How Credential Guard works

By officedocspr5

Archived: 2026-04-05 22:40:14 UTC

Kerberos, NTLM, and Credential Manager isolate secrets by using Virtualization-based security (VBS). Previous versions of Windows stored secrets in its process memory, in the Local Security Authority (LSA) process `lsass.exe`.

With Credential Guard enabled, the LSA process in the operating system talks to a component called the *isolated LSA process* that stores and protects those secrets, `LSAIso.exe`. Data stored by the isolated LSA process is protected using VBS and isn't accessible to the rest of the operating system. LSA uses remote procedure calls to communicate with the isolated LSA process.

For security reasons, the isolated LSA process doesn't host any device drivers. Instead, it only hosts a small subset of operating system binaries that are needed for security and nothing else. All the binaries are signed with a certificate that VBS trusts, and the signatures are validated before launching the file in the protected environment.


Diagram of the Credential Guard architecture.

Secrets protected by Credential Guard are protected in memory and isolated at runtime by the hypervisor using Virtual Secure Mode (VSM). On recent supported hardware with TPM 2.0, VSM data that is persisted will be protected by a key called the *VSM master key*, which is protected by device firmware protections. To learn more, see System Guard: How a hardware-based root of trust helps protect Windows. The VSM master key is protected by the TPM, ensuring that the key and secrets protected by Credential Guard can only be accessed in a trusted environment.

Credential Guard doesn't typically persist authentication data (NTLM hash and TGTs), as that data is lost between reboots and refreshed when the user signs into the system. This means that it isn't dependent on the VSM master key or the TPM to protect that data at reset.

Note

The VBS master key might not be protected by the TPM in any of the following environments:

- If Secure Boot is disabled
- If a TPM isn't available on the firmware

Some ways to store credentials aren't protected by Credential Guard, including:

- When Credential Guard is enabled, NTLMv1, MS-CHAPv2, Digest, and CredSSP can't use the signed-in credentials. Thus, single sign-on doesn't work with these protocols. However, applications can prompt for credentials or use credentials stored in the Windows Vault, which aren't protected by Credential Guard with any of these protocols

Caution

It's recommended that valuable credentials, such as the sign-in credentials, aren't used with NTLMv1, MS-CHAPv2, Digest, or CredSSP protocols.

- Software that manages credentials outside of Windows feature protection
- Local accounts and Microsoft Accounts
- Credential Guard doesn't protect the Active Directory database running on Windows Server domain controllers. It also doesn't protect credential input pipelines, such as Windows Server running Remote Desktop Gateway. If you're using a Windows Server OS as a client PC, it will get the same protection as it would when running a Windows client OS
- Key loggers
- Physical attacks
- Doesn't prevent an attacker with malware on the PC from using the privileges associated with any credential. We recommend using dedicated PCs for high value accounts, such as IT Pros and users with access to high value assets in your organization
- Non-Microsoft security packages
- Supplied credentials for NTLM authentication aren't protected. If a user is prompted for and enters credentials for NTLM authentication, these credentials are vulnerable to be read from LSASS memory. These same credentials are vulnerable to key loggers as well
- Kerberos service tickets aren't protected by Credential Guard, but the Kerberos Ticket Granting Ticket (TGT) is protected
- When Credential Guard is enabled, Kerberos doesn't allow *unconstrained Kerberos delegation* or *DES encryption*, not only for signed-in credentials, but also prompted or saved credentials
- When Credential Guard is enabled on a VM, it protects secrets from attacks inside the VM. However, it doesn't provide protection from privileged system attacks originating from the host
- Windows logon cached password verifiers (commonly called *cached credentials*) don't qualify as credentials because they can't be presented to another computer for authentication, and can only be used locally to verify credentials. They're stored in the registry on the local computer and provide validation for credentials when a domain-joined computer can't connect to AD DS during user logon. These *cached logons*, or more specifically, *cached domain account information*, can be managed using the security policy setting **Interactive logon: Number of previous logons to cache** if a domain controller isn't available

- 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

---