Dell PowerEdge RAID Controller 12 User’s Guide

PERC H365i Front DC-MHS and PERC H365i Adapter Cards

Regulatory Model: UCSA-1200 and UCSF-1230
June 2025
Rev. A00

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

Dell Technologies PowerEdge RAID Controller12

Dell Technologies PowerEdge RAID Controller12 or PERC12 is a series of RAID disk array controllers that are developed by Dell for its PowerEdge servers. The PERC H365i Front DC-MHS and PERC H365i Adapter controllers have the following characteristics:

- Reliability, high performance, and fault-tolerant disk subsystem management.
- RAID control capabilities including support for RAID levels 0, 1, and 10.
- Gen 4 PCIe x8 host interfaces.
- Supports Dell-qualified Serial Attached SCSI (SAS), Serial Advanced Technology Attachment (SATA), and PCIe SSD (NVMe) drives.
- Supports drive speeds for NVMe drives are 8 GT/s (Gen 3) and 16 GT/s (Gen 4) at maximum x2 lane width.
- Supports data rate throughput of 6 Gbps for SAS 2.0, 12 Gbps for SAS 3.0, and 22.5 Gbps for SAS 4.0 drives.
- Supports data rate of throughput of 6 Gbps for SATA 3.0 drives.

NOTE:

- The PERC 12 controller tools such as PERCCLI2, drivers, and firmware are not backward compatible with previous versions of PERC controllers.
- Mixing disks of different speed (7,200 RPM, 10,000 RPM, or 15,000 RPM) and bandwidth (6 Gbps, 12 Gbps, or 24 Gbps) while maintaining the same drive type (SAS or SATA) and technology (hard drive or SSD) is supported.
- PERC12 controllers support only single SCSI LUN and single NVMe namespace devices. Multi-LUN and Multi-Namespace devices are not supported.
- PERC12 series controllers do not support BIOS, and are not listed in the BIOS Setup section. The Storage boot operation is available only in the UEFI mode.
- Shingled Magnetic Recording (SMR) drives are not supported on PERC12 controllers.
- Mixing NVMe drives with SAS and SATA is not supported. Also, mixing hard drive and SSD in a virtual disk is not supported.
- SAS4 "22.5 Gbps" speed is used synonymously with "24G" and "24 Gbps" in documents and some applications. 22.5 Gbps is the data rate and 24 Gbps is the link speed.
- For the safety, regulatory, and ergonomic information that is associated with these devices, and for more information about the Integrated Dell Remote Access Controller (iDRAC) or Lifecycle Controller remote management, see the server-specific technical documentation.

CAUTION: For Japan Only—This is a Class A equipment. Operation of this equipment in a residential environment could cause Radio-wave interference. In this case, the user may be required to take corrective actions. (VCCI-A)

Topics:

Features of PERC H365i Front DC-MHS

This section provides a list of components that are used in the PERC H365i Front DC-MHS controller card.

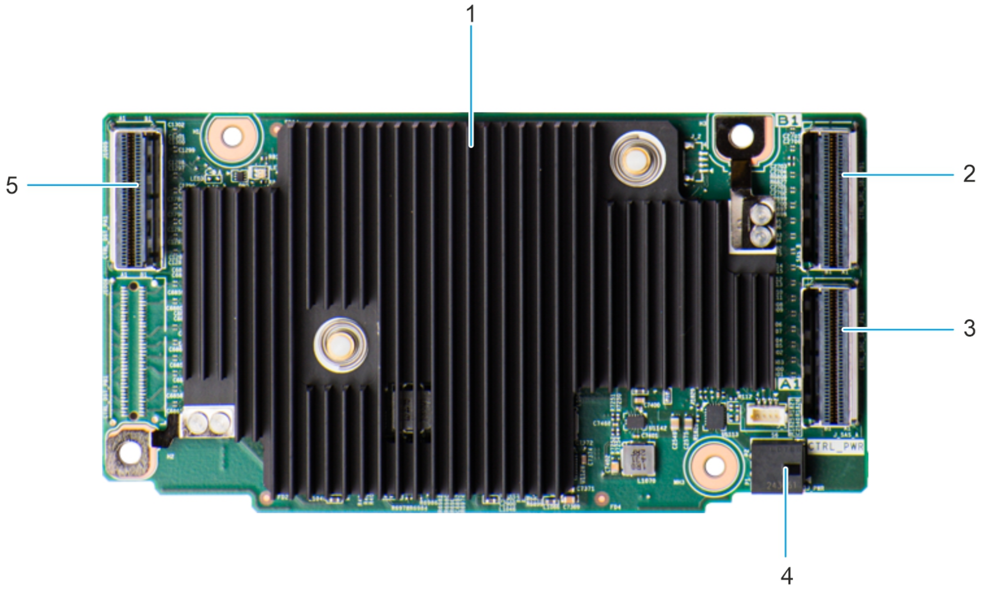


Figure 1. PERC H365i Front DC-MHS

1. Heat sink
2. PCIe connector B
3. PCIe connector A
4. Backplane connector B
5. Backplane connector A

Features of PERC H365i Adapter

This section provides a list of components that are used in the PERC H365i Adapter controller card.

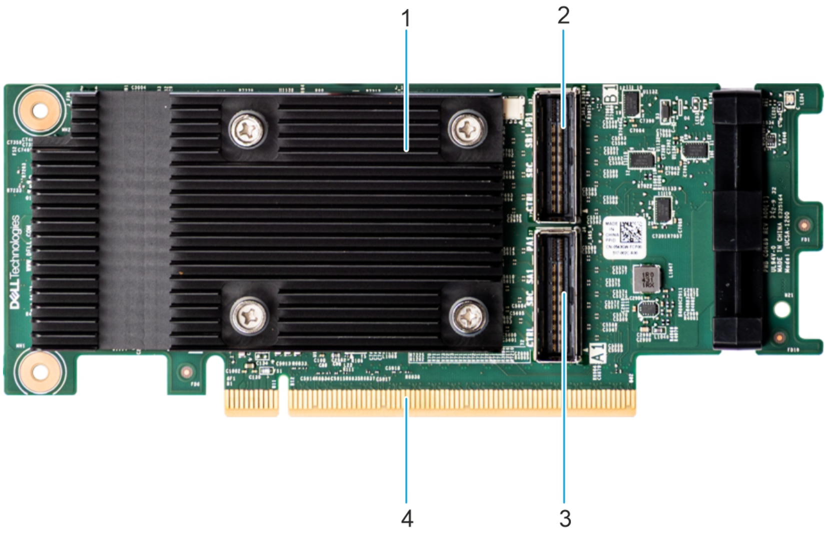


Figure 2. Features of PERC H365i Adapter

1. Heatsink
2. Backplane Connector-B
3. Backplane Connector-A
4. PCIe connector

Technical specifications of PERC12 H365i series cards

The following table lists the specifications of PERC12 H365i series cards.

Table 1. Technical specifications of PERC12 H365i series cards

Feature	PERC H365i Adapter	PERC H365i Front DC-MHS
RAID levels	0, 1, and 10	0, 1, and 10
Non–RAID	Yes	Yes
Host bus type	8-lane, PCIe 4 at 16 Gbps	8-lane, PCIe 4 at 16 Gbps
Side-band Management	I2C, PCIe VDM	I2C, PCIe VDM
Enclosures per port	Not applicable	Not applicable
Processor	Broadcom RAID-on-chip, SAS4016 chipset	Broadcom RAID-on-chip, SAS4016 chipset
Battery/ Energy pack support	No	No
Local Key Management security	Yes	Yes
iDRAC Local Key Management (iLKM)	Yes	Yes
Secure enterprise key manager security	Yes	Yes
Queue depth	Approximately 2,000	Approximately 2,000
Nonvolatile cache	No	No
Cache function	Write-through	Write-through
Max no of VDs in RAID mode	4	4
Max no of disk groups	4	4
Max number of VDs per disk group	4	4
Hot-swap devices supported	Yes	Yes
Auto-Configure behavior (Primary and Execute once)	Yes	Yes
Online capacity expansion	No	No
Dedicated hot spare	No	No
Global hot spare	Yes (Max. 4 drives)	Yes (Max. 4 drives)
Supported Drive Types	22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS. Gen3 (8 GT/s) and Gen4 (16 GT/s) NVMe	22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS. Gen3 (8 GT/s) and Gen4 (16 GT/s) NVMe
VD strip element size	Both 64 KB and 256 KB allowed on a hard drive. Only 64 KB allowed on an SSD.	Both 64 KB and 256 KB allowed on a hard drive. Only 64 KB allowed on an SSD.
NVMe PCIe support	Gen 4	Gen 4
Configuration maximum SAS/SATA hard drives support	● Without SAS Expander: 16 drives per controller ● With SAS Expander: Depends on your PowerEdge server model.	● Without SAS Expander: 16 drives per controller ● With SAS Expander: Depends on your PowerEdge server model.
Configuration maximum NVMe hard drives support	● Without PCIe Switch Expander: Eight drives per controller ● With PCIe Switch Expander: Depends on your PowerEdge server model.	● Without PCIe Switch Expander: Eight drives per controller ● With PCIe Switch Expander: Depends on your PowerEdge server model.

Table 1. Technical specifications of PERC12 H365i series cards (continued)

Feature	PERC H365i Adapter	PERC H365i Front DC-MHS
Controller maximum hard drives supported	● 24 NVMe ● With Expander—32 (Depends on your PowerEdge server model.) ● With Non-Expander backplane (SAS/SATA)—16 ● With Non-Expander (NVMe)—8 (x2)	● 24 NVMe ● With Expander—32 (Depends on your PowerEdge server model.) ● With Non-Expander backplane (SAS/SATA)—16 ● With Non-Expander (NVMe)—8 (x2)
Drive sector size supported	512B, 512e, and 4Kn	512B, 512e, and 4Kn
Storage Boot Support	UEFI-only	UEFI-only

Operating systems supported by PERC12 cards

- For a list of supported operating systems by a specific server for the PERC12 cards, see Dell Technologies Enterprise operating systems support.
- For the latest list of supported operating systems and driver installation instructions, see the operating system documentation at Operating System Documentation.
- For specific operating system service pack requirements, see the Drivers and Downloads section at Dell Technologies support site.

Applications and User Interfaces supported by PERC12

PERC12 card management applications include the Comprehensive Embedded Management (CEM), Dell OpenManage Storage Management, the Human Interface Infrastructure (HII) Configuration Utility, and the PERC Command Line Interface (CLI). They enable you to manage and configure the RAID system, create and manage multiple disk groups, control and monitor multiple RAID systems, and provide online maintenance.

Topics:

Comprehensive Embedded Management

Comprehensive Embedded Management (CEM) is a storage management solution for Dell systems that enables you to monitor the RAID and network controllers that are installed on the system using iDRAC without an operating system that is installed on the system.

Using CEM enables you to do the following:

- Monitor devices with and without an operating system that is installed on the server.
- Provide a specific location to access monitored data of the storage devices and network cards.
- Allows controller configuration for all 12th generation of PERC 12 controllers.

ⓘ **NOTE:** If you boot the system to HII (F2) or Lifecycle Controller (F10), then you cannot view the PERC cards on the CEM UI. The PERC cards are displayed on the CEM UI only after the system boot is complete.

Human Interface Infrastructure Configuration Utility

The Human Interface Infrastructure (HII) configuration utility is a storage management application integrated into the system BIOS <F2>. It is used to configure and manage your Dell PowerEdge RAID Controller (PERC) virtual disks and physical disks. This utility is independent of the operating system.

The PERC Command-Line Interface

The PERC Command-Line Interface (CLI) is a storage management application. This utility allows you to set up, configure, and manage your Dell PowerEdge RAID Controller (PERC) by using the CLI.

ⓘ **NOTE:** For more information, see the *Dell PowerEdge RAID Controller CLI Reference Guide* available on the support site.

3

Features of PowerEdge RAID Controller 12

Topics:

Controller features

This section lists the following controller features supported on Dell Technologies PowerEdge RAID Controller12 cards:

- Hardware Root of Trust
- Security Protocol and Data Model (SPDM)
- Device enumeration
- UEFI Secure Boot
- Auto-Configure Behavior (Execute Once)
- Auto-Configure Behavior (Primary and Secondary settings)
- Disk roaming
- Hardware Accelerated I/O
- Non–RAID disks
- Physical disk power management
- Firmware update
- Snapdump
- Physical disk coercion

Hardware Root of Trust

Hardware Root of Trust (RoT) builds a chain of trust by authenticating all the firmware components prior to its execution and permits only the authenticated firmware to be installed and upgraded. The controller boots from an Internal Boot ROM (IBR) that establishes the initial RoT and this process authenticates and builds a chain of trust with succeeding software using this RoT.

Security Protocol and Data Model (SPDM)

Security Protocol and Data Model (SPDM) is a mechanism by which iDRAC can verify the authenticity of the PERC in the system. Each PERC card is manufactured with a unique Device Identity certificate that is signed by Dell to ensure that the PERC is a Dell Certified controller. iDRAC will automatically retrieve a Device Identity certificate from the PERC card during boot and verify its identity against the PERC and notify the user if the device could not be authenticated. The SPDM feature is supported in the PERC 8.11.0.0-15-22 or later versions.

Device enumeration

All devices attached to the controller are assigned an ID from a persistent range of numbers. This includes backplanes, physical disks, and virtual disks. When a backplane is discovered, it is assigned a range of IDs based on the number of slots the backplane has. Each slot is assigned a dedicated ID in ascending order from the reserved range. When a disk is inserted, an ID allocated to the slot will be assigned.

Virtual disks are assigned an ID based on creation. The first virtual disk created will be assigned ID 1 and increases for each virtual disk. If a virtual disk is deleted, a newly created virtual disk will reuse that ID before using the next free ID. The newly created virtual disk will only reuse that ID if more than 120 seconds have passed since the pervious virtual disk was deleted.

- Operating system device enumeration
  - All devices are presented to the operating system as a SCSI device.
  - Virtual disks and non-RAID disks are presented to the OS in the order of their ID.
  - In case of some automated OS installation processes, by default, the OS is installed on the disk that is first presented to the system. If you are installing to a virtual disk, it is recommended to make the first created VD the OS. If you installing to a non-RAID disk, it is recommended to install the disk in slot 0 of the front backplane.
  - Only Virtual Disks and non-RAID disks are exposed to the OS. Unconfigured disks are hidden from the OS.

NOTE: For Linux servers only:

- Using the Device Reporting Order feature, you can select the order in which you can present either VDs or non-RAID drives to the OS.
- Using the First Device feature, you can select the order in which the physical device must be presented to the OS. The physical device will be enumerated first during the OS installation (when the OS has the latest Inbox drivers).

NOTE: Operating system enumeration may not be in this order if virtual disks or non-RAID disks are created while the operating system is running. The operating system may name devices based on the order in which they were created resulting in the operating system enumeration changing after reboot. It is recommended to restart the system for the final device enumeration after creating any virtual disk or non-RAID disk.

UEFI Secure Boot

UEFI Secure Boot is a technology that eliminates a major security void that may occur during a handoff between the UEFI firmware and UEFI operating system (OS). In UEFI Secure Boot, each component in the chain is validated and authorized against a specific certificate before it is allowed to load or run. Secure Boot removes the threat and provides software identity checking at every step of the boot-Platform firmware, Option Cards, and OS BootLoader. For more information about using UEFI Secure Boot in PowerEdge servers, see the "Secure Boot Configuration from BIOS Settings or F2" section of the iDRAC User's Guide available on the support site.

To view a list of supported operating systems, see PowerEdge server supported operating systems. By default, Windows and VMware support UEFI Secure Boot on both in-box and out-of-box drivers. However, Linux supports Secure Boot only with in-box drivers. For Out-of-Box Linux drivers, you must install Broadcom public key in the UEFI or OS signature database.
For information about installing signature database, see the technical documentation of the respective platform or OS. The Broadcom Public database key is provided with a OS driver package on the Dell support site. The following table lists the OS and their supported driver types and also indicates whether or not the UEFI Secure Boot feature is supported wth PERC12.

Table 2. UEFI Secure Boot Supported Operating systems on PowerEdge servers using PERC 12

Operating System	Driver Type	Secure Boot Supported	Signature Database
Microsoft Windows Server	In-Box	Yes	Native
Microsoft Windows Server	Out-of-Box	Yes	Native
RHEL	In-Box	Yes	Native
RHEL	Out-of-Box	Yes (with DB Install)	Broadcom Public
SUSE SLES	In-Box	Yes	Native
SUSE SLES	Out-of-Box	Yes (with DB Install)	Broadcom Public
VMware	VMware-provided	Yes	Native
Ubuntu	In-Box	Yes	Native

Auto-Configure Behavior (Execute Once)

The Auto-Configure Behavior (execute once) operation configures eligible ready-state drives based on the selected configuration. The default Auto-Config Behavior is Off. The supported configuration options for this feature are:

- Single drive RAID 0 with write-through cache policy
- Non-RAID disk
- Secured single drive RAID 0 with write-through cache policy
- Secured non-RAID disk

NOTE: The secured configuration options are available only when controller security is enabled and SEDs are present.

NOTE: The cache policy settings do not apply to non-RAID drives.

Auto-Configure Behavior (Primary and Secondary settings)

The Auto-Configure Behavior feature is used to configure new unconfigured drives (ready-state drives) during reboot and hot-insertion based on the selected configuration options (primary and secondary settings). The primary setting of Auto-Configure Behavior is used until the maximum configuration for the selected option is reached. Secondary setting of Auto-Configure Behavior is used after the maximum configuration for primary Auto-Configure option is reached.

Primary and secondary Auto-Configure settings do not impact known unconfigured drives during boot and hot-insertion. Known unconfigured drives are drives that were previously configured as virtual disk, hot-spare, or non-RAID disk and are now in the Ready state because the configuration on those drives was deleted.

When primary and secondary Auto-Configure options are changed from Off to any other settings, all unconfigured drives (including known devices) present on the controller remain unconfigured or in ready state.

NOTE: Secured configuration options are available only when the controller security is enabled.

The following table provides options for the supported primary Auto-Configure Behavior:

Table 3. Auto-Configure Behavior settings

Settings	Description
Off	The Auto-Configure Behavior feature is disabled. All new unconfigured drives remain in unconfigured or ready state. Existing configured drives are not affected when primary, secondary, or both Auto-Configure settings are changed to **Off**. **NOTE:** Applications use **Off** and **Ready** terms interchangeably for this setting.
Non–RAID	New unconfigured drives are configured as non-RAID disks during boot or during hot-insertion. All known unconfigured drives and existing configured drives remain unaffected during boot, hot-removal, or reinsertion.
Secured Non-RAID Disk	New unconfigured drives are configured as non-RAID disks during boot or hot-insertion. All known unconfigured drives and existing configured drives remain unaffected during boot, hot-removal, or reinsertion. SEDs are secured with the controller security key.

NOTE: Secondary Auto-Configure settings may not be supported on certain drive types. In such cases, the only available secondary Auto-Configure behavior option is Off.

Disk roaming

Disk roaming is when a physical disk is moved from one cable connection or backplane slot to another on the same controller. The controller automatically recognizes the relocated physical disks and logically assigns them to the virtual disks that are part of the disk group. If the physical disk is configured as a non–RAID disk, then the relocated physical disk is recognized as a non–RAID disk by the controller.

CAUTION: It is recommended that you perform a disk-roaming operation only when the server is powered off. Do not move drives between slots when the server is running. If it is attempted, maintain a 4-second delay between the removal and insertion operation for SAS or SATA devices. Maintain an 8-second delay between

> **the removal and insertion operation for NVMe devices. Inability to observe this delay may result in issues while detecting devices.**

Using disk roaming

About this task

Perform the following steps to use disk roaming:

Steps

1. Power off the server, PDs, enclosures, and server components.
2. Disconnect power cables from the server.
3. Move the physical disks to desired positions on the backplane or the enclosure.
4. Perform a safety check. Make sure the physical disks are inserted properly.
5. Power on the server.

Results

The controller detects the RAID configuration from the configuration data on the physical disks.

Hardware Accelerated I/O

The PERC12 provides improved hardware accelerated I/O when compared to the previous generation of controllers. The following table lists the different types of I/O provided by PERC 12 and previous generation of storage controllers:

Table 4. Comparison of performance for different I/O type for PERC 12 and previous generation of controllers

I/O Type	VD Cache	Hardware Accelerated in previous generations	Hardware Accelerated in PERC12 generation
SAS/SATA non-RAID Read-Write	N/A	Yes	Yes
NVMe non-RAID Read Write	N/A	Yes	Yes
Any RAID Level Single-Strip-Read	Write-Through	Yes	Yes
R0, R1, R10 Single-Strip-Write	Write-Through	Yes	Yes
Any RAID Level Multi-Strip-Read	Write-Through	No	Yes
R0, R1, R10 Multi-Strip-Write	Write-Through	No	Yes
Degraded VD-Read	Write-Through	No	Yes

Non–RAID disks

A non–RAID disk is a single disk to the host, and not a RAID volume. The only supported cache policy for non-RAID disks is Write-Through, and cannot be altered. Non-RAID disks provide passthrough support allowing the operating system nearly full access to the drive. All drives are presented to the host as a SAS target. The controller will convert the SAS/SCSI command to the appropriate SATA or NVMe command.

Physical disk power management

Physical disk power management is a power-saving feature of PERC12 series cards. The feature allows disks to be spun down based on disk configuration and I/O activity. The feature is supported on all rotating SAS and SATA disks, and includes unconfigured and hot-spare disks. By default, the physical disk power management feature is enabled on unconfigured drives and disabled on hot-spare drives.

Firmware update

Upgrade or downgrade the PERC12 firmware using Update Packages or PERC CLI. See Manage the PERC12 firmware.

Secure firmware update

Enables you to upgrade firmware by using an RSA encryption-decryption algorithm. The firmware upgrade operations you perform on a PERC 12 controller are secure. You can upgrade the PERC firmware by using only a Dell certified firmware.

Online firmware update support from iDRAC using PLDM

Starting from PERC 12 firmware version 8.11.0.0.18-25/8.11.0.0.15-25 Update Packages (DUPs), the Online firmware update operation is supported using iDRAC interfaces. This is supported by the Platform Level Data Model (PLDM) standard. However, a System Reset operation may still be required to activate the newly downloaded firmware in exceptional cases such as presence of preserved cache or update to firmware components related to power handling or caching.

ⓘ **NOTE:** Before performing an online firmware update operation for PERC12 series controllers, ensure that you have the following iDRAC versions:

- For 17G PowerEdge servers, iDRAC 1.20.50.50 and later .
- For 16G PowerEdge servers, iDRAC 7.20.30.50 and later .

Snapdump

The Snapdump feature provides the Dell Technical Support team with the debug information that can help to find the cause of firmware failure. In the instance of firmware failures, the firmware collects the logs and information at the time of failure, which are stored in a compressed file that is called a snapdump.

Snapdumps are also generated manually to provide additional debug information. When a Snapdump is generated, it is stored in the controller's cache memory. In the event of a power loss, the controller offloads the Snapdump as part of its cache preservation mechanism. By default, Snapdumps are saved until you restrart the server four times, and then it is deleted..

ⓘ **NOTE:** The HBA465 series and H365 series controllers do not have DDR or NAND Flash. Therefore, a Snampdump data is stored in SPI Flash. Because of this, it can store only one active snapdump at a time.

ⓘ **NOTE:** The I/O operation will pause for about 5–10 seconds while collecting the on-demand snapdump.

To generate, delete, or download a stored snapdump, see the *Dell PowerEdge RAID Controller CLI Reference Guide* available on the support site.

Physical disk coercion

Enables you to create consistent disk size for drives that have slightly different sizes. Use the coercion feature in HII to match the sizes of drives that are slightly larger with the smaller drives in case you want to insert slightly smaller drives later. PERC 12 controllers support coercion modes such as **None (32 MiB)**, **128 MiB**, or **1 GiB**. Default mode is **128 MiB**. For virtual disks and hot-spares, the last **512 MiB** is used for configuration information.

Coerced size = (raw disk size minus 512 MiB configuration information) rounded down to the nearest full coercion mode size bucket.

