Microsoft

Secured-core Servers

Enabling Guide

Supermicro Solutions for Microsoft Azure Stack HCI

Table of Contents

1 Overview

This document provides a guidance for product specific steps to configure Secured-core Server AQ certified servers to a fully protected state.

2 Applicable products

The configuration guidance applies to the following products.

Intel®-based X13 systems

- SYS-511E-WR
- SYS-111E-WR
- SYS-111C-NR
- SYS-621H-TN12R
- SYS-211GT-HNC8R

AMD EPYC™-based H13 systems

- AS -2115GT-HNTR
- AS -2025HS-TNR
- AS -1125HS-TNR
- AS -1115CS-TNR
- AS -1015CS-TNR
- AS -2015CS-TNR

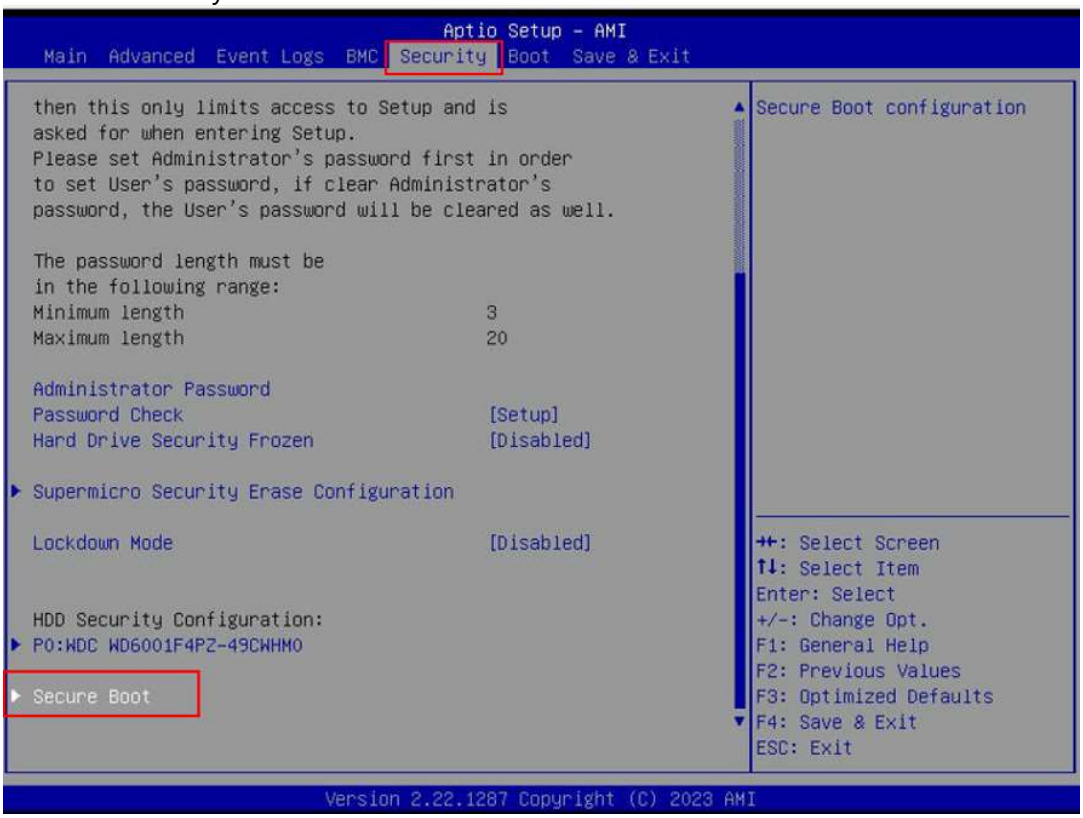
Note: Above list will be updated as more systems SKUs will be validated for Azure Stack HCI solution.

3 UEFI Settings

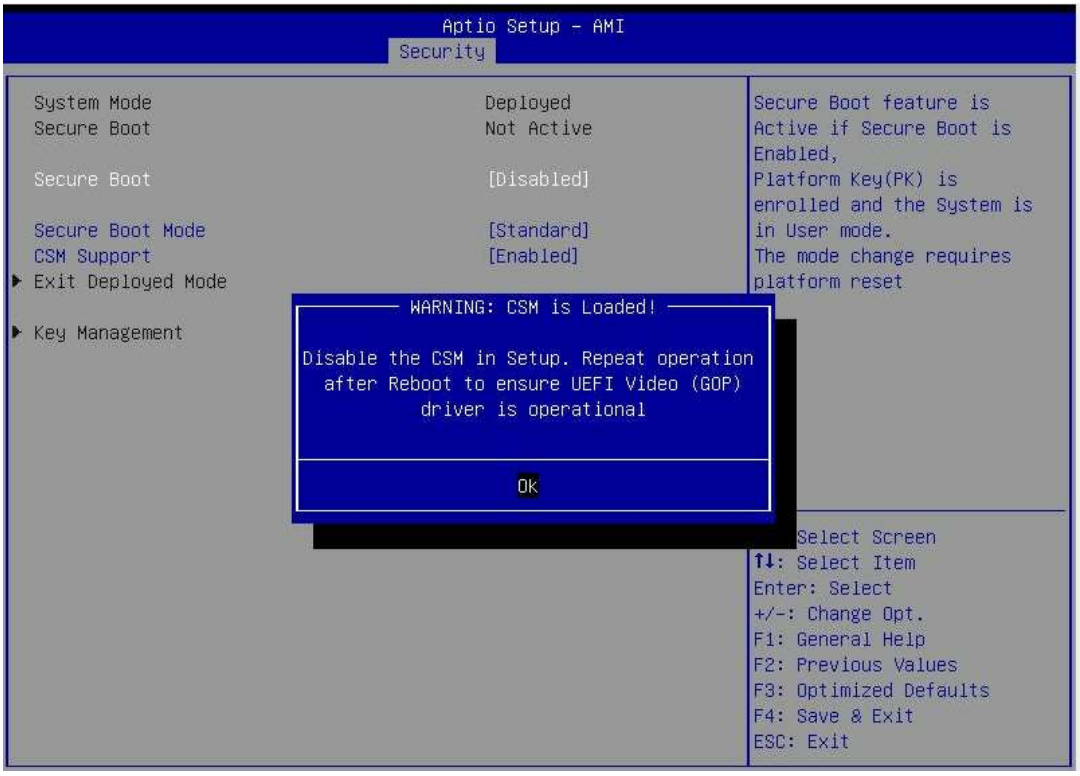
For Intel®-based X13 and X12 systems

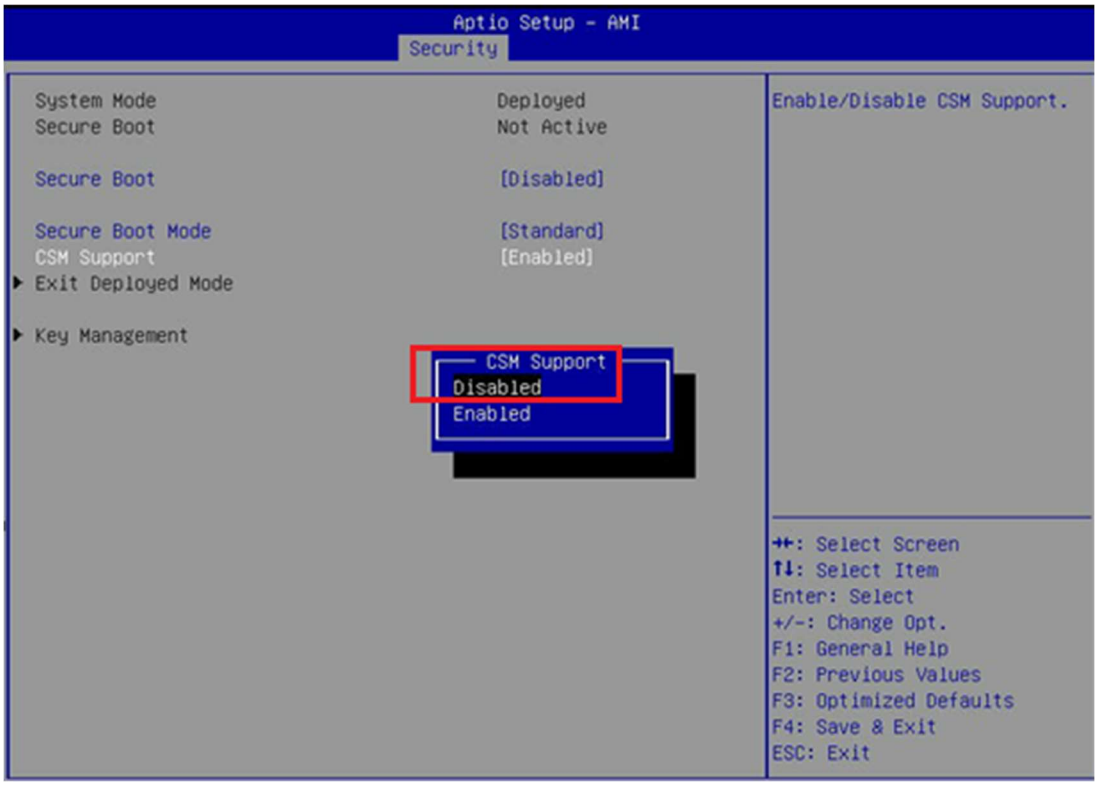
1. Press <DEL> to Enter to the BIOS setup

2. Go to the Security tab and choose Secure Boot



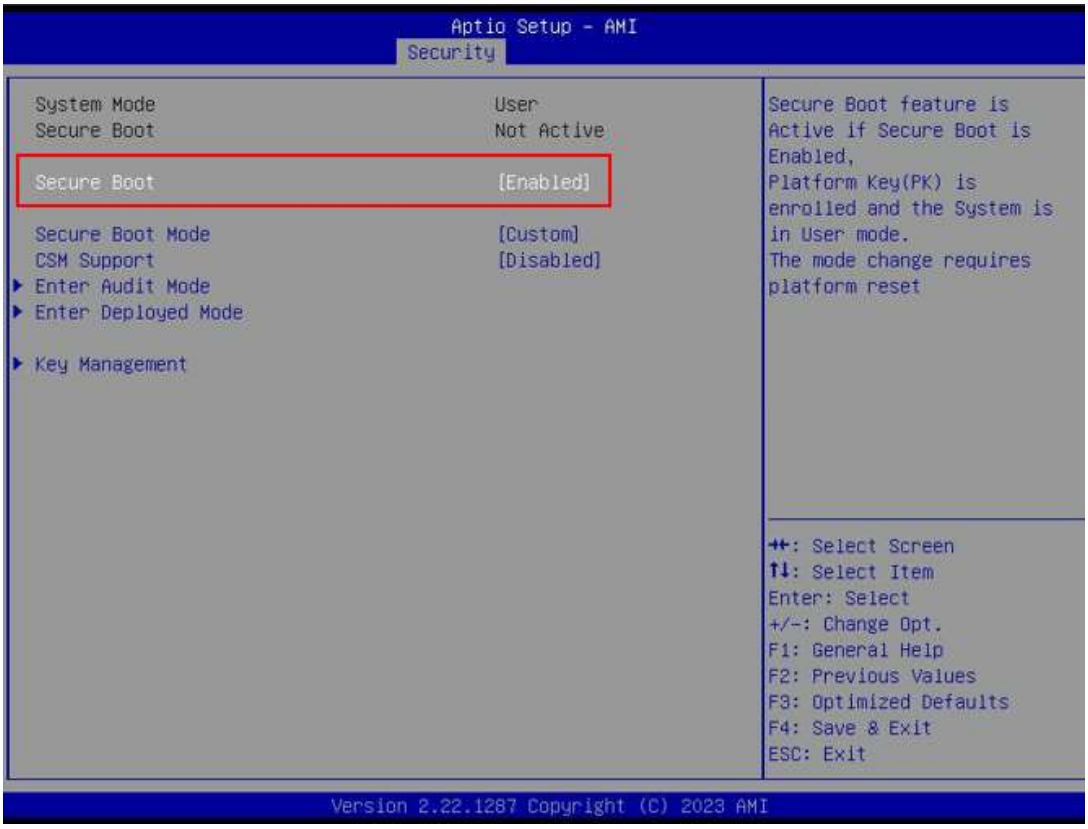
3. Disable CSM Support



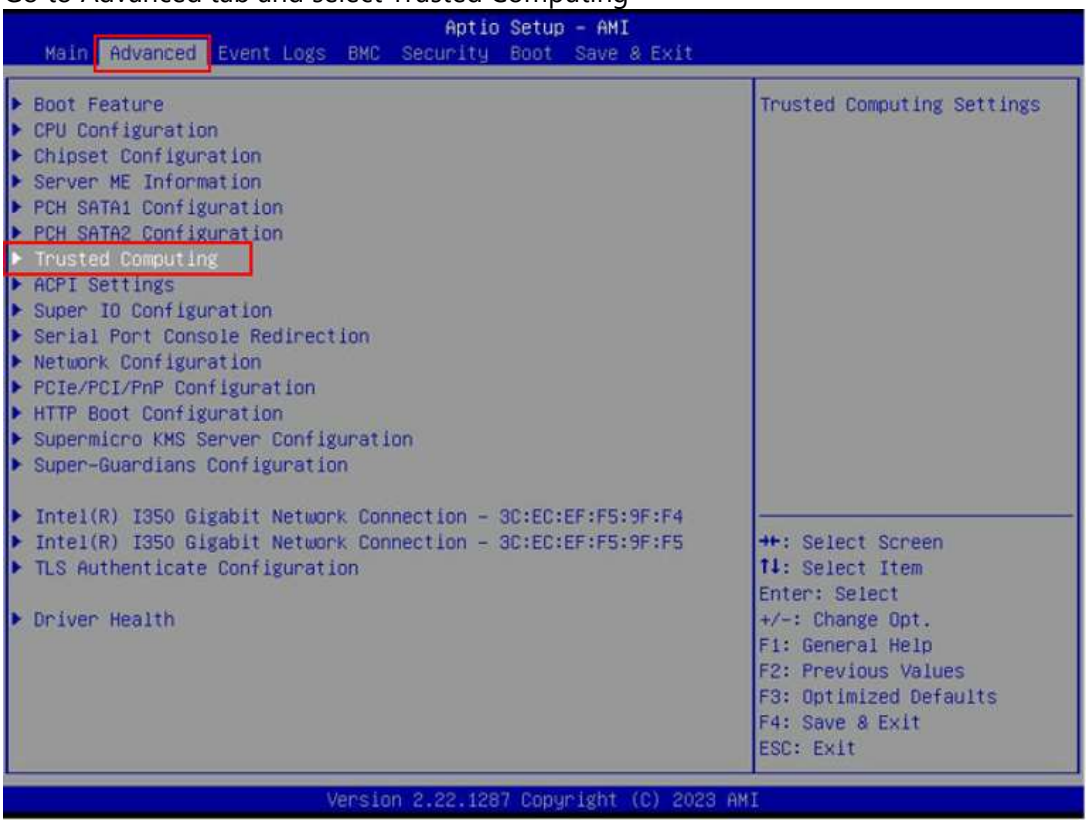


4. Save and reboot the system and enter the BIOS again

