Hewlett Packard Enterprise

Technical white paper

Check if the document is available in the language of your choice.

IMPLEMENTING MICROSOFT WINDOWS SERVER 2022 USING HPE PROLIANT SERVERS, STORAGE, AND NETWORKING OPTIONS

CONTENTS

WINDOWS SERVER 2022 EDITIONS

Windows Server 2022 is available in both Datacenter and Standard editions. The default installation is Server Core, but a full desktop experience can be optionally installed and user guidance is provided in this document for both.

NOTE
You cannot convert between Windows Server 2022 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.

OVERVIEW

Windows Server 2022 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 2022 on HPE servers.

HPE Service Pack for ProLiant (SPP) information

The HPE Service Pack for ProLiant 2021.10.0 or newer provides firmware, drivers, and tools for supported HPE ProLiant servers and has been tested with the general availability build of Windows Server 2022.

It can be found on the here: spp.hpe.com.

Supported HPE servers

NOTE
HPE Gen9 and older servers are not supported.

HPE Gen10 servers

TABLE 1. Supported HPE Gen10 servers

HPE server	ROM family	Minimum ROM version
HPE Apollo 4200 XL420	U39	2.52_07-08-2021
HPE Apollo 4510 XL450	U40	2.52_07-08-2021
HPE Synergy SY660	I43	2.54_09-03-2021
HPE Synergy SY480	I42	2.54_09-03-2021
HPE ProLiant DL160	U31	2.52_07-08-2021
HPE ProLiant DL560	U34	2.52_07-08-2021
HPE ProLiant DL580	U34	2.52_07-08-2021
HPE ProLiant ML110	U33	2.52_07-08-2021
HPE ProLiant ML350	U41	2.52_07-08-2021
HPE ProLiant DL385	A40	2.50_07-08-2021
HPE ProLiant DL180	U31	2.52_07-08-2021
HPE ProLiant DL325	A41	2.50_07-08-2021
HPE ProLiant DL360	U32	2.52_07-08-2021
HPE ProLiant DL380	U30	2.52_07-08-2021
HPE Superdome Flex	N/A	3.40.80
HPE ProLiant ML30	U44	2.50_07-08-2021

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"

HPE Gen10 Plus servers

TABLE 2. Supported HPE Gen10 Plus servers

HPE server	ROM family	Minimum ROM version
HPE Apollo XL220n	U47	1.50_08-27-2021
HPE Apollo XL225n	A46	2.50_07-29-2021
HPE Apollo XL290n	U47	1.50_08-27-2021
HPE Apollo 4200 XL420	U50	1.50_08-27-2021
HPE Apollo XL645d	A48	2.50_07-29-2021
HPE Apollo XL675d	A47	2.50_07-29-2021
HPE ProLiant DL325	A43	2.50_08-09-2021
HPE ProLiant DL345	A43	2.50_08-09-2021
HPE ProLiant DL365	A42	2.50_08-09-2021
HPE ProLiant DL360	U46	1.50_08-27-2021
HPE ProLiant DL380	U46	1.50_08-27-2021
HPE ProLiant DL385	A42	2.50_08-09-2021
HPE MicroServer	U48	2.50_07-08-2021
HPE Superdome Flex 280	N/A	3.40.80
HPE Synergy SY480	I44	1.52_09-22-2021

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"

HPE Gen10 Plus v2 servers

TABLE 3. Supported HPE Gen10 Plus v2 servers

HPE server	ROM family	Minimum ROM version
HPE ProLiant DL325	A43	2.50_08-09-2021
HPE ProLiant DL385	A42	2.50_08-09-2021

TABLE 4. Supported HPE Embedded RAID Controllers

Controller	Driver name	Version
S100i	Smartdq.sys	1010.14.0.0
SR100i	Smartdq2.sys	1010.124.60.1188

