

Configure Secured-core server

Article • 09/01/2023

Secured-core is a collection of capabilities that offers built-in hardware, firmware, driver and operating system security features. This article shows you how to configure Secured-core server by using Windows Admin Center, the Windows Server Desktop Experience, and Group Policy.

Secured-core server is designed to deliver a secure platform for critical data and applications. For more information, see [What is Secured-core server?](#)



Prerequisites

Before you can configure Secured-core server, you must have the following security components installed and enabled in the BIOS:

- Secure Boot.
- Trusted Platform Module (TPM) 2.0.
- System firmware must meet preboot DMA protection requirements and set appropriate flags in ACPI tables to opt into and enable Kernel DMA Protection. To learn more about Kernel DMA Protection, see [Kernel DMA Protection \(Memory Access Protection\) for OEMs](#).
- A processor with support enabled in the BIOS for:
 - Virtualization extensions.
 - Input/Output Memory Management Unit (IOMMU).
 - Dynamic Root of Trust for Measurement (DRTM).
 - Transparent Secure Memory Encryption is also required for AMD based systems.

Important

Enabling each of the security features in the BIOS can vary based on your hardware vendor. Make sure to check your hardware manufacturer's Secured-core server enablement guide.

You can find hardware certified for Secured-core server from the [Windows Server Catalog](#) , and Azure Stack HCI servers in the [Azure Stack HCI Catalog](#) .

Enable security features

To configure Secured-core server you need to enable specific Windows Server security features, select the relevant method and follow the steps.

GUI

Here's how to enable Secured-core server using the user interface.

1. From the Windows desktop, open the **Start** menu, select **Windows Administrative Tools**, open **Computer Management**.
2. In Computer management, select **Device Manager**, resolve any device error if necessary.
 - a. For AMD based systems, confirm the DRTM Boot Driver device is present before continuing
3. From Windows desktop, open the **Start** menu, select **Windows Security**.
4. Select **Device security** > **Core isolation details**, then enable **Memory Integrity** and **Firmware Protection**. You might not be able to enable Memory Integrity until you've enabled Firmware Protection first and restarted your server.
5. Restart your server when prompted.

Once your server has restarted, your server is enabled for Secured-core server.

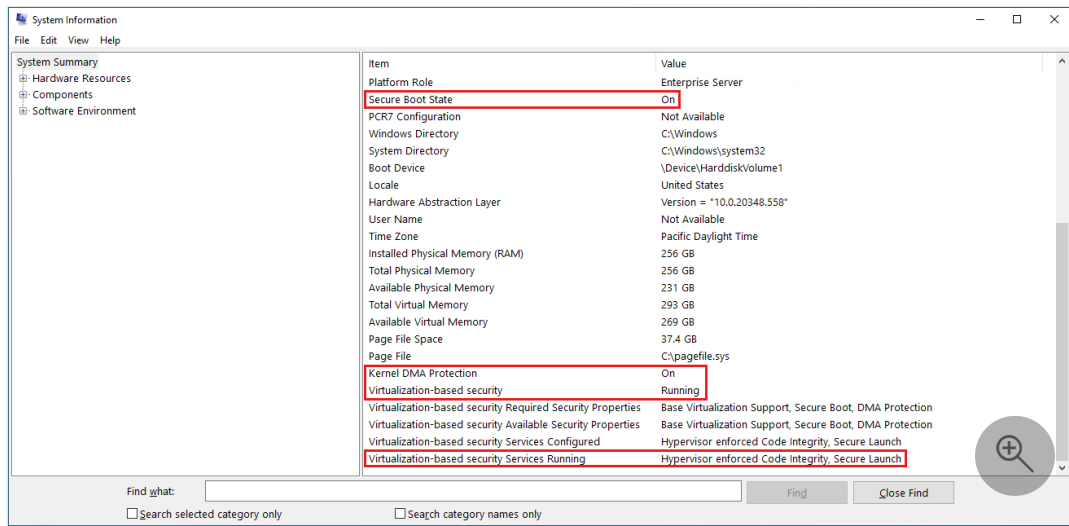
Verify Secured-core server configuration

Now that you've configured Secured-core server, select the relevant method to verify your configuration.

GUI

Here's how to verify your Secured-core server is configured using the user interface.

1. From the Windows desktop, open the **Start** menu, type `msinfo32.exe` to open System Information. From the System Summary page, confirm:
 - a. **Secure Boot State** and **Kernel DMA Protection** is On.
 - b. **Virtualization-based security** is Running.
 - c. **Virtualization-based security Services** Running shows **Hypervisor enforced Code Integrity** and **Secure Launch**.



Next steps

Now that you've configured Secured-core server, here are some resources to learn more about:

- [Virtualization-based Security \(VBS\)](#)
- [Memory integrity and VBS enablement](#)
- [System Guard Secure Launch](#)