HPE ProLiant Compute

Technical white paper

Implementing Microsoft Windows Server 2025 using HPE ProLiant servers, storage, and networking options

Contents

Overview 3
Windows Server 2025 editions 3
Windows Server diagnostic data (telemetry) 3
Service Pack for ProLiant (SPP) information 3
Supported HPE servers 3
Supported Processors 3
HPE ProLiant Gen10 Plus servers 4
HPE ProLiant Gen10 Plus v2 servers 5
HPE ProLiant Gen11 servers 5
HPE Alletra servers 5
HPE Cray servers 6
HPE Synergy servers 6
Additional HPE servers 6
HPE Storage 6
Configuring and validating Secured-core servers 7
Configuring Secured-core 7
Configuring UEFI/BIOS settings 8
Configuring Windows Server VBS, HVCI, and System Guard 8
Confirm the Secured-core state 10
Confirm Secure Boot, Kernel DMA Protection, VBS, HVCI, and System Guard 10
Installing Windows Server 2025 11
Windows Server 2025 mitigations for Meltdown and Spectre 11
Intel Virtual RAID on CPU (VROC) for HPE ProLiant Gen10 Plus and HPE ProLiant Gen11 servers 11
Drivers for Intel VROC 13
Installing Windows Server 2019, or Windows Server 2025 on an Intel VROC RAID volume 14
Installing the Service Pack for ProLiant (SPP) 15
Installing the Service Pack for ProLiant on Windows Server Core 16
Installing the Service Pack for ProLiant (SPP) on Windows Server 2025 with Desktop (UI) 17
Remote deployment 17
Procedure to add Baseline 17
Known issues 19
Resources 22

Overview

Windows Server 2025 is the next Windows Server Long Term Servicing Channel (LTSC) release from Microsoft. It features enhanced security as well as scalability and performance improvements. This document explains how to successfully implement Windows Server 2025 on HPE servers.

Windows Server 2025 editions

Windows Server 2025 is available in both Datacenter and Standard editions. The default installation is Server Core, but a full Desktop Experience can be optionally installed, and in this document, user guidance is available for both.

Note

You cannot convert between Windows Server 2025 installations of Server Core and Server with Desktop Experience. A change requires a complete reinstallation.

Windows Server diagnostic data (telemetry)

To continuously improve the quality of Windows Server, Microsoft encourages customers to provide feedback and diagnostic data. This diagnostic data is distinct from functional data, and Microsoft avoids collecting personal information wherever possible. HPE customers can benefit from the improvements made by Microsoft via the analysis of diagnostic data from Windows Server. Hewlett Packard Enterprise encourages our customers to enable telemetry to improve our customer support.

Service Pack for ProLiant (SPP) information

The SPP for supported HPE ProLiant servers has been tested with Windows Server 2025. Use 2024.09 SPP or newer from here: techlibrary.hpe.com/us/en/enterprise/servers/products/service_pack/spp/index.aspx

Supported HPE servers

Please visit the Windows Server Certification and Support | HPE to get the latest Windows Server OS support matrix on HPE servers.

Note

HPE ProLiant Gen9 and older servers are not supported on Windows Server 2025.
HPE ProLiant Gen10, Gen10 Plus, Gen11 servers are launched before Windows Server 2025 OS release, system ROM update to minimum version is required before installing Windows Server 2025. Please refer to Table 1 to Table 8.

Supported Processors

Several HPE servers support multiple generations of processors, thus it is advised that for older processors and if in doubt, check the following sources:

– Windows Server Catalog: windowsservercatalog.com/

– Windows Processor Requirements: Windows Processor Requirements | Microsoft Learn

For example, Intel® Second through Fifth Gen Xeon SP processors are supported so this excludes x1xx processors. Similarly, for AMD EPYC 7xx2 and 7xx3 are supported but EPYC 7xx1 are not supported. Some HPE servers support drop-in processor upgrades and the earlier processor model may not be supported.

Note

Microsoft guidance on Windows Server installation using AMD EPYC 9xx4 processors: learn.Microsoft.com/en-us/troubleshoot/windows- server/virtualization/support-and-installation-instructions-for-amd-epyc-9004-series-server-processors

The HPE ProLiant system ROMs and other HPE software and drivers are available in the latest SPP at spp.hpe.com.
For a complete list of supported options on your server, see the HPE QuickSpecs. Notes: HPE has implemented a new naming standard for help customers quickly and easily identify the network adapters, please refer the original and new product name mapping list, see Notice: HPE Network Adapters - Product Renaming Framework And Plan For HPE Network Adapters.

HPE ProLiant Gen10 servers

Table 1. Supported HPE ProLiant Gen10 servers

HPE server	ROM family	Minimum ROM version
HPE Edgeline EL8000 and HPE ProLiant e910	H08	3.20_05-27-2024
HPE Edgeline EL8000t and HPE ProLiant e910t	H08	3.20_05-27-2024
DL380 Gen10	U30	3.20_05-27-2024
DL160 Gen10	U31	3.20_05-27-2024
DL180 Gen10	U31	3.20_05-27-2024
DL360 Gen10	U32	3.20_05-27-2024
ML110 Gen10	U33	3.20_05-27-2024
DL560 Gen10	U34	3.30_07-31-2024
DL580 Gen10	U34	3.30_07-31-2024
XL420 Gen10	U39	3.30_07-31-2024
XL450 Gen10	U40	3.32_08-29-2024
ML350 Gen10	U41	3.20_05-27-2024

HPE ProLiant Gen10 Plus servers

Table 2. Supported HPE Gen10 Plus servers

HPE server	ROM family	Minimum ROM version
e920 Gen10 Plus	H10	2.22_09-05-2024
MicroServer Gen10 Plus	U48	3.40_08-01-2024
DL365 Gen10 Plus	A42	3.10_05-16-2024
DL385 Gen10 Plus	A42	3.10_05-16-2024
DL325 Gen10 Plus	A43	3.10_05-16-2024
DL345 Gen10 Plus	A43	3.10_05-16-2024
DL385 Gen10 Plus	A43	3.10_05-16-2024
XL225n Gen10 Plus	A46	3.10_05-16-2024
DL360 Gen10 Plus	U46	2.12_06-14-2024
DL380 Gen10 Plus	U46	2.12_06-14-2024
XL220n Gen10 Plus	U47	2.12_06-14-2024
XL290n Gen10 Plus	U47	2.12_06-14-2024
XL420 Gen10 Plus	U50	2.20_08-07-2024
DL20 Gen10 Plus	U60	2.10_05-16-2024
ML30 Gen10 Plus	U61	2.10_05-16-2024

HPE ProLiant Gen10 Plus v2 servers

Table 3. Supported HPE ProLiant Gen10 Plus v2 servers

HPE server	ROM family	Minimum ROM version
DL385 Gen10 Plus v2	A42	3.10_05-16-2024
DL325 Gen10 Plus v2	A43	3.10_05-16-2024
MicroServer Gen10 Plus v2	U64	2.10_05-16-2024

