Guide Cisco public IIIIII CISCO The bridge to possible

Secured-Core Servers Enabling Guide

Cisco UCS C240 M6 Rack Servers

Contents

1. Overview	3
2. Applicable products	3
3. UEFI settings	4
4. OS settings	6
4.1. Install platform-specific drivers (optional)	6
4.2. Configure OS to enable VBS, HVCI, and Windows Defender System Guard	6
4.2.1 Windows Admin Center (WAC)	6
4.2.2 Configure registry key	7
4.2.3 Windows Security App (for Windows Server OS with Desktop experience only)	8
4.2.4 Configure registry key	10
5 Confirm the secured-core state	10
5.1. TPM 2.0	10
5.2. Secure boot, Kernel DMA Protection, VBS, HVCI and Windows Defender System Guard	10
6. Support	11

1. Overview

The Secured-core functionality spans the following areas:

Hardware root-of-trust: Trusted Platform Module 2.0 (TPM 2.0) come standard with Secured-core servers. TPM 2.0 provides a secure store for sensitive keys and data, such as measurements of the components loaded during boot. This hardware root-of-trust raises the protection provided by capabilities like BitLocker which uses the TPM 2.0 and facilitates creating attestation-based workflows that can be incorporated into zero-trust security strategies.

Firmware protection: There is a clear rise in security vulnerabilities being reported in the firmware space given the high privileges that firmware runs with and the relative opacity of what happens in firmware to traditional anti-virus solutions. Using processor support for Dynamic Root of Trust of Measurement (DRTM) technology, along with DMA protection, Secured-core systems isolate the security critical hypervisor from attacks such as this.

Virtualization-Based Security (VBS): Secured-core servers support VBS and Hypervisor-based Code Integrity (HVCI). VBS and HVCI protects against this entire class of vulnerabilities given the isolation VBS provides between the privileged parts of the operating system such as the kernel and the rest of the system. VBS also provides additional capabilities that customers can enable like Credential Guard which better protects domain credentials.

For more information on Secured-core server, click on the following link:

https://learn.microsoft.com/en-us/windows-server/security/secured-core-server.

This document provides 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.

Cisco UCS[®] C240 M6 Rack Servers

The Secured-core Server AQ for Cisco UCS C240 M6 can be viewed by clicking on the link below:

https://www.windowsservercatalog.com/item.aspx?idltem=E54A6B96-A7E5-F36E-B057-FB242217F960&bCatID=1333.

Windows Server 2022 Certified	Windows Server 2019 Windows Server 2016 UCS (by Cis) Certified Certified	co Systems, Inc.
Compat	ible with the followir	ng versions of Microsoft Windows
Windows Garage 2822 Certified	Windows Server 2022 x64	 Certified for Windows NV-DIMM-I Capable Secured-core Server Software-Defined Data Center (SDDC) Premium
Windows Songe 2019 Cartified	Windows Server 2019 x64	Certified for Windows Hardware Assurance NV-DIMM-I Capable Software-Defined Data Center (SDDC) Premium
Windows Server 2016 Cartified	Windows Server 2016 x64	 Certified for Windows Hardware Assurance Software-Defined Data Center (SDDC) Premium

3. UEFI settings

Cisco UCS server firmware release 4.2(2f) or later is required to enable and configure secured core on Cisco UCS C240 M6 standalone rack servers. The image below shows the minimum server firmware and BIOS version required to enable Secured-core feature on UCS C240 M6 servers:

🗲 diala Cisco	Integrated Management Controller			
A / Chassis / Sum	mary 🚖			
Server Proper	ties	Cisco Integrated M	Management Controller (Cisco IM	AC) Information
Product Name:	UCS C240 M8SN	Hostname:	C240-WZP260901KW	
Serial Number:	WZP260901KW	IP Address:	192.168.0.235	
PID:	UCSC-C240-M6SN	MAC Address:	EC:F4:0C:0D:8C:A0	
UUID:	AE73D3B2-CA4C-4396-AE6E-844EC226D950	Firmware Version:	4.2(2f)	
BIOS Version:	C240M6.4.2.2f.0.0806222232	Current Time (UTC):	Tue Nov 15 09:42:32 2022	
Description:		Local Time:	Tue Nov 15 01:42:32 2022 PST -0800 (NTP)	
Asset Tag:	Unknown	Timezone:	America/Los_Angeles	Select Timezone

Download and upgrade the server firmware using the Cisco UCS Host Upgrade Utility (HUU) from the link below:

https://software.cisco.com/download/home/286329285/type.

