Enabling Windows Server 2019 Device Guard and Credential Guard on Lenovo ThinkSystem Servers

Introduces the Device Guard and Credential Guard features

Provides steps to enable Device Guard and Credential Guard

Describes how to check the status of the features

Explains what Lenovo servers support the features

Guiqing Li

LENOVO PRESS

Abstract

Device Guard and Credential Guard are two important security features of the Microsoft Windows Server operating system that leverage virtualization capabilities from the hardware and the hypervisor to provide additional protection for critical subsystems and data. Customers can implement these features to secure their devices and data, such as user or system secrets, and hashed credentials.

To benefit from these two features, the servers you are protecting must meet certain baseline hardware, firmware and software requirements. Lenovo® ThinkSystem™ servers support these two security features in conjunction with Windows Server 2019.

This document introduces Device Guard and Credential Guard, and shows users how to enable them on supported Lenovo ThinkSystem servers. This paper is intended for IT specialists, technical architects and sales engineers who want to learn more about Device Guard and Credential Guard and how to enable them. It is expected that readers have some experience with Windows Server administration.

Contents

Introduction 3
Secure Boot setting 4
Enabling Device Guard 4
Enabling Credential Guard. 7
Deploying Device Guard and Credential Guard in a VM 9
Lenovo ThinkSystem server support 10
References. 10
Author. 11
Notices 12
Trademarks 13

Introduction

Device Guard and Credential Guard are features of the Virtualization-based Security (VBS) technology of Microsoft Windows Server, used to leverage the virtualization extensions of the CPU and the hypervisor to protect critical processes and their memory against tampering from malicious attack.

Device Guard and Credential Guard are two different security features and they offer different protections against different types of threats.

Virtualization-based Security (VBS)

Virtualization-based security, or VBS, uses hardware virtualization features to create and isolate a secure region of memory from the normal operating system. Windows can use this “virtual secure mode” to host a number of security solutions, providing them with greatly increased protection and preventing the use of malicious exploits which attempt to defeat protections.

One such example of security solution is Hypervisor-Enforced Code Integrity (HVCI), commonly referred to as Memory Integrity, which uses VBS to significantly strengthen code integrity policy enforcement.

VBS uses the Windows hypervisor to create this virtual secure mode (VSM), and to enforce restrictions that protect vital system and operating system resources, or to protect security assets such as authenticated user credentials. Virtual secure mode doesn’t really provide any security by itself. Instead, virtual secure mode is more of an infrastructure-level component of the OS and is the basis for other security features.

Device Guard

Device Guard is a combination of enterprise-related hardware and software security features that designed to sequester a computer system against new and unknown malware. It will lock a device down so that it can only run trusted applications that you define in your code integrity policies, while simultaneously hardening the OS against kernel memory attacks by using virtualization-based protection of code integrity. Its focus is preventing malicious or unauthorized code from running on your devices.

Device Guard consists of three primary security features:

- Configurable Code Integrity (CCI) – Ensures that only trusted code runs from the boot loader onwards.
- VSM Protected Code Integrity – Moves Kernel Mode Code Integrity (KMCI) and Hypervisor Code Integrity (HVCI) components into VSM, hardening them from attack. This component is designed to ensure that only trusted code is allowed to run.
- Platform and UEFI Secure Boot – Ensuring the boot binaries and UEFI firmware are signed and have not been tampered with.

When using virtualization-based security to isolate Code Integrity, the only way kernel memory can become executable is through a Code Integrity verification. This means that kernel memory pages can never be Writable and Executable (W+X) and executable code cannot be directly modified.

Credential Guard

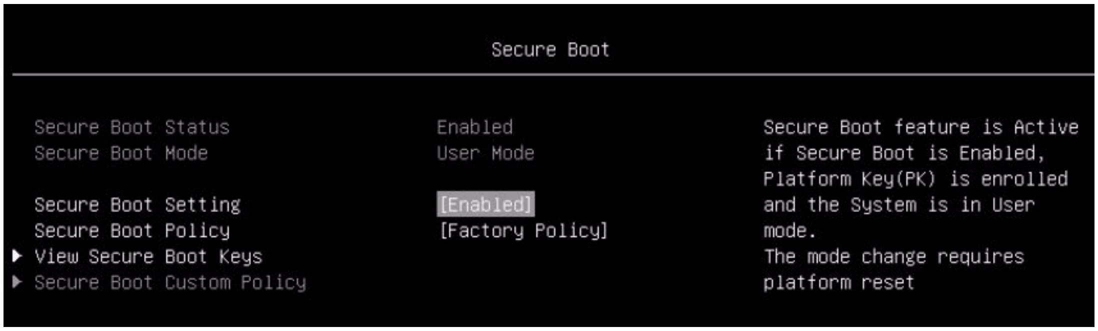
Credential Guard uses virtualization-based security to isolate secrets so that only privileged system software can access them. It can help to minimize the impact and breadth of a Pass the Hash style attack. Its focus is preventing attackers from stealing credentials and providing a kind of protection for your data, such as user and system secrets, hashed credentials.

