

The Lenovo logo is displayed in white text on a black rectangular background.

Enabling the Secured-Core Feature of Microsoft Windows Server 2022 and Azure Stack HCI on Lenovo ThinkSystem Servers

Introduces the Secured-core feature of Windows Server 2022 and Azure Stack HCI

Lists which Lenovo servers support Secured-core

Describes how to enable Secured-core on ThinkSystem servers

Shows how to check the status of Secured-core

Guiqing Li
Hussein Jammal
Laurentiu Petre



Abstract

Secured-core is a new feature of Microsoft Windows Server 2022 and Microsoft Azure Stack HCI that brings powerful threat protections together to provide multi-layer security across hardware, firmware, and the operating system. It uses the Trusted Platform Module 2.0 and System Guard to boot up Windows Server securely and minimize risks from firmware vulnerabilities.

To be certified for Secured-core, new server firmware protection features are required. ThinkSystem servers with 3rd Gen or 4th Gen Intel Xeon Scalable processors and AMD EPYC 7003 or 7004 Series processors are certified.

This document introduces Secured-core feature, and shows users how to enable it on supported Lenovo® ThinkSystem servers. This paper is intended for IT specialists and IT administrators who are familiar with security features of Windows Server and want to enable Secured-core on applicable Lenovo servers running Windows Server 2022.

At Lenovo Press, we bring together experts to produce technical publications around topics of importance to you, providing information and best practices for using Lenovo products and solutions to solve IT challenges.

See a list of our most recent publications at the Lenovo Press web site:

<http://lenovopress.com>

Do you have the latest version? We update our papers from time to time, so check whether you have the latest version of this document by clicking the **Check for Updates** button on the front page of the PDF. Pressing this button will take you to a web page that will tell you if you are reading the latest version of the document and give you a link to the latest if needed. While you're there, you can also sign up to get notified via email whenever we make an update.

Contents

Introduction	3
Supported Lenovo servers	6
Enabling Secured-core in UEFI	7
Platform-specific driver installation in Windows Server 2022 for AMD-based system	11
Enabling Secured-core in Windows Server 2022.	12
Confirming Secured-core is enabled	15
Enabling Secured-core in Azure Stack HCI	17
Resources	20
Change history	21
Author	21
Notices	22
Trademarks	23

Introduction

A certified Secured-core server takes full advantage of hardware, firmware, driver, and operating system capabilities to enable advanced Windows Server 2022 security features to further protect the operating environment from the boot process through to data in memory.

The protections enabled by a Secured-core server are targeted to create a secure platform for critical applications and sensitive data used on that server and provide further assurance that the hypervisor or the operating system has not been tampered with and access to data in memory is protected.

The Secured-core functionality is built on the following distinct security components:

- ▶ Hardware root-of-trust with TPM 2.0
- ▶ Firmware Protection with DRTM
- ▶ Windows System Guard
- ▶ Virtualization-based Security (VBS)

These are discussed in the following sections.

Tip: Secured-core was first introduced in Windows Server 2022, and is a combination of security features implemented in hardware, firmware, driver and the operating system. However, there is no actual feature named “Secured-core”; instead, it is just a group of security-related settings in UEFI and in Windows that are enabled.

Azure Stack HCI OS “22H2” Kernel is based on Windows Server 2022. HCI OS contains additional HCI Cloud capabilities not found in Windows Server. This distinction is particularly important when looking for appropriate device drivers. Since Lenovo does not designate distinct drivers for the HCI OSes, for HCI OS 22H2, it uses drivers designated for Windows Server 2022.

To be certified for Secured-core, new server firmware protection features are required. ThinkSystem servers with 3rd Gen or 4th Gen Intel Xeon Scalable processors and AMD EPYC 7003 or 7004 Series processors are certified.

Hardware root-of-trust with TPM 2.0

Trusted Platform Module 2.0 (TPM 2.0) comes standard with Secured-core servers. A TPM 2.0 chip can check the integrity of the UEFI and firmware of the devices, comparing it to the information that has been burned into the chip by Lenovo during manufacturing.

This Secure Boot capability ensures that no unauthorized firmware or software has been loaded before the OS. It gives customers a secure store for sensitive keys and data during early boot process and the isolations from software-based attacks. This hardware root-of-trust provides a hardware level verification that the rest of the operating system and applications can rely on.

Figure 1 steps through a trusted boot process in which UEFI uses TPM to measure initial BIOS, Option ROMs, device drivers, and OS components prior to their execution by checking data integrity, consistent of PCR values or hash values. The boot process ensures that, when the OS loads and the user logs in, the system is trusted.

Tip: Measured boot is a way for OS to record the chain of measurements of software components and configuration information in the TPM through the initialization of the Windows operating system.

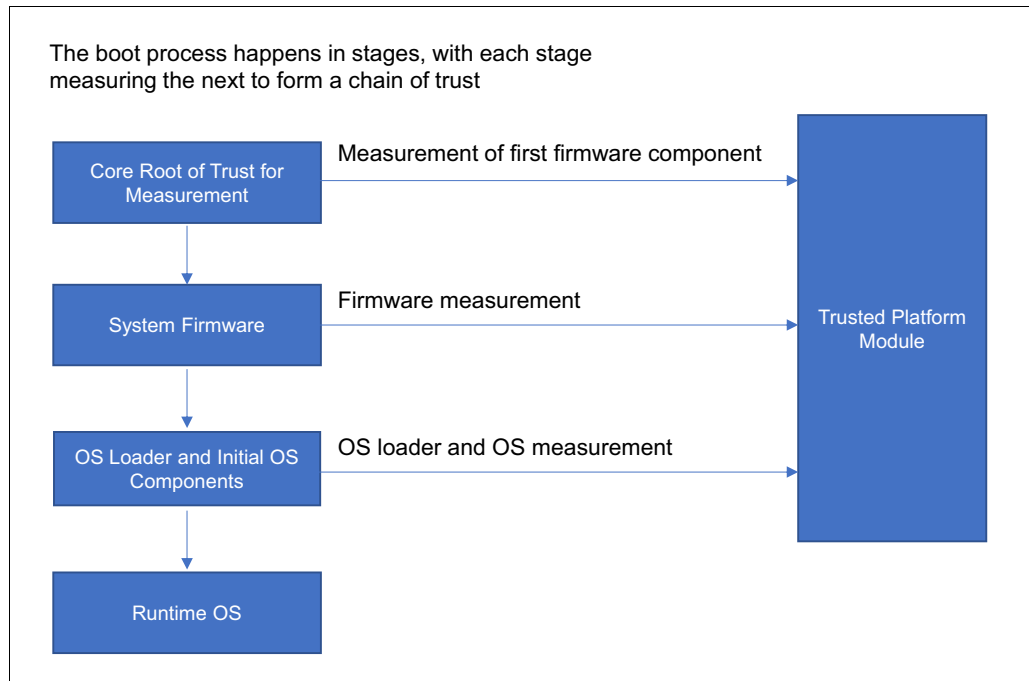


Figure 1 How Windows uses the Trusted Platform Module for measured boot

Firmware protection with DRTM

Firmware executes with high privileges and is often invisible to traditional anti-virus solutions, which has given rise to numbers of firmware-based attacks. Attackers compromise the boot flow to achieve low-level malware behavior that is hard to detect, posing a significant risk to systems.

To keep the server's firmware and hardware trustworthy and healthy, the server should be able to detect and block malicious software that runs before the operating system initializes or during the boot process itself.

There are two techniques to measure early boot UEFI components:

- ▶ Static Root of Trust for Measurement (SRTM)

SRTM provides a fixed piece of trusted code in the UEFI that is loaded at the start of the entire booting chain. SRTM has some shortcomings, however: the SRTM flow is brittle that a minor change can invalidate the chain of trust, and SRTM gives only the load time guarantee but not the run time guarantee for the launched environment.

- ▶ Dynamic Root of Trust for Measurement (DRTM)

DRTM is a trust mechanism using Intel's Trusted Execution Technology (TXT) or AMD's SKINIT technology to provide run time protection and guarantee. In contrast with the SRTM, DRTM has the advantage that the launch of the measured environment can occur at any time without resorting to a platform reset.

