Credential Guard overview

By officedocspr5

Archived: 2026-04-05 14:08:56 UTC

▶

Credential Guard prevents credential theft attacks by protecting NTLM password hashes, Kerberos Ticket Granting Tickets (TGTs), and credentials stored by applications as domain credentials.

Credential Guard uses Virtualization-based security (VBS) to isolate secrets so that only privileged system software can access them. Unauthorized access to these secrets can lead to credential theft attacks like *pass the hash* and *pass the ticket*.

When enabled, Credential Guard provides the following benefits:

- **Hardware security**: NTLM, Kerberos, and Credential Manager take advantage of platform security features, including Secure Boot and virtualization, to protect credentials
- **Virtualization-based security**: NTLM, Kerberos derived credentials, and other secrets run in a protected environment that is isolated from the running operating system
- **Protection against advanced persistent threats**: when credentials are protected using VBS, the credential theft attack techniques and tools used in many targeted attacks are blocked. Malware running in the operating system with administrative privileges can't extract secrets that are protected by VBS

Note

While Credential Guard is a powerful mitigation, persistent threat attacks will likely shift to new attack techniques, and you should also incorporate other security strategies and architectures.

Default enablement

Starting in **Windows 11, 22H2** and **Windows Server 2025**, VBS and Credential Guard are enabled by default on devices that meet the requirements.

The default enablement is **without UEFI Lock**, thus allowing administrators to disable Credential Guard remotely if needed.

When Credential Guard is enabled, VBS is automatically enabled too.

Note

If Credential Guard is explicitly disabled *before* a device is updated to Windows 11, version 22H2 / Windows Server 2025 or later, default enablement does not overwrite the existing settings. That device will continue to have Credential Guard disabled even after updating to a version of Windows that enables Credential Guard by default.

Default enablement on Windows

Devices running Windows 11, 22H2 or later have Credential Guard enabled by default if they:

- Meet the license requirements
- Meet the hardware and software requirements
- Aren't explicitly configured to disable Credential Guard

Note

Devices running Windows 11 Pro/Pro Edu 22H2 or later may have Virtualization-based Security (VBS) and/or Credential Guard automatically enabled if they meet the other requirements for default enablement, and have previously run Credential Guard. For example if Credential Guard was enabled on an Enterprise device that later downgraded to Pro.

> To determine whether the Pro device is in this state, check if the following registry key exists: `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0\IsolatedCredentialsRootSecret`. If you wish to disable Credential Guard, see configure Credential Guard.

Default enablement on Windows Server

Devices running Windows Server 2025 or later have Credential Guard enabled by default if they:

- Meet the license requirements
- Meet the hardware and software requirements
- Aren't explicitly configured to disable Credential Guard
- Are joined to a domain
- Aren't a domain controller

System requirements

For Credential Guard to provide protection, the device must meet certain hardware, firmware, and software requirements.

Devices that exceed the minimum hardware and firmware qualifications receive additional protections and are more hardened against certain threats.

Hardware and software requirements

Credential Guard requires the features:

- Virtualization-based security (VBS)
- Secure Boot

While not required, the following features are recommended to provide additional protections:

- Trusted Platform Module (TPM), as it provides binding to hardware. TPM versions 1.2 and 2.0 are supported, either discrete or firmware

- UEFI lock, as it prevents attackers from disabling Credential Guard with a registry key change

For detailed information on protections for improved security that are associated with hardware and firmware options, see additional security qualifications.

Credential Guard in virtual machines

Credential Guard can protect secrets in Hyper-V virtual machines, just as it would on a physical machine. When Credential Guard is enabled on a VM, secrets are protected from attacks *inside* the VM. Credential Guard doesn't provide protection from privileged system attacks originating from the host.

The requirements to run Credential Guard in Hyper-V virtual machines are:

- The Hyper-V host must have an IOMMU
- The Hyper-V virtual machine must be generation 2

Note

Credential Guard is not supported on Hyper-V or Azure generation 1 VMs. Credential Guard is available on generation 2 VMs only.

Windows edition and licensing requirements

The following table lists the Windows editions that support Credential Guard:

Windows Pro	Windows Enterprise	Windows Pro Education/SE	Windows Education
No	Yes	No	Yes

Credential Guard license entitlements are granted by the following licenses:

Windows Pro/Pro Education/SE	Windows Enterprise E3	Windows Enterprise E5	Windows Education A3	Windows Education A5
No	Yes	Yes	Yes	Yes

For more information about Windows licensing, see Windows licensing overview.

Application requirements

When Credential Guard is enabled, certain authentication capabilities are blocked. Applications that require such capabilities break. We refer to these requirements as *application requirements*.

Applications should be tested before deployment to ensure compatibility with the reduced functionality.

Warning

Enabling Credential Guard on domain controllers isn't recommended. Credential Guard doesn't provide any added security to domain controllers, and can cause application compatibility issues on domain controllers.

Enabling Credential Guard on Exchange Server isn't supported and can lead to performance issues.

Note

Credential Guard doesn't provide protections for the Active Directory database or the Security Accounts Manager (SAM). The credentials protected by Kerberos and NTLM when Credential Guard is enabled are also in the Active Directory database (on domain controllers) and the SAM (for local accounts).

Applications break if they require:

- Kerberos DES encryption support
- Kerberos unconstrained delegation
- Kerberos TGT extraction
- NTLMv1

Applications ask and expose credentials to risk if they require:

- Digest authentication
- Credential delegation
- MS-CHAPv2
- CredSSP

Applications might cause performance issues when they attempt to hook the isolated Credential Guard process `LSAIso.exe`.

Services or protocols that rely on Kerberos, such as file shares or remote desktop, continue to work and aren't affected by Credential Guard.

Next steps

- Learn how Credential Guard works
- Learn how to configure Credential Guard
- Review the advice and sample code for making your environment more secure and robust with Credential Guard in the Additional mitigations article
- Review considerations and known issues when using Credential Guard

---