The authentication process used by the Windows OS is a function of the Local Security Authority (LSA). LSA provides interactive authentication services, generates security tokens, manages the local security policy and manages the system's audit policy. Credential Guard works by moving the LSA into Isolated User Mode, the virtualized space created by virtual secure mode. Data stored by the isolated LSA process is protected by VBS and is not accessible to the rest of the operating system.

Credential Guard can also protect secrets in a Hyper-V virtual machine, just as it would on a physical machine. When Credential Guard is deployed on a VM, secrets are protected from attacks inside the VM.

Secure Boot setting

Before enabling the Device Guard and Credential Guard features in the OS, ensure that secure boot is enabled. If not, change secure boot to Enabled in BIOS setting via **System Settings** → **Security** → **Secure Boot Configuration** → **Secure Boot** as shown in Figure 1.



```
                              Secure Boot
-----------------------------------------------------------------------------------
  Secure Boot Status          Enabled              Secure Boot feature is Active
  Secure Boot Mode            User Mode            if Secure Boot is Enabled,
                                                   Platform Key(PK) is enrolled
  Secure Boot Setting         [Enabled]            and the System is in User
  Secure Boot Policy          [Factory Policy]     mode.
▶ View Secure Boot Keys                            The mode change requires
▶ Secure Boot Custom Policy                        platform reset
```

Figure 1 Enable Secure boot

Enabling Device Guard

This section describes how to enable Device Guard and how to verify that it is working properly.

Device Guard can be enabled in the Group Policy Editor or by using the Device Guard and Credential Guard hardware readiness tool. The readiness tool can be downloaded from:

https://www.microsoft.com/download/details.aspx?id=53337

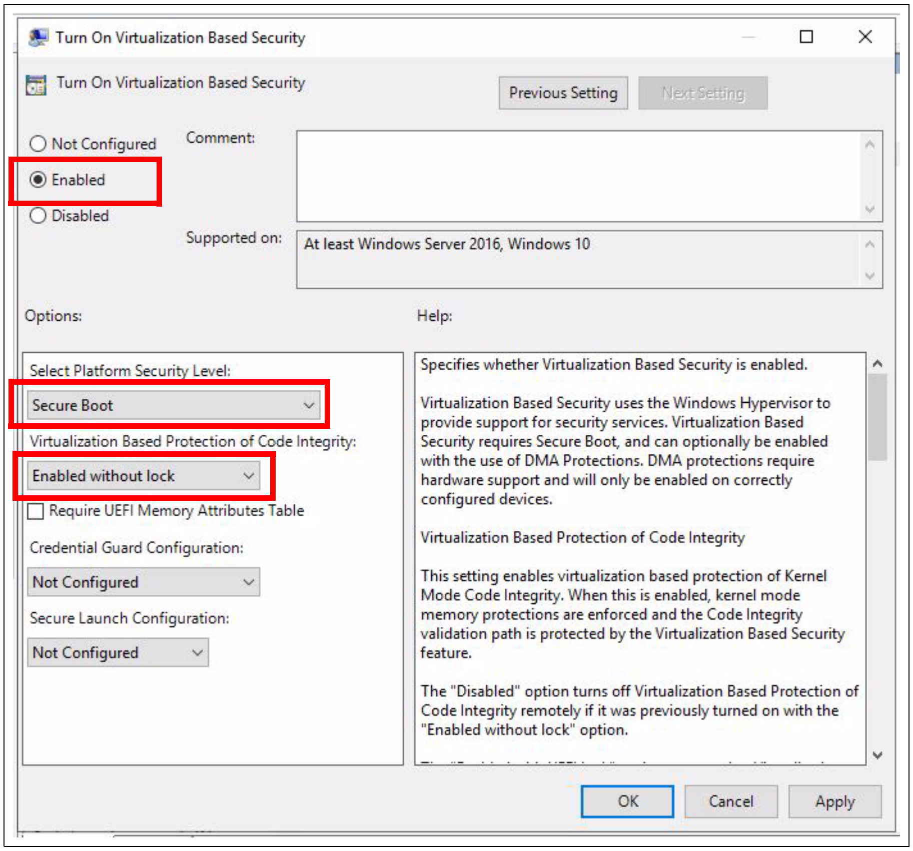
Enabling Device Guard in Group Policy setting

Start **gpedit.msc** in the Run command console to launch Group Policy Management Console and navigate to **Computer Configuration** → **Administrative Templates** → **System** → **Device Guard**.