Set Drive Coercion Mode

To provide consistent disk size for drives that are slightly different in sizes, set the drive coercion mode in HII.

Steps

1. Log in to HII.
2. Go to **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. Select the **Drive Coercion Mode** and click **Apply Changes**.

Virtual disk features

NOTE: All VDs are exposed as 4k sector devices to the host and operating system.

This section lists the following virtual disk features that are supported on PERC12 cards:

- Auto-import foreign virtual drives
- Virtual disk migration
- Virtual disk initialization
- Background operations

Auto-import foreign virtual drives

By default, this feature is enabled on a PERC 12 controller. Foreign Virtual Drives (VDs) are automatically imported when a server is either restarted, or a controller is reset or replaced. Ensure that you verify the new VD number after automatically importing because a VD number may change after an auto-import operation. To resolve any issues pertaining to auto-importing, see the Troubleshooting section in this User's Guide.

Virtual disk migration

The PERC12 series supports migration of virtual disks from one controller to another without taking the target controller offline. The controller can import RAID virtual disks in optimal, degraded, or partially degraded states. You cannot import a virtual disk that is offline. When a controller detects a configured physical disk, it marks the physical disk as foreign, and generates an alert indicating that a foreign disk was detected.

NOTE: You cannot migrate data managed by earlier versions such as PERC 10 and PERC 11 to PERC 12 controllers. However, you can migrate data of unsecured non-RAID disks from PERC 10 and PERC 11 to the latest PERC 12 controllers.

NOTE: The source controller must be offline prior to performing the disk migration.

NOTE: Importing secured VDs is supported as long as the appropriate Local Key Management (LKM) is supplied or configured.

NOTE: An additional reboot operation may be required for the UEFI BIOS to detect a newly imported Virtual disk.

NOTE: Importing a manually offlined VD is not supported. Recreate the VD exactly as it was before it was offline to get the configuration back.

Virtual disk write cache policy

The write-cache policy of a virtual disk determines how the controller handles Write operations to the virtual disk.

Table 5. Write cache policies

Feature	Description
Write-through	The controller sends a data transfer completion response to the host system when the disk subsystem has received all the data in a transaction.

Table 5. Write cache policies

Feature	Description
	NOTE: Certain data patterns and configurations perform better with a write-through cache policy.

NOTE: All RAID volumes are presented as write-through to the operating system (Windows and Linux) independent of the actual write-cache policy of the virtual disk. PERC cards manage the data in the cache independently of the operating system or any applications.

Conditions under which forced write-through with no battery is used

The H365i series of controllers do not support a battery pack. Therefore, the default mode of write-cache is write-through.

Virtual disk initialization

The PERC12 series controllers support two types of virtual disk initialization:

- Full initialization
- Fast initialization

CAUTION: Initializing virtual disks erases files and file systems while keeping the virtual disk configuration intact.

Full initialization

NOTE: When the full initialization operation is in progress, you cannot perform any host data I/O operations on the VDs.

Performing a full initialization operation on a virtual disk overwrites all blocks and deletes any data that previously existed on the virtual disk. Full initialization of a virtual disk eliminates the need for the virtual disk to undergo a Background Initialization (BGI). Full initialization can be performed after the virtual disk is created. For more information on how to create a virtual disk and configure virtual disk parameters (full initialization) in HII, see Create virtual disk and configure virtual disk parameters.

NOTE: If the system reboots during a full initialization operation, the operation is abruptly stopped and a BGI operation starts on the virtual disk.

Fast initialization

A fast initialization on a virtual disk overwrites the first and last 8 MiB of the virtual disk, clearing any boot records or partition information. The operation takes only 2–3 seconds to complete, but it is followed by BGI, which takes longer to complete.

NOTE: During full or fast initialization, the host cannot access the virtual disk. As a result, if the host attempts to access the virtual disk while it is initializing, all I/O sent by the host will fail.

NOTE: When using iDRAC to create a virtual disk, the drive undergoes fast initialization. During this process all I/O requests to the drive will respond with a sense key of **Not Ready** and the I/O operation will fail. If the operating system attempts to read from the drive as soon as it discovers the drive and while the fast initialization is still in process, the I/O operation fails and the operating system reports an I/O error.

Background operations

Background initialization

Background Initialization (BGI) is an automated process that writes parity or mirror data on newly created virtual disks. BGI does not run on RAID 0 virtual disks. You can control the BGI rate in the HII application. Any change to the BGI rate does not take effect until the next BGI operation is started.

ⓘ **NOTE:**

- If you cancel BGI, it automatically restarts within five minutes.
- Unlike full or fast initialization of virtual disks, background initialization does not clear data from the physical disks.
- Consistency Check (CC) and BGI typically cause some loss in performance until the operation completes.

Consistency check and BGI perform similar functions in that they both correct parity errors. However, CC reports data inconsistencies through an event notification, while BGI does not. You can start CC manually, but not BGI.

Consistency checks

Consistency Check (CC) is a background operation that verifies and corrects the mirror or parity data for fault tolerant virtual disks. It is recommended that you periodically run a consistency check on virtual disks. You can manually start a CC using the HII Configuration Utility or the PERC CLI application. To start a CC using the HII Configuration Utility, see Check consistency of VDs.

ⓘ **NOTE:** CC or BGI typically causes some loss in performance until the operation completes.

CC and BGI both correct parity errors. However, CC reports data inconsistencies through an event notification, while BGI does not. You can start CC manually, but not BGI.

Drive features

This section lists the following hard drive features supported on PERC12 cards:

- Self-Encrypting Drives (SEDs)
- Opal Security Management
- Instant secure erase
- 4KB sector drives
- Non-Volatile Memory Express
- Conditions under which a PERC supports an NVMe drive

Self-Encrypting Drives (SEDs)

The PERC12 series of cards support SEDs for protection of data against loss or theft by the use of encryption technology on the drives. There is one security key per controller. You can manage the security key using Local Key Management (LKM) or OpenManage Secure Enterprise Key Manager also referred as Secure Enterprise Key Manager (SEKM). The security key is used by the controller to lock and unlock access to encryption-capable physical disks. To use this feature, you must:

- Have SEDs in your system.
- Create a security key.

SEDs that are secured by a non-PERC entity cannot be used by PERC. Ensure that the SED is re-provisioned in an applicable manner by the non-PERC entity before connecting to PERC. For more information, see Security key and RAID management.

ⓘ **NOTE:** You cannot enable security on non-optimal virtual disks.

ⓘ **NOTE:** PERC12 supports Trusted Computing Group (TCG) Enterprise Security Subsystem Classes (SSC) SAS or SATA SEDs, and TCG Opal SSC NVMe drives.

Opal Security Management

Opal Security Management of Opal SEDs requires security key management support. You can use integrated Dell Remote Access Controller (iDRAC) to generate the security key for the Opal drives which is used as an authentication key to lock and unlock the Opal drives.

Instant secure erase

Instant Secure Erase (ISE) drives use the same encryption technology as SEDs but do not allow the encryption key to be secured. The encryption technology allows the drive to be re-purposed and securely erased using the cryptographic erase function.

> ⓘ **NOTE:** ISE drives do not provide protection against reading the drive data in case of a theft.

Cryptographic Erase with PSID Revert

The controller firmware supports reverting an SED state to the factory default with the help of Physical Security Identifier (PSID). The PSID, or Physical SID of the drive, is a 32-character password assigned by the drive manufacturer during production. A host system cannot change the password. The PSID is on the drive label in a readable format, and depending on the drive manufacturer, it may also be available in a bar code format. If a drive is in the locked state and the key is not known then a cryptographic erase with PSID is required. The SED physical security ID (PSID) is required for reverting an SED to the non-secured factory state. For enhanced security, the PSID is accessible only by removing the drive and examining the drive label. In addition to reverting the drive state to factory default serttings, it also secure erases all existing data.

> ⓘ **NOTE:** The PSID can only be used for reverting the drive; it does not grant access to any encrypted data present on the drive.

Physical disk erase

The Physical disk erase feature allows data that is saved on disks to be securely erased so that data cannot be recovered. The PERC 12 series controllers provide four methods for erasing disks—Physical Disk Erase, Cryptographic Erase, Sanitize Block Erase, and Sanitize Overwrite.

- Physical disk erase—Erases drives by writing data pattern on disks with varying number of passes. Physical disk erase is supported on non-ISE and non-SEDs.
- Cryptographic Erase—Cryptographically erases disks by changing the media encryption key. This feature is supported on ISE or SEDs. In case of SEDs, unsecures the drives and reverts them to factory security settings. See Instant secure erase and Self-Encrypting Drives (SEDs).
- Sanitize Block Erase—Alters information by setting the physical blocks to a vendor specific value.
- Sanitize Overwrite Erase—Alters information by setting physical blocks to a user-specific value. Also, it can do multiple overwrite operations and invert the pattern between consecutive overwrite passes.

Sanitize Erase operation

The Sanitize Block Erase or Sanitize Overwrite Erase operation managed by the controllers can be triggered using PERC CLI. Prerequisites for performing this operation are:

- Have an unconfigured physical disk.
- Physical disks must support only the necessary sanitize method.

> ⓘ **NOTE:** If drive supports the cryptographic erase operation, drive will not be eligible to perform the required sanitize operation. Limitations of the PERC managed Sanitize Erase operation are:
>
> - After the sanitize erase operation is started, the non-RAID drive creation operation will be blocked while an erase operation is in progress.

4KB sector drives

The PERC12 series controllers support 4 KB sector drives. Before installing Windows on 4KB sector drives, see Unable to install the Microsoft Windows operating system .

ⓘ **NOTE:** Mixing 512–byte native and 512–byte emulated drives in a VD is allowed, but mixing 512–byte and 4 KB native drives in a VD is not allowed.

ⓘ **NOTE:** All VDs are exposed to the host as a 4K device.

Non-Volatile Memory Express

Non-Volatile Memory Express (NVMe) is a standardized, high-performance host controller interface and a storage protocol for communicating with non-volatile memory storage devices over the PCIe interface standard. The PERC12 controller supports up to 8 direct-attach NVMe drives. The PERC12 controller is a PCIe endpoint to the host, a PowerEdge server, and configured as a PCIe root complex for downstream PCIe NVMe devices connected to the controller.

ⓘ **NOTE:** The NVMe drive on the PERC12 controller is identified as a SCSI disk in the operating system. The NVMe CLI will not work for the attached NVMe drives.

Conditions under which a PERC supports an NVMe drive

- A single Namespace must be present.
- The NameSpace Identifier (NSID) with ID 1, which is (NSID=1), must be present.
- The namespace with NSID=1 must be formatted without end-to-end data protection information and must have the metadata disabled
- PERC supports 512-bytes or 4 KB sector disk drives for NVMe devices.

Drive recovery for NVMe initialization failure

If an NVMe drive fails to initialize, the drive that is connected to PERC can be recovered in HII. The NVMe initialization errors in the drives are listed as recoverable and nonrecoverable errors in HII.

The recoverable drives are identified as the following in the HII: `Unusable (Recoverable), Error: <error string>`. The nonrecoverable drives are listed as `Usable` in HII. Metadata and End-to-end Data Protected (EEDP) formatted disks cannot be recovered when connected to PERC 12.

Drive recovery with correctable NVMe initialization errors

Recover the drives with recoverable NVMe initialization errors in HII to enable the drives to work properly.

Steps

1. Log in to HII.
2. Click **Main Menu** > **Device Management** > **Enclosure X**.
   The drives with recoverable and non-recoverable errors are listed.
3. Select the drive and click **Recover**.
   If the drive data is successfully recovered, the drive is listed under physical drives and removed from the recoverable error list. If the drive has other recoverable errors, the drive is listed again in the recoverable errors list.
4. If the repair is not successful, click **Recover**.
   If the error is still not resolved or if the drive has other non-recoverable errors, the drive is moved to the non-recoverable error list.

Fault tolerance

The Controller series cards support the following:

- The SMART feature

- Patrol Read

The following sections describe methods to achieve fault tolerance.

The SMART feature

The SMART feature monitors certain physical aspects of all motors, heads, and physical disk electronics to help detect predictable physical disk failures. Data on SMART compliant physical disks can be monitored to identify changes in values and determine whether the values are within threshold limits. Many mechanical and electrical failures display some degradation in performance before failure.

A SMART failure is also referred to as predicted failure. There are numerous factors of a predicted physical disk failure—bearing failure, a broken read or write head, and changes in spin-up rate. Also, there are factors related to read or write surface failure, such as seek error rate and excessive bad sectors.

NOTE: For detailed information on SCSI interface specifications, see t10.org. For detailed information on SATA interface specifications, see t13.org.

Patrol Read

The Patrol read feature is designed as a preventative measure to ensure physical disk health and data integrity. Patrol read scans and resolves potential problems on configured physical disks. The Dell OpenManage Storage Management application can be used to start patrol-read and change its behavior.

Some properties of the patrol-read feature are:

- Runs on all disks on the controller that are configured as part of a virtual disk, including hot-spares.
- The Patrol read feature does not run on physical disks that are not part of non-RAID disks, virtual disks, or drives that are in Ready state.
- The amount of controller resources dedicated to patrol read operations adjusts based on the number of outstanding disk I/O operations. For example, if the system is processing a large number of I/O operations, then patrol read uses fewer resources to allow the I/O to take a higher priority.
- Patrol read does not run on disks that are involved in any of the following operations:
  - Rebuild
  - Replace member
  - Full or background initialization
  - Consistency Check
  - Online capacity expansion (OCE)

  NOTE: By default, patrol read automatically runs every seven days on configured hard drives.

For more information about patrol read, see the *Dell OpenManage Storage Management User's Guide* available at OpenManage Manuals.

Physical disk failure detection

If a disk fails and it is replaced with a new disk, the controller will automatically start a rebuild on the new disk. See, Configured slot behavior. Automatic rebuilds can also be performed on hot-spares. If you have configured hot-spares, the controller will automatically try to use them to rebuild the degraded virtual disk.

Using persistent hot spare slots

The PERC12 series is configured so that the system backplane or storage enclosure disk slots are dedicated as hot spare slots.

Any slots with hot-spares are persistent. If a hot spare disk fails or is removed, a replacement disk that is inserted into the same slot automatically becomes a hot spare with the same properties as the hot spare slot it is replacing. If the replacement disk does not match the disk protocol and technology, it does not become a hot spare.

For more information about persistent hot-spares, see the Dell OpenManage documentation available on the support site.

ⓘ **NOTE:** If all the VDs that are associated with a global hot spare are removed, then the hot spare will be converted to a global hot spare.

ⓘ **NOTE:** If all the VDs attached to a controller are removed from a system, then the hot spare slots, if any, will be deleted.

Configured slot behavior

This feature is similar to persistent hot spare slot behavior. If a fault-tolerant VD is configured to the system and a drive is replaced, the configured slot will automatically rebuild on the inserted drive regardless of the data on the drive. This operation overwrites the data on the drive. The copy-back feature is not supported on H365 series controllers.

Table 6. Drive state operation

Drive state/operation	Drive state	Slot configured in VD
Insert an unconfigured drive into the system.	Ready	Rebuild or copyback starts.
Insert the configured drive into the system.	Foreign	● Rebuild or copyback starts. ● Original drive data lost
Insert a configured locked drive into the system (unlockable).	Foreign	Cryptographic Erase (If configured VD is not secured). ● Rebuild or copyback starts. ● Original drive data lost
Insert a locked drive into the system (nonunlockable).	Foreign locked	Foreign locked

Physical disk hot-swapping

Hot swapping is the manual replacement of a disk while the PERC12 series cards are online and performing their normal functions. Ensure that the following requirements are met before hot-swapping a physical disk:

- The system backplane or enclosure must support hot-swapping.
- To perform a rebuild or copyback operation, the replacement drive must be of the same protocol and disk technology. For example, only a SAS hard drive can replace a SAS hard drive and only a SATA SSD can replace a SATA SSD.

ⓘ **NOTE:** To check if the backplane supports hot-swapping, see the platform-specific Installation and Service Manual available on the support site.

Using Replace Member and Revertible hot-spares

The Replace Member functionality enables a previously commissioned hot-spare to revert to a usable hot-spare. When a disk failure occurs within a virtual disk, an assigned hot-spare—dedicated or global—is commissioned and begins rebuilding until the virtual disk is optimal. After the failed disk is replaced in the same slot and the rebuild to the hot-spare is complete, the controller automatically starts to copy data from the commissioned hot spare to the newly inserted disk. After the data is copied, the new disk is a part of the virtual disk and the hot-spare is reverted to being a ready hot-spare. This allows hot-spares to remain in specific enclosure slots. While the controller is reverting the hot-spare, the virtual disk remains optimal. The controller automatically reverts a hot-spare only if the failed disk is replaced with a new disk in the same slot. If the new disk is not placed in the same slot, a Manual Replace Member operation can be used to revert a previously commissioned hot-spare.

ⓘ **NOTE:** A Manual Replace Member operation typically causes a temporary impact on disk performance. After the operation is complete, performance returns to normal state.

ⓘ **NOTE:** Replace member is also referred to as "copyback and replace" in some management applications or events.

Automatic Replace Member with predicted failure

An Automatic Replace Member feature is triggered when there is a SMART predictive failure reported on the VD of a PD. The Automatic Replace Member featuerd is initiated when the first SMART error occurs on a physical disk that is part of a virtual disk. The target disk needs to be a hot-spare that qualifies as a rebuild disk. The physical disk with the SMART error is marked as failed only after the successful completion of the replacement task. This prevents the array from reaching degraded state.

If an Automatic Replace Member operation occurs using a source disk that was originally a hot-spare (that was used in a rebuild), and a new disk is added and set as a target disk for the replace member operation, the hot-spare drive will revert to the hot-spare state after the operation completes.

NOTE: To enable the Automatic Replace Member feature, use the Dell OpenManage Storage Management application.

Install and remove a PERC12 card

Topics:

Before working inside your system

Prerequisites

Follow the safety guidelines listed in Safety instructions.

Steps

1. Power off the system and all attached peripherals.
2. Disconnect the system from the electrical outlet and disconnect the peripherals.
3. If applicable, remove the system from the rack.

   For more information, see the Rail Installation Guide relevant to your rail solutions at PowerEdge Manuals.
4. Remove the system cover.

Safety instructions

⚠ **CAUTION: Ensure that two or more people lift the system horizontally from the box and place it on a flat surface, rack lift, or into the rails.**

⚠ **WARNING: Opening or removing the PowerEdge server cover while the server is powered on may expose you to a risk of electric shock.**

⚠ **WARNING: Do not operate the server without the cover for a duration exceeding five minutes. Operating the system without the system cover can result in component damage.**

ⓘ **NOTE:** Many repairs may only be done by a certified service technician. You should only perform troubleshooting and simple repairs as authorized in your product documentation, or as directed by the online or telephone service and support team. Damage due to servicing that is not authorized by Dell is not covered by your warranty. Read and follow the safety instructions that are shipped with your product.

⚠ **CAUTION: To ensure proper operation and cooling, all system bays and fans must always be populated with a component or a blank.**

ⓘ **NOTE:** It is recommended that you always use an antistatic mat and antistatic strap while working on components inside the server.

ⓘ **NOTE:** To ensure proper operation and cooling, all system bays and fans must always be populated with a component or a blank.

ⓘ **NOTE:** While replacing the hot swappable PSU, after next server boot, the new PSU automatically updates to the same firmware and configuration of the replaced one.

Remove the PERC H365i Front DC-MHS card

Describes the tasks that must be completed to remove the PERC H365i Front DC-MHS card from a PowerEdge server. This procedure is recommended for authorized service technicians and should only be performed with proper training and equipment.

Prerequisites

△ **CAUTION: Many repairs may only be done by a certified service technician. You should only perform troubleshooting and simple repairs as authorized in your product documentation, or as directed by the online or telephone service and support team. Damage due to servicing that is not authorized by Dell is not covered by your warranty. Read and follow the safety instructions that are shipped with your product.**

ⓘ **NOTE:** It is recommended that you always use a static mat and anti-static wrist strap while working on components inside the system.

Steps

1. Power off the server, including any attached peripherals, and disconnect the system from the electrical outlet and peripherals.
2. Open the system.
3. Locate the PERC card in the controller carrier at the front of the system.

   △ **CAUTION: To prevent damage to the card, you must hold the card by its edges only.**

4. Unscrew the fasteners on the controller carrier and slide the carrier away from the backplane, disconnecting the controller from the backplane.
5. Disconnect any cables that are connected to the card:
   a. Press down and hold the metal tab on the cable connector.
   b. Pull the cables out of the connector.
6. Remove the PERC controller from the controller carrier.
7. Insert the replacement controller into the carrier and secure it with the appropriate screws.
8. Take the replacement storage controller and reconnect the cables before reconnecting it to the backplane.
9. Close the system.
10. Reconnect the system to its electrical outlet and turn the system on, including any attached peripherals.

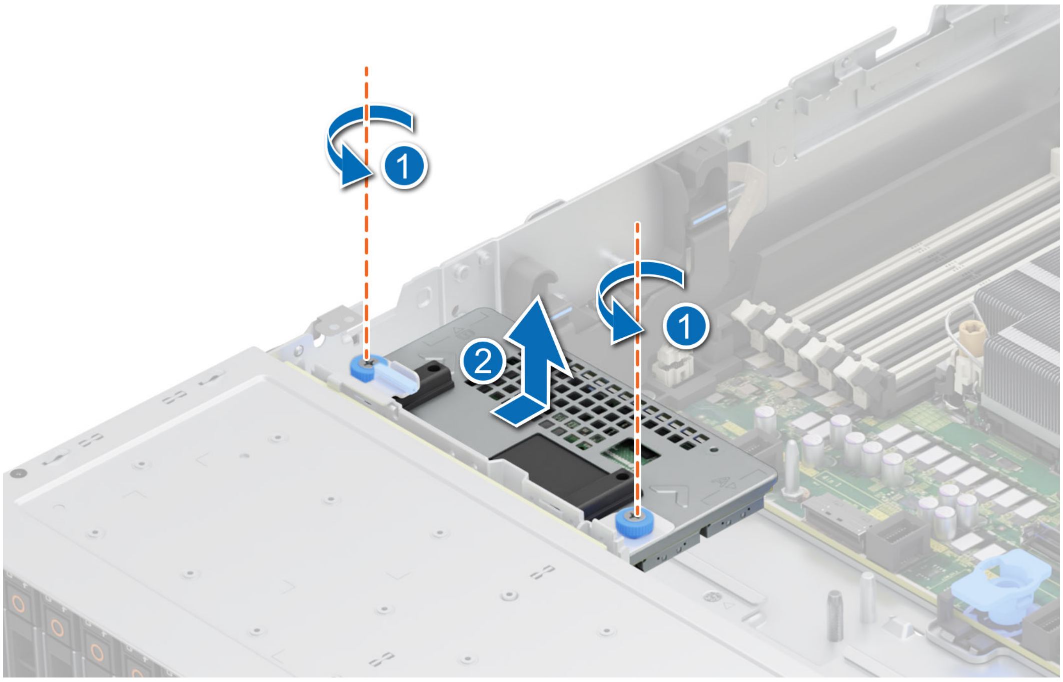


Figure 3. Remove the PERC H365i Front DC-MHS card

Install the PERC H365i Front DC-MHS card

Describes the tasks that must be completed to remove the PERC H365i Front DC-MHS card from a PowerEdge server. This procedure is recommended for authorized service technicians and should only be performed with proper training and equipment.

Prerequisites

⚠ **CAUTION: Many repairs may only be done by a certified service technician. You should only perform troubleshooting and simple repairs as authorized in your product documentation, or as directed by the online or telephone service and support team. Damage due to servicing that is not authorized by Dell is not covered by your warranty. Read and follow the safety instructions that are shipped with your product.**

ⓘ **NOTE:** It is recommended that you always use a static mat and anti-static wrist strap while working on components inside the system.

Steps

1. Power off the system, including any attached peripherals, and disconnect the system from the electrical outlet.

   ⓘ **NOTE:** Perform a graceful shutdown of the sled to ensure that data in the cache is moved to the disk before the controller is removed.