Refer to the link below for a step-by-step guide to upgrade the server firmware using the Cisco UCS Host Upgrade Utility:

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/lomug/4-2/b_cisco-host-upgradeutility-user-guide-4-2/m_upgrading-the-firmware.html. Log in to Cisco[®] Integrated Management Controller (IMC) and navigate to the **Compute > BIOS > Configure Boot Order** tab and complete the below steps:

- Select **UEFI** from the drop-down menu for **Configured Boot Mode**.
- Enable UEFI Secure Boot by clicking on the check box and click on the Save Changes box to save the settings.

You will be prompted for a reboot for the changes to take effect.

*	cisco Integrate	d Management	Controller		
n / Cor	mpute / BIOS 🔺				
BIOS	Remote Management	Power Policies	PID Catalog	Persistent Memory	
Enter BIG	OS Setup Clear BIOS CMOS	Restore Manufacturir	ng Custom Settings	Restore Defaults	
Config	ure BIOS Configure Bo	ot Order Config	ure BIOS Profile	Secure Boot Certificate Management	
BIOS	Properties				
	Runnin UEFI Sec Actual B	g Version C240M6.4 cure Boot 🗹 oot Mode Uefi	4.2.2f.0.0806222232	1	
	Configured B	oot Mode UEFI		(UEFI Secure Boot is enabled, disable it to modify Configured Boot Mo	de.)
	Last Configured Boot Orde	er Source CIMC		¥	

In Cisco Integrated Management Controller (IMC), navigate to the **Compute > BIOS > Configure BIOS > Security** tab and enable the following settings and click **Save**.

- **Trusted Platform Module State** Trusted Platform Module (TPM), which is a component that securely stores artifacts that are used to authenticate the server. The platform-default setting is enabled.
- **TPM Minimal Physical Presence** TPM Minimal Physical Presence, which enables or disables the communication between the OS and BIOS for administering the TPM without compromising the security. The platform-default setting is disabled.
- Intel Trusted Execution Technology (TXT) Support Intel Trusted Execution Technology (TXT), which
 provides greater protection for information that is used and stored on the business server. The platformdefault setting is enabled and when you only enable TXT, it implicitly enables TPM, VT, and VTDio.
- **DMA Control Opt-In Flag** Enabling this token enables Windows 2022 Kernel DMA Protection feature. The OS treats this as a hint that the IOMMU should be enabled to prevent DMA attacks from possible malicious devices. The platform-default setting is disabled.

A / Compute / BIOS ★ BIOS Remote Management Power Polici Enter BIOS Setup Clear BIOS CMOS Restore Manu Configure BIOS Configure Boot Order Ca I/O Server Management Security P Note: Default values are shown in bold. Reboot Host Immediately:	ies PID Catalog P ifacturing Custom Settings onfigure BIOS Profile Processor Memory	ersistent Memory Restore Defaults Secure Boot Certificate Manage Power/Performance	ment	
BIOS Remote Management Power Polici Enter BIOS Setup Clear BIOS CMOS Restore Manu Configure BIOS Configure Boot Order Cr I/O Server Management Security P Note: Default values are shown in bold. Reboot Host Immediately:	ies PID Catalog P ifacturing Custom Settings onfigure BIOS Profile Processor Memory	ersistent Memory Restore Defaults Secure Boot Certificate Manage Power/Performance	ment	
Enter BIOS Setup Clear BIOS CMOS Restore Manu Configure BIOS Configure Boot Order Cd V/O Server Management Security P Note: Default values are shown in boot. Reboot Host Immediately: SHA-1 PCR Bank: Enabled TPM Pending Operation: None Intel Trusted Execution Technology Sup Enabled	onfigure BIOS Profile	Restore Defaults Secure Boot Certificate Manage Power/Performance	ment	
Configure BIOS Configure Boot Order Configure BIOS Configure Boot Order	onfigure BIOS Profile	Secure Boot Certificate Manage Power/Performance	ment	
I/O Server Management Security P Note: Default values are shown in book. Reboot Host Immediately: SHA-1 PCR Bank: Enabled TPM Pending Operation: None Intel Trusted Execution Technology Sup Enabled	rocessor Memory	Power/Performance		
Note: Default values are shown in bold. Reboot Host Immediately: SHA-1 PCR Bank: Enabled TPM Pending Operation: None Intel Trusted Execution Technology Sup Enabled				
Reboot Host Immediately: SHA-1 PCR Bank: Enabled TPM Pending Operation: None Intel Trusted Execution Technology Sup Enabled				
SHA-1 PCR Bank: Enabled TPM Pending Operation: None Intel Trusted Execution Technology Sup Enabled				
TPM Pending Operation: None Intel Trusted Execution Technology Sup Enabled		Trusted Platfo	rm Module State: Enabled	•
Intel Trusted Execution Technology Sup Enabled		si	HA256 PCR Bank: Enabled	•
	- i *	TPM Minimal PI	hysical Presence: Enabled	•
Total Memory Encryption (TME): Enabled	i v	Pow	er ON Password: Disabled	d 💌
SW Guard Extensions (SGX): Disable	d 🔻	Multikey Total Memory End	cryption (MK-T Disabled	d 💌
SGX Pkg info In-Band Access: Disable	d 🔻	so	X Factory Reset: Disabled	d v
Select Owner EPOCH input type: Manual	User Defined Owner EP(👻	Ĩ	SGX QoS: Enabled	•
SGX Auto MP Registration Agent: Disable	d v	s	GX Write Enable: Enabled	•
SProcessor Epoch 1: 0		SPro SPro	ocessor Epoch 0: 0	
SGX PUBKEY HASH1: 0		SGX SGX	PUBKEY HASH0: 0	
SGX PUBKEY HASH3: 0		SGX SGX	PUBKEY HASH2: 0	
DMA Control Opt-In Flag: Enabled				•
	i v	LIMIT C	PU PA to 46 Bits: Enabled	