Supported options

TABLE 5. Supported HPE Smart Array Controllers

Controller	Driver name	Version
P408i-p SR	Smartpqi.sys	1010.6.0.1025
P408e-p SR	Smartpqi.sys	1010.6.0.1025
E208i-p SR	Smartpqi.sys	1010.6.0.1025
E208i-a SR	Smartpqi.sys	1010.6.0.1025
E208e-p	Smartpqi.sys	1010.6.0.1025
P408i-a SR	Smartpqi.sys	1010.6.0.1025
P816-a SR	Smartpqi.sys	1010.6.0.1025
SR932i-p	Smartpqi.sys	1010.6.0.1025
SR416i-a	Smartpqi.sys	1010.6.0.1025
E208i-c	Smartpqi.sys	1010.6.0.1025
P408i-c	Smartpqi.sys	1010.6.0.1025
P408i-p	Smartpqi.sys	1010.6.0.1025
P408i-sb	Smartpqi.sys	1010.6.0.1025
P408e-m	Smartpqi.sys	1010.6.0.1025
P416ie-m SR	Smartpqi.sys	1010.6.0.1025
P204i-b	Smartpqi.sys	1010.6.0.1025
P204i-c	Smartpqi.sys	1010.6.0.1025
NS204i-p	Inbox	N/A
NS204i-d	Inbox	N/A

TABLE 6. HPE MegaRAID Controllers

Controller	Driver name	Version
MR216i-p	Inbox	7.716.2.0
MR216i-a	Inbox	7.716.2.0
MR416i-p	Inbox	7.716.2.0
MR416i-a	Inbox	7.716.20

TABLE 7. Supported HPE Networking Adapters

Controller	Driver name	Version
HPE Ethernet 1Gb 4-port BaseT I350-T4 Adapter	Inbox driver	Inbox driver
HPE Ethernet 1Gb 4-port BaseT I350-T4 OCP3 Adapter	Inbox driver	Inbox driver
HPE Ethernet 10Gb 2-port SFP+ X710-DA2 Adapter	Inbox driver	Inbox driver
HPE Ethernet 10Gb 2-port SFP+ OCP3 X710-DA2 Adapter	Inbox driver	Inbox driver
HPE Ethernet 1 Gb 2-port 363i Adapter	Inbox driver	Inbox driver
HPE Ethernet 10Gb 2-port FLR-SFP+ X710-DA2 Adapter	Inbox driver	Inbox driver
HPE Ethernet 10Gb 2-port SFP+ X710-DA2 Adapter	Inbox driver	Inbox driver
HPE Ethernet 10Gb 2-port SFP+ X520-DA2 Adapter	Inbox driver	Inbox driver
HPE Ethernet 10Gb 2-port FLR-SFP+ X520-DA2 Adapter	Inbox driver	Inbox driver
HPE Ethernet 10Gb 2-port FLR-T X550-AT2 Adapter	Inbox driver	Inbox driver
HPE Ethernet 10Gb 2-port FLR-SFP+ X710-DA2 Adapter	Inbox driver	Inbox driver
HPE Ethernet 1Gb 4-port FLR-T I350-T4V2 Adapter	Inbox driver	Inbox driver
HPE Ethernet 1Gb 4-port BASE-T I350-T4V2 Adapter	Inbox driver	Inbox driver
HPE Ethernet 1Gb 2-port BASE-T I350-T2V2 Adapter	Inbox driver	Inbox driver
HPE Ethernet 1 Gb 4-port 366i Adapter	Inbox driver	Inbox driver
HPE Ethernet 10Gb 4-port SFP+ X710-DA4 Adapter	Inbox driver	Inbox driver
HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter	Inbox driver	Inbox driver
HPE Ethernet 1Gb 2-port 368i Adapter	Inbox driver	Inbox driver
HPE Ethernet 1Gb 4-port 369i Adapter	Inbox driver	Inbox driver
HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter	Inbox driver	Inbox driver
HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter	Inbox driver	Inbox driver
HPE Ethernet 10Gb 2-port 568i Adapter	Inbox driver	Inbox driver
HPE Ethernet 1Gb 2-port 361i Adapter	Inbox driver	Inbox driver
HPE Ethernet 1Gb 2-port BASE-T BCM5720 Adapter	Inbox driver	Inbox driver
HPE Ethernet 1 Gb 2-port 330i Adapter	Inbox driver	Inbox driver
HPE Ethernet 1Gb 4-port BASE-T BCM5719 Adapter	Inbox driver	Inbox driver
HPE Ethernet 1Gb 4-port FLR-T BCM5719 Adapter	Inbox driver	Inbox driver
HPE Ethernet 1 Gb 4-port 331i Adapter	Inbox driver	Inbox driver
HPE Ethernet 1 Gb 2-port 332i Adapter	Inbox driver	Inbox driver
Broadcom BCM57416 Ethernet 10Gb 2-port BASE-T Adapter for HPE	Inbox driver	Inbox driver
Broadcom BCM57416 Ethernet 10Gb 2-port BASE-T OCP3 Adapter for HPE	Inbox driver	Inbox driver
Broadcom BCM57412 Ethernet 10Gb 2-port SFP+ Adapter for HPE	Inbox driver	Inbox driver
Broadcom BCM57412 Ethernet 10Gb 2-port SFP+ OCP3 Adapter for HPE	Inbox driver	Inbox driver
HPE Ethernet 10/25Gb 2-port SFP28 BCM57414 Adapter	Inbox driver	Inbox driver
Broadcom BCM57414 Ethernet 10/25Gb 2-port SFP28 OCP3 Adapter for HPE	Inbox driver	Inbox driver
HPE Ethernet 10/25Gb 2-port FLR-SFP28 BCM57414 Adapter	Inbox driver	Inbox driver
HPE Ethernet 10Gb 2-port FLR-T BCM57416 Adapter	Inbox driver	Inbox driver
Broadcom BCM57414 Ethernet 10/25Gb 2-port SFP28 Adapter for HPE	Inbox driver	Inbox driver
HPE Ethernet 10Gb 2-port BASE-T BCM57416 Adapter	Inbox driver	Inbox driver
HPE Ethernet 10Gb 2-port SFP+ BCM57414 Adapter	Inbox driver	Inbox driver
HPE Mellanox Cx6-DX- SU Gen4 X 16	Mlx5.sys	2.70.24708.0
HPE Ethernet 10Gb 2-port SFP+ MCX4621A-ACAB OCP3 Adapter	Mlx5.sys	2.70.24728.0
HPE Ethernet 10/25Gb 2-port SFP28 MCX512F-ACAT Adapter	Mlx5.sys	2.70.24728.0
Mellanox MCX562A-ACAI Ethernet 10/25Gb 2-port SFP28 OCP3 Adapter for HPE	Mlx5.sys	2.70.24728.0
HPE Ethernet 10Gb 2-port SFP+ MCX4121A-XCAT Adapter	Mlx5.sys	2.70.24728.0
HPE Ethernet 100Gb 2-Port QSFP28 MCX516A-CCAT Adapter	Mlx5.sys	2.70.24728.0
HPE Ethernet 100Gb 2-Port QSFP56 MCX623436AS-CDAT Adapter	Mlx5.sys	2.70.24728.0
HPE Ethernet 100Gb 2-Port QSFP56 MCX623106AS-CDAT Adapter	Mlx5.sys	2.70.24728.0
Mellanox MCX631102AS-ADAT Ethernet 10/25Gb 2-port SFP28 Adapter for HPE	Mlx5.sys	2.70.24728.0
Mellanox MCX631432AS-ADAI Ethernet 10/25Gb 2-port SFP28 OCP3 Adapter for HPE	Mlx5.sys	2.70.24728.0