To turn on Device Guard, perform the following steps, as shown in Figure 2.

1. Edit the policy **Turn On Virtualization Based Security** and choose **Enabled**.
2. For **Select Platform Security Level** choose **Secure boot**.
3. For **Virtualization Based Protection of Code Integrity** choose **Enabled without lock**.

These are shown in Figure 2.


Turn On Virtualization Based Security
Turn On Virtualization Based Security
Previous Setting
Next Setting
Comment:
Options:
Help:
OK
Cancel
Apply

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows Server 2016, Windows 10

Select Platform Security Level: Secure Boot

Virtualization Based Protection of Code Integrity: Enabled without lock

□ Require UEFI Memory Attributes Table

Credential Guard Configuration: Not Configured

Secure Launch Configuration: Not Configured

Specifies whether Virtualization Based Security is enabled.

Virtualization Based Security uses the Windows Hypervisor to provide support for security services. Virtualization Based Security requires Secure Boot, and can optionally be enabled with the use of DMA Protections. DMA protections require hardware support and will only be enabled on correctly configured devices.

Virtualization Based Protection of Code Integrity

This setting enables virtualization based protection of Kernel Mode Code Integrity. When this is enabled, kernel mode memory protections are enforced and the Code Integrity validation path is protected by the Virtualization Based Security feature.

The "Disabled" option turns off Virtualization Based Protection of Code Integrity remotely if it was previously turned on with the "Enabled without lock" option.

Figure 2 Enable Device Guard in Group Policy setting

Enabling Device Guard using the Readiness Tool

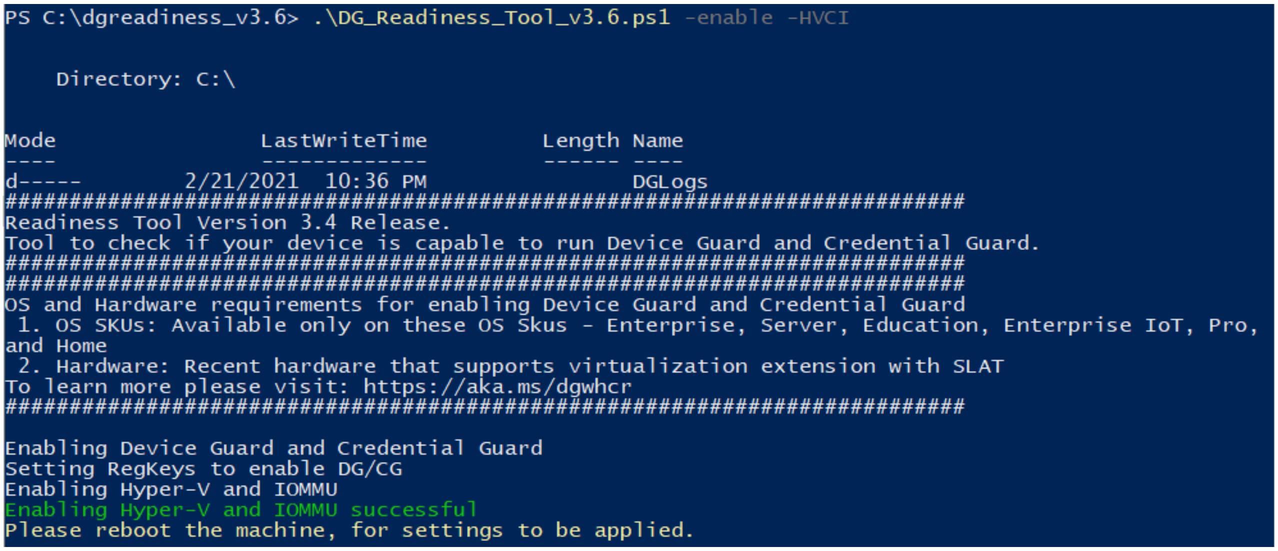
Download Device Guard and Credential Guard hardware readiness tool from:

https://www.microsoft.com/download/details.aspx?id=53337

Open an Administrator PowerShell script, locate the directory into which you unzipped the Readiness Tool and run the following PowerShell command to enable HVCI.

```
PS> .\DG_Readiness_Tool_v3.6.ps1 -enable -HVCI
```

The output of the command is shown in Figure 3.



