Hewlett Packard Enterprise

HPE MR Storage Administrator User Guide

Abstract

This document includes feature, installation, and configuration information for HPE MR Storage Administrator users. It is intended for users with a good working knowledge of storage hardware and configuration of logical drives and arrays. Hewlett Packard Enterprise assumes you are qualified in the servicing of computer equipment and trained in recognizing hazards in products with hazardous energy levels.

Part Number: MR-Stor-Admin-UG111-59CS
Published: September 2025
Edition: 1.10

For a comprehensive list of changes to this document, see the Revision History.

Table of Contents

HPE MR Storage Administrator Application Overview

The HPE MR Storage Administrator application is a web-based application that lets you monitor, maintain, troubleshoot, and configure MegaRAID products. The HPE MR Storage Administrator graphical user interface (GUI) helps you to view, create, and manage storage configurations.

- **Monitoring and Configuring**: The HPE MR Storage Administrator application lets you monitor the controllers and configure the drives on the controller.

  The application displays the status of the controller cards, volumes, and drives on the controller. The device status icons are displayed on their respective pages to notify you in case of drive failures and other events that require your immediate attention. Real-time email notifications on the status of the server are sent based on your alert settings. The system errors and events are recorded and displayed in an event log file. Additionally, you can also import or clear foreign configurations.
- **Maintaining**: Using the HPE MR Storage Administrator application, you can perform system maintenance tasks, such as updating the controller firmware.
- **Troubleshooting**: The HPE MR Storage Administrator application displays information that is related to drive failures, device failures, and so on.

  The application also provides recommendations and displays contextual links, helping you to easily locate drives and devices that have issues and troubleshoot them. In addition, you can download a complete report of all the devices and their configurations, properties, and settings and send it to the support teams for further analysis and troubleshooting.

Support Matrix

The following table provides the support requirements for the HPE MR Storage Administrator application.

Table 1: Hardware and Software Support Matrix

Support	Version/Flavors
Supported Controllers	• HPE MR416i-p Gen11 • HPE MR416i-o Gen11 • HPE MR216i-p Gen11 • HPE MR216i-o Gen11 • HPE MR408i-o Gen11 • HPE MR416i-p Gen 10+ • HPE MR416i-a Gen 10+ • HPE MR216i-p Gen 10+ • HPE MR216i-a Gen 10+ • HPE Smart Array P824i-p MegaRAID Gen10 Controller
Supported operating systems	
Microsoft	• Microsoft Hyper-V Server 2022 • Microsoft Hyper-V Server 2019 • Microsoft Hyper-V Server 2016 • Microsoft Windows Server 2016 (Datacenter) • Microsoft Windows Server 2016 (Standard) • Microsoft Windows Server 2016 (Essentials) • Microsoft Hyper-V Server 2012 R2 • Microsoft Windows Server 2016 RS3 • Microsoft Windows Server 2012 R2 (Foundation) • Microsoft Windows Server 2012 R2 (Essentials) • Microsoft Windows Server 2012 R2 (Standard) • Microsoft Windows Server 2012 R2 (Datacenter)

Support	Version/Flavors
Linux	• Red Hat Enterprise Linux 9.1 • Red Hat Enterprise Linux 9 • Red Hat Enterprise Linux 8.7 • Red Hat Enterprise Linux 8.6 • Red Hat Enterprise Linux 8.5 • Red Hat Enterprise Linux 8.4 • Red Hat Enterprise Linux 8.3 • Red Hat Enterprise Linux 8.2 • Red Hat Enterprise Linux 8.1 • Red Hat Enterprise Linux 7.8 • Red Hat Enterprise Linux 7.8 • Red Hat Enterprise Linux 7.7 • SUSE Linux Enterprise Server 15 SP5 • SUSE Linux Enterprise Server 15 SP4 • SUSE Linux Enterprise Server 15 SP3 • SUSE Linux Enterprise Server 15 SP2 • SUSE Linux Enterprise Server 15 SP1 • SUSE Linux Enterprise Server 12 SP5 • SUSE Linux Enterprise Server 12 SP4 • SUSE Linux Enterprise Server 12 SP3
Ubuntu	• Ubuntu 22.04 LTS • Ubuntu 20.04 LTS • Ubuntu 18.04 LTS
openEuler	• openEuler 20.03 LTS
Supported web browsers	• Windows Internet Explorer 9.0 and later • Mozilla Firefox version 9.0 and later • Google Chrome version 16.0 and later
Supported networks	• Internet Protocol versions 4 and 6 • Network Address Translation • Domain • HTTP, HTTPS

HPE MR Storage Administrator Feature Support Matrix

The following tables outline the feature support for HPE Smart Array MegaRAID controllers with respect to software features and firmware features.

Table 2: MegaRAID Firmware Feature Support Matrix

Feature Name	MegaRAID Firmware
RAID level	RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50, and RAID 60
Maximum drives	240
Maximum spans	8
Maximum volumes	240
Maximum media errors	256
Drive-mixing support	No.
Strip size support	64 KB, 128 KB, 256 KB, 512 KB, and 1024 KB
Maximum volumes per array	64
Multipath	No
Controller reset support	Yes

Table 3: Software Feature Support

Feature Name	Description
Server Dashboard	The Server Dashboard is the default landing page in the application. The Server Dashboard displays the overall summary of the server and the devices attached to it. You can troubleshoot, configure, maintain, and monitor the controllers from the Server Dashboard. See Server Dashboard for more information.
Controller Dashboard	The Controller Dashboard lets you perform controller related actions and view all the information pertaining to a controller. See Controller Dashboard for more information
Simple Configuration	The Simple Configuration option is the quickest and easiest way to create a new storage configuration. When you select Simple Configuration mode, the system creates the best configuration possible using the available drives. See Creating a New Storage Configuration Using the Simple Configuration Option for more information.
Advanced Configuration	The Advanced Configuration option provides an easy way to create a new storage configuration. The Advanced Configuration option gives you greater flexibility than Simple Configuration because you can select the physical drive and volume parameters when you create a volume. In addition, you can use the Advanced Configuration option to create spanned arrays. See Creating a New Storage Configuration Using the Advanced Configuration Option for more information.
Foreign Configuration (Import/ Clear)	A *foreign configuration* is a RAID configuration that already exists on a replacement set of drives that you install in a storage system. You can use the application to import the foreign configuration to the controller or clear the foreign configuration so that you can create a new configuration using these drives. See Importing or Clearing Foreign Configurations for more information.
Clear Configuration	The Clear Configuration feature lets you clear all existing configurations on a selected controller. See Clearing the Configuration for more information.
Update Firmware	The Update Firmware feature lets you update the controller firmware. See Updating the Controller Firmware for more information.

Feature Name	Description
Online Firmware Update	The Online Firmware Update feature lets you update the controller firmware. See Updating the Controller Firmware for more information.
Controller Operations	
Setting Consistency Check Properties	The Consistency Check operation verifies the correctness of the data in volumes that use RAID levels 1, 5, 6, 10, 50, and 60, configurations. For example, in a system with parity, checking the consistency means calculating the data on one drive and comparing the results to the contents of the parity drive. See Running Consistency Checks for more information.
Scheduling Consistency Check	The Scheduling Consistency Check feature lets you periodically run a consistency check on fault-tolerant volumes. See Scheduling a Consistency Check Operation for more information.
Setting Patrol Read Properties	A Patrol Read operation periodically verifies all sectors of the drives connected to a controller, including the system reserved area in the RAID configured drives. You can run a Patrol Read operation for all RAID levels and for all spare drives. A Patrol Read operation is initiated only when the controller is idle for a defined period and has no other background activities. See Setting the Patrol Read Properties for more information.
Starting Patrol Read	A Starting Patrol Read operation lets you start a patrol read operation. See Starting a Patrol Read Operation for more information.
Stopping Patrol Read	A Stopping Patrol Read operation lets you stop an already started patrol read operation. See Stopping a Patrol Read Operation for more information.
Managing Link Speed	A Managing Link Speed operation lets you change the link speed between the controller and an expander or between the controller and a drive that is directly connected to the controller. See Managing SAS Storage Link Speed for more information.
Setting Adjustable Task Rates	A Setting Adjustable Task Rates operation lets you change the Rebuild Rate, Transformation Rate, Patrol Read Rate, BGI Rate, and Consistency Check Rate for a controller. See Setting Adjustable Task Rates for more information.
Discarding Preserved Cache	If the controller loses access to one or more volumes, the controller preserves the data from the volume. This preserved cache is called *Pinned Cache*. This cache is preserved until you import the volume or discard the cache. As long as pinned cache exists, you cannot perform certain operations on the volume. See Discarding Pinned Cache for more information.
Downloading Serial Output Log	The Serial Output Log file contains the firmware terminal log entries for the controller. The log information is shown as total number of entries available on the firmware side. See Downloading the Serial Output Log for more information.
Background Operations	Provides information on Background Operations Support, such as Pause, Resume, Abort, and so on. See Background Operations Support for more information.
Advanced Software Features	
Fast Path	The MegaRAID FastPath software is a high-performance I/O accelerator for solid state drive (SSD) arrays connected to a MegaRAID controller card. This advanced software is an optimized version of MegaRAID technology that can dramatically boost storage subsystem and overall application performance; particularly those that demonstrate high random read/write operation workloads – when deployed with a MegaRAID SATA+SAS controllers connected to SSDs. See MegaRAID Fast Path Advanced Software for more information.
RAID 5 and RAID 6	• **RAID 5** Uses data striping and parity data across three or more drives (distributed parity) to provide high data throughput and data redundancy, especially for applications that require random access. • **RAID 6** Uses data striping and parity data across three or more drives (distributed parity) to provide high data throughput and data redundancy, especially for applications that require random access. RAID 6 can survive the failure of two drives.
Volume Operations	

Feature Name	Description
Volume Settings/Modifying Volume Properties	A Volume Settings/Modifying Volume Properties operation lets you configure the volumes. See Selecting Volume Settings for more information.
Start and Stop Locating a Volume	If the drives reside in a disk enclosure, you can identify them by making their LEDs blink. See Start and Stop Locating a Drive for more information.
Erasing a Volume	An Erasing a Volume operation lets you erase data on Non SEDs (normal HDDs) using the Drive Erase option. The Erase operation is performed as a background task. See Erasing a Drive for more information.
Initializing a Volume	An Initializing a Volume operation lets you select the **Fast Initialization** or **Full Initialization** option to initialize a drive immediately under the **Advanced Configuration** wizard. See Initializing a Volume for more information.
Starting Consistency Check on a Volume	A Consistency Check operation verifies whether all stripes in a volume with a redundant RAID level have correct parity or mirror values. The Consistency Check operation involves mirroring data when an inconsistent stripe is detected for a RAID 1 configuration, and re-creating the parity from the peer disks in the case of a RAID 5 and RAID 6 configuration. This mechanism applies to variants and secondary RAID levels based on RAID 1 and RAID 5 configurations. See Starting Consistency Check on a Volume for more information.
Expanding the Online Capacity of a Volume	The transformation feature lets you expand the capacity of a volume by adding new drives or making use of unused space on existing disks, without requiring a reboot. See Expanding the Capacity of a Volume While Online for more information.
Deleting a Volume	The Deleting a Volume feature lets you delete a volume. See Deleting a Volume for more information.
Drive Operations	
Assign Global Spare Drives	A global spare drive replaces a failed drive in any redundant array, as long as the capacity of the global spare drive is equal to or greater than the coerced capacity of the failed drive. See Assigning Global Spare Drives for more information.
Remove Global Spare Drives	A Remove Global Spare Drives operation lets you remove global spare drives. See Removing a Global Spare Drive for more information.
Assign Dedicated Spare Drives	A dedicated spare drive provides protection to one or more specified arrays on the controller. See Assigning Dedicated Spare Drives for more information.
Start and Stop Locating Drive	If the drives are in a disk enclosure, you can identify them by making their LEDs blink. See Start and Stop Locating a Drive for more information.
Making a Drive Online and Offline	The Making a Drive Online and Offline feature lets you change the state of a drive. See Making a Drive Offline and Making a Drive Online for more information.
Replacing a Drive	The Replacing a Drive feature lets you replace a drive if the drive shows signs of failing. See Replacing a Drive for more information.
Rebuilding a Drive	If a drive that is configured as RAID 1, 5, 6, 10, 50, or 60 fails, the firmware automatically rebuilds the data on a spare drive to prevent data loss. The Rebuild operation is a fully automatic process. You can monitor the progress of drive rebuilds in the **Background Processes in Progress** window. See Rebuilding a Drive for more information.
Erasing a Drive	The Erasing a Drive feature lets you erase data on Non SEDs (normal HDDs). The Erase operation is performed as a background task. See Erasing a Drive for more information.
Sanitizing a Drive	The Sanitizing a Drive feature lets you erase the data that resides on a drive using the Sanitize feature. The Sanitize feature is similar to the Drive Erase feature that is already supported by your controller, except that the Sanitize function is performed by the drive firmware, whereas the Drive Erase function is performed by the controller firmware. See Sanitizing a Drive for more information.
Converting Unconfigured Bad Drive to Unconfigured Good Drive	When you force a drive offline, it enters the Unconfigured Bad state. If a drive contains valid disk data format (DDF) metadata, its drive state is Unconfigured Good. See Converting an Unconfigured Bad Drive to an Unconfigured Good Drive for more information.

Feature Name	Description
Make Unconfigured Good Drive	When you power down a controller and insert a new drive, and if the inserted drive does not contain valid DDF metadata, the drive status is listed as *JBOD* (Just a Bunch of Drives) when you power up the system again. When you power down a controller and insert a new drive, and if the drive contains valid DDF metadata, its drive state is listed as Unconfigured Good. A new drive in the JBOD drive state is exposed to the host operating system as a stand-alone drive. See Make Unconfigured Good Drives and Make JBOD Drives for more information.
Make JBOD	The Make JBOD feature lets you create JBODs. See Making a JBOD Drive for more information.
Event Logs	
Viewing Event Logs	The application monitors the activity and performance of the server and all of the controllers attached to it. See Viewing Event Logs for more information.

Upgrade Requirements

Complete the tasks that follow while upgrading the HPE MR Storage Administrator application.

Browser Cache

Clear the browser cache on the client on which you are using LSA for the following reasons:

- If you are upgrading from a previous version of LSA.
- To clear the saved passwords, so passwords are not saved in the browser.

StandAlone Installer

The StandAlone installer has the following components:

- A backend with a local agent (without remote agent management capability)
- A monitor (without remote monitoring capability).
- A client (without remote and managed server capabilities)

The StandAlone installer has the following features and limitations:

- Does not permit the discovery of other hosts that are running the LSI Storage Authority
- Permits self-registration of the current host using OpenSLP but does not have any interface for server discovery detection from the network
- Provides capability to configure LDAP information
- Does not permit to add managed servers through the UI.

Installing the HPE MR Storage Administrator Software on the Microsoft Windows Operating System

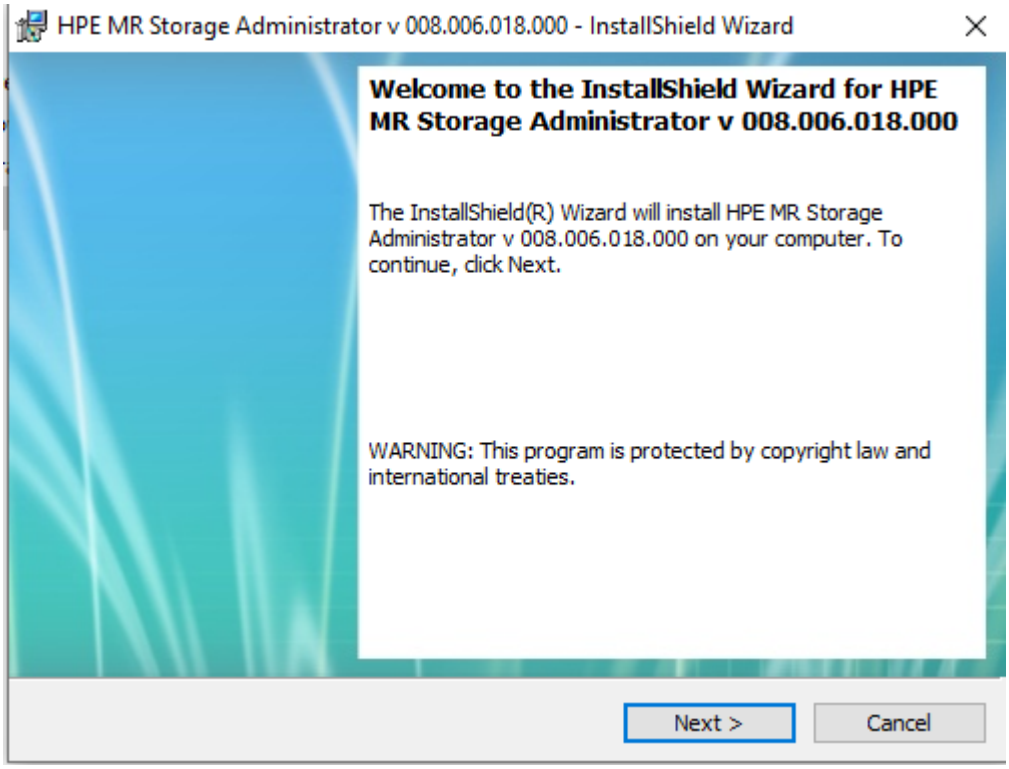
This section provides the procedure for installing HPE MR Storage Administrator Software on the Microsoft Windows operating system.

> **NOTE**
> The `LSA_HOME` directory is only accessible by administrators.

Perform the following steps to install the HPE MR Storage Administrator .

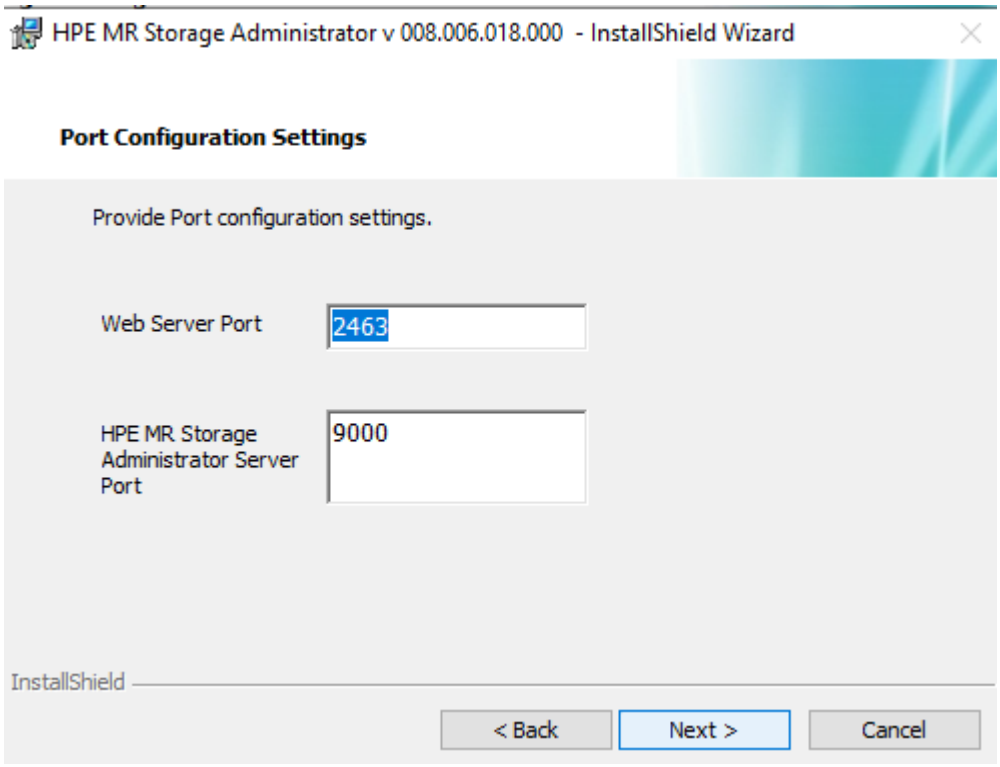
1. Run the HPE MR Storage Administrator `setup.exe` file.
   The **InstallShield Wizard** dialog appears.

   Figure 1: InstallShield Wizard Dialog

2. Click **Next**.
   The **License Agreement** dialog appears.
3. Read the agreement and select the **I accept the terms in the license agreement** radio button, and click **Next**.
   The **Customer Information** dialog appears.
4. Enter your user name and the organization name, and click **Next**.
   The **Port Configuration Settings** dialog appears.