TABLE 7. Supported HPE Networking Adapters (continued)

Controller	Driver name	Version
HPE Ethernet 10Gb 2-port SFP+ MCX4621A-ACAB OCP3 Adapter	Mlx5.sys	2.70.24728.0
Mellanox MCX512F-ACHT Ethernet 10/25Gb 2-port SFP28 Adapter for HPE	Mlx5.sys	2.70.24728.0
HPE Ethernet 10/25Gb 2-port SFP28 MCX562A-ACAI OCP3 Adapter	Mlx5.sys	2.70.24728.0
HPE Ethernet 10/25Gb 2-port SFP28 MCX4121A-ACUT Adapter	Mlx5.sys	2.70.24728.0
HPE Ethernet 10Gb 2-port 548SFP+ Adapter	Mlx5.sys	2.70.24728.0
HPE Ethernet 10/25Gb 2-port FLR-SFP28 MCX4121A-ACFT Adapter	Mlx5.sys	2.70.24728.0
HPE Ethernet 100Gb 1-port QSFP28 MCX515A-CCAT Adapter	Mlx5.sys	2.70.24728.0
HPE Ethernet 10/25Gb 2-port FLR-SFP28 QL41401-A2G Converged Network Adapter	qevbda.sys qenda.sys	8.58.16,0 8.58.12.0
HPE Ethernet 10Gb 2-port BASE-T QL41401-A2G Adapter	qevbda.sys qenda.sys	8.58.16,0 8.58.12.0
HPE Ethernet 10Gb 2-port SFP+ QL41401-A2G Adapter	qevbda.sys qenda.sys	8.58.16,0 8.58.12.0
HPE Ethernet 10/25Gb 2-port SFP28 QL41401-A2G Adapter	qevbda.sys qenda.sys	8.58.16,0 8.58.12.0
HPE StoreFabric CN1200R-T Converged Network Adapter	qevbda.sys qenda.sys	8.58.16,0 8.58.12.0
HPE StoreFabric CN1300R Converged Network Adapter	qevbda.sys qenda.sys	8.58.16,0 8.58.12.0
Marvell QL41232HQCU Ethernet 10/25Gb 2-port SFP28 OCP3 Adapter for HPE	Qevbd.sys	8.58.16.0
Marvell QL41232HLCU Ethernet 10/25Gb 2-port SFP28 Adapter for HPE	Qevbd.sys	8.58.16.0
Marvell QL41134HLCU Ethernet 10Gb 4-port SFP+ Adapter for HPE	Qevbd.sys	8.58.16.0
Marvell QL41132HLRJ Ethernet 10Gb 2-port BASE-T Adapter for HPE	Qevbd.sys	8.58.16.0
Marvell QL41132HQRJ Ethernet 10Gb 2-port BASE-T OCP3 Adapter for HPE	Qevbd.sys	8.58.16.0
Marvell QL41132HQCU Ethernet 10Gb 2-port SFP+ OCP3 Adapter for HPE	Qevbd.sys	8.58.16.0
Marvell QL41132HLCU Ethernet 10Gb 2-port SFP+ Adapter for HPE	Qevbd.sys	8.58.16.0
Marvell QL41232HLCU Ethernet 10/25Gb 2-port SFP28 Adapter for HPE	Qevbd.sys	8.58.16.0
HP StoreFabric CN1100R Dual Port Converged Network Adapter	evbda.sys bxnd60a.sys	7.13.206.0 7.13.198.0
HPE StoreFabric CN1100R-T Adapter	evbda.sys bxnd60a.sys	7.13.206.0 7.13.198.0
HPE FlexFabric 10Gb 2-port FLR-T 57810S Adapter	evbda.sys bxnd60a.sys	7.13.206.0 7.13.198.0
HPE FlexFabric 10Gb 4-port FLR-T 57840S Adapter	evbda.sys bxnd60a.sys	7.13.206.0 7.13.198.0
HPE Ethernet 10Gb 2-port SFP+ 57810S Adapter	evbda.sys bxnd60a.sys	7.13.206.0 7.13.198.0
HPE Ethernet 10Gb 2-port BASE-T 57810S Adapter	evbda.sys bxnd60a.sys	7.13.206.0 7.13.198.0
HPE FlexFabric 10Gb 2-port FLR-SFP+ 57810S Adapter	evbda.sys bxnd60a.sys	7.13.206.0 7.13.198.0
HPE SN1200E	Elxfc.sys	12.8.518.0-12
HPE SN1600E	Elxfc.sys	12.8.518.0-12
HPE 3530c	Elxfc.sys	12.8.518.0-12
HPE 5330c	Elxfc.sys	12.8.518.0-12
HPE SN1610E	Elxfc.sys	12.8.518.0-12
HPE SN1100Q	QL2xxx.sys	9.4.5.20
HPE SN1600Q	QL2xxx.sys	9.4.5.20
HPE SN1610Q	QL2xxx.sys	9.4.5.20
HPE FlexFabric 536FLR-T Adapter	Bnx2fc.sys	7.13.206.0
HPE FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter	Bnx2fc.sys	7.13.206.0
HPE FlexFabric 10Gb 2-port 533FLR-T Adapter	Bnx2fc.sys	7.13.206.0
HPE Ethernet 10Gb 2-port 530T Adapter	Bnx2fc.sys	7.13.206.0
HPE Ethernet 10Gb 2-port 530SFP+ Adapter	Bnx2fc.sys	7.13.206.0
HPE CN1200R	Qedf.sys	8.58.1.0
HPE CN1300R	Qedf.sys	8.58.1.0

TABLE 8. Supported HPE Nimble Storage External Arrays

AF/HF/CS Series 6.x FW

TABLE 9. Supported HPE MSA Storage External Arrays

MSA 1050 series FW: VE270
MSA 2050 series FW: VL270
MSA 1060/2060 series FW: IN110

TABLE 10. Supported HPE Primera Storage External Arrays

HPE Primera 600 series FW: 4.3

TABLE 11. Supported HPE Alletra Storage External Arrays

HPE Alletra 9000 series FW: 9.x
HPE Alletra 6000 series FW: 6.x

TABLE 12. Supported HPE XP Storage External Arrays

HPE XP7 FW: 80-xx-xx
HPE XP8 FW: 90-xx-xx

CONFIGURING AND VALIDATING SECURED-CORE

Secured-core servers use a combination of hardware features, firmware enablement and Windows Server operating system capabilities to provide protection against current and future malware and rootkit types of security exploits. In general, 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 AQ (Additional Qualification) defines the additional set of requirements to support and enable the Secured-core capabilities explained above with Windows Server 2022. Systems that meet it are listed in the Windows Server Catalog.

Applicable products

The following platforms are Secured-core capable, using the processor families listed below:

AMD EPYC 7xx3 series processors (codename Milan)

- HPE ProLiant DL325 Gen10 Plus v2 server
- HPE ProLiant DL345 Gen10 Plus server
- HPE ProLiant DL365 Gen10 Plus server
- HPE ProLiant DL385 Gen10 Plus v2 server
- HPE ProLiant XL225n Gen10 Plus (HPE Apollo 2000 System)
- HPE ProLiant XL645d Gen10 Plus (HPE Apollo 6500 System)

- HPE ProLiant XL675d Gen10 Plus (HPE Apollo 6500 System)

3rd Generation Intel® Xeon® Scalable processors (codename Ice Lake)

- HPE ProLiant DL360 Gen10 Plus
- HPE ProLiant DL380 Gen10 Plus
- HPE ProLiant XL220n Gen10 Plus (HPE Apollo 2000 System)
- HPE ProLiant XL290n Gen10 Plus (HPE Apollo 2000 System)
- HPE Apollo 4200 Gen10 Plus System
- HPE Synergy 480 Gen10 Plus

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 in order to enable the Secured-core features, such as the DRTM driver for AMD platform. See the Installing the HPE Service Pack for ProLiant (SPP) section below for more information.

Configuring UEFI/BIOS settings

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

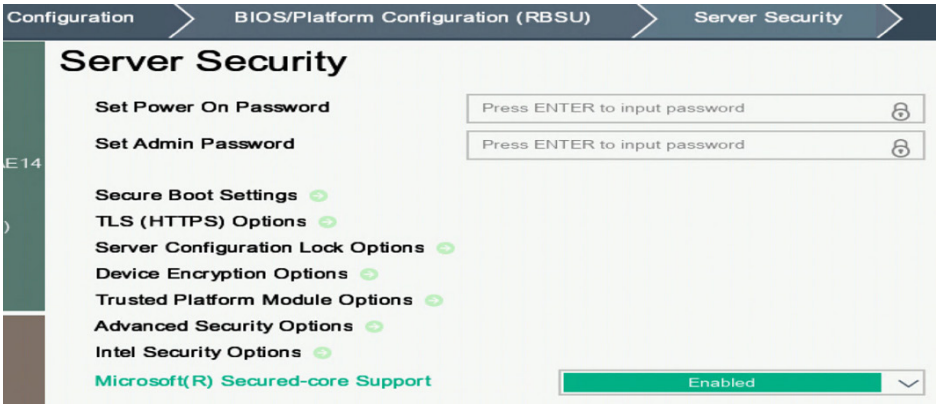

FIGURE 1. Secured-core configuration button in Gen10 Plus BIOS

Configuring Windows Server VBS, HVCI, and System Guard

To enable Secured-core features Virtualization-based security (VBS), Hypervisor Enforced Code Integrity (HVCI), and System Guard must be enabled on the OS, choose one of the following three (3) options for enabling these features. Choose a method and then proceed to confirm 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. Windows Admin Center (WAC) see Figure 2

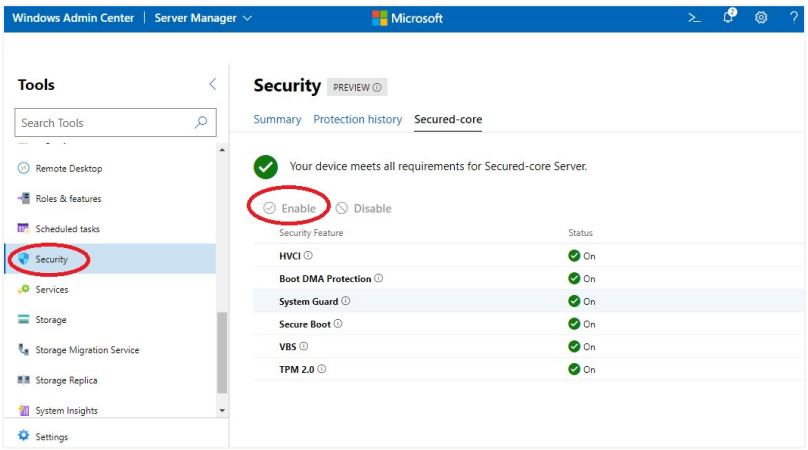

FIGURE 2. Secured-core configuration in Windows Admin Center (WAC)

3. Windows Security App (For Windows Server OS with Desktop experience only) see Figure 3 and Figure 4

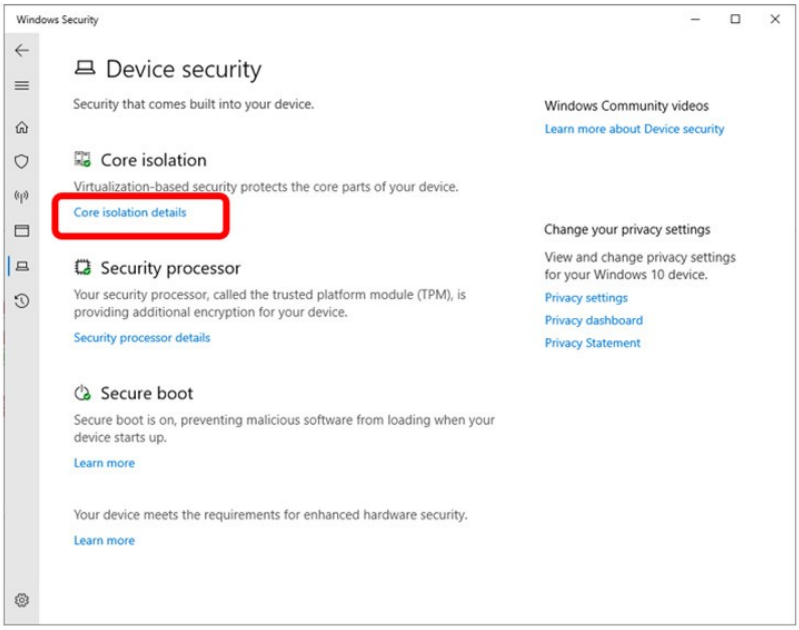

FIGURE 3. Secured-core configuration in Windows Security App

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.

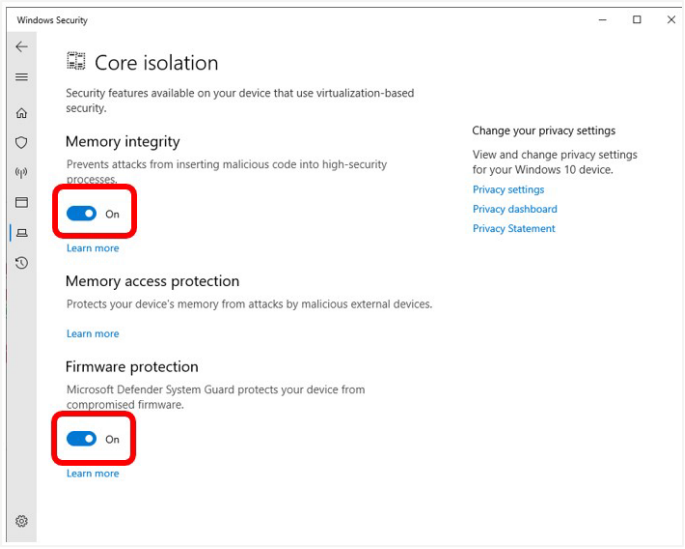

FIGURE 4. Secured-core configuration in Windows Security App

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 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

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

INSTALLING WINDOWS SERVER 2022

When deploying Windows Server 2022, 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 business 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 HPE Service Pack for ProLiant.

Windows Server 2022 mitigations for Meltdown and Spectre

Windows Server 2022 includes mitigations for Meltdown and Spectre vulnerabilities. However, the patches are not enabled by default and require the following registry keys (in order to pass validation with the Speculation Control 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 Windows Server guidance to protect against speculative execution side-channel vulnerabilities for more information.

For more information on Spectre or Meltdown mitigation: HPE support communication—customer bulletin

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

Speculation Control Validation PowerShell Script

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

INSTALLING THE HPE SERVICE PACK FOR PROLIANT (SPP)

This section describes the installation of the HPE Service Pack for ProLiant 2021.10.0 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 2022 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 8.9.0. 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/product-catalog/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 HPE 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 SUM folder.

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

1. Download and mount the HPE 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

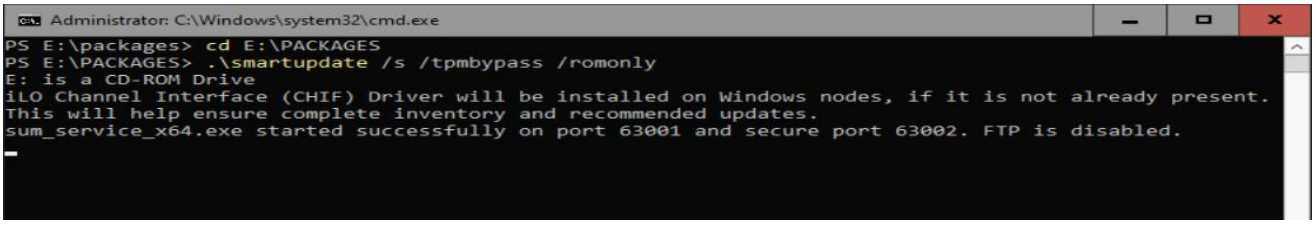

FIGURE 7. Running ".\smartupdate /s /tpmbypass /romonly" from the E:\PACKAGES folder to install the HPE Service Pack for ProLiant via PowerShell command line

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, see the Smart Update Manager 8.8.0 CLI and Interactive CLI Guide.

Installing the HPE Service Pack for ProLiant (SPP) on Windows Server 2022 with Desktop (UI)

Either the command line deployment explained above or the following Smart Update process using a browser may be used.

1. Step 1. Download and mount the HPE Service Pack for ProLiant .ISO on the local system
2. Step 2: Install 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 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 HPE 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 HPE Service Pack for ProLiant 2021.10.0 (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 (2021.10.0 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 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: Startup fails when Firmware protection is turned on—Windows Server | Microsoft Docs

RESOURCES

HPE Storage: hpe.com/storage/spock

What's new in Windows Server 2022: docs.microsoft.com/en-us/windows-server/get-started/whats-new-in-windows-server-2022

Microsoft Windows Server home page: microsoft.com/en-us/windows-server

Features Generally Available: docs.microsoft.com/en-us/windows-server/get-started/editions-comparison-windows-server-2022

Intelligent Provisioning User Guide for HPE ProLiant Gen10, HPE ProLiant Gen10 Plus Servers, and HPE Synergy: support.hpe.com/hpesc/public/docDisplay?docId=a00112754en_us&page=index.html

Installing and running Microsoft Windows Server 2019 and Windows Server 2022 on HPE Superdome Flex technical white paper: hpe.com/psnow/doc/a00074577enw

Deploying Microsoft Windows Server on HPE Superdome Flex 280 Servers, white paper: hpe.com/psnow/doc/a50003037ENW

Products sold prior to the November 1, 2015 separation of Hewlett-Packard Company into Hewlett Packard Enterprise Company and HP Inc. may have older product names and model numbers that differ from current models.

LEARN MORE AT

hpe.com/us/en/servers.html

a50003760ENW, Rev. 3

Hewlett Packard Enterprise