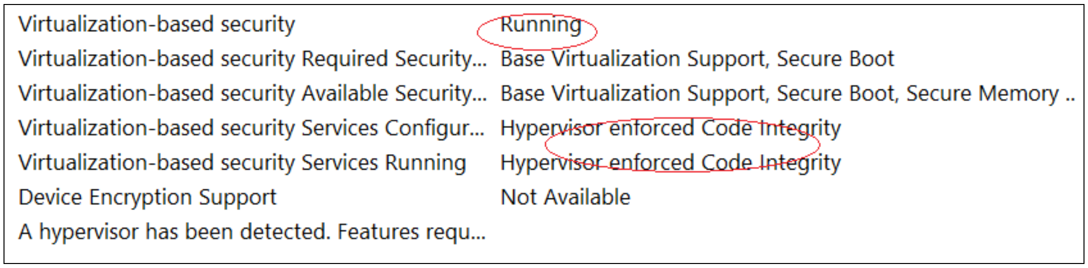
```
PS C:\dgreadiness_v3.6> .\DG_Readiness_Tool_v3.6.ps1 -enable -HVCI


    Directory: C:\


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        2/21/2021  10:36 PM                DGLogs
###########################################################################
Readiness Tool Version 3.4 Release.
Tool to check if your device is capable to run Device Guard and Credential Guard.
###########################################################################
###########################################################################
OS and Hardware requirements for enabling Device Guard and Credential Guard
 1. OS SKUs: Available only on these OS Skus - Enterprise, Server, Education, Enterprise IoT, Pro,
and Home
 2. Hardware: Recent hardware that supports virtualization extension with SLAT
To learn more please visit: https://aka.ms/dgwhcr
###########################################################################

Enabling Device Guard and Credential Guard
Setting RegKeys to enable DG/CG
Enabling Hyper-V and IOMMU
Enabling Hyper-V and IOMMU successful
Please reboot the machine, for settings to be applied.
```

Figure 3 Enable Device Guard by DG_Readiness Tool

Restart the system.

Checking the status of Device Guard in msinfo32

After a system restart, you can check that Device Guard is enabled by running **`MSinfo32`** and checking the bottom of the displayed System Summary page as shown in Figure 4.



Virtualization-based security	Running
Virtualization-based security Required Security...	Base Virtualization Support, Secure Boot
Virtualization-based security Available Security...	Base Virtualization Support, Secure Boot, Secure Memory ..
Virtualization-based security Services Configur...	Hypervisor enforced Code Integrity
Virtualization-based security Services Running	Hypervisor enforced Code Integrity
Device Encryption Support	Not Available
A hypervisor has been detected. Features requ...	

Figure 4 Check Device Guard in msinfo32

You should see the following entries:

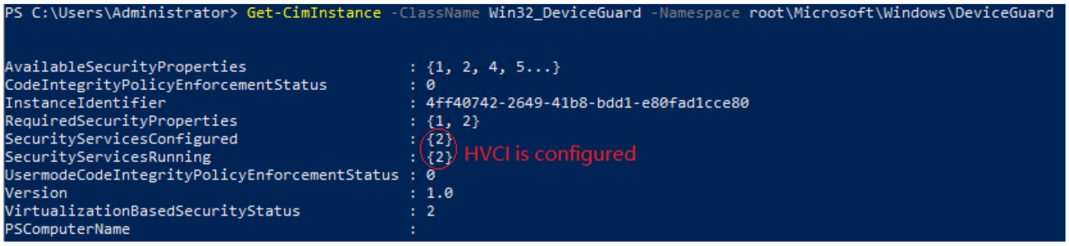
Virtualization-Based Security	**Running**
Virtualization-Based Security Services Configured	**Hypervisor enforced Code Integrity**
Virtualization-Based Security Services Running	**Hypervisor enforced Code Integrity**

Checking the status of Device Guard in PowerShell

In PowerShell, run the following command to verify if Device Guard is enabled or not.

```
PS> Get-CimInstance -ClassName Win32_DeviceGuard -Namespace
root\Microsoft\Windows\DeviceGuard
```

The output is shown in Figure 5.



```
PS C:\Users\Administrator> Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard


AvailableSecurityProperties                  : {1, 2, 4, 5...}
CodeIntegrityPolicyEnforcementStatus         : 0
InstanceIdentifier                           : 4ff40742-2649-41b8-bdd1-e80fad1cce80
RequiredSecurityProperties                   : {1, 2}
SecurityServicesConfigured                   : {2}
SecurityServicesRunning                      : {2}
UsermodeCodeIntegrityPolicyEnforcementStatus : 0
Version                                      : 1.0
VirtualizationBasedSecurityStatus            : 2
PSComputerName                               :
```

HVCI is configured

Figure 5 Check Device Guard by PowerShell command

The output of this command provides details of the available hardware-based security features as well as those features that are currently enabled. Refer to the official website of Microsoft to learn more about each subitem:

https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/enable-virtualization-based-protection-of-code-integrity

Enabling Credential Guard

This section describes how to enable Credential Guard and how to verify that it is working properly.