By leveraging built-in silicon instructions or firmware enclaves, DRTM allows the system to freely boot into untrusted code initially, but shortly after launches the system into a trusted state by taking control of all CPUs and forcing untrusted, exploitable code down a specific and measured code path before launching into a trusted state. Then the control of the DRTM environment is transferred to the Hypervisor and OS. The boot chain of trust is setup finally, then hypervisor or OS kernel can be booted securely.

Figure 2 shows the DRTM process works to secure the system.

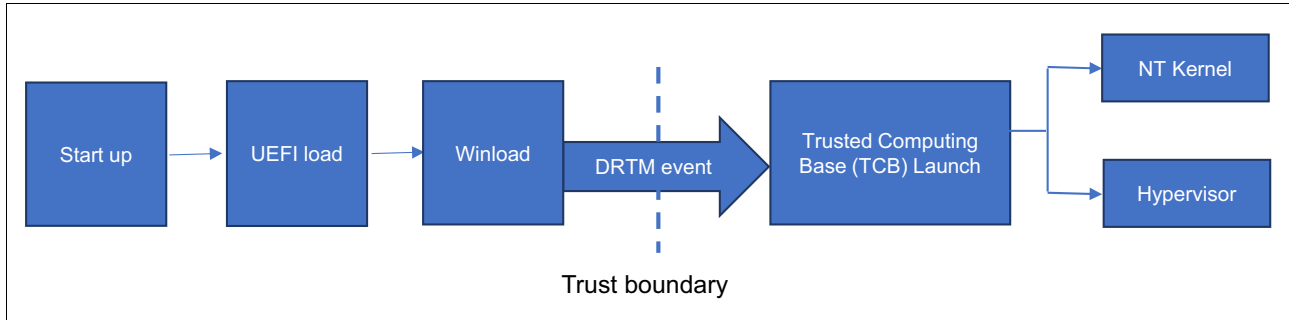


Figure 2 Using DRTM to securely launch Hypervisor and OS

System Guard with Kernel DMA protection

PCIe devices are direct memory-addressing (DMA)-capable, which means they have direct access to read and write system memory, without having to involve the system processor in these operations. This DMA capability makes PCIe devices the highest performing devices, however, having PCI hot-plug devices (such as NVMe hot-swap drives) externally and easily accessible also means unattended device could have a malicious PCIe device plugged into it, which could read the system memory or load malicious code into it, with no protection.

This kind of “drive-by DMA attacks” using PCIe hot plug devices can lead to the disclosure of sensitive information residing on a system, or even the injection of malware that allows attackers to bypass the lock screen or control the system remotely. Kernel DMA Protection is the feature designed to protect the system against this type of attack.

Windows makes use of the system Input/Output Memory Management Unit (IOMMU) to block external peripherals from starting and performing DMA unless the drivers for these peripherals support memory isolation, such as DMA-remapping. DMA remapping restricts the device to a certain pre-assigned memory region, which confirms the device is allocated a clear space of memory to perform its functions and doesn't have access to any other information stored in system memory. Devices whose drivers are incompatible with DMA remapping are prevented from direct memory access by default until an authorized user is logged onto the system.

Kernel DMA Protection requires the support from the processor, new UEFI firmware, and drivers. With this feature, the OS and the system firmware protect the system against malicious and unintended DMA attacks for all DMA-capable devices. Currently this feature is only available on ThinkSystem servers with 3rd Gen Intel Xeon Scalable processors and AMD EPYC 7003 Series processors. ThinkSystem servers with newer processors are also planned to support the feature. Kernel DMA Protection only protects against drive-by DMA attacks after the OS is loaded.

Virtualization-based Security (VBS) support

Secured-core servers support virtualization-based security (VBS) features and Hypervisor-protected code integrity (HVCI) so as to leverage virtualization capabilities from hardware and the hypervisor to provide additional protection for critical subsystems and data.

VBS uses hardware virtualization features to create and isolate a secure region of memory from the normal operating system. VBS runs this separate secure kernel at a higher trust level than the actual Windows system kernel. Then the OS kernel and user-mode processes cannot access the protected functions and data directly, thus protecting them from malware infection. VBS also allows for the use of Credential Guard to provide preventative defense for sensitive assets like credentials.

Hypervisor-based code integrity (HVCI) uses VBS to check the integrity of kernel mode drivers and binaries before they are started and prevents unsigned drivers or system files from being loaded into system memory. Enabled with HVCI, a Secured-core server only starts executables signed by known and approved authorities. This ensures that code running within the trusted computing base runs with integrity and is not subject to exploits or attacks.

Supported Lenovo servers

For Secured-core support, the servers must meet certain baseline hardware, firmware and software requirements. At the time of writing, the following Lenovo ThinkSystem servers and ThinkAgile™ MX system are certified as supporting Secured-core with Windows Server 2022:

- ▶ ThinkAgile MX3530
- ▶ ThinkAgile MX3531
- ▶ ThinkAgile MX630 V3
- ▶ ThinkAgile MX630 V3 CN
- ▶ ThinkAgile MX630 V3 IS
- ▶ ThinkAgile MX650 CN
- ▶ ThinkAgile MX650 IS
- ▶ ThinkAgile MX650 V3
- ▶ ThinkEdge SE350 V2
- ▶ ThinkEdge SE360 V2
- ▶ ThinkEdge SE450
- ▶ ThinkEdge SE455 V3
- ▶ ThinkServer DN8848 V2
- ▶ ThinkServer SR590 V2
- ▶ ThinkSystem SD630 V2
- ▶ ThinkSystem SD650 V2
- ▶ ThinkSystem SN550 V2
- ▶ ThinkSystem SR250 V2
- ▶ ThinkSystem SR258 V2
- ▶ ThinkSystem SR630 V2
- ▶ ThinkSystem SR630 V3
- ▶ ThinkSystem SR635
- ▶ ThinkSystem SR635 V3
- ▶ ThinkSystem SR645
- ▶ ThinkSystem SR645 V3
- ▶ ThinkSystem SR650 V2
- ▶ ThinkSystem SR650 V3
- ▶ ThinkSystem SR655
- ▶ ThinkSystem SR655 V3

- ▶ ThinkSystem SR665
- ▶ ThinkSystem SR665 V3
- ▶ ThinkSystem SR670 V2
- ▶ ThinkSystem ST250 V2
- ▶ ThinkSystem ST258 V2
- ▶ ThinkSystem ST50 V2
- ▶ ThinkSystem ST58 V2
- ▶ ThinkSystem ST650 V2

To get the current list of certified Lenovo server, go to the Windows Server Catalog:

<https://www.windowsservercatalog.com/results.aspx?&bCatID=1333&cpID=23292&avc=132&ava=0&avt=0&avq=140&OR=1&PGS=25>

Enabling Secured-core in UEFI

This section describes the UEFI settings to enable the Secured-core feature on ThinkSystem servers.

To enable Secured-core, you need the support from the UEFI firmware, so ensure the firmware version installed in your system can fulfill this requirement. The recommendation is to use the latest UEFI firmware version for your server to get Secured-core support.

For the latest UEFI firmware for ThinkSystem, go to the Lenovo support site:

<https://datacentersupport.lenovo.com/us/en/products/servers/thinksystem>

For ThinkServer SR590 V2 and DN8848 V2, use the following site:

<https://datacentersupport.lenovo.com/cn/zc>

For ThinkAgile MX3530 and MX3531, use the guidance in the Best Recipe document from Lenovo site:

<https://datacentersupport.lenovo.com/us/en/products/solutions-and-software/thinkagile-mx>

For ThinkEdge SE450, go to the Lenovo support site:

<https://datacentersupport.lenovo.com/us/en/products/servers/thinkedge>

Enabling Secured-core in UEFI for Intel-based system

To support Secured-core for Intel-based systems, you will need to set the following UEFI items.