2. Open the system.
3. Connect the PERC card to the carrier and ensure that the screws are properly fastened in place.

   ⚠ **CAUTION: To prevent damage to the card, hold the card by its edges only.**

4. Connect the cable connectors to the card.

   ⓘ **NOTE:** Ensure that you connect the cable according to the connector labels on the cable. The cable does not function properly if reversed.

5. Align the carrier with the guide pins until the controller is securely seated.
6. Slide the card into the connector until it is fully seated in the connector. Tighten the screws on the carrier that connect to the chassis to secure the carrier.
7. Close the system.
8. Reconnect the system to its electrical outlet and power on the system and any attached peripherals.

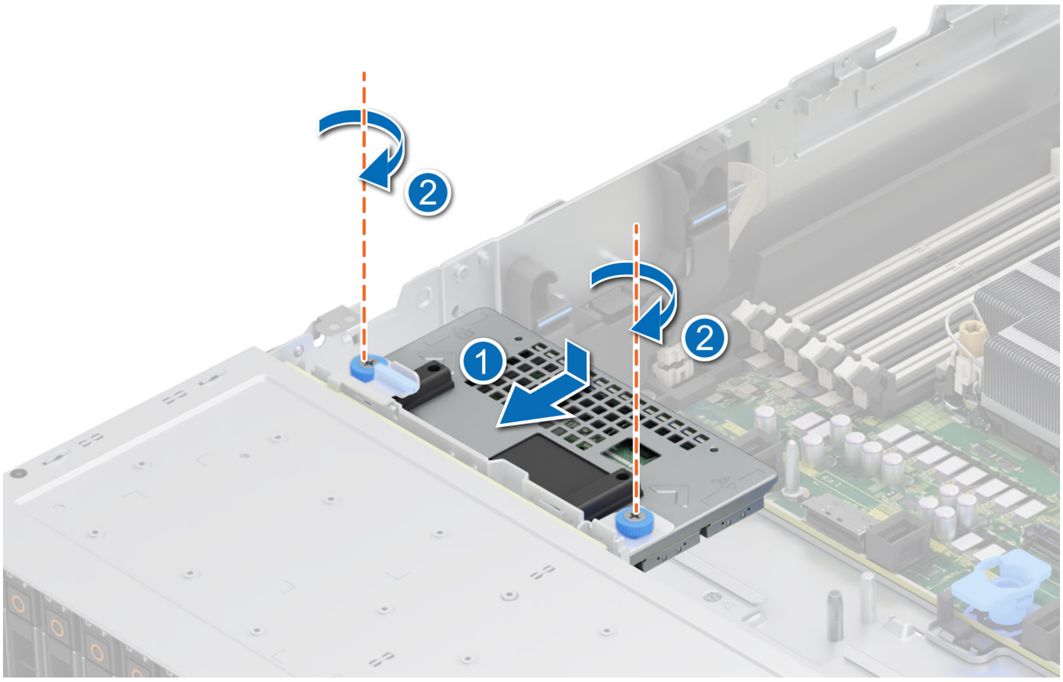


Figure 4. Install the PERC H365i Front DC-MHS card

Remove the PERC H365i Adapter

Prerequisites

> ⚠ **CAUTION: Many repairs may only be done by a certified service technician. You should only perform troubleshooting and simple repairs as authorized in your product documentation, or as directed by the online or telephone service and support team. Damage due to servicing that is not authorized by Dell is not covered by your warranty. Read and follow the safety instructions that are shipped with your product.**

- You have read and complied with the safety guidelines that are listed in Safety instructions.
- You have completed the procedures in Before working inside your system.

Steps

1. Power off the server, including any attached peripherals, and disconnect the system from the electrical outlet and peripherals.
2. Remove the system cover.
3. Locate the PERC H365i Adapter in the expansion riser on the system board.

   > ⚠ **CAUTION: To prevent damage to the card, hold the card by its edges only.**

4. Unfasten and lift the riser from the system board. Remove the PERC H365i Adapter card from the system.
5. Disconnect the SAS cables from the card:
   a. Press down and hold the metal tab on the SAS cable connector.
   b. Pull the SAS cable out of the connector.
6. Replace the storage controller and reconnect the SAS cable before inserting them into the riser.
7. Reinstall the riser on the system board and fasten the riser.
8. Install the system cover.
9. Reconnect the system to its electrical outlet and turn the system on, including any attached peripherals.

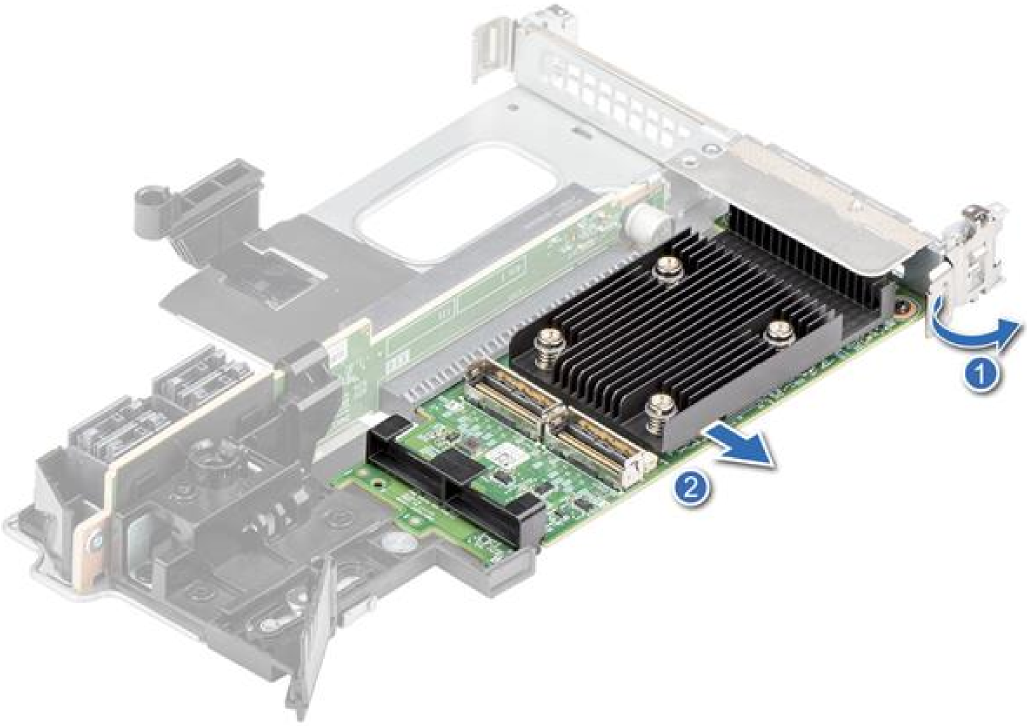


Figure 5. Remove the PERC H365i Adapter

Install the PERC H365i Adapter

Prerequisites

- You have read and complied with the safety guidelines that are listed in Safety instructions.
- You have completed the procedures in Before working inside your system.

Steps

1. Power off the system, including any attached peripherals, and disconnect the system from the electrical outlet.

   ⓘ **NOTE:** It is recommended that you always use a static mat and anti-static wrist strap while working on components inside the system.

2. Remove the system cover.
3. Connect the SAS data cable connectors to the card.

   ⓘ **NOTE:** Ensure that you connect the cable according to the connector labels on the cable. The cable does not function properly if reversed.

4. Align the card-edge connector with the connector on the system board.

   ⚠ **CAUTION: To prevent damage to the card, hold the card by its edges only.**

5. Press the card-edge down until the card is fully seated.
6. Route the SAS cable through the channel on the inner side of the chassis to the backplane.

7. Attach the connector that is labeled SAS A to connector SAS A on the backplane, and attach the connector that is labeled SAS B to connector SAS B on the backplane.
8. Install the system cover.
9. Reconnect the system to its electrical outlet and turn the system on, including any attached peripherals.

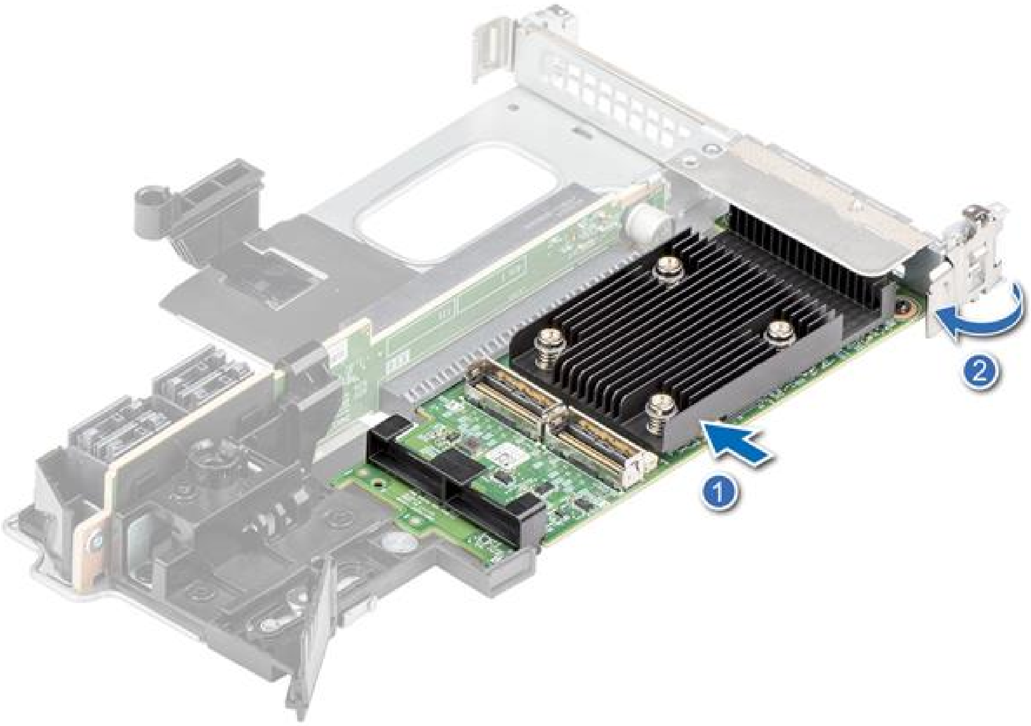


Figure 6. Install the PERC H365i Adapter

5

Driver support for PERC H365i Adapter and PERC H365i Front DC-MHS controller cards

The PERC H365i Adapter and PERC H365i Front DC-MHS cards require software drivers to operate with the supported operating systems.

This chapter contains the procedures for installing the drivers for the H365 series controller cards. The two methods for installing a driver that is discussed in this chapter are:

- **Installing a driver during operating system installation**: Use this method if you are performing a new installation of the operating system and want to include the drivers.
- **Updating existing drivers**: Use this method if the operating system and the RAID controllers are already installed and you want to update to the latest drivers.

ⓘ **NOTE:** It is recommended to download the latest Out-of-Box (OoB) drivers from the Dell Support site because the Inbox drivers in the operating system may not contain the full functionality and the latest fixes.

Topics:

Creating the device driver media

Use one of the following two methods to create the device driver media:

- Download and save PERC H365i Adapter and PERC H365i Front DC-MHS drivers from the support site
- Download and save PERC H365i Adapter and PERC H365i Front DC-MHS drivers from the Dell Systems Service and Diagnostic Tools

Download and save PERC H365i Adapter and PERC H365i Front DC-MHS drivers from the support site

Download the latest Out-Of-Box (OOB) drivers from the Dell Support site because the Inbox drivers in the operating system may not contain the full functionality and the latest fixes.

About this task

To download drivers from the Dell Support website, do the following:

Steps

1. Go to the support site.
2. Enter the Service Tag of your system in the **Choose by Service Tag to get started** box or select **Choose from a list of all Dell products**.
3. Select the system type, operating system, and the SAS RAID category from the drop-down menu.
   The drivers that are applicable to your selection are displayed.
4. Download the required drivers to a USB drive, CD, or DVD.
5. When installing an operating system, use the media that you created to load the driver. For more information about reinstalling the operating system, see the operating system documentation at Operating System Documentation.

Download and save PERC H365i Adapter and PERC H365i Front DC-MHS drivers from the Dell Systems Service and Diagnostic Tools

About this task

To download drivers from the **Dell Systems Service and Diagnostic Tools** media:

Steps

1. Insert the **Dell Systems Service and Diagnostics Tools** media in your system.
   The **Welcome to Dell Service and Diagnostic Utilities** screen is displayed.
2. Select your system model and operating system.
3. Click **Continue**.
4. From the list of drivers displayed, select the driver that you require .
5. Select the self-extracting ZIP file and click **Run**.
6. Copy the driver to a CD, DVD, or USB drive.
7. Repeat steps 1 to 6 for all the drivers that you require.

Windows driver installation

Before you install the Windows driver for PERC H365i Adapter and PERC H365i Front DC-MHS, you must first create a device driver media.

- Read the Microsoft **Getting Started** document that shipped with your operating system.
- Ensure that your system has the latest BIOS, firmware, and driver updates. If required, download the latest BIOS, firmware, and driver updates from the support site.
- Create a device driver media using one of the following methods:
  - USB drive
  - CD
  - DVD

Install PERC H365 series card driver during a Windows Server 2025 installation

About this task

To install the driver:

Steps

1. Start the system using the Windows Server 2025 media.
2. Follow the on-screen instructions until you reach **Where do you want to install Windows Server 2025** window, and then select **Load driver**.
3. When prompted to insert the media, insert the installation media and browse to the appropriate location.
4. Select **Controller** from the list.
5. Click **Next** and continue the installation process.

Install PERC H365i Adapter and PERC H365i Front DC-MHS while newly installing Windows

About this task

To install the driver:

Steps

1. Boot the system using Windows or newer media.
2. Follow the on-screen instructions to go to the **Where do you want to install Windows** window, and then select **Load driver**.
3. When prompted, insert the installation media and browse to the appropriate location.
4. Select the driver files.
5. Click **Next** and continue installation.

Install PERC H365i Adapter and PERC H365i Front DC-MHS driver on which Windows is already installed

About this task

Perform the following steps to configure the driver for the controller on which Windows is already installed:

Steps

1. Power off the system.
2. Install the new SAS controller in the system.

   For instructions on installing the controller in the system, see Install and remove a PERC12 card.
3. Power on the system.
   The **Found New Hardware Wizard** screen displays the detected hardware device.
4. Click **Next**.
5. On the **Locate device driver** screen, select **Search for a suitable driver for my device** and click **Next**.
6. Browse and select the drivers on the e **Locate Driver Files** screen.
7. Click **Next**.
8. Click **Finish**.
9. Reboot the system when prompted.

Update PERC H365i Adapter and PERC H365i Front DC-MHS driver that runs on the Microsoft Windows operating system

Prerequisites

ⓘ **NOTE:** Close all applications on your system before you update the driver.

Steps

1. Insert the media containing the driver.
2. Select **Start** > **Settings** > **Control Panel** > **System**.
   The **System Properties** screen is displayed.

   ⓘ **NOTE:** The path to **System** may vary based on the operating system family.
3. Click the **Hardware** tab.
4. Click **Device Manager**.
   The **Device Manager** screen is displayed.

   ⓘ **NOTE:** The path to **Device Manager** may vary based on the operating system family.
5. Expand **Storage Controllers** by double-clicking the entry or by clicking the plus (+) symbol next to **Storage Controllers**.
6. Double-click the controller for which you want to update the driver.
7. Click the **Driver** tab and click **Update Driver**.
   The screen to update the device driver wizard is displayed.

8. Select **Install from a list or specific location**.
9. Click **Next**.
10. Follow the steps in the wizard and browse to the location of the driver files.
11. Select the INF file from the drive media.
12. Click **Next** and continue the installation steps in the wizard.
13. Click **Finish** to exit the wizard and reboot the system for the changes to become effective.

    ⓘ **NOTE:** Dell provides the Dell Update Package (DUP) to update drivers on systems running RHEL 8 or RHEL 9. DUP is an executable application that updates drivers for specific devices. DUP supports CLI and silent execution.

Linux driver installation

The Driver Update Disk (DUD) image files are created only for those operating system releases in which the native (in-box) driver is insufficient for installation. If an operating system is being installed with a corresponding DUD image file, see Load the driver while installing an operating system. If not, use the native device driver and then:

- For RHEL 8 and RHEL 9: Install or update a RPM driver package using the KMOD support.
- For SLES15 SP5: Install or update a RPM driver package using the KMP support.

.

ⓘ **NOTE:** To view the complete list of boot loader options, see the installation guide of your operating system.

Install or update a RPM driver package using the KMOD support

Prerequisites

ⓘ **NOTE:** This procedure is applicable for RHEL 8.0 and later versions.

About this task

To install the RPM package with KMOD support, do the following:

Steps

1. Expand tarball driver release package.
2. Install the driver package by running the command: `rpm -ihv kmod-mpi3mr-<version>.rpm`.

    ⓘ **NOTE:** Use `rpm -Uvh <package name>` when upgrading an existing package.

3. If the previous device driver is in use, you must restart the system for the updated driver to take effect.
4. Verify the loaded driver version by running the following command: `modinfo mpi3mr`.

Install or update a RPM driver package using the KMP support

Prerequisites

ⓘ **NOTE:** This procedure is applicable for SUSE Enterprise Linux 15.x.

About this task

To install the RPM package with KMP support, do the following:

Steps

1. Expand the tarball driver release package.
2. Install the driver package by running the commands: `rpm -ivh broadcom-mpi3mr-kmp-<version>.rpm`

ⓘ **NOTE:** Use `rpm -Uvh broadcom-mpi3mr-kmp-<version>.rpm` to update an existing package.

3. If the previous device driver is in use, you must restart the system for the updated driver to take effect.
4. Verify the loaded driver version by running the following command: `modinfo mpi3mr`.

Load the driver while installing an operating system

About this task

ⓘ **NOTE:** Steps provided are general steps for the Linux based operating systems. For exact information about loading drivers while installing operating systems, see the Dell technical documentation of the operating system on the Dell support site or the official support of the operation system vendor.

Steps

1. Perform the following operation to install the driver media:
    a. Download the PERC Linux driver ISO image file from the Dell Support Site, or install the Lifecycle Controller driver pack.
    b. Mount the ISO file to the server, burn the ISO to CD/DVD, or copy the ISO image file to USB. The USB has to match with the ISO file.
    c. For Lifecycle Controller driver pack, boot the Lifecycle Controller and complete the tasks prompted by the operating system deployment wizard.
2. Boot to the installer.
3. On the Bootloader screen, select **E** and press Enter.
4. Do one of the following:
    - If the operating system is RHEL, the CLI displays the syntax `vmlinuz`. Enter **inst.dd**.

      For example, when you are prompted with the command `vmlinuz intrd=initrd.img inst.stage2=hd:LABEL=RHEL-7.0\x20x86_64 quiet inst.dd`.
    - If the operating system is SLES, the CLI displays the syntax `linuxefi..` Enter **dud=1**.

      For example, when you are prompted with the command `linuxefi/boot/x86_64/loader/linux splash=silent dud=1`.

    ⓘ **NOTE:** Boot parameters may vary based on the operating system version. See operating system installation manuals for exact boot parameter syntax.
5. Attach the driver media (ISO, USB).
6. Press F10 to boot to the operating system.
7. Wait for the OS image file to boot and OS installer to begin. When prompted, select the driver media (for example, USB, CD, or an ISO image file).
8. When prompted, select the driver media.
    If applicable, select the PERC driver `mpi3mr`.

    ⓘ **NOTE:** Ensure that the selected driver is indicated bt an **X** symbol.
9. Extract or load the driver.
10. Before proceeding or closing the **Driver Select** menu, disconnect the driver media.

    ⓘ **NOTE:** Ensure that you disconnect the driver media so that the drivers are loaded successfully. If the installation media is deleted, reattach it.
11. Press C or select **Exit** to go to the installation.

6

Manage the PERC12 firmware

This section provides information about downloading, installing, and upgrading the PERC12 firmware using the Dell Update Package (DUP). The 17G PowerEdge servers support only PERC365 versions 8.11.0.0.15-22 and later. You cannot downgrade to an earlier version of PERC365 on 17G servers.

NOTE: The PCIe Switch-based configuration support is available in firmware 8.4.0.0.18-27 and later versions.

Topics:

- Upgrade firmware controller using Dell Update Package (DUP)

Upgrade firmware controller using Dell Update Package (DUP)

About this task

NOTE: If the Online Capacity Expansion operation is in progress then you cannot update the firmware version.

Steps

1. Go to the Drivers and Downloads page on the support site.
2. Locate your controller.
3. Download the DUP file.
    a. To upgrade by using Windows or iDRAC, download the Windows executable file.
    b. To upgrade using Linux, download the **.bin** file.

    NOTE: For VMware, firmware must be upgraded by using iDRAC or the PERC CLI.
4. Install the DUP by doing one of the following:
    a. For Windows, run the executable file in the Windows environment.
    b. For Linux, run the **.bin** file in the Linux environment.
    c. For iDRAC, click **System iDRAC** > **Maintenance** > **System Update**, upload Windows executable, and then install.

7

Manage PERC12 controllers using HII Configuration Utility

The Human Interface Infrastructure (HII) configuration utility is a storage management application integrated into the System BIOS <F2>. It is used to configure and manage the controller(s), virtual disks, and physical disks. This utility is independent of the operating system.

Topics:

Enter the PERC12 HII Configuration Utility

About this task

Perform the following steps to boot to the HII Configuration Utility:

Steps

1. Power on the server.
2. When the server starts, press F2 to open the **System Setup** page.
3. Click **Device Settings**.
   The **Device Settings** page lists all the RAID controllers in the system.

   To access the management menu of the controller, use the arrow keys or the mouse device.

   ⓘ **NOTE:** For more information about each option, click Help in the upper-right corner. For information about individual options pause the pointer over each link and view the description in the bottom pane.

   ⓘ **NOTE:** Some of the options within the HII Configuration Utility are not present if the controller does not support the corresponding feature. Options may also be grayed out if the feature is not applicable to the current configuration.

Exit the PERC12 HII Configuration Utility

About this task

To exit the HII Configuration Utility, do the following:

Steps

1. Click **Finish** at the bottom-right corner on the **System Setup Main Menu** page.
2. When prompted to confirm if you want to perform the operation, click **Yes**.

Navigate to the PERC12 Configuration Utility

Steps

1. Enter the UEFI configuration Utility. See Enter the PERC12 HII Configuration Utility.
   The **Device Settings** screen displays a list of NIC ports and the RAID controllers.
2. To enter PERC12 configuration utility, click the appropriate PERC controllers.
   The **Dashboard view** screen is displayed.

View the HII Configuration Utility dashboard

The following table lists the features that are displayed in the Dashboard View page of the HII Configuration Utility:

Table 7. Dashboard view screen

Dashboard view options	Description
Main menu	Displays the following configuration options: ● **Configuration Management** ● **Controller Management** ● **Virtual Disk Management** ● **Device Management**
Help	Press F1 to view context-sensitive Help information.
Configuration Management	Displays the following options under **Configuration Management**: ● **Create Virtual Disk**—Creates a virtual disk by selecting RAID level, hard drives, and virtual disk parameters. ● **Create Profile Based Virtual Disk**—Creates a virtual disk by using a wizard. This wizard makes intelligent choices based on the profile that you selected. ● **View Disk Group Properties**—Displays associated virtual disks for the disk group and any available free capacity. ● **View Global Hot Spares**—Displays the drives that are assigned as global hot spare devices. ● **Convert to Non-RAID disk**—Allows changing the state of the RAID capable disks to Non-RAID disks. ● **Clear Configuration**—Deletes all existing configurations on the RAID controller. ● **Convert to RAID Capabale**—Allows changing the state of the hard drive from Non-RAID to RAID capable. ● **Convert to Secure Non-RAID Disk**—Allows changing the state of the RAID capable drives to secure non-RAID disks.
Controller Management	Displays controller status and basic properties of the controller: ● **Advanced Controller Management**—Provides to links to various controller management activities. ● **Advanced Controller Properties**—Displays memory-related properties.
Virtual Disk Management	Displays the properties of a specific virtual disk. You can perform operations such as Initialization and Check Consistency. You can perform operations such as Initialization, Consistency Check, Delete Virtual Disk, and Secure Virtual Disk.
Device Management	Displays logical enclosure details and the hard drives that are attached to it.