Credential Guard can be enabled in the Group Policy Editor or by using the Device Guard and Credential Guard hardware readiness tool. The readiness tool can be downloaded from:

https://www.microsoft.com/download/details.aspx?id=53337

Enabling Credential Guard in Group Policy Editor

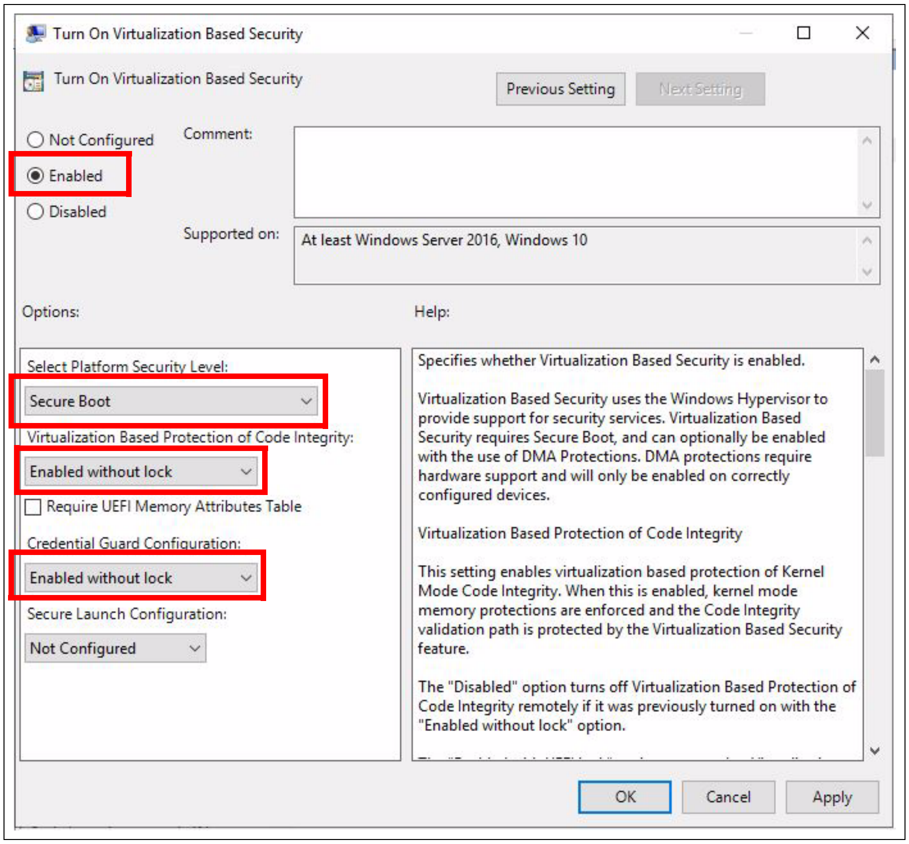
To turn on just Credential Guard, do the following settings:

1. Edit the policy **Turn On Virtualization Based Security** and select **Enabled**.
2. For **Select Platform Security Level**, select **Secure Boot**.
3. For **Virtualization Based Protection of Code Integrity** select **Enabled without lock**.

   Setting this entry to **Enabled without lock** allows virtualization based protection of code integrity to be disabled remotely by using Group Policy.

   Conversely setting it to **Enabled with UEFI lock** ensures that Virtualization Based Protection of Code Integrity cannot be disabled remotely. In order to disable the feature, you must set the Group Policy to **Disabled** as well as remove the security functionality from each computer, with a physically present user, in order to clear con-figuration persisted in UEFI.
4. For **Credential Guard Configuration** select **Enabled without lock**.

These are shown in Figure 6.



Turn On Virtualization Based Security

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2016, Windows 10

Options:

Select Platform Security Level: Secure Boot

Virtualization Based Protection of Code Integrity: Enabled without lock

□ Require UEFI Memory Attributes Table

Credential Guard Configuration: Enabled without lock

Secure Launch Configuration: Not Configured

Help:

Specifies whether Virtualization Based Security is enabled.

