Configure Credential Guard

By officedocspr5

Archived: 2026-04-05 21:47:27 UTC

This article describes how to configure Credential Guard using Microsoft Intune, Group Policy, or the registry.

Starting in Windows 11, 22H2 and Windows Server 2025, Credential Guard is enabled by default on devices which meet the requirements.

System administrators can explicitly enable or disable Credential Guard using one of the methods described in this article. Explicitly configured values overwrite the default enablement state after a reboot.

If a device has Credential Guard explicitly turned off before updating to a newer version of Windows where Credential Guard is enabled by default, it will remain disabled even after the update.

Credential Guard should be enabled before a device is joined to a domain or before a domain user signs in for the first time. If Credential Guard is enabled after domain join, the user and device secrets may already be compromised.

To enable Credential Guard, you can use:

- Microsoft Intune/MDM
- Group policy
- Registry

The following instructions provide details about how to configure your devices. Select the option that best suits your needs.

- **Intune/CSP**
- **GPO**
- **Registry**

To configure devices with Microsoft Intune, create a Settings catalog policy and use the following settings:

Category	Setting name	Value
Device Guard	Credential Guard	Select one of the options: - **Enabled with UEFI lock** - **Enabled without lock**

Important

If you want to be able to turn off Credential Guard remotely, choose the option **Enabled without lock**.

Assign the policy to a group that contains as members the devices or users that you want to configure.

Alternatively, you can configure devices using a custom policy with the DeviceGuard Policy CSP.

Setting
Setting name: Turn On Virtualization Based Security **OMA-URI**: `./Device/Vendor/MSFT/Policy/Config/DeviceGuard/EnableVirtualizationBasedSecurity` **Data type**: int **Value**: `1`
Setting name: Credential Guard Configuration **OMA-URI**: `./Device/Vendor/MSFT/Policy/Config/DeviceGuard/LsaCfgFlags` **Data type**: int **Value**: **Enabled with UEFI lock**: `1` **Enabled without lock**: `2`

Once the policy is applied, restart the device.

Checking Task Manager if `LsaIso.exe` is running isn't a recommended method for determining whether Credential Guard is running. Instead, use one of the following methods:

- System Information
- PowerShell
- Event Viewer

You can use *System Information* to determine whether Credential Guard is running on a device.

1. Select **Start**, type `msinfo32.exe`, and then select **System Information**
2. Select **System Summary**
3. Confirm that **Credential Guard** is shown next to **Virtualization-based Security Services Running**

You can use PowerShell to determine whether Credential Guard is running on a device. From an elevated PowerShell session, use the following command:

```
(Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard).SecurityServicesR
```

The command generates the following output:

- **0**: Credential Guard is disabled (not running)
- **1**: Credential Guard is enabled (running)

Perform regular reviews of the devices that have Credential Guard enabled, using security audit policies or WMI queries.

Open the Event Viewer (`eventvwr.exe`) and go to `Windows Logs\System` and filter the event sources for *WinInit*:

Event ID

Description

13 (Information)

```
Credential Guard (LsaIso.exe) was started and will protect LSA credentials.
```

`14` (Information)

```
Credential Guard (LsaIso.exe) configuration: [**0x0** | **0x1** | **0x2**], **0**
```

- The first variable: **0x1** or **0x2** means that Credential Guard is configured to run. **0x0** means that it's not configured to run.
- The second variable: **0** means that it's configured to run in protect mode. **1** means that it's configured to run in test mode. This variable should always be **0**.

`15` (Warning)

```
 Credential Guard (LsaIso.exe) is configured but the secure kernel isn't running;
continuing without Credential Guard.
```

`16` (Warning)

```
Credential Guard (LsaIso.exe) failed to launch: [error code]
```

`17`

```
Error reading Credential Guard (LsaIso.exe) UEFI configuration: [error code]
```

There are different options to disable Credential Guard. The option you choose depends on how Credential Guard is configured:

- Credential Guard running in a virtual machine can be disabled by the host
- If Credential Guard is enabled **with UEFI Lock**, follow the procedure described in disable Credential Guard with UEFI Lock
- If Credential Guard is enabled **without UEFI Lock**, or as part of the default enablement update, use one of the following options to disable it:
    - Microsoft Intune/MDM
    - Group policy

- Registry

The following instructions provide details about how to configure your devices. Select the option that best suits your needs.

- **Intune/CSP**
- **GPO**
- **Registry**

If Credential Guard is enabled via Intune and without UEFI Lock, disabling the same policy setting disables Credential Guard.

To configure devices with Microsoft Intune, create a Settings catalog policy and use the following settings:

Category	Setting name	Value
Device Guard	Credential Guard	**Disabled**

Assign the policy to a group that contains as members the devices or users that you want to configure.

Alternatively, you can configure devices using a custom policy with the DeviceGuard Policy CSP.

Setting
Setting name: Credential Guard Configuration **OMA-URI**: `./Device/Vendor/MSFT/Policy/Config/DeviceGuard/LsaCfgFlags` **Data type**: int **Value**: `0`

Once the policy is applied, restart the device.

If Credential Guard is enabled with UEFI lock, follow this procedure since the settings are persisted in EFI (firmware) variables.

Note

This scenario requires physical presence at the machine to press a function key to accept the change.

1. Follow the steps in Disable Credential Guard
2. Delete the Credential Guard EFI variables by using bcdedit. From an elevated command prompt, type the following commands:

```
 mountvol X: /s
copy %WINDIR%\System32\SecConfig.efi X:\EFI\Microsoft\Boot\SecConfig.efi /Y
bcdedit /create {0cb3b571-2f2e-4343-a879-d86a476d7215} /d "DebugTool" /application osloader
bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} path "\EFI\Microsoft\Boot\SecConfig.efi"
```

```
bcdedit /set {bootmgr} bootsequence {0cb3b571-2f2e-4343-a879-d86a476d7215}
bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} loadoptions DISABLE-LSA-ISO
bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} device partition=X:
mountvol X: /d
```

3. Restart the device. Before the OS boots, a prompt appears notifying that UEFI was modified, and asking for confirmation. The prompt must be confirmed for the changes to persist.

From the host, you can disable Credential Guard for a virtual machine with the following command:

```
Set-VMSecurity -VMName <VMName> -VirtualizationBasedSecurityOptOut $true
```

- 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

---

Source: https://docs.microsoft.com/windows/access-protection/credential-guard/credential-guard-manage