Configuration management

Create virtual disk and configure virtual disk parameters

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Configuration Management** > **Create Virtual Disk**.
3. Select the RAID level. You can select PDs from either unconfigured capacity or free capacity.
   The list of hard drives appear.
4. Click **Select Physical Disks**. See Select physical disks for creating VDs.
5. Select the hard drives for the selected RAID level and click **OK**.
6. Click **Confirm** and click **Yes**.
7. Click **OK**. The **CONFIGURE VIRTUAL DISK PARAMETERS** section is displayed.

   ⓘ **NOTE:** Mixing of TCG Enterprise and TCG Opal SED protocols in a virtual disk is not supported.

   Table 8. Virtual disk parameters and their descriptions

Virtual disk parameters	Description
Virtual Disk Name	Enter the name of the virtual disk.
Virtual Disk Size	Displays the maximum capacity available for the virtual disk.
Virtual Disk Size Unit	Displays the virtual disk storage space either in GiB or TiB.
Strip Element Size	Select the strip element size. The disk striping involves partitioning each hard drive storage space in stripes of the sizes 64 KiB and 256 KiB.
Read Cache Policy	Displays the controller read policy. By default, the read cache policy is set to **No Read-Ahead**.
Write Cache Policy	Displays the controller write cache policy. You can set the write policy to: ● **Write-Through**—The controller sends a data transfer completion signal to the host when the disk subsystem has received all the data in a transaction. By default, the **Write Cache Policy** is set to **Write-Through**.
Disk Write Cache Policy	Select the disk cache policy to **Default**, **Enable**, or **Disable**. By default, the **Disk Write Cache Policy** is set to **Default**.
Default Initialization	Select the default initialization to: ● **No** —Virtual disk is not initialized. ● **Fast**—The first and last 8 MB of the virtual disk is initialized. ● **Full**—Entire virtual disk is initialized. For more information, see Virtual disk initialization. By default, the default initialization is set to No.

8. Click **Create virtual disk**.
9. Click **Confirm** and click **Yes**. The virtual disk is created.

Select physical disks for creating VDs

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Configuration Management** > **Create Virtual Disk**.
3. Click **Select Physical Disks**.
4. Select the media type. For example, SSD, HDD, or both. Based on your selection, the drives are displayed for creating RAID drives.

5. Select the interface type. For example, SAS, SATA, or NVMe.
6. Select the logical sector size. For example, 512B, 4KiB, or both.

Create a profile based virtual disk

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Configuration Management** > **Creating Profile Based Virtual Disk**.
   The following list of RAID modes are displayed:
   - **Generic RAID 0**
   - **Generic RAID 1**
   - **Generic RAID 10**
   - **File Server**
   - **Web/Generic Server**
   - **Database**

   Based on the RAID mode selected, one or more the hard drive selection criteria are displayed.
3. From the **Physical Disk Selection Criteria** drop-down menu, select a criterion based on your requirement.
   The Profile Parameters of the selected option is displayed.

   NOTE: Based on the physical disk selection criteria, if enough disks are not available to satisfy the applicable RAID level, then the **Physical Disk Selection Criteria** option is disabled.

   NOTE: Before using drives for profile-based VD creation, ensure that the drives are securely erased. When selecting a drive, ensure that you do not mix:
   - Hard drive and SSDs.
   - NVMe, SAS, and SATA types.
   - Drives that support only Physical Region Page (PRP) and that support both PRP and Scatter Gather List (SGL).
   - 512b and 4K block-size drives.
   - Drives of different link speeds such as 3G, 6G, 12G, and 24G, or 2.5GT, 5.0GT, 8.0GT, 16.0GT, or 32.0GT.
   - Drives of SED and non-SED types.
   - SEDs are not secured.
   - Drives of single and multiple LUN types.
4. Click **Create Virtual Disk**.
5. Select **Confirm** and click **Yes** to continue.
   The virtual disk is created with the parameters of the profile selected.

View disk group properties

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Configuration Management** > **View Disk Group Properties**.
   The list of disk group properties are displayed:

Table 9. disk group properties

Properties	Descriptions
Capacity Allocation	Displays all the virtual disks that are associated with the specific disk group. It also provides information about the available free disk space.
Secured	Displays whether the disk group is secured or not.

View global hot spare devices

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Configuration Management** > **View Global Hot-Spares**.
   The list of PDs that are allocated as global hot-spares is displayed.

Convert a hard drive to a non–RAID drive

To convert a hard drive to a a non–RAID disk from the HII Configuration Utility, perform the following steps:

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Device Management** > **Logical Enclosure <enclosure Number>**. An enclosure number can be 0, 1, 2, 3, 4, and so on.
   All the hard drives associated with the selected enclosure are listed.
3. Select the hard drive.
4. From the **Operations** list, select **Convert to non-RAID Capable**.
5. Click **Go**.
6. When prompted to indicate if you want to covert the selected PDs to non-RAID types, select the **Confirm** check box, and then click **Yes**.
   The PDs are converted to non-RAID PDs.

Convert a hard drive to a RAID capable drive

To convert a hard drive to a non–RAID disk from the HII Configuration Utility, perform the following steps:

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Device Management** > **Logical Enclosure <enclosure Number>**. An enclosure number can be 0, 1, 2, 3, 4, and so on.
   All the hard drives that are associated with the selected enclosure are listed.
3. Select the hard drive.
4. From the **Operations** list, select **Convert to RAID Capable**.
5. Click **Go**.
6. When prompted to indicate if you want to covert the selected PDs to RAID types, select the **Confirm** check box, and then click **Yes**.
   The hard drives are converted to a RAID capable drive.

Delete configurations

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Configuration Management** > **Clear Configuration**.
3. △ **CAUTION: It is recommended that you back up data that is stored on the virtual disks and hot spare disks on the controller before deleting the virtual drive.**

   When prompted to indicate if you want to delete VDs and hot-spares, select the **Confirm** check box, and then click **Yes**.
   The virtual disks and hot spare disks available on the controller are deleted successfully.

Advanced controller management

Save persistent events

To save persistent events, you must have a USB or file system on the server.

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management**.
3. Enter the filename and select events to save. Click **Save Persistent Events**.
4. When prompted to indicate if you want to save persistent events, click **OK**.

Clear persistent events

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management**.
3. Click **Clear Persistent Events**.
4. Click **OK**.

Manage snapdump

Prerequisites

To save the snapdump, you must have a USB or a file system that is attached to the server before starting the server. For information about the Snapdump feature, see Snapdump.

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management**.
3. Click **Manage Snapdump**.
4. In the OPERATIONS section, select a file system and its corresponding directory. To save the Snapdump data of the selected file, click **Save new On-Demand Snapdump**. To delete the Snapdump data, click **Clear All Snapdumps**.
5. Click **OK**.

Enable security

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management**.
3. Click **Enable security**, select **Local Key Management**.
4. Click **Ok**.
5. If you want to use the security key generated by the controller, click **Suggest Security Key** and **OK**.
   The operation is successful.
6. Enter the key in the **Security Key** and **Confirm** boxes.
7. Select the **I Recorded the Security Settings For Future Reference** check box and click **Enable Security**.
8. Select **Confirm** and click **Yes**.
9. Click **OK**.
   The operation is successful.

Disable security

You can disable the LKM security feature by using the HII.

About this task

ⓘ **NOTE:** Before disabling the drive security feature, ensure that all secured drives are are either erased or removed.

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management**.
3. Click **Disable security**.
4. When prompted if you want to disable security, click **Confirm**, and then click **Yes**.

Change security settings

Steps

1. Enter the PERC12 HII Configuration Utility
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management**.
3. Click **Change Security Settings**, select **Change Current Security Settings**.
4. Click **Ok**.
5. If you want to use the security key generated by the controller, click **Suggest Security Key** and confirm the security key by re-entering.
   The operation is successful.
6. Click **Save Security Settings**.
7. Select **Confirm** and click **Yes**.
8. Click **Ok**.

Restore factory default settings

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management** > **Set Factory Defaults**.
3. Select **Confirm** and click **Yes**.

Manage the SAS Storage link speed

About this task

To change the storage link speed of the eligible SAS/SATA disks, do the following:

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management** > **Manage SAS Storage Link Speed**.
3. To change the link speed, select the appropriate options for each link, and then click **Apply Changes**.
4. Click **OK**.

Manage the PCIe storage interface

About this task

To change the storage interface of the eligible NVMe disks, do the following:

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management** > **Manage PCIe Storage Interface**.
3. To change the link speed, click **View/Change Link Speed** and select the appropriate options for each port, and then click **Apply Changes**.
4. Select the **Confirm** check box and click **Yes**.
5. Click **OK**.

   ⓘ **NOTE:** Physical drive slot numbers do not correlate with the controller PHY numbers. The hard drive slot numbers that are displayed on the HII may not be the same slot numbers in which the drives are installed.

Auto-Configure Behavior Management

About this task

To change the Auto-Configured Behavior of the eligible disks, do the following:

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management** > **Manage Controller Personality**.
3. To change the Auto-Configured behavior (Primary or Secondary or both) on all the new disks that will be inserted, select the appropriate options for **Auto-Configure Behavior (Primary)** and **Auto-Configure Behavior (Secondary)**, and then click **Apply Changes**.
4. To run immediate one-time Auto-Configure operation, select the **Auto-Configure Behavior (Execute Once)** option, and then click **Apply Now**.

Advanced controller properties

Set the patrol read mode

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. Click **Patrol Read**.
   The following options are displayed:
   - Start—Starts patrol-read for the selected controller.
   - Suspend—Suspends the ongoing patrol-read operation on the controller.
   - Resume—Resumes the suspended patrol-read operation.
   - Stop—Stops patrol-read for the selected controller.
   - Rate—Indicates the percentage of system resources that are dedicated to perform the patrol-read operation.
   - State—Displays the current state of the patrol operation.
   - Iterations Completed—Indicates that the number of patrol-read iterations completed .
4. To enable or disable patrol-read and to correct unconfigured areas on the hard drive, click **Correct Unconfigured Areas**.
5. Click **Apply Changes**.

Configure hot spare drives

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. Click **Spare**.
   The following options are displayed:
   - **Replace Member**—Enables or disables the option to replace the member.
   - **Auto Replace Member on HDD Predictive Failure**—Enables or disables the option to start a Replace Member operation if a predictive failure error is detected on a PD.
   - **Auto Replace Member on SSD Predictive Failure**—Enables or disables the option to start a Replace Member operation if a predictive failure error is detected on an SSD.
4. Select the applicable option and click **Apply Changes**.
   The changes are saved successfully.

Set task rates

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. Click **Task Rates**.
   The following options are displayed:
   - **Background Initialization (BGI) Rate**
   - **Patrol Read Rate**
   - **Consistency Check Rate**
   - **Rebuild Operating Mode Priority**: Available in 8.8.0.0.18-26 and later versions of PERC12 controllers.
     - Rebuild—The rebuild operation is given priority over the host system's IOPS.
     - Host I/O—The host Input/Output operations are given priority over the rebuild operation.
4. You can make the necessary changes and then **Apply Changes**.
   The task rates operation is completed successfully.

Controller properties

Set a drive as the first device to OS

About this task

The First Device feature is available only on Linux based servers. Using the First Device feature, you can select the order in which the PD or VD must be presented to the OS. You can also select the PD or VD on which you can install the OS Do the following:

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. In the **Controller Properties** section, from the **First Device** drop-down menu, select the PD or VD that must be set as the first device.
4. Click **Apply Changes**.
   The selected Physical Device or Virtual Drive is set as the first device.

Device reporting order

About this task

The Device Reporting Order feature is available only on Linux-based servers. Enables you select the order in which either non-RAID drives or VDs must be listed first to the operating system. Do the following:

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. In the **Controller Properties** section, from the **Device Reportig Order** drop-down menu, select to either first present a non-RAID drive or VD to the operating system.
4. Click **Apply Changes**.
   The devices are presented to the operating system based on the order you selected.

Manage the write-cache feature of NVMe devices

About this task

To enable the write-cache feature on NVMe devices, do the following:

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. In the **Controller Properties** section, set the **Write Cache for NVMe Devices** feature to Enabled, Disabled, or Default.
4. Click **Apply Changes**.
   The write-cache policy of NVMe devices is updated.

Manage the write-cache feature of SATA devices

About this task

To enable the write-cache feature on SATA devices, do the following:

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. In the **Controller Properties** section, set the **Write Cache for SATA Devices** feature to Enabled, Disabled, or Default.
4. Click **Apply Changes**.
   The write-cache policy of SATA devices is updated.

Select boot mode

About this task

To select the boot mode, perform the following steps:

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. In the **Controller Properties** section, select either **Continue on Errors** or **Safe Mode on Errors** from the **Boot Mode** list.

   ⓘ **NOTE:** By default, the boot mode option is set to **Continue on Errors**.

Table 10. Boot mode options

Option	Description
Continue on Errors	The controller attempts to automatically clear errors and continue booting. Errors can result in safe mode if the controller is unable to clear them.
Safe Mode on Errors	The controller is routed to safe mode when critical errors arise. PERC firmware disables most of the features on the controller. The controller requires attention from the user to acknowledge and rectify the issues.

4. Click **Apply Changes**.
   The boot mode operation is completed successfully.

Abort the consistency check

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Properties**.
3. In the **Controller Properties** section, set the **Abort Consistency Check on Error** option to **Enabled** or **Disabled**.
4. Click **Apply Changes**.
   The option to abort the consistency check operation on a redundant virtual disk is enabled if there is any inconsistency found in the data.

Virtual disk management

Virtual disk numbering

Virtual disks are numbered in ascending order beginning from the lowest, which is ID 1.

View virtual disk properties

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Virtual Disk Management**.
   All the virtual disks that are associated with the RAID controller are displayed.
3. To view the properties, click the virtual disk. You can view the following properties of the virtual disk:

Table 11. Virtual disk properties

Option	Description
Operation	Select one of the following: ● **Delete Virtual Disk**: Deletes the selected VDs. ● Fast Initialization ● Full Initialization: See Full initialization. ● Consistency Check (available for all RAID levels except for RAID 0 VD). See Check consistency of VDs. ● Expand Virtual Disk
Name	Indicates the name of the virtual disk.
RAID level	Indicates the RAID level of the virtual disk.
Status	Indicates the status of the virtual disk. The possible options are: ● Ready ● Degraded

Table 11. Virtual disk properties (continued)

Option	Description
	- Offline - Failed
Size	Indicates the size of the virtual disk.
Disk Group	Indicates the disk group of the virtual drive.

Configure virtual disk policies

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Virtual Disk Management**.
   All the virtual disks that are associated with the RAID controller are displayed.
3. Select the virtual disk.
4. Click **Advanced**.
   You can view the following virtual disk policies:

Table 12. Virtual disk policies

Option	Description
Current Cache Status	Indicates the current read and write cache policies for the virtual disk.
Access Policy	Indicates the current access policy for the virtual disk.
Default Read Cache Policy	Allows selection of the read cache policy for the virtual disk. The available option is Write-Through.
Current Power Save Policy	Indicates the current power saving policy of the VD.
Default Write Cache Policy	Allows selection of the write cache policy for the virtual disk. The available options are: **Write Through**.
Disk Write Cache Policy	Allows selection of the **Disk Write Cache Policy** for the virtual disk. The possible options are: - Default (Disk Default) - Enable - Disable

5. Click **Apply Changes**.
   The changes that are made are saved successfully.

View advanced properties of a virtual disk

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Virtual Disk Management**.
   All the virtual disks that are associated with the RAID controller are displayed.
3. Click the virtual disk.
   The properties of the virtual disk are displayed.
4. Click **Advanced**.
   You can view the following additional properties of the virtual disk:

Table 13. Advanced properties of the virtual disk

Option	Description
Strip element size	Indicates the strip element size for the virtual disk.

Table 13. Advanced properties of the virtual disk (continued)

Option	Description
Secured	Indicates whether the virtual disk is secured or not.
Bad blocks	Indicates whether the virtual disk has corrupted blocks.
Data format for I/O	Indicates the data format for I/O operations (only available for NVMe drives)

View physical disks associated with a virtual disk

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Virtual Disk Management**.
   All the virtual disks associated with the RAID controller are displayed.
3. Click on a virtual disk.
   The properties of the virtual disk are displayed.
4. Click **View Associated Physical Disks**.
   All the physical disks that are associated with the virtual disk are displayed.
5. From the **Associated Physical Disks** section, select the physical disk.
6. Click **View Physical Disk Properties** to view the physical disk properties.

Configure Virtual Disks

When configuring the virtual disks, you should consider the workload intended. For example, RAID 1 for a simple boot disk or RAID 10 for transactional database (small random-read and random-write operations). Virtual disks that are configured on hard drives should use the cache settings or write-through feature.

Virtual disks that are configured on SSDs can use the same controller default settings as used by hard drives. Most users copy data of operating system files or database to the new array. Using such default settings provide optimum performance in this configuration. After copying, the array can be used as-is based on the number and type of SSDs.

Check consistency of VDs

Prerequisites

To enable consistency check from the HII Configuration Utility, do the following:

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Virtual Disk Management**.
   The list of virtual disks is displayed.
3. Select the virtual disk.

   NOTE: Consistency check cannot be run on RAID 0 virtual disks.

4. From the **Operations** list, select **Check Consistency**.
5. Click **Go**.
6. When prompted to indicate if you want to start the checking operation, select the **Confirm** check box, and then click **Yes**.

Device management

View enclosure or backplane properties

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Device Management** > **Logical Enclosure <enclosure number>**. An enclosure number can be 0, 1, 2, 3, 4, and so on.
   All the hard drives that are associated with the selected enclosure are listed.

   ⓘ **NOTE:** Fields associated with properties that are not applicable are hidden.

Table 14. Enclosure or backplane properties

Option	Description
Enclosure ID	Displays the persistent ID of the enclosure.
Bay ID	Displays the Bay ID of the enclosure.
Name	Displays the name of the enclosure.
Connector name	Indicates the type of physical connection to the enclosure. All connectors for internal controllers are identified by "00".
State	Displays the state of the enclosure.
Vendor ID	Displays the vendor ID of the enclosure.
Product ID	Displays the product ID of the enclosure.
Location	Displays the location of the enclosure. Location is either internal or external.
Type	Displays the type of the enclosure. The types of enclosures are **Virtual SES**, **SAS Expander**, and **Managed PCIe Switch**.
Product Revision Level	Displays the product revision level of the enclosure.
Number of Slots	Displays the number of slots in the enclosure.
Number of Physical Disks	Indicates the number of PDs installed on the enclosure.

ⓘ **NOTE:** "Partner" refers to the devices that have multiple paths to communicate for redundancy and load balancing.

ⓘ **NOTE:** The Partner entries are displayed only for backplane devices in multipath. Else, it will not be displayed.

View hard drive properties

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Device Management** > **Logical Enclosure <enclosure number>**. An enclosure number can be 0, 1, 2, 3, 4, and so on.
   The enclosure properties and all the hard drives that are associated with the selected enclosure are listed.
3. To view the properties of a PD, click the corresponding PD link.

   ⓘ **NOTE:** Fields associated with features that are not applicable are hidden.

Table 15. Physical disk Dashboard View

Option	Description
Operation	The list of operations you can perform on the selected hard drive. The options are: ● Blink ● Unblink ● Assign global hot spare. ● Cryptographic erase ● Convert to non–RAID disk. ● Make Offline ● Replace Member ● Cryptographic Erase with PSID convert ● Prepare for removal ● Start/Spin-up
Connection	Displays the connection status of the hard drive.
Slot number	The PD slot to which the controller is connected.
Persistent ID	Persistent ID of the hard drive.
Status	Status of the hard drive.
Size	Size of the hard drive.
Type	Type of the hard drive.
Model	Model of the hard drive.
Part Number	Part number of the hard drive.
Serial Number	Serial of the hard drive.
Vendor	Name of the PD manufacturer.
Firmware Revision Level	Indicates the version of the firmware that is installed on the PD.
Manufacturing Date	Date of manufacture of the PD.
Associated Virtual Disk	Indicates the VD that is associated with this PD.

4. To view additional properties of the hard drive, click **Advanced**.

Table 16. Advanced hard drive properties

Option	Description
SMART status	SMART status of a physical disk
SAS Address/WWID	WWN number of the device.
Disk Power state	Power condition (On or Power Save) of the hard drive
Interface	Indicates the type of device that is used as an interface. For example, SAS or parallel SCSI.
Capable Speed	Indicates the read/write speed capability of PD in Gbps.
Negotiated Speed	Negotiated link speed of the device.
Capable Link Width	Capable link width of the device.
Negotiated Link Width	Negotiated link width of the device.
Number of Connections	Indicates that the number of paths do the PD.
Cryptographic erase capable.	Cryptographic erase capability of the hard drive.
Encryption Capable	Indicates whether the drive can be encrypted.
Supported Data Format	Indicated for NVMe drives only.

Table 16. Advanced hard drive properties (continued)

Option	Description
ATA Security Enabled	Indicates whether the ATA Security features are enabled on the hard drive.
Media format corrupted	Indicates whether the hard drive media format is corrupted.
Temperature (C)	Indicates the current temperature of the PD.
Unmap Capabality	Indicates whether the hard drive is unmap capable.
Write Same-Unmap Capability	Indicates whether the hard drive is Write Same-Unmap capable.

5. To view information about the Logical Unit Number (LUN) and NVMe namespace properties of a PD, click **Logical Unit/ Namespace Information**.

Table 17. LUN/Namespace data of a hard drive

Option	Description
NVMe Namespace ID	Indicates LUN and Namespace properties.
Status	Indicates the working status of a LUN.
Size	Indicates the maximum storage size of the LUN.
Total Unconfigured Space	Total free space available for RAID array.
Total Configured Space	Total used drive space for RAID array.
Logical Sector Size	Supports either 512B or 4KiB types.
Physical Sector Size	Supports either 512B or 4KiB types.
Media Error Count	Number of physical errors detected on the PD.
Other Error Count	Other errors are detected on the PD.
Predictive Failure Count	Predictive errors detected on the PD.
Firmware Managed Security	Indicates whether the PD security is managed by the controller firmware.
Current Write-Cache	Indicates whether the current write-cache mode of the PD is enabled.
Default Write-Cache	The default write-cache mode of the PD.
Secured	Indicates whether the PD is secured.
Locked	Indicates whether the PD is locked.

To view information about the next PD associated with the enclosure, click **New Physical Disk**.

Cryptographic erase

Cryptographic erase is a process to erase all data permanently on an encryption-capable and unconfigured physical disk, and reset the security attributes. Cryptographic erase on an Self Encrypting Drives (SED) will unsecure the disk.

Prerequisites

- The non-RAID and virtual disks associated with the drive are deleted.
- The disks are not dedicated as hot-spares.

About this task

The Cryptographic erase feature is supported only on Instant Secure Erase (ISE) and SEDs.

Steps

1. Enter the PERC12 HII Configuration Utility.

2. Click **Main Menu** > **Device Management** > **Logical Enclosure <enclosure Number>**. An enclosure number can be 0, 1, 2, 3, 4, and so on.
   All the physical disks associated with the selected enclosure are listed.
3. Select a physical disk.
4. From the **Operations** list, select **Cryptographic Erase**.

   ⓘ **NOTE:** The Cryptographic Erase option is displayed only if the drive installed is ISE or SED capable.

5. Click **Go**.
6. When prompted to indicate if you want to start the cryptographic erase operation, select the **Confirm** check box, and then click **Yes**.
   The cryptographic erase operation is successfully completed.

Cryptographic Erase with PSID Revert

This feature is available only in H365 series controllers. PSID erase is a process to erase all data permanently on an encryption-capable and unconfigured physical disk, and reset the security attributes. PSID erase on a Self Encrypting Drive (SED) will unsecure the disk.

Prerequisites

- The non-RAID drives associated with the drive are deleted.
- Remove the drive, note down the PSID printed on the drive so you can enter in the PSID field of HII, and then insert the drive back into the slot.

About this task

The PSID erase feature is supported only on SEDs.