1. Enable Secure boot in UEFI settings via **System Settings** → **Security** → **Secure Boot Configurations** → **Secure Boot** as shown in Figure 3.

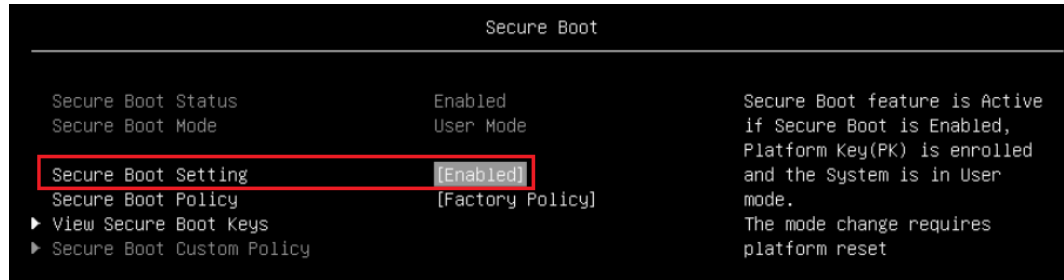


Figure 3 Enable Secure boot

2. Enable TPM 2.0 in UEFI settings via **System Settings** → **Security** → **Secure Boot Configurations** → **Trusted Platform Module** → **TPM 2.0** as shown in Figure 4.

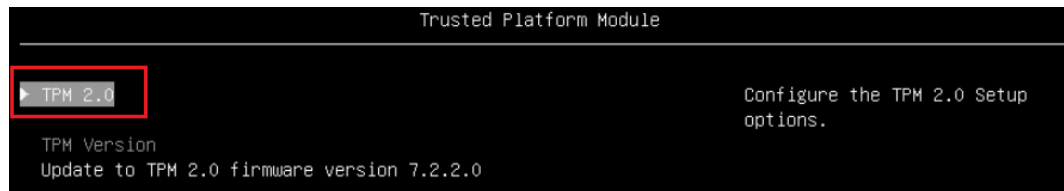


Figure 4 Enable TPM 2.0

3. Enable Intel TXT in UEFI settings via **System Information** → **Socket Configuration** → **Processor Configuration** → **Enable Intel TXT** as shown in Figure 5.

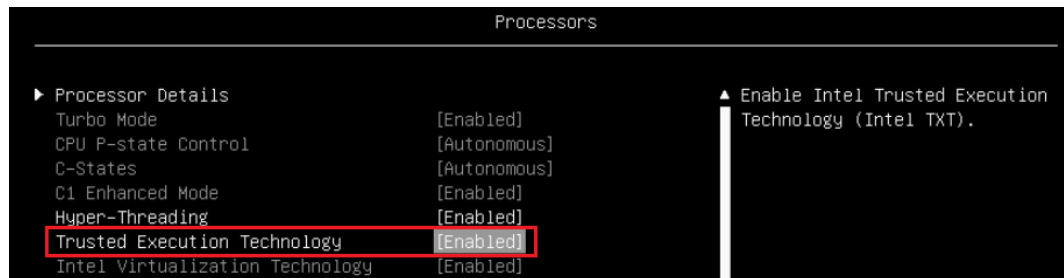


Figure 5 Enable Intel TXT

4. Enable Intel VT-d and DMA protection in UEFI settings via **System Setting** → **Devices and I/O Ports** → **Intel VT for Directed I/O (VT-d)** and **System Setting** → **Devices and I/O Ports** → **DMA Control Opt-In Flag** as shown in Figure 6.

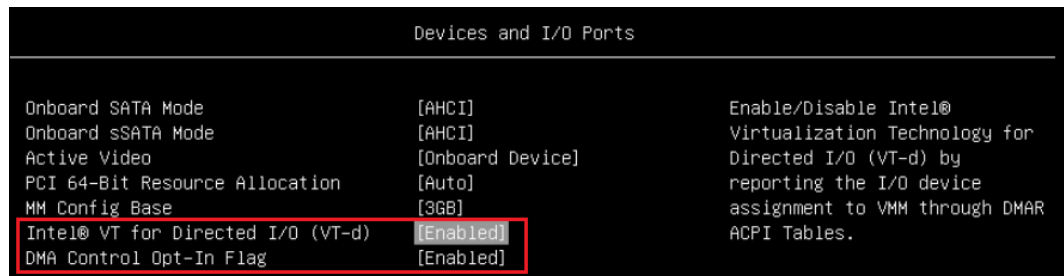


Figure 6 Enable Intel VT-d and DMA protection

Enabling Secured-core in UEFI for AMD-based 1-socket system

AMD EPYC 7003 Series processors support Secured-core however EPYC 7002 Series do not. Lenovo ThinkSystem SR635 and SR655 feature both AMD EPYC 7002 and AMD EPYC 7003 families of processors. To enable Secured-core on Lenovo SR635 and SR655, you'd make sure your processors are AMD EPYC 7003, not AMD EPYC 7002.

To support Secured-core for AMD-based 1-socket system, you will need to set the following UEFI items.

1. Enable Secure boot in UEFI settings via **System Configuration and Boot Management** → **Security** → **Secure Boot** as shown in Figure 7 on page 9.

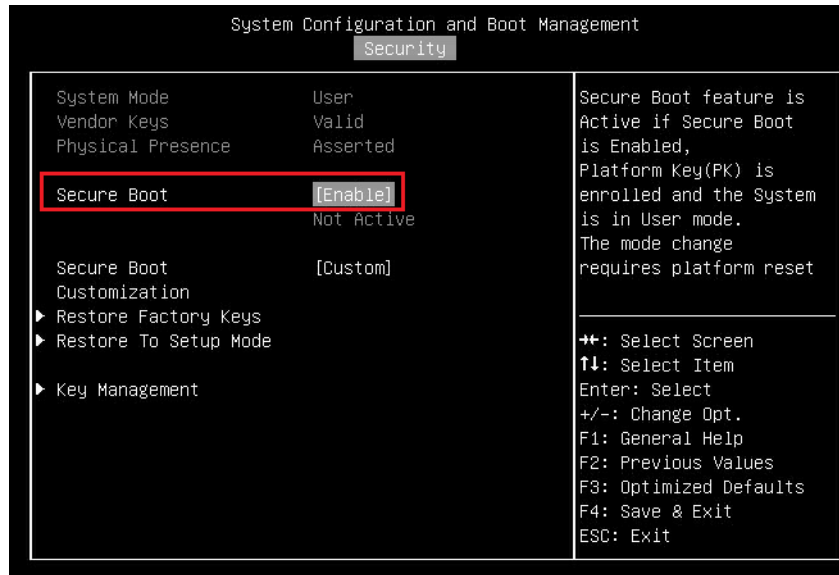


Figure 7 Enable Secure Boot for AMD-based 1-socket system

2. Enable TPM 2.0 in UEFI settings via **System Configuration and Boot Management** → **Security** → **Trusted Computing** as shown in Figure 8.

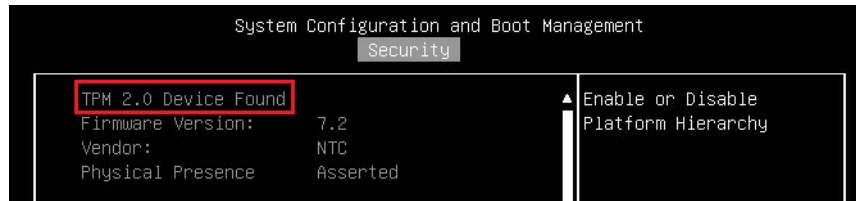


Figure 8 Enable TPM 2.0 for AMD-based 1-socket system

3. Enable Secured-Core in UEFI settings via **System Configuration and Boot Management Socket Configuration** → **Advanced** → **CPU Configuration** → **Secured-Core** as shown in Figure 9.

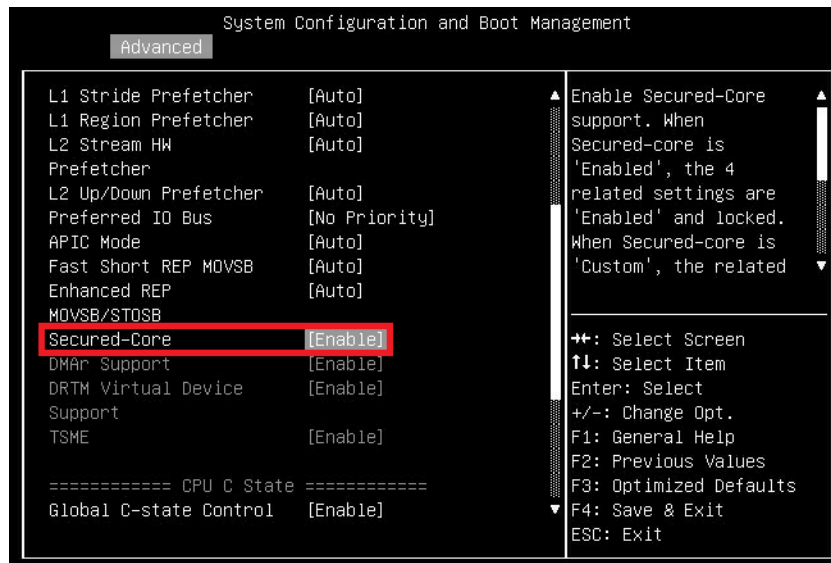


Figure 9 Enable Secured-core for AMD-based 1-socket system

Enabling Secured-core in UEFI for AMD-based 2-socket system

Like Lenovo ThinkSystem SR635 and SR655, ThinkSystem SR645 and SR665 also feature both AMD EPYC 7002 and AMD EPYC 7003 families of processors. To enable Secured-core on Lenovo SR645 and SR665, you'd make sure your processors are belong to AMD EPYC 7003, not AMD EPYC 7002.

To support Secured-core for AMD-based 2-socket system, you will need to set the following UEFI items.

1. Enable Secure boot in UEFI settings via **System Settings** → **Security** → **Secure Boot Configurations** → **Secure Boot Setting** as shown in Figure 10.



Figure 10 Enable Secure Boot for AMD-based 2-socket system

2. Enable TPM 2.0 in UEFI settings via **System Settings** → **Security** → **Secure Boot Configurations** → **Trusted Platform Module** → **TPM 2.0** as shown in Figure 11.

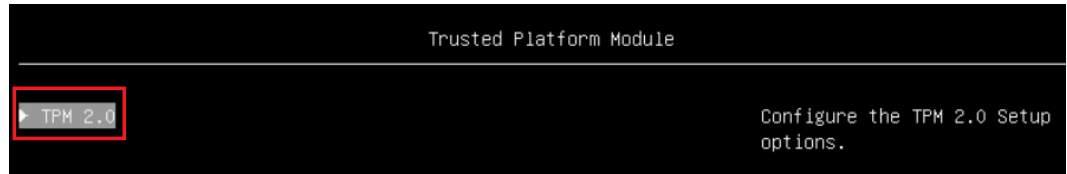


Figure 11 Enable TPM 2.0 for AMD-based 2-socket system

3. Enable Secured-Core in UEFI settings via **System Settings** → **Processors** → **Secured-Core** → **Secured-Core** as shown in Figure 12.

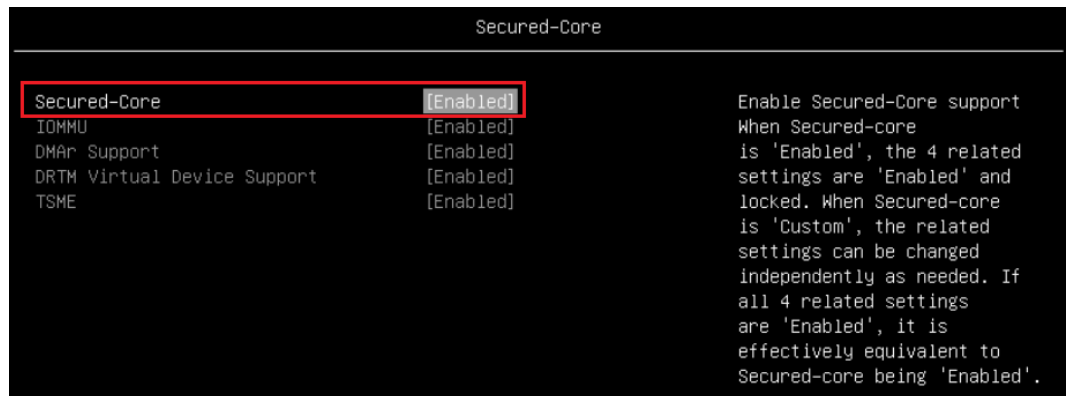


Figure 12 Enable Secured-core for AMD-based 2-socket system

Platform-specific driver installation in Windows Server 2022 for AMD-based system

To support Secured-core on AMD-based system, after UEFI setting is ready we should install platform specific driver. Take example for SR665, to get the latest chipset driver in Windows Server 2022, download it from the Lenovo support site:

<https://datacentersupport.lenovo.com/us/en/products/servers/thinksystem/sr665/downloads/driver-list/>

Then install this chipset driver in Windows Server 2022. After the driver is installed successfully, AMD EPYC DRTM Driver should be found in device manager as shown in Figure 13.

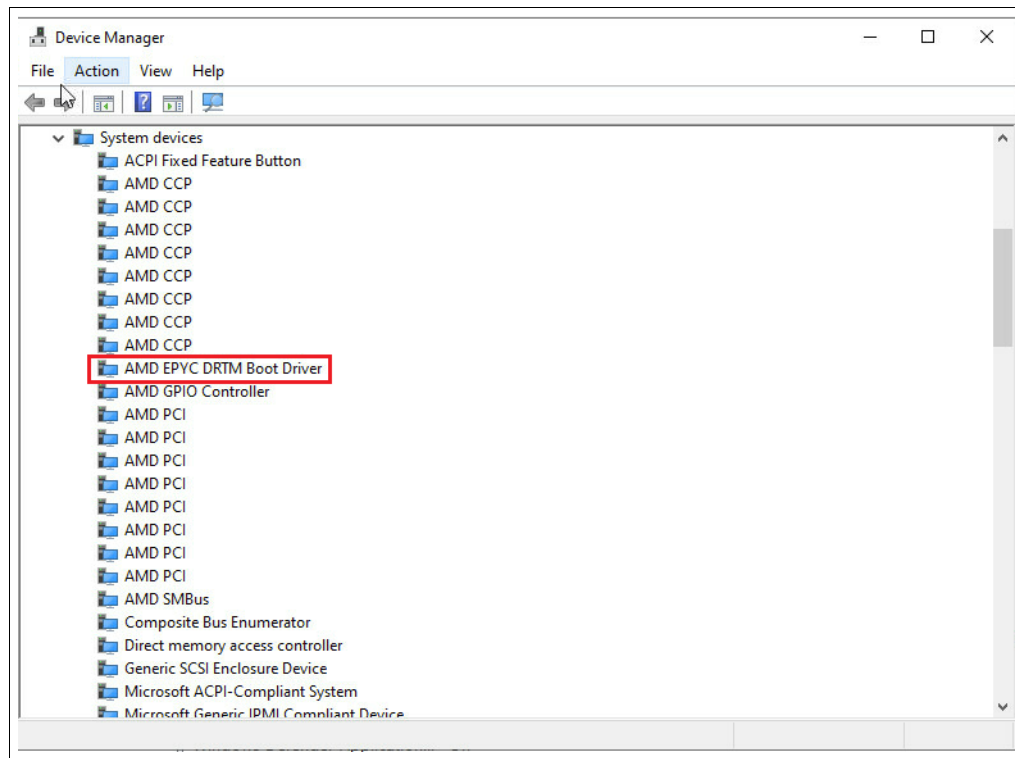


Figure 13 DRTM driver is installed successfully for AMD-based system

Make sure UEFI setting is ready for Secured-core before installing chipset driver on AMD-based system because this driver depends on Secured-core setting in UEFI.