4. OS settings

4.1. Install platform-specific drivers (optional)

Post OS installation, download the relevant Windows driver image for the Cisco UCS server software from the link below, and install the drivers for chipset, storage, network, etc.

https://software.cisco.com/download/home/286329285/type/283853158/release/4.2(2d).

4.2. Configure OS to enable VBS, HVCI, and Windows Defender System Guard

To configure secured-core features on the OS, there are several different ways to do so. Choose one of the following three options to enable VBS, HVCI, and Windows Defender System Guard.

4.2.1 Windows Admin Center (WAC)

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

From the Server Manager view, choose the target server.

Windows Admin Center \mid Server Manager \vee		-	Microsoft	>_	Ω	۲
Server connections						
+ Add 🖻 Connect 🖷 Manage as	Remove	Edit Tags	5 items 🛛 Search			Q
□ Name ↑	Туре	Last connected	Managing as	Tags		
azs-hci1-n1.ucs-spaces.lab	Servers	Never	ucs-spaces\hciadmin	azs-hci-m	6-c1.ucs	spaces.lab.
azs-hci1-n2.ucs-spaces.lab	Servers	Never	ucs-spaces\hciadmin	azs-hci-m	6-c1.ucs	spaces.lab.
azs-hci1-n3.ucs-spaces.lab	Servers	Never	ucs-spaces\hciadmin	azs-hci-m	6-c1.ucs	spaces.lab.
azs-hci1-n4.ucs-spaces.lab	Servers	Never	ucs-spaces\hciadmin	azs-hci-m	6-c1.ucs	-spaces.lab.

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

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

Click on a feature name that does not 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 that all of the secured-core features are showing as "On" before proceeding to validation.

Tools	Security PREVIEW ①	
Search Tools	Summary Protection history Secured-core	
Local users & groups	What is Secured-core server?	
📥 Networks	Your device meets all requirements for Secured-core Serv	ver.
🕵 Packet monitoring		
fif Performance Monitor	Enable Disable Security Feature	Status
PowerShell	Hypervisor Enforced Code Integrity (HVCI)	🕑 On
Processes	Boot DMA Protection \odot	🕑 On
III Registry	System Guard ①	🕗 On
	Secure Boot ①	📀 On
🐼 Remote Desktop	Virtualization-based Security (VBS)	🕑 On
- Roles & features	Trusted Platform Module 2.0 (TPM 2.0) ①	🕑 On
5 Scheduled tasks		
💎 Security		

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

Windows Admin Center	Server Manager	V Micros	oft	≻	Ω	۲
azs-hci1-n1.ucs-	spaces.lab					
Tools	<	Overview				
Search Tools	Q	🔿 Restart 🕐 Shutdown 🕜 Enable Disk Me	etrics 🧷 Edit computer ID			
Overview	c *	Computer name Domain azs-hci1-n1 ucs-spaces.lab	Operating syst Microsoft A	tem Zure S	tack H	ICI

4.2.2 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

4.2.3 Windows Security App (for Windows Server OS with Desktop experience only)

Launch the Windows Security app from the start menu.



Choose "Device security" and then 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.

4.2.4 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 that all of the secured-core features are properly configured and running, complete the following steps:

5.1. TPM 2.0

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

TpmPresent	1	True
TpmReady	:	True
TpmEnabled	:	True
TpmActivated	:	True

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

Launch msinfo32 from the 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

https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html.

Americas Headquarters

Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at https://www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA