Microsoft

Secured-core Servers

Enabling Guide

HCI Validated Nodes for Azure Stack HCI

Powered by 3rd Gen Intel® Xeon® Scalable Processors

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.

QuantaGrid D53XQ-2U, QuantaGrid D53X-1U

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. QCT BIOS version 3A18.Q202 or higher

Configure BIOS/UEFI for Secured-Core

- **Enter BIOS/UEFI Setup**
  1. Power on the System
  2. Press **F2** or **Del** into Setup screen
- **Enable Intel® VT for Directed I/O (VT-d)**
  1. Select Setup Utility
  2. Select Socket Configuration -> IIO Configuration from the Advanced screen
  3. Select Intel® VT for Directed I/O (VT-d) -> Press **Ctrl + F7** to open more features
  4. Enable **Intel® VT for Directed I/O**
  5. Enable **PCIe ACSCTL**
  6. Enable **DMA Control Opt-In Flag**
  7. Enable **Pre-boot DMA Protection**
  8. Press **ESC twice** to go back to the Advanced screen
- **Enable Intel® TXT**
  1. Select Socket Configuration -> Processor Configuration from the Advanced screen
  2. Enable **VMX**
  3. Enable **Enable SMX**
  4. Enable **Intel® TXT**
  5. Press **ESC twice** to go back to the Advanced screen
  6. Select TPM 2.0 Provision from the Security screen
  7. Enable **TPM 2.0 Provisioning**
  8. Press **ESC** to go back to the Security screen
- **Enable Secure Boot**
  - Select Administer Secure Boot
  - Enable **Enforce Secure Boot**
  - Press **F10** to save and exit (Maybe restart the System)
- **Make sure and save all of the above settings**

4 OS Settings

4.1 Install platform specific drivers (optional)

None.

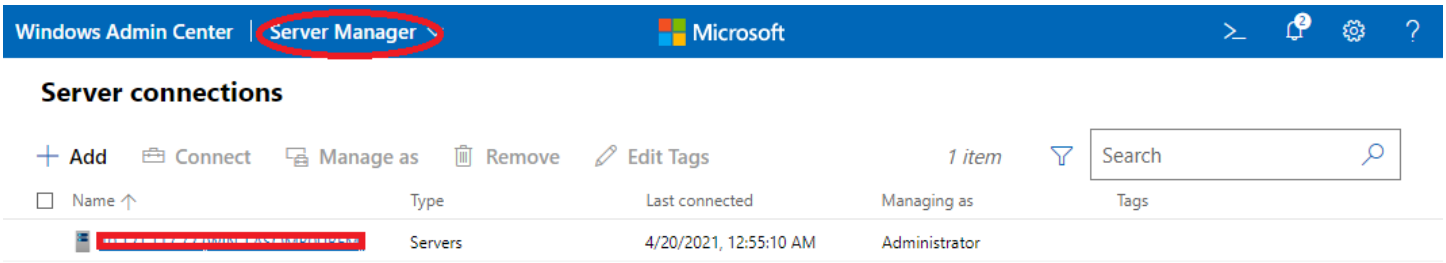
4.2 Configure OS to enable VBS, HVCI and System Guard

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 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.