HPE ProLiant Gen11 servers

Table 4. Supported HPE ProLiant Gen11 servers

HPE ProLiant Gen11 servers	ROM family	Minimum ROM version
DL20 Gen11	U65	1.52_07-11-2024
ML30 Gen11	U65	1.52_07-11-2024
DL145 Gen11	A58	1.10_06-20-2024
DL325 Gen11	A56	1.66_07-11-2024
DL345 Gen11	A56	1.66_07-11-2024
DL365 Gen11	A55	1.66_07-11-2024
DL385 Gen11	A55	1.66_07-11-2024
DL320 Gen11	U63	2.30_08-09-2024
DL360 Gen11	U54	2.30_08-09-2024
DL380 Gen11	U54	2.30_08-09-2024
DL380a Gen11	U58	2.30_08-09-2024
DL560 Gen11	U59	2.30_08-09-2024
ML110 Gen11	U63	2.30_08-09-2024
ML350 Gen11	U54	2.30_08-09-2024
MicroServer Gen11	U65	1.52_07-11-2024
E930T Gen11	H11	2.30_08-09-2024

HPE Alletra servers

Table 5. Supported HPE Alletra servers

HPE Alletra	ROM family	Minimum ROM version
HPE Alletra Storage Server 4140	U57	2.30_08-09-2024
HPE Alletra Storage Server 4110	U58	2.30_08-09-2024
HPE Alletra Storage Server 4120	U58	2.30_08-09-2024

HPE Cray servers

Table 6. Supported HPE Cray servers

HPE Cray servers	ROM family	Minimum ROM version
HPE Cray XD225v	CA2K	5.27_V1.11
HPE Cray XD295v	CA2K	5.27_V1.11

Note: HPE Cray XD225v/XD295v is only certified for Windows Server 2025 with AMD EPYC 9xx5 series processors.

HPE Synergy servers

Table 7. Supported HPE Synergy servers

HPE Synergy servers	ROM family	Minimum ROM version
HPE Synergy SY480 Gen11	I45	2.32_09-09-2024
HPE Synergy SY480 Gen10	I42	3.32_08-29-2024
HPE Synergy SY660 Gen10	I43	3.32_08-29-2024
HPE Synergy SY480 Gen10 Plus	I44	2.22_09-05-2024

HPE Synergy software releases can be found here:
techhub.hpe.com/us/en/enterprise/docs/index.aspx?doc=/eginfolib/synergy/sw_release_info/index.html

For Windows Server support with HPE Synergy Servers, refer to support.hpe.com/docs/display/public/synergy-sw-release/index.html

Additional HPE servers

See Windows Server Certification and Support | Hewlett Packard Enterprise (hpe.com)

HPE Moonshot	ROM family	Minimum ROM version
HPE ProLiant m750 Server Blade	H09	3.30_05-16-2024

HPE Storage

Table 8. Supported HPE Alletra 5000, HPE Alletra 6000, and HPE Nimble Storage external arrays

Platform	Model	O/S / Firmware version
HPE Alletra 4000 series	4110, 4120, 4140	HPE-1
HPE Alletra 5000 series	5000	NimOS 5.2.x and later
HPE Alletra 6000 series	6000	NimOS 5.2.x and later
HPE Alletra 9000 series	9000	4.5.x 9.5.x
HPE Apollo 4000 series	4200 Gen10 Plus	HPE-1
HPE GreenLake for Block Storage MP/ HPE Alletra Storage MP	10000	10.2 10.3 10.3.1 10.4.x (Jun 24)
HPE MSA	Gen6 (1060/206X)	IN210 and later
HPE Nimble Storage	AF/HF/CS series including “BlueTail” Gen6	NimOS 5.2.x and later

HPE Primera	All-Flash (A630, A650 and A670), Converged/Hybrid (C630, C650, C670) "Minotaur" (660, 680)	4.5.x 9.5.x
HPE StoreEasy	N/A	No plan for initial support
HPE StoreOnce	HPE StoreOnce VSA, HPE StoreOnce Gen4 Appliances, HPE StoreOnce Gen4+ Appliances	4.1.2, 4.1.3, 4.2.1, 4.2.3, 4.3.0, 4.3.2, 4.3.4, 4.3.5, 4.3.6, 4.3.7 4.3.7, 4.3.8, 4.3.9, 5.0
HPE StoreVirtual VSA	N/A	No plan for initial support
HPE XP	HPE XP7, HPE XP8	80-06-xx-xx, 90-08-xx-xx

Configuring and validating Secured-core servers

Secured-core servers use a combination of hardware features, firmware enablement, and Windows Server OS capabilities to protect against current and future malware, and rootkit types of security exploits. In general, a Secured-core server provides:

– Comprehensive security—A suite of protection in a single enablement designed to work from **boot** to OS protection
  - Hardware root of trust using Trusted Platform Module 2.0 (TPM 2.0)
  - Firmware protection enabled by processor support for Dynamic Root of Trust of Measurement (DRTM) technology, along with DMA protection
  - Virtualization-based security (VBS) and hypervisor-based code integrity (HVCI)

– Preventative defense designed to prevent future exploits and attacks

The Secured-core server Additional Qualification (AQ) defines the additional set of requirements to support and enable the Secured-core capabilities explained previously with Windows Server 2025. Systems that meet it are listed in the Windows Server Catalog.

Configuring Secured-core

This section provides guidance for steps to configure Secured-core to a fully protected state. You may also need to install additional software from the HPE ProLiant support pack to enable the Secured-core features, such as the DRTM driver for the AMD platform. See the "Installing the Service Pack for ProLiant (SPP)" section for more information.

Note

It is advised that Secured-core be configured in the BIOS before OS installation and that Secured-core be configured (through registry keys or Windows Admin Center) before roles such as Hyper-V are added.

Configuring UEFI/BIOS settings

On the applicable servers listed previously, a Microsoft Secured-core support option is available in the BIOS to easily configure all the necessary BIOS settings, as shown in Figure 1.

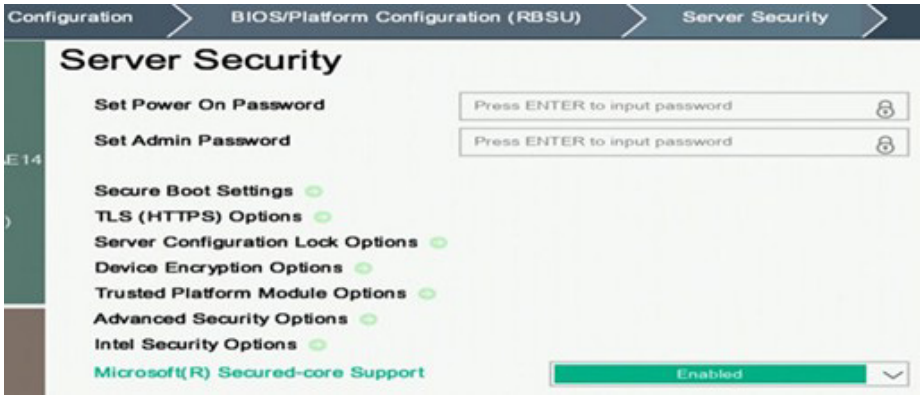

Figure 1. Secured-core configuration button in Gen10 Plus BIOS

Configuring Windows Server VBS, HVCI, and System Guard

To enable the Secured-core feature, virtualization-based security (VBS), Hypervisor Enforced Code Integrity (HVCI), and System Guard must be enabled in the OS. Choose one of the following three options for enabling these features and then proceed to confirm if all the Secured- core features are properly configured and running.

1. Registry key settings

   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

2. For Windows Admin Center (WAC), see Figure 2.

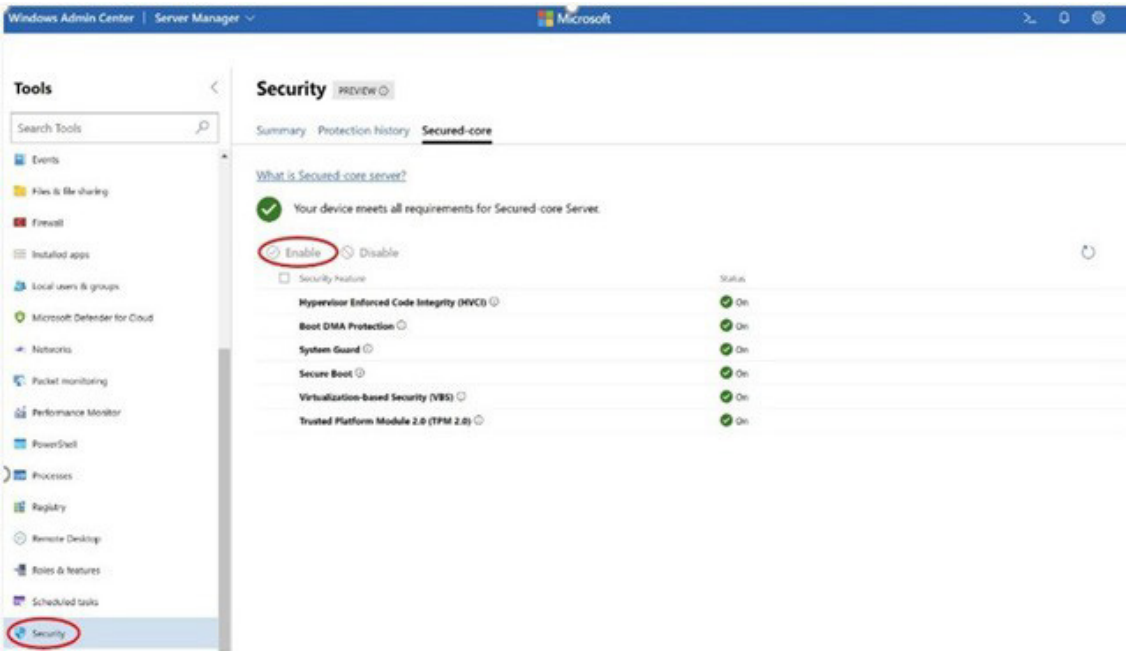

Figure 2. Secured-core configuration in Windows Admin Center (WAC)

3. Windows Security App (for Windows Server OS with Desktop Experience only), see Figures 3 and 4.

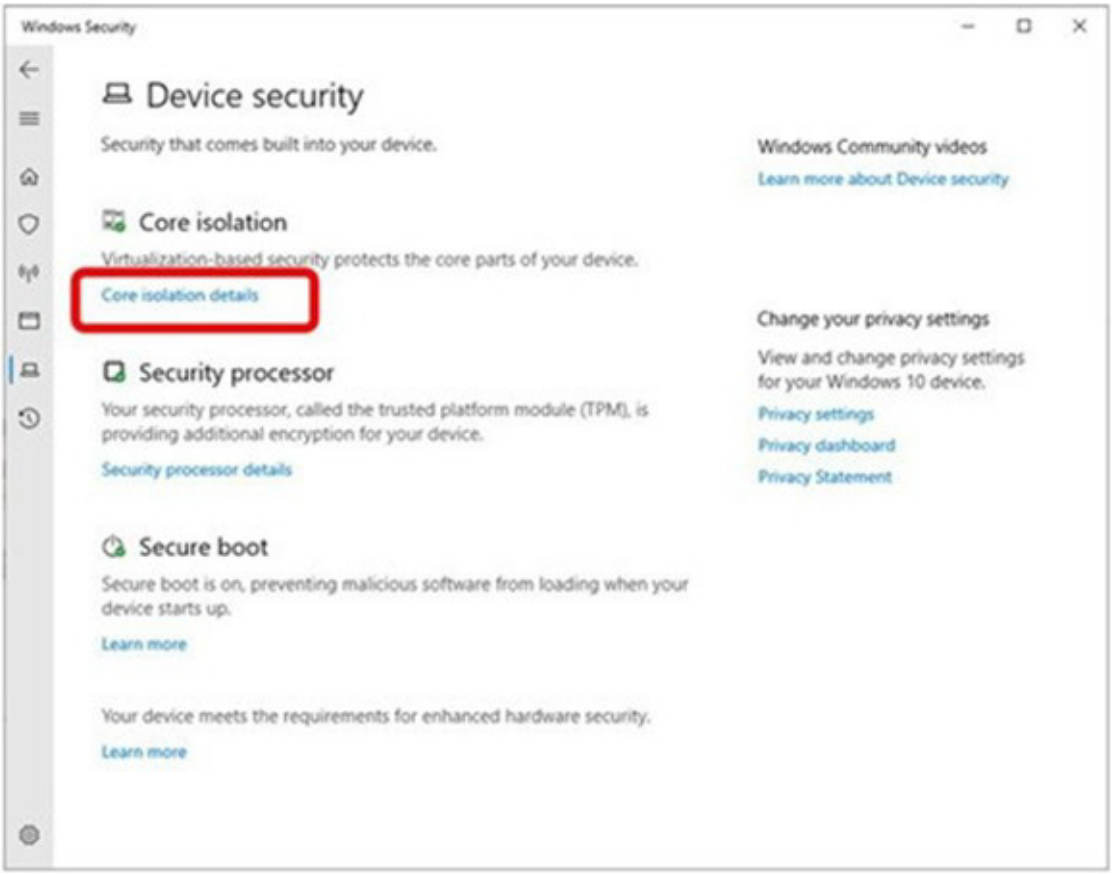

Figure 3. Secured-core configuration in Windows Security App—Device security

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.

