Microsoft

Secured-core Servers

Enabling Guide

March 2022

NEC Corporation

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.

https://www.58support.nec.co.jp/global/download/w2022/index.html

3 UEFI Settings

Enable "**Microsoft(R) Secured-core Support**" by using "System Utility"*.

System Utilities ＞ System Configuration > BIOS/Platform Configuration (RBSU) > Server Security
Microsoft(R) Secured-core Support = [Enabled] (default: Disabled)

* Please refer "Users Guide" for the server to find "System Utility".
https://www.58support.nec.co.jp/global/download/
(Please search "Model Name" to find the server at "Search by Model")

4 OS Settings

4.1 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.

4.1.1 Configure Registry Key

Open command prompt with Administrator privileges and run following commands to set registry keys.

```
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