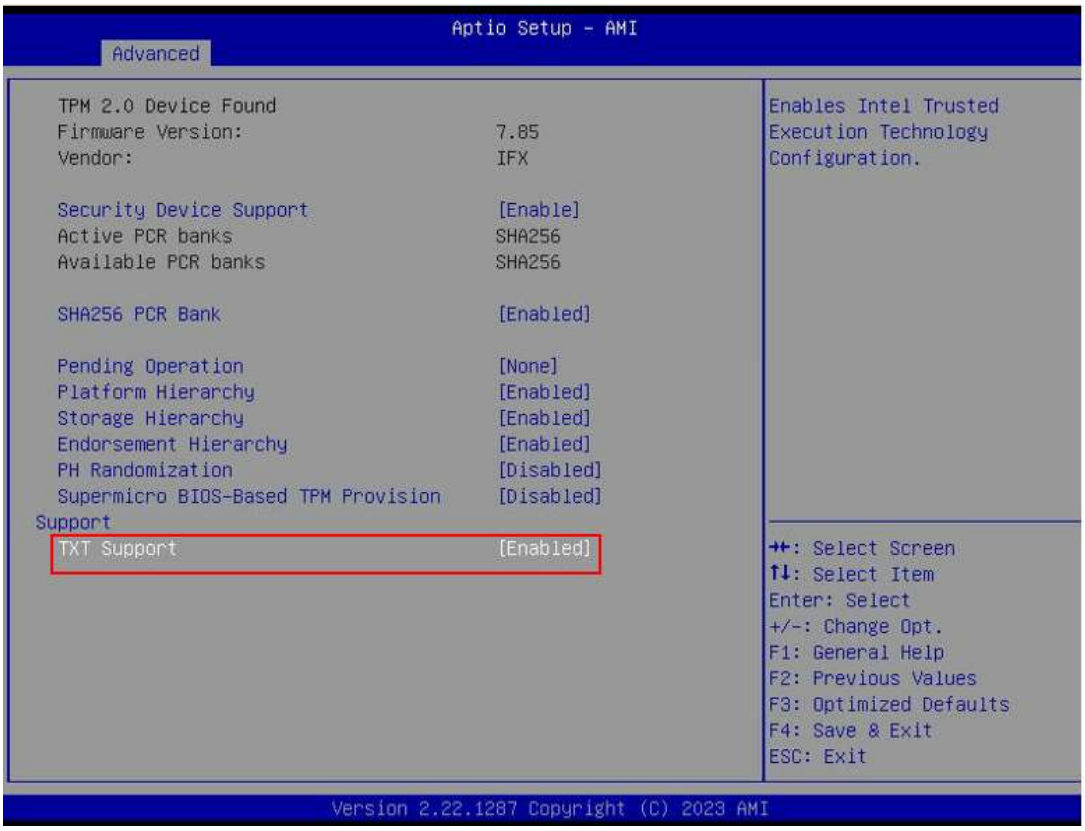
5. Enable Secure boot



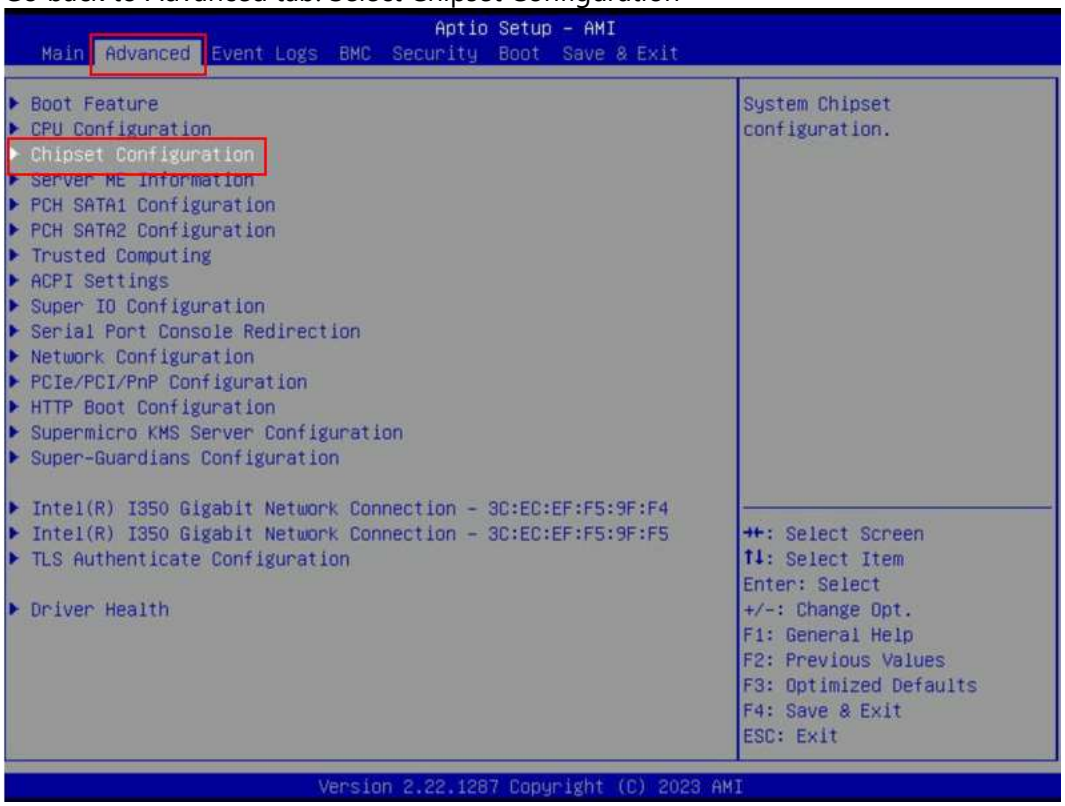
6. Go to Advanced tab and select Trusted Computing



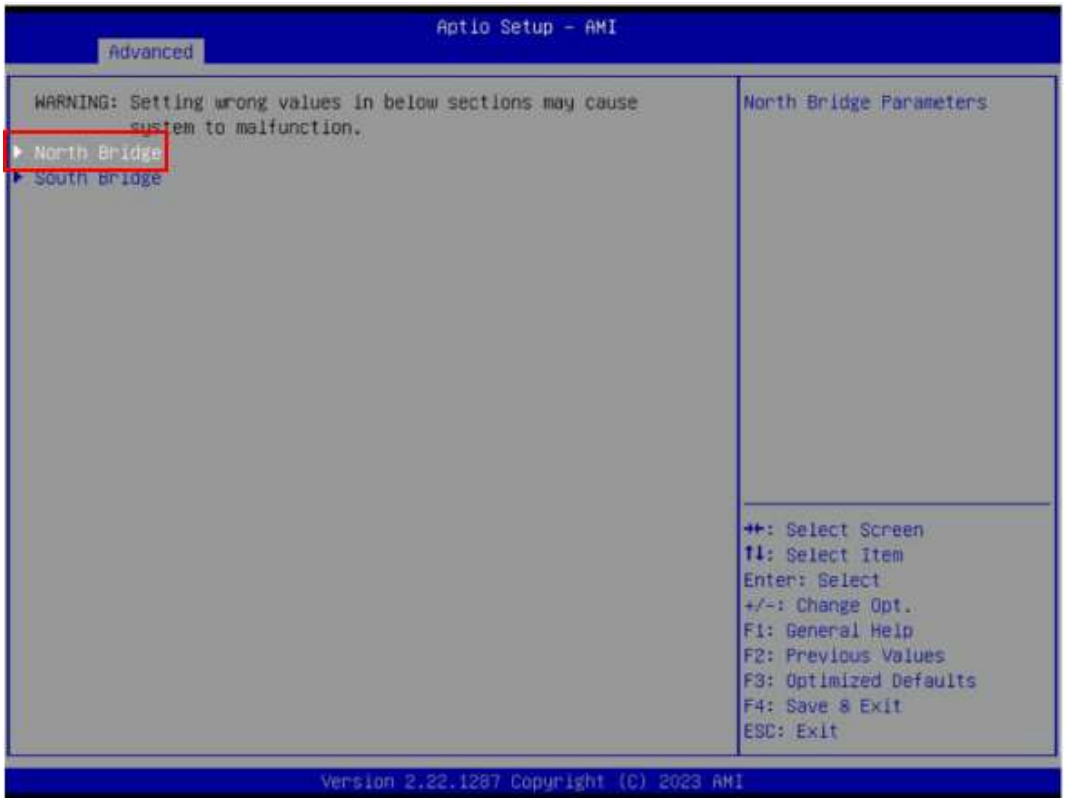
7. Enable TXT Support:



8. Go back to Advanced tab. Select Chipset Configuration



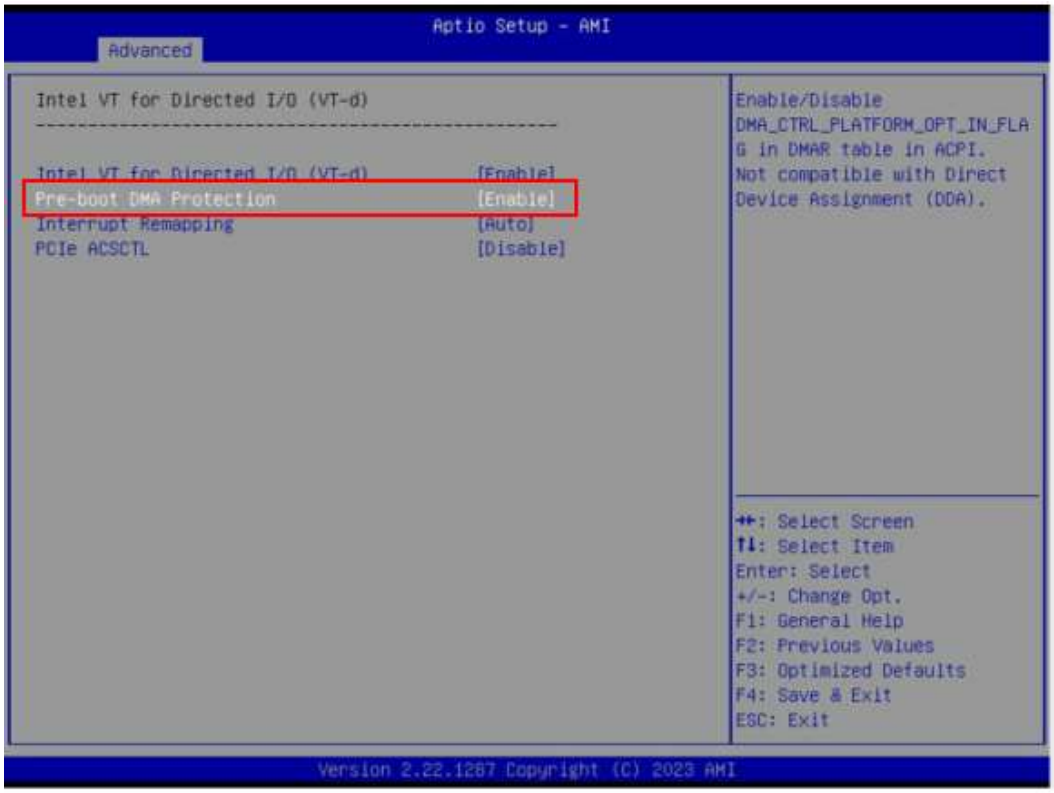
9. Select North Bridge



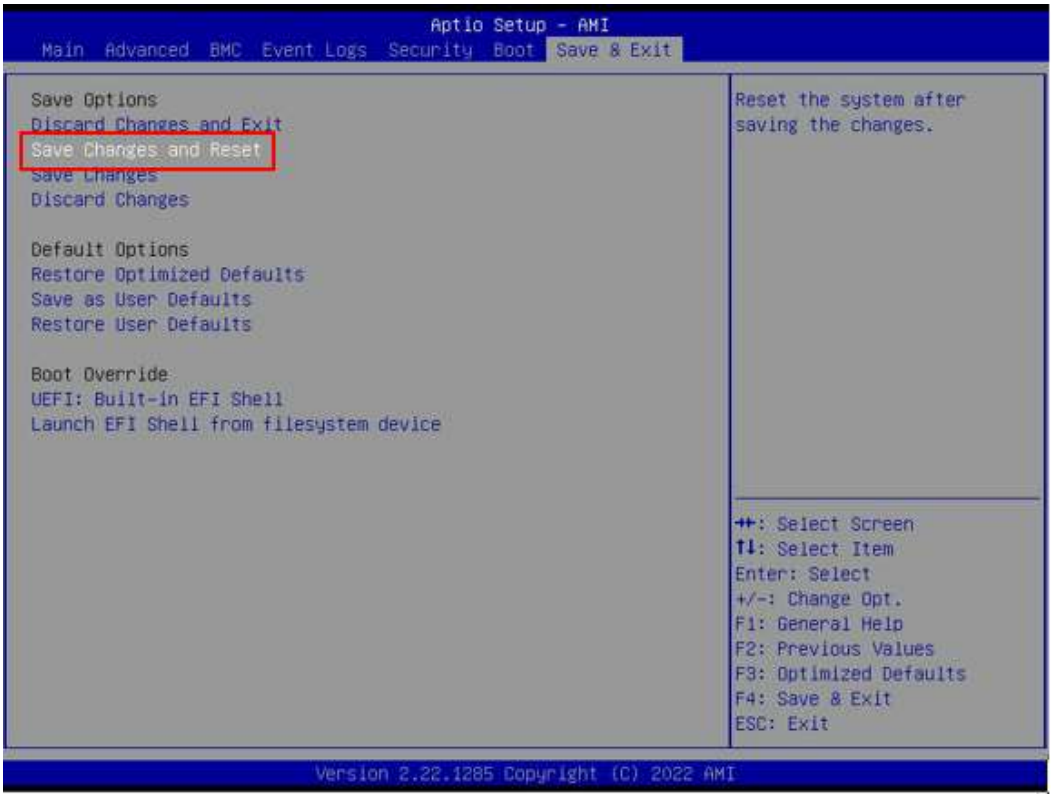
10. Select IIO Configuration

11. Select Intel VT for Directed I/O (VT-d)

12. Enable Pre-boot DMA Protection



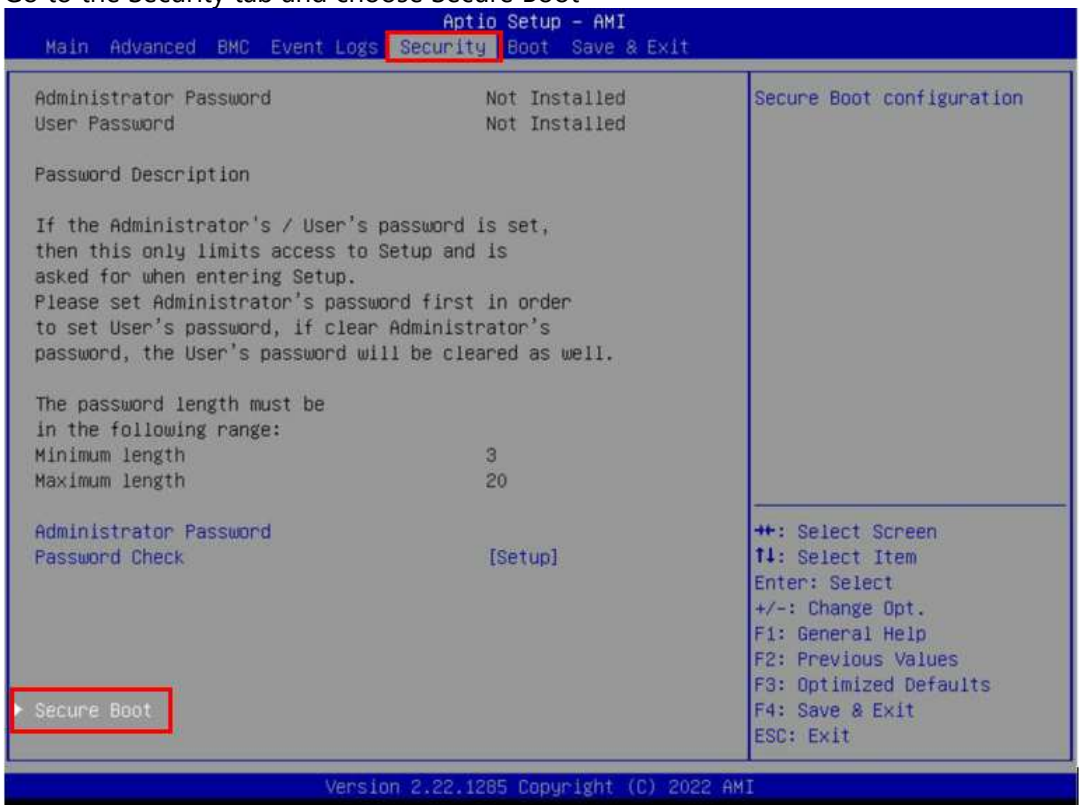
13. Save changes and reset the system



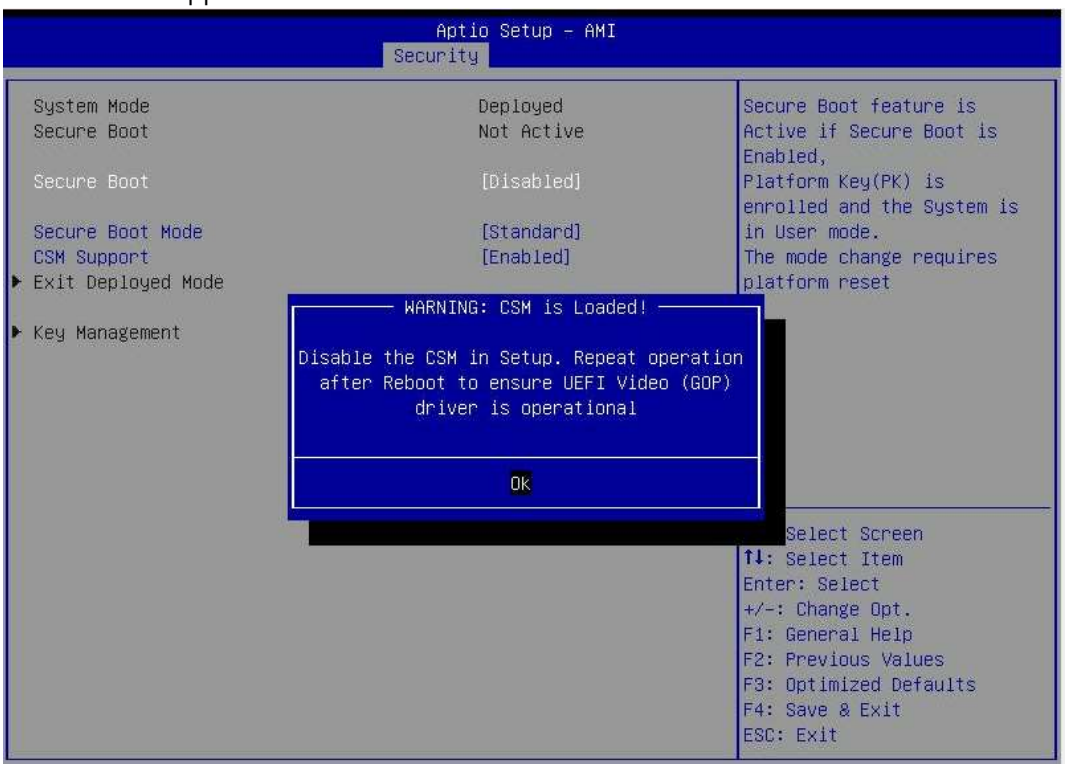
For AMD EPYC™-based H13 systems

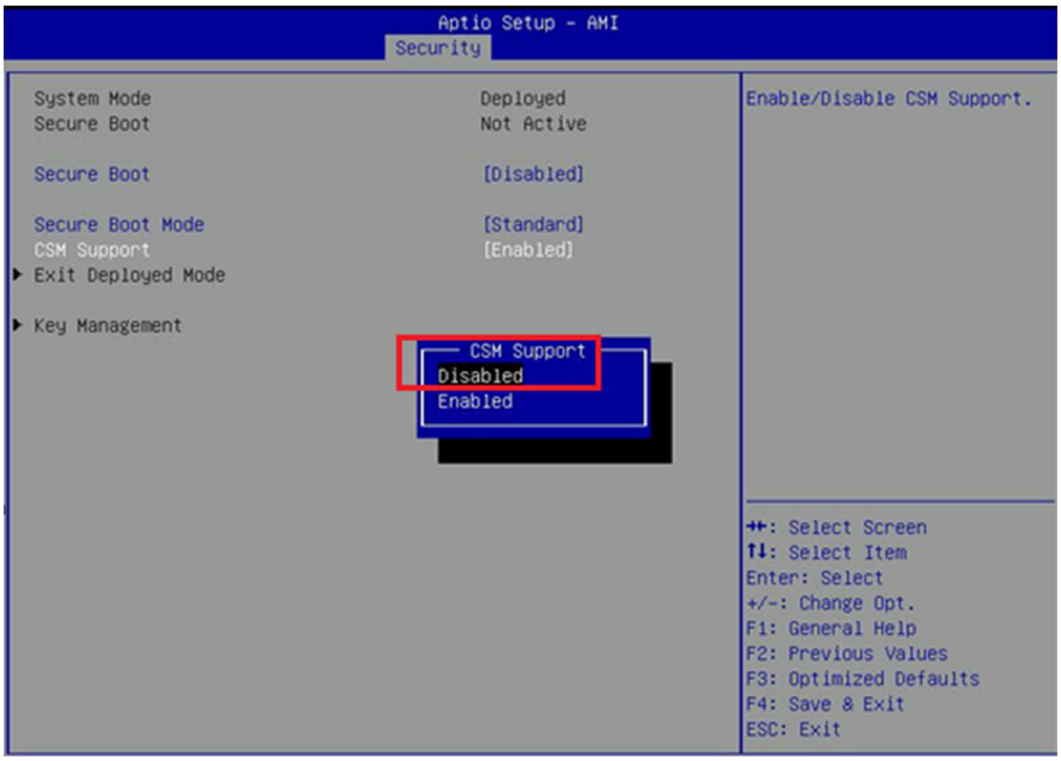
1. Press <DEL> to Enter to the BIOS setup

2. Go to the Security tab and choose Secure Boot



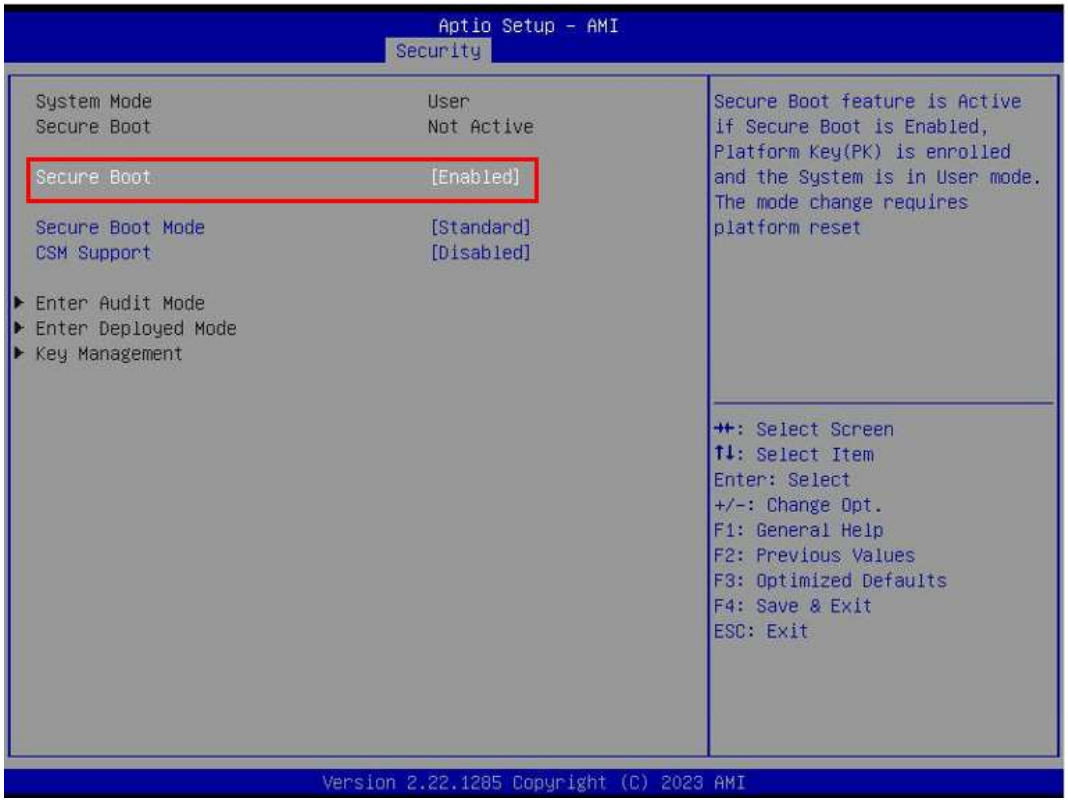
3. Disable CSM Support



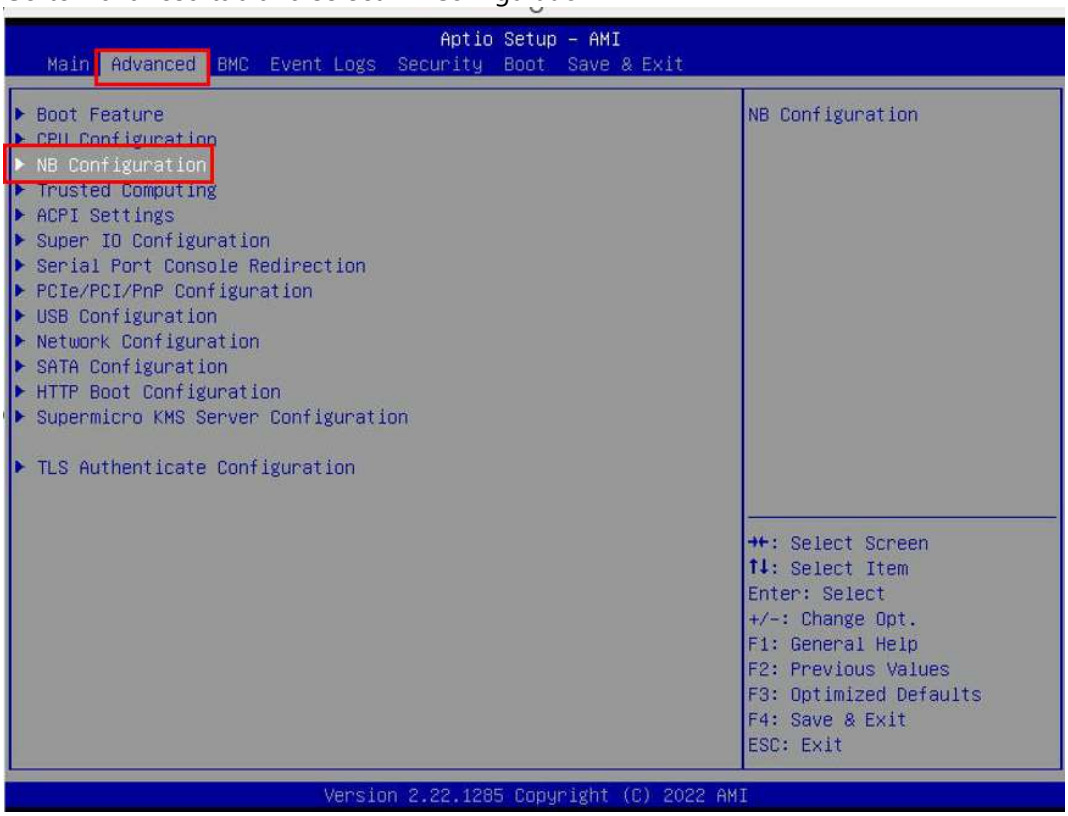


4. Save and reboot the system. Enter the BIOS again

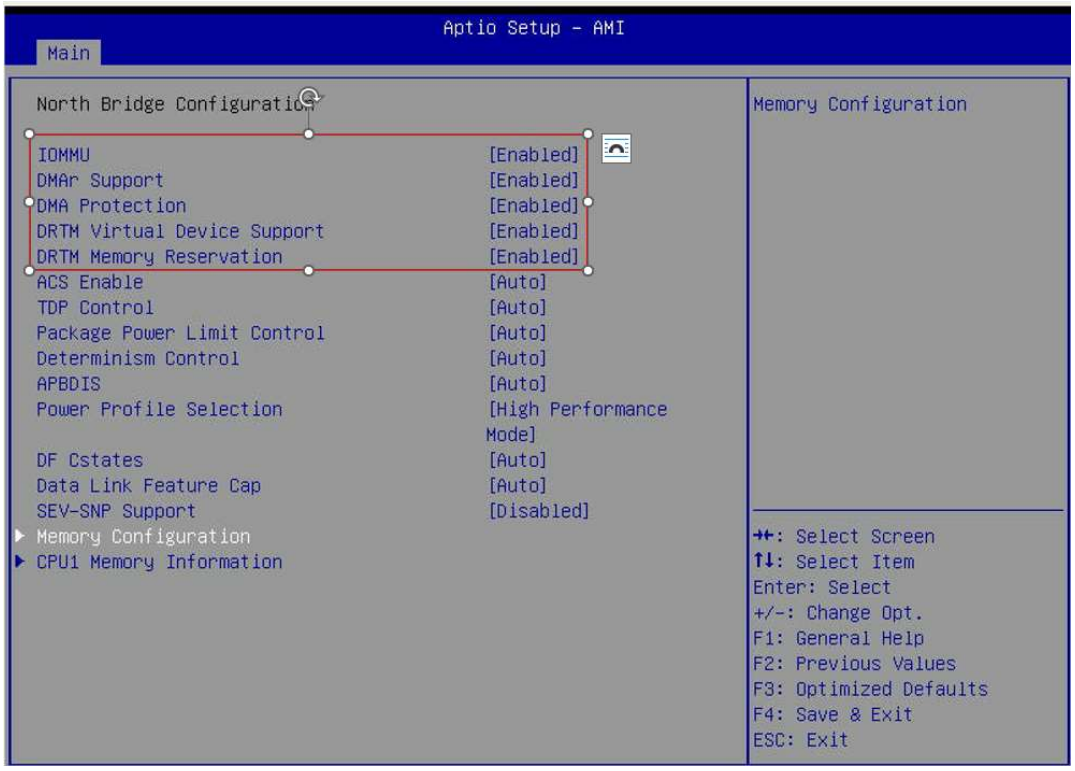
5. Enable Secure boot