Virtualization Based Security uses the Windows Hypervisor to provide support for security services. Virtualization Based Security requires Secure Boot, and can optionally be enabled with the use of DMA Protections. DMA protections require hardware support and will only be enabled on correctly configured devices.

Virtualization Based Protection of Code Integrity

This setting enables virtualization based protection of Kernel Mode Code Integrity. When this is enabled, kernel mode memory protections are enforced and the Code Integrity validation path is protected by the Virtualization Based Security feature.

The "Disabled" option turns off Virtualization Based Protection of Code Integrity remotely if it was previously turned on with the "Enabled without lock" option.

Figure 6 Enable Credential Guard in Group Policy setting

Enabling Credential Guard using the DG_Readiness Tool

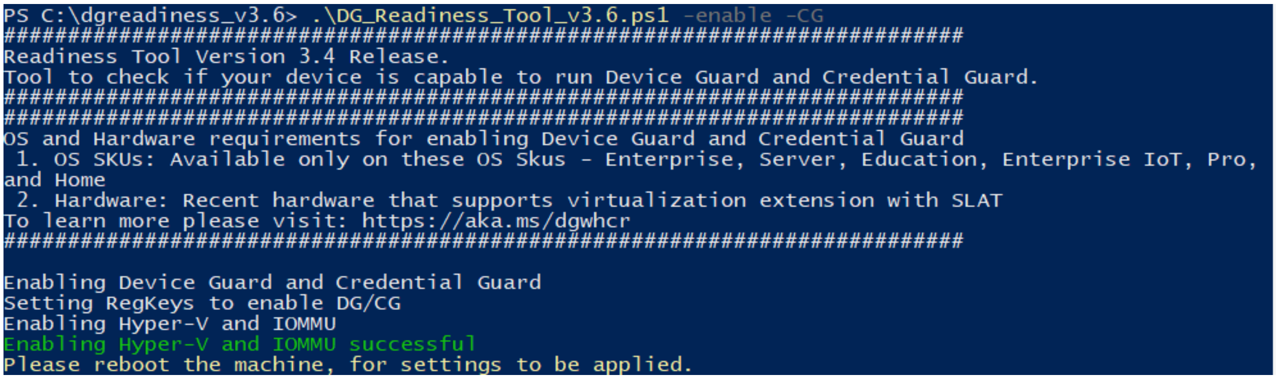
Download Device Guard and Credential Guard hardware readiness tool from:

https://www.microsoft.com/download/details.aspx?id=53337

Open an Administrator PowerShell script, locate the directory into which you unzipped the Readiness Tool and run the following PowerShell command to enable Credential Guard.

```
PS> .\DG_Readiness_Tool_v3.6.ps1 -enable -CG
```

The output of the command is shown in Figure 7. Restart the system to complete the task.

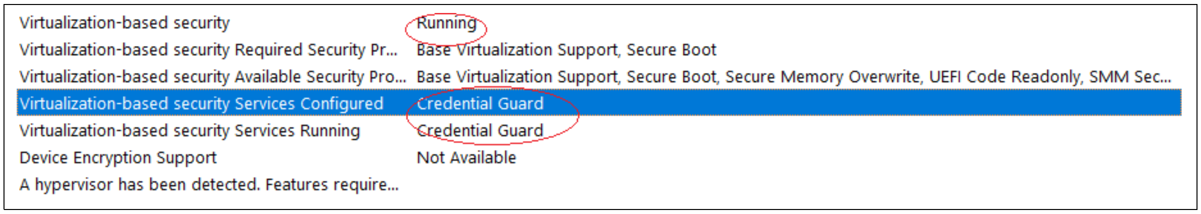


```
PS C:\dgreadiness_v3.6> .\DG_Readiness_Tool_v3.6.ps1 -enable -CG
###########################################################################
Readiness Tool Version 3.4 Release.
Tool to check if your device is capable to run Device Guard and Credential Guard.
###########################################################################
###########################################################################
OS and Hardware requirements for enabling Device Guard and Credential Guard
 1. OS SKUs: Available only on these OS Skus - Enterprise, Server, Education, Enterprise IoT, Pro,
and Home
 2. Hardware: Recent hardware that supports virtualization extension with SLAT
To learn more please visit: https://aka.ms/dgwhcr
###########################################################################

Enabling Device Guard and Credential Guard
Setting RegKeys to enable DG/CG
Enabling Hyper-V and IOMMU
Enabling Hyper-V and IOMMU successful
Please reboot the machine, for settings to be applied.
```

Figure 7 Enable Credential Guard by DG_Readiness Tool

Checking the status of Credential Guard in msinfo32

After a system restart, you can check that Credential Guard is enabled by running **`MSinfo32`** and checking the bottom of the displayed System Summary page as shown in Figure 8.



