **Virtualization-Based Security (VBS)** — managed via the policy:
System\Device Guard\Turn On Virtualization Based Security
- **Local Security Authority (LSA) Protection** — managed via the policy:
System\Local Security Authority\Configure LSASS to run as a protected process

While there are no changes to the recommended settings for these policies in this release, we want to highlight their role in strengthening system defenses and provide guidance to help you make informed deployment decisions.

UEFI lock enforces these protections in a way that prevents local or remote tampering—even by administrators. This aligns with strong security requirements in sensitive or high-assurance environments. However, it also introduces important operational considerations:

- Some hardware platforms may not fully support UEFI lock
- Compatibility issues, reduced performance, or system instability may occur
- Once enabled, UEFI lock is difficult to reverse

Please let us know your thoughts by commenting on this post or through the [Security Baseline Community](#).