Microsoft

Secured-core Servers

Enabling Guide

Lenovo

ThinkAgile MX Series

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.

Lenovo ThinkAgile MX650V3 IS Integrated systems & ThinkAgile MX650V3 VN validated nodes (based on SR650 V3)

Lenovo ThinkAgile MX630V3 IS Integrated systems & ThinkAgile MX630V3 VN validated nodes (based on SR630 V3)

Lenovo ThinkAgile MX3530 Integrated Systems and ThinkAgile MX3531 Validated nodes which are based on Lenovo ThinkSystem SR650 V2 servers.

Lenovo ThinkAgile MX3330 Integrated Systems and ThinkAgile MX3331 Validated nodes which are based on Lenovo ThinkSystem SR630 V2 servers.

Lenovo ThinkEdge SE450 validated nodes.

Lenovo ThinkSystem SR250 V2, ST250 V2 and ST50 V2 validated nodes.

Lenovo ThinkSystem SR665 validated nodes
Lenovo ThinkSystem SR655 validated nodes
Lenovo ThinkSystem SR645 validated nodes
Lenovo ThinkSystem SR635 validated nodes

3 UEFI Settings

To enable Secured-core feature, ensure the firmware version installed in your system can fulfill the requirement. The recommendation is to use the latest firmware version for your server to get Secured-core support.

3.1 Enabling Secured-core in UEFI for Intel-based system

For Intel-based system, make sure the following UEFI settings are enabled.

- System Settings -> Security -> Secure Boot Configurations -> Secure Boot Settings
- System Settings -> Security -> Secure Boot Configurations -> Trusted Platform Module -> TPM 2.0
- System Settings -> Socket Configuration -> Processor Configuration -> Trusted Execution Technology
- System Setting -> Devices and I/O Ports -> Intel VT for Directed I/O (VT-d)

- System Setting -> Devices and I/O Ports -> DMA Control Opt-In Flag

3.2 Enabling Secured-core in UEFI for AMD based 1-socket system

AMD EPYC 7002 Series processors don't support Secured-core. Lenovo ThinkSystem SR635 and SR655 feature both AMD EPYC 7002 and AMD EPYC 7003 families of processors. To enable Secured-core on Lenovo SR635 and SR655, you'd make sure your processors are belong to AMD EPYC 7003, not AMD EPYC 7002.

To support Secured-core for AMD-based 1-socket system, you will need to enable the following UEFI items.

- System Configuration and Boot Management -> Security -> Secure Boot
- System Configuration and Boot Management -> Security -> Trusted Computing -> TPM 2.0 Device Found
- System Configuration and Boot Management Socket Configuration ->Advanced -> CPU Configuration -> Secured-Core

3.3 Enabling Secured-core in UEFI for AMD based 2-socket system

Like Lenovo ThinkSystem SR635 and SR655, ThinkSystem SR645 and SR665 also feature both AMD EPYC 7002 and AMD EPYC 7003 families of processors. To enable Secured-core on Lenovo SR645 and SR665, you'd make sure your processors are belong to AMD EPYC 7003, not AMD EPYC 7002.

To support Secured-core for AMD-based 2-socket system, you will need to enable the following UEFI items.

- System Settings -> Security -> Secure Boot Configurations -> Secure Boot Setting
- System Settings -> Security -> Secure Boot Configurations -> Trusted Platform Module -> TPM 2.0
- System Settings ->Processors -> Secured-Core -> Secured-Core

4 OS Settings

4.1 Install platform specific driver

To support Secured-core on AMD-based system, after UEFI setting is ready we should install platform specific driver. After the driver is installed successfully, AMD EPYC DRTM Driver should be found in device manager Please make sure UEFI setting is ready for Secured-core before installing chipset driver on AMD-based system because this driver depends on Secured-core setting in UEFI.

For Intel-based system, no platform specific driver needs to be installed for Secured-core.

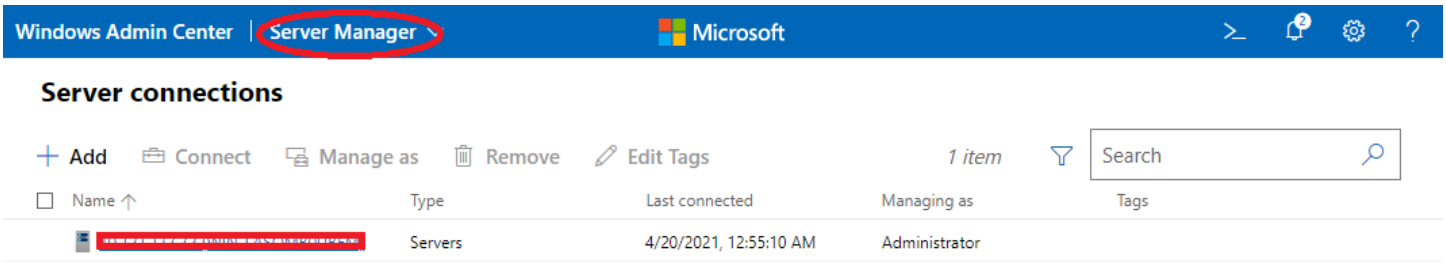
4.2 Configure OS to enable VBS, HVCI and System Guard

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.