Virtualization-based security	Running
Virtualization-based security Required Security Pr...	Base Virtualization Support, Secure Boot
Virtualization-based security Available Security Pro...	Base Virtualization Support, Secure Boot, Secure Memory Overwrite, UEFI Code Readonly, SMM Sec...
Virtualization-based security Services Configured	Credential Guard
Virtualization-based security Services Running	Credential Guard
Device Encryption Support	Not Available
A hypervisor has been detected. Features require...	

Figure 8 Check Credential Guard in msinfo32

You should see the following entries:

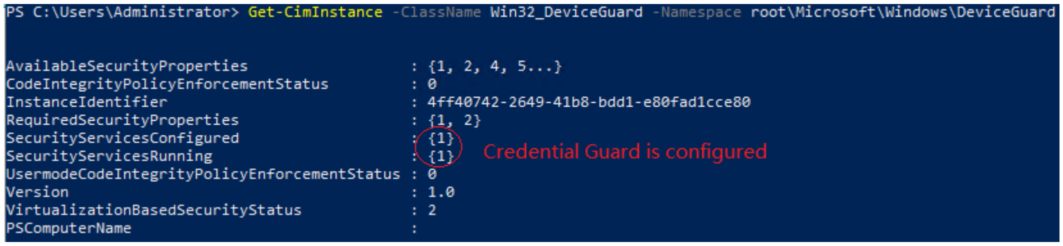
Virtualization-Based Security	**Running**
Virtualization-Based Security Services Configured	**Credential Guard**
Virtualization-Based Security Services Running	**Credential Guard**

Checking the status of Credential Guard by PowerShell command

In PowerShell, run the following command to verify if Credential Guard is enabled or not:

```
PS> Get-CimInstance -ClassName Win32_DeviceGuard -Namespace
root\Microsoft\Windows\DeviceGuard
```

The output is shown in Figure 9.



```
PS C:\Users\Administrator> Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard


AvailableSecurityProperties                  : {1, 2, 4, 5...}
CodeIntegrityPolicyEnforcementStatus         : 0
InstanceIdentifier                           : 4ff40742-2649-41b8-bdd1-e80fad1cce80
RequiredSecurityProperties                   : {1, 2}
SecurityServicesConfigured                   : {1}
SecurityServicesRunning                      : {1}
UsermodeCodeIntegrityPolicyEnforcementStatus : 0
Version                                      : 1.0
VirtualizationBasedSecurityStatus            : 2
PSComputerName                               :
```