Figure 2: Port Configuration Settings Dialog

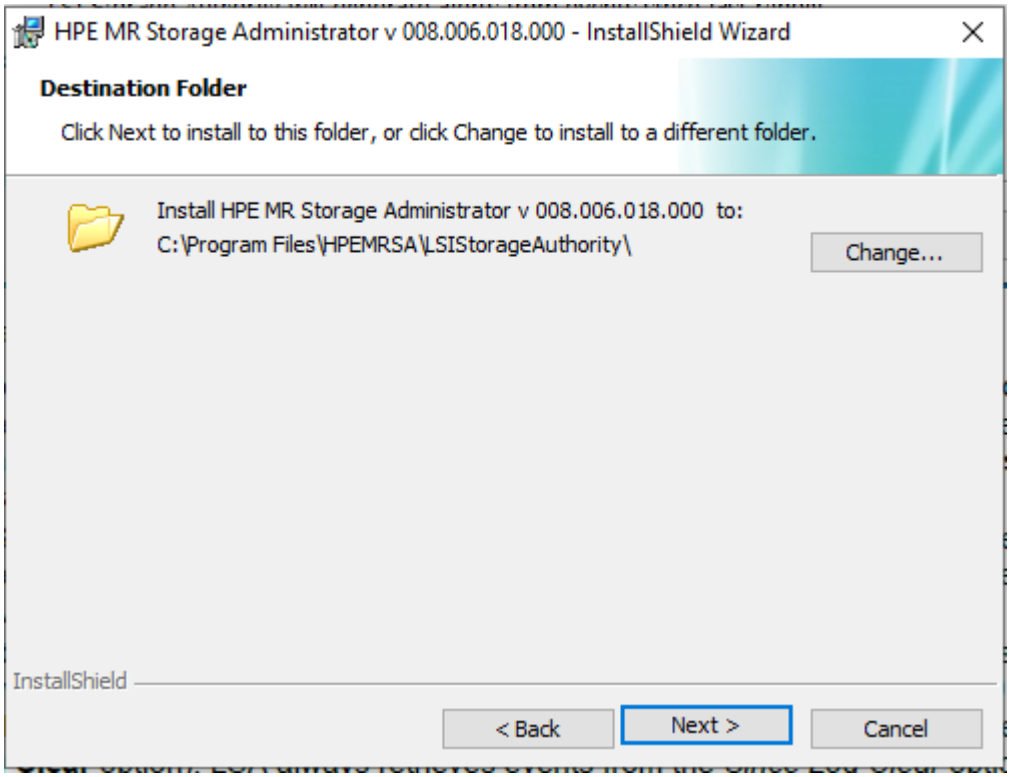


By default, LSA communicates on **Web Server Port 2463** and **LSA Server Port 9000**. Ensure that these ports are available to be used by LSA. Depending on your environment, if these ports are not available, specify the port details here. You can also edit the details of this port after installation. See Changing the HPE MR Storage Administrator Software Port Number and Changing the nginx Web Server Port Numbers.

5. Click **Next** to proceed.

   The **Destination Folder** dialog appears with the default file path.

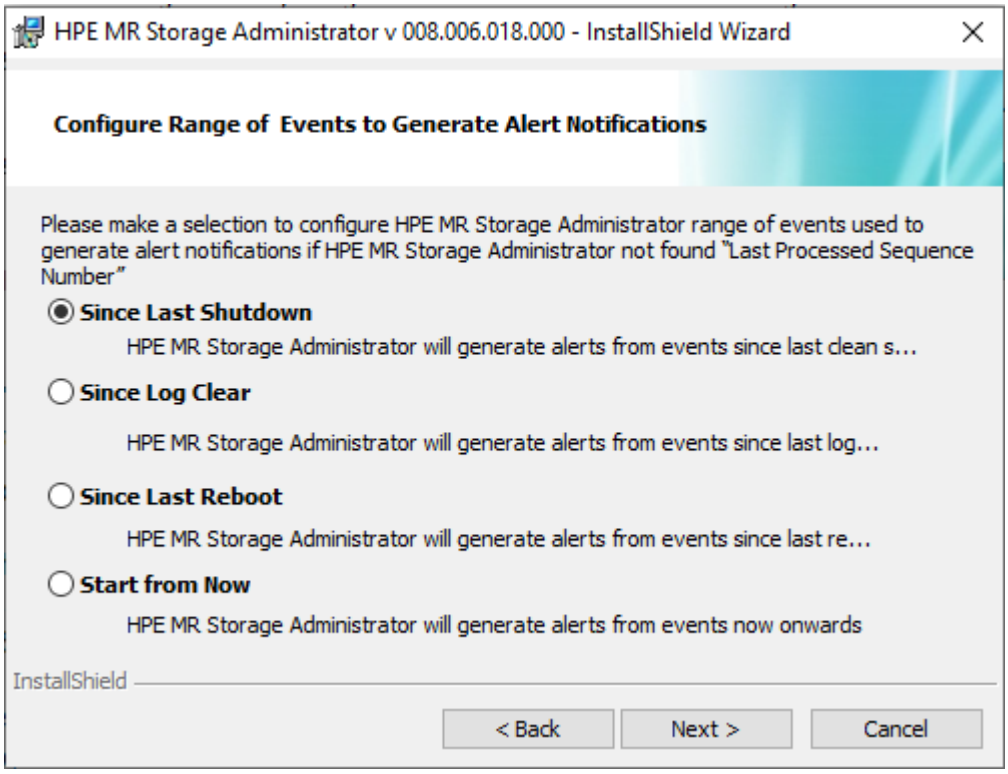
Figure 3: Destination Folder Dialog



6. (Optional) Click **Change** to select a different destination folder for the installation files.
7. Click **Next**.

   The **Configure Range of Events to Generate Alert Notifications** dialog appears. You can configure alert notifications to get early notification of application or service issues and problem occurrences.

Figure 4: Configure Range of Events to Generate Alert Notifications



The following configuration options are available:

- **Since Last Shutdown**: Select this option to retrieve events from the last clean shutdown. By default, you can only retrieve the last 30 events. If there are any progress events as part of the last 30 events, those progress events are part of the event history. If the sequence numbers are less than the last log that was cleared (**Since Log Clear** option), LSA always retrieves events from the *Since Log Clear* option.
- **Since Log Clear**: Select this option to retrieve events from the last log that was cleared. By default, you can only retrieve the last 30 events. If there are any progress events as part of the last 30 events, those progress events are not part of the event history.
- **Since Last Reboot**: Select this option to retrieve events from the last time the system was restarted. By default, you can only retrieve the last 30 events. If there are any progress events as part of the last 30 events, those progress events are not part of the event history. If the sequence numbers are less than the last log that was cleared (**Since Log Clear** option), LSA always retrieves events from the *Since Log Clear* option.
- **Start From Now**: Select this option to retrieve events from now.

You can also change these configuration options as per your requirement at any point in time by editing the `lsa.conf` file in the `LSI Storage Authority /conf` directory and choosing the required parameter. For example, if you have selected **Since Last Shutdown** as a configuration option to retrieve events during the time of installation and you want to change it to **Since Last Reboot**, through the `lsa.conf` file, go to `# Retrieve range of events used to generate alert notification, if LSA not found LastProcessedSeqNum` section in the `lsa.conf` file, change the `retrieve_range_of_events_since =` to 2 (`retrieve_range_of_events_since = 2`).

> **NOTE**
> You must restart the LSI Storage Authority service for the configuration changes to take effect.

8. Click **Next**. The **Ready to Install the Program** windows appears. Click **Next**.
   Depending on the setup type you have selected, the **InstallShield Wizard Completed** dialog appears.

9. (Optional) Select the **Show the Windows Installer log** check box to view the windows installer log file.
   The log file (`LSA_install.log`) is created in the same folder from where the `setup.exe` is installed.
10. Ensure that port 2463 is not blocked by a firewall.
    The Windows Firewall settings are located under **Control Panel** > **Windows Firewall**.
11. Click **Finish**.

Installing in Noninteractive Mode

You must log in to the system with root privileges. You can also open the command prompt as root and run the installer through the command line.

Perform the following steps to install the LSI Storage Authority software in noninteractive mode:

1. From the command line, run the `vcredist_x86.exe /Q` command to install the *Microsoft Visual C++ 2008 Redistributable Package for x86* if it is not already installed.

   The Microsoft Visual C++ 2008 Redistributable Package for x86 (`vcredist_x86.exe`) is available under the directory `<Package_Dir>\ISSetupPrerequisites\{270b0954-35ca-4324-bbc6-ba5db9072dad}\VC Redist 2008 Installation`.

   OpenSLP is bundled with LSA 2.2 and later. While installing LSA, if OpenSLP is not installed ensure that you select the option to install OpenSLP, and LSA seamlessly installs the required version of OpenSLP. See OpenSLP for more information.
2. Depending on the type of installation required, run the `setup.exe /s /v/qn ADDLOCAL=` command. The types of installation and their associated alert notifications available are as follows:

Type of Installation	Type of Event Notification	Event Notification Choice
Gateway	Since Last Shutdown	0
StandAlone	Since Log Clear	1
DirectAgent	Since Last Reboot	2
Light Weight Monitor	Start From Now	3

   Example: If you require the Light Weight Monitor to be installed, you must to run the `setup.exe /s /v/qn ADDLOCAL=LightWeightMonitor INSTALLATIONCHOICES=129 INSTALLDIR=CustomDirecotryLocation` command.

Uninstalling in Interactive Mode

You can uninstall the LSI Storage Authority either through the **Control Panel** or the application shortcut in the **Start** menu.

Uninstalling the LSI Storage Authority Software through the Application Shortcut in the Start Menu

1. Select **Start** > **All Programs** > **LSI** > **LSI Storage Authority** > **Uninstall LSI Storage Authority**.

Uninstalling the LSI Storage Authority Software through the Control Panel

1. If you are using the Microsoft Windows Server 2012 operating systems, select **Add/Remove Programs** from the **Control Panel**. If you are using the Microsoft Windows 8 operating systems, select **Programs and Features** from the **Control Panel**.
2. Select the LSI Storage Authority software from the list, and click **Uninstall**.

Uninstalling in Noninteractive Mode

You must log in to the system with root privileges. You can also open the command prompt as root and run the installer through the command line.

Perform the following step to install the LSI Storage Authority software in noninteractive mode:

From the command line, run the `msiexec.exe /x <productcode>/qn` command to uninstall LSA.

Where *<productcode>* is a unique product code associated with each LSA installation and *<LSA_HOME_PATH>* is the location where the LSA is installed.

Example: `msiexec.exe /x {20660CCB-7C70-4D61-8D18-FB7FA3C476C9}/qn`

Before you begin to uninstall LSA, if any file has been manually copied to the *<LSA_HOME>* directory by you other than the standard installation package contents, make sure you delete those files. If you fail to remove the files that have been manually copied to the *<LSA_HOME>* directory, the uninstallation process may fail.

Installing the HPE MR Storage Administrator Software on the Linux Operating System

The HPE MR Storage Administrator software supports both the interactive and the noninteractive modes of Linux installation.

1. Run the `rpm -ivh MRStorageAdministrator-xx.rpm` command from the installation disk.
2. Extract the contents of the zip file and install the appropriate package on the operating system.

The following is the corresponding OS support information:

- `gcc_4.8.x` — RHEL 7.x and supported operating systems of `gcc_8.3.x` and `gcc_11.2.x`
- `gcc_8.3.x` — RHEL 8.x, SLES 15 SPx, and supported operating systems of `gcc_11.2.x`
- `gcc_11.2.x` — RHEL 9.x, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS
- `gcc_4.8.x` — LSA Installer in this folder supports gcc_4.8.x and higher
- `gcc_8.3.x` — LSA Installer in this folder supports gcc_8.3.x and higher
- `gcc_11.2.x` —LSA Installer in this folder supports gcc_11.2.x and higher

64-bit Linux operating systems

This package contains `gcc_4.8.x , gcc_8.3.x` and `gcc_11.2.x`.

Ubuntu

Use `install_deb.sh` to install the HPE MR Storage Administrator .

> **NOTE**
> Ensure the `Connect automatically` checkbox is selected. The checkbox is available under **Network Connections**.

Installing in the Interactive Mode

You must log in to the system with root privileges. You can also open the command prompt as root and run the installer through the command line.

Perform the following steps to install the LSI Storage Authority software in the interactive mode.

1. Run the `./install.csh` command from the installation disk.
2. Read the license agreements for the software package. If you agree to the terms of the license agreements, press **Y**. Otherwise, press **N** to exit the installation.
3. The **Configure Range of Events to Generate Alert Notifications** dialog appears. You can configure alert notifications to get early notification of application or service issues/problem occurrences.

   The following configuration options are available:

   - **Since Last Shutdown**: Select this option to retrieve events from the last clean shutdown.
   - **Since Log Clear**: Select this option to retrieve events from the last log that was cleared.
   - **Since Last Reboot**: Select this option to retrieve events from the last time the system was restarted.
   - **Start From Now**: Select this option to retrieve events from now.

   You can also change these configuration options as per your requirement at any point in time by editing the `lsa.conf` file in the `LSI Storage Authority/conf` directory and choosing the required parameter. For example, if you have selected **Since Last Shutdown** as a configuration option to retrieve events during the time of installation and you want

to change it to **Since Last Reboot**, through the `lsa.conf` file, go to `# Retrieve range of events used to generate alert notification, if LSA not found LastProcessedSeqNum` section in the `lsa.conf` file, change the `retrieve_range_of_events_since =` to 2 (`retrieve_range_of_events_since = 2`). You must restart the LSI Storage Authority service for the configuration changes to take effect.

4. Enter the nginx server port number. The port range is from1 to 65535. The default port number is 2463.
5. Enter the LSI Storage Authority application port numbers. The port range is from 1 to 65535. The default port number is 9000.

   Ensure that the nginx_port number and the LSA_port number are in the between the range, 1 to 65535 and are different. If the nginx_port number and the LSA_port number are not specified in the command line, the default values are used.

   By default, LSA communicates on Web Server Port 2463 and LSA Server Port 9000. Ensure that these ports are available to be used by LSA. Depending on your environment, if these ports are not available, specify the port details here. You can also edit this port details after installation.
6. Ensure that port 2463 is not blocked by a firewall.
7. Extract the contents of the zip file and install the 64-bit Linux operating systems. The `LSA_Linux.zip` file contains files for 64-bit platforms.

   NOTE
   MRSA only supports 64-bit operating systems.

   NOTE
   Ensure that **Connect automatically** check box is selected, which is available under **Network Connections**.
8. To launch theHPE MR Storage Administrator , navigate to your browser and enter your IP Address followed by`:2463`. For example, `http://135.24.237.36:2463`.

Installing in the Noninteractive Mode

To install the LSI Storage Authority Software in a noninteractive or silent mode, use the following commands.

1. (Optional) If VC Redist 2010 and VC Redist 2015 are not installed on the server, complete the following steps.
   a) Install the VC Redist 2010 package from the command line `vcredist_x64.exe /Q`.

      VC Redist 2010 (`vcredist_x64.exe`) is available in the `<Package_Dir>\ISSetupPrerequisites \{7f66a156-bc3b-479d-9703-65db354235cc}\` directory.
   b) Install the VC Redist 2015 package from the command line `vc_redist.x64.exe /Q`.

   VC Redist 2015 (`vc_redist.x64.exe`) is available in the `<Package_Dir>\ISSetupPrerequisites \{D093EE4D-527D-4CC7-AB3C-DCE3219FA508}\` directory.
2. If OpenSLP is not installed, install the OpenSLP from the command line `openslp_3.0.0_0_x64`.

   OpenSLP is available in the `<Package_Dir>\ISSetupPrerequisites\{23401E90-6962-476F-9D92-F9027E91A490}\` directory.

3. Use one of the following modes to install the software.
   - Gateway – `setup.exe /s /v"/qn ALLUSERS=1 ADDLOCAL=Gateway INSTALLATIONCHOICES=0 EVENTNOTIFICATIONCHOICES=3`
   - StandAlone – `setup.exe /s /v"/qn ALLUSERS=1 ADDLOCAL=StandAlone INSTALLATIONCHOICES=1 EVENTNOTIFICATIONCHOICES=3`
   - DirectAgent – `setup.exe /s /v"/qn ALLUSERS=1 ADDLOCAL=DirectAgent INSTALLATIONCHOICES=2 EVENTNOTIFICATIONCHOICES=3`
   - Light Weight Monitor – `setup.exe /s /v"/qn ALLUSERS=1 ADDLOCAL=LightWeightMonitor INSTALLATIONCHOICES=129 EVENTNOTIFICATIONCHOICES=3`

Type of Installation	Type of Event Notification	Event Notification Choice
Gateway	Since Last Shutdown	0
StandAlone	Since Log Clear	1
DirectAgent	Since Last Reboot	2
Light Weight Monitor	Start From Now	3

4. (Optional) To change the default directory structure, provide the following input with each mode of installation.

```
Setup.exe /s /v"/qn ALLUSERS=1 ADDLOCAL=LightWeightMonitor INSTALLATIONCHOICES=129
 INSTALLDIR=CustomDirecotryLocation
```

5. (Optional) To redirect the LSA installer logs, use the following command.

```
setup.exe /s  /v"/l*v \"<PATH_TO_LOG_FILE>\<FILE_NAME>.log\""  /v"/qn ALLUSERS=1 ADDLOCAL=Gateway
 INSTALLATIONCHOICES=0 EVENTNOTIFICATIONCHOICES=3 INSTALLDIR=CustomDirecotryLocation
```

Uninstalling the LSI Storage Authority Software on the Linux Operating System

Perform the following step to uninstall the Linux operating system.

Run the `uninstaller.sh` script (`/opt/lsi/LSIStorageAuhority/uninstaller.sh`). Alternatively, you can run the `rpm -e <rpm_name>` command to uninstall the RPMs from the target system.

Command usage example: `rpm -e LSIStorageAuhority-1.00xx.xxxx-xxxx`

Performing Initial Configuration

After successfully installing the LSI Storage Authority, you must set up these initial configurations.

Changing the HPE MR Storage Administrator Software Port Number

Perform the following steps to change the HPE MR Storage Administrator port numbers.

1. Open the `lsa.conf` file in the `LSIStorageAuthority/conf` directory.
2. Enter the new port number in the `listening_port` field.

   Prior to assigning the port number, ensure that the port is available for usage.
3. Save the `lsa.conf` file.
4. Open the `nginx.conf` file in the `LSI Storage Authority/server/conf` directory.
5. Replace all of the `fastcgi_pass 127.0.0.1:9000` instances with `fastcgi_pass 127.0.0.1:<new port number>`.
6. Save the `nginx.conf` file.
7. Open the `portconfig.properties` file in the `LSIStorageAuthority` directory.
8. Enter the new port number in the `<Client Port> <new port number> </Client Port>` field.
9. Save the `portconfig.properties` file.
10. Restart the nginx service and the HPE MR Storage Administrator Service.

Changing the nginx Web Server Port Numbers

Perform the following steps to change the nginx web server port numbers.

1. Open the `nginx.conf` file in the `LSIStorageAuthority/server/conf` directory.
2. Replace all of the `listen 2463 default_server ssl` instances with `listen <new port> default_server ssl`.
3. Save the `nginx.conf` file.
4. Restart the nginx service and the HPE MR Storage Administrator .

Changing the Nginx Read Timeout

On VMware, when you request process-intensive operations such as creating **240 Volumes**, **Drive Initialization**, **Consistency Check**, **Drive Erase**, and so on, the VMware ESXi Server may time out, resulting in a delay of the operation that is being performed.

To avoid the VMware ESXi Server getting timed out, perform the following steps to change the nginx FCGI Read Timeout.

1. Open the `nginx.conf` file in the `LSIStorageAuthority/server/conf` directory.
2. In the `nginx.conf` file, search for the `fastcgi_read_timeout` field.
3. Modify or increment the value present in the `fastcgi_read_timeout` to anywhere between `900` to `2000` depending on your requirement.
4. Save the `nginx.conf` file.
5. Restart the nginx service and the HPE MR Storage Administrator .

Performing the Initial Setup

After you successfully log into the HPE MR Storage Administrator application, it is recommended that you perform the initial setup tasks before proceeding.

Displaying or Blocking a Private IP Address

This section outlines the strategy that the application follows to display or block a private IP address in a corresponding sub-net.

- **Private IP address** – A private IP address is a non-Internet facing IP address on an internal network.
  Private IP addresses are provided by network devices, such as routers, using network address translation (NAT).
- **Virtual IP address** – A virtual IP address (VIPA) is an IP address that is assigned to multiple domain names or servers that share an IP address based on a single network interface card (NIC).
  VIPAs are allocated to virtual private servers, websites, or any other application that resides on a single server. The host server for these applications has a network IP address that is assigned by a network administrator, whereas the different server applications have VIPAs. VIPAs enhance network load balancing and redundancy.
- **Automatic Private IP Addressing** – Automatic Private IP Addressing (APIPA) is a feature of Windows-based operating systems that enable a computer to automatically assign itself an IP address when no Dynamic Host Configuration Protocol (DHCP) server is available to perform that function.
  APIPA serves as a DHCP server failover mechanism and makes it easier to configure and support small local area networks.
- **Private IP Address Range** – The following is the IP address range which falls under either the private, (or) Virtual, (or) APIPA category:
  - **NAT** – `10.0.0.0 - 10.255.255.255`
  - **Private (or) Virtual** – `172.16.0.0 - 172.31.255.255` or `192.168.0.0 - 192.168.255.255`
  - **APIPA** – `169.254.0.0` to `169.254.255.255`

The use cases that follow provide details on how the application behaves in various situations:

Table 4: Use Case #1: Without Blocking the Private IP

Use Case	Standalone / Client	Remarks
No NIC CARD (Windows)	Loopback (or) 127.0.0.1	As the server is not in network, the gateway cannot access the standalone server.
No NIC CARD (Linux)	Loopback (or) 127.0.0.1	Because the server is not in network, the gateway cannot access the standalone server.
Static IP	Using Static IP	—
DHCP IP	Using the DHCP IP	—
Private IP	Using the Private IP	In a more secured environment, private IP address cannot be accessed outside the server.

Table 5: Use Case #2: After Blocking the Private IP

Use Case	Standalone / Client	Remarks
No NIC CARD (Windows)	Loopback (or) 127.0.0.1	As the server is not in network, the gateway cannot access the standalone server.
No NIC CARD (Linux)	Loopback (or) 127.0.0.1	Because the server is not in network, the gateway cannot access the standalone server.
Static IP	Using Static IP	—
DHCP IP	Using the DHCP IP	—
Private IP	If a valid IP exists, it is displayed. If no valid IP exists, Loopback (or) 127.0.0.1 is displayed.	In a more secured environment, because a private IP address cannot be accessed outside the server, the application does not populate a private IP address.