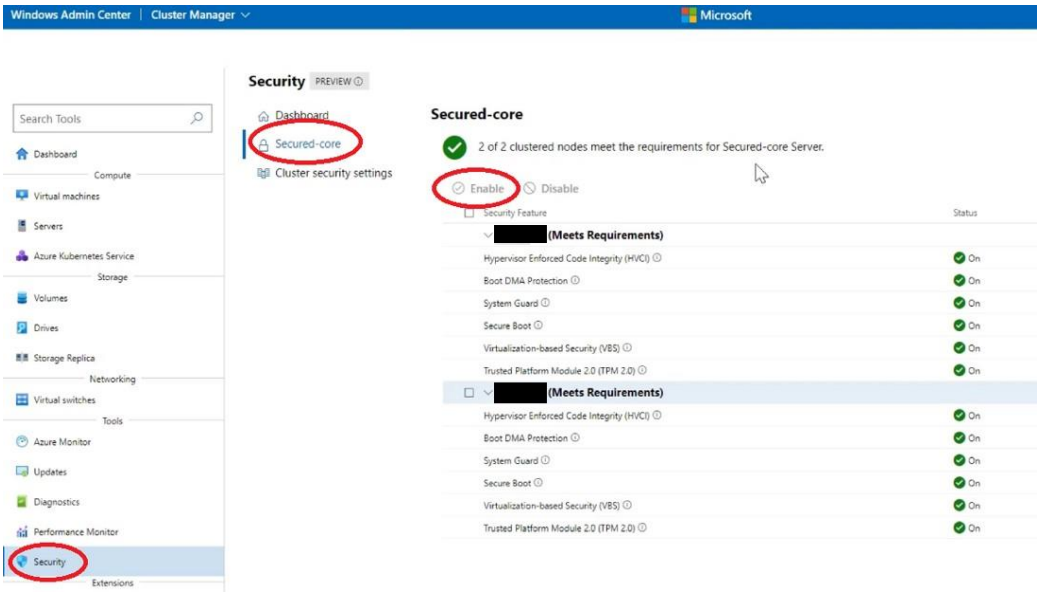
Scroll down for "Security" in the Tools menu on the left.

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

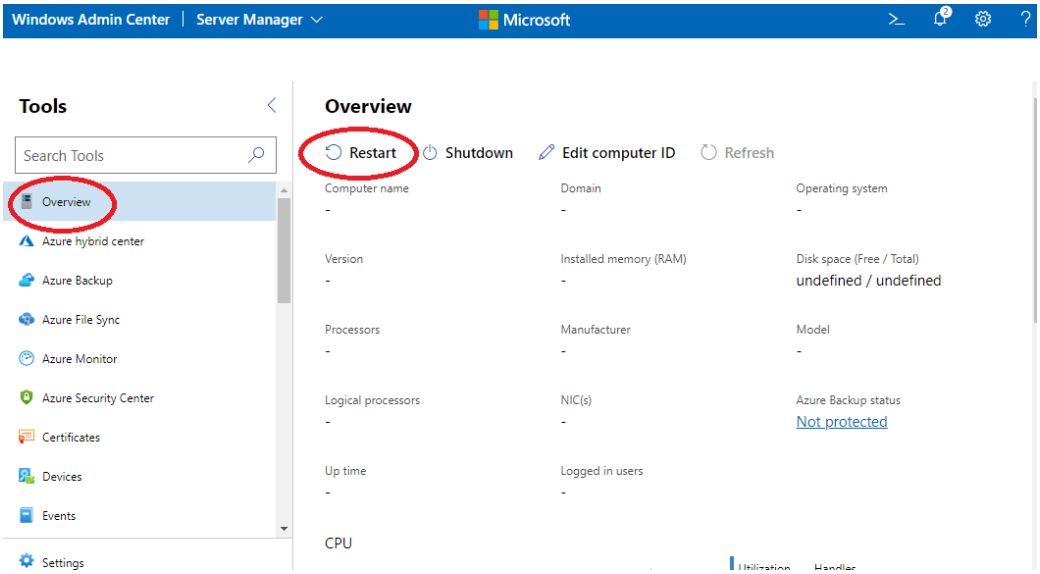
Click on a feature name that doesn't show as "On" and click "Enable". Repeat this for all disabled features.

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.