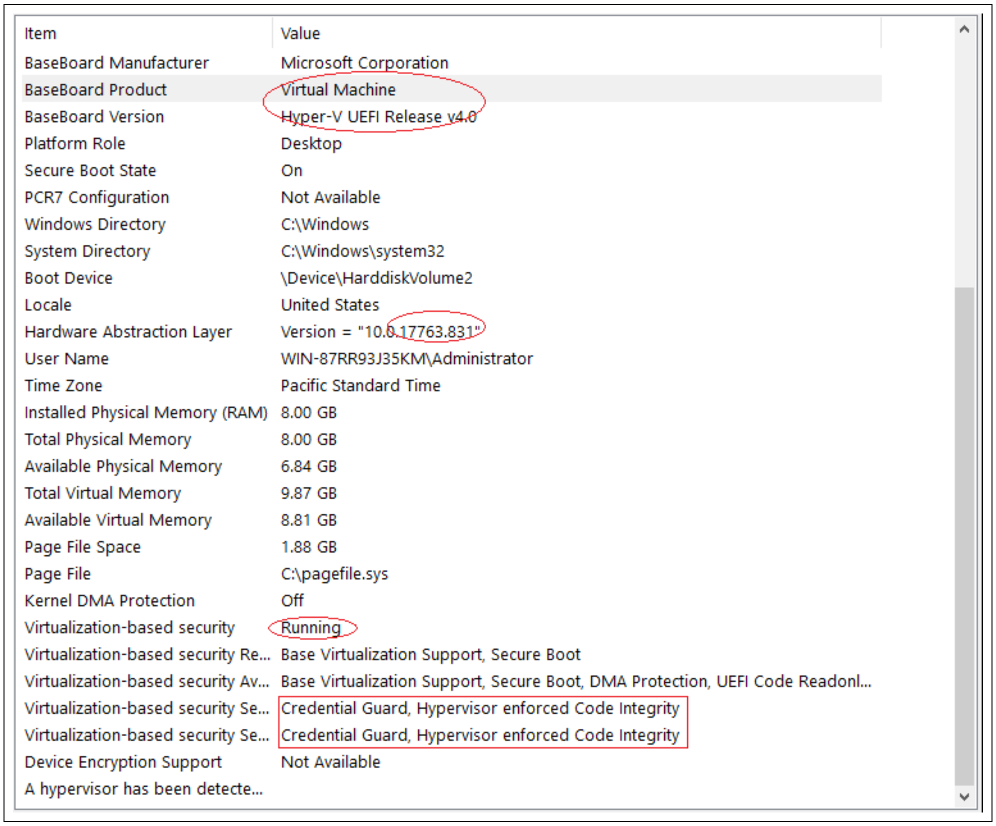
Credential Guard is configured

Figure 9 Check Credential Guard by PowerShell command

Deploying Device Guard and Credential Guard in a VM

Both Device Guard and Credential Guard can protect a Hyper-V virtual machine, just as they do on a physical machine. To implement these two features on VM, the Hyper-V virtual machine must be Generation 2. You can check requirements for running HVCI in Hyper-V virtual machines.

Figure 10 shows a VM running both DG and CG on a supported host. In this VM, both DG and CG are enabled in Group Policy.



Item	Value
BaseBoard Manufacturer	Microsoft Corporation
BaseBoard Product	Virtual Machine
BaseBoard Version	Hyper-V UEFI Release v4.0
Platform Role	Desktop
Secure Boot State	On
PCR7 Configuration	Not Available
Windows Directory	C:\Windows
System Directory	C:\Windows\system32
Boot Device	\Device\HarddiskVolume2
Locale	United States
Hardware Abstraction Layer	Version = "10.0.17763.831"
User Name	WIN-87RR93J35KM\Administrator
Time Zone	Pacific Standard Time
Installed Physical Memory (RAM)	8.00 GB
Total Physical Memory	8.00 GB
Available Physical Memory	6.84 GB
Total Virtual Memory	9.87 GB
Available Virtual Memory	8.81 GB
Page File Space	1.88 GB
Page File	C:\pagefile.sys
Kernel DMA Protection	Off
Virtualization-based security	Running
Virtualization-based security Re...	Base Virtualization Support, Secure Boot
Virtualization-based security Av...	Base Virtualization Support, Secure Boot, DMA Protection, UEFI Code Readonl...
Virtualization-based security Se...	Credential Guard, Hypervisor enforced Code Integrity
Virtualization-based security Se...	Credential Guard, Hypervisor enforced Code Integrity
Device Encryption Support	Not Available
A hypervisor has been detecte...	

Figure 10 Check Device Guard and Credential Guard on VM in msinfo32

Lenovo ThinkSystem server support

Support for Device Guard and Credential Guard requires the processor to support Secure Boot and it be enabled in UEFI. The server also needs to support Windows Server 2019.

Lenovo OSIG lists all the ThinkSystem servers that support Windows Server 2019:

https://lenovopress.com/osig#server_families=thinksystem&os_families=microsoft-windows-server&os_versions=windows-server-2019&support=all

References

- Microsoft web page for Virtualization-based Security (VBS)

  https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-vbs

- Microsoft web page for virtualization-based protection of code integrity

  https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/introduction-to-device-guard-virtualization-based-security-and-windows-defender-application-control

- Microsoft web page for Credential Guard https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-how-it-works

- Microsoft web page for Device Guard and Credential Guard Demystified

  https://techcommunity.microsoft.com/t5/iis-support-blog/windows-10-device-guard-and-credential-guard-demystified/ba-p/376419

- Lenovo OS Interoperability Guide:

  https://lenovopress.com/osig

Author

Guiqing Li is a Windows Engineer working in the Lenovo Infrastructure Solutions Group based in Beijing, China. She has more than ten years of experience with driver development, and four years of experience with Windows debugging.

Special thanks to the following specialist for their contributions and suggestions:

- Gary Cudak, Lenovo OS architect for OS Enablement and Preload
- Boyong Li, Lenovo Windows Engineer for Windows Enablement
- Amy Gou, Lenovo Assurance Engineer for OS Certification
- David Watts, Lenovo Press

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

This document was created or updated on June 3, 2021.

Send us your comments via the **Rate & Provide Feedback** form found at
http://lenovopress.com/lp1486

Trademarks