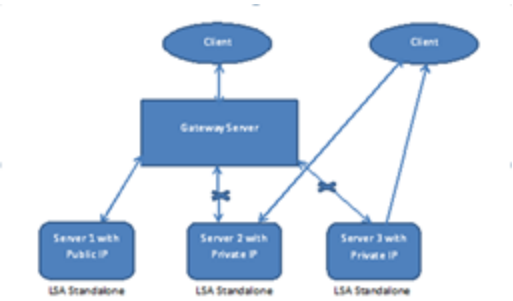
Why does the application blocks certain IP addresses: In an enterprise world, when a computer is assigned a private IP address, the local devices see this computer through its private IP address. However, devices residing outside of your local network cannot directly communicate through the private IP address, but uses your router's public IP address to communicate. You must use a NAT router to directly access a local device assigned a private IP address.

In a more secure environment, although the application is able to discover and display the private IP address through the gateway server, when a request is made through the gateway server, the private IP is not accessible. Because the application cannot access the private IP, the application is unable to service the requests which are meant for the private IP.

Because of the previously mentioned reason, when the installation is a gateway, the corresponding gateway server is not able to communicate with the private IP address which in turn becomes an issue. The application works if the private IP addresses are behind the NAT router, which is the most preferable option in an enterprise world.

The diagram that follows shows how a private IP address should be accessed in enterprise networks and the problems with the private IP address:

Figure 5: Private IP Address Access



Alert Settings

The **Alert Settings** tab lets you perform these actions:

- Change the alert delivery method for different severity levels.
- Specify different alert delivery methods for inside and outside the application.
- Revert back to the default alert delivery methods and the default severity level of an individual event.
- Save the alert settings on the server.

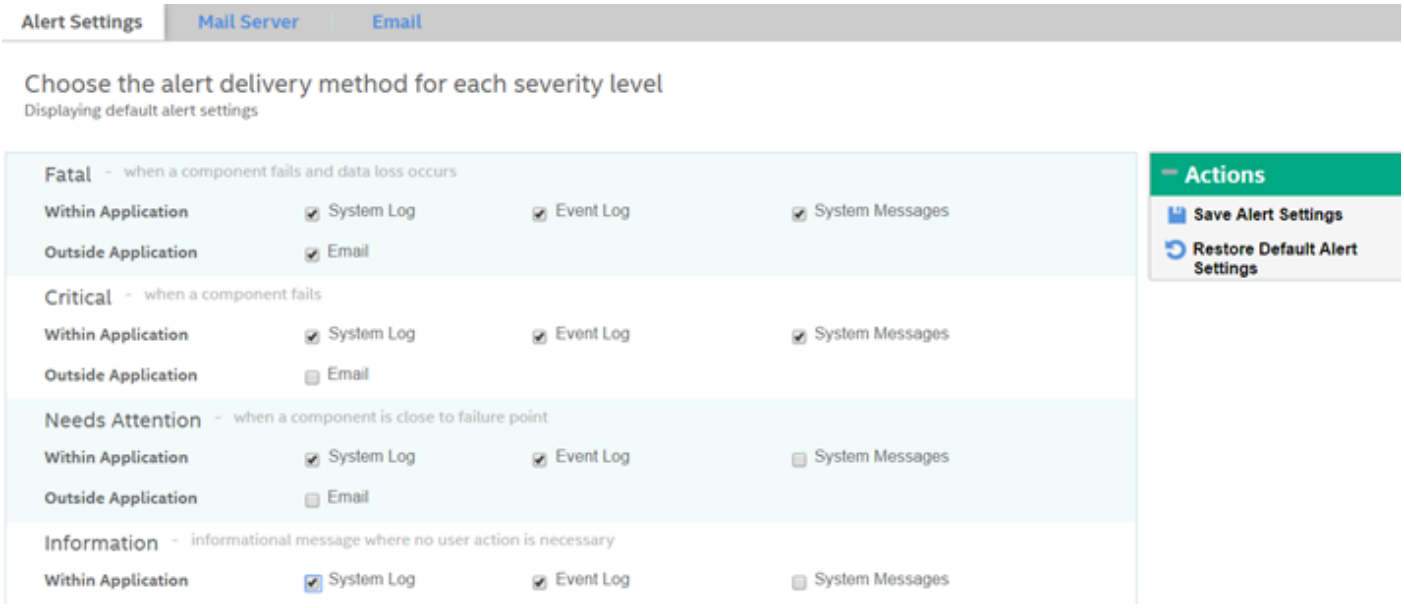
Based on the severity level (Information, Warning, Critical, and Fatal), the default alert delivery methods change. By default, each severity level has one or more alert delivery methods configured for it. The different alert delivery methods are as follows:

- **System Log** – By default, all of the severity events are logged in the local system log.
  In the Windows operating system (OS), the system log is logged in **Event Viewer** > **Application**. In the Linux OS, the system log is logged in **var** > **log**.
- **Event Log** – By default, all the severity events appear in the event log.
  Click **View Event Log** to view the event log. Each message that appears in this log has a severity level that indicates the importance of the event (severity), an event ID, a brief description, and a date and timestamp (when it occurred).
- **System Messages** – By default, fatal and critical events are displayed as system messages.
  System messages are displayed in a yellow bar at the top of the Server Dashboard and the Controller Dashboard. System messages let you view multiple events in a single location.
- **Email** – By default, fatal events are displayed as email notifications.
  Based on your configuration, the email notifications are delivered to your inbox. In the email notification, aside from the event's description, the email also contains system information and the controller's image details. Using this additional information, you can determine the system and the controller on which the fatal error occurred.

To change the alert delivery method for each severity level, perform these steps:

1. Click **Settings** in the Server Dashboard.
   The **Alert Settings** page appears, with the default alert delivery methods for each severity level.

   Figure 6: Alert Settings Page



2. Select the desired alert delivery method for each severity level by clicking the required check box.
3. Click **Save Alert Settings** to save the settings on the server.
   Click **Restore Default Alert Settings** to revert back to the default alert delivery settings.

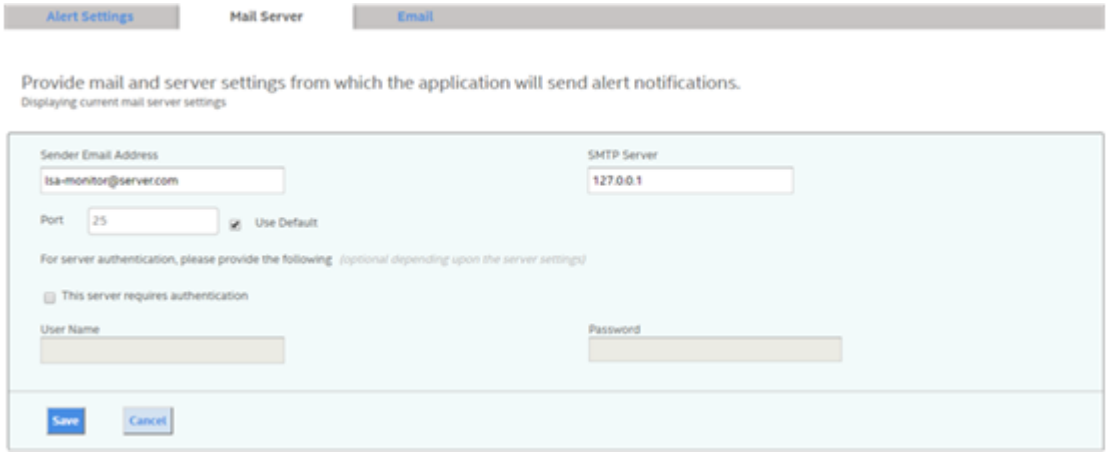
Setting Up the Email Server

Perform these steps to enter or edit the mail and the SMTP server settings.

1. Click the **Mail Server** tab on the **Settings** page.

   The **Mail Server** page displays the current mail server settings.

Figure 7: Mail Server Window



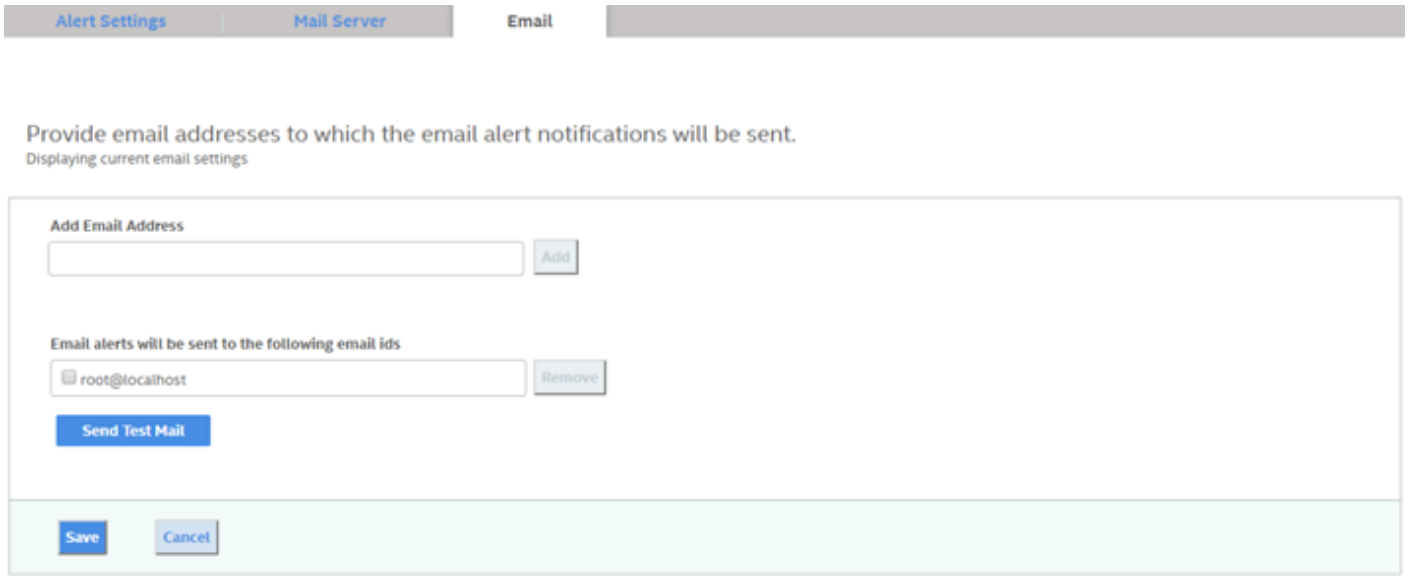
2. Specify the details in the respective fields as per your requirement.
3. Select the **This server requires authentication** check box on your SMTP server if the authentication login feature is enabled. To enable this feature, specify the authentication details in the **User Name** and **Password** fields respectively.
4. Click **Save**.

Adding the Email Addresses of Alert Notification Recipients

Perform these steps to add email addresses of recipients of the alert notifications.

1. Click the **Email** tab in the **Setting** page.

   Figure 8: Email Window



2. Specify the details in the respective fields as per your requirement.
3. Click **Save**.

Configuring Different Types of Access

1. To enable logging in with a user name and password, complete the following steps.

   NOTE
   By default, the application is installed without a login so the user can access the application without entering a user name and password.

   a) Stop the MRSA services and nginx services.
   b) Go to the file `<MRSA_Home>/LSIStorageAuthority\conf`.
   c) Open the file `LSA.conf`.
   d) Update the following field value to `0`.

   ```
   # bypass authentication (use with caution)
   bypass_authentication = 1
   ```

   e) Start the MRSA services and nginx services.

2. To enable remote access of the application, complete the following steps.

   NOTE
   By default, the application is installed in the localhost mode. The user can only access the application from the local host IP.

   a) Stop the MRSA services and nginx services.
   b) Go to `<MRSA_Home>/LSIStorageAuthority\server\conf`.
   c) Open the file `nginx.conf`.
   d) Edit the following lines:

   ```
   listen       127.0.0.1:2463 default_server;
   ```

   Uncomment the following lines:

   ```
   #use below configuration to allow inbound access to this port from remote servers
   #listen       2463 default_server;
   ```

   e) 4) Start the MRSA services and nginx services.

Server Dashboard

The Server Dashboard is the default landing page for the software. The **Server Dashboard** displays the overall summary of the server and the devices that are attached to it. You can troubleshoot, configure, maintain, and monitor the controllers from the **Server Dashboard**. The following figure and table describes this page.

Figure 9: Server Dashboard Window

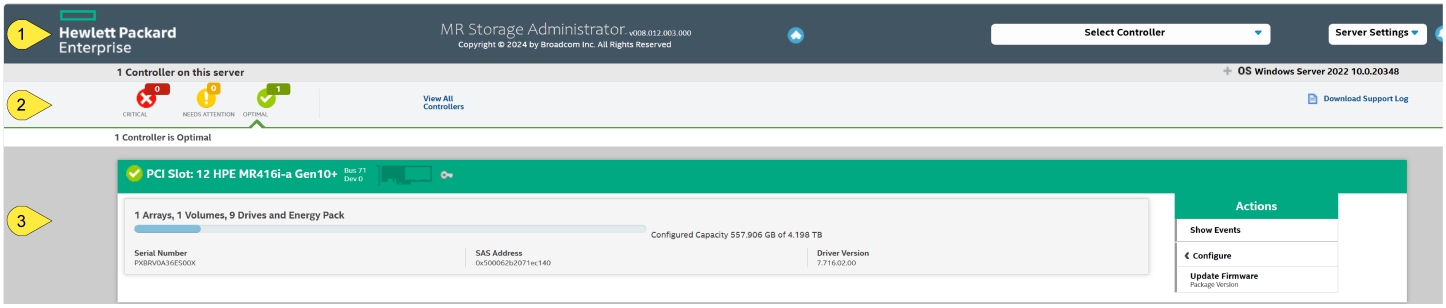


Table 6: Server Dashboard Description

Callout	Description
1	**Main Navigation** – The main navigation window helps you to traverse among the various views. This navigation is available across all of the pages in the software. The description follows: •  : Helps you to navigate to the server dashboard from any page in the software. • **Select Controllers**: Lists the controllers that you are monitoring. The color-coded controller status icons (red, amber, and green) indicate the health status of all the controllers based on their criticality. Click a controller to navigate to its dashboard. • – Click **@Settings** to perform initial settings. – Click **View Server Profile** and expand the + button to view the server configuration such as the server IP, server name, OS Name, OS version, OS architecture, and the version of the software that is installed. You can also view the controller information such as controller hardware, enclosure of the controller, and information about the drives and volumes associated with the controller. •  : Lets you enable or disable system messages. •  : Displays the application context-sensitive help.
2	**Controller Status** – Description as follows: • Displays the status of all of the controllers that are connected to the server. It displays the total number of controllers and status icons based on their criticality: – **Critical**: Indicates that a critical error exists on the controller and the controller needs immediate attention. – **Needs Attention**: Indicates that an error exists on the controller that needs attention, however, not immediately. – **Optimal**: Indicates that the controller is operating in an optimal state. • Displays critical issues of failed devices and provides recommendations for troubleshooting. You can also see contextual links, which help you to easily locate the device and initiate troubleshooting. Based on the criticality of the controller, the application displays information about that particular controller in the controller information pane. For example, if a controller is in the critical state, that controller is opened by default. If you want to view information about other controllers, click the respective Controller Status icon. Click **View All Controllers** to view information about all of the controllers. **OS Information** – Displays the server's operating system information. **Download Support Log** – Lets you download the support log, which contains consolidated information about the server and all the devices to which it is connected.
3	• **Controller Information**: Displays information about the controller. • **Controller Status**: When multiple controllers are connected, the controllers are sorted based on the bus device function. The controllers are indexed with numbers 0, 1, 2, and so on. • Controller summary • Controller properties • Controller issues • Controller event logs • Lets you perform these tasks: – Configure the controllers. See Controller Configurations. • Download diagnostics. • Update the controller firmware. • View, download, and clear event logs. • Perform various operations on the controller. See Managing Controllers • Navigate to any of the controllers to see its specific view by clicking the appropriate controller.

Controller Dashboard

You can perform controller related actions and view all the information pertaining to a controller from the Controller Dashboard. The figure and table that follows describes this page.

Figure 10: Controller Dashboard Window

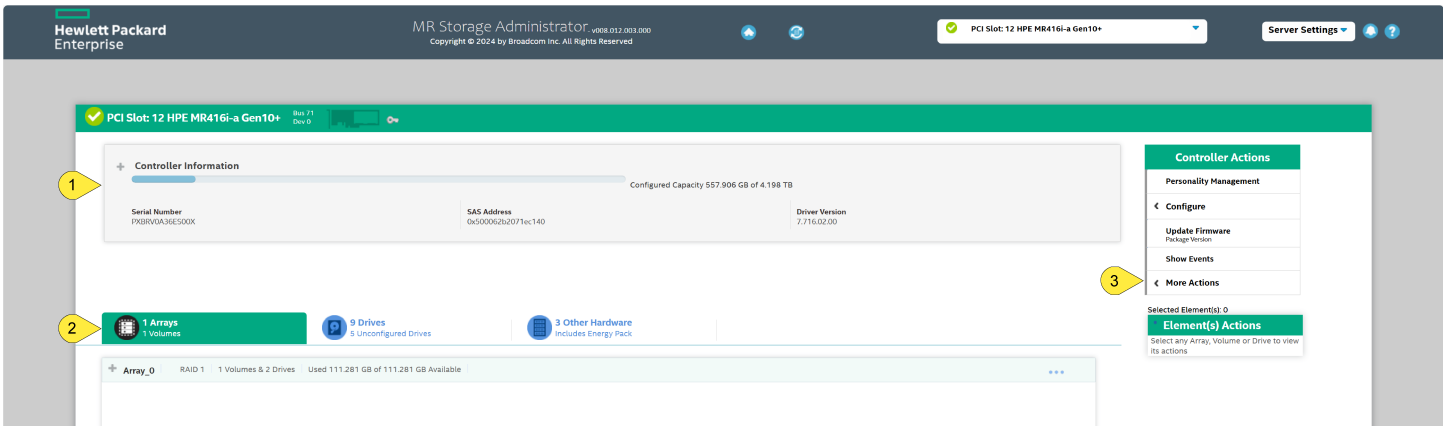


Table 7: Controller Dashboard Description

Callout	Description
1	**Controller Summary** – Displays the name of the MegaRAID controller card. The color-coded icons indicate the status of the controller card. Displays the basic controller properties, such as the controller serial number, vendor ID, SAS address, driver version, device ID, host interface, and so on. Click the icon to view the advanced properties of the controller, such as the NVRAM details, BIOS version, firmware properties, emergency spare properties, and so on.
2	**Controller Views** – Displays all of the configured arrays, volumes, and drives associated with the selected controller card. It also displays the hardware, such as enclosures and backplanes associated with the controller. All these views are displayed as tabs. Click the icon to view to view detailed information about the device. For example, click an array to view the associated volumes and drives. Select any device from the expanded view to perform relevant actions and view device properties.
3	**Controller Actions** – Lets you perform the following actions: • Create a configuration • Clear a configuration • Update the controller firmware • Import or clear foreign configurations • View premium features • View the event log

Controller Configurations

You can use the application to create and modify storage configurations on systems with Hewlett Packard Enterprise controllers.

You can create RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50, and RAID 60 storage configurations.

The supported RAID levels differ or might not be supported for some controllers. For more information, see HPE MR Storage Administrator Feature Support Matrix.

You can create these types of configurations:

- **Simple Configuration**
  Specifies a limited number of settings and has the system select drives for you. This option is the easiest way to create a volume. See Creating a New Storage Configuration Using the Simple Configuration Option for details.
- **Advanced Configuration**
  Lets you choose additional settings and customize volume creation. This option provides greater flexibility when creating volumes for your specific requirements. See Creating a New Storage Configuration Using the Advanced Configuration Option for details.

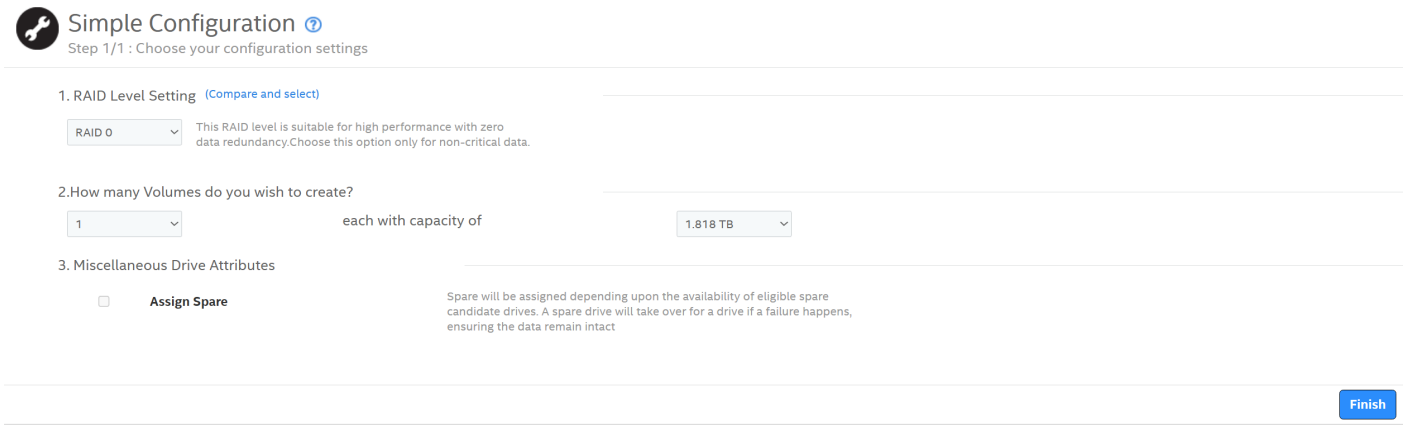
Creating a New Storage Configuration Using the Simple Configuration Option

The Simple Configuration option is the quickest and easiest way to create a new storage configuration. When you select Simple Configuration mode, the system creates the best configuration possible using the available drives.