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Device Management** > **Logical Enclosure <enclosure Number>**. An enclosure number can be 0, 1, 2, 3, 4, and so on.
   All the hard drives associated with the selected enclosure are listed.
3. Select a hard drive.
4. From the **Operations** list, select **Cryptographic Erase with PSID Revert**.

   ⓘ **NOTE:** The Cryptographic Erase with PSID Revert option is displayed only if the drive installed is SED capable.

5. Enter the PSID key of the drive.
6. Click **Go**.
7. When prompted to indicate if you want to start the erase operation, select the **Confirm** check box, and then click **Yes**.
   The Cryptographic Erase with PSID Revert operation is successfully completed.

Sanitize Block or Overwrite Erase operation

Sanitize secure erase is a process that a drive performs to erase all data permanently by modifying physical block to a user or vendor-specific value. Sanitize can be managed by the PERC or by an application running on the OS. See the Physical Disk Erase section in this guide.

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Device Management** > **Logical Enclosure <enclosure Number>**. An enclosure number can be 0, 1, 2, 3, 4, and so on.
   All the physical disks associated with the selected enclosure are listed.
3. Select a physical disk. Ensure that the drive is not configured.
4. From the **Operations** list, select the required Sanitize Erase operation.

ⓘ **NOTE:** The Cryptographic Erase option is displayed only if the drive installed is ISE or SED capable.

5. Click **Go**.
6. When prompted to indicate if you want to start the sanitize erase operation, select the **Confirm** check box, and then click **Yes**.
   The sanitize erase operation is successfully completed.

Assigning a global hot-spare

To assign a global hot spare from the HII Configuration Utility, do the following:

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Device Management** > **Logical Enclosure <enclosure Number>**. An enclosure number can be 0, 1, 2, 3, 4, and so on.
   All the physical disks associated with the selected enclosure are listed.
3. Select the physical disk.
4. From the **Operations** list, select **Assign Global Hot Spare**.
5. Click **Go**.
6. When prompted to indicate if you want to assign the selected PDs as hot-spares, select the **Confirm** check box, and then click **Yes**.
   The PDs are assigned as global hot-spare devices.

Convert to Non–RAID disk

To convert a physical disk to non–RAID disk using the HII Configuration Utility, do the following:

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Configuration Management** > **Convert to Non–RAID Disk**.
   A list of available PDs is displayed.
3. Select the physical disk to convert to Non-RAID disk.
4. Click **OK**.
5. Click **Confirm**.
6. Click **Yes**.
   The non-RAID disk is successfully created.

Convert a hard drive to a non–RAID drive

To convert a hard drive to a a non–RAID disk from the HII Configuration Utility, perform the following steps:

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Device Management** > **Logical Enclosure <enclosure Number>**. An enclosure number can be 0, 1, 2, 3, 4, and so on.
   All the hard drives associated with the selected enclosure are listed.
3. Select the hard drive.
4. From the **Operations** list, select **Convert to non-RAID Capable**.
5. Click **Go**.
6. When prompted to indicate if you want to covert the selected PDs to non-RAID types, select the **Confirm** check box, and then click **Yes**.
   The PDs are converted to non-RAID PDs.

Security key management in HII configuration utility

The HII Configuration Utility enables you to create and manage security keys and create secured virtual disks. The following section describes the menu options specific to security key management and provides instructions to perform the configuration tasks. The contents in the following section apply to the **HII Configuration Utility**.

- The **Controller Management** screen displays controller information and action menus. You can perform the following security-related actions through the controller management menu:
  - **Security Key Management**—Create, update, or delete a Local Key Management (LKM) security key.
- The **Virtual Disk Management** screen displays hard drive information and action menus. You can perform the following security-related actions through the virtual disk management menu:
  - **Secure Disk Group**—Secures all virtual disks in disk group.
  - **Create secure virtual disk**—Creates a new virtual disk that is secured with the security key on the controller.
- The **Device Management** > **Enclosure X** screen displays hard drive information and action menus. You can perform the following security-related actions through the hard drive management menu:
  - **Secure non–RAID disk**—Secures the non–RAID disk with the controller security key.
  - **Cryptographic Erase**—Permanently erases all data on the hard drive and resets the security attributes.

For more information about the Device Management screen and the Virtual Disk Management screen, see Device management and Virtual disk management.

8

Security key and RAID management

Topics:

Security key implementation

The PERC12 series of cards support Self-Encrypting Drives (SEDs) for protection of data against loss or theft of SEDs. Protection is achieved by the use of encryption technology on the drives. There is one security key per controller. It is recommended that you use the SEKM or iLKM feature to manage the security keys. The security key is used by the controller to lock and unlock access to encryption-capable hard drives. To use this feature, you must:

1. Have SEDs in your server.
2. Have created a security key.

ⓘ **NOTE:** In external enclosures and a C6600 PowerEdge server, if the main system is shut down, drives will remain in an unlocked state until the drives are power cycled.

ⓘ **NOTE:** The iDRAC Auto Secure feature does not secure drives that are associated with PERC12 controllers.

Local Key Management

You can use Local Key Management (LKM) to generate the key ID and the Security Key that is required to secure the physical disks. You can secure physical disks, change security keys, and manage secured foreign configurations using this security mode.

Create a security key

About this task

ⓘ **NOTE:** There is no security key backup option when you create a security key; you need to remember your security key.

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management** > **Enable Security**.
3. Select the **Security Key Management** mode as as the local key management type.
4. Click **Ok**.
5. In the **Security Key Identifier** box, enter an identifier for your security key.

   ⓘ **NOTE:** The Security Key Identifier is a clear-text label that enables you to associate the correct security key with the controller.

6. If you want to use the security key generated by the controller, click **Suggest Security Key**.
   Assigns a security key suggested by the controller automatically.
7. In the **Security Key** box, enter the security key.

   ⓘ **NOTE:** Security key is case-sensitive. You must enter a minimum of 8 or a maximum of 32 characters. Ensure that the characters contain at least one number, one lower case letter, one upper case letter, and one non-alphanumeric character.

8. In the **Confirm** box, re-enter the security key.

   ⓘ **NOTE:** If the security key entered in the **Security Key** and **Confirm** boxes do not match, then you are prompted with a message to reenter the security key.

9. Select the **I Recorded the Security Settings for Future Reference** check box.
10. Click **Enable Security**.
    The Security Key is created successfully.

Change security settings

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management** > **Change Security Settings.**
3. Do the following:
   a. To change the security key identifer, enter a new key identifier in the **Enter a New Security Key identifier** box.
   b. To keep existing key identifier, select the **Use the existing Security Key Identifier** check box.
4. Enter the existing security key.
5. Set security key:
   a. To change the security key, enter a new security key in the **Enter a New Security Key** box. Re-enter the new security key to confirm.
   b. To keep the existing security key, select the **Use the Existing Security Key** check box.
6. Select the **I recorded the Security Settings for Future Reference** check box.
7. Click **Save Security Settings**.
8. Click **Confirm**, and then click **Yes**.
   The security settings of the controller are saved.

Disable security key

Prerequisites

- All secured virtual disks and non-RAID disks must be deleted or removed to disable security.
- All secured disks must be cryptographically erased.
- Any Auto Secure non-RAID options must be disabled.

About this task

The **Disable Security Key** feature is available only if a security key present on the controller.

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management** > **Disable Security**.
   You are prompted to confirm whether you want to continue.
3. Click **Confirm**.
4. Click **Yes**.
   The security key is disabled successfully.

   ⓘ **NOTE:** All secured disks must be erased or removed to disable security.

Create a secured virtual disk

About this task

To create a secured virtual disk, you must first create security key for the controller.

ⓘ **NOTE:** Do not mix the following when creating a secured VD:

- SAS and SATA drives
- HDDs and SSDs
- NVMe drives with HDDs and SSDs
- TCG Enterprise and TCG Opal SED protocols

ⓘ **NOTE:** To disable the security features, you must disable the Auto Secure Configuration settings.

After creating the security key, do the following:

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Configuration Management** > **Create Virtual Disk**.
3. Select the **Secure Virtual Disk** option.
4. Click **Create Virtual Disk**.
   The secure virtual disk is created successfully.

Secure a non-RAID disk

In HII, secure a non-RAID disk by using the security key of the controller.

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Device Management** > **Logical Enclosure <enclosure Number>**. An enclosure number can be 0, 1, 2, 3, 4, and so on.
   All the physical disks associated with the selected enclosure are listed.
3. Select a non-RAID disk.

4. From the **Operations** drop-down menu, select **Secure Non-RAID Disk**.

Secure a pre-existing virtual disk

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Virtual Disk Management**.
   The list of virtual disks is displayed.
3. Select a virtual disk.
4. From the **Operations** drop-down menu, select **Secure Virtual Disk**.

   NOTE: The virtual disks can be secured only when the virtual disks are in Optimal state.

Import a secured non-RAID disk

If you are inserting a non-RAID disk into a system that has a controller key different from the security key on the drive, the security key from the system in which it was initially secured must be provided in HII.

Prerequisites

NOTE: The controller must have an existing security key before importing a secured non-RAID disk.

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Configuration Management** > **Manage Foreign Configurations**.
3. Select **Enter Security Key For Locked Drives** and enter the security key if you are importing drives with a different security key.
   The drive's key will be changed to the controller key.
4. If required, convert the drive to a non-RAID drive.

Import a secured virtual disk

Prerequisites

NOTE: The controller must have an existing security key before importing secured foreign virtual disk.

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Configuration Management** > **Manage Foreign Configurations**.
3. Click **Import Foreign Configuration**.
4. To import a VD by using a different security key, enter the new security key.
5. When prompted to conform if you want to perform the operation, click **Confirm**.
6. Click **Yes**.
   The foreign configuration is imported successfully.

   NOTE: By using PERC 12, you cannot import foreign configuration data of previous PERC versions.

Dell Technologies OpenManage Secure Enterprise Key Manager (SEKM)

This feature allows the PERC to receive a security key from a remote server instead of saving the key on a local controller. This protects data on secured disks under the PERC if the disks or the entire system is stolen. For more information about configuring OpenManage Secure Enterprise Key Manager (SEKM) and Sockets Layer (SSL) or Transport Layer Security (TLS) related configuration, see the iDRAC User's Guide available on the support site. See the Enable OpenManage Secure Enterprise Key Manager (SEKM) on PowerEdge Servers technical white paper available on the Dell support site.

ⓘ **NOTE:** When replacing a controller enabled with enterprise key management, the user must re-enable enterprise key management on the controller from iDRAC.

ⓘ **NOTE:** If key exchange fails during boot, view and correct any connection issues with the key server that is identified in the iDRAC Lifecycle log, and then cold reboot the server.

ⓘ **NOTE:** VDs will no longer be automatically rekeyed when they are unlocked. They are rekeyed when they are imported. Non-RAID and unconfigured drives will still be automatically rekeyed.

ⓘ **NOTE:** The Relock feature is supported on NVMe drives for both native and foreign locked drives and SAS/SATA for foreign locked drives.

Supported controllers for OpenManage Secure Enterprise Key Manager (SEKM)

Enterprise key manager mode is supported on the PERC H365i Adapter and PERC H365i Front DC-MHS controllers, and allows the creation of secured virtual disks and non–RAID disks. For more information about supported platforms, see the iDRAC User's Guide available on the support site.

Manage the Server Enterprise Key Manager (SEKM) feature

iDRAC manages the SEKM features. For instructions on enabling enterprise key manager mode, see the SEKM section in the relevant version of the iDRAC User's Guide available on the support site.

ⓘ **NOTE:** When the SEKM mode is enabled, the controller waits up to two minutes for iDRAC to send keys, and then the PERC continues to boot.

ⓘ **NOTE:** iDRAC performs rotation of keys. Any attempt to rekey the controller through a different management application is not supported.

Disable the Secure Enterprise Key Manager (SEKM) feature

The SEKM mode can be disabled only by using the iDRAC interfaces such as GUI and RACADM.

For information about disabling SEKM, see the "SEKM Functionalities" section in the releavant iDRAC User's Guide available on the support site. Also see the Enable OpenManage Secure Enterprise Key Manager (SEKM) on Dell PowerEdge Servers technical white paper available on the support site.

Manage virtual disks in the SEKM mode

The VDs in SEKM mode are managed in the same way as in local key manager mode. SED capable VDs can be secured during or after creation.

Manage non–RAID disks in the SEKM mode

Non–RAID disks are managed in the same way in enterprise key manager mode as in local key manager mode. SED capable non–RAID disks can be secured after creation.

Transition of drives from Local Key Management to Secure Enterprise Key Management

PERC enables transition from Local Key Management (LKM) mode to Secure Enterprise Key Manager (SEKM) mode without disabling LKM security first. For instructions on transitioning from LKM mode to SEKM mode, see the iDRAC User's Guide of the relevant iDRAC version available on the support site.

You cannot transition from LKM to SEKM when:

- The snapdump is present on PERC.
- The Sanitize operation on a physical disk is in progress.
- The LKM key does not match with the current key of PERC.

Local Key Management

You can use Local Key Management (LKM) to generate the key ID and the Security Key that is required to secure the physical disks. You can secure physical disks, change security keys, and manage secured foreign configurations using this security mode.

Create a security key

About this task

ⓘ **NOTE:** There is no security key backup option when you create a security key; you need to remember your security key.

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management** > **Enable Security**.
3. Select the **Security Key Management** mode as as the local key management type.
4. Click **Ok**.
5. In the **Security Key Identifier** box, enter an identifier for your security key.

   ⓘ **NOTE:** The Security Key Identifier is a clear-text label that enables you to associate the correct security key with the controller.

6. If you want to use the security key generated by the controller, click **Suggest Security Key**.
   Assigns a security key suggested by the controller automatically.
7. In the **Security Key** box, enter the security key.

   ⓘ **NOTE:** Security key is case-sensitive. You must enter a minimum of 8 or a maximum of 32 characters. Ensure that the characters contain at least one number, one lower case letter, one upper case letter, and one non-alphanumeric character.

8. In the **Confirm** box, re-enter the security key.

   ⓘ **NOTE:** If the security key entered in the **Security Key** and **Confirm** boxes do not match, then you are prompted with a message to reenter the security key.

9. Select the **I Recorded the Security Settings for Future Reference** check box.
10. Click **Enable Security**.
    The Security Key is created successfully.

Change security settings

Steps

1. Enter the PERC12 HII Configuration Utility.

2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management** > **Change Security Settings.**
3. Do the following:
    a. To change the security key identifer, enter a new key identifier in the **Enter a New Security Key identifier** box.
    b. To keep existing key identifier, select the **Use the existing Security Key Identifier** check box.
4. Enter the existing security key.
5. Set security key:
    a. To change the security key, enter a new security key in the **Enter a New Security Key** box. Re-enter the new security key to confirm.
    b. To keep the existing security key, select the **Use the Existing Security Key** check box.
6. Select the **I recorded the Security Settings for Future Reference** check box.
7. Click **Save Security Settings**.
8. Click **Confirm**, and then click **Yes**.
   The security settings of the controller are saved.

Disable security key

Prerequisites

- All secured virtual disks and non-RAID disks must be deleted or removed to disable security.
- All secured disks must be cryptographically erased.
- Any Auto Secure non-RAID options must be disabled.

About this task

The **Disable Security Key** feature is available only if a security key present on the controller.

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Controller Management** > **Advanced Controller Management** > **Disable Security**.
   You are prompted to confirm whether you want to continue.
3. Click **Confirm**.
4. Click **Yes**.
   The security key is disabled successfully.

   ⓘ **NOTE:** All secured disks must be erased or removed to disable security.

Create a secured virtual disk

About this task

To create a secured virtual disk, you must first create security key for the controller.

ⓘ **NOTE:** Do not mix the following when creating a secured VD:

- SAS and SATA drives
- HDDs and SSDs
- NVMe drives with HDDs and SSDs
- TCG Enterprise and TCG Opal SED protocols

ⓘ **NOTE:** To disable the security features, you must disable the Auto Secure Configuration settings.

After creating the security key, do the following:

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Configuration Management** > **Create Virtual Disk**.
3. Select the **Secure Virtual Disk** option.

4. Click **Create Virtual Disk**.
   The secure virtual disk is created successfully.

Secure a non-RAID disk

In HII, secure a non-RAID disk by using the security key of the controller.

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Device Management** > **Logical Enclosure <enclosure Number>**. An enclosure number can be 0, 1, 2, 3, 4, and so on.
   All the physical disks associated with the selected enclosure are listed.
3. Select a non-RAID disk.
4. From the **Operations** drop-down menu, select **Secure Non-RAID Disk**.

Secure a pre-existing virtual disk

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Virtual Disk Management**.
   The list of virtual disks is displayed.
3. Select a virtual disk.
4. From the **Operations** drop-down menu, select **Secure Virtual Disk**.

   ⓘ **NOTE:** The virtual disks can be secured only when the virtual disks are in Optimal state.

Import a secured non-RAID disk

If you are inserting a non-RAID disk into a system that has a controller key different from the security key on the drive, the security key from the system in which it was initially secured must be provided in HII.

Prerequisites

ⓘ **NOTE:** The controller must have an existing security key before importing a secured non-RAID disk.

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Configuration Management** > **Manage Foreign Configurations**.
3. Select **Enter Security Key For Locked Drives** and enter the security key if you are importing drives with a different security key.
   The drive's key will be changed to the controller key.
4. If required, convert the drive to a non-RAID drive.

Import a secured virtual disk

Prerequisites

ⓘ **NOTE:** The controller must have an existing security key before importing secured foreign virtual disk.

Steps

1. Enter the PERC12 HII Configuration Utility.
2. Click **Main Menu** > **Configuration Management** > **Manage Foreign Configurations**.
3. Click **Import Foreign Configuration**.
4. To import a VD by using a different security key, enter the new security key.
5. When prompted to conform if you want to perform the operation, click **Confirm**.
6. Click **Yes**.
   The foreign configuration is imported successfully.

   ⓘ **NOTE:** By using PERC 12, you cannot import foreign configuration data of previous PERC versions.

Dell Technologies OpenManage Secure Enterprise Key Manager (SEKM)

This feature allows the PERC to receive a security key from a remote server instead of saving the key on a local controller. This protects data on secured disks under the PERC if the disks or the entire system is stolen. For more information about configuring OpenManage Secure Enterprise Key Manager (SEKM) and Sockets Layer (SSL) or Transport Layer Security (TLS) related configuration, see the iDRAC User's Guide available on the support site. See the Enable OpenManage Secure Enterprise Key Manager (SEKM) on PowerEdge Servers technical white paper available on the Dell support site.

ⓘ **NOTE:** When replacing a controller enabled with enterprise key management, the user must re-enable enterprise key management on the controller from iDRAC.

ⓘ **NOTE:** If key exchange fails during boot, view and correct any connection issues with the key server that is identified in the iDRAC Lifecycle log, and then cold reboot the server.

ⓘ **NOTE:** VDs will no longer be automatically rekeyed when they are unlocked. They are rekeyed when they are imported. Non-RAID and unconfigured drives will still be automatically rekeyed.

ⓘ **NOTE:** The Relock feature is supported on NVMe drives for both native and foreign locked drives and SAS/SATA for foreign locked drives.

Supported controllers for OpenManage Secure Enterprise Key Manager (SEKM)

Enterprise key manager mode is supported on the PERC H365i Adapter and PERC H365i Front DC-MHS controllers, and allows the creation of secured virtual disks and non–RAID disks. For more information about supported platforms, see the iDRAC User's Guide available on the support site.

Manage the Server Enterprise Key Manager (SEKM) feature

iDRAC manages the SEKM features. For instructions on enabling enterprise key manager mode, see the SEKM section in the relevant version of the iDRAC User's Guide available on the support site.

ⓘ **NOTE:** When the SEKM mode is enabled, the controller waits up to two minutes for iDRAC to send keys, and then the PERC continues to boot.

ⓘ **NOTE:** iDRAC performs rotation of keys. Any attempt to rekey the controller through a different management application is not supported.

Disable the Secure Enterprise Key Manager (SEKM) feature

The SEKM mode can be disabled only by using the iDRAC interfaces such as GUI and RACADM.

For information about disabling SEKM, see the "SEKM Functionalities" section in the releavant iDRAC User's Guide available on the support site. Also see the Enable OpenManage Secure Enterprise Key Manager (SEKM) on Dell PowerEdge Servers technical white paper available on the support site.

Manage virtual disks in the SEKM mode

The VDs in SEKM mode are managed in the same way as in local key manager mode. SED capable VDs can be secured during or after creation.

Manage non–RAID disks in the SEKM mode

Non–RAID disks are managed in the same way in enterprise key manager mode as in local key manager mode. SED capable non–RAID disks can be secured after creation.

Transition of drives from Local Key Management to Secure Enterprise Key Management

PERC enables transition from Local Key Management (LKM) mode to Secure Enterprise Key Manager (SEKM) mode without disabling LKM security first. For instructions on transitioning from LKM mode to SEKM mode, see the iDRAC User's Guide of the relevant iDRAC version available on the support site.

You cannot transition from LKM to SEKM when:

- The snapdump is present on PERC.
- The Sanitize operation on a physical disk is in progress.
- The LKM key does not match with the current key of PERC.

iDRAC Local Key Management (iLKM)

This feature allows the H365 series controller to receive a security key from iDRAC. This protects data on secured disks that are attached to the controller if the drives are stolen. For more information about configuring iLKM, see the iDRAC User's Guide available on the support site.

Enable or disable the iDRAC Local Key Management (iLKM) feature

The iLKM mode can be enabled or disabled only by using the iDRAC interfaces such as GUI and RACADM. For information about enabling or disabling iLKM, see the "iLKM Functionalities" section in the relevant iDRAC User's Guide available on the support site.

9

Security key and PERC H365i Adapter controller management

The PERC H365i Adapter controller supports host-managed SEDs.

The controller supports security management of non-RAID SEDs from the host device. A host application is allowed to manage the non-RAID SEDs by directly sending security commands. A third-party software application is used to manage SEDs.

10

Troubleshooting issues in PERC12 series cards

To get help for resolving issues in your Dell Technologies PowerEdge RAID Controller12 series cards, you can contact your Dell Technical Service representative.

Topics:

Unable to import the VD for 120 s after recently removing the VD

Error Message:	Unable to temporarily (for 120 s) import a VD that was recently removed resulting in the creation of a preserved cache on that VD.
Corrective Action:	Wait 120 s before attempting to import the VD or delete the preserved cache, and then retry to import the VD.

Observed a controller fault while updating the controller firmware when using Linux operating system

Error Message: Observed a controller fault while updating the controller firmware when using the Linux operating system.

Probable Cause: Because the controller driver version is earlier than 8.9.1.0.50.

Corrective Action: Known issue. Update the driver version and retry the operation.

Virtual drive Blink and Unblink operations are unavailable in iDRAC UI and HII

Error Message: VD Blink and Unblink operations are greyed out on the iDRAC user interface.

Corrective Action: Known issue. No corrective action required. Use the locate command: `perccli2 /c0/e32/s0 start locate`. For more information, see the "Locate a drive" section in the PERC12 CLI Reference Guide available on the support site.

The SMART data of SATA SSDs is unavailable from iDRAC

Error Message: The SMART data of SATA SSDs is unavailable from iDRAC when it is connected to a PERC12 or HBA465 series controller.

Corrective Action: Known issue. Use the PERCCLI2 to view the SMART data about the SATA SSDs.

When secured drives are hot-removed or hot-inserted in the server, iDRAC doesn't generate the PD Unlock event

Error Message: When secured drives are hot-removed or hot-inserted in the server, iDRAC doesn't generate the PD Unlock event.

Probable Cause: The PD Unlock event is happening before the PD Insert event.

Corrective Action: Known issue. No response action is required. There is no functional impact. The secure drives will be already in unlock state.

During a Key Exchange Failure scenario in SEKM mode, native locked drives are Identified as "Locked with Foreign Key" in all interfaces

Error Message: When key exchange fails in the SEKM mode, the native locked drives are identified as "Locked with foreign key".

Probable Cause: Could be one of the following: 1) An issue in connecting to the SEKM server. 2) A key is deleted from the KMS.

Corrective Action: Known issue. Check the SEKM server connectivity to iDRAC.

