

Secured-core Servers

Enabling Guide



AZS Integrated Systems for Azure Stack HCI

HCI Validated Nodes for Azure Stack HCI

Powered by 3rd Gen Intel® Xeon® Scalable Processors

Table of Contents

1	Overview.....	3
2	Applicable products.....	3
3	UEFI Settings.....	3
4	OS Settings.....	4
4.1	Install platform specific drivers (optional)	4
4.2	Configure OS to enable VBS, HVCI and System Guard	4
4.2.1	Windows Admin Center (WAC) (Preview)	4
4.2.2	Windows Security App (For Windows Server OS with Desktop experience only)	5
4.2.3	Configure Registry Key.....	7
5	Confirm the Secured-core state.....	8
5.1	TPM 2.0.....	8
5.2	Secure boot, Kernel DMA Protection, VBS, HVCI and System Guard	8
6	Support.....	8

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.

AZS-6112, AZS-6212, AZS-6224, HCI-6112, HCI-6208, HCI-6212, HCI-6224, Kepler 2-Node (with 3rd Gen Intel® Xeon), Kepler 3-Node (with 3rd Gen Intel® Xeon)

3 UEFI Settings

Prerequisite

1. TPM Firmware v7.85 – To find the version on your server, use `(Get-TPM).ManufacturerVersion` in PowerShell as Administrator.
2. Intel BIOS version SE5C620.86B.01.01.**0004**.x or higher

Note: BIOS version .0004 can only support single boot drive with Secured-Core features enabled. Future version (version number TBD) will support RAID 1 boot.

Configure BIOS/UEFI for Secured-Core

- **Enter BIOS/UEFI Setup**
 1. Boot System
 2. F2 to enter into Setup screen
- **Verify Virtualization Technology is enabled**
 1. Select Advanced
 2. Select Processor Configuration
 3. Ensure Intel® Virtualization Technology is already enabled. If it's not enabled, select the item and Enter.
 4. Esc to go back to the Advanced screen
- **Enable Intel® VT for Directed I/O**
 1. Select Integrated IO Configuration from the Advanced page
 2. Enable Intel® VT for Directed I/O
 3. Enable ACS Control
 4. Enable DMA Control Opt-In Flag
 5. Enable Pre-boot DMA Protection
 6. Esc to go back to the Advanced screen
- **Enable Intel® TXT – this needed previous setting enabled before it's available**
 - Select Processor Configuration
 - Enable Intel® TXT
 - Esc **twice** to go back to the initial Setup screen
- **Enable Secure Boot**
 - Select Boot Maintenance Manager
 - Select Advanced Boot Options
 - Select Secure Boot Configuration
 - Enable Attempt Secure Boot
- **Save** all of the settings by hitting F10 then Y to Save and Exit

4 OS Settings

4.1 Install platform specific drivers (optional)

None

4.2 Configure OS to enable VBS, HVCI and System Guard

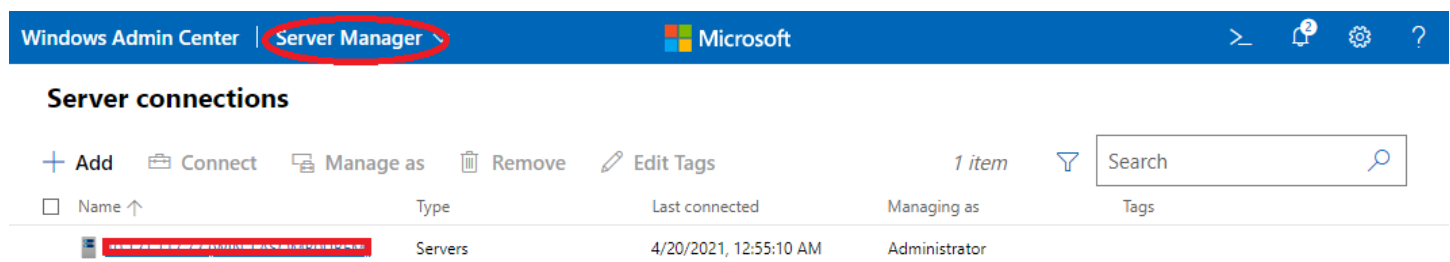
To configure Secured-core features on the OS, there are several different ways to do it. Choose one of the following 3 options to enable VBS, HVCI and System Guard.