Perform these steps to create a simple storage configuration:

1. Select **Configure** > **Simple Configuration** from the Server Dashboard or the Controller Dashboard.
   The **Simple Configuration** page opens.

   Figure 11: Simple Configuration Page



2. Select a RAID level for the array from the available RAID level option drop-down box.
3. (Optional) – Click **Compare and Select** to view detailed information about each RAID level.
   When you use the Simple Configuration option, the RAID controller supports RAID levels 0, 1, 5, 6, and 10. The window text provides a brief description of the RAID level that you select. The RAID levels you can choose depend on the number of drives available.

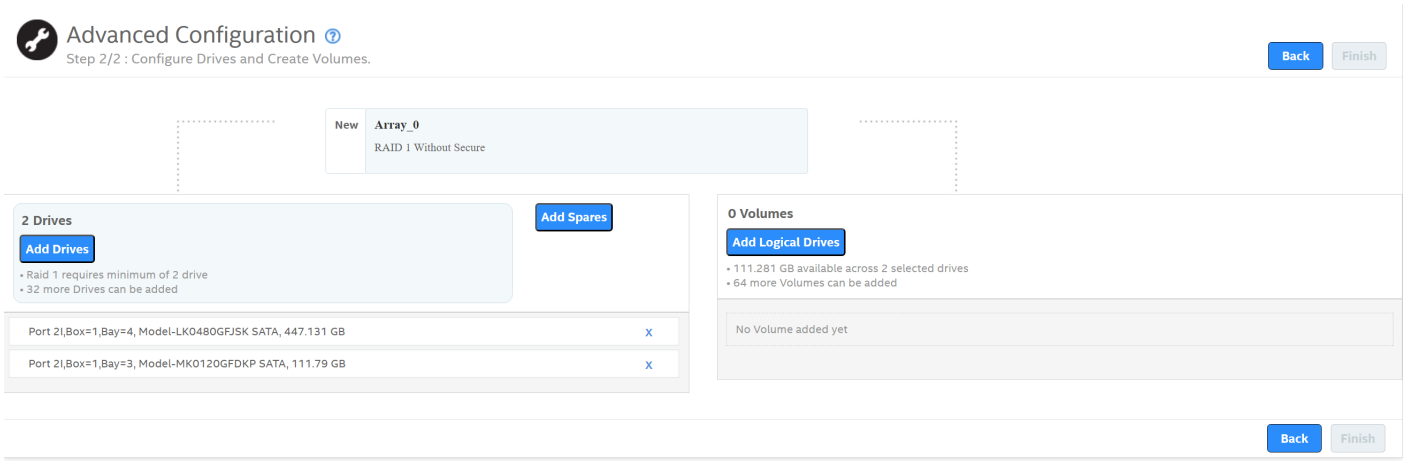
4. Select the number of volumes you want to create.
5. Select the capacity of the volumes.
   Each volume has the same capacity.
6. Select the **Assign Spare** check box if you want to assign a dedicated spare drive to the new volume.
   If an Unconfigured Good drive is available, that drive is assigned as a spare drive. Spare drives are drives that are available to replace failed drives automatically in a redundant volume (RAID 1, RAID 5, RAID 6, or RAID 10).
7. Click **Finish**.
   A message appears stating that the configuration is successfully created.

Creating a New Storage Configuration Using the Advanced Configuration Option

The Advanced Configuration option provides an easy way to create a new storage configuration. The Advanced Configuration option gives you greater flexibility than simple configuration because you can select the drives and the volume parameters when you create a volume. In addition, you can use the Advanced Configuration procedure to create spanned arrays. Perform these steps to create an advanced storage configuration.

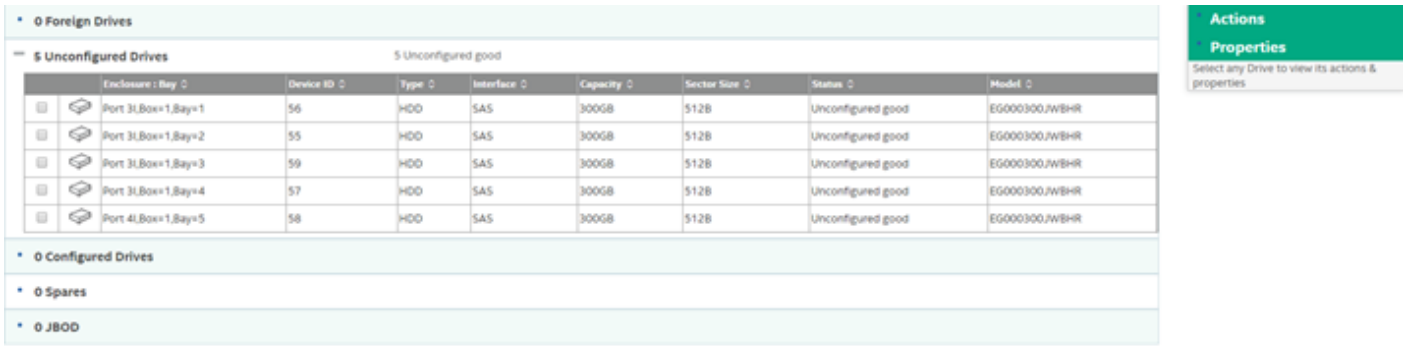
1. Select **Configure** > **Advanced Configuration** from the Server Dashboard or the Controller Dashboard.
   The **Advanced Configuration** page is displayed.

   Figure 12: Advance Configuration Page



2. Select a RAID level for the array from the drop-down box.
3. (Optional) – Click **Compare and Select** to view the detailed information on each RAID level.
   When you use the Advanced Configuration option, the RAID controller supports RAID levels 10, 50, and 60. The **Compare and Select** option provides you a brief description of the RAID level that you select. The RAID levels that you can choose depend on the number of drives available.
4. Click **Next**.
5. Click **Add Drives** to add drives to the array.
6. (Optional) – Select the span depth using the slider bar.
7. Click **Add Drives** to add drives to the array.
   The **Available Unconfigured Drive** window appears.

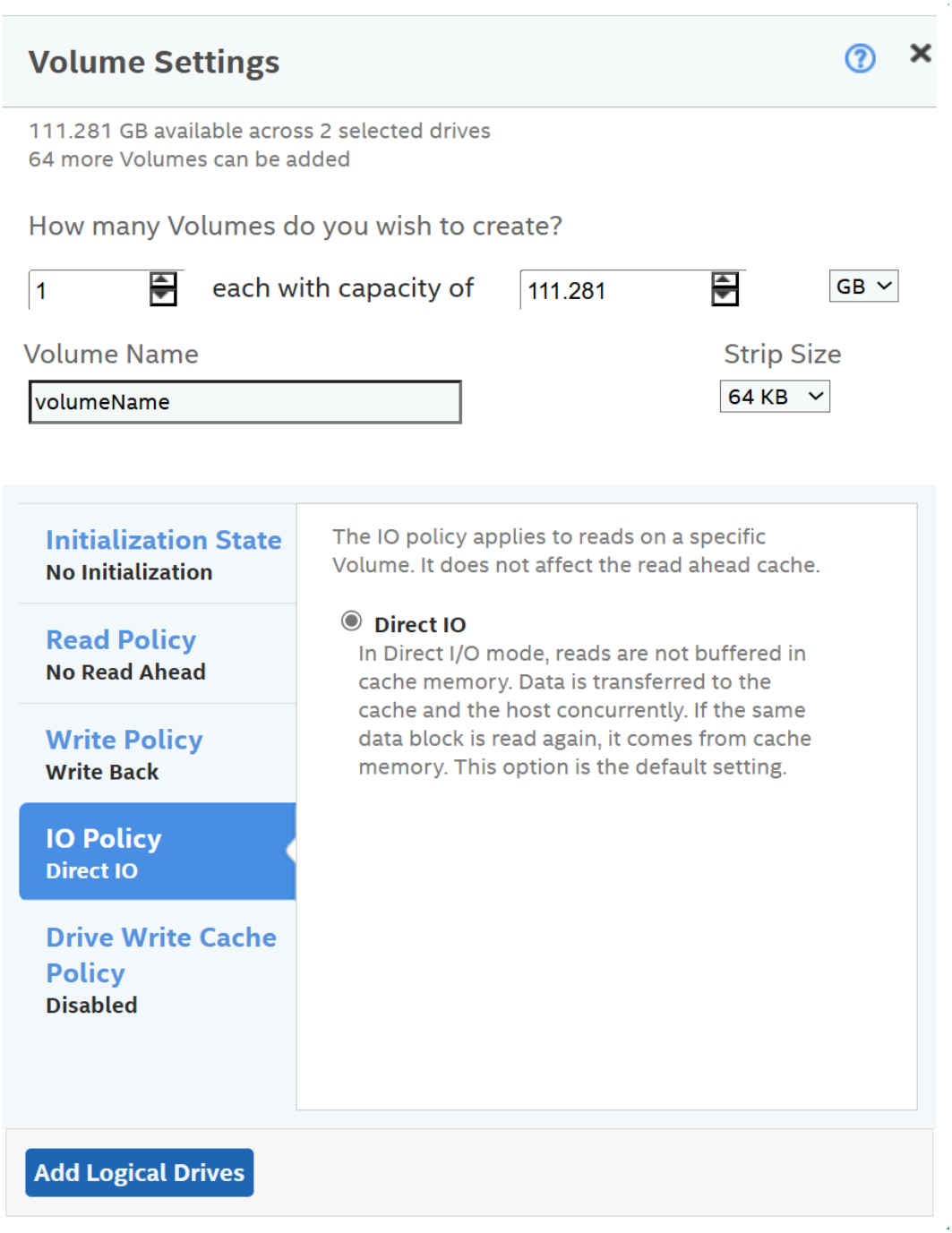
Figure 13: Available Unconfigured Drive Window



For information on adding unconfigured drives to the array, see Selecting Available Unconfigured Drives.

8. Select the drives from the list of available unconfigured drives and click **Add Drives**.
9. Click **Add Volumes** to add volumes to the array.
   The **Volume Settings** window appears.

Figure 14: Volume Settings Window



For information on configuring volumes, see Selecting Volume Settings.

10. Specify all the required details and click **Add Volumes**.
11. Click **Finish**.
    A message appears confirming that your configuration is complete.

Selecting Available Unconfigured Drives

The **Available Unconfigured Drive** window lets you add drives and spare drives to the array.

Perform these steps to add drives and spare drives to the array.

1. Select the drives to add from the **Available Unconfigured Drives** window, and click **Add Drives**.

   The selected drives appear in the **Advanced Configuration** window.

   You can click the  icon to remove the drives that you have already added.
2. Click **Add Spares** to add dedicated spare drives to the array.
   The **Available Unconfigured Drives** window appears.
3. Select the drives you want to add as spare drives and click **Add Spare Drives**.
   The selected spare drives appear in the **Advanced Configuration** window.

Selecting Volume Settings

The **Volume Settings** window enables you to configure the volumes. Detailed descriptions for all of the parameters are present in the **Volume Settings** window.

The volume settings differ or might not be supported for some controllers. For more information, see HPE MR Storage Administrator Feature Support Matrix.

Perform these steps to configure a volume:

1. Specify the number of volumes you want to create.
2. Specify the size of the volumes you want to create.

   Each volume has the same capacity. If you specify the capacity first and then the number of volumes, the volume capacity is adjusted with the available capacity.
3. Specify a name for the volume in the **volume Name** field.

   The volume name can have a maximum of 15 characters.
4. Select a strip size from the **Strip Size** drop-down list.
   Strip sizes of `64 KB`, `128 KB`, `256 KB`, `512 KB`, and `1 MB` are supported.
5. Specify the initialization state.
   The options follow:
   - **Fast Initialization**
   - **Full Initialization**
   - **No Initialization**
6. Specify the read policy for the volume.
   The options follow:
   - **No Read Ahead**
   - **Always Read Ahead**
7. Specify the write policy for the volume.
   The options follow:
   - **Write Through**
   - **Write Back**
   - **Always Write Back**

8. Specify the I/O policy for the volume.
   The options follow:
   - **Cached IO**
   - **Direct IO**
9. Specify a disk cache setting for the volume.
   The options follow:
   - **Unchanged**
   - **Disabled**
   - **Enabled**
10. Click **Add volumes**.
    The newly created volume appears in the **Advanced Configuration** window just below the **volumes** section.

    NOTE

    You will lose some drive capacity if you choose drives with uneven and large capacity while creating a volume.

    If you want to modify the volume settings before completing the configuration, click the  icon.

    The **volume Settings** window opens.

    Modify the settings as desired and click **Modify volume**.

Clearing the Configuration

You can clear all existing configurations on a selected controller.

Perform these steps to clear the existing configurations on a controller.

1. Navigate to the Controller Dashboard.
2. Click **Configure**, then click **Clear Configuration**.
   A confirmation message appears.
3. Select **Confirm** and click **Yes, Clear configuration** to clear existing configurations on the controller.

   NOTE
   Operating system or file system drives cannot be cleared.

Importing or Clearing Foreign Configurations

A foreign configuration is a RAID configuration that already exists on a replacement set of drives that you install in a computer system. You can use the application to import the foreign configuration to the controller or clear the foreign configuration so that you can create a new configuration using these drives.

Perform these steps to import or clear foreign configurations.

1. Navigate to the Controller Dashboard.
2. Click **Configure**, then click **Foreign Configuration**.
   The **Foreign Configuration** window appears, which lists all of the foreign configurations.
3. Click one of these options:
   - **Import All**: Import the foreign configurations from all the foreign drives.
   - **Clear All**: Remove the configurations from all the foreign drives.

4. Click **Re-Scan** to refresh the window.

UNMAP Capability Feature

The UNMAP capability feature is a SCSI command that is used to reclaim unused LBAs from the SSD. The UNMAP feature allows an application or OS to tell the storage array that the disk blocks contain deleted data so the array can deallocate the blocks. Deallocation reclaims storage space and helps in wear leveling management. Using the UNMAP capability feature extends the SSD lifespan.

NOTE
The UNMAP Capability feature can be enabled on the volume using SAS and NVMe SSD only.

UNMAP Capability Feature Behavior

MRSA behavior for MegaRAID 7.8 designs and later include the behaviors that follow.

- Display the PD Property, whether the PD (physical drive) is UNMAP capable or not.
- Display the PD Capability, whether the PDs can be used for volumes for the UNMAP feature.
- Lets users create an UNMAP supported volume.

MRSA behavior for MegaRAID 7.8 designs include the following limitations.

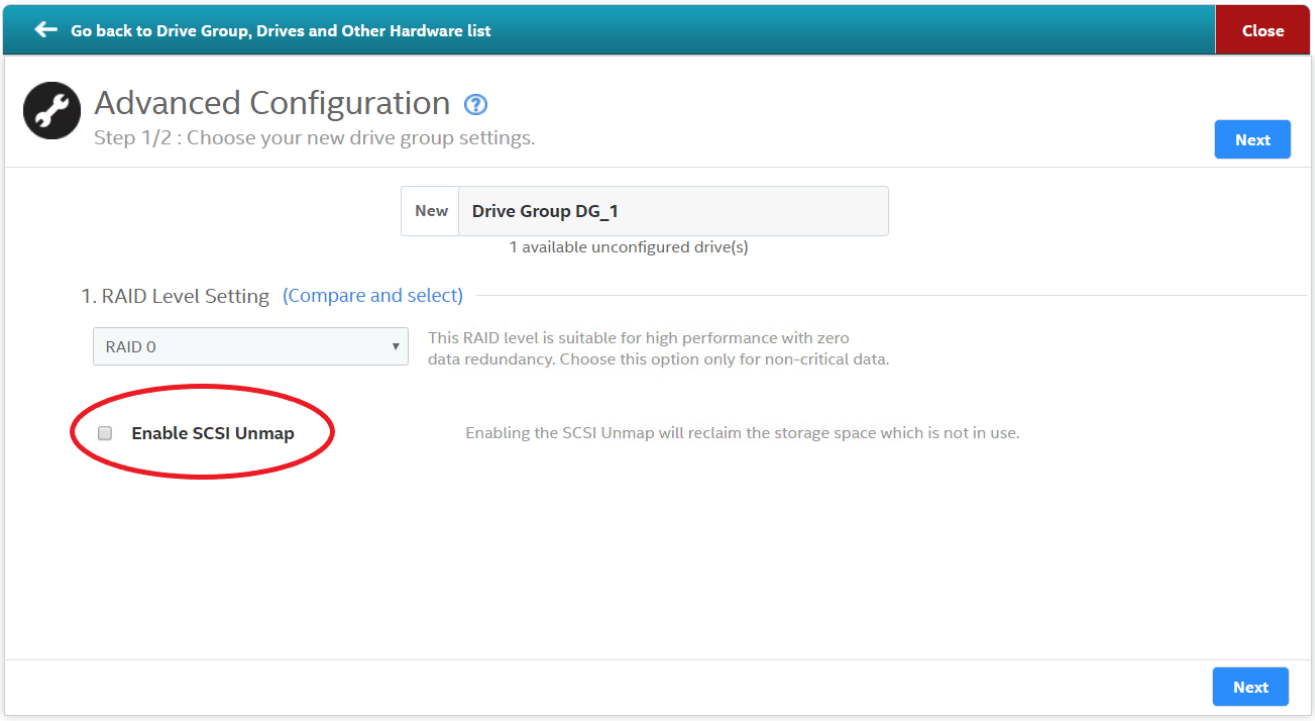
- The UNMAP feature is not supported for EPD/JBOD designs.
- Host software applications cannot support firmware in designs earlier than MegaRAID 7.8 because of the change in the MegaRAID firmware API.

UNMAP Feature Support

When using the UNMAP feature, you can perform the actions that follow.

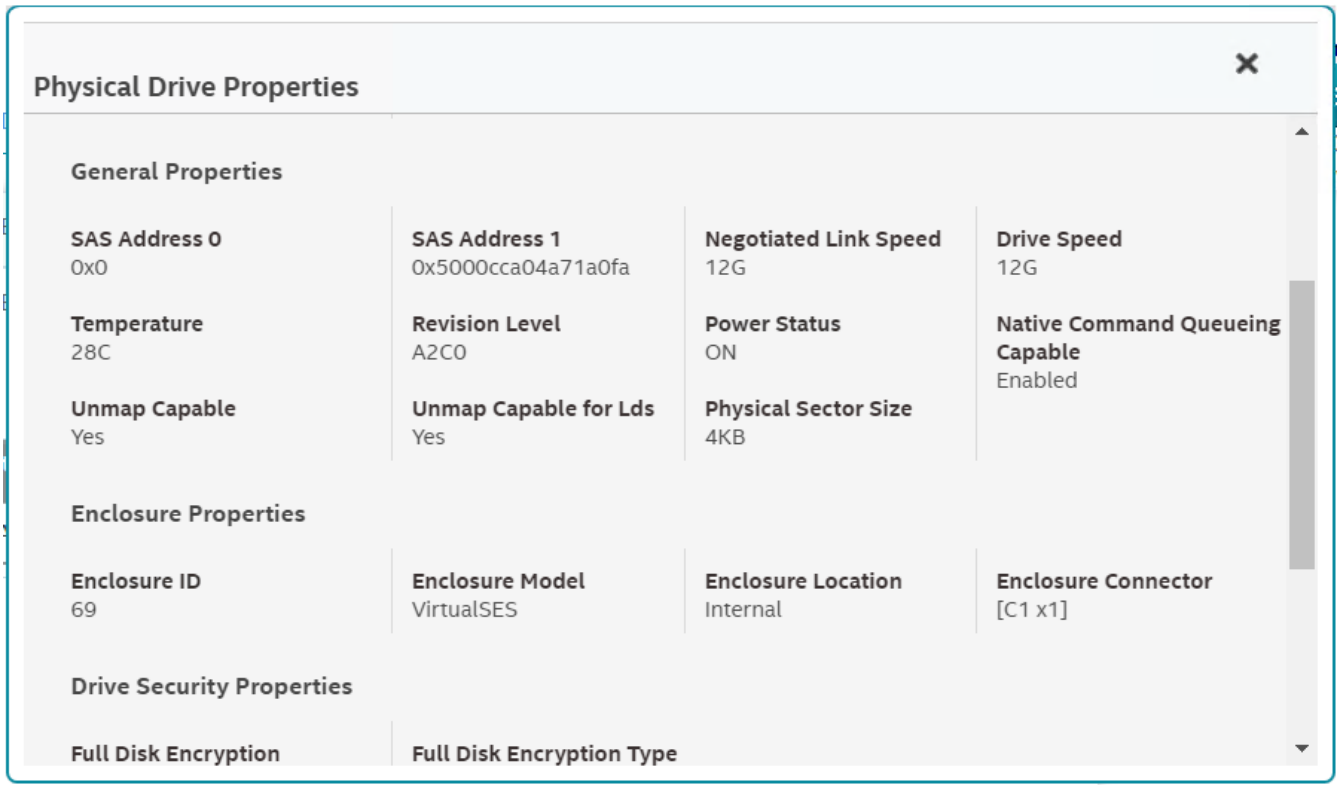
- Enable the UNMAP capability during SCSI volume creation.

Figure 15: Enable the UNMAP Feature During Volume Creation



- Show the PD level UNMAP properties.

Figure 16: Drive Level UNMAP Properties Window



Changing Behavior Modes

Perform the following steps to change the behavior mode and parameters:

1. In the **Change Personality** page, select the **Change Auto-configure behavior** check box.
2. From the **Select Behavior Mode** drop-down list, select an appropriate behavior mode.