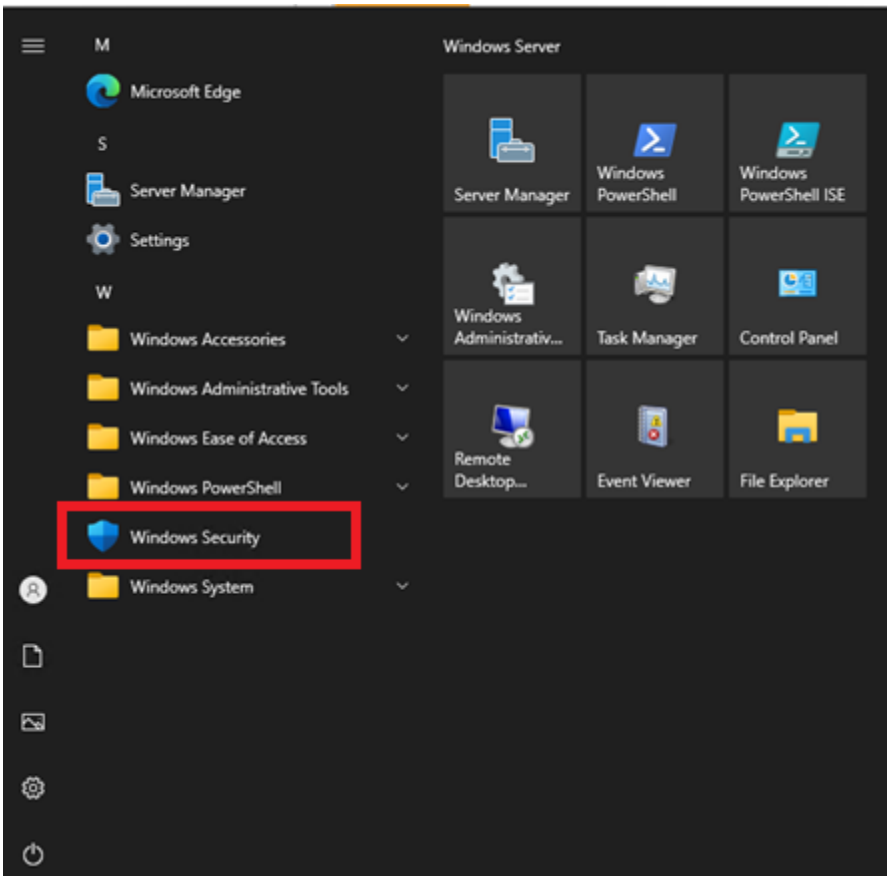


You will be prompted for a reboot for the changes to take effect. Go to “Overview” and click “Restart”.