After importing the foreign configuration of the associated global hot-spare drive on a PERC12 series controller, the drive is still reported as both Online and global hot-spare

Error Message: After importing the foreign configuration of the associated global hot-spare drive on a PERC12 or HBA465 series controller, the drive is still reported as both Online and global hot-spare

Probable Cause: The drive type of a commissioned Global Hot Spare was incorrectly set as Global Hot Spare during the foreign import operation.

Corrective Action: Reset the controller by running the `perccli2 /c0 reset` command at the PERC12 CLI.

LED Operations using ESXCLI Commands for H365, H965, and HBA465 Series controller is not available using VMware ESXi OS

Error Message: The – `esxcli storage core device physical get -d naa.58ce38ee2182900d` command used to locate the drive by blinking or unblinking the LED when using an ESXi7 or ESXi8 operating system.

Probable Cause: The LSU Plugin does not have SL8 embedded to support the blink and unblink operations.

Corrective Action: Known Issue with a VMware ESXi Operating System. Use the locate command: `perccli2 /c0/e32/s0 start locate`. For more information, see the "Locate a drive" section in the PERC12 CLI Reference Guide available on the support site.

Backplane slot count may be reported as 32 if there is an error with the backplane during discovery or runtime

Error Message: Backplane is indicated as faulty and slot-count is shown as 32 even though the configuration supports less than 32.

Corrective Action: Known issue. No functional impact. System will require a reset to recover from this behavior. For more information about backplanes, see the Installation and Service Manual (ISM) of the respective server model available on the support site.

Single virtual disk performance or latency in hypervisor configurations

Multi-initiator or hypervisor configurations running multiple I/O workloads to a single RAID array may experience degraded performance or latency. This is caused by upper layers sending separate I/O workloads for each virtual machine to the storage subsystem which ends up being a random I/O workload to the underlying RAID array. For I/O workload configurations that require lower latency restrictions and higher I/O performance it may be beneficial to run fewer I/O workloads to individual RAID arrays or to use separate RAID arrays and hard drives for each I/O workload. Other considerations are making sure to use Solid State Drives (SSDs) to improve random I/O workload performance.

Performance degradation may also be observed when background operations such as initialization, consistency check, or rebuilds are running on the virtual disk. See your hypervisor storage best practices or performance best practices guides for additional configuration support.

Unable to discover or detect a PERC card

Error Message: `A discovery error has occurred, please power cycle the system and all the enclosures attached to this system.`

Probable Cause: This message indicates that disk topology discovery did not complete within 120 seconds. The cables from the PERC controller to the backplane might be improperly connected.

Corrective Action: Check the cable connections and fix any problems. Restart the system.

Unable to install the Microsoft Windows operating system

Ensure that you perform the following step before installing Windows on 4 KB sector drives:

1. Read and understand the updates to the version of Windows that you have installed. You can find this information in the Microsoft help. For more information, see Microsoft support policy for 4 K sector hard drives in Windows.

Only UEFI is supported and not BIOS

Issue Only UEFI boot is supported by HBA465 and PERC12 controllers. BIOS is not supported.

Corrective Action: Expected behavior. No action is required.

A fault firmware state is detected

Error Message: `Firmware is in Fault State. Controller: Broadcom MPI3 I/O Controller (Fault). The controller is in a Fault state: Faultcode <FaultCode>; Additional code: <Code> : <Code> : <Code>`

Corrective Action: Contact your Technical Support team.

Foreign configuration not found in HII

Error Message: `The foreign configuration message is present during POST but no foreign configurations are present in the foreign view page in HII configuration utility. All virtual disks are in an optimal state.`

Corrective Action: Ensure all your PDs are present and all VDs are in optimal state. Clear the foreign configuration using **HII configuration utility** or **Dell OpenManage Server Administrator Storage Management**.

⚠ CAUTION: **The physical disk goes to Ready state when you clear the foreign configuration.**

If you insert a physical disk that was previously a member of a virtual disk in the system, and that disk's previous location has been taken by a replacement disk through a rebuild, you must manually remove the foreign configuration flag of the newly inserted disk.

Degraded state of virtual disks

A redundant virtual disk is in a degraded state when one or more physical disks have failed or are inaccessible. For example, if a RAID 1 virtual disk consists of two physical disks and one of them fails or becomes inaccessible, the virtual disk becomes degraded.

To recover a virtual disk from a degraded state, you must replace the failed physical disk and rebuild it. Once the rebuilding process is complete, the virtual disk state changes from degraded to optimal.

Boot-time errors

The following table lists error messages, probable causes, and recommended response action to resolve the issue.

Table 18. Boot-time issues and corrective actions

Description	Error Message	Probable Cause	Recommended Corrective Action
Removed or Missing Device	Some configured disks have been removed from the system or are no longer accessible. Check the cables and ensure that all drives are installed in the slots.	Some configured drives are removed. Else, they may not be accessible anymore. Or, the cables from PERC to the backplane may be improperly connected.	Check the cables and ensure that all drives are installed in the slots. If there are no cable-related issues, restart the server.
Removed or Missing Device	The following VDs are missing <VD Names>. If you proceed or continue to start the Configuration Utility, these VDs is removed from the configuration. To use VDs later, you must import them.	Because some configured drives are removed. Else, they may not be accessible anymore. Or, the cables from PERC to the backplane may be improperly connected.	Check the cables and ensure that all drives are installed in the slots. If there are no cable-related issues, restart the server.
Removed or Missing Device	The following VDs are missing <VD Names> complete spans. If you proceed or continue to start the Configuration Utility, these VDs is removed from the configuration. To use VDs later, you must import them.	Because some configured drives are removed. Else, they may not be accessible anymore. Or, the cables from PERC to the backplane may be improperly connected.	Check the cables and ensure that all drives are installed in the slots. If there are no cable-related issues, restart the server.
Removed or Missing Device	All drives that are associated with the previous configuration are no longer associated with the configuration.	Because some configured drives are removed. Else, they may not be accessible anymore. Or, the cables from PERC to the backplane may be improperly connected.	Check the cables and ensure that all drives are installed in the slots. If there are no cable-related issues, restart the server.
Offline VD	The following VDs have missing PDs: <VD_Names>. If you continue or start the Configuration Utility, these VDs is identified as Offline, and may become inaccessible.	Some configured drives are either removed or have stopped functioning, resulting in the VDs to be identified as Offline.	Check the cables and ensure that all drives are installed in the slots. If there are no cable-related issues, restart the server.
The Foreign Configuration Import operations did not import any drives.	The Foreign Configuration Import operations did not import any drives.	Either the Foreign Configuration is incompatible with this controller or the Foreign Configuration is incomplete.	Make sure that either the drives necessary for this configuration are installed or remove the incompatible configuration.
Factory Setting Corrupt	The nonvolatile data validation operation is unsuccessful.	The factory settings of the controller may have been corrupted.	Upgrade the firmware by using the correct NV Data. Or, contact the Technical Support team.

Table 18. Boot-time issues and corrective actions (continued)

Description	Error Message	Probable Cause	Recommended Corrective Action
Factory Setting Corrupt	Unable to read the MPB file of the personality, OEM ID, or Profile ID. The controller is switching to Safe Mode.	The factory settings of the controller may have been corrupted.	Contact the Dell Technical support team.
Factory Setting Corrupt	The NVRAM layout is either corrupted or has a mismatch, and therefore, is reinitialized.	The factory settings of the controller may have been corrupted, and therefore, reinitialized.	Upgrade the firmware by using the correct NV Data. Or, contact the Technical Support team.
Enclosure/ Backplane Count exceeded.	The number of enclosures or backplanes that are connected to the connector <connectorName> has exceeded the maximum number.	Backplanes or enclosures that are connected to the connector are more than the maximum allowed.	Power off the server and remove the backplanes or enclosures to ensure that the number is less than the maximum value.
Physical Disk Count exceeded.	The number of PDs connected is more than the supported value of <number> drives.	The installed PDs are more than the maximum allowed.	Power off the server and remove the PDs to ensure that the number is less than the maximum value.
Topology Error	An invalid SAS topology is detected in <name>.	Either a nonfunctional or corrupted PD is inserted in the server.	Remove any recently inserted PDs from the server.
Discovery Error	Unable to discover the controller: <%s>.	The controller could not be discovered within 120 s. Cables from the PERC to the backplane might be improperly connected.	Check the cable connection between PERC and the server. Power cycle the server and all attached enclosures.
Unable to communicate with Key management server.	Unable to communicate with the SEKM Server. If you continue, there will be a drive security key error and all the secured configurations are marked as foreign. Check the connection with the SEKM server, reboot the machine to retry switching to EKM.	Connection Information between iDRAC and the Key Management Server (KMS) may have changed. Or, An iDRAC controller discovery issue may have occurred preventing the key exchange within the timeout period.	See the iDRAC User's Guide of the relevant version on the support site, ensure that the KMS communication is successful, and then restart the server.
Safe Mode entered	The controller booted in the safe mode.	An internal issue forced the controller to boot in the safe mode.	View the server screen to get information about why the controller booted to a safe mode, and then take the recommended corrective action.
Safe Mode Exited	The controller has exited the safe mode.	Not applicable.	No response action is required.

Event log errors

The following table lists error messages, probable causes, and recommended response action to resolve the Event Log errors.

ⓘ **NOTE:** The text that is used in the following messages may vary based on the type of management application.

Table 19. Run-time issues and corrective actions

Description	Error Message	Probable Cause	Recommended Corrective Action
Correctable Error During BGI	A medium error was corrected on the following virtual drive during background initialization: <VD_Name> at <variable Name>,	The drive had a correctable mediumerror, and the data is recovered. The drive may be getting corrupted or facing a data-rot.	Verify the SMART status of the drive, and if necessary, replace the drive.

Table 19. Run-time issues and corrective actions (continued)

Description	Error Message	Probable Cause	Recommended Corrective Action
	<PD_Name>, LUN <Name>, Count <Number>.		
Uncorrectable Error During BGI	The Background Initialization operation is completed in the virtual drive <VD_Name> with uncorrectable errors.	One or more uncorrectable errors are detected during the BGI operation. Data may be lost.	Verify the SMART status of the drive and ensure that the data is backed up.
Uncorrectable Error During BGI	The Background Initialization operation is completed in the virtual drive <VD_Name> with uncorrectable errors.	An uncorrectable error was detected during the BGI operation. Data may be lost.	Verify the SMART status of the drive and ensure that the data is backed up.
BGI Failed	Unable to complete the Background Initialization operation on the virtual drive <VD_Name>.	A hard drive may have failed during the BGI operation which made the virtual drive appear as offline.	Check the health status of virtual drives and hard drives, and then replace corrupted drives if necessary.
Error Corrected during consistency check	The Consistency Check operation corrected an error on the drive: <VD_Name> at <variable Name>, <PD_Name>, LUN <Name>, Count <Number>.	The drive had a medium error and corrected during Consistency Check. Data may be lost.	Verify the SMART status of the drive and ensure that the data is backed up.
Consistency check completed with corrected errors.	The Consistency Check operation was completed on the drive: <VD_Name> Corrections <correctionData>.	The drive had a correctable mediumerror, and the data is recovered. The drive may be getting corrupted or facing a data-rot.	Verify the SMART status of the drive, and if necessary, replace the drive.
Uncorrectable media errors detected during consistency check	The Consistency Check operation detected uncorrectable multiple medium errors on the drive: <VD_Name> at <variable Name>, <PD_Name>, LUN <Name>, Count <Number>.	The drive had a medium error and corrected during Consistency Check. Data may be lost.	Check the health status of virtual drives and PDs, and then replace corrupted drives if necessary.
Unable to complete consistency check.	Unable to complete the Consistency Check operation on the virtual drive <VD_Name>.	Consistency Check has failed on virtual drive which could be because of media errors.	Check the health status of the virtual drives and PDs. Replace any nonfunctional drives.
Consistency check completed with uncorrectable errors.	The Consistency Check (CC) operation is completed with uncorrectable errors on the virtual drive <VD_Name>.	Medium Errors were not corrected after CC. If the virtual drive is not redundant (or is degraded), then data cannot be regenerated and the medium error cannot be resolved. Data may be lost.	Check the health status of virtual drives and hard drives, and then replace corrupted drives if necessary.
Consistency check logging disabled due to too many inconsistencies	Inconsistency data on the virtual drive <VD_Name> cannot be logged in because too many inconsistencies are detected on the virtual drive, and the feature is disabled during the Consistency Check operation.	The Consistency Check operation detected multiple inconsistencies and disabled data logging.	Check the health status of virtual drives and hard drives, and then replace corrupted drives if necessary.
Virtual drive Initialization failed	Unable to initialize the virtual drive <VD_Name>.	A disk could have failed during initialization causing the virtual drive to go offline.	Check the health status of virtual drives and hard drives, and then replace corrupted drives if necessary.

Table 19. Run-time issues and corrective actions (continued)

Description	Error Message	Probable Cause	Recommended Corrective Action
Physical drive erase errors.	Data on the following hard drive cannot be cleared: <PD Name>, <Path Name>, <ErrorDescription>.	The drive could have either failed or returned an error during the Clear operation.	Check the health and SMART status of hard drives, and then replace corrupted drives if necessary.
Physical drive error	An error is detected on the following physical drive: <PD Name>, <Path Name>, <ErrorDescription>.	An error is detected on the hard drive.	Check the health and SMART status of hard drives, and then replace corrupted drives if necessary.
Physical drive not supported	The hard drive <PD Name> is either not supported by the controller or is in an unsupported format.	The hard drive is either not supported by the controller or is in an unsupported format.	Replace the drive or reformat by using a supported file format.
Physical drive not certified warning	The hard drive <PD Name> is not certified.	The hard drive is not manufactured as per Dell technical specifications and cannot guarantee that the hard drive will be fully compliant with Dell standards and functionalities.	Use a hard drive that complies with Dell standards and retry the operation.
Media error corrected during patrol-read	The patrol-read operation corrected a medium error on the hard drive <PD Name>, LUN <LUN Name>.	The drive had a medium error and corrected during Consistency Check. Data may be lost.	Verify the SMART status of the drive and ensure that the data is backed up.
Uncorrectable media error detected during patrol-read	The patrol-read operation detected an uncorrectable medium error on the hard drive <PD Name>, LUN <LUN Name>.	An uncorrectable error was detected during the patrol-read operation. Data may be lost.	Check the health status of virtual drives and hard drives, and then replace corrupted drives if necessary.
Physical drive Predictive Failure	A predictive failure is detected in the physical drive: <PD Name>.	The SMART data is indicating that the drive may fail soon.	Replace the drive and ensure that therebuild or copy-back operation is successful.
A bad block punctured on the hard drive	A bad block is being punctured on the physical drive: <PD Name>, LUN <LUN Name>.	LBA on the hard drive was punctured. Data may be lost.	Check the health status of virtual drives and hard drives, and then replace corrupted drives if necessary.
Unable to rebuild the array because of an error on the source disk.	Unable to rebuild the hard drive <PD Name> because of an error in the source drive.	Source drive that is failed because of which the Rebuild operation cannot proceed. Data may be lost.	Replace any bad drives and re-create virtual drive from backup.
Unable to rebuild the array because of an error on the target disk.	Unable to rebuild the hard drive <PD Name> because of an error in the target drive.	Target drive failed due to which the Rebuild operation cannot be continued.	Replace any bad drives and restart the Rebuild operation.
Unrecoverable error that is detected during rebuild	An unrecoverable medium error is detected during the Rebuild operation on the hard drive: <PD Name>, LUN <LUN Name>.	An uncorrectable error was detected during the rebuild. Data may be lost.	Check the health status of virtual drives and PDs, and then replace corrupted drives if necessary.
Media error corrected during operation	A medium error is corrected during the recovery operation on the hard drive: <PD Name>, LUN <LUN Name>.	A medium error was detected during the BGI operation. Data may be lost.	Verify the SMART status of the drive and ensure that the data is backed up.

Table 19. Run-time issues and corrective actions (continued)

Description	Error Message	Probable Cause	Recommended Corrective Action
Unrecoverable error detected during operation	An unrecoverable medium error is detected during the recovery operation on the hard drive: <PD Name>, LUN <LUN Name>.	Medium Errors were not corrected after recovery. If a virtual drive is not redundant (or is degraded), data cannot be regenerated and medium error cannot be resolved. Data may be lost.	Check the health status of virtual drives and hard drives, and then replace corrupted drives if necessary.
SCSI Sense Data	An unexpected Sense error is on the hard drive: <PD Name>, Path <Path Name>, CDB <CDB Name>, Sense <Sense Name>.	The drive returned sense data for the SCSI CDB. This can include info during drive power-on, firmware update, or errors.	If the event is seen consistently in logs, contact the Technical Support team.
Physical drive is not accessible.	Unable to access the PD: <PD Name>.	An error occurred during the discovery or initialization of the drive. The drive may be corrupted.	Remove or reinstall the drive. Check the health or SMART status of the hard drive. For NVMe drives, run the Recovery operation of the supported format.
Hot-Spare no longer covers all arrays.	The global hot spare <PD Name> no longer covers all the arrays.	The assigned global hot spare hard drive is not of the same type to cover all the virtual drives in the system.	Ensure to assign a global hot spare hard drive which is of the same type of the other VD. Else, use dedicated hot spare for virtual drives that are not covered.
Unable to communicate with backplane or enclosure.	The controller is unable to communicate with the enclosure <enclosure Name>.	The cable may be loose or damaged.	Ensure that the cables are connected and not damaged. Restart the server if necessary.
Backplane or enclosure discovery error	Discovery error detected for enclosure <enclosure name> (receptacle <receptacle number >) - < error code>.	Error is probably caused by cables, backplane firmware, or slot connections.	Check all cables and drives and ensure that they are properly seated. AC power-cycle the system. If the issue persists, contact your Technical Support team.
PHY/Slot bad	The enclosure with hard drive <PD Name> is not detected by controller in the slot <slotName>.	The hard drive is inserted in the slot but not detected by the controller. The hard drive may be corrupted.	Ensure that the cables are connected and not damaged. Restart the server if necessary.
The backplane or enclosure is unstable.	The enclosure <enclosure Name> is unstable.	The backplane or enclosure has detected an error.	Ensure that the cables are connected and not damaged. Upgrade the enclosure firmware and restart the server.
Hardware issues that are detected on backplane or enclosure	The enclosure <enclosure Name> is has hardware issue.	The backplane or enclosure has indicated that there is a hardware failure or issue.	Ensure that the cables are connected and not damaged. Upgrade the enclosure or backplane firmware and restart the server. If the issue persists, contact your Technical Support team.
Enclosure is not responding.	The enclosure with hard drive <enclosure Name> is not responding.	The backplane is not responding to the controller.	Ensure that the cables are connected and not damaged. Upgrade the enclosure or backplane firmware and restart the server. If the issue persists,

Table 19. Run-time issues and corrective actions (continued)

Description	Error Message	Probable Cause	Recommended Corrective Action
			contact your Technical Support team.
Disk missing	The following hard drive is missing: <PD Name>.	A configured hard drive is not detected after resetting or restarting the controller.	If this issue is unexpected, ensure that the cables are properly connected and the hard drives are seated, and then restart the server.
Virtual disk offline because of missing disks	The following virtual drives are not detected, and therefore, the hard drives go offline: <VD Names>.	One or more of the hard drives is bad and has gone offline.	Check the health status of the hard drives and replace any bad drives.
Virtual drive is partially degraded.	The virtual drive <VD Name> is partially degraded.	One or more of the hard drives is bad and has gone offline.	Check the health status of the hard drives and replace any bad drives.
Virtual drive is degraded.	The VD <VD Name> is now fully degraded.	One or more of the hard drives is bad and has gone offline.	Check the health status of the hard drives and replace any bad drives.
Virtual drive is offline.	The virtual drive <VD Name> is now offline.	One or more of the hard drives is bad and has gone offline.	Check the health status of the hard drives and replace any bad drives.
Physical drive command timeout	The command that is timed out waiting for response: <PD Name>, Path <Path Name>, CDB <CDB Name>, Sense <Sense Name>.	The drive Command that is timed out waiting for a response. This may occur due to an error or in cases where the device is reset such as a firmware update. Command may have been retried.	Check the health or SMART status of the drive and replace any failing drives. Try restarting the server or controller. If the issue persists, contact the Technical Support team.
Disk Reset	The hard drive <PD Name>, Path <pathname> is reset.	The drive was reset. This can happen in an attempt to recover from an error during device discovery.	If the issue is persistently seen in logs, contact the Technical Support team.
Bad Block table for virtual drive 80% full	The bad block table on the virtual drive <VD Name> is 80% full.	Multiple uncorrectable medium errors were found on the drive and added to the LDBBM table.	Check the health status of the hard drives and replace any bad drives.
Bad block logging for virtual drive that is disabled because of too many bad blocks.	Unable to log the block <blockName> on the hard drive <PD Name>, LUN <LUN Name> at <Count> because of a block table on the virtual drive <VD Name>l.	Multiple uncorrectable medium errors were found on the drive and added to the LDBBM table.	Check the health status of the hard drives and replace any bad drives.
Uncorrectable media error is detected on the virtual drive.	An uncorrectable medium error was logged for virtual drive <VD Name>: Hard drive <PD Name>, LUN <LUN Name> at <Count> because of a block table on the virtual drive <VD Name>.	Uncorrectable multiple medium errors were found on the disk. Data may be lost.	Check the health status of the hard drives and replace any bad drives.
Media error corrected on virtual drive	A medium error was corrected on the virtual drive <VD Name> at <name>.	Medium Error was found on the disk and corrected. Data may be lost.	Verify the SMART status of the drive and ensure that the data is backed up.
Bad block table for virtual disk is 100% full.	The bad block table on the virtual drive <VD Name> is 100% full.	Multiple uncorrectable medium errors were found on the drive and added to the LDBBM table.	Check the health status of the hard drives and replace any bad drives.

Table 19. Run-time issues and corrective actions (continued)

Description	Error Message	Probable Cause	Recommended Corrective Action
Physical drives update timeout	The Microcode Update operation timed out on the hard drives <PD Name>.	The drive firmware update operation did not complete within the specified time limit. The firmware may still have updated successfully.	Verify if the drive firmware is fully updated. Else, retry the operation. If the firmware cannot be upgraded, then contact your Technical Support team.
The security key that is entered is invalid.	Unable to unlock the drive because an invalid security key is entered.	An incorrect security key ID is used to unlock the drive or controller.	Enter a valid security key ID and retry the operation. If multiple drives use the same key ID anddifferent security keys, then remove the extra drives and separately import the drives.
Unable to unlock drives because of invalid security key.	Unable to unlock the drive because the security key that is provided by Escrow is invalid.	The security key ID provided by Escrow is invalid.	If multiple drives use the same keyID and different security keys, then remove the extra drives and import the disks separately.
A Drive Security Error is detected.	Security subsystem issues are detected on the hard drive <PD Name>.	There is an issue when managing the security of the drive.	Remove, reinstall the drive, and then retry the operation. If the issue persists, contact your Technical Support team.
Locked drives are not accessible because of a key exchange error.	Unable to access the secured configuration because an incorrect security key is entered.	Either an incorrect security key is entered or a key is not entered at all. Locked drives remain locked and cannot be accessed.	Using iDRAC, verify the SEKM status of the server. Resolve any network communication issues with the KMS server. To retry exchanging the security key, restart the server.
Invalid security key or key id entered	An invalid security key of the drive is entered.	The security key or key ID of the drive does not match the drive information.	Ensure that the correct security key and key ID are entered to unlock the drive.
Unable to communicate with the external key manager.	Unable to communicate with the external key manager.	Either an incorrect security key is entered or a key is not entered at all. Locked drives remain locked and cannot be accessed.	Using iDRAC, verify the SEKM status of the server. Resolve any network communication issues with the KMS server. To retry exchanging the security key, restart the server.
Physical drive Erase Error	Unable to erase data on the hard drive: <PD Name>, Path <pathname>, Error Data <error Info>.	The drive may have an internal error or failed during the Erase operation.	Retry the operation. If the issue persists , contact your Technical Support team. If the data must be erased, then follow the DoD 5220.22-M Standard for Drive Erasure to physically destroy the storage device.
Controller temperature exceeded the warning threshold.	The controller temperature exceeded the threshold value. This may indicate inadequate server cooling. Currently switching to a low-performance mode.	The server fans may not functioning properly.	Check the health of server fans and replace if necessary. To improve cooling, increase or offset the fan speed.
Controller temperature exceeded a critical threshold.	The controller has been shut down because the server temperature reached the threshold value. This indicates that the server cooling is inadequate.	The server cooling fans may not be functioning properly.	Increase or offset the fan speed to improve cooling.