   The available behavior modes are based on the current firmware support.

   - **Unconfigured Good/NONE** – If a user selects this option when a new disk or an old disk with no DDF (Data Disk Format) metadata is inserted in the system, it becomes Unconfigured Good Drive. The Unconfigured Good Drive keeps in Unconfigured Good after a reboot.
   - **JBOD** – If all the physical drives are in unconfigured good state, once you select the JBOD mode, all the physical drives are automatically converted to JBOD physical drives. When a new disk or old disk with new DDF metadata is inserted in the system, it becomes a JBOD. The Unconfigured Good Drive is automatically converted to JBOD after a reboot.

     NOTE

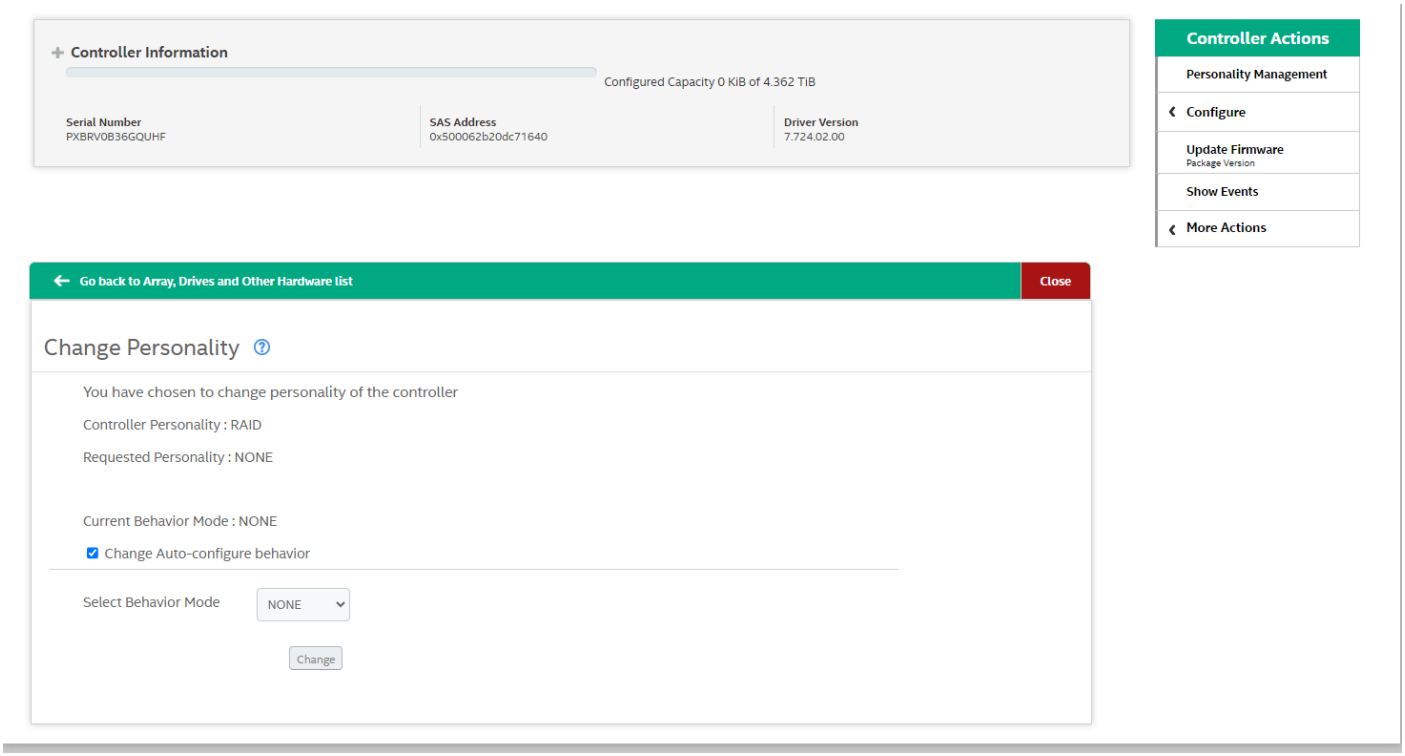
     For firmware versions earlier than 52.26.3-5250, Auto-Configure behavior is set to JBOD and cannot be configured for all the controller models.

     For firmware versions 52.26.3-5250 or later, Auto-Configure behavior can be configured.

     For HPE MR200 controllers, by default it is set to JBOD.

     For HPE MR400 controllers, by default it is set to None.

Figure 17: Change Personality Dialog



3. Select the appropriate behavior mode and click **Change**.

Background Operations Support

The application provides background Pause, Resume, Abort, Pause All, Resume All, and Abort All features that enhance the functionality where operations running in the background on a drive or a volume can be paused for some time, and resumed later.

The background operations, including Consistency Check, Rebuild, Replace, and Initialization are supported by an Abort operation. If any operation is stopped before completion, it is considered to be aborted. An aborted operation cannot be resumed from the place where it was stopped.

To perform Pause, Resume, and Abort operations, go to the **Background Processes in Progress** window in the Server dashboard or the Controller dashboard, and perform the following steps. The **Background Processes in Progress** window appears.

Figure 18: Background Processes in Progress Window

- **Pause** – Click **Pause** to suspend the background operation taking place at that particular point of time.
  When the operations are paused, the **Resume** option appears instead of the **Pause** option.
- **Resume** – Click **Resume** to resume the operation from the point where it was suspended.
- **Abort** – Click **Abort** to abort the ongoing active operation.
- **Pause All** – Click **Pause All** to suspend all the active operations.
  This option is enabled only if one or more background operations are in an Active state.
- **Resume All** – Click **Resume All** to resume all Paused operations from the point at which they were paused.
  This option is disabled if no operations are paused.
- **Abort All** – Click **Abort All** to abort all active operations.

  NOTE

  If the Copyback progress bar does not automatically display the progress of the Copyback operation for small-size volumes, set the maximum event grouping time gap to `0` in the `LSA.conf` file.

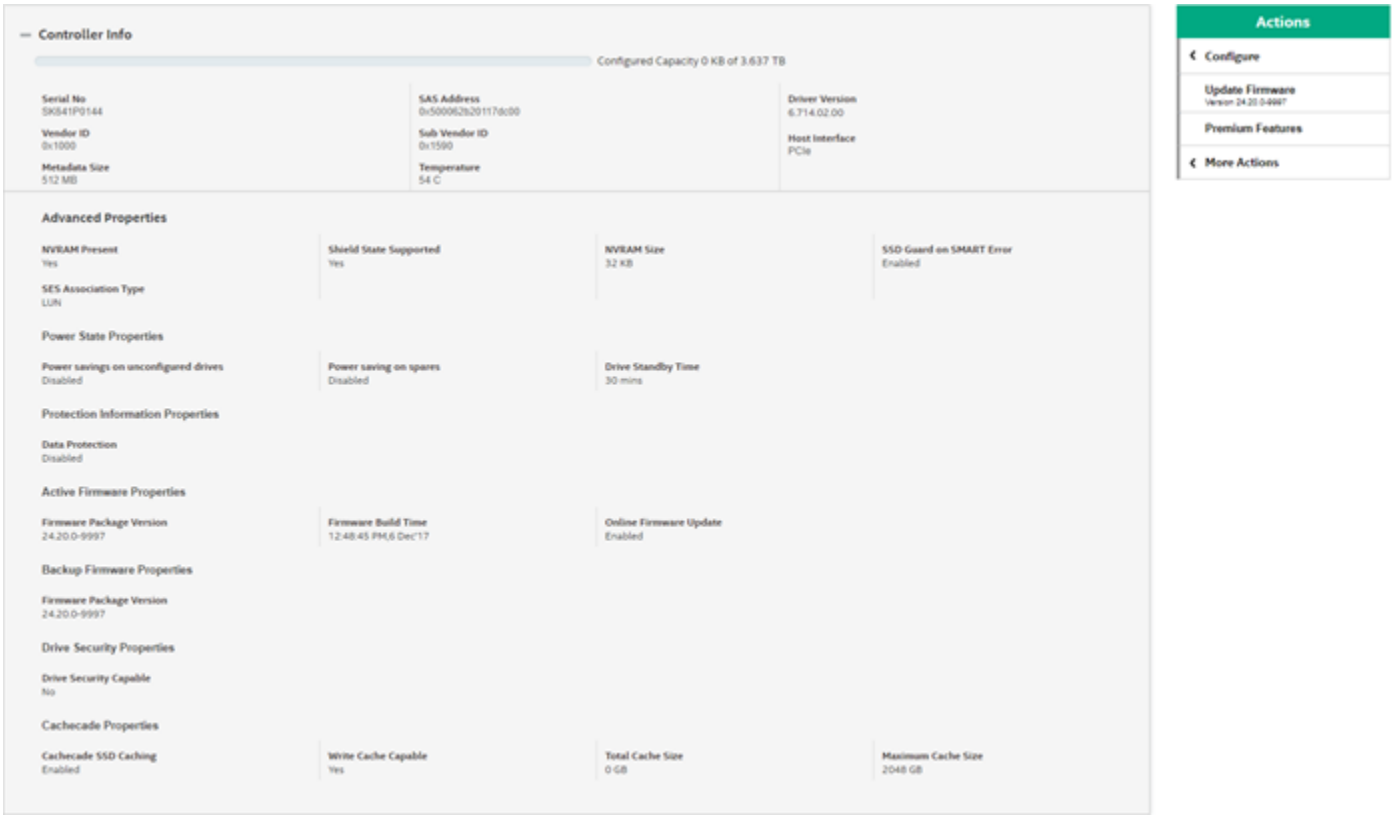
Managing Controllers

The HPE MR Storage Administrator application lets you monitor the activity of all the controllers present in the system and the devices to which they are attached.

Viewing Controller Properties

The Controller Dashboard displays basic controller properties. Click the icon to view the advanced properties of the controller.

Figure 19: Basic and Advanced Controller Properties Window



Running Consistency Checks

The Consistency Check operation verifies the correctness of the data in volumes that use RAID levels 1, 5, 6, 10, 50, and 60, configurations. For example, in a system with parity, checking consistency means calculating the data on one drive and comparing the results to the contents of the parity drive. You should periodically run a consistency check on fault-tolerant volumes.

Because RAID 0 does not provide data redundancy, you cannot run a consistency check on RAID 0 volumes.

To run a consistency check, you must first set the Consistency Check properties, then you can either schedule a consistency check to run at a defined interval chosen by you or you can start the Consistency Check operation immediately.

Setting Consistency Check Properties

Perform these steps to set the properties for a consistency check.

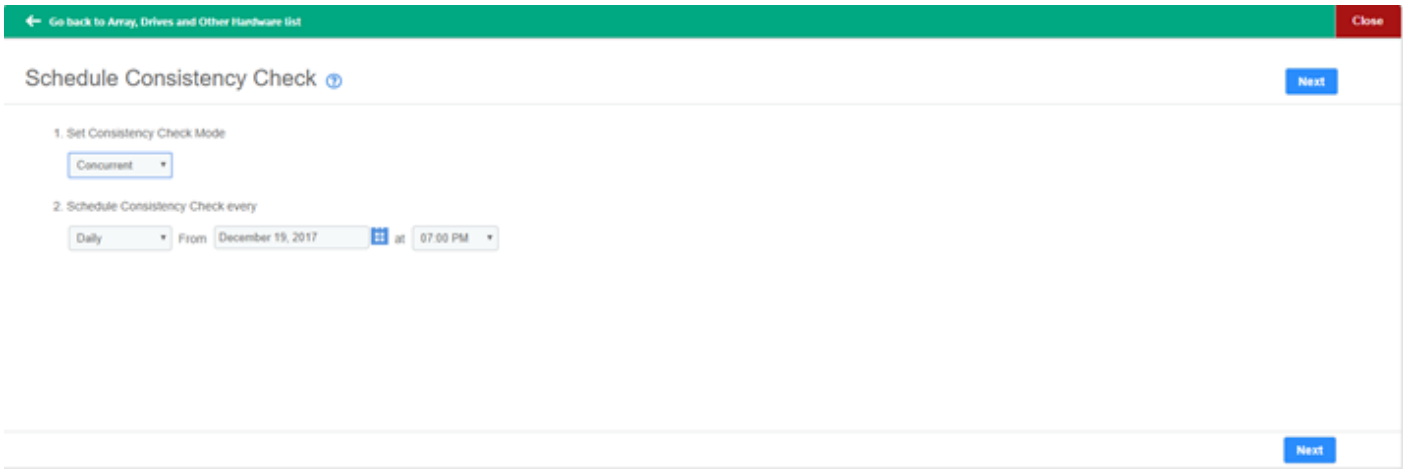
1. In the Controller Dashboard, select **More Actions** > **Set Consistency Check Properties**.
   The **Set Consistency Check Properties** dialog appears.
2. Choose one of these two options:
   - **Continue Consistency Check and Fix Error** – The RAID controller continues the consistency check, and if it finds any errors, fixes them.
   - **Stop Consistency Check On Error** – The RAID controller stops the consistency check operation if it finds any errors.
3. Click **Save**.

Scheduling a Consistency Check Operation

Perform these steps to schedule a Consistency Check operation:

1. In the Controller Dashboard, select **More Actions** > **Schedule Consistency Check**.
   The **Schedule Consistency Check** page appears.

   Figure 20: Schedule Consistency Check Dialog



2. Set the **Consistency Check Mode**.
   The available options are:
   - **Concurrent** – Run a Consistency Check operation concurrently on all volumes.
   - **Sequential** – Run a Consistency Check operation on one volume at a time.
   - **Disable** – Disables the Consistency Check feature.
3. Set the desired interval at which you want to check the consistency of a drive.
   The available options are:
   - **Hourly**, **Daily**, **Weekly**, **Monthly**, and **Continuously**.
   - Select an appropriate date and time range.
4. Click **Next**.

   The **Schedule Consistency Check** page appears, letting you add the volumes on which you want to perform a Consistency Check operation.

5. Click **Add Volumes**.

   The **Available Volume** dialog appears which lists all the volumes present in the selected array.

6. Select the volume on which you want to run the a Consistency Check operation.
7. Click **Save**.

   The consistency check runs based on the frequency/interval chosen by you. You can also monitor the progress of the consistency check operation. See Background Operations Support

8. (Optional) – Select the volume, from the Controller View section, on which you want to immediately perform a Consistency Check operation, then go to **More Actions** > **Start Consistency Check**.

   NOTE
   If you try to run a Consistency Check operation on a volume that has not been initialized, a confirmation dialog appears, asking for your confirmation.

Running a Patrol Read Operation

The Patrol Read option lets you periodically verify all sectors of the drives connected to a controller, including the system reserved area in the RAID configured drives. You can run a Patrol Read operation for all RAID levels and for all spare drives. A Patrol Read operation is initiated only when the controller is idle for a defined period and has no other background activities. You can set the Patrol Read properties and start the Patrol Read operation, or you can start the Patrol Read operation without changing the properties.

Setting the Patrol Read Properties

Perform these steps to set the Patrol Read properties.

1. Select **More Actions** > **Set Patrol Read Properties** in the Controller Dashboard.
   The **Available Volumes** dialog appears.
2. Select the volumes for which you want to set the Patrol Read properties and click **Add Volumes**.
   The **Set Patrol Read Properties** dialog appears.
3. Click **Select Volumes**.

   Click the icon to remove the volumes you have already added.

4. Click **Next**.
5. Perform these steps to set the properties:
   a) Select an operation mode for patrol read from the **Set Patrol Read Mode** drop-down list.
      The options follow:
      - **Automatic** – The Patrol Read operation runs automatically at the time interval you specify.
      - **Manual** – The Patrol Read operation runs only when you manually start it, by selecting **Start Patrol Read** from the Controller Dashboard.
      - **Disabled** – The Patrol Read operation does not run.

   b) (Optional) – Specify a maximum number of drives to include in the Patrol Read operation concurrently.
      The count must be a number from 1 to 255.
   c) Select the frequency at which the Patrol Read operation runs from the drop-down list.
      The default frequency is **Weekly** (168 hours), which is suitable for most configurations. The other options are **Hourly**, **Daily**, and **Monthly**.

d) Select the month, day, and year on which to start the Patrol Read operation.
e) Select the time of day to start the Patrol Read operation.
f) (Optional) – Select the **Start Patrol Read Now** check box.
g) (Optional) – Select the **Run Patrol Read Non-Stop** check box.

6. Click **Finish**.
   You can monitor the progress of the Patrol Read operation. See Background Operations Support.

Starting a Patrol Read Operation

Perform these steps to start a Patrol Read operation.

1. Select **More Actions** > **Start Patrol Read** on the Controller Dashboard.
   A warning message appears.
2. Click **Start Patrol Read** to start a Patrol Read operation.
   You can monitor the progress of the Patrol Read operation. See Background Operations Support.

Stopping a Patrol Read Operation

Perform this step to stop a Patrol Read operation.

Select **More Actions** > **Stop Patrol Read** on the Controller Dashboard.

Managing SAS Storage Link Speed

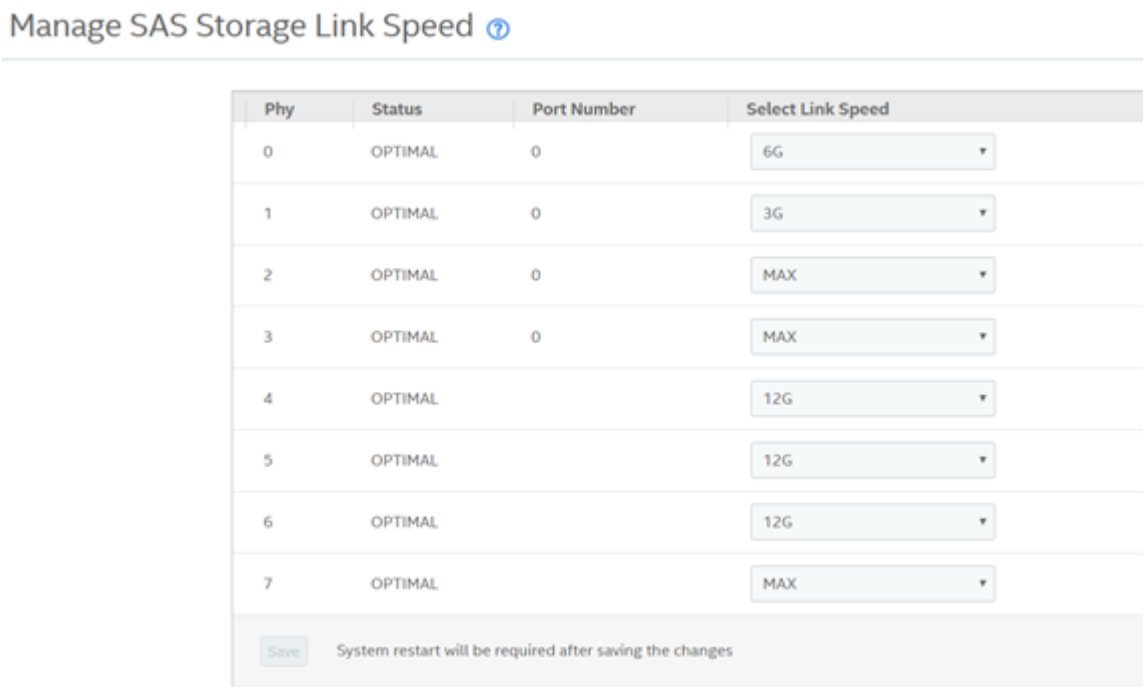
The Managing SAS Storage Link Speed feature lets you change the link speed between the controller and an expander or between the controller and a drive that is directly connected to the controller. All phys in a SAS port can have different link speeds or can have the same link speed. You can select a link speed setting. However, if phys in a SAS port have different link speed settings and if a phy is connected to a drive or an expander, the firmware overrides the link speed setting you have selected and instead uses the common maximum link speed among all the phys.

NOTE
Lane speeds for UBM backplanes cannot be modified.

Perform these steps to change the link speed.

1. Select **More Actions** > **Manage SAS Storage Link Speed** on the Controller dashboard.
   The **Manage SAS Storage Link Speed** dialog appears.

Figure 21: Manage SAS Storage Link Speed Window



- The **Phy** column displays the system-supported phy link values.
  The phy link values range from 0 through 7.
- The **Status** column displays the status of the link speed.
- The **Port Number** column displays the port numbers.
- The **Select Link Speed** column displays the phy link speeds.

2. Select the desired link speed from the **Select Link Speed** field using the drop-down selector.
   The link speed values are **MAX**, **3G**, **6G**, or **12G**.

   By default, the link speed in the controller is set to **MAX** or the value last saved by you. The 12G link speed is supported for some SAS-3 expanders.
3. Click **Save**.
   The link speed value is now reset. The change takes place after you restart the system.

Managing PCIe Storage Interface

A lane represents a set of differential signal pairs, one pair for transmission and one pair for reception, similar to SAS phys.

