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 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.

3 UEFI Settings

To enable Secured-core feature, first you need to update the UEFI version to be later than Nov, 2021. Second, please 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 -> Enable Intel TXT
- 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

4 OS Settings

4.1 Install platform specific drivers (optional)

This section is intentionally left blank.

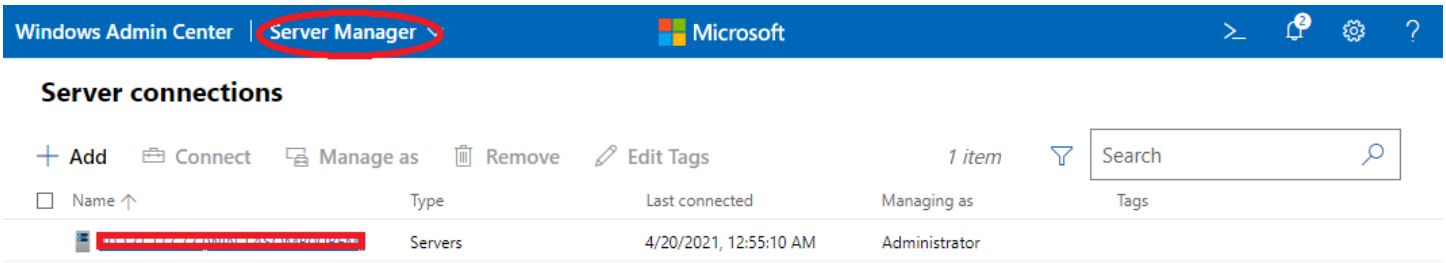
4.2 Configure OS to enable VBS, HVCI and System Guard

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.



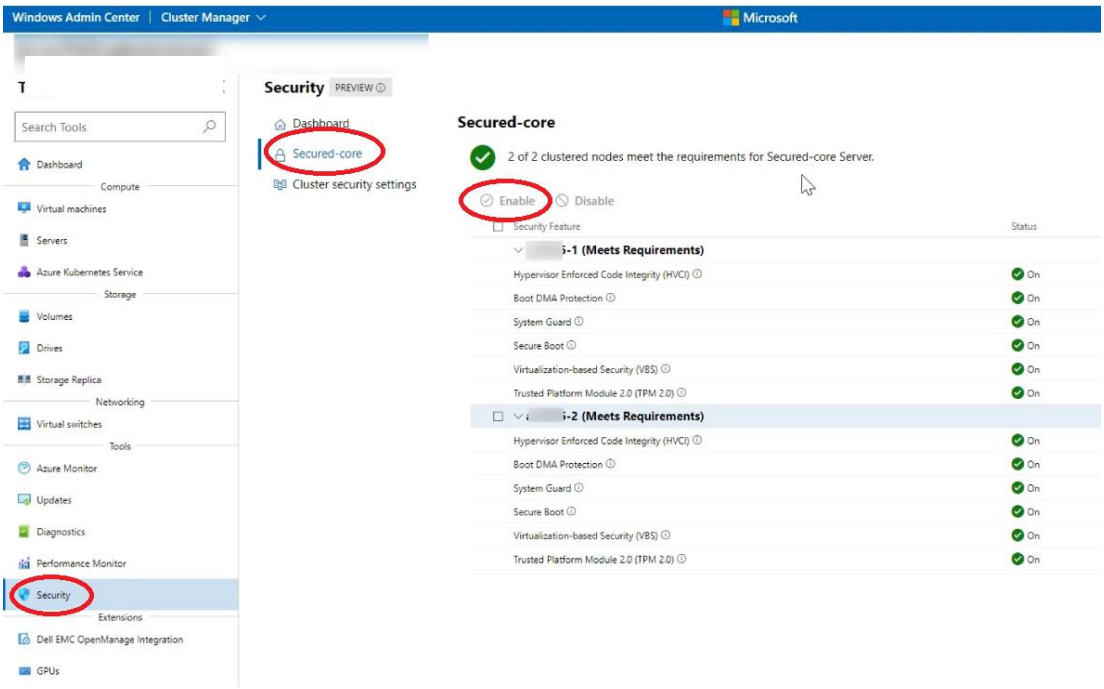
Scroll down for “Security” in the Tools menu on the left.

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

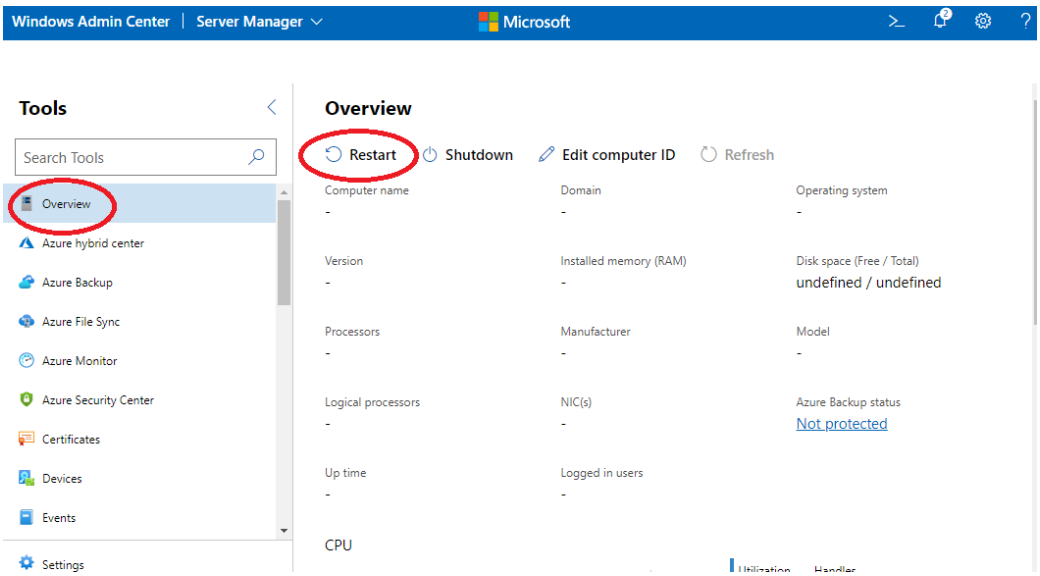
Click on a feature name that doesn’t show as “On” and click “Enable”. Repeat this for all disabled features.

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.