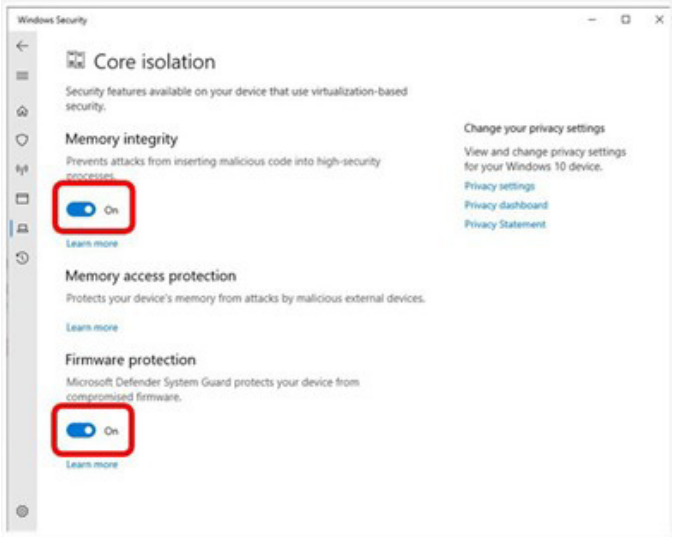

Figure 4. Secured-core configuration in Windows Security App—Core isolation

Confirm the Secured-core state

Confirm TPM 2.0

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

```
TpmPresent                : True
TpmReady                  : True
TpmEnabled                : True
TpmActivated              : True
```

Figure 5. Confirmation of TPM 2.0 readiness for Secured-core

Confirm Secure Boot, Kernel DMA Protection, VBS, HVCI, and 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, 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

Figure 6. Proper state of security for Secured-core, as shown in msinfo32

At this point, roles such as Hyper-V can be added and can be verified.

Note

If Hyper-V Virtualization Enabled in Firmware appears as **No**, then check the event log for Event ID 124.

– `Get-WinEvent -FilterHashtable @{LogName- “System”;ID=124} -MaxEvents 20`

To resolve this error, it may be necessary to clear the TPM in the BIOS. See the Configuring Trusted Platform Module options on HPE.com for more information. If BitLocker drive encryption has been enabled, it must be suspended before rebooting into BIOS and clearing the TPM.

Installing Windows Server 2025

When deploying Windows Server 2025, customers have a choice of Server Core or the full Desktop version for both Standard and Datacenter editions (another edition, Windows Server Essentials, is for small businesses and not covered here). Just as in previous versions of Windows Server, the installation can be performed from DVD media or using the HPE iLO Virtual Media. Boot controller drivers for HPE Smart Array controllers listed are provided in-box (included on the OS media .iso), and any other required drivers can be provided using HPE iLO Virtual Media during the setup procedure.

The following sections also provide information on updating drivers and software with the latest Service Pack for ProLiant.

Windows Server 2025 mitigations for Meltdown and Spectre

Windows Server 2025 includes mitigations for Meltdown and Spectre vulnerabilities. However, the patches are not enabled by default and require the following registry keys (to pass validation with the SpeculationControl Validation PowerShell Script).

```
“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management” /v FeatureSettingsOverride /t REG_DWORD /d 72 /f
```

```
“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management” /v FeatureSettingsOverrideMask /t REG_DWORD /d 3 /f
```

See the KB4072698: Windows Server and Azure Stack HCI guidance to protect against silicon-based microarchitectural and speculative execution side-channel vulnerabilities for more information.

For more information on Spectre or Meltdown mitigation, see the HPE support communication—customer bulletin

ADV180002 | Guidance to mitigate speculative execution side-channel vulnerabilities (Security Advisory)

SpeculationControl Validation PowerShell script

Note that additional vulnerabilities may be discovered, and additional guidance may need to be followed along with the previously mentioned.

Intel Virtual RAID on CPU (VROC) for HPE ProLiant Gen10 Plus and HPE ProLiant Gen11 servers

The Intel Virtual RAID on CPU (Intel VROC) family of products provides RAID solutions for both NVMe SSD and SATA devices for HPE servers. It is a software-based solution utilizing Intel CPU features to RAID or host bus adapter (HBA) direct connected drives. It supports both Intel SFF SSDs and HPE SFF SSDs and can be configured within HPE ProLiant server ROM-Based Setup Utilities (RBSU).

The product family includes the following two products:

– Intel VROC (VMD NVMe RAID) provides enterprise RAID solutions on platforms that support Intel Volume Management Device (Intel VMD) on Intel® Xeon® Scalable processors.
– Intel VROC (SATA RAID) provides enterprise RAID solution for SATA devices connected to SATA and sSATA Intel Platform Control Hub (Intel PCH) configured for RAID.

Configuring UEFI/BIOS settings for Intel VROC

RAID management through the BIOS setup environment incorporates the functionality of Intel VROC and Intel VROC Pre-Operating System (Pre-OS) management components so that RAID management and control can begin within the BIOS setup directly. This setup enables the creation of RAID volumes that you can assemble in advance for the installation of an OS.

RAID-level options available with Intel VROC are RAID 0 (stripe), RAID 1 (mirror), RAID 5 (parity), and RAID 10 (RAID 1+0 striped mirror).

Enabling Intel VROC (SATA RAID) for SATA or sSATA on BIOS/Platform Configuration (RBSU)

Procedure

1. During POST, press the F9 option that allows you to access the BIOS setup menu.
2. Select the menu option System Configuration.
3. In the System Configuration menu, click the menu option BIOS/Platform Configuration (RBSU).
4. In the BIOS/Platform Configuration (RBSU) menu, click the menu option Storage Options.
5. In the Storage Options menu, click the menu option SATA Controller Options.
6. In the SATA Controller Options menu, click the menu option Embedded SATA Configuration.
7. From the drop-down list, select Intel VROC SATA Support as shown in Figure 7.
8. Press F12 to save changes and reboot the system.

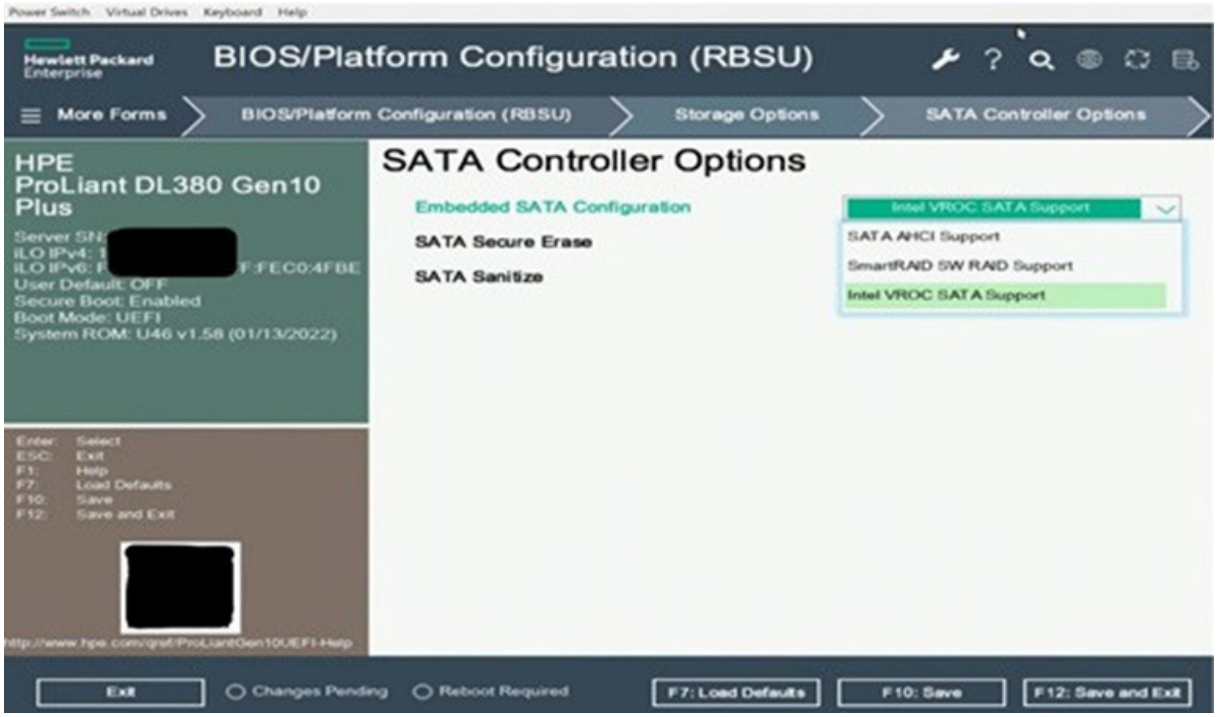

Figure 7. Intel VROC SATA support option in BIOS

Enabling Intel VMD and Intel VROC NVMe on BIOS/Platform Configuration (RBSU)
Procedure

1. During POST, press the F9 option that allows you to access the BIOS setup menu.
2. Click the menu option System Configuration.
3. In the System Configuration menu, click the menu option BIOS/Platform Configuration (RBSU).
4. In the BIOS/Platform Configuration (RBSU) menu, click the menu option Storage Options.
5. In the Storage Options menu, click the menu option NVM Express Options.
6. In the NVM Express Options menu, click the menu option Intel(R) NVMe.
7. In the Intel(R) NVMe Options menu, click the menu option Intel(R) CPU VMD Support. From the drop-down list, select Enabled All CPU NVMe Root Ports.
8. Click the menu option Intel(R) VROC Support. From the drop-down list, select Intel VROC for HPE NVMe as shown in Figure 8.
9. Press F12 to save changes and reboot the system.

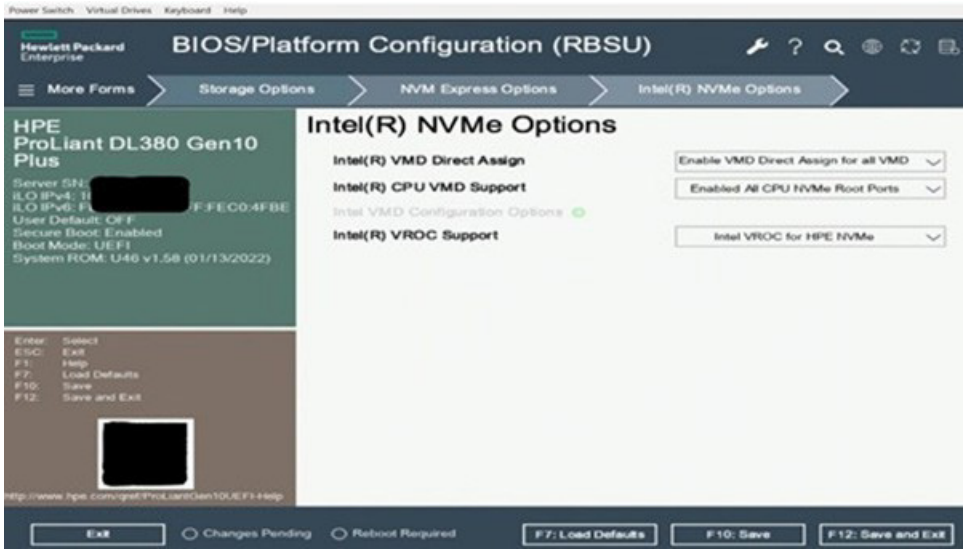

Figure 8. Intel VROC NVMe support option in BIOS

Drivers for Intel VROC

Intel VROC is integrated within the HPE BIOS. The Intel VROC solution has two driver components: the pre-boot or UEFI driver, and the OS driver. The UEFI driver is embedded in the system BIOS and is referred to as the RSTe NVMe UEFI driver while the OS driver must be loaded at the OS installation time; both contain version numbers. HPE provides three different drivers and a CLI tool for the Windows OS: one driver package each for Intel VROC NVMe, VROC SATA, and VROC sSATA controllers.

VROC 9.0 is the official version supported for Windows Server 2025.

Download links for Intel Virtual RAID on CPU driver Microsoft Windows Server 2019/2022 and Microsoft Windows Server 2025:

Intel Virtual RAID on CPU package VROC CLI for Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022 and Microsoft Windows Server 2025 | HPE Support

Intel Virtual RAID on CPU With VMD Technology Driver for Microsoft Windows Server 2019 and Microsoft Windows Server 2022

Intel Virtual RAID on CPU Software for SATA SSDs for Windows Server 2019 and Windows Server 2022

Intel Virtual RAID on CPU Software for sSATA SSDs for Windows Server 2019 and Windows Server 2022

Gen11 Intel Virtual RAID on CPU Software for tSATA SSDs for Microsoft Windows Server 2019 and Microsoft Windows Server 2022

Intel Virtual RAID on CPU package VROC GUI for Windows Server 2019 and Microsoft Windows Server 2022

Intel VROC User Guide

Installing Windows Server 2019, or Windows Server 2025 on an Intel VROC RAID volume

Prerequisites

– You have enabled Intel VMD and created a volume using Intel VROC (with RAID protection strongly advised).

– You have a Windows OS image mounted and are prepared to supply the Intel VROC driver to detect the RAID volume. (HPE NVMe driver and Intel VROC NVMe driver provided by HPE are used as examples).

Procedure

– Download the driver for Windows for your Intel VROC RAID controller and extract the smart component to an empty folder on C: drive.

– Click "Virtual Drives" to mount the folder through HPE iLO.

– Click "Browse" and navigate to where you have the driver saved, and then click "Ok".

– Highlight the selected driver and click Next to install as shown in Figure 9. It may take several minutes to complete the installation of the selected driver.

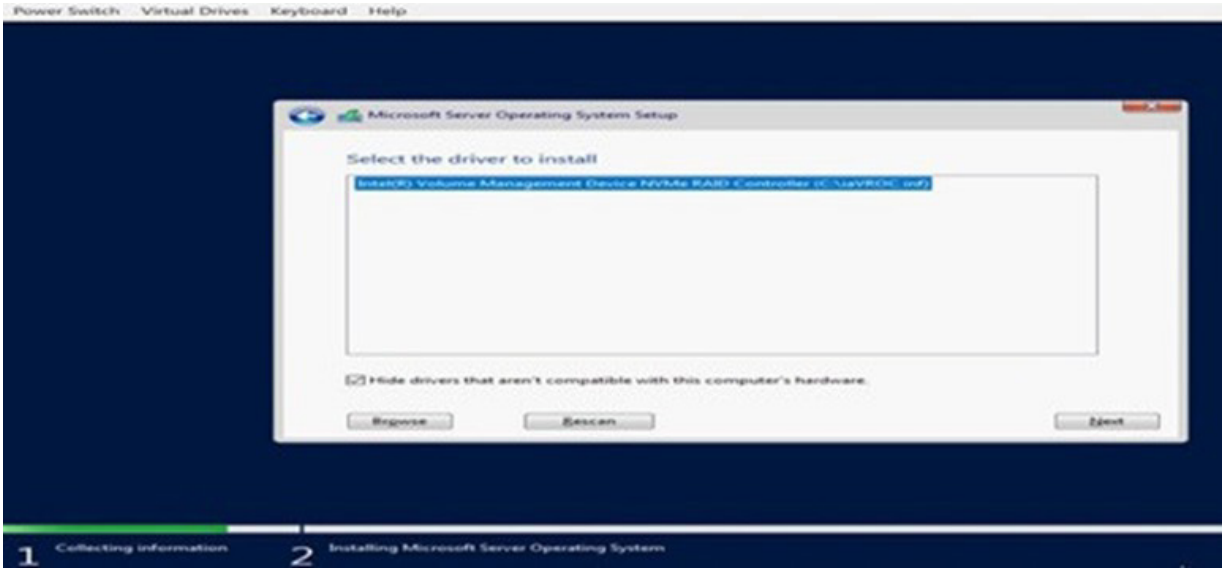

Figure 9. Selecting Intel VROC NVMe driver during OS installation

– After installing the appropriate driver, the RAID volume appears, as shown in Figure 10. If the drive does not immediately appear, use the Refresh tool to rescan the system for the RAID volume.

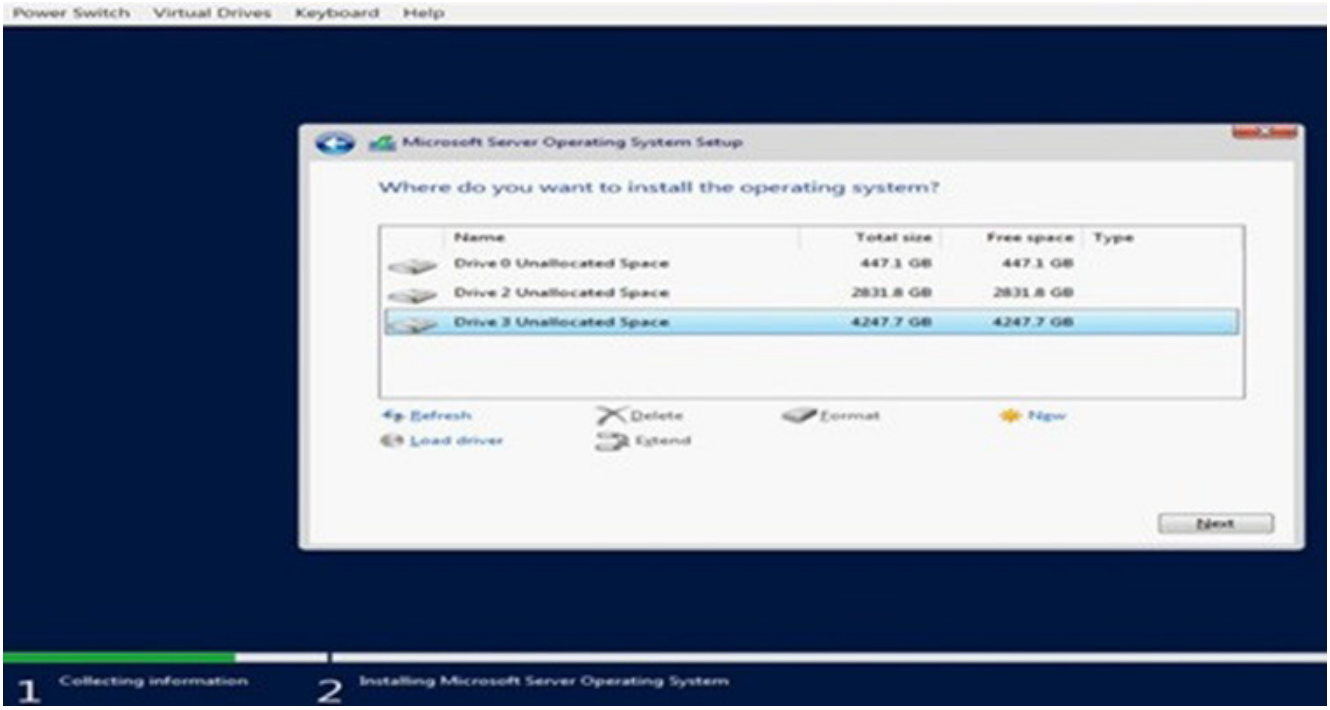

Figure 10. Selecting volume for OS installation

– Select the volume and click Next to proceed with the installation of your Windows OS.

Installing the Service Pack for ProLiant (SPP)

This section describes the installation of the HPE Service Pack for ProLiant 2024.09.00 or newer on both Server Core and Desktop Experience versions. The HPE Service Pack for ProLiant is available by entitlement, which means that an active warranty or HPE Support agreement is required. The HPE Service Pack for ProLiant provides the necessary drivers and firmware for Windows Server 2025 versions on supported HPE servers and is available at: spp.hpe.com.

The HPE Service Pack for ProLiant can be deployed using Smart Update Manager (SUM) version 10.7.0. SUM has a browser-based GUI, as well as scriptable, interactive command line, and file-driven interfaces. For more information on SUM, see hpe.com/us/en/productcatalog/detail/pip.5182020.html.

The HPE Service Pack for ProLiant can be deployed via the following scenarios:

– Local deployment
– Remote deployment

Caution
When a TPM is installed and enabled on the server, data access is locked if the user fails to follow the proper procedure for updating the system or option firmware. Microsoft recommends temporarily disabling Windows BitLocker prior to updating any system firmware. After the firmware flash is complete, the server should be rebooted, and BitLocker can be re-enabled.

Depending on your environment, it may be necessary to perform the following optional configuration tasks: disable the firewall (temporarily), enable Remote Management, and add the SNMP service and WMI SNMP Provider Windows features. The following PowerShell commands perform these configuration tasks:

- `netsh advfirewall set currentprofile state off`
- `netsh advfirewall set allprofiles settings remotemanagement enable`
- `Add-WindowsFeature SNMP-Service`
- `Add-WindowsFeature SNMP-WMI-Provider`

Installing the Service Pack for ProLiant on Windows Server Core

Since Windows Server Core does not contain a full UI and a browser, it is necessary to update HPE drivers and software using SUM from the command line. Windows Server Core provides only a command prompt for the user logged in. The Smart Update Manager (SUM) can be run from this command prompt using the smartupdate.bat file located in the PACKAGES folder.

To apply smart updates to Server Core (without UI interaction) using CMD or Windows PowerShell:

1. Download and mount the Service Pack for ProLiant, ISO on the local system
2. Run smartupdate.bat from the PACKAGES folder of the mounted SPP .ISO, for example,

   ```
   E:\PACKAGES\smartupdate /s /tpmbypass /romonly
   ```

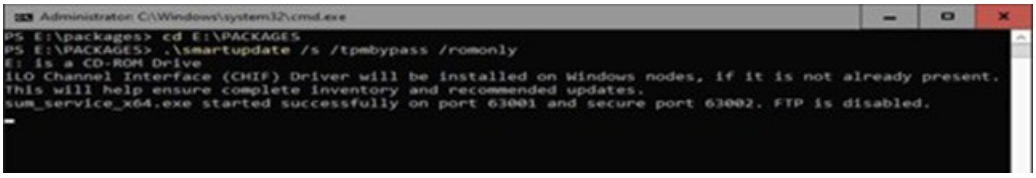

Figure 11. Running ".\smartupdate /s /tpmbypass /romonly" from the E:\PACKAGES folder to install the Service Pack for ProLiant through PowerShell command line

Note

This process may take up to 30 minutes to complete.

A common error message is a **failed dependency**, which can be due to the presence of a TPM module in the server. If this is the case, it is necessary to run the Smart Update in two commands:

- \smartupdate /s /tpmbypass /romonly
- \smartupdate /s /tpmbypass /softwareonly

For detailed instructions on using this command-line option, SUM 12.2.0 CLI guide.

Installing the Service Pack for ProLiant (SPP) on Windows Server 2025 with Desktop (UI)
Either the command-line deployment explained previously or the following Smart Update process using a browser may be used.

1. Step 1: Download and mount the Service Pack for ProLiant .ISO on the local system
2. Step 2: Install the certificate as follows:
   a. Navigate to E:\packages\assets\certificates and select the CA security certificate
   b. Right-click and select Open. Click Open again on the Open File—Security Warning
   c. Click Install Certificate
   d. Select Local Machine under Store Location and click Next
   e. Select "Place all certificates in the following store" and click Browse
   f. Select Trusted Root Certification Authorities and click OK
   g. Click Next and then click Finish
   h. Click OK twice to exit the Certificate Import Wizard
3. Navigate to E:\PACKAGES\ and double-click on the smartupdate.bat file to launch smartupdate
4. Click Localhost Guided Update
5. On the Localhost Guided Update screen, click OK
6. Once the inventory has been completed, click Next
7. On the Deployment summary screen, click Deploy
8. Once deployment has completed, click Reboot if required

Remote deployment
The procedures for remote deployment are the same for both Windows Server Core and Windows Server with Desktop (UI) since it is performed remotely.

1. Download and mount the Service Pack for ProLiant .ISO file on the local system. Navigate to the PACKAGES folder of the mounted SPP and run smartupdate.bat
2. You may need to add a security certificate exception or bypass the browser warning that the self-signed certificate does not validate security

Procedure to add Baseline
1. On the SUM home screen, click **Baseline Library**
2. On the Baseline Library screen, click **Add Baseline**

Note
If you want to clear the **Add Baseline** screen, click **Start Over**.

---

1. SUM opens the **Add Baseline** screen
2. Select **Browse** and navigate to the mounted SPP
3. Click **Add**. SUM should return to Baseline successfully added message
4. Under the Smart Update Manager drop-down menu, click **Nodes** (under Options)

Add servers as remote nodes and install the SPP:

1. From the **Nodes** screen, click **Add Node**
2. Select **Add a single node** or **known range of nodes**
3. Enter the IP address or range
4. Enter a description for the node
5. In the **Type of node to add** field, select the node type, which should be Windows

Note
Selecting the correct node type often helps SUM complete adding the node faster.

6. Select the Service Pack for ProLiant 2024.09.0 (or newer) bundle as a baseline here. If the SPP has not been added, select **+Add Baseline** and browse to the location where you mounted the SPP.
7. Select a **group** from the list (optional).
8. Select one of the following:
   a. Use current credentials (requires existing trust relationship with the node). This option is for Windows nodes only.
   b. Enter administrator credentials: Enter the user name and password for a user with administrator privileges on the node. Windows users can use domain / user name if the user has administrator permission.
9. Click **Add**. In the **Added Nodes** section, SUM displays the nodes you selected.

Performing node inventory

1. From the Nodes screen, highlight the node and then select **Actions -> Inventory**
2. SUM displays the baseline associated with the node. If you want to reassign the baseline that SUM will use for inventory, select a baseline, additional package, or both
3. Click **Inventory**. SUM displays errors to resolve before you can deploy updates

Deploying a node procedure

1. From the Nodes screen, select a node to update, and then select **Actions -> Review/Deploy**
2. Select the **Installation Options** tab to change options if necessary. You may need to select the **Ignore Warnings** checkbox if a TPM is detected. Be sure to follow the instructions provided if it says to suspend BitLocker before performing firmware updates
3. Select the **Reboot Options** tab to set options if desired
4. Select the HPE iLO **Repository Options** tab to manage the HPE iLO Repository if desired
5. Select the components from the **Baseline** and **Associated Packages** tabs where you want to change any deployment selections (2024.09.0 SPP [or newer] bundle should be ready to deploy)
6. Click **Deploy**. SUM verifies any changes that you made are valid and then begins deploying components
7. In the General section of the Node screen, click **View log** for the node, and then click **View log** for the component you installed to view the details of the installation

Known issues

Issue: Fails to install Linux® OS on Virtual Machine under Hyper-V on Windows Server 2025

Description: After installing Hyper-V and installing all the prerequisites required to install after creating the VM, the VM failed to install OS, it shows the Bootable image is not mounted even when it is mounted

Resolution: See KB article with workaround "For hosts with more than 64 logical processors, specify the number of **virtual processors** at VM creation using Windows Admin Center, PowerShell, or another tool."

learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/plan/should-i-create-a-generation-1-or-2-virtual-machine-in-hyper-v

Issue: Black screen issue when installing Matrox graphic driver

Description: When installing Matrox graphic driver (the display driver for HPE iLO remote console) in previous versions of SPP, the system is still alive but user will lose display on HPE iLO remote console.

Resolution: Matrox has added the fix into Windows Server 2025 driver 4.6.0.x version. For customers with the black screen, we suggest to connect a local monitor or use remote desktop connection or use HPE iLO power button to reboot the system. The display of HPE iLO remote console will be back after the reboot.

Issue: Windows Server 2025 OS installation on a diskless system using iSCSI boot through BIOS iBFT is not able to complete.

Description: Bugcheck Inaccessible_Boot_Device or DRIVER_IRQL_NOT_LESS_OR_EQUAL or infinite boot cycle happening at first reboot

Resolution: Update to 11B OS hotfix to the WS2025 installation media and apply NIC vendor driver in WinPE setup stage to start OS installation. See improvements section of KB5046617 published November 12, 2024—KB5046617 (OS Build 26100.2314)—Microsoft Support.

Issue: GPU-P live migration feature on Windows Server 2025

Description: Drivers for supporting the Windows Server 2025 GPU-P live migration feature may not available until later.

Resolution: Reference: KB article to get the detailed introduction on GPU-P requirements.
learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/gpu-partitioning?pivots=windows-server

Issue: Microsoft-Windows-Kernel-Boot Event ID 124 Logged

Description: On an HPE ProLiant Gen10 Plus series server, users might observe the following event error message with Event ID 124 under Windows system event log after installing Windows Server OS or while installing a hypervisor on HPE ProLiant Gen10 Plus servers using HPE DVD media or HPE pre-install image system event log error message:

"The Virtualization Based Security Enablement Policy Check at Phase 7 Failed with Status: unknown NTSTATUS Error Code 0xc028014b"

Resolution: To address the issue, clear the Trusted Module Platform (TPM) as follows:

1. From the Start Menu, click Start, type PowerShell, and then click Windows PowerShell run as administrator or right-click the Start button and select Windows PowerShell (Admin).
2. At the command prompt, type Clear-TPM and hit Enter.
3. Restart the system for the change to take effect.

Issue: Enabling firmware protection (Intel TXT) without Secured-core support may cause Hyper-V role installation failure or block Hyper-V startup if already installed.

Description: The new Secured-core BIOS feature is only available when the platform detects a supported processor. If the user chooses to enable an individual component such as Intel TXT, then Hyper-V may be blocked. The system may log Event ID 124, Kernel-Boot, stating, "The virtualization-based security enablement policy check at phase 0 failed with status: Virtual Secure Mode (VSM) is not initialized. The hypervisor or VSM may not be present or enabled."

Workaround: Do not enable firmware protection (Intel TXT) instead of Secured-core. Do not attempt to use either for Windows Server 2019 or earlier versions, especially if Hyper-V is desired.

See the Startup failure when Firmware protection is turned on—Windows Server Microsoft documentation

Issue: Protection for Secure Boot BlackLotus UEFI bootkit (CVE-2023-24932) is not enabled by default.

Description: Secure Boot is recommended by Microsoft to make a safe and trusted path from the Unified Extensible Firmware Interface (UEFI) through the Windows Trusted Boot sequence. Secure boot helps prevent bootkit malware in the boot sequence. Disabling Secure Boot puts a device at risk of being infected by bootkit malware. Fixing the Secure Boot bypass described in CVE-2023-24932 requires revoking boot managers. This could cause issues for some device's boot configurations. Microsoft has introduced KB5025885 for users review and to determine whether you need to enable the protections now or wait for a future update from Microsoft.

Resolution: HPE WS2025 minimum BIOS version include the new "Windows UEFI CA 2023" in default Secure Boot DB, and it's highly recommended to follow the Mitigation Deployment Guidelines in KB5025885 to enable the protections manually.

Issue: Enabling Intel Trust Domain Extensions (TDX) in BIOS may cause problems with Windows Server boot or stability.

Description: Intel Trust Domain Extensions (TDX) is available in BIOS for future support and confidential computing, but should not be used for Windows Server at this time.

Workaround: Do not enable Intel Trust Domain Extensions (TDX) in BIOS when using Windows Server 2025.

Issue: Support for SR100i and S100i software RAID has not been provided for Windows Server 2025.

Description: SR100i and S100i software RAID are available on Windows Server 2019 and 2022.

Workaround: Replace the software RAID with hardware RAID or remain on Windows Server 2019 or 2022.

Issue: HPE ProLiant m750 Server Blade may display "yellow bangs" (warnings) in Device Manager for Windows Server 2025.

Description: The HPE ProLiant m750 Server Blade RBSU has two display options. Both default settings are enabled.

Workaround: Uninstall one of the "Microsoft Basic Display Adapters" or it is safe to ignore the warning.

Issue: The kernel debug drivers for NIC on current shipping Windows Server OS does not support PCI multi segment.

Description: While setting live kernel debugging on a system, the connection cannot be established successfully. PCI multi segment is enabled by default on G11/G12 server with multi-processors.

Workaround: There are 2 work arounds to get kernel debug connection: Option1, go to RBSU advanced menu (press "Ctrl+A" in RBSU home page) and disable the PCI multi segment. Option2, swap the NIC card to PCI segment 0 slots.

Issue: For some hardware configurations, setup might stop responding on the first screen of the installation. This lack of response might last for up to 40 minutes.

Description: While using old Windows Server 2025 media for installation, there are long hangs/delays in Windows setup before you can proceed to select the next menu.

Resolution: This is Microsoft known issue which has been fixed in 11B,2024 patch, please use the latest Microsoft Windows Server 2025 media (the OS build version after 26100.2314) for installation. HPE offers replacement media for customers who purchase Windows Server license from HPE or an HPE authorized reseller; proof of purchase is required. The request can be logged via our media replacement site and include the information that the ISO file is requested. ebiz3.mentormediacorp.com/HPEDGRCR/.

Issue: DL525 Gen13 servers may fail to boot to Windows Server 2025 after Secured-core is enabled.

Description: On HPE ProLiant DL525 Gen13 servers running Service pack for HPE ProLiant Gen13 Version 2026.09.00.00, enabling Secured-core by following the procedure described in Configuring Secured-core may prevent the system from booting into Windows Server 2025. After the Secured-core configuration is completed, the server may stop responding at the HPE logo screen during the boot process.

Resolution: This issue is caused by an AMD Dynamic Root of Trust for Measurement (DRTM) driver defect. The required AMD chipset driver that resolves the issue is included in HPE ProLiant Gen13 SPP Version 2026.11.00.00 and later releases. HPE recommends upgrading to SPP Version 2026.11.00.00 or a newer release before enabling Secured-core on DL525 Gen13 servers.

Issue: Windows Server 2025 installation media released before January 2027 may fail to boot on HPE ProLiant Gen13 servers with Secure Boot enabled.

Description: On HPE ProLiant Gen13 servers, Secure Boot is enabled by default. These platforms require boot components signed by the Windows UEFI CA 2023 certificate. Older Windows Server 2025 installation media may contain boot components signed by Microsoft Windows Production PCA 2011, which are not included in the default Secure Boot database on Gen13 servers. As a result, the installation media might fail to boot when Secure Boot is enabled.

Resolution: HPE recommends using the latest Windows Server 2025 installation media obtained through your authorized Microsoft distribution channel. Windows Server 2025 installation media released in 2027 or later uses Windows UEFI CA 2023-signed boot components by default and can boot HPE ProLiant Gen13 servers with Secure Boot enabled. Installation media released before 2027 uses boot components signed by Microsoft Windows Production PCA 2011 and must be updated to use Windows UEFI CA 2023-signed boot components before it can boot HPE ProLiant Gen13 servers with Secure Boot enabled. If you must continue using older Windows Server 2025 installation media, Microsoft provides a PowerShell-based process to update the media with Windows UEFI CA 2023-signed boot components. For detailed instructions, see the Microsoft article: Updating Windows bootable media to use the PCA2023 signed boot manager.

Resources

What's new in Windows Server 2025

Microsoft Windows Server home page

Comparison of Standard, Datacenter, and Datacenter: Azure Edition editions of Windows Server 2025

Intelligent Provisioning User Guide for HPE ProLiant Gen10, HPE ProLiant Gen10 Plus Servers, and Synergy

Installing and running Microsoft Windows Server on HPE Superdome Flex techinical white paper

Installing Microsoft Windows Server operating system | Installing Operating Systems on HPE Superdome Flex 280 Server

HPE Storage - SPOCK

Learn more at

HPE.com/servers

Visit HPE.com

Chat now

© Copyright 2026 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

AMD is a trademark of Advanced Micro Devices, Inc. Intel and Intel Xeon are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Azure, BitLocker, Hyper-V, Microsoft, PowerShell, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All third-party marks are property of their respective owners.

a50003760ENW, Rev. 11

HEWLETT PACKARD ENTERPRISE

hpe.com