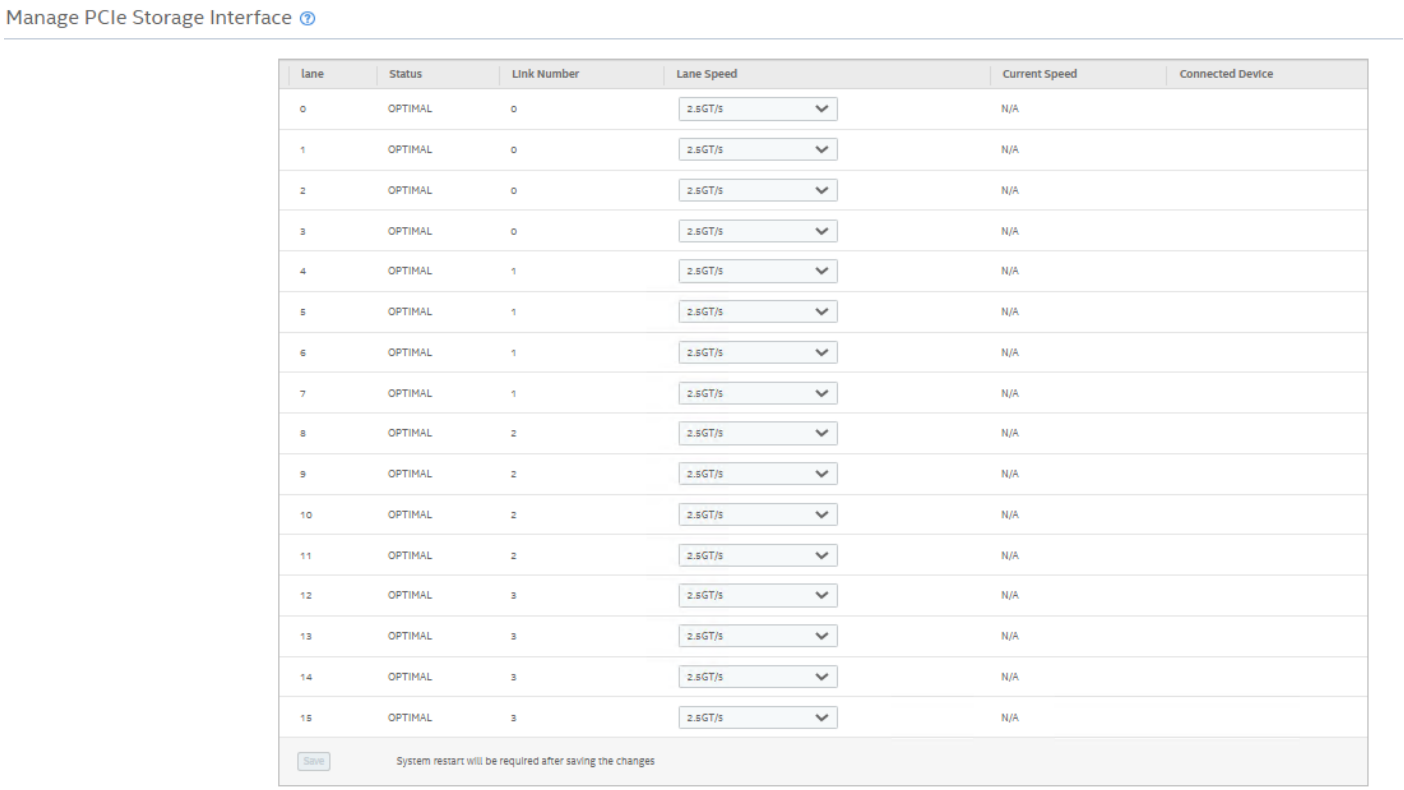
The Managing PCIe Storage Interface feature allows you to change the lane speed between a controller and an expander or between the controller and a drive that is directly connected to the controller. MRSA 2.4 and later versions support both SAS/SATA topologies and PCIe topologies using the same device phys to manage the lane speed.

> **NOTE**
> Lane speeds for UBM backplanes cannot be modified.

Perform the following steps to change the lane speed.

1. In the Controller dashboard, select **More Actions** > **Manage PCIe Storage Interface**.
   The **Manage PCIe Storage Interface Dialog** appears.

Figure 22: Manage PCIe Storage Interface Dialog



- The **Lane** column displays the system-supported lane values.
- The **Status** column displays the status of the lane.
- The **Link Number** column displays the link numbers.
- The **Lane Speed** column displays the lane speed.

2. Select the desired lane speed from the **Lane Speed** field using the drop-down selector.
   The lane speed values are **Unknown**, **2.5GT/s**, **5GT/s**, **8GT/s**, and **16GT/s**.

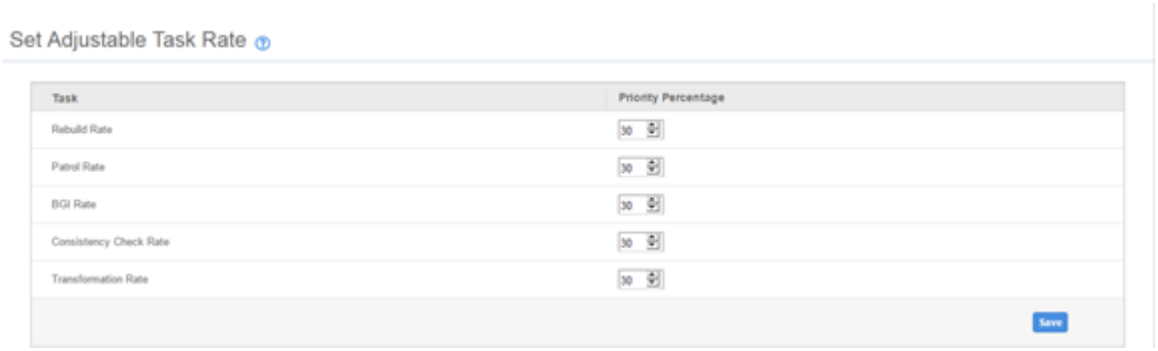
   By default, the lane speed in the controller is **8GT/s** or the value last saved by you.
3. Click **Save**.
   The lane speed value is now reset. The change takes place after you restart the system.

Setting Adjustable Task Rates

Perform these steps to set the adjustable task rates.

1. Select **More Actions** > **Set Adjustable Task Rate** on the Controller Dashboard.
   The **Set Adjustable Task Rates** dialog appears.

Figure 23: Set Adjustable Task Rate Dialog



2. Enter changes, as needed, in the following task rates:

   NOTE
   Setting any of these rates to perform faster can result in the system I/O rate being slower.

   - **Rebuild Rate** – Enter a number from 0 to 100 to control the rate at which a rebuild is performed on a drive when it is necessary.

     The higher the number, the faster the rebuild occurs.
   - **Patrol Rate** – Enter a number from 0 to 100 to control the rate at which Patrol Read operations are performed.

     The Patrol Read function monitors drives to find and resolve potential problems that could cause drive failure. The higher the number, the faster the Patrol Read operation occurs.
   - **Background Initialization (BGI) Rate** – Enter a number from 0 to 100 to control the rate at which volumes are initialized in the background.

     Background initialization establishes mirroring or parity for a RAID volume while allowing full host access to the volume. The higher the number, the faster the initialization occurs.
   - **Check Consistency Rate** – Enter a number from 0 to 100 to control the rate at which a consistency check is performed.

     A Consistency Check operation scans the consistency data on a fault tolerant volume to determine whether the data has become corrupted. The higher the number, the faster the Consistency Check operation is performed.
   - **Transformation Rate** – Enter a number from 0 to 100 to control the rate at which transformation of a volume occurs.

     The higher the number, the faster the transformation occurs.

3. Click **Save** to set the new task rates.

Discarding Pinned Cache

If the controller loses access to one or more volumes, the controller preserves the data from the volume. This preserved cache is called *pinned cache*. This cache is preserved until you import the volume or discard the cache. As long as pinned cache exists, you cannot perform certain operations on the volume.

ATTENTION

If foreign configurations exist, import the foreign configuration before you discard the pinned cache. Otherwise, you might lose data that belongs to the foreign configuration.

Perform these steps to discard the pinned cache.

1. Select **More Actions** > **Discard Preserved Cache** on the Controller Dashboard.

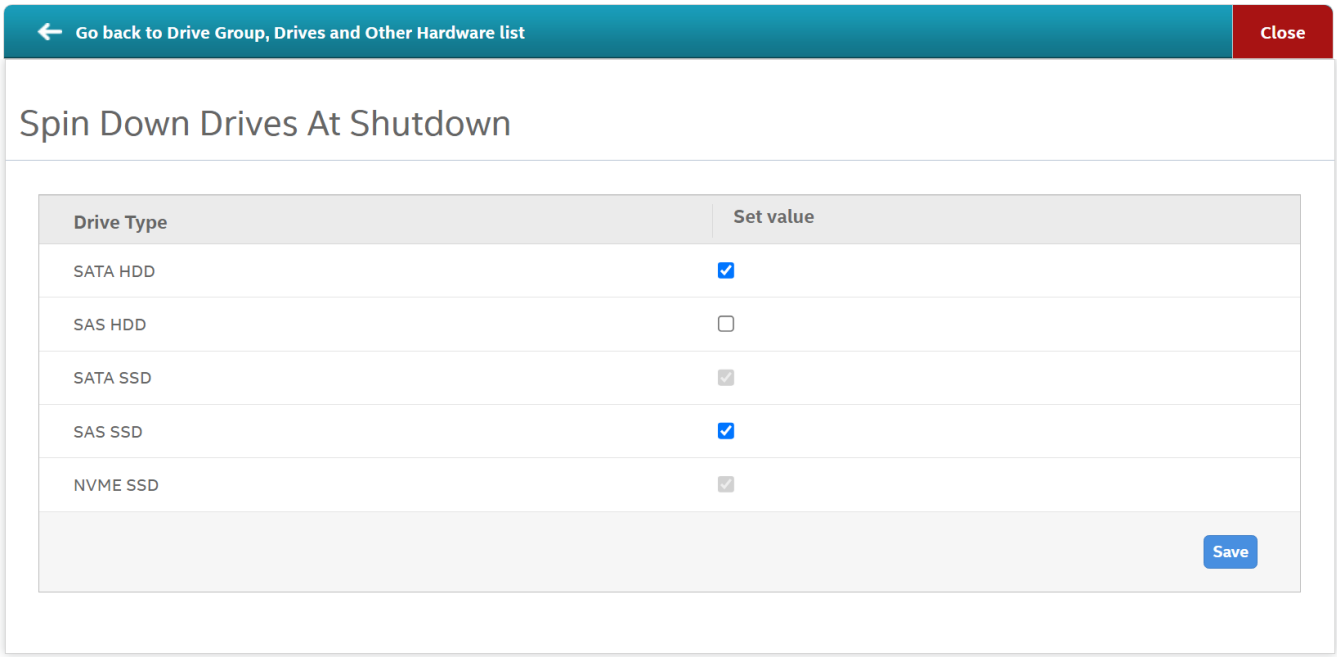
   NOTE
   The **Discard Preserved Cache** option is displayed only if pinned cache is present on the controller.

   A message appears, prompting you to confirm your choice.
2. Select **Confirm** and click **Yes, Discard**.

Spin Down

LSA allows the controller operations to set spin down drives during a shutdown operation.

1. In the Controller dashboard, select **More Actions** > **Spin Down Drives At Shutdown**.
2. Select the **Drive Type** to spin down at shutdown.



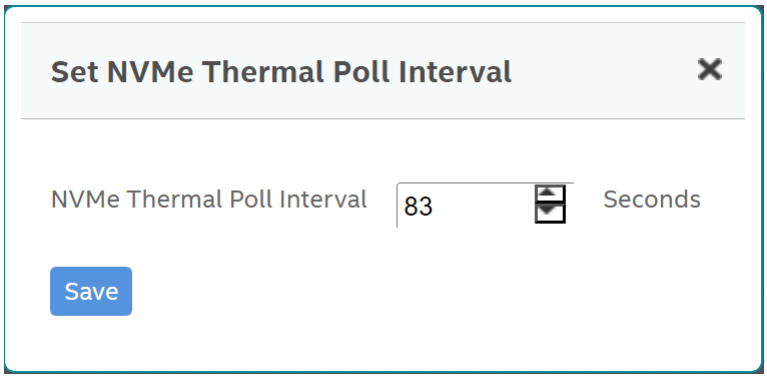
3. Click **Save**.

NVMe Thermal Poll Interval

Perform these steps to set the increase the frequency of temperature polling for NVMe drives. Adjusting the frequency of temperature polling helps achieve better cooling.

1. Select **More Actions** > **Set NVMe Thermal Poll Interval** on the Controller Dashboard.
   The **Set NVMe Thermal Poll Interval** dialog appears.

Figure 24: Set NVMe Thermal Poll Interval Dialog



2. Enter the thermal poll interval, in seconds.
3. Click **Save**.

Downloading the Serial Output Log

You can download the **Serial Output Log** file, which contains the firmware terminal log entries for the controller. The log information is shown as total number of entries available on the firmware side. Perform this step to download the Serial Output Log file.

Select **More Actions** > **Download Serial Output Log** on the Controller Dashboard.

The `Serial_Output_Log` file is downloaded.

Updating the Controller Firmware

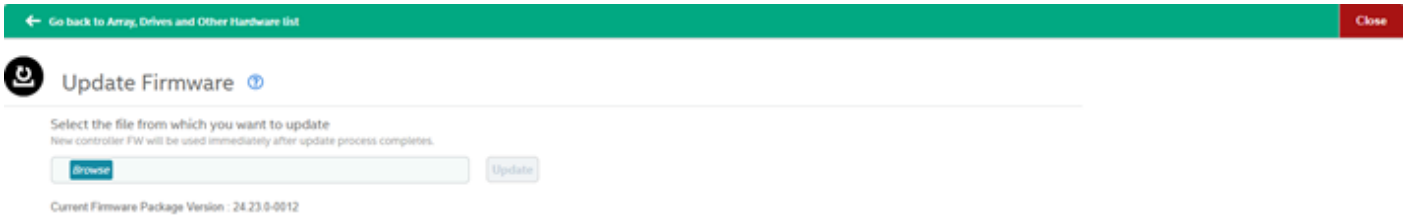
The application lets you update the controller firmware.

Perform these steps to update the controller firmware.

1. Navigate to the Controller Dashboard.
2. Click **Update Firmware**.

   The **Update Firmware** window appears. It also displays the current controller firmware version.

   Figure 25: Update Firmware Window



3. Click **Browse** to locate and open the `.rom` file.
4. Click **Update**.

   After the update is complete, a message is displayed that confirms the success of the update and displays the new version of the controller firmware.

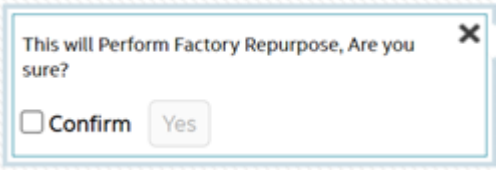
Clearing NVRAM

The application lets you clear the NVRAM.

1. Navigate to the Controller Dashboard.
2. Select **More Actions** > **Factory Repurpose** on the Controller Dashboard.

   A message appears, prompting you to confirm your choice.
3. Select **Confirm** > **Yes**.

   Figure 26: Perform Factory Repurpose Dialog



MegaRAID Advanced Software Features

The MegaRAID Advanced Software (Premium) are features that the HPE MR Storage Administrator application supports on certain HPE Smart Array MR controllers.

The MegaRAID advanced software includes these features:

- MegaRAID FastPath
- RAID 5 and RAID 6

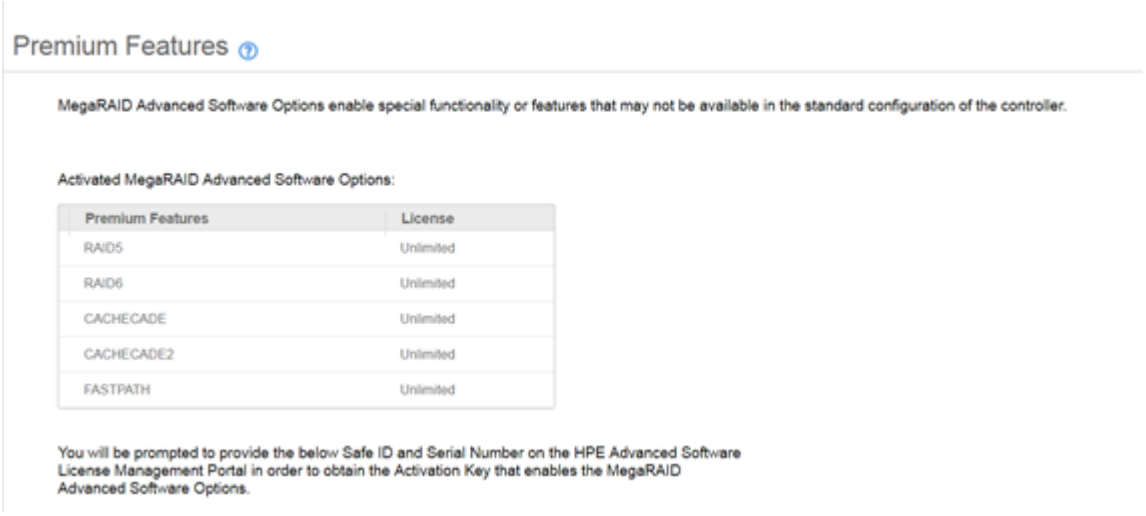
The MegaRAID software licensing authorizes you to enable the MegaRAID advanced software features. By default, the MegaRAID Advanced Software (Premium Features) is enabled.

The **Premium Features** option on the Controller Dashboard lets you use the MegaRAID Advanced Software features.

Perform these steps to use the advanced controller features:

1. Select **Actions** > **Premium Features** on the Controller Dashboard.
   The **Premium Features** window opens.

   Figure 27: Premium Features Window



MegaRAID Fast Path Advanced Software

The MegaRAID FastPath software is a high-performance I/O accelerator for solid state drive (SSD) arrays connected to a MegaRAID controller card. This advanced software is an optimized version of MegaRAID technology that can dramatically boost storage subsystem and overall application performance. Particularly those that demonstrate high random read/write operation workloads – when deployed with a MegaRAID SATA+SAS controller connected to SSDs.

MegaRAID SafeStore Encryption Services

The MegaRAID SafeStore software, together with self-encrypting drives (SEDs), secures a drive's data from unauthorized access or modification resulting from theft, loss, or repurposing of drives. If you remove an SED drive from its storage system or the server in which it resides, the data on that drive is encrypted, and it becomes useless to anyone who attempts to access it without the appropriate security authorization.

Auto Lock with Local Key Management locks the SED using an authentication key. When secured in this manner, the drive's data encryption key is locked whenever the drive is powered down. In other words, the moment the SED is switched off or unplugged, it automatically locks down the drive's data. When the drive is powered back on, it requires authentication before being able to unlock its encryption key and read any data on the drive. This action protects against any type of insider or external theft of drives or systems.

The instant Secure Erase feature allows you to instantly and securely render data on SED drives unreadable, saving businesses time and money by simplifying the decommissioning of drives and preserving hardware value for returns and repurposing.

You can enable, change, and disable the drive security feature. You can also import a foreign configuration using the SafeStore Encryption Services advanced software.

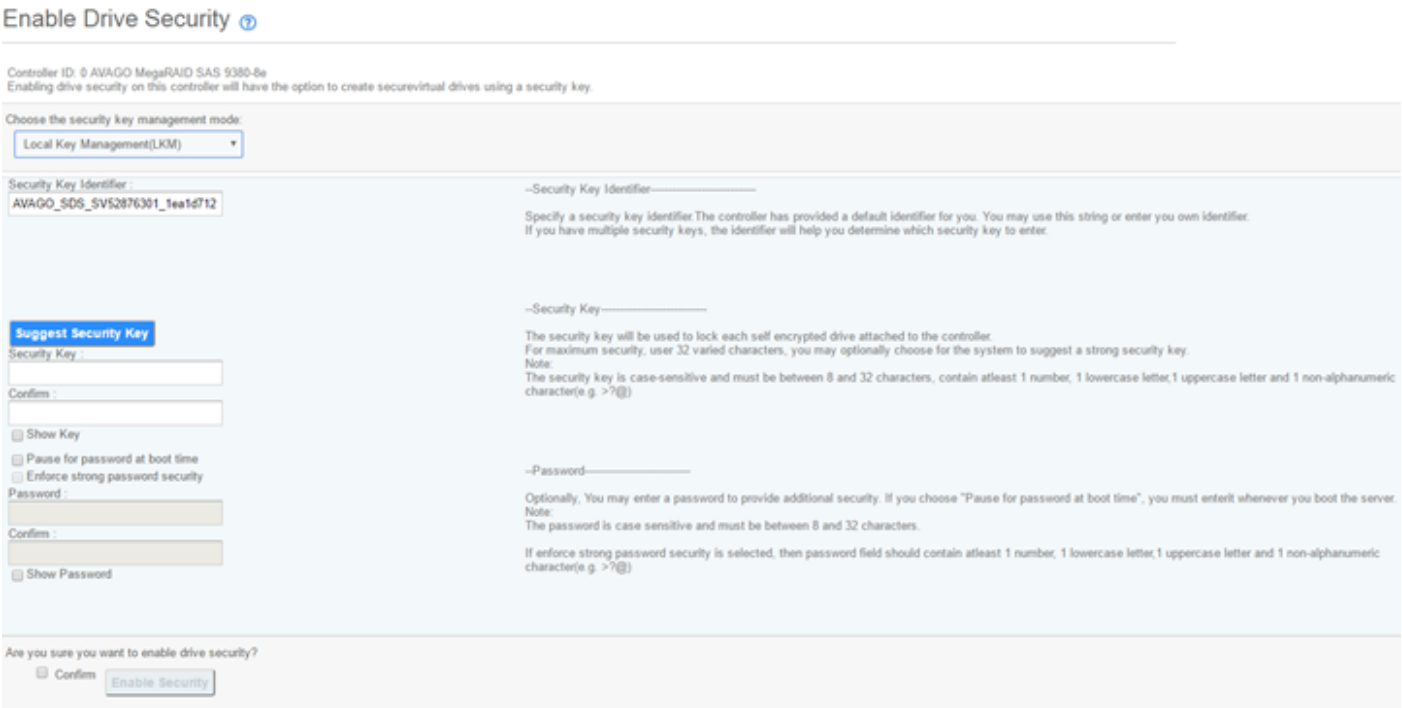
Enabling Drive Security

Ensure that MFC settings related to security are enabled in the firmware.
Perform the following steps to enable security on the drives.

