

Windows 11 24H2 security baseline

Microsoft is pleased to announce the release of the security baseline package for Windows 11, version 24H2!

Please download the content from the [Microsoft Security Compliance Toolkit](#), test the recommended configurations, and customize / implement as appropriate.

This release includes several changes to further assist in the security of enterprise customers, including additional protections to LAN Manager, Kerberos, User Account Control, Microsoft Defender Antivirus updates, and more.

Mark of the Web

You may have seen previous discussions on the Mark of the Web (MotW) within our baselines at some point. A new setting has been added and configured, located at `Windows Components\File Explorer\Do not apply the Mark of the Web tag to files copied from insecure sources`. This new setting will be enforced with a value of `Disabled`. This adds the MotW when copying a file from a network share (in the Internet Zone) into the local file system. If necessary, Zone Mapping can be used to map any file shares that are deemed trusted into the Trusted/Intranet Zones.

LAN Manager

For each release, we conduct a complete review of settings as part of our security baseline. Based on the latest review, we are updating our recommended settings for LAN Manager (Lanman) including Lanman Server and Lanman Workstation.

- `Network\Lanman Server`
 - `Audit client does not support encryption` – set to a value of `Enabled`
 - `Audit client does not support signing` – set to a value of `Enabled`
 - `Audit insecure guest logon` – set to a value of `Enabled`
 - `Enable authentication rate limiter` – set to a value of `Enabled`
 - `Enable remote mailslots` – set to a value of `Disabled`
 - `Mandate the maximum version of SMB` – set to a value of `Enabled: SMB 3.1.1`
 - `Mandate the minimum version of SMB` – set to a value of `Enabled: SMB 3.0.0`
 - `Set authentication rate limiter delay (milliseconds)` – set to a value of `Enabled: 2000`
- `Network\Lanman Workstation`
 - `Audit insecure guest logon` – set to a value of `Enabled`
 - `Audit server does not support encryption` – set to a value of `Enabled`
 - `Audit server does not support signing` – set to a value of `Enabled`
 - `Enable remote mailslots` – set to a value of `Disabled`

- Mandate the maximum version of SMB – set to a value of Enabled: SMB 3.1.1
- Mandate the minimum version of SMB – set to a value of Enabled: SMB 3.0.0
- Require Encryption – set a value of Disabled

Configure hash algorithms for certificate logon

A new setting, located at `System\KDC` and `System\Kerberos`, has been added for smart card crypto agility. This setting lets users configure the hash algorithm to be used in certificate-based smart card (PKINIT) authentication of Kerberos. With this configuration, customers have the option to prevent SHA-1 from being used. The security baseline recommends support for SHA-256, SHA-384, and SHA-512, but does not recommend support for SHA-1. It's important to note these settings are useful only if both the client and KDC (Windows Server 2025) are configured this way in the environment.

Sudo command

Located at `System\Configure the behavior of the sudo command`, this setting allows the customization of how the sudo command operates. Sudo for Windows can be used as a potential escalation of privilege vector when enabled in certain configurations. The baseline configures this setting to a value of Disabled, which disables sudo for Windows.

Microsoft Defender Antivirus

Microsoft Defender Antivirus (MDAV) plays a critical part in our security story. We are constantly making improvements to the product and have included six new settings in this release.

- `Windows Components\Microsoft Defender Antivirus\Control whether exclusions are visible to local users` – set to a value of Enabled
- `Windows Components\Microsoft Defender Antivirus\Features\Enable EDR in block mode` – set to a value of Enabled
- `Windows Components\Microsoft Defender Antivirus\Network Inspection System\Convert warn verdict to block` – set to a value of Enabled
- `Windows Components\Microsoft Defender Antivirus\Real-time Protection\Configure real-time protection and Security Intelligence Updates during OOBE` – set to a value of Enabled
- `Windows Components\Microsoft Defender Antivirus\Reporting\Configure whether to report Dynamic Signature dropped events` – set to a value of Enabled
- `Windows Components\Microsoft Defender Antivirus\Scan\Scan excluded files and directories during quick scans` – set to a value of Enabled: 1

User Account Control

Two settings affecting User Account Control have been added.

- Enhanced Privilege Protection Mode helps provide an additional layer of protection against malware and other threats by isolating sensitive data and processes. Located in the security template at `Security Options\Behavior of the elevation prompt for administrators in Enhanced Privilege Protection Mode`, the baseline configures this setting to Prompt for credentials on secure desktop.
- A second policy controls whether enhanced privilege protection is applied to admin approval mode elevations. Located in the security template at `Security Options\Configure type of Admin Approval Mode`, we recommend setting this to a value of Admin Approval Mode with enhanced privilege protection.

Additional items worth considering

The following settings should be evaluated based on your environment.

Delegated Managed Service Account (dMSA)

We have introduced a new policy called Enable delegated Managed Service Account (dMSA) Logons which is located at `System\Kerberos`. This controls dMSA logons for the machine. If you enable this policy setting, dMSA logons will be supported by the Kerberos client. Please review the [prerequisites](#) before adjusting the policy setting.

By default, dMSA is disabled because the Domain Controller (DC) must also be upgraded to Windows Server 2025 for the feature to function properly. If the DC is running a version earlier than Server 2025, the necessary schema updates for dMSA will not be present.

If your DC has been upgraded to Windows Server 2025, we suggest enabling this policy on both the client and DC sides. When enabled, you may need to specify realms, i.e., which domains or parts of the directory can authenticate and access the dMSA account. A child domain on an older server version can still interact with the accounts while maintaining security boundaries. It allows for a smoother transition and coexistence of features across a mixed-version environment. For example, if you have a primary domain called corp.contoso.com running on Windows Server 2025 and an older child domain called legacy.corp.contoso.com running on an older version of Windows Server (e.g., Windows Server 2022), you may specify the realm as legacy.corp.contoso.com. To learn more, see [Setting up delegated Managed Service Accounts \(dMSA\) in Windows Server 2025](#).

Windows Protected Print

Windows Protected Print (WPP) is the new, modern and more secure print for Windows built from the ground up with security in mind. WPP blocks 3rd party drivers and hardens the entire print stack from attacks. WPP is designed to work with [Mopria certified](#) printers. While not yet configured in the security baseline, we recommend you consider the setting `Printers\Configure Windows protected print` as later versions of the baselines will look to enable this very important feature. You can learn more about the security benefits in our [blog post](#).

Microsoft Defender Antivirus

There are several Microsoft Defender Antivirus (MDAV) settings we recommend you consider.

- `Windows Components\Microsoft Defender Antivirus\Real-time Protection\Configure performance mode status` is beneficial for developers

who utilize Dev Drive on Windows 11. More information on Dev Drive can be found [here](#).

The following two settings are specific to VDI environments.

- Windows Components\Microsoft Defender Antivirus\Network Inspection System\Turn on asynchronous inspection **helps to ensure there is no slowdown in the detection process.**
- Windows Components\Microsoft Defender Antivirus\Security Intelligence Updates\Configure security intelligence updates according to the scheduler for VDI clients **controls the flow of the SIUs.**

Other changes

We have decided to remove System\Group Policy\Configure registry policy processing from the security baseline after feedback from our support engineers on the numerous issues that were being traced back to it.

Several minor discrepancies between the documentation and group policies were noted since the last release. These should all be addressed going forward.

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