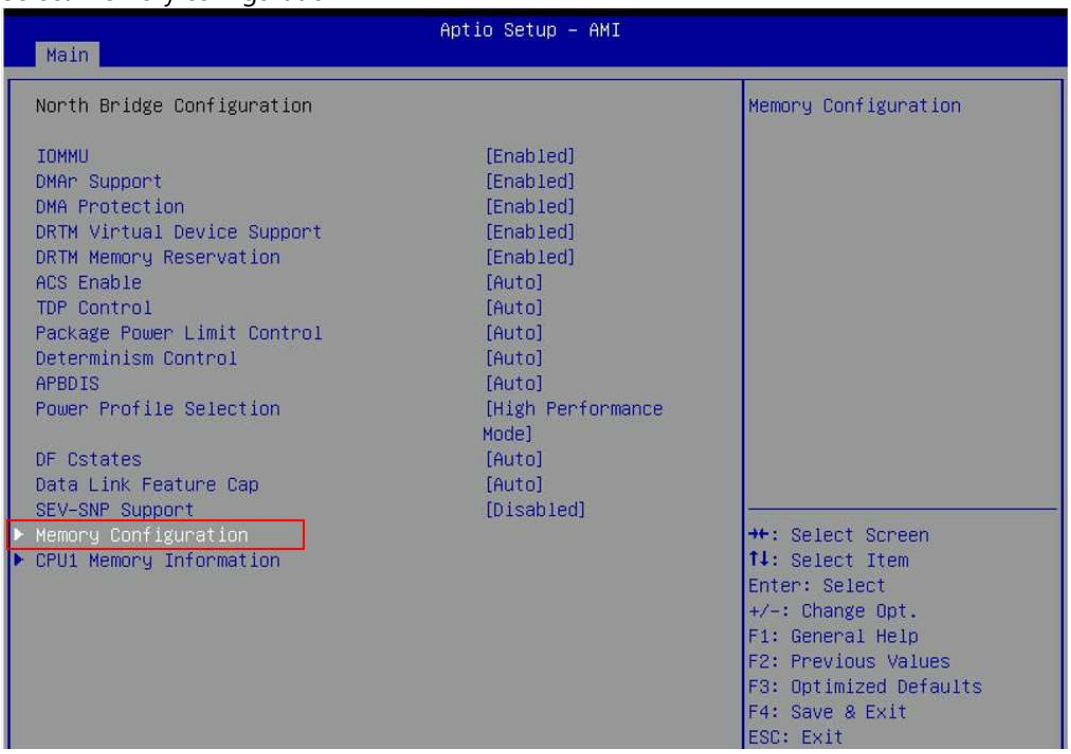
6. Go to Advanced tab and select NB Configuration



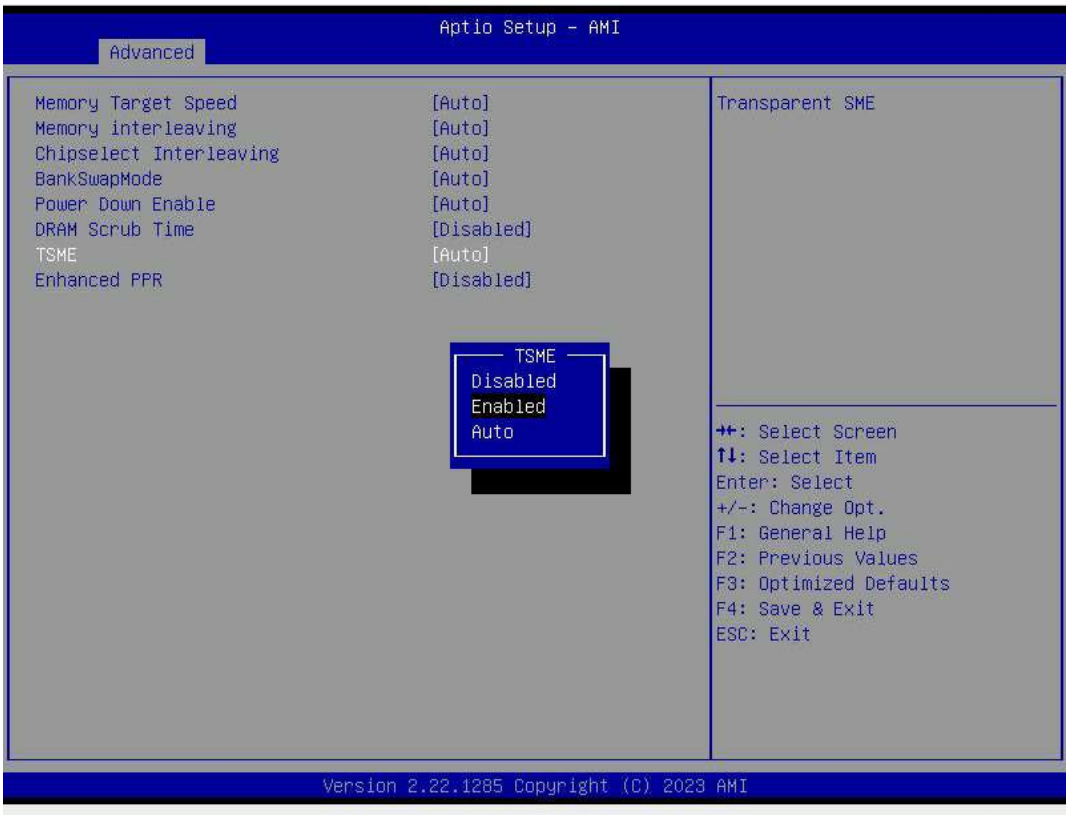
7. Enable the following functions:
   IOMMU [Enabled]
   DMAr Support [Enabled]
   DMA Protection [Enabled]
   DRTM Virtual Device Support [Enabled]
   DRTM Memory Reservation [Enabled]

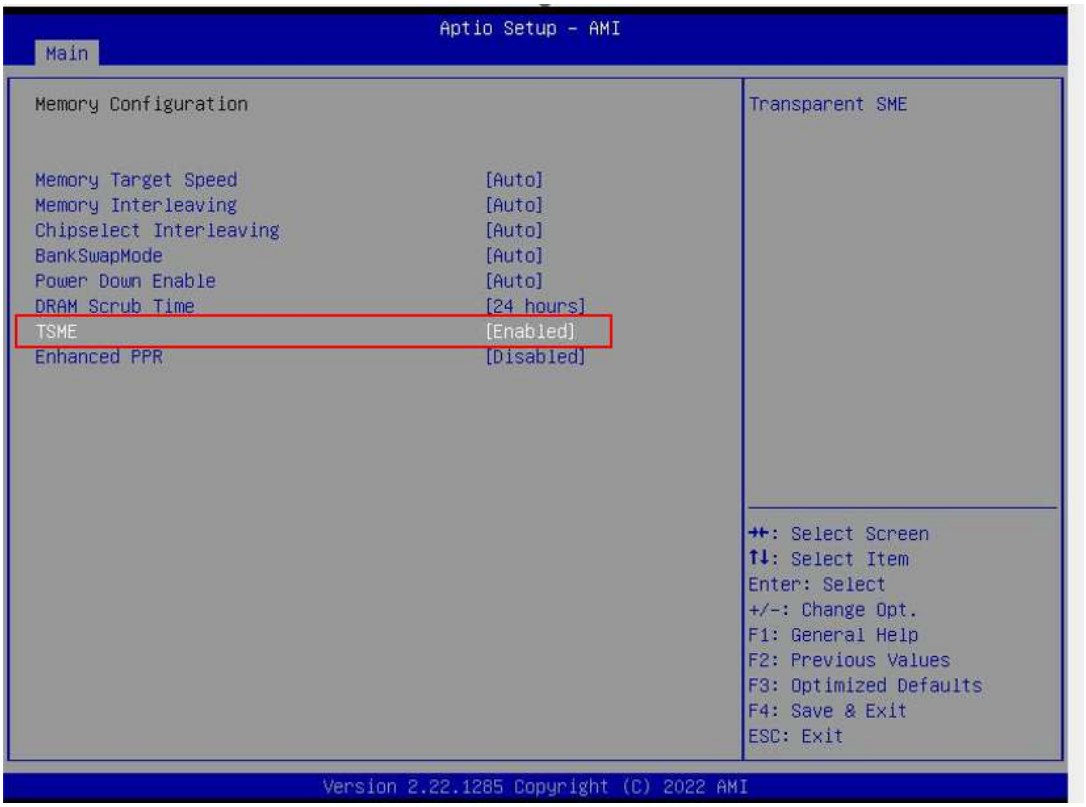


8. Select Memory configuration

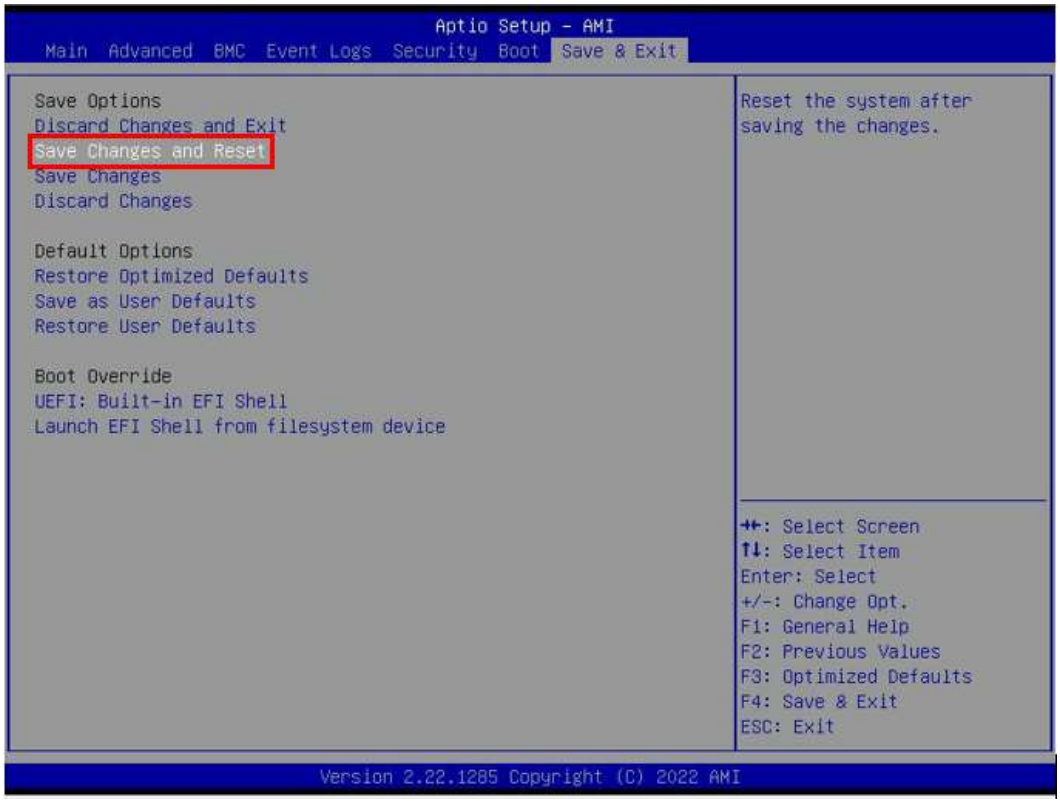


9. Enable TSME





10. Save changes and reset the system



4 OS Settings

4.1 Install platform specific drivers (optional)

The latest chipset drivers need to be installed in the OS for both Intel and AMD based systems. Please visit specific product page on www.supermicro.com, and then download latest drivers for that system model.

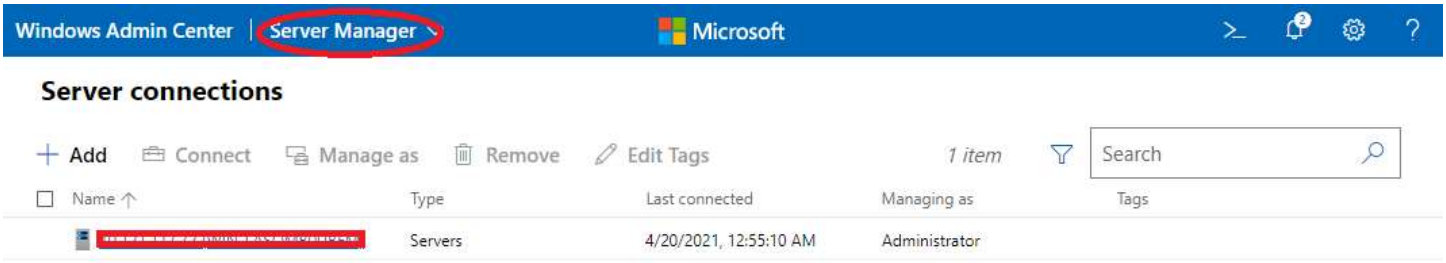
4.2 Configure OS to enable VBS, HVCI and System Guard

To configure Secured-core features on the OS, there are several different ways to do it. Choose one of the following 3 options to enable VBS, HVCI and System Guard.

4.2.1 Windows Admin Center (WAC)

From any PC or server configured for PowerShell remoting to the test target, download the Windows Admin Center and install.
Add the target server for management in the Windows Admin Center.

From the Server Manager view, choose the target server.



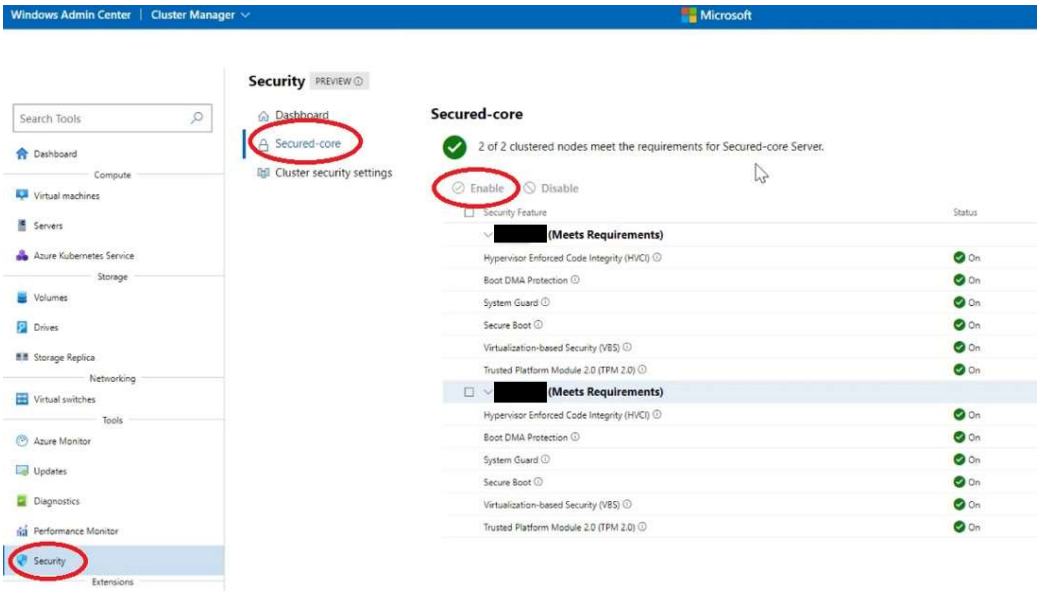
Scroll down for “Security” in the Tools menu on the left.

You can enable HVCI, System Guard and VBS from the Windows Admin Center.

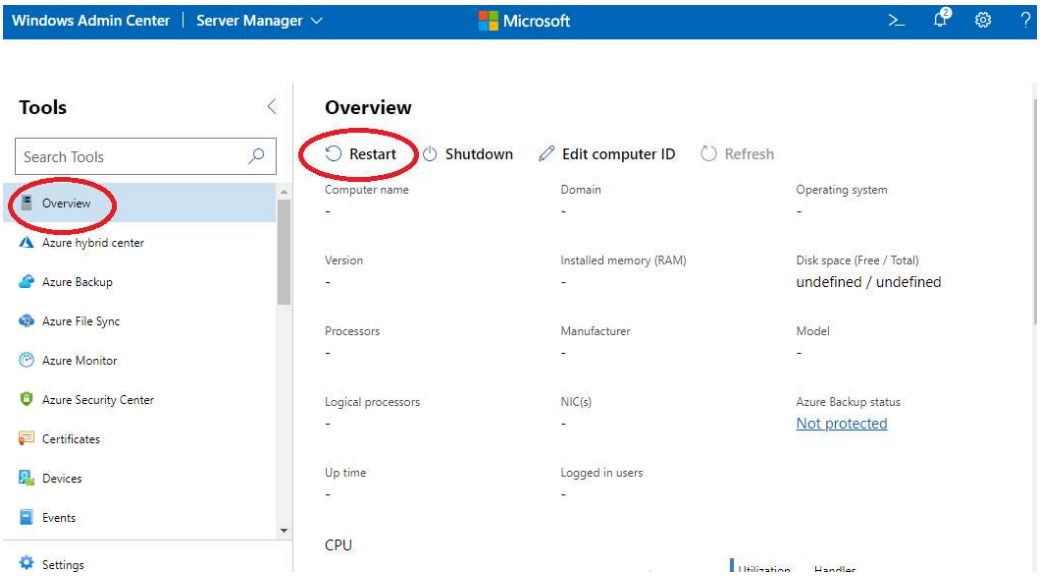
Click on a feature name that doesn’t show as “On” and click “Enable”. Repeat this for all disabled features.

If the Boot DMA Protection, Secure Boot or TPM2.0 are not shown as “On”, you will need to enable the feature in the UEFI.

Ensure all of the Secured-core features are showing as “On” before proceeding to validation.

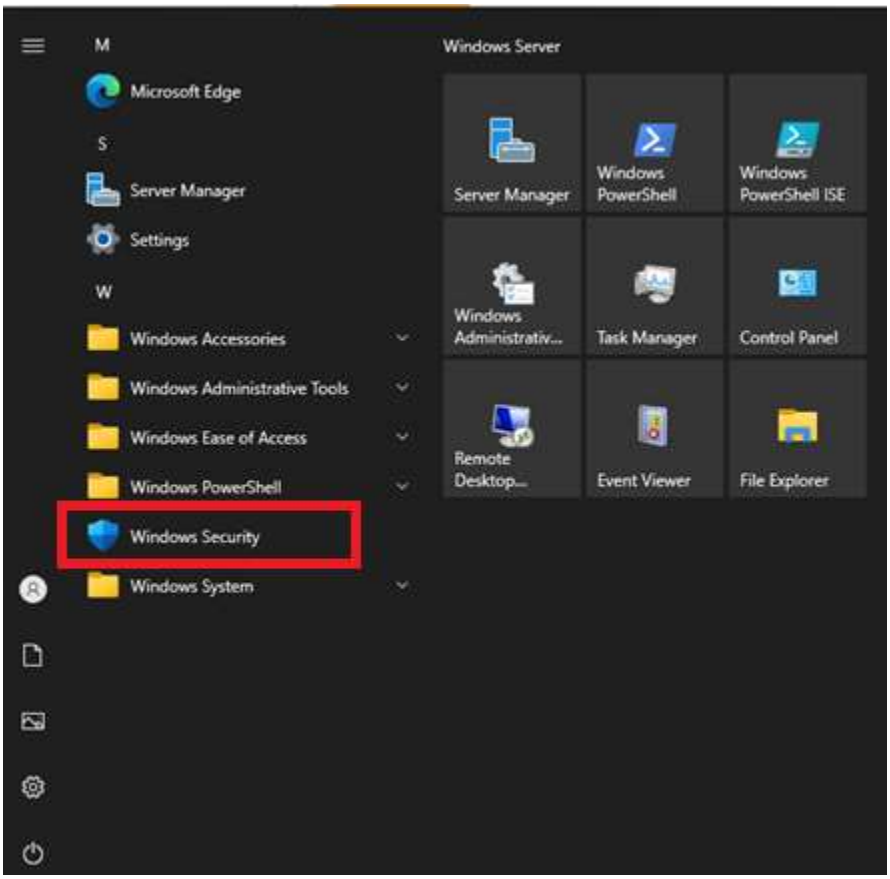


You will be prompted for a reboot for the changes to take effect. Go to “Overview” and click “Restart”.

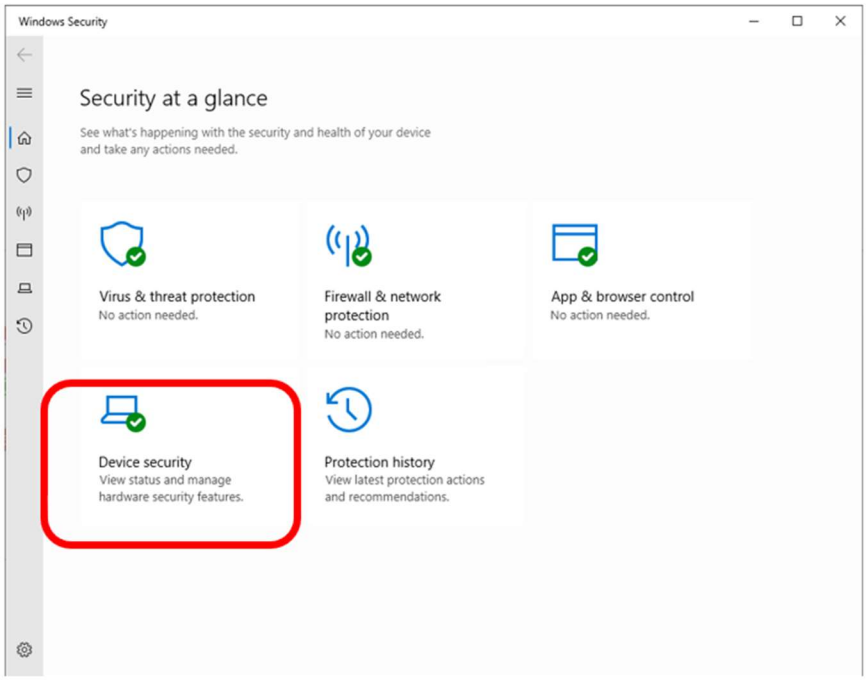


4.2.2 Windows Security App (For Windows Server OS with Desktop experience only)

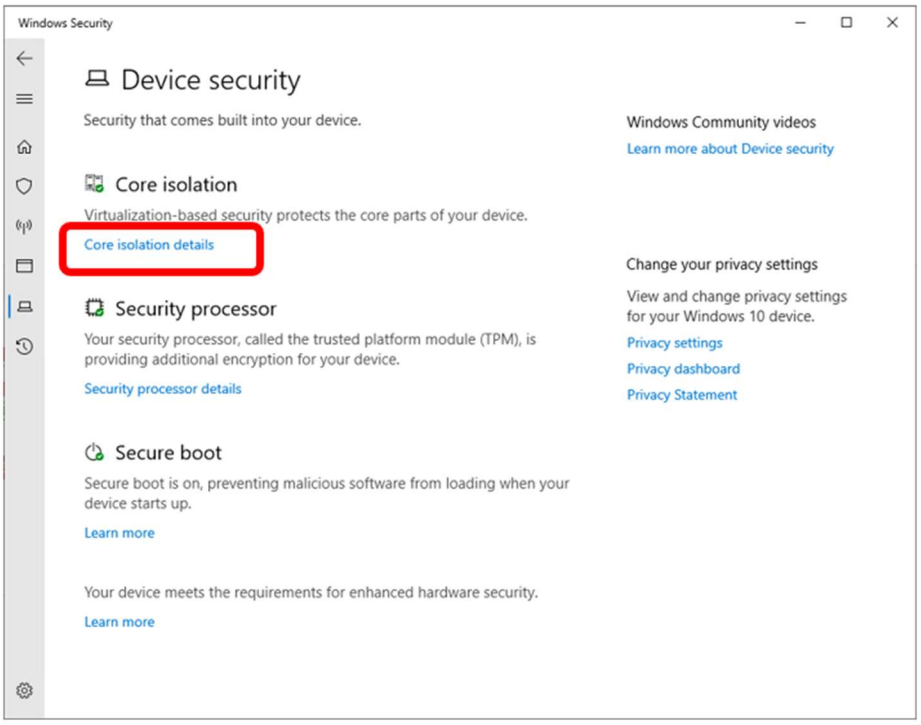
Launch the Windows Security app from the start menu.



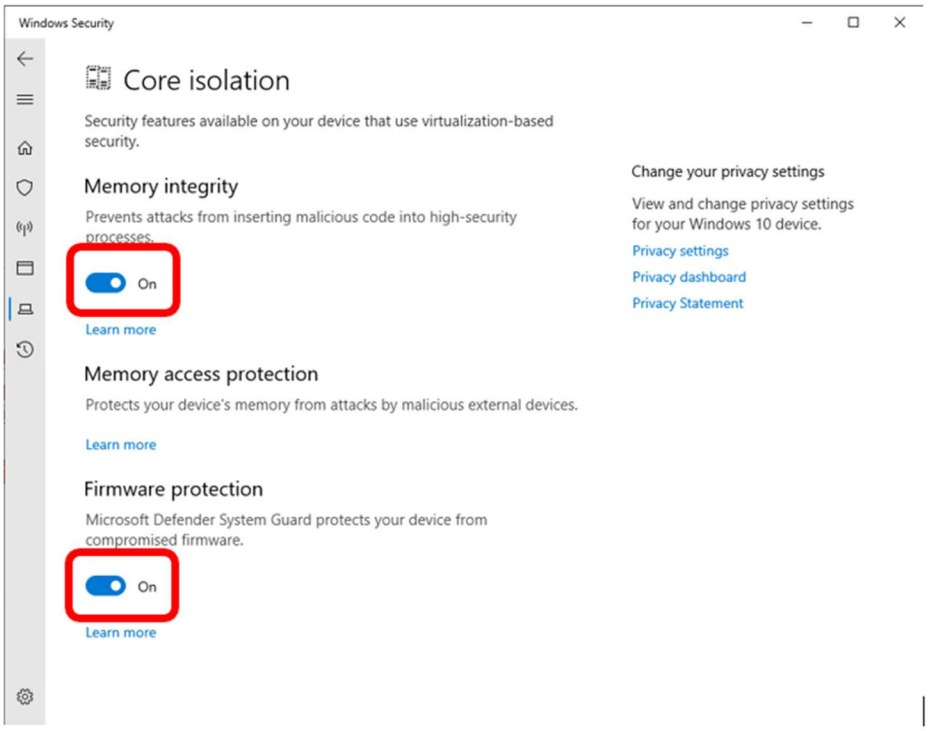
Choose “Device security”.



Click the “Core isolation details”.



Set the slider switches for both “Memory integrity” and “Firmware protection” to “On”.



You will be prompted for a reboot for these settings to take effect.

4.2.3 Configure Registry Key

Alternatively, you can configure the following registry key settings to achieve the same result.

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

5 Confirm the Secured-core state

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

5.1 TPM 2.0

Run get-tpm in a PowerShell and confirm the following:

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

5.2 Secure boot, Kernel DMA Protection, VBS, HVCI and System Guard

Launch msinfo32 from command prompt and confirm the following values:

- "Secure Boot State" is "On"
- "Kernel DMA Protection" is "On"

- "Virtualization-Based Security" is "Running"
- "Virtualization-Based Security Services Running" contains the value "Hypervisor enforced Code Integrity" and "Secure Launch"

Secure Boot State	On

Kernel DMA Protection	On
Virtualization-based security	Running
Virtualization-based security Required Security Properties	
Virtualization-based security Available Security Properties	Base Virtualization Support, Secure Boot, DMA Protection,
Virtualization-based security Services Configured	Hypervisor enforced Code Integrity, Secure Launch
Virtualization-based security Services Running	Hypervisor enforced Code Integrity, Secure Launch

6 Support

For questions about Supermicro solutions for Azure Stack HCI, please send message via the following link: [Supermicro contact for Azure Stack HCI]