For Intel-based system, no platform specific driver needs to be installed for Secured-core.

Enabling Secured-core in Windows Server 2022

After the UEFI settings are enabled for Secured-core support and the platform-specific driver installation for AMD-based system is successful, you will need to enable settings in the operating system.

There are two ways to set up the Secured-core in Windows Server 2022:

- ▶ “Enabling Secured-core using the Windows Security GUI”
- ▶ “Enabling Secured-core using PowerShell commands” on page 15

Enabling Secured-core using the Windows Security GUI

To enable Secured-core by using the Windows Security App (Windows Server with Desktop experience only), perform the following steps:

1. Launch the Windows Security app from the Start menu, Figure 14.

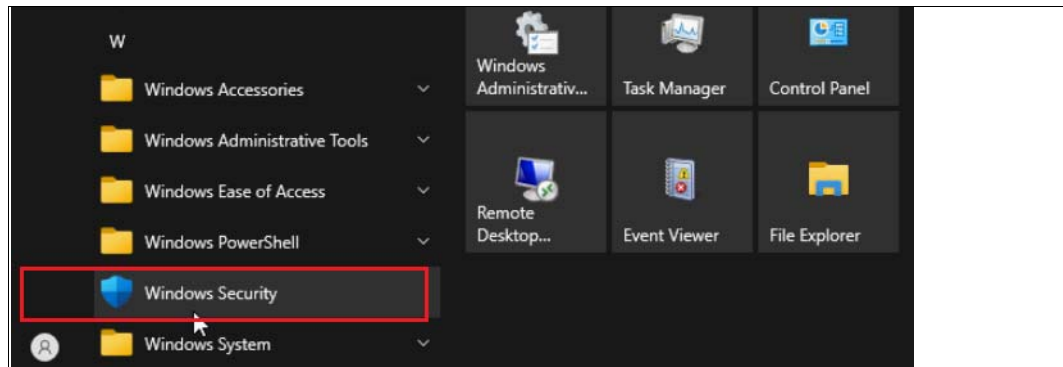


Figure 14 Launch Windows Security App

2. Choose **Device security**, Figure 15.

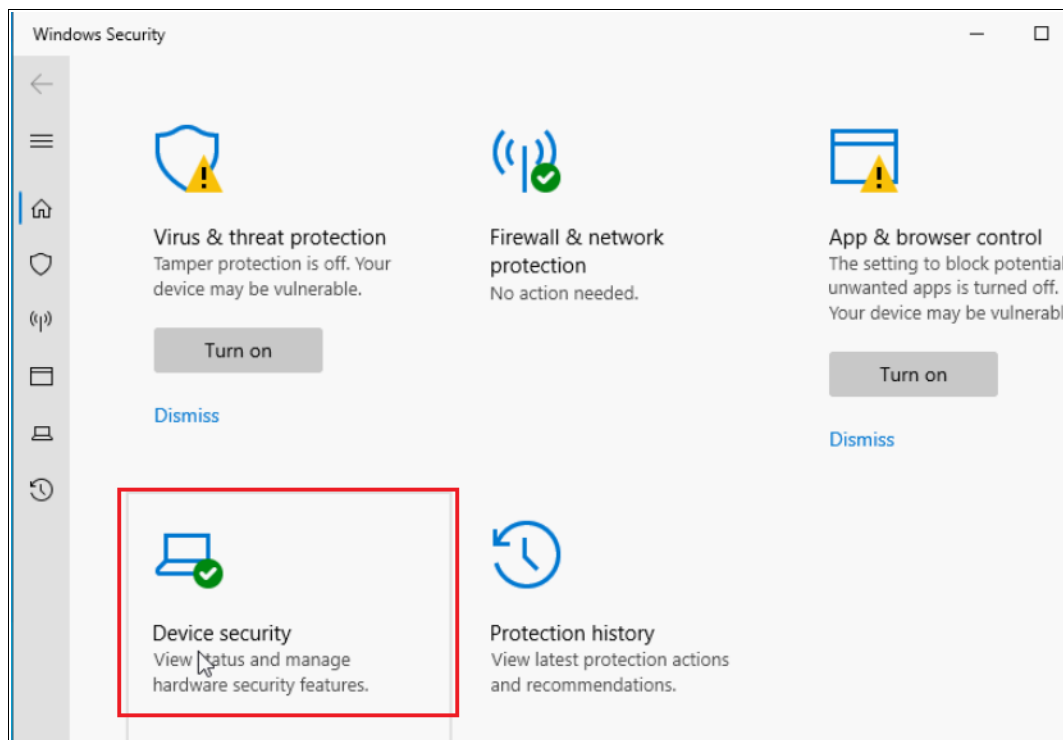


Figure 15 Device security

3. Click **Core isolation details** as shown in Figure 16.

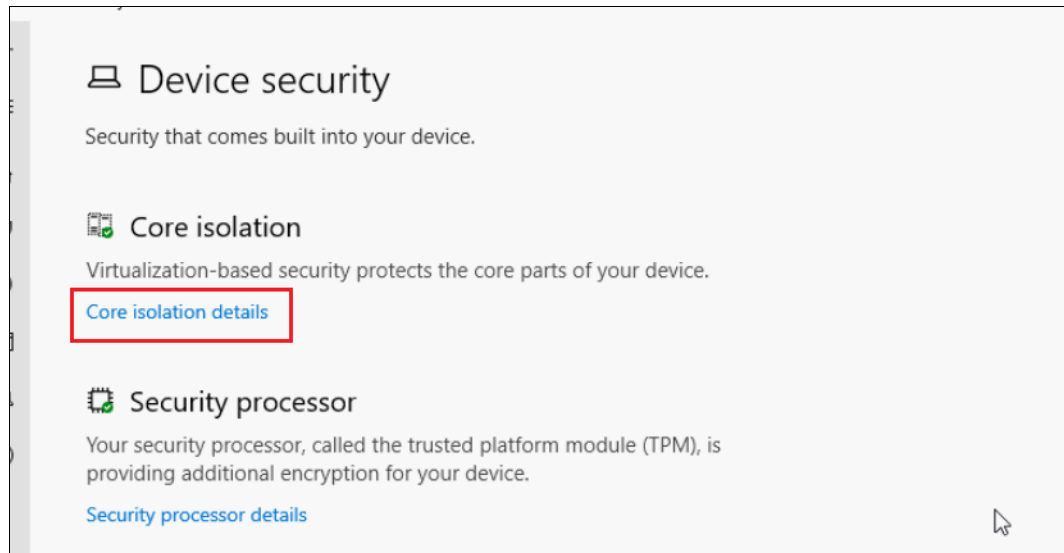


Figure 16 Core isolation details

4. Set both **Memory integrity** and **Firmware protection** to On, Figure 17.

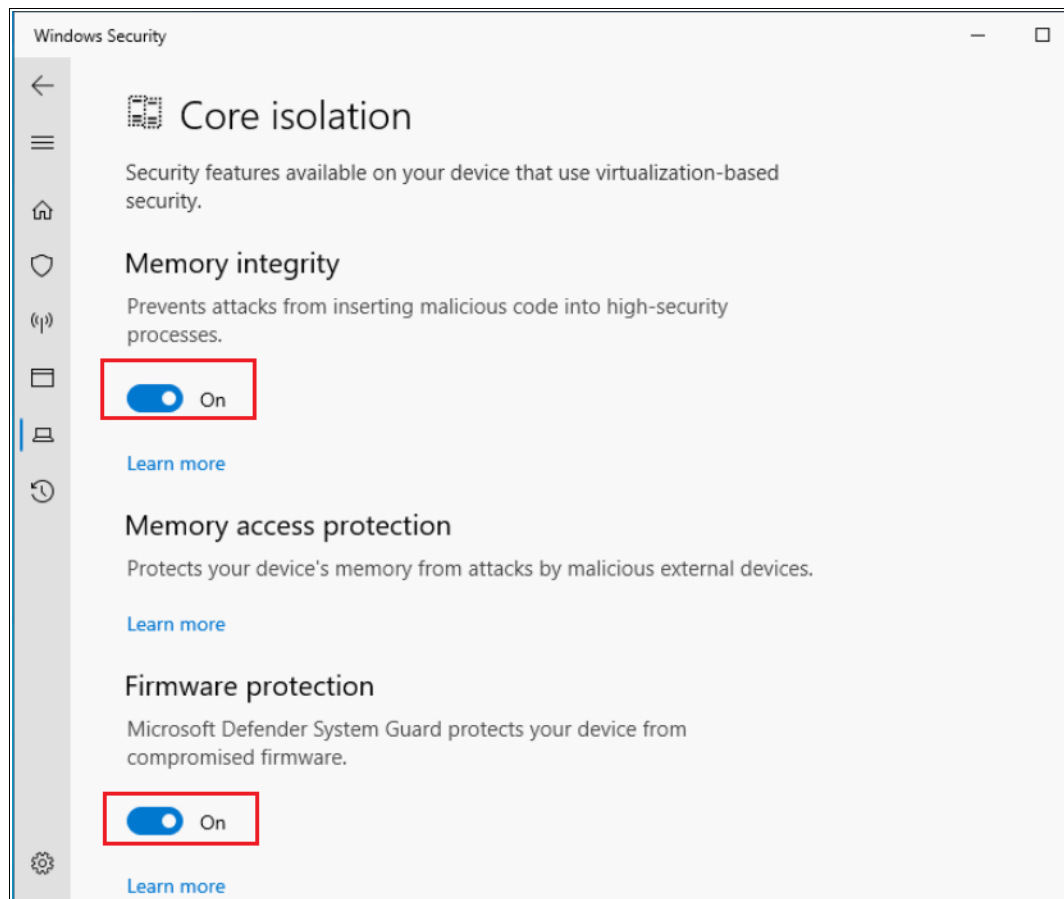


Figure 17 Enable Memory Integrity and Firmware Protection

If Memory Integrity or Firmware Protection cannot be set to On, it means the system doesn't meet the requirement for this enhanced security feature. Check that the UEFI version meets requirements and UEFI settings are ready as described in "Enabling Secured-core in UEFI" on page 7. Secured-core is not supported in any older Windows Server versions such as Windows Server 2019.