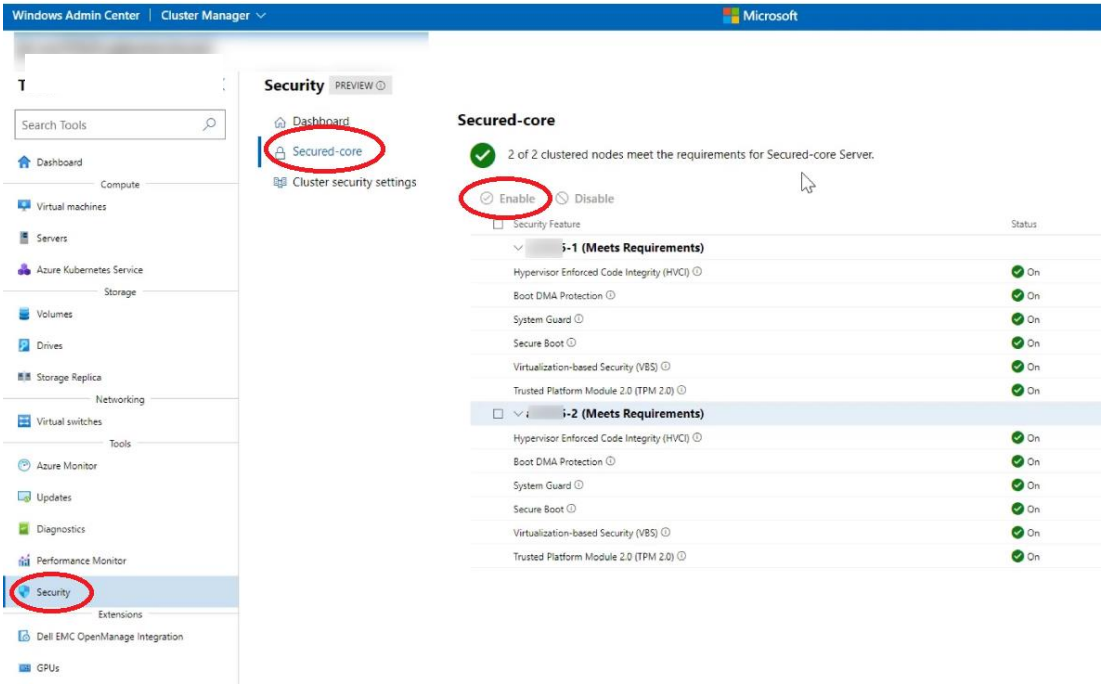
Scroll down for “Security” in the Tools menu on the left.

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

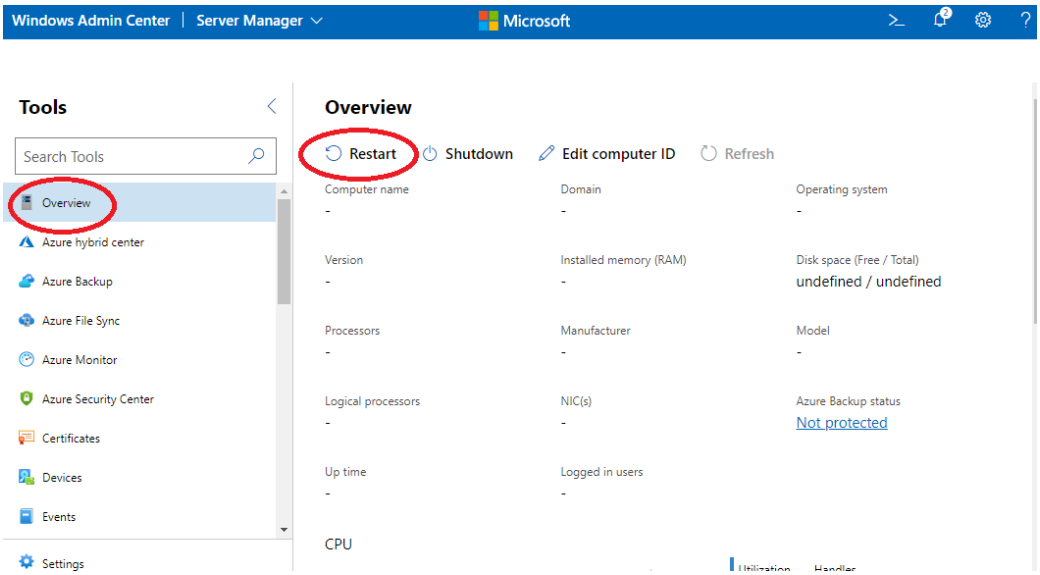
Click on a feature name that doesn’t show as “On” and click “Enable”. Repeat this for all disabled features.

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 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 /

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

You can contact Support to obtain help for your issue.

You can receive hardware service through a Lenovo Authorized Service Provider. To locate a service provider authorized by Lenovo to provide warranty service, go to https://datacentersupport.lenovo.com/ service provider and use filter searching for different countries. For Lenovo support telephone numbers, see https://datacentersupport.lenovo.com/supportphonelist for your region support details.