4.2.1 Option 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.



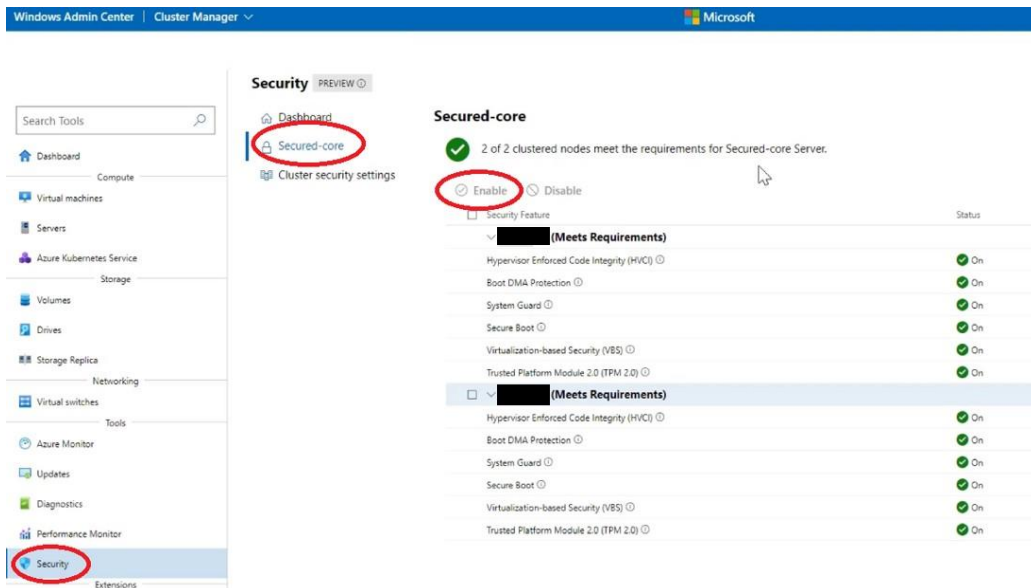
Scroll down for "Security" in the Tools menu on the left.

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

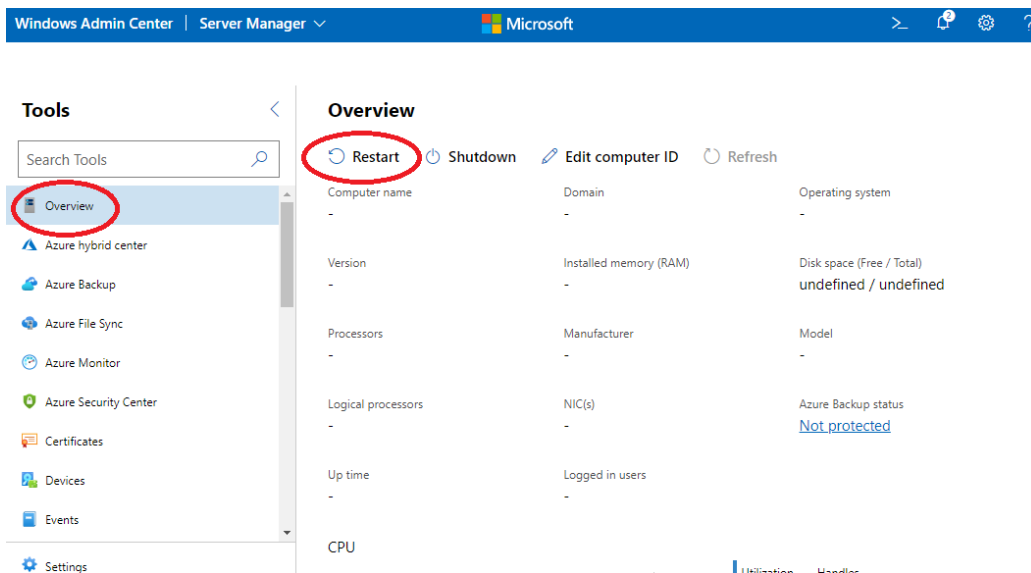
Click on a feature name that doesn't show as "On" and click "Enable". Repeat this for all disabled features.

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.

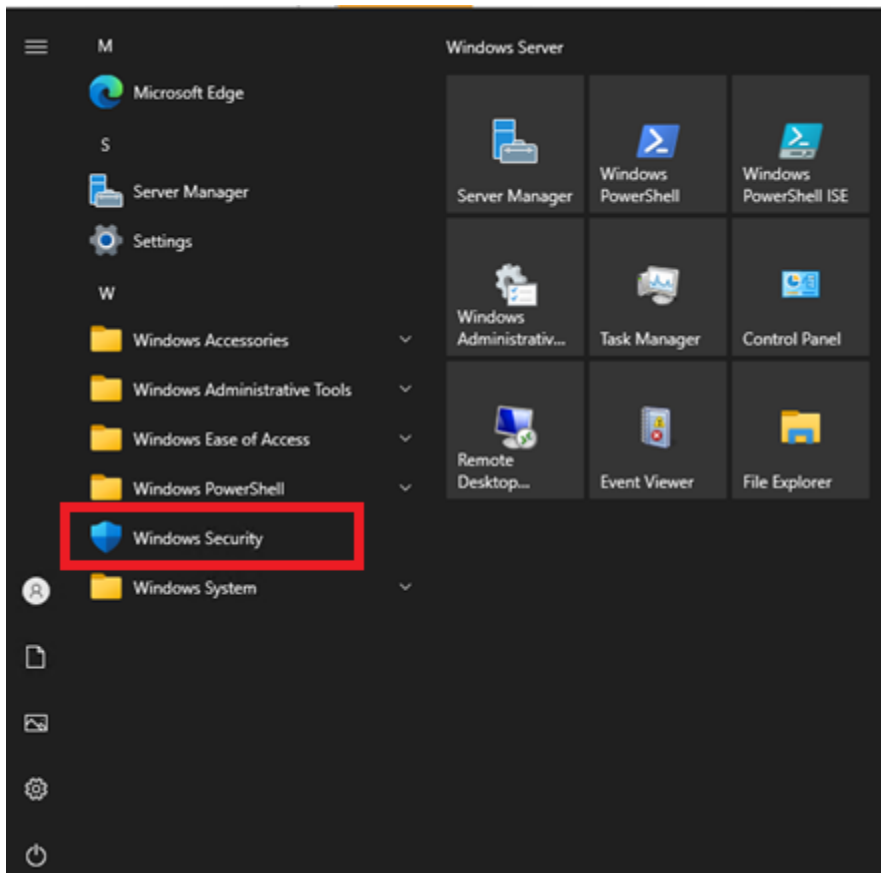


You will be prompted for a reboot for the changes to take effect. Go to "Overview" and click "Restart".