Secured-core in virtual machines: Currently Secured-core is not supported in VMs. Kernel DMA protection and Secure Launch are technologies for hardening host hardware and are not applicable to VMs. Therefore, in VMs Memory Integrity or Firmware Protection fails to be set to On.

5. Reboot the system to make the changes take effect.

Enabling Secured-core using PowerShell commands

Use the following three PowerShell commands to enable Secured-core, Figure 18

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\HypervisorEnforcedCodeIntegrity" /v "Enabled" /t REG_DWORD /d 1 /f

reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\HypervisorEnforcedCodeIntegrity" /v "WasEnabledBy" /t REG_DWORD /d 0 /f

reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\SystemGuard" /v "Enabled" /t REG_DWORD /d 1 /f
```

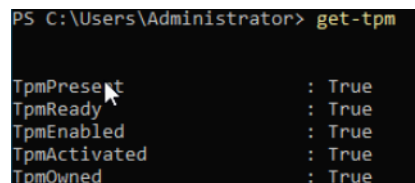
Figure 18 PowerShell commands to enable Secured-core

After these registry settings are finished, a system reboot is required to make the changes take effect.

Confirming Secured-core is enabled

To confirm all the Secured-core features are properly configured and running, follow the steps below:

1. To confirm TPM 2.0 is enabled, issue **get-tpm** in a PowerShell and confirm that TpmPresent, TpmReady, TpmEnabled and TpmActivated are all "True" as shown in Figure 19.