Table 19. Run-time issues and corrective actions (continued)

Description	Error Message	Probable Cause	Recommended Corrective Action
Unable to secure a virtual drive in the future.	Unable to secure the virtual drive <VD Name> in future because it is a non-SED.	One of the hard drives hosting the virtual drive is not SED-capable.	Replace the non-SED with an SED-capable one.
Discovery error	The drive cannot be discovered because of an SAS topology error: <Error Description>.	An error occurred during device discovery.	Remove all the newly added or nonfunctioning hardware. If the issue persists, contact your Technical Support team.
Safe Mode Error	The controller booted to the Safe mode because of critical issues.	The controller has an error during boot that requires user attention.	Correct the errors reported by the controller.
Firmware Update Failure	A validation issue occurred during the firmware update operation: <Issue Description>.	Failed to validate the incoming firmware image file.	Ensure that the firmware image used is correct and retry the operation. If the issue persists, contact your Technical Support team.
Firmware Update Failure	A programming issue occurred during the firmware update operation: <Issue Description>.	Programming of the incoming firmware image to the flash failed.	Ensure that the firmware image used is correct and retry the operation. If the issue persists, contact your Technical Support team.
Firmware Update Failure	Unable to complete the Online activate operation while preparing the controller.	The new firmware may require offline activation.	Perform a system reset to activate the firmware offline.
Security Key cleaned up.	The Escrow key ID <key ID> is cleaned up.	The security key that was saved in the memory for unlocking and importing the drive is erased. Any drive that uses this key which is not imported or rekeyed will be locked.	No action is required. If disks need to be imported then remove the disks, wait 10 seconds, and reinsert the disks. If using LKMs then provide the key to unlock the disks. If using SEKMs then wait for the key exchange to occur. Import the configuration after the disks are unlocked.
Drive Initialization Error	An initialization issue is detected in the physical drive <PD Name>.	An initialization issue is detected in the hard drive during the initialization or discovery of the drive. The drive may not be in a good state.	Remove or reinstall the drive. Check the health or SMART status of the hard drive. For NVMe drives, run the Recovery operation of the supported format.
Command timed out on hard drive	During backplane firmware update operation, the Command Timeout event is displayed in PERC.	The backplane may have been reset after updating the firmware, and therefore the commands that are sent by PERC to the backplane could be timed out.	No response action is required.
An I/O delay is observed when a virtual drive state changes.	An I/O delay is observed when a virtual drive state changes.	The controller has a delay time of 4 s for SAS/SATA and 8 s for NVMe drive removal processing to prevent unnecessary rebuild operations. This delay can introduce a short pause in I/O when the virtual drive state changes.	No response action is required.

Table 19. Run-time issues and corrective actions (continued)

Description	Error Message	Probable Cause	Recommended Corrective Action
Unable to complete the Drive MAKERS Authority disable operation during the securing operation.	Failed to disable the MAKERS authority on the drive.	An error occurred while securing the drive or the drive may not support MAKERS authority.	Retry the operation. If the issue persists contact support. f the issue persists, contact your Technical Support team.
Unable to complete the Drive MAKERS Authority enable operation during the erase operation.	Failed to enable the MAKERS authority on the drive.	An error occurred while erasing the drive or the drive may not support MAKERS authority.	Retry the operation. If the issue persists contact support. f the issue persists, contact your Technical Support team.
Drive firmware download port lock on reset operation that is failed during securing operation.	Failed to disable the firmware download port on the drive.	An error occurring during securing or drive may not support the firmware download port control setting.	Retry the operation. If the issue persists contact support. f the issue persists, contact your Technical Support team.
Drive firmware download port unlock operation failed during erase operation.	Failed to enable the firmware download port on the drive.	An error occurring during erase or Drive may not support the firmware download port control setting.	Retry the operation. If the issue persists contact support. f the issue persists, contact your Technical Support team.
Firmware Update Failure during back-to-back Firmware update operations from operating system.	Unknown Error: Operation failed	The controller could still be performing online activation in the background.	Ensure that you provide an interval of five minutes before attempting a back-to-back firmware update for online activation. The following message is displayed during online activation: `Online activation initiated to activate the downloaded firmware package.`

Application issues

The following table lists error messages, probable causes, and recommended response action to resolve the issues in general applications.

Table 20. General application issues and corrective actions

Description	Error Message	Probable Cause	Recommended Corrective Action
Reboot Required	Restart the server to complete the requested operation.	The operation was successful but requires a system restart to make the changes effective.	Restart the server to make the changes effective.
Reset Required	The operation is successful but reset the controller settings to make the changes effective.	The operation was successful but requires a controller reset to finish.	Reset the controller to make the changes effective.
Locked Disks Present	Unable to complete the operation because locked foreign configuration(s) is present.	The operation cannot be completed because some locked disks are present.	Remove the locked disks or cryptographically erase the locked disks to clear the security status, and then retry the operation.

Table 20. General application issues and corrective actions (continued)

Description	Error Message	Probable Cause	Recommended Corrective Action
Foreign Configuration	No foreign configuration is detected.	A foreign scan was run but no foreign configuration is present.	Ensure all foreign disks are present and drives are detected, then run the scan again
Low Memory	Insufficient controller memory to process the operation. Try again later.	Controller or system memory is low.	Close open applications and retry the operation. Contact Dell Support if the issue persists.
Application Compatibility	The command is unknown and not supported currently. The command: <commandName>.	The application may not be compatible with the controller firmware.	Update application and controller firmware to the latest version.
Controller Busy	The requested command is not supported because the controller firmware initialization is not complete.	The controller is still initializing from boot or reset.	Wait some time for the controller to boot then retry the operation.
Foreign Configuration	The foreign configuration cannot be imported because the configuration is not complete.	Some disks are missing from the foreign configuration.	Ensure that all foreign disks are present and drives are detected, then run the scan again.
Drive Security	The requested operation cannot be completed because the controller already has the security key.	The operation is not supported when the controller is in either the LKM or EKM mode.	Disable the drive security mode on the controller and retry the operation.
Drive Security	The requested operation cannot be completed because the security key is not present.	Operation is not supported when the controller is not in the LKM or EKM mode.	Disable the drive security mode on the controller and retry the operation.
Drive Security	The requested operation cannot be completed because the security key is invalid.	An incorrect Security Key or Key ID was entered when changing the key.	Enter the correct key and retry the operation.
Application Compatibility	The requested operation cannot be performed because of an internal error.	The application may not be compatible with the controller firmware.	Update application and controller firmware to the latest version.
Snapdump Error	The requested operation cannot be performed because of the existing snapdump. Clear all the snapdump and reinitiate the operation.	Some operations cannot be performed when there are debug log snapdumps present on the controller.	Download all snapdumps from the controller then clear the snapdumps and retry the operation.
Snapdump Error	The requested operation cannot be performed because no snapdump is present.	No snapdumps are present when trying to download a debug log.	Generate a new on-demand snapdump.
Snapdump Error	The requested operation cannot be performed because the on-demand snapdump is not allowed.	The controller does not support snapdump generation or is in a state where a snapdump cannot be generated such as bad DDR or is in a fault condition.	Ensure that the controller supports snapdump functionality. Check the controller's DDR is healthy and that the controller is not in a fault state.
Snapdump Error	The requested operation cannot be performed because there is an ongoing on-demand snapdump.	There is an ongoing snapdump being collected. On-demand snapdump can only be collected once every 10 minutes.	Retry the operation after some time.
Hardware Error	The requested operation cannot be completed because of a hardware error. The extended Status code: <statusCode>.	The controller may be in a faulty state, or the hardware may not be fully functional.	Retry the operation after some time. If the issue persists, contact the Dell Technical Support team.
Firmware Error	The requested operation cannot be completed because of a controller firmware error. The extended Status code: <statusCode>.	The controller may be in a faulty state or the has an internal error.	Retry the operation after some time. If the issue persists, contact the Dell Technical Support team.

Table 20. General application issues and corrective actions (continued)

Description	Error Message	Probable Cause	Recommended Corrective Action
Invalid ID	The requested operation cannot be completed because the ID is invalid. The extended Status code: <statusCode>.	The application is no longer in sync with the firmware, or the device is unavailable.	Retry the operation after some time. If the issue persists, contact the Dell Technical Support team.
Device not Found	The requested operation cannot be completed because the device is not detected. The extended Status code: <statusCode>.	The requested device is not available.	Ensure that the correct device ID is selected when running the commands. If the issue persists, contact the Dell Technical Support team.
Invalid Sequence Number	Check the configuration and retry the operation. The extended Status code: <statusCode>.	The application is no longer synchronized with the firmware.	Retry the operation after some time. If the issue persists, contact the Dell Technical Support team.
Invalid Argument	The requested command has invalid arguments. The extended Status code: <statusCode>.	The application is no longer compatible with the controller firmware or no longer in sync with the firmware.	Update the application and controller firmware to the latest version and retry the operation after some time. If the issue persists, contact the Dell Technical Support team.
Command Not supported for drive	The requested command is not supported for the drive. The extended Status code: <statusCode>.	The VD may be in a state where the specific operation is not supported or the command is not supported at all.	Ensure that the controller and drive support the feature. For performing erase operations on PDs, the drives must be in Unconfigured state.
Command Not supported for VD	The requested command is not supported for the virtual drive. The extended Status code: <statusCode>.	The VD may be in a state where the specific operation is not supported or the command is not supported at all.	Ensure that the controller and VD support the feature.
Command Not supported for Controller	The requested command is not supported. The extended Status code: <statusCode>.	The Controller or Configuration may be in a state where the specific operation is not supported or the command is not supported at all.	Confirm that Controller supports the feature. Ensure that the controller and VDs are healthy state.
Controller Busy	The requested command cannot be completed because the maximum limit is exceeded. The extended Status code: <statusCode>.	Too many commands are run on the controller.	Wait some time for some commands to complete then retry the operation.
Drive Mixing Violation	Mixing of the drive type is not supported. Add the same type of drives to perform the operation. The extended Status code: <statusCode>.	Mixing of some hard drive properties are not supported (Sector Size, Media Type, or Protocol).	Ensure that the same type of drives are being used for the operation.
Force Option Required	This command can be processed only with the Force option.	The command may be erasing data or causing a short performance degradation.	The Force parameter is required for any operation that may erase data or cause performance degradation. Select or add the option and retry running the command.
Configuration Present	This command can be processed only when no configuration is present.	The operation cannot be run while a configuration is present.	Clear the configuration from the controller or remove all the configured devices from the system.

Table 20. General application issues and corrective actions (continued)

Description	Error Message	Probable Cause	Recommended Corrective Action
Controller not responding	The controller firmware is not responding.	The controller may be busy processing other commands or has an issue.	Wait some time and try the operation again. If the issue persists, then try restarting the server.
PCI Error	The requested operation cannot be performed because of a PCI error.	A PCIe error has occurred.	N/A
Drive Error	The requested operation cannot be performed because of an error is detected on the drive.	An error occurred on the drive.	Wait some time then retry the operation. If the issue persists, contact the Dell Technical Support team.
Storage space on the drive is too less	The requested operation cannot be performed because storage space of the drive is too less.	The replaced drive has too less storage capacity for the array.	Replace the drive with a drive that has high storage capacity.
Drive does not support security	The requested operation cannot be performed because the drive is not security-capable.	The selected or replaced drive is not security-capable.	Replace the drive with a security-capable drive.
Drive security protocol mismatch	The requested operation cannot be performed because the security type of the drive is inappropriate.	The selected or replaced drive does not support the compatible security protocol.	Replace the drive with a drive that is compatible with the security protocol.
Drive Type Mismatch	The requested operation cannot be performed because the drive type is incorrect.	The selected or replaced drive does not match with the drives already in the array.	Ensure that the drive type matches either SAS, SATA, or NVMe; 512n or 4kn; or HDD or SSD.
Drive Sector Type mismatch	The requested operation cannot be performed because the block size of the drive does not match with other drives in the array.	The block size of the selected or replaced drive does not match with the drives already in the array	Ensure that the sector size of the drive matches 512n or 4kn.
Security not enabled	The requested operation cannot be performed because the security feature of the drive is not enabled.	The security mode of the controller is not enabled.	Enable security on the controller and retry the operation.
Wrong Enclosure	The command cannot be run because the drive is not a part of this enclosure.	An incorrect enclosure ID is entered.	Enter a correct enclosure ID in the command and retry the operation.
No SEKM capable Agent Detected	The requested operation cannot be performed because the Security External Key Management (SEKM) server is not detected.	iDRAC may not be compatible with SEKM or does not support the SEKM feature.	Update iDRAC and ensure that SEKM features are supported.
Command Not supported for Raid Level	The requested operation cannot be performed for the current RAID level.	The operation may not be supported for RAID levels such as running BGI or CC on a RAID 0 array.	Ensure that the operation is supported for the RAID array.
VD Wrong state	The requested operation cannot be performed because the VD is in a wrong state.	The VD may be in a degraded or offline state where the operation is unsupported.	Ensure that the VD is in a healthy state.
Too many retries	Unable to run the command because the maximum number of retries is exceeded.	The command is run for more than the maximum stipulated number of attempts.	Wait for some time and retry the operation. If the issue persists, contact the Dell Technical Support team.
Feature Not Supported	The requested operation cannot be performed because the feature is not supported.	The feature is not supported on the controller.	No response action is required because the feature is not supported.

Table 20. General application issues and corrective actions (continued)

Description	Error Message	Probable Cause	Recommended Corrective Action
Secure Devices Present	The requested operation cannot be completed because there are one or more secure drives present on this controller.	The operation cannot be performed because there are secured drives present on the controller.	By using the cryptographic erase operation, erase the secured drives or remove the drives from the server, and then retry the operation.
Operation disabled	The requested operation cannot be performed because the operation is currently disabled.	The operation cannot be performed because the feature is disabled or turned off.	Re-enable the feature and retry the operation.
Operation in Progress	The requested operation cannot be performed because some operation is currently in progress.	The operation cannot be performed because there is already another operation in progress.	Wait for the current operation to complete or stop the current operation.
Controller in SafeMode	The requested command is not supported because the controller is running in safe mode.	The controller is running in safe mode because of some internal issues.	Check the health of the controller and configuration and correct any errors
Controller Faulted	An issue is detected with the controller firmware.	An issue is detected in the controller which can result in an auto-reset or snapdump operation.	Save the snapdump that is generated by the controller and Contact the Dell Technical Support team.
Drive Security State error	The requested operation cannot be performed because of the current SED state of the drive.	The operation is not supported because the drive is in an unsupported security state. A drive may be secured when it should be unsecured.	Check the security state of the drive. Perform a cryptographic erase or secure operation as needed.
Auto-Configuration Enabled	The requested operation cannot be completed because of a secured auto-configure setting.	The auto-configuration option is enabled.	Change the auto-configuration setting to the default (Unconfigured) setting then retry the operation.

Security key errors

Secured foreign import errors

A foreign configuration is a RAID configuration that already exists on a replacement physical disk that you install in a system. A secured foreign configuration is a RAID configuration that was created under a different security key.

There are two scenarios in which a secured foreign import fails:

- **The security key authentication fails**—A virtual disk secured with a security key different from the current controller security key cannot be imported without authentication of the original security key used to secure them. Supply the correct security key to import the secured foreign configuration. If you have lost or forgotten the security key, the secured foreign disks remain locked (inaccessible) until the appropriate security key is entered or disks are erased.
- **The secured virtual disk is in an offline state after supplying the correct security key**—You must check to determine why the virtual disk failed and correct the problem.

Failure to select or configure non Self-Encrypting Disks non-SED

A virtual disk can be either secured or unsecured depending on how it was configured when created. In order to create a secured virtual disk, the controller must have a security key present and must contain SEDs only. In order to select/configure non-SED, you must create an unsecured virtual disk. You can create an unsecured virtual disk even if there is a security key. Select the **Secure VD** option as **No** in the **Create New VD** menu. For steps on how to create an unsecured virtual disk, see Create virtual disk and configure virtual disk parameters.

Failure to delete security key

A security key is used to lock or unlock access to a security-enabled component. This key is not utilized in the actual encryption of data. If a security key is present, both secured and unsecured virtual disks may exist.

To delete the security key, you must have a previously established security key present on the controller and there cannot be any configured secured disks. If there are configured secured virtual disks, remove or delete them.

Failure of Cryptographic Erase on encryption-capable physical disks

Cryptographic Erase is the process of securely erasing all data permanently on an encryption-capable physical disk and resetting the security attributes. It is used in scenarios such as deleting a foreign configuration in the event of a forgotten or lost security key, or unlocking a disk that had been previously locked.

ⓘ **NOTE:** PERC12 does not support unlocking disks from past generations or from third-party secured configurations.

You can perform Cryptographic Erase only on encryption-capable disks that are not hot spares and not configured as non-RAID or virtual disks. Ensure that the conditions are met. See Cryptographic erase.

General issues

PERC goes into Safe and Unresponsive state

Issue	After performing the rekey operation on the volume of a drive where the iLKM feature is enabled, and then restarting the server, the Red Screen of Death (RSOD) issue is observed. The PERC state becomes Safe Mode or Unresponsive.
Corrective Action:	Remove the locked drives from the server and restart the server. After restarting, install the locked drives again into the server.

Enclosure state is indicated as faulty instead of need attention

Issue	When a drive that cannot be accessed is removed, the enclosure state is indicated as faulty instead of Need Attention.
Corrective Action:	Expected behavior. No action is required.

Lifecycle log indicates drive number as unknown

Issue	After performing a cryptographic operation, Lifecycle log data displays the serial number of a drive as unknown. Also, PPID, product ID, revision, and serial number data are not displayed on the Lifecycle Controller user interface.
Corrective Action:	Expected behavior. Perform a Cold Reboot operation on the server.

An NVMe drive is not indicated as unsupported when EEDP is enabled

Issue	An NVMe drive on which the EEDP feature is enabled is not indicated as unsupported when the PI type is set to 1, 2, or 3.
Corrective Action:	Expected behavior. No action is required. Dell does not support NVMe drives on which the EEDP feature is enabled.

Enclosure is not functional when an NVMe drives without a namespace is inserted

Issue An enclosure becomes non-funcational when an NVMe drive without a namespace is inserted.

Corrective Action: Expected behavior. Remove the NVMe drive that does not have a namespace.

perccli2 commands and OS DUPs must have the controller host driver 8.0.0.69.0 for proper functioning

Issue The perccli2 commands and operating system DUPs require the controller host driver minimum version of 8.0.0.69.0 for proper functioning. They do not work on inbox drivers earlier than 8.0.0.69.0.

Corrective Action: Expected behavior. No action is required.

PERC card has yellow bang in Windows operating system device manager

Issue: The device is displayed in **Device Manager** but has a yellow exclamation mark.

Corrective Action: Reinstall the driver. For more information on reinstalling drivers, see Driver support for PERC H365i Adapter and PERC H365i Front DC-MHS controller cards.

PERC card not seen in operating systems

Issue: The device does not appear in the **Device Manager**.

Corrective Action: Power off the system and reseat the controller.

Unlocked drives if not imported appear as locked

Issue: If drives are unlocked but not imported, the drives appear as locked even after the controller is reset.

Corrective Action: Remove the drives from the system.

Physical disk issues

Enclosure is not functional when an NVMe drives without a namespace is inserted

Issue An enclosure becomes non-funcational when an NVMe drive without a namespace is inserted.

Corrective Action: Expected behavior. Remove the NVMe drive that does not have a namespace.

An NVMe drive is not indicated as unsupported when EEDP is enabled

Issue An NVMe drive on which the EEDP feature is enabled is not indicated as unsupported when the PI type is set to 1, 2, or 3.

Corrective Action: Expected behavior. No action is required. Dell does not support NVMe drives on which the EEDP feature is enabled.

Lifecycle log indicates drive number as unknown

Issue After performing a cryptographic operation, Lifecycle log data displays the serial number of a drive as unknown. Also, PPID, product ID, revision, and serial number data are not displayed on the Lifecycle Controller user interface.

Corrective Action: Expected behavior. Perform a Cold Reboot operation on the server.

Unconfigured drives are not listed in the OS or Hardware Diagnostics

Issue Unconfigured drives (ready-state drives) are not listed in the OS or Hardware Diagnostics of Lifecycle Controller.

Corrective Action: Expected behavior. No action is required.

Physical disk in failed state

Issue: One of the physical disks in the disk array is in the failed state.

Corrective Action: Update the PERC cards to the latest firmware available on the support site and replace the drive.

The PDR6 Error and Event message is saved in the log data when a new drive is inserted

Issue: The PDR6 Error and Event message is saved in the log data when a new drive is inserted.

Probable Cause: When the auto rebuild feature is enabled and the drive is inserted, then the drive status becomes Offline and then Rebuilding.

Corrective Action: Expected behavior. No action is required because this behavior does not imply that the drive has permanently become offline.

Unable to rebuild a fault tolerant virtual disk

Issue: Cannot rebuild a fault tolerant virtual disk. For more information, see the alert log for virtual disks.

Probable Cause: The replacement disk is too small or not compatible with the virtual disk.

Corrective Action: Replace the failed disk with a compatible good physical disk with equal or greater capacity.

An NVMe drive is indicated as faulty when moving the drive to new backplane using hot-insertion

Issue:	When moving an NMVe drive to a different backplane slot, if the NVMe drive is hot-removed and hot-inserted in a different slot too quickly, then the drive may be indicated as faulty.
Probable Cause:	NVMe drive is moved between slots too quickly.
Corrective Action:	Wait at least 8 seconds after a hot-pull event before re-inserting the drive in an alternate slot.

Fatal error or data corruption reported

Issue:	Fatal error(s) or data corruption(s) are reported when accessing virtual disks.
Corrective Action:	Contact your Technical Support team.

Multiple disks are inaccessible

Issue:	Multiple disks are simultaneously inaccessible.
Probable Cause:	Multiple physical disk errors in a single array typically indicate a failure in cabling or connection and could involve the loss of data.
Corrective Action:	You can recover the virtual disk after multiple physical disks become simultaneously inaccessible. Perform the following steps to recover the virtual disk:

⚠ **CAUTION: Follow the safety precautions to prevent electrostatic discharge.**

1. Turn off the system, check cable connections, and reseat physical disks.
2. Ensure that all the disks are present in the enclosure.
3. Turn on the system and enter the **HII Configuration Utility**.
4. Import the foreign configuration.
5. Press <F> at the prompt to import the configuration, or press <C> to enter the **HII Configuration Utility** and either import or clear the foreign configuration.

If the virtual disk is redundant and transitioned to **Degraded** state before going **Offline**, a rebuild operation starts automatically after the configuration is imported. If the virtual disk has gone directly to the **Offline** state due to a cable pull or power loss situation, the virtual disk is imported in its **Optimal** state without a rebuild occurring.

ⓘ **NOTE:** You can use the **HII Configuration Utility** or Dell OpenManage storage management application to perform a manual rebuild of multiple physical disks.

Rebuilding data for a failed physical disk

Issue:	Rebuilding data for a physical disk that is in a failed state.
Probable Cause:	Physical disk is failed or removed.
Corrective Action:	If you have configured hot-spares, the PERC card automatically tries to use one of the hot-spares to rebuild a physical disk that is in a failed state. Manual rebuild is necessary if no hot-spares with enough capacity to rebuild the failed physical disks are available. You must insert a physical disk with enough storage in the subsystem before rebuilding the physical disk.

ⓘ **NOTE:** You can use the **HII Configuration Utility** or Dell OpenManage storage management application to perform a manual rebuild of an individual physical disk.

Virtual disk fails during rebuild using a global hot-spare

Issue: A virtual disk fails during rebuild while using a global hot spare.

Probable Cause: One or more disks in the virtual disks fails or is disconnected while the rebuild is in progress.