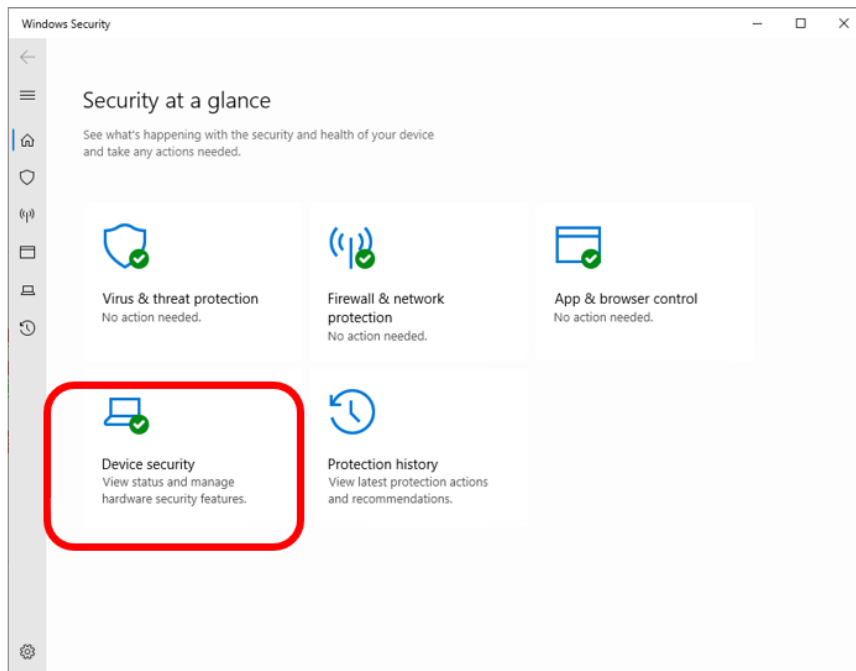


4.2.2 Option 2 - Windows Security App (For Windows Server OS with Desktop experience only)

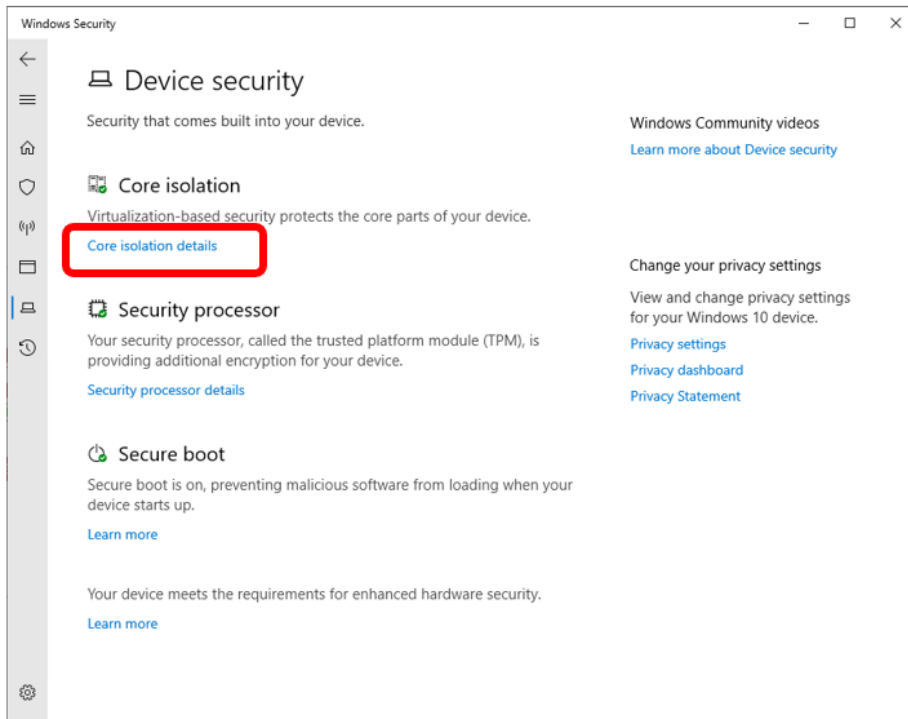
Launch the Windows Security app from the start menu.



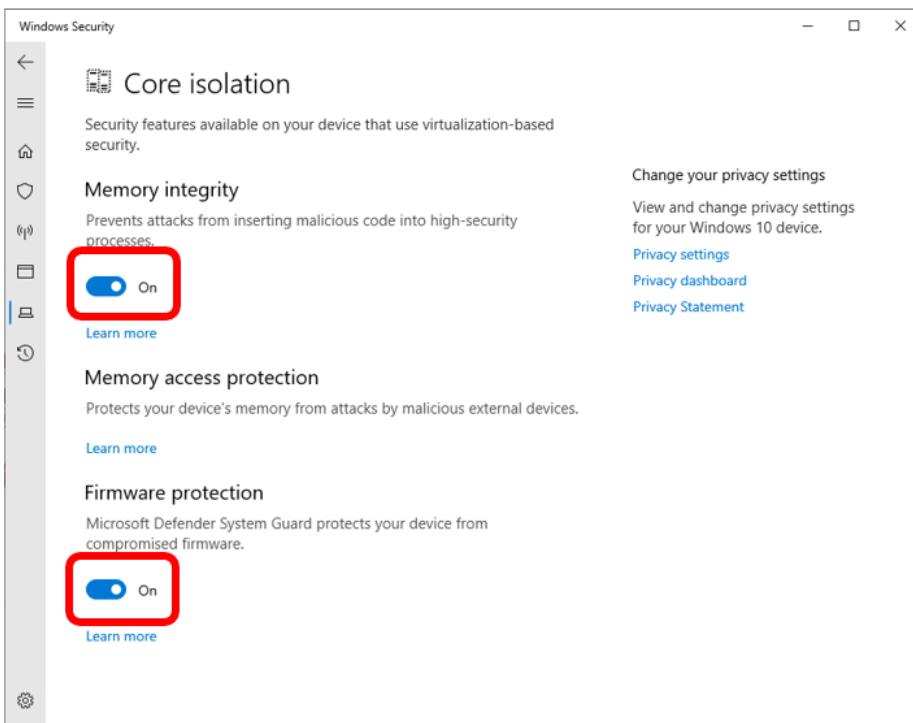
Choose "Device security".



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 Option 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

Contact DataON Support using the following methods:

1. Email: support@dataonstorage.com
2. Web: <https://dataonsupport.dataonstorage.com>
3. Phone: (714) 441-8820