```
PS C:\Users\Administrator> get-tpm

TpmPresent      : True
TpmReady        : True
TpmEnabled      : True
TpmActivated    : True
TpmOwned       : True
```

Figure 19 TPM 2.0 check

- To check that Secure Boot is enabled, start `msinfo32` and in the System Summary page, verify that Secure Boot State is set to On, as shown in Figure 20.

Secure Boot State	On
PCR7 Configuration	Not Available
Windows Directory	C:\Windows
System Directory	C:\Windows\system32
Boot Device	\Device\HarddiskVolume1
Locale	United States
Hardware Abstraction Layer	Version = "10.0.20348.143"

Figure 20 Secure Boot check

- In the Windows Server GUI, go to **Windows security** → **Device security** → **Core isolation** and verify that Memory Integrity and Firmware Protection are set to On, as shown in Figure 21.

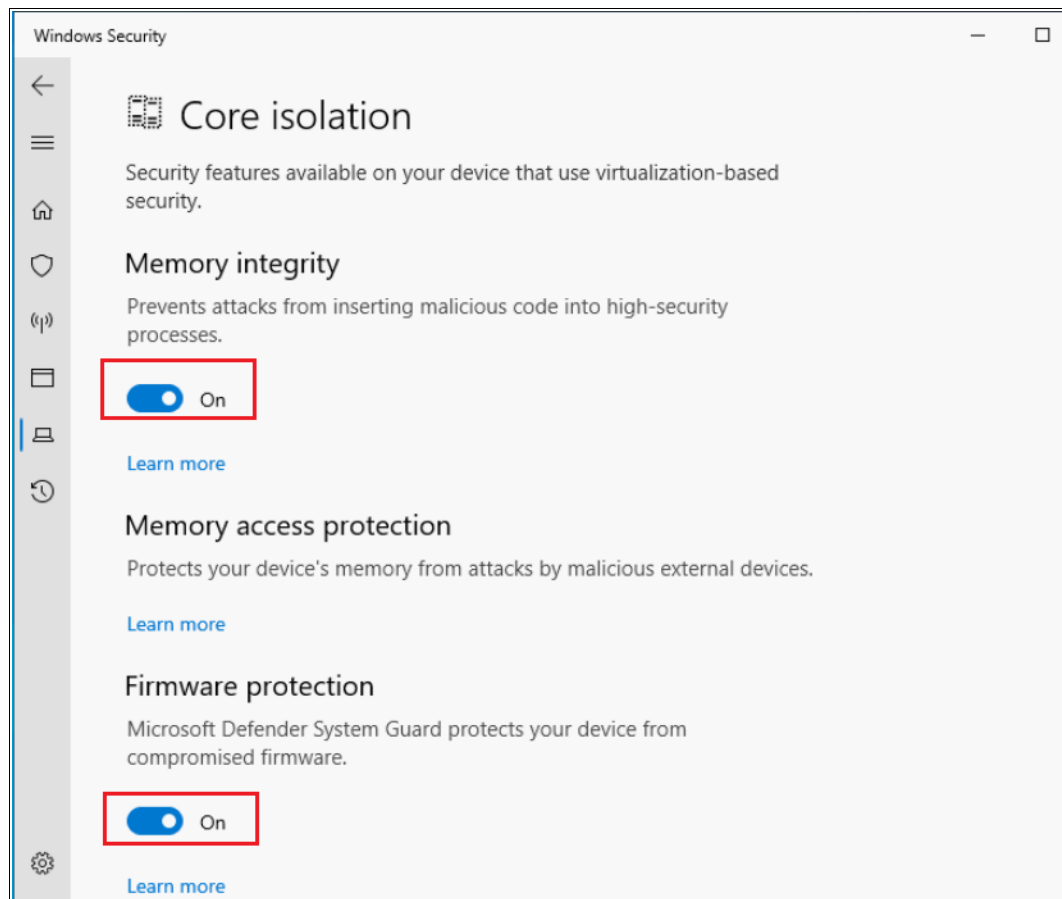


Figure 21 Memory Integrity and Firmware Protection check

- Verify that Kernel DMA Protection, VBS, HVCI and Secure Launch are enabled, by starting `msinfo32` and checking the System Summary page for the following values, as shown in Figure 22 on page 17:
 - **Kernel DMA Protection** is On
 - **Virtualization-Based Security** is Running
 - **Virtualization-Based Security Services Configured** contains the value Hypervisor enforced Code Integrity, Secure Launch

- **Virtualization-Based Security Services Running** contains the value Hypervisor enforced Code Integrity, Secure Launch

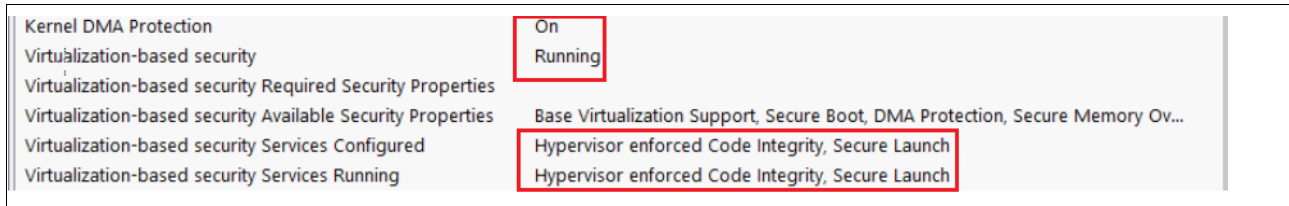


Figure 22 Kernel DMA Protection, VBS, HVCI and Secure Launch check

If all the Secured-core features above are properly configured and running, it means Secured-core feature is working well in your system and you can benefit from this feature to protect your critical applications and sensitive data.

Enabling Secured-core in Azure Stack HCI

Secured-core is also can be enabled in Azure Stack HCI with 22H2 or above version for Windows Solution. Azure Stack HCI is a core OS that doesn't support a full graphics user experience, so the way of enabling Secured-core in UEFI is the same, while in OS some steps are different.

The steps are as follows:

1. Install platform-specific driver for AMD-based System.

As with Windows Server 2022, for AMD-based system, after Secured-core is enabled in UEFI chipset driver should be installed before enabling Secured-core in OS. After finishing installing this driver, we can check DRTM boot driver by Azure Stack HCI management tool, Windows Admin Center, or PowerShell command.

- a. From Windows Admin Center select the destination server and from the left side menu select Devices. Once it is selected, we can use the search box on the top right side to type dr and filter the devices as shown in Figure 23.

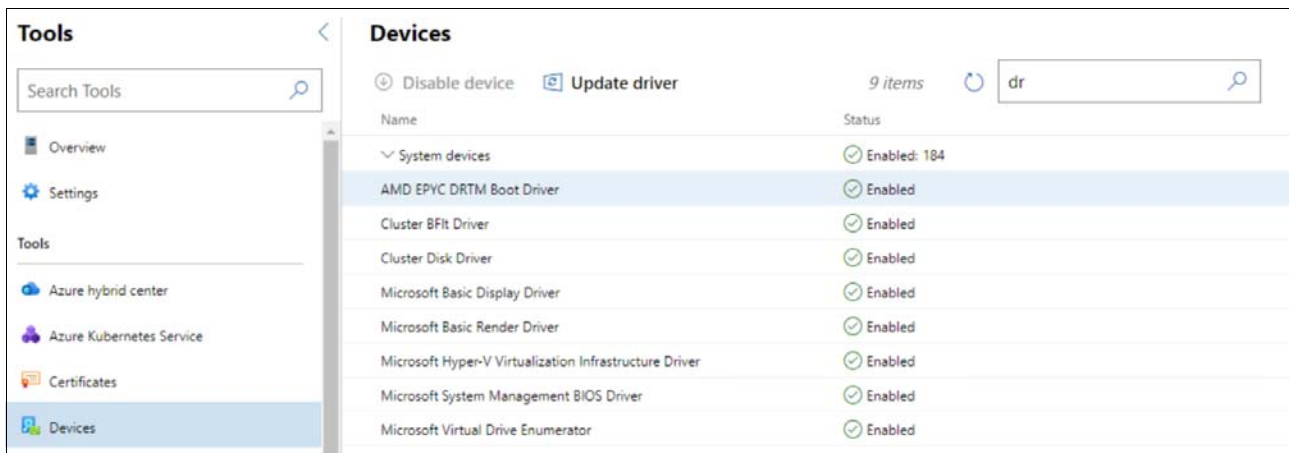


Figure 23 Check DRTM driver by Windows Admin Center

- b. From an elevated powershell prompt enter the following PowerShell command:

```
Get-WmiObject win32_pnpsigneddriver | ?{$_devicename -like "*AMD EPYC DRTM*"} | SELECT devicename, driverversion
```

The output should list the driver's name and version as shown in Figure 24.

```
devicename                driverversion
-----                -
AMD EPYC DRTM Boot Driver 1.10.2.0
```

Figure 24 Check DRTM driver by PowerShell command

2. Enable Secured-core in Azure Stack HCI by Windows Admin Center

There are two ways to enable Secured-core in Azure Stack HCI. One is to use the PowerShell commands as Windows Server 2022, the other is to use Windows Admin Center.

It is recommended to have the latest version of Windows Admin Center as some features might not be the same across all versions. In this case 2306 build 1.5.2306.14001 is used.

- a. Open Windows Admin center and select the server that will have the Secure Cored enabled.
- b. In the search box located on the top left side enter "Security" and select it as shown in Figure 25.

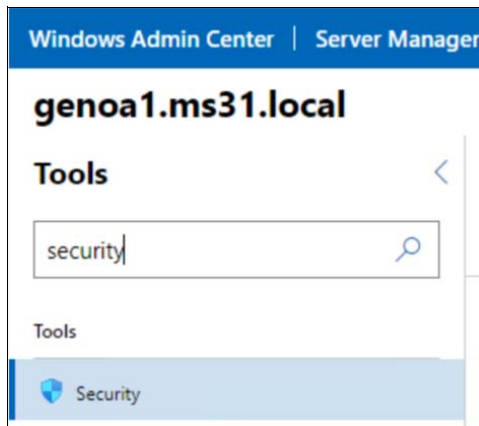


Figure 25 Open Security tool in Windows Admin Center

- c. Select the Secured-Core tab. Once this is selected all the requirements for Secure-Core are displayed as shown in Figure 26.

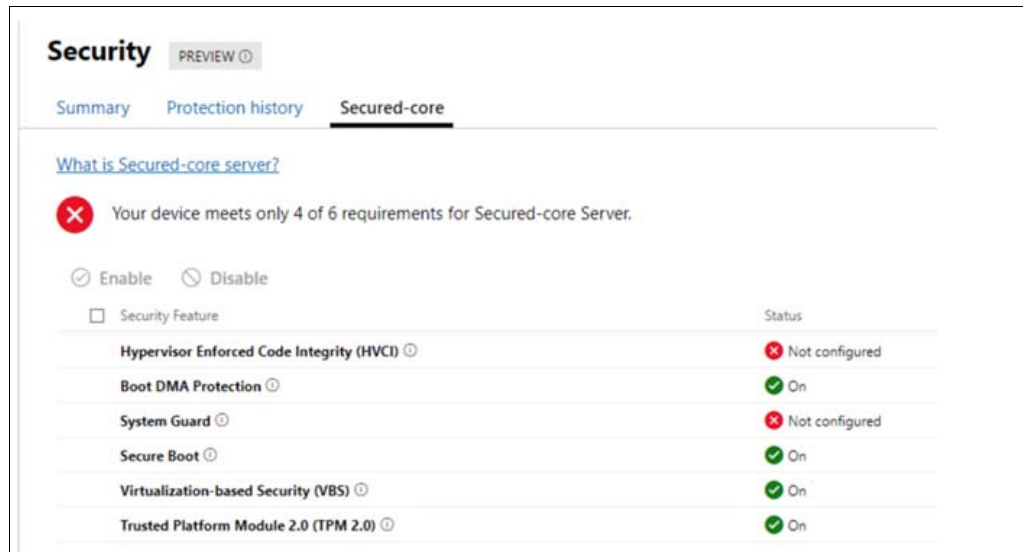


Figure 26 Open Secured-core tool in Windows Admin Center

- d. To enable Secure-Core we need to activate the remaining Security Features that are not configured as shown in Figure 27. After all of them are enabled restart the system.

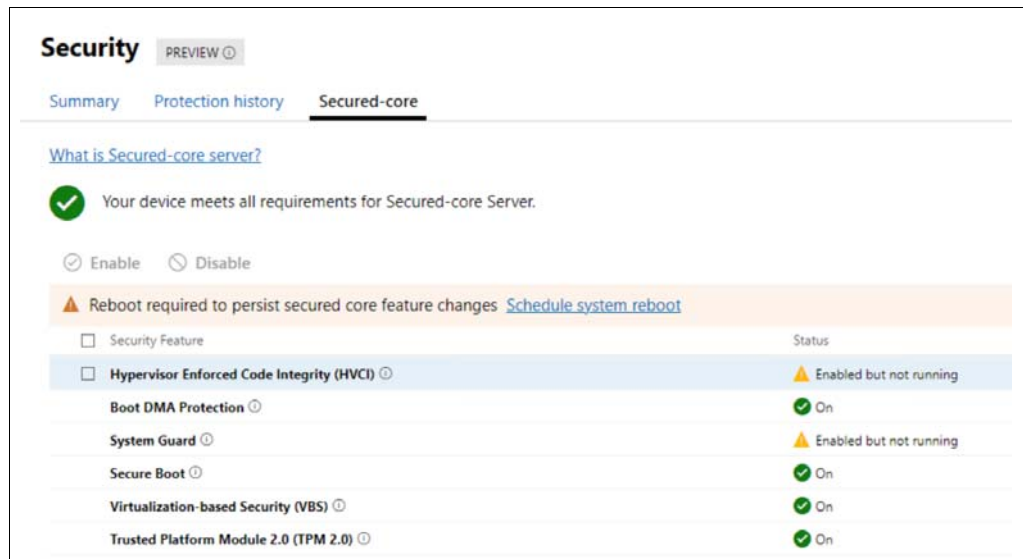


Figure 27 Enable Secured-core in Windows Admin Center

- e. All the features should be enabled as Figure 28.

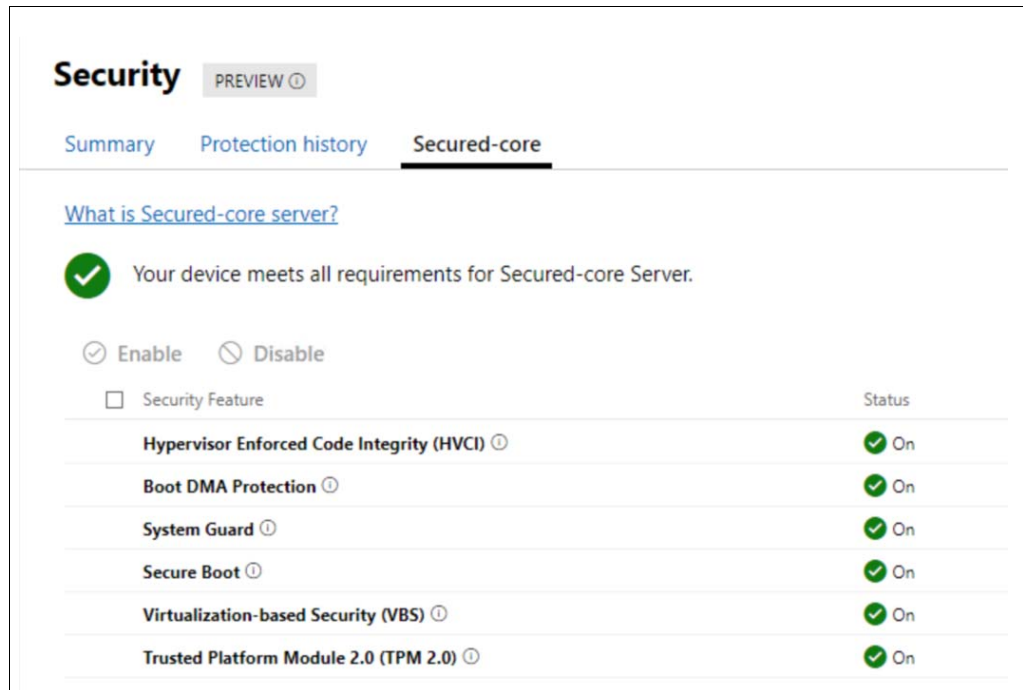


Figure 28 Secured-core is enabled in Azure Stack HCI

3. Confirm Secured-core is enabled in Azure Stack HCI
- a. To check the status of Secure boot, issue `Confirm-SecureBootUEFI` in a PowerShell and confirm the output to be true as shown in Figure 29.

```
PS C:\> Confirm-SecureBootUEFI
True
PS C:\> _
```

Figure 29 Secure boot check in Azure Stack HCI

- b. Check the status of TPM as Windows Server 2022 by PowerShell command `get-tpm`.
- c. Check Secured-core status by Windows Admin Center. If Secured-core is enabled successfully, it will be shown as Figure 28.

Resources

- ▶ Lenovo drivers for Windows
<https://windows-server.lenovo.com/repo/latest/>
- ▶ Microsoft web page for Secured-core
<https://docs.microsoft.com/en-us/windows-server/security/secured-core-server>
- ▶ Microsoft web page for new features in Windows Server 2022
<https://docs.microsoft.com/en-us/windows-server/get-started/whats-new-in-windows-server-2022>
- ▶ Microsoft web page for Kernel DMA protection (KDMA)

<https://docs.microsoft.com/en-us/windows/security/information-protection/kernel-dma-protection-for-thunderbolt>

- ▶ Microsoft web page for Dynamic Root of Trust for Measurement (DRTM)
<https://www.microsoft.com/security/blog/2020/09/01/force-firmware-code-to-be-measured-and-attested-by-secure-launch-on-windows-10/>
- ▶ Microsoft web page for Trusted Platform Module
<https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/how-windows-uses-the-tpm>
- ▶ Microsoft web page for Virtualization-based Security (VBS)
<https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-vbs>

Change history

November 2023:

- ▶ Added section “Enabling Secured-core in Azure Stack HCI” on page 17

December 2022:

- ▶ Updated the list of supported servers: “Supported Lenovo servers” on page 6
- ▶ Added information about UEFI settings for AMD servers
 - “Enabling Secured-core in UEFI for AMD-based 1-socket system” on page 9
 - “Enabling Secured-core in UEFI for AMD-based 2-socket system” on page 10
- ▶ Added Windows Server 2022 information for AMD systems: “Platform-specific driver installation in Windows Server 2022 for AMD-based system” on page 11

First published: March 31, 2022

Author

Guiqing Li is a Windows Engineer at the Lenovo ISG in Beijing, China. She has more than ten years of experience with driver development, and five years of experience with Windows debugging.

Hussein Jammal is a senior solutions architect engineer and Microsoft Solution Lead in EMEA working in Bucharest, Romania. He has over 13 years of experience in the IT engineering field.

Laurentiu Petre is a solutions engineer working in Bucharest, Romania. He has over 10 years of experience in the IT field being accustomed with large scale deployments of Microsoft Exchange and other Microsoft products.

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

- ▶ Vinay Kulkarni, Lenovo Principal Technical Consultant
- ▶ Gary Cudak, Lenovo OS architect for OS Enablement and Preload
- ▶ Boyong Li, Lenovo Senior Windows Engineer for Windows Enablement
- ▶ 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 November 13, 2023.

Send us your comments via the **Rate & Provide Feedback** form found at <http://lenovopress.com/lp1578>

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. These and other Lenovo trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by Lenovo at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of Lenovo trademarks is available from <https://www.lenovo.com/us/en/legal/copytrade/>.

The following terms are trademarks of Lenovo in the United States, other countries, or both:

Lenovo®
Lenovo(logo)®

ThinkAgile™
ThinkServer®

ThinkSystem™

The following terms are trademarks of other companies:

Intel, Xeon, and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft, PowerShell, Windows, Windows Server, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.