1. In the Controller dashboard, select **More Actions** > **Enable Drive Security**.
2. Select the **Local Key Management (LKM)** option from the **Choose the security key management mode** drop-down list.

   The **Enable Drive Security** dialog appears with the following options that lets you enable the drive security.

   Figure 28: Enable Drive Security



   To enable drive security, the following details must be specified:

   - **Security Key Identifier** – The controller, by default, assigns a security key identifier.
     However, you can change this security key identifier as per your requirement. If you have more than one security key identifier, the controller helps you to determine which security key identifier to enter.
   - **Security Key** – Provides you with an option to create secure volumes by specifying the security key.

The security key provided by you locks each SED drive attached to the controller.

- **Suggest Security Key** – Alternatively, you can click this option to have the system create a security key for you.
- **Password** – You can also specify a password to provide additional drive security.
- **Pause for password at boot time** and **Enforce strong password security** – If you select the **Pause for password at boot time**, you are prompted to provide the password each time you restart your server.
  If you select **Enforce strong password security**, the system enforces you to specify a strong password.
- **Show Key** and **Show Password** – You can either select or clear the **Show Key** and **Show Password** check boxes. By default, they are not selected.

To enable drive security, perform the following steps:

3. Either use the default security key identifier provided by the controller or specify a new security key identifier.

   NOTE
   If you create more than one security key, ensure that you change the security key identifier. Otherwise, you cannot differentiate between the security keys.

4. Either click **Suggest Security Key** to have the system create a security key for you, or enter a new security key in the **Security Key** field and confirm.
5. (Optional) – Select the **Show Key** check box.

   If you choose this option, the security key that you specify, or the security key that is created by the system if you have clicked **Suggest Security Key**, will be visible to you. If you do not select this option, the security key will not be visible to you.

   NOTE
   Ensure that you note down this security key somewhere for future reference. If you are unable to provide the security key when it is required by the system, you will lose access to your data.

   The security key is case-sensitive. It must be between 8 and 32 characters and contain at least one number, one lowercase letter, one uppercase letter, and one nonalphanumeric character (for example, < > @ +). The space character is not permitted.

   Non-U.S. keyboard users must be careful not to enter double-byte character set (DBCS) characters in the security key field. The firmware works with the ASCII character set only.

6. (Optional) – Select the **Pause for password at boot time** check box.

   If you choose this option, you are prompted to provide the password each time you restart your server.

7. (Optional) – Select the **Enforce strong password security** check box.

   If you choose this option, make sure the password is between 8 and 32 characters and contain at least one number, one lowercase letter, one uppercase letter, and one non-alphanumeric character (for example, < > @ +). The space character is not permitted. The password is case-sensitive.

8. (Optional) – Enter a password in the **Password** field and confirm the same password once again in the **Confirm** field.
9. (Optional) – Select the **Show Password** check box.

   If you choose this option, the password that you specify will be visible to you. If you do not select this option, the password will not be visible to you.

   Warning messages appear if there is a mismatch between the characters entered in the **Password** field and the **Confirm** field, or if you have entered an invalid character.

CAUTION
Make sure to write down this password somewhere for future reference. If you are unable to provide the password when it is required by the system, you will lose access to your data.

10. Select the **Confirm** check box, then click **Enable Security** to confirm that you want to enable drive security on this controller.

Changing Drive Security Settings

NOTE
Drive security settings cannot be changed when EKM is enabled. Changes to drive security settings for EKM will fail from MRSA.

Perform the following steps to change the encryption settings for the security key identifier, security key, and password.

1. In the Controller dashboard, select **More Actions** > **Change Drive Security**.

   The **Change Drive Security** dialog appears.

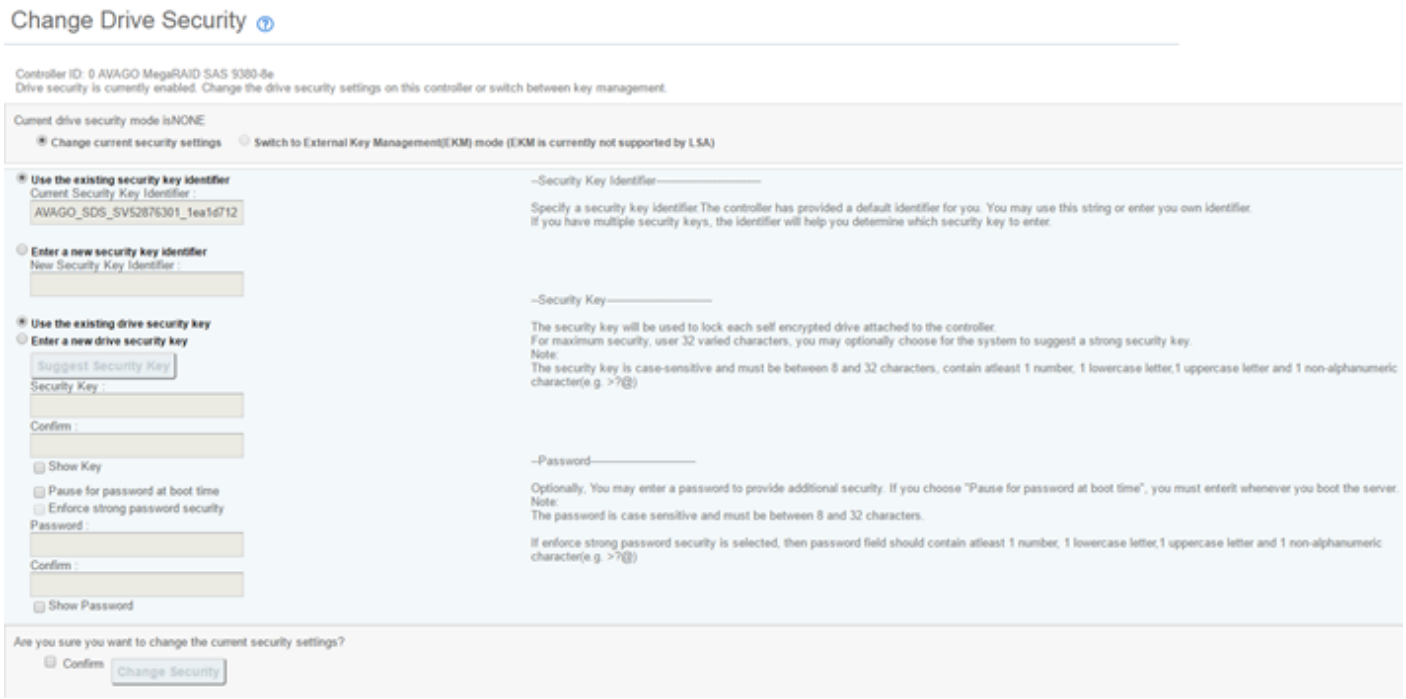
   Figure 29: Change Drive Security Dialog

2. Select the **Change current security settings** radio button from the **Current drive security mode is FW** field.

   When LKMS is enabled, MRSA will show the current drive security mode as**FW/USER** instead of LKM.

   The following options appear, which list the actions you can perform including editing the security key identifier, the security key, and the password.

   Figure 30: Change Drive Security Dialog Options



3. Either you can use the existing security key identifier assigned by the controller, or you can specify a new security key identifier.

   If you change the security key, you need to change the security key identifier. Otherwise, you cannot differentiate between the security keys.

4. Either select the **Use the existing drive security key** option or select the **Enter a new drive security key** to specify a new security key and confirm once again.
5. Either click **Suggest Security Key** to have the system create a security key, or you can enter a new security key in the **Security Key** text field.
6. (Optional) – Select the **Show Key** check box.

   NOTE
   The security key is case-sensitive. It must be between 8 and 32 characters and contain at least one number, one lowercase letter, one uppercase letter, and one non-alphanumeric character (for example, < > @ +).
7. (Optional) – Select the **Pause for password** at boot time check box.

   If you choose this option, you are prompted to provide the password each time you restart your server.
8. (Optional) – Select the **Enforce strong password security** check box.

   If you choose this option, make sure the password is between 8 and 32 characters and contain at least one number, one lowercase letter, one uppercase letter, and one non-alphanumeric character (for example, < > @ +). The space character is not permitted. The password is case-sensitive.
9. If you chose to use a password, either enter the existing password or enter a new password, and confirm once again.
10. (Optional) – Select the **Show Password** check box.

    If you choose this option, the password that you specify will be visible to you. If you do not select this option, the password will not be visible to you.
11. Select the **Confirm** check box and click **Change Security** to change the security settings.

    The **Authenticate Drive Security Settings** dialog appears. Your authentication is required for the changes to take effect. Enter the new security key that you just specified in the **Security Key** field.
12. Enter the new security key that you just specified and click **Authenticate** to authenticate the changes.

    The existing configuration on the controller is updated to use the new security settings.

Disabling Drive Security

ATTENTION
If you disable drive security, your existing data is not secure and you cannot create any new secure volumes. Disabling drive security does not affect the security of data on foreign drives. If you have removed any drives that were previously secured, you still need to enter the password when you import them. Otherwise, you cannot access the data on those drives. If there are any secure drive groups on the controller, you cannot disable drive security. A warning dialog appears if you attempt to do so. To disable drive security, you must first delete the volumes on all of the secure drive groups.

Perform the following steps to disable drive security:

1. In the Controller dashboard, select **More Actions** > **Disable Drive Security**.

   A warning message appears asking for your confirmation.
2. Select **Confirm** and click **Yes, Disable Drive Security**.

   The software disables drive security.

Importing or Clearing a Foreign Configuration – Security-Enabled Drives

Perform the following steps to import or clear foreign configuration for security-enabled drives.

1. Enable drive security to allow importation of security-enabled foreign drives.
2. After you create a security key, navigate to the Controller dashboard, and click **Configure**, then click **Foreign Configuration**.

   If locked drives (security is enabled) exist, the **Unlock Foreign Drives** dialog appears.
3. Enter the security key to unlock the configuration.

   The **Foreign Configuration** window appears, which lists all of the foreign configurations.
4. Click one of the following options:
   - **Import All**: Import the foreign configurations from all the foreign drives.
   - **Clear All**: Remove the configurations from all the foreign drives.
5. Click **Re-Scan** to refresh the window.
6. Repeat the import process for any remaining drives because locked drives can use different security key, and you must verify whether there are any remaining drives to be imported.

Managing Arrays

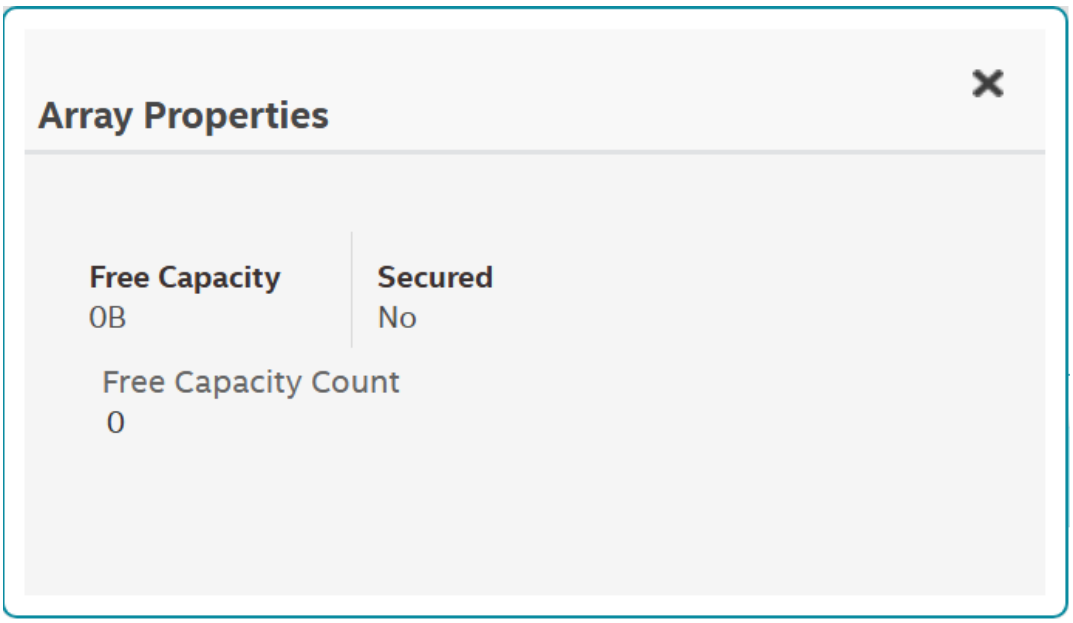
The HPE MR Storage Administrator application lets you monitor the status of arrays and spanned arrays. The following lists the array states:

- Optimal: An array whose members are all online.
- Partially Degraded: An array with a redundant RAID level that can sustain one or more member disk failure.
- Degraded: An array with a redundant RAID level with one or more member failures and can no longer sustain a subsequent drive failure (with the exception in PRL-11).
- Offline: An array with one or more member disk failures and data is no longer available

Viewing Array Properties

Select an array in the Controller Dashboard to view its properties.

Figure 31: Array Properties Window



If you have selected multiple volumes or multiple drives, click the (Expand button) to perform actions such as starting a Consistency Check operation and so on. This expansion is applicable for all the scenarios where you have selected multiple volumes or multiple drives and performing certain actions through the **Actions** dialog.

Table 8: Array Properties Description

Property	Description
Free Capacity	Indicates the free space available in the array.
Secured	Indicates whether the array is secured.
Free Capacity Count	The number of holes present on the array. Selecting the count lists the holes and the capacity of the array.

Adding a Volume to an Array

You can add volumes to an existing array if sufficient storage space is present in the existing volumes of the array.

Perform these steps to add a volume to an existing array:

1. Navigate to the Controller Dashboard and click an array name (for example, **Array_1**).
   In the right pane, under **Actions**, the **Add Volumes** option appears.
2. Click **Add Volumes**.
   The **Volumes Settings** window appears.
3. Specify the settings for the volumes you want to create.
   See Selecting Volume Settings for details on creating volumes.
4. Click **Volumes Settings**.
   The newly created volume gets added to the selected array.

RAID Level Transformation

RAID level transformation is the process of converting one RAID configuration to another. You can perform RAID level transformation at the array level. The table that follows describes the valid RAID level transformation matrix.

Table 9: Array – RAID Level Transformation Description

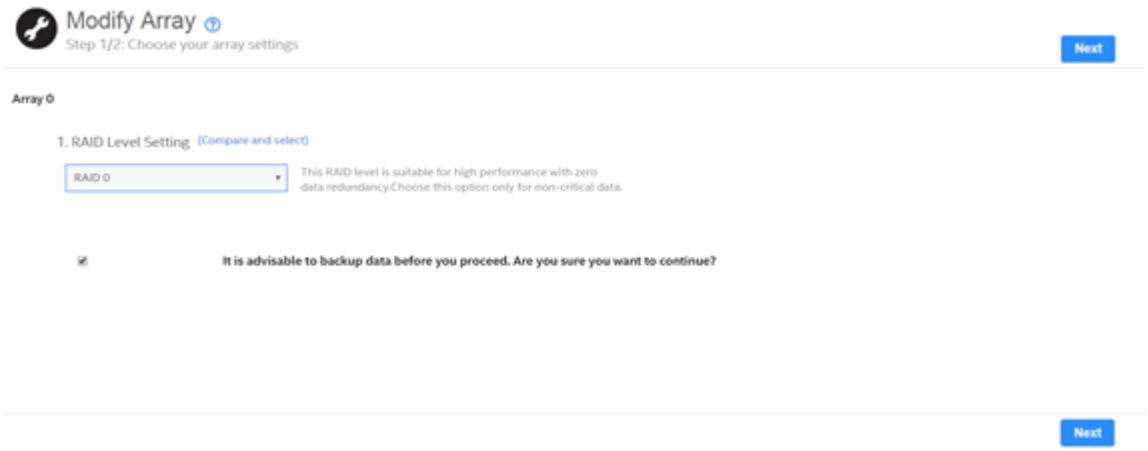
Initial RAID Level	Migrated RAID Level
RAID 0	RAID 1
RAID 0	RAID 5
RAID 0	RAID 6
RAID 1	RAID 0
RAID 1	RAID 5
RAID 1	RAID 6
RAID 5	RAID 0
RAID 5	RAID 6
RAID 6	RAID 0
RAID 6	RAID 5

Migrating the RAID Level of an Array

Perform these steps to migrate the RAID level of an array.

1. Navigate to the Controller Dashboard and click an array name (for example, **Array_1**).
   In the right pane, under **Actions**, the **Modify Array** option appears.
2. Click **Modify Array**.
   The **Modify Array** window appears.

Figure 32: Modify Array Window



3. Select the RAID level to which you want to migrate the array from the **RAID Level Setting** drop-down menu.

   It is recommended you back up the data *before* you change the RAID levels.

   > **ATTENTION**
   > Checking the **"It is advisable to back up data before you proceed. Are you sure you want to continue?"** checkbox does *NOT* launch a backup. You must follow the prescribed process to perform an array backup.

4. Click **Next**.

   The **Modify Array** dialog appears and provides you an option to add, remove, or directly change the RAID level. Depending on the source and the target RAID levels, you can also add drives directly without having to choose an option.

   Figure 33: Modify Array Settings Dialog

Adding Drives to a Configuration

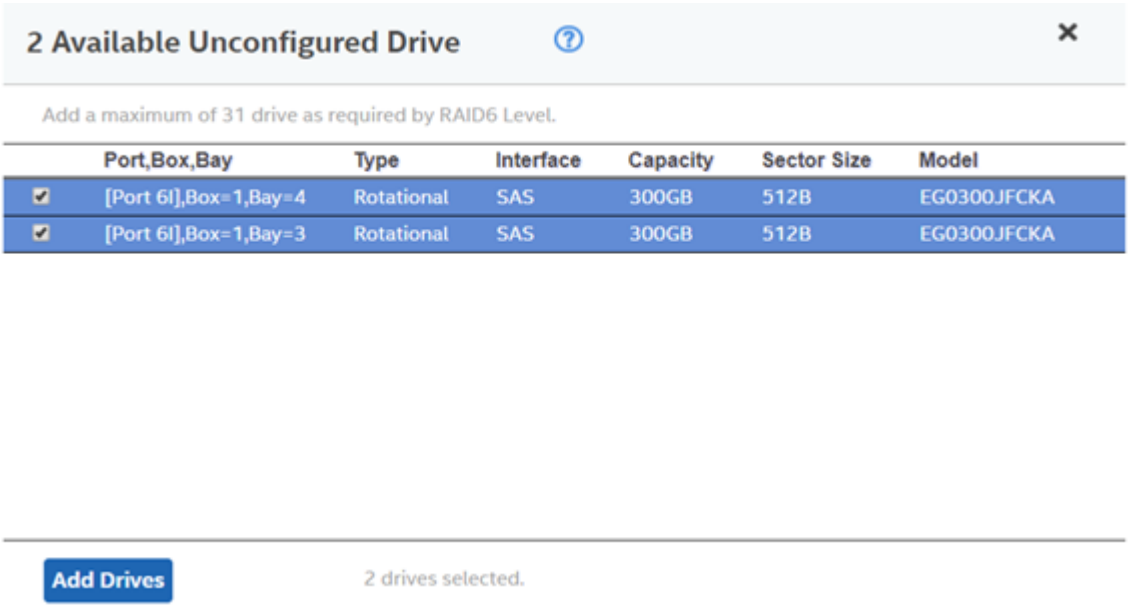
For example, if you migrate the RAID level of a array from RAID 0 to RAID 5, the **Modify Array** wizard lets you add unconfigured drives to the existing configuration to enable the RAID level transformation.

1. Click **Add Drives** in the **Modify Array** window.

   > **NOTE**
   > The drives you add must have the same capacity as or greater capacity than the drives already in the array, or you cannot change the RAID level.

   The **Available Unconfigured Drive** window appears. It lists the drives you can add, and it states whether you must add a minimum number of drives to change the RAID level from the current level to the new RAID level.

Figure 34: Available Unconfigured Drive Window



2. Select the available unconfigured drives and click **Add Drives**.
3. Click **Finish**.

   The RAID level is migrated. A confirmation message appears. You can monitor the progress of the transformation. See Background Operations Support.

Removing Drives from a Configuration

For example, if you migrate the RAID level of a array from RAID 5 to RAID 0, the **Modify Array** wizard lets you remove drives from the existing configuration to enable the RAID level transformation.

1. Select **Remove drives** in the **Modify Array** window, and click **Next**.

   The **Modify Array** window appears and it states the number of drives that you must remove to change the RAID level from the current level to a new RAID level and the maximum number of drives that can be removed.

2. Click the X icon to remove the drives.
3. Click **Finish**.

   The RAID Level is migrated. A confirmation message appears. You can monitor the progress of the transformation. See Background Operations Support.

Migrating the RAID Level Without Adding or Removing Drives

For example, if you migrate the RAID level of your array from RAID 5 to RAID 0, the **Modify Array** wizard lets you migrate the RAID level without adding or removing the drives.

Select **Migrate RAID level** in the **Modify Array**, and click **Next**.

The RAID level is migrated. A confirmation message appears. You can monitor the progress of the transformation. See Background Operations Support.

Managing Volumes

The HPE MR Storage Administrator application lets you perform various operations on the volumes.

The firmware supports the following volume states on the controller:

- **Optimal** – A volume whose members are all online.
- **Partially Degraded** – A volume with a redundant RAID level that can sustain one or more member disk failure. This state also applies to the volume's member drives. Currently, a RAID 6 or RAID 60 volume is the only volume that can be `Partially Degraded`.
- **Degraded** – A volume with a redundant RAID level with one or more member failures and can no longer sustain a subsequent drive failure (with exception in PRL-11).
- **Offline** – A volume with one or more member disk failures and data is no longer available (corresponds to DDF `Failed` state).

Viewing Volume Properties

Select a volume from an array in the Controller Dashboard to view its properties.

Figure 35: Volume Properties

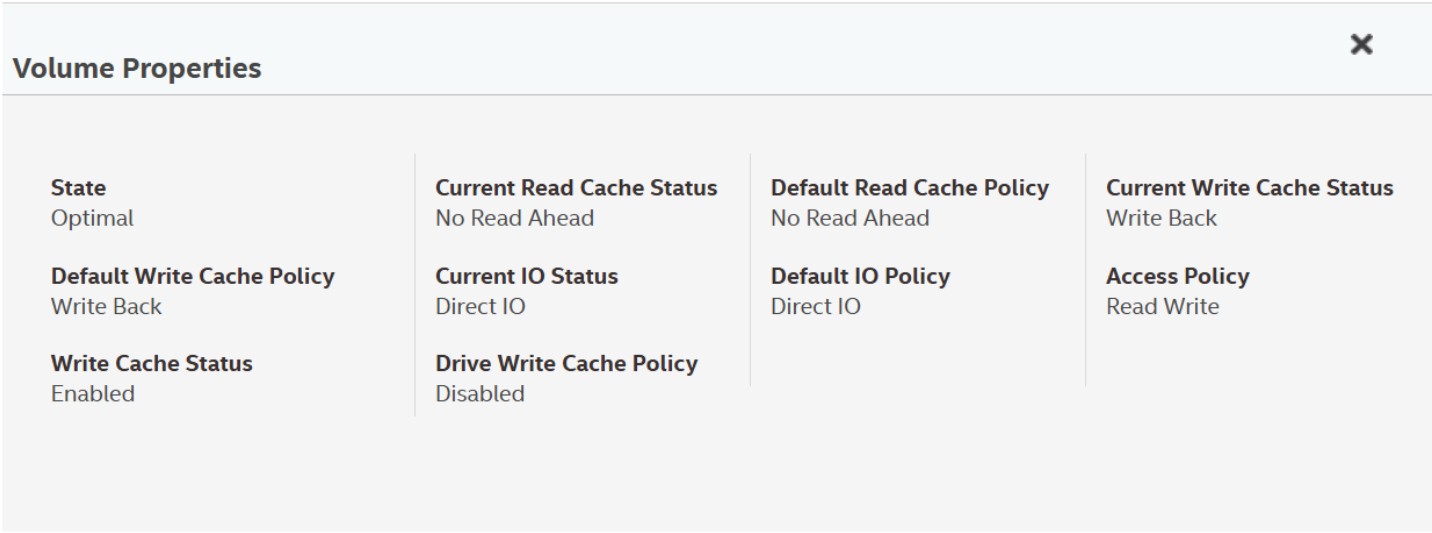


Table 10: Volume Properties

Property	Description
State	The current status of the volume. These options are available: • **Optimal** • **Partially Degraded** • **Degraded** • **Offline**
Current Read Cache Status	The current read cache status for the volume. These options are available: • **Read Ahead** • **No Read Ahead**

Property	Description
Default Read Cache Status	The default read cache status for the volume. These options are available: • **Read Ahead** • **No Read Ahead**
Current Write Cache Status	The current write cache status for the volume. These options are available: • **Write Through** • **Write Back** • **Always Write Back**
Default Write Cache Status	The default write cache status for the volume. These options are available: • **Write Through** • **Write Back** • **Always Write Back**
Default IO Policy	The input/output policy for the volume. These options are available: • **Direct IO** • **Cached IO**
Access Policy	The access policy for the volume. These options are available: • **Read Write** • **Read Only** • **Hidden** – The Hidden policy is applicable for only hidden volumes. No other access policies are applicable after you select Hidden as the access policy.
Write Cache Status	The current state of the write-back cache. The status depends on the battery status and the controller status for write-back operations. • **Enabled** – When the current cache policy is `Write Back`. • **Disabled** – The current cache policy is `Write Through`, `JBOD`, or `Always Write Back`. • **Temporarily Disabled** – The firmware is moving to `Write Back` or `Write Through`. For example, pinned cache, the firmware is downloading, or reconstruction and charging is occuring.
Drive Write Cache Policy	The volume cache setting. These options are available: • **Unchanged** • **Enable** • **Disable**

Modifying Volume Properties

You can change the read policy, write policy, and other volume properties at any time after a volume is created. Perform these steps to modify the volume settings.

1. Navigate to the Controller Dashboard, click an array name (for example, **Array_1**).

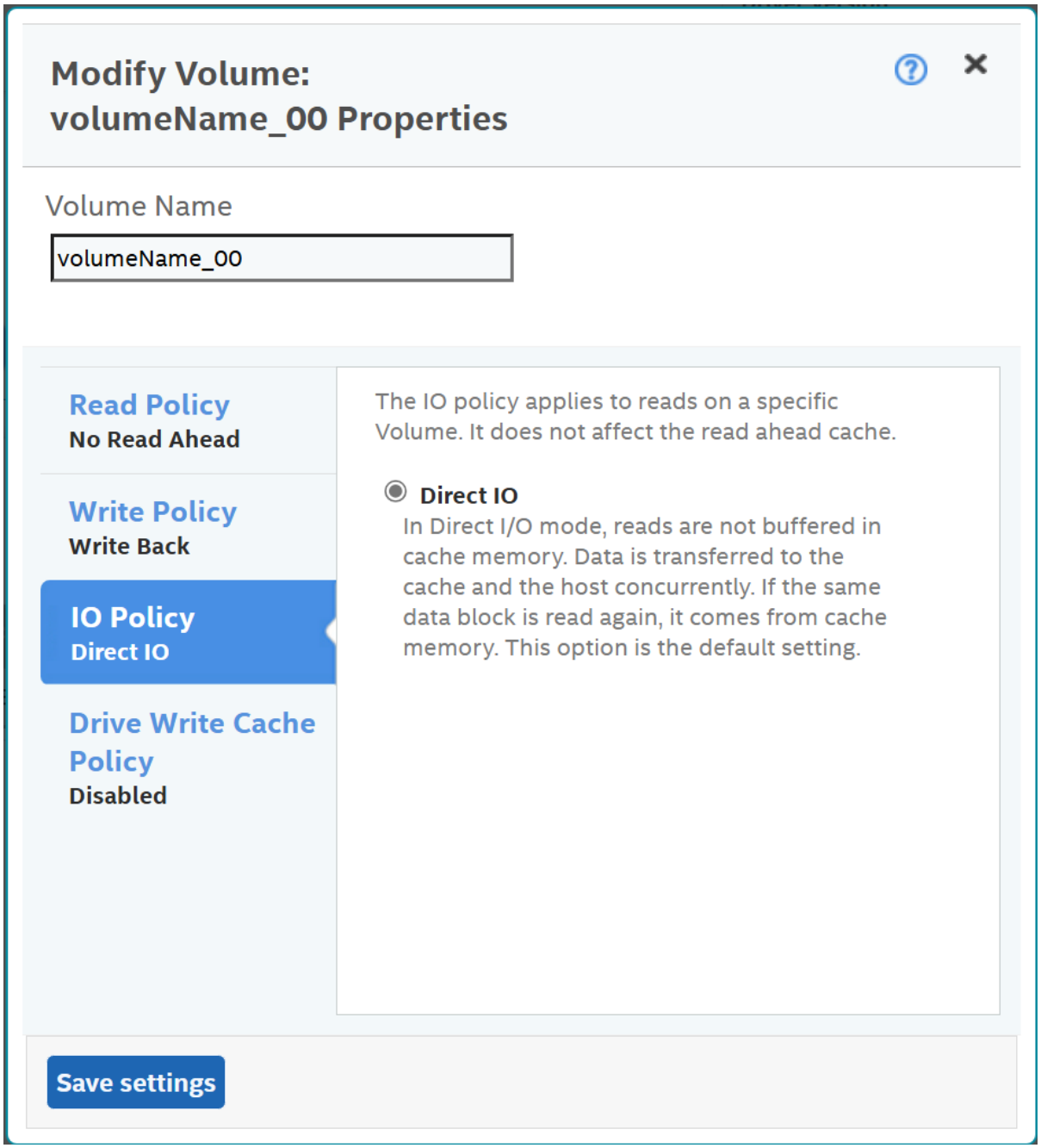
   Click the  icon that corresponds to the array to display its contents.

   The volumes and drives associated with the selected array appear.

2. Click the volume whose settings you want to change.
3. Select **More Actions** > **Modify Properties**.

   The **Modify <Volume Name>** dialog appears.

Figure 36: Modify Volume Dialog



4. Change the volume properties as needed.
   For information about these properties, see Selecting Volume Settings.

5. Click **save settings**.

Start and Stop Locating a Volume

If the drives that contain the volumes are located in a disk enclosure, you can identify them by making their LEDs blink. Perform these steps to identify the volumes:

1. Navigate to the Controller Dashboard, click an array name (for example, **Array_1**).

   Click the  icon that corresponds to the array to display its contents.

   The volumes and drives associated with the selected array appear.
2. Click the volume that you want to locate in the disk enclosure.
3. Select **Actions** > **Start Locate**.

   The LEDs on the drives in the volume start blinking.
4. To stop the LEDs from blinking, select **Actions** > **Stop Locate**.

Erasing a Volume

The volume erase function operates on a specified volume and overwrites all user-accessible locations. It supports nonzero patterns and multiple passes. The volume erase function optionally deletes the volume and erases the data within the volume's LBA range. The volume erase function is a background operation, and it posts events to notify users of their progress.

> **NOTE**
> Use disk management tools within the operating system to first unmount the volume before performing an erase.

Perform these steps to erase a volume.

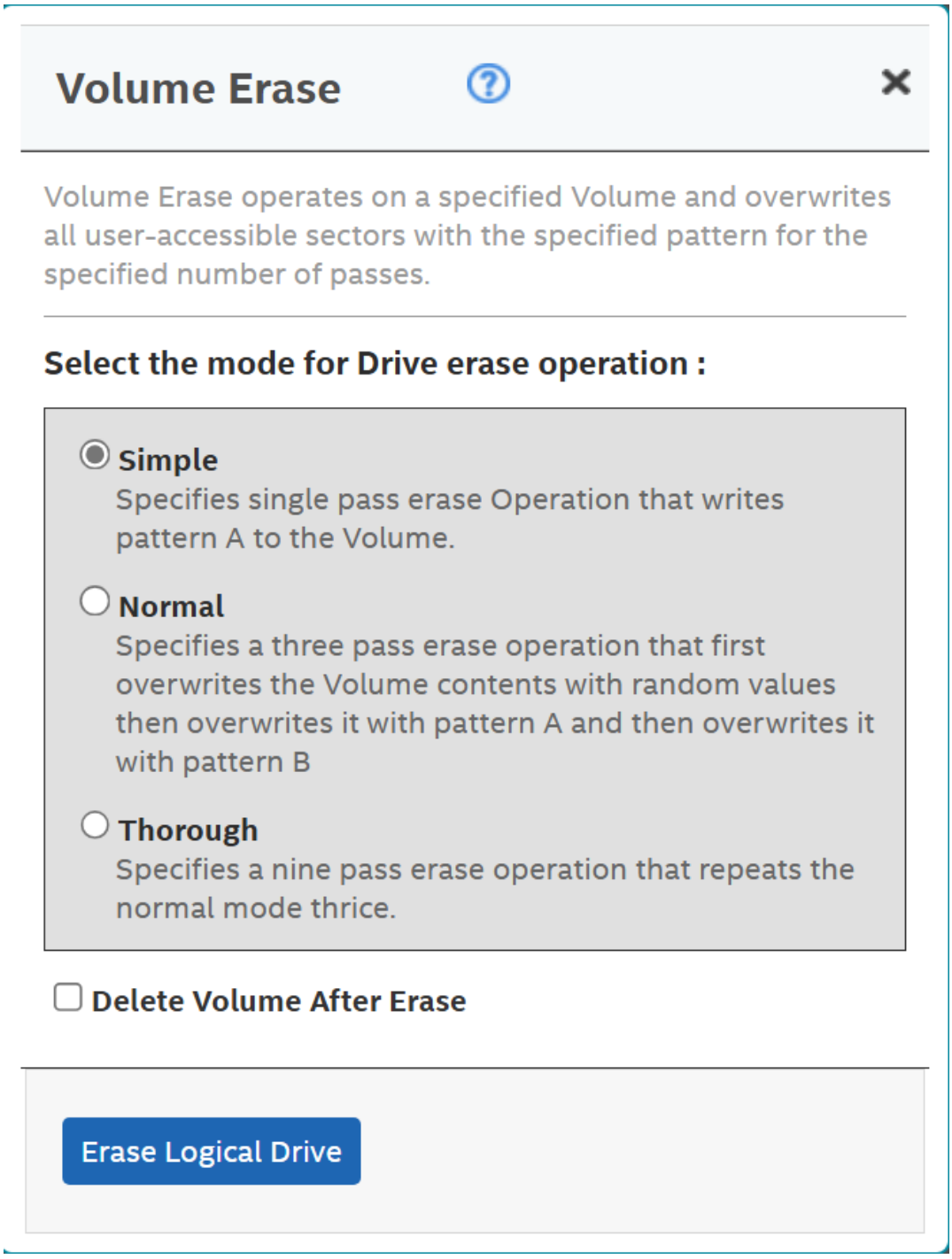
1. Navigate to the Controller Dashboard, click a array name (for example, **Array**).

   Click the  icon corresponding to a array to display its contents.

   The volumes and drives associated with the selected array appear.
2. Click the volume whose content you want to erase.
3. Select **Actions** > **Erase**.

   The **Volume Erase** dialog appears.

Figure 37: Volume Erase Dialog



The dialog shows these modes:

- **Simple**
- **Normal**
- **Thorough**

4. Select a mode and click **Erase Volume**.
   A warning message appears asking for your confirmation.
5. Click **Yes, Erase Drive**.
   After the volume erase operation has started, the **Stop Erase** option is enabled in the **Actions** menu. You can monitor the progress of the erase operation. See Background Operations Support.
6. Select the **Delete Volume After Erase** check box to delete the volume after the erase operation has completed.

Initializing a Volume

When you create a new volume with the **Advanced Configuration** wizard, you can select the **Fast Initialization** or **Full Initialization** option to initialize the drive immediately. However, you can select **No Initialization** if you want to initialize the volume later.

Perform these steps to initialize a volume after completing the configuration process.

1. Navigate to the Controller Dashboard, click an array name (for example, **Array_1**).
   Click the  icon that corresponds to the array to display its contents.
   The volumes and drives associated with the selected array appear.
2. Click the volume that you want to initialize.
3. Select **Actions** > **Start Initialize**.
   A warning message appears.

   ATTENTION
   Initialization erases all data on the volume. Make sure to back up any data you want to keep before you initialize a volume. Make sure the operating system is not installed on the volume you are initializing.
4. Select the **Fast Initialization** check box if you want to use this option.
   If you leave the check box unselected, the software runs a Full Initialization on the volume.
5. Click **Yes, Start Initialization** to begin the initialization.
   You can monitor the progress of the initialization. See Background Operations Support.

Starting Consistency Check on a Volume

Perform the following steps to start consistency check on a volume. For more information of consistency check, see Running Consistency Checks.

1. Navigate to the Controller Dashboard, click an array name (for example, **Array_1**).
   Click the  icon that corresponds to that array to display its contents.
   The volumes and drives associated with the selected array appear.
2. Click the volume on which you want to start consistency check.
3. Select **Actions** > **Start Consistency Check**.
   The consistency check operation starts. You can see the progress of this operation in the **Background Processes in Progress** section. After the consistency check operation has started, the **Stop Consistency Check** option is enabled in the **Actions** menu.

Expanding the Capacity of a Volume While Online

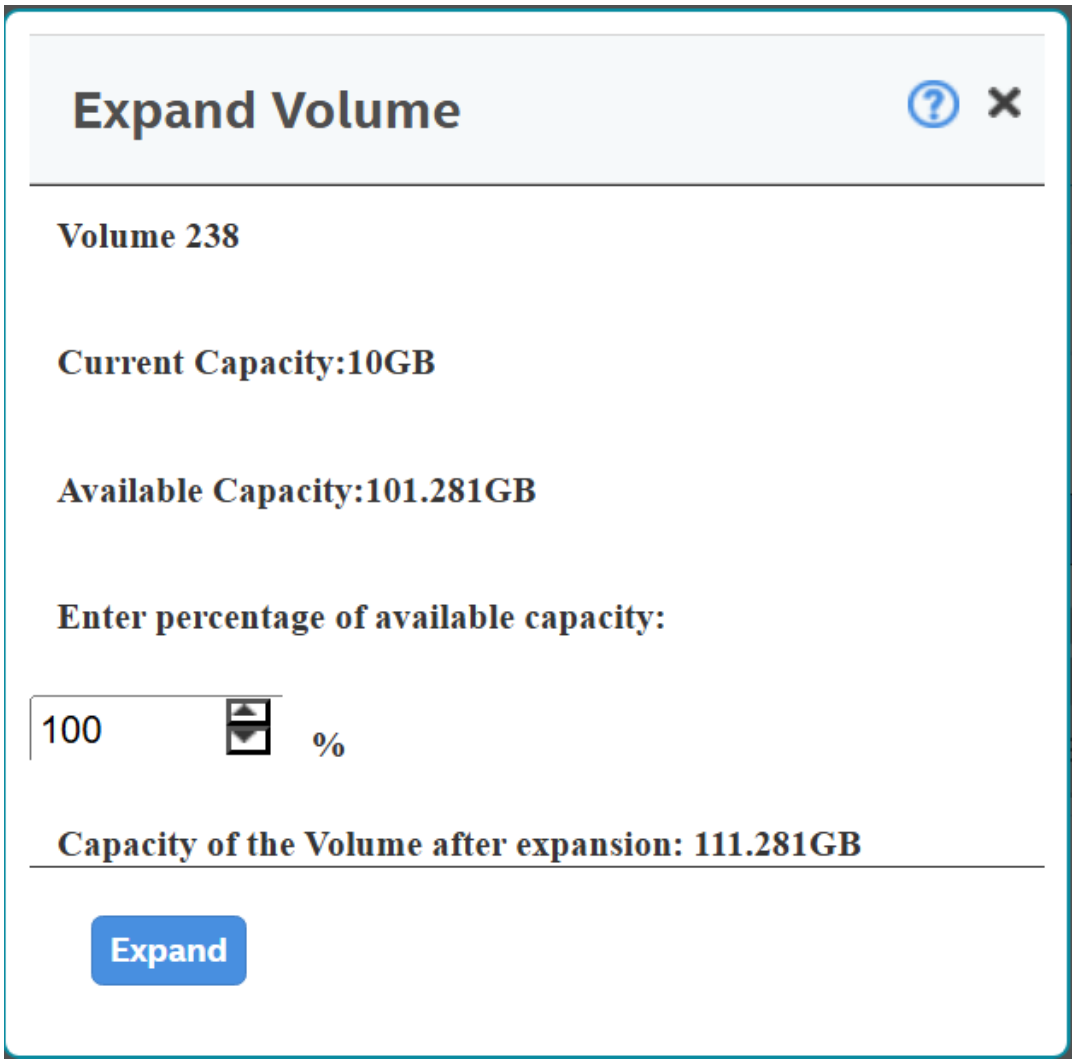
Transformation lets you expand the capacity of a volume by adding new drives or making use of unused space on existing disks, without requiring a reboot. Perform these steps to expand the capacity of a volume.

ATTENTION
Make sure to back up the data on the volume before you proceed with the transformation and expand the array before performing an transformation operation.

1. Navigate to the Controller Dashboard, click an array name (for example, **Array_1**).

   Click the + icon that corresponds to the array to display its contents.
   The volumes an drives associated with the selected array appear.
2. Click the volume whose capacity you want to expand.
3. Select **More Actions** > **Expand**.
   The **Expand Volume** dialog appears.

   Figure 38: Expand Volume Dialog



4. Select the percentage of the available capacity that you want the volume to use.
5. Click **Expand**.
   The volume expands by the selected percentage of the available capacity.

Deleting a Volume

You can delete volumes on a controller to reuse that space for new volumes.

CAUTION
All data on a volume is lost when you delete it. Make sure to back up the data before you delete a volume.

Perform the following steps to delete a volume.

1. Navigate to the Controller Dashboard, click an array name (for example, **Array_1**).

   Click the  icon that corresponds to the array to display its contents.
   The volumes an drives associated with the selected array appear.
2. Click the volume that you want to delete.
3. Select **Actions** > **Delete**.
   A confirmation dialog appears.
4. Select **Confirm** and click **Yes, Delete** to proceed with the delete operation.

   NOTE
   You can delete an operating system or file system volume. However, if you try to do so, the following message appears.

```
Selected Volume has an OS/FS, are you sure you want to delete it?
```

Managing Drives

The HPE MR Storage Administrator application lets you manage all the drives connected to the controller.

The firmware defines the following states for the physical disks connected to the controller:

- **Unconfigured Good** – A drive accessible to the RAID controller but not configured as a part of a virtual drive.
- **Online** – A disk accessible to the RAID controller and configured as part of a virtual drive.
- **Failed** – A disk drive that is part of a virtual drive, but has failed and is no longer usable.
- **Rebuild** – A disk drive to which data is being