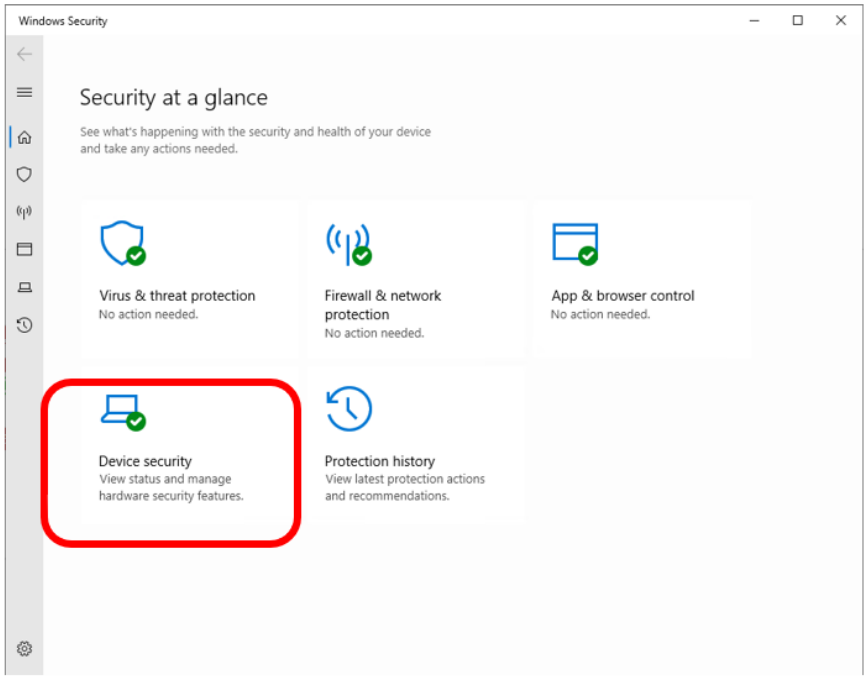


4.2.2 Windows Security App (For Windows Server OS with Desktop experience only)

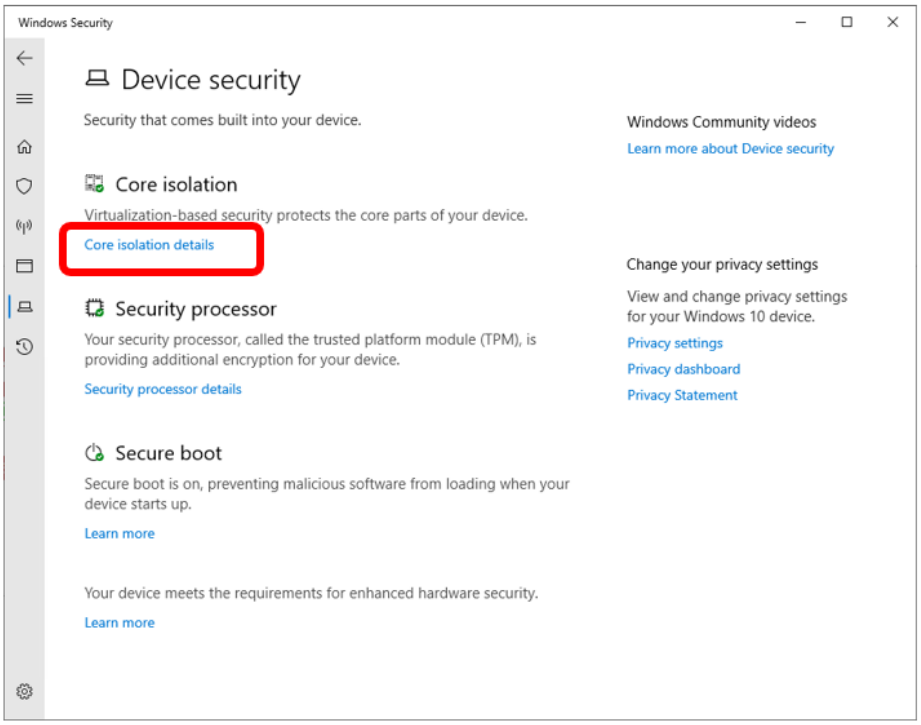
Launch the Windows Security app from the start menu.



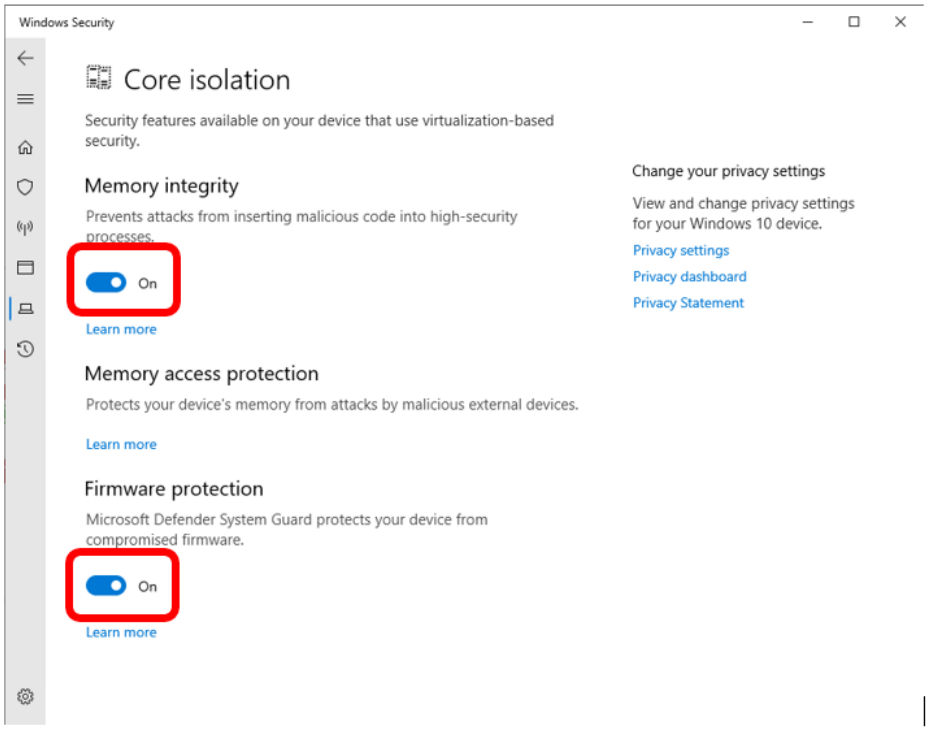
Choose “Device security”.



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

Contact QCT Support using the following methods:

1. E-mail: https://go.qct.io/contact/contact-qct-solutions/
2. Web: https://www.qct.io
3. Phone: +886-3-286-0707