Corrective Action: No action is required. The global hot spare reverts to **Hot spare** state and the virtual disk is in **Failed** state.

Physical disk takes a long time to rebuild

Issue: A physical disk is taking longer than expected to rebuild.

Description: A physical disk takes longer to rebuild when under high I/O stress. There is only one rebuild I/O operation for every five host I/O operations.

Corrective Action: If possible, reduce I/O stress on the physical disk or increase the value of rebuild rate controller parameter.

Drive removal and insertion in the same slot generates a foreign configuration event

Issue: When a drive which is part of a virtual disk is removed and reinserted into the same slot the drive goes through a transient state of being foreign for a short period of time before rebuilding.

Description: This transient state could be reported as an event in management applications as **A foreign configuration was detected on RAID Controller is SL x**, where x is the slot of the RAID controller.

Corrective Action: No action is required on the foreign configuration state of the drive as it is transient and the controller handles the event automatically.

SMART errors

SMART monitors the internal performance of all motors, heads, and physical disk electronics and detects predictable physical disk failures.

NOTE: For information about SMART errors' reports that could indicate hardware failure, see the *Dell OpenManage Storage Management User's Guide* available at OpenManage Manuals.

SMART error detected on a non–RAID disk

Issue: A SMART error is detected on a non–RAID disk.

Corrective Action: Perform the following steps:

1. Back up your data.
2. Replace the affected physical disk with a new physical disk of equal or higher capacity.
3. Restore from the backup.

SMART error detected on a hard drive in a non–redundant virtual disk

Issue: A SMART error is detected on a hard drive in a non–redundant virtual disk.

Corrective Action: Perform the following steps:

1. Back up your data.

2. Use **Replace Member** to replace the disk manually.
3. Replace the affected hard drive with a new hard drive of equal or higher capacity.
4. Restore from the backup.

SMART error detected on a hard drive in a redundant virtual disk

Issue: A SMART error is detected on a hard drive in a redundant virtual disk.

Corrective Action: Perform the following steps:

1. Back up your data.
2. Force the hard drive offline.

> **NOTE:** If a hot spare is present, the rebuild starts with the hot spare after the disk is forced offline.

3. Replace the disk with a new hard drive of equal or higher capacity.
4. Perform the **Replace Member** operation.

> **NOTE:** The **Replace Member** operation allows you to copy data from a source hard drive of a virtual disk to a target hard drive that is not a part of the virtual disk.

Replace member errors

> **NOTE:** For more information about the **Replace Member** features, see Configure hot spare drives.

Source disk fails during replace member operation

Issue: The source disk fails during the **Replace Member** operation and the **Replace Member** operation stops due to the source physical disk error.

Probable Cause: Physical disk failure or physical disk is removed or disconnected.

Corrective Action: No action required. If the virtual disk can tolerate disk failure, and the source data is available from other disks in the virtual disk, the rebuild begins automatically on the target disk, using the data from the other disks, if the virtual disk cannot tolerate the failure, the virtual disk goes to offline state and the replace member operation is stopped.

Target disk fails during replace member operation

Issue: The target disk failure reported during the **Replace Member** operation, and the **Replace Member** operation stops.

Probable Cause: Physical disk failure or physical disk is removed or disconnected.

Corrective Action: It is recommended that you replace or check the target drive, and restart the **Replace Member** operation or perform the operation on a different target drive.

A member disk failure is reported in the virtual disk which undergoes replace member operation

Issue: The source and the target drive which is part of **Replace Member** operation are online, while a different drive which is a member of the virtual drive reports a failure.

Probable Cause: Physical disk failure or physical disk is removed or disconnected.

Corrective Action: A rebuild starts if there any hot-spares configured or you may replace the failed drive. The **Replace Member** operation continues as far as the source virtual disk can tolerate the drive failure. If the source virtual disk fails, the **Replace Member** is stopped, otherwise the virtual disk continues to be in degraded state.

Linux operating system errors

Virtual disk policy is assumed as write-through

Error:

```
<Date:Time> <HostName> kernel: sdb: asking for cache data
failed<Date:Time> <HostName> kernel: sdb: assuming drive cache: write
through
```

Corrective Action: The error message is displayed when the Linux Small Computer System Interface (SCSI) mid-layer asks for physical disk cache settings. The controller firmware manages the virtual disk cache settings on a per controller and a per virtual disk basis, so the firmware does not respond to this command. The Linux SCSI mid-layer assumes that the virtual disk's cache policy is **Write-Through**. SDB is the device node for a virtual disk. This value changes for each virtual disk. Except for this message, there is no effect of this behavior on normal operation. The cache policy of the virtual disk and the I/O throughput are not affected by this message. The cache policy settings for the PERC SAS RAID system remain unchanged.

Unable to register SCSI device

Error:

```
smartd[smartd[2338] Device: /dev/sda, Bad IEC (SMART) mode page, err=-5,
skip device smartd[2338] Unable to register SCSI device /dev/sda at line
1 of file /etc/smartd.conf.
```

Corrective Action: This is a known issue. An unsupported command is entered through the user application. User applications attempt to direct Command Descriptor Blocks to RAID volumes. The error message does not affect the feature functionality. The `Mode Sense/Select` command is supported by firmware on the controller. However, the Linux kernel **daemon** issues the command to the virtual disk instead of to the driver **IOCTL** node. This action is not supported.

Drive indicator codes

The LEDs on the drive carrier indicates the state of each drive. Each drive carrier has two LEDs: an activity LED (green) and a status LED (bicolor, green/amber). The activity LED blinks whenever the drive is accessed.

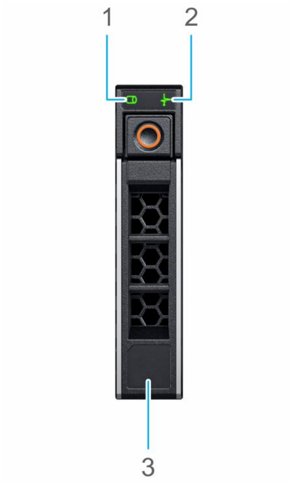


Figure 7. Drive indicators

1. Drive activity LED indicator
2. Drive status LED indicator
3. Drive capacity label

If the drive is in the Advanced Host Controller Interface (AHCI) mode, the status LED indicator does not power on. Drive status indicator behavior is managed by Storage Spaces Direct. Not all drive status indicators may be used.

> **NOTE:** For information about the Drive LED indicator codes in an MD24XX series enclosure, see the Dell PowerVault MD24XX Direct-Attach Storage for PowerEdge Servers Owner's Manual available on the support site.

Table 21. Drive indicator codes

Drive status indicator code	Condition
Blinks green twice per second	The drive is being identified or preparing for removal
Off	The drive is ready for removal **NOTE:** The drive status indicator remains off until all drives are initialized after the system is powered on. Drives are not ready for removal during this time.
Blinks green, amber, and then powers off	There is an expected drive failure
Blinks amber four times per second	The drive has failed or faulted or not detected.
Blinks green slowly	The drive is rebuilding
Solid green	The drive is online
Blinks green for three seconds, amber for three seconds, and then powers off after six seconds	The rebuild has stopped

The AutoSecure feature is not supported

Issue The AutoSecure feature of iDRAC is not supported by PERC 12 and HBA465 controllers.

Corrective Action: Expected behavior. No action is required.

HII error messages

Unhealthy Status of the drivers

Error: `One or more boot driver(s) have reported issues. Check the Driver Health Menu in Boot Manager for details.`

Probable Cause: This message might indicate that the cables are not connected, the disks might be missing, or the UEFI driver might require configuration changes.

Corrective Action:

1. Check if the cables are connected properly, or replace missing hard drives, if any and then restart the system.
2. Press any key to load the driver health manager to display the configurations. The Driver Health Manager displays the driver(s), which requires configuration.
3. Alternately, if the UEFI driver requires configuration, press any key to load the Configuration Utility.

Rebuilding a drive during full initialization

Issue: Automatic rebuild of drives is disabled for virtual disk during full initialization.

Corrective Action: After full initialization the drive will automatically start its rebuild on its corresponding virtual disk.

11

Appendix—RAID description

RAID is a group of independent physical disks that provides high performance by increasing the number of disks used for saving and accessing data.

△ **CAUTION: In the event of a physical disk failure, a RAID 0 virtual disk fails, resulting in data loss.**

A RAID disk subsystem offers the following benefits:

- Improved I/O performance and data availability.
- Improved data throughput because several disks are accessed simultaneously. The physical disk group appears either as a single storage unit or multiple logical units to the host system.
- Improved data storage availability and fault tolerance. Data loss caused by a physical disk failure can be recovered by rebuilding missing data from the remaining physical disks containing data or parity.

Topics:

Summary of RAID levels

Following is a list of the RAID levels supported by the PERC12 series of cards:

- RAID 0 uses disk striping to provide high data throughput, especially for large files in an environment that requires no data redundancy.
- RAID 1 uses disk mirroring so that data written to one physical disk is simultaneously written to another physical disk. RAID 1 is good for small databases or other applications that require small capacity and complete data redundancy.
- RAID 5 uses disk striping and parity data across all physical disks (distributed parity) to provide high data throughput and data redundancy, especially for small random access.
- RAID 6 is an extension of RAID 5 and uses an additional parity block. RAID 6 uses block-level striping with two parity blocks distributed across all member disks. RAID 6 provides protection against double disk failures, and failures while a single disk is rebuilding. If you are using only one array, deploying RAID 6 is more effective than deploying a hot spare disk.
- RAID 10 is a combination of RAID 0 and RAID 1, uses disk striping across mirrored disks. It provides high data throughput and complete data redundancy.
- RAID 50 is a combination of RAID 0 and RAID 5 where a RAID 0 array is striped across RAID 5 elements. RAID 50 requires at least six disks.
- RAID 60 is a combination of RAID 0 and RAID 6 where a RAID 0 array is striped across RAID 6 elements. RAID 60 requires at least eight disks.

The following table lists the minimum and maximum disks supported on each RAID levels.

Table 22. Minimum and maximum disks supported on each RAID levels

RAID Level	Minimum disk	Maximum disk
0	1	32
1	2	2
5	3	32
6	4	32
10	4	240
50	6	240
60	8	240

RAID 10 configuration

Any RAID 10 volume that has more than 32 drives require spanning. Each span can contain up to 32 drives. Drives must be distributed evenly across all the spans with each span containing an even number of drives.

NOTE: Spans in a RAID 10 volume are only supported if spans are even. Uneven spanned RAID 10 cannot be imported from previous controller generations.

The following table shows the RAID 10 configurations.

Table 23. RAID 10 configurations

Disk or span count	RAID 10 capable	Disk or span count	RAID 10 capable	Disk or span count	RAID 10 capable	Disk or span count	RAID 10 capable
4 (1)	Yes	64 (2)	Yes	124	No	184	No
6 (1)	Yes	66 (3)	Yes	126 (7)	Yes	186	No
8 (1)	Yes	68	No	128 (4)	Yes	188	No
10 (1)	Yes	70 (5)	Yes	130 (5)	Yes	190	No
12 (1)	Yes	72 (3)	Yes	132 (6)	Yes	192 (6)	Yes
14 (1)	Yes	74	No	134	No	194	No
16 (1)	Yes	76	No	136	No	196 (7)	Yes
18 (1)	Yes	78 (3)	Yes	138	No	198	No
20 (1)	Yes	80 (4)	Yes	140 (5)	Yes	200	No
22 (1)	Yes	82	No	142	No	202	No
24 (1)	Yes	84 (6)	Yes	144	Yes	204	No
26 (1)	Yes	86	No	146	No	206	No
28 (1)	Yes	88 (4)	Yes	148	No	208 (8)	Yes
30 (1)	Yes	90 (3)	Yes	150 (5)	Yes	210 (7)	Yes
32 (1)	Yes	92	No	152	No	212	No
34	No	94	No	154 (7)	Yes	214	No
36 (2)	Yes	96 (3)	Yes	156 (6)	Yes	216	No
38	No	98 (7)	Yes	158	No	218	No
40 (2)	Yes	100 (5)	Yes	160 (5)	Yes	220	No
42 (2)	Yes	102	No	162	No	222	No
44 (2)	Yes	104 (4)	Yes	164	No	224 (8)	Yes
46	No	106	No	166	No	226	No
48 (2)	Yes	108 (6)	Yes	168 (6)	Yes	228	No
50 (2)	Yes	110 (5)	Yes	170	No	230	No
52 (2)	Yes	112 (4)	Yes	172	No	232	No
54 (2)	Yes	114	No	174	No	234	No
56 (2)	Yes	116	No	176 (8)	Yes	236	No
58	No	118	No	178	No	238	No
60 (2)	Yes	120 (4)	Yes	180 (6)	Yes	240 (8)	Yes
62	No	122	No	182 (7)	Yes	-	-

RAID terminology

Disk striping

Disk striping allows you to write data across multiple physical disks instead of just one physical disk. Disk striping involves partitioning each physical disk storage space in stripes of the following sizes: 64 KB, 128 KB, 256 KB, 512 KB, and 1 MB. The stripes are interleaved in a repeated sequential manner. The part of the stripe on a single physical disk is called a stripe element.

For example, in a four-disk system using only disk striping (used in RAID 0), segment 1 is written to disk 1, segment 2 is written to disk 2, and so on. Disk striping enhances performance because multiple physical disks are accessed simultaneously, but disk striping does not provide data redundancy.

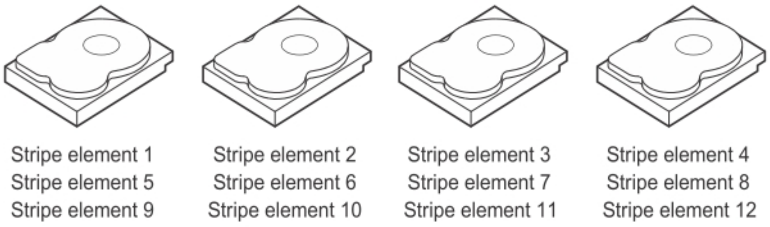


Figure 8. Example of disk striping (RAID 0)

Disk mirroring

With mirroring (used in RAID 1), data written to one disk is simultaneously written to another disk. If one disk fails, the contents of the other disk can be used to run the system and rebuild the failed physical disk. The primary advantage of disk mirroring is that it provides complete data redundancy. Both disks contain the same data at all times. Either of the physical disks can act as the operational physical disk.

Disk mirroring provides complete redundancy, but is an expensive option because each physical disk in the system must be duplicated.

NOTE: Mirrored physical disks improve read performance by read load balance.

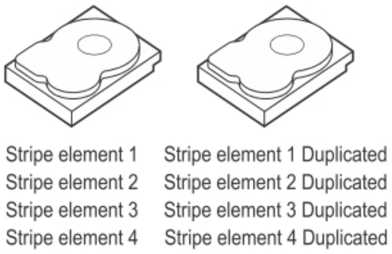

Stripe element 1
Stripe element 2
Stripe element 3
Stripe element 4
Stripe element 1 Duplicated
Stripe element 2 Duplicated
Stripe element 3 Duplicated
Stripe element 4 Duplicated

Figure 9. Example of Disk Mirroring (RAID 1)

Spanned RAID levels

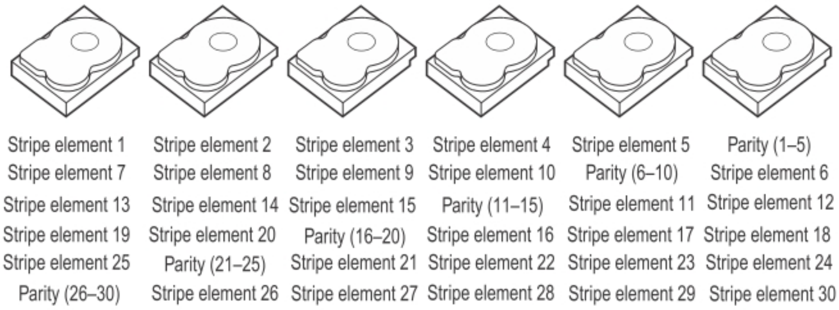
Spanning is a term used to describe the way in which RAID levels 10, 50, and 60 are constructed from multiple sets of basic, or simple RAID levels. For example, a RAID 10 has multiple sets of RAID 1 arrays where each RAID 1 set is considered a span. Data is then striped (RAID 0) across the RAID 1 spans to create a RAID 10 virtual disk. Similarly, RAID 50 and RAID 60 combine multiple sets of RAID 5 or RAID 6 respectively with striping.

Parity data

Parity data is redundant data that is generated to provide fault tolerance within certain RAID levels. In the event of a disk failure, the parity data can be used by the controller to regenerate user data. Parity data is present for RAID 5, 6, 50, and 60.

The parity data is distributed across all the physical disks in the system. If a single physical disk fails, it can be rebuilt from the parity and the data on the remaining physical disks. RAID level 5 combines distributed parity with disk striping. Parity provides redundancy for one physical disk failure without duplicating the contents of the entire physical disks.

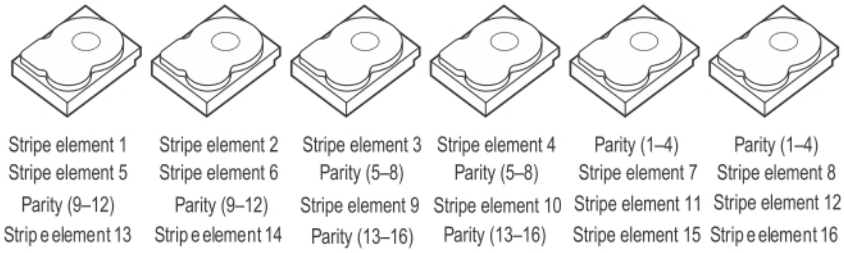
RAID 6 combines dual distributed parity with disk striping. This level of parity allows for two disk failures without duplicating the contents of entire physical disks.



Stripe element 1	Stripe element 2	Stripe element 3	Stripe element 4	Stripe element 5	Parity (1–5)
Stripe element 7	Stripe element 8	Stripe element 9	Stripe element 10	Parity (6–10)	Stripe element 6
Stripe element 13	Stripe element 14	Stripe element 15	Parity (11–15)	Stripe element 11	Stripe element 12
Stripe element 19	Stripe element 20	Parity (16–20)	Stripe element 16	Stripe element 17	Stripe element 18
Stripe element 25	Parity (21–25)	Stripe element 21	Stripe element 22	Stripe element 23	Stripe element 24
Parity (26–30)	Stripe element 26	Stripe element 27	Stripe element 28	Stripe element 29	Stripe element 30

Figure 10. Example of Distributed Parity (RAID 5)

NOTE: Parity is distributed across multiple physical disks in the disk group.



Stripe element 1	Stripe element 2	Stripe element 3	Stripe element 4	Parity (1–4)	Parity (1–4)
Stripe element 5	Stripe element 6	Parity (5–8)	Parity (5–8)	Stripe element 7	Stripe element 8
Parity (9–12)	Parity (9–12)	Stripe element 9	Stripe element 10	Stripe element 11	Stripe element 12
Stripe element 13	Stripe element 14	Parity (13–16)	Parity (13–16)	Stripe element 15	Stripe element 16

Figure 11. Example of Dual Distributed Parity (RAID 6)

NOTE: Parity is distributed across all disks in the array.

12

Getting help

Topics:

Recycling or End-of-Life service information

Take back and recycling services are offered for this product in certain countries. If you want to dispose of system components, visit the Dell Recycle Worldwide website and select the relevant country.

Contacting Dell

Dell provides online and telephone based support and service options. If you do not have an active internet connection, you can find Dell contact information on your purchase invoice, packing slip, bill or Dell product catalog. The availability of services varies depending on the country and product, and some services may not be available in your area. To contact Dell for sales, technical assistance, or customer service issues:

Steps

1. Visit the support site.
2. Select your country from the drop-down menu on the lower right corner of the page.
3. For customized support:
   a. Enter the system Service Tag in the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** field.
   b. Click **Submit**.
      The support page that lists the various support categories is displayed.
4. For general support:
   a. Select your product category.
   b. Select your product segment.
   c. Select your product.
      The support page that lists the various support categories is displayed.
5. For contact details of Dell Global Technical Support:
   a. Click **Contact Technical Support**.
   b. The **Contact Technical Support** page is displayed with details to call, chat, or e-mail the Dell Global Technical Support team.

Locating the Express Service Code and Service Tag

The unique Express Service Code and Service Tag is used to identify the system.

The information tag is located on the front of the system rear of the system that includes system information such as Service Tag, Express Service Code, Manufacture date, NIC, MAC address, QRL label, and so on. If you have opted for the secure default access to iDRAC, the Information tag also contains the iDRAC secure default password. If you have opted for iDRAC Quick Sync 2, the Information tag also contains the OpenManage Mobile (OMM) label, where administrators can configure, monitor, and troubleshoot the PowerEdge servers.

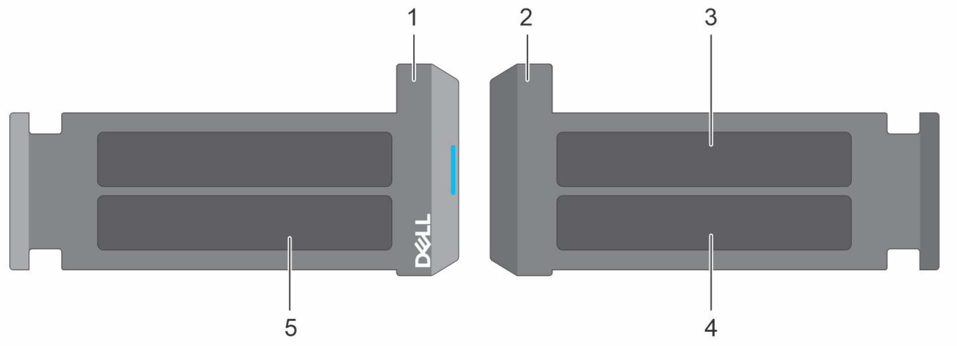


Figure 12. Locating the Express Service Code and Service tag

1. Information tag (front view)
2. Information tag (back view)
3. OpenManage Mobile (OMM) label
4. iDRAC MAC address and iDRAC secure password label
5. Service Tag, Express Service Code, QRL label

The Mini Enterprise Service Tag (MEST) label is located on the rear of the system that includes Service Tag (ST), Express Service Code (Exp Svc Code), and Manufacture Date (Mfg. Date). The Exp Svc Code is used by Dell to route support calls to the appropriate personnel.

Alternatively, the Service Tag information is located on a label on left wall of the chassis.

13

Documentation resources

This section provides information about the documentation resources for your system.

To view the document that is listed in the documentation resources table:

- From the Dell support site:
  1. Click the documentation link that is provided in the Location column in the table.
  2. Click the required product or product version.

     NOTE: To locate the product name and model, see the front of your system.

  3. On the Product Support page, click **Manuals & documents**.
- Using search engines:
  - Type the name and version of the document in the search box.

Table 24. Other documentation resources for your system

Task	Document	Location
Setting up your system	For more information about installing and securing the system into a rack, see the Rail Installation Guide included with your rail solution. For information about setting up your system, see the *Getting Started Guide* document that is shipped with your system.	PowerEdge Server Manuals
Configuring your system	For information about the iDRAC features, configuring and logging in to iDRAC, and managing your system remotely, see the Integrated Dell Remote Access Controller User's Guide. For information about understanding Remote Access Controller Admin (RACADM) subcommands and supported RACADM interfaces, see the RACADM CLI Guide for iDRAC. For information about Redfish and its protocol, supported schema, and Redfish Eventing implemented in iDRAC, see the Redfish API Guide. For information about iDRAC property database group and object descriptions, see the Attribute Registry Guide. For information about Intel QuickAssist Technology, see the Integrated Dell Remote Access Controller User's Guide.	PowerEdge Server Manuals
	For information about earlier versions of the iDRAC documents. To identify the version of iDRAC available on your system, on the iDRAC web interface, click **?** > **About**.	iDRAC Manuals

Table 24. Other documentation resources for your system (continued)

Task	Document	Location
	For information about updating drivers and firmware, see the Methods to download firmware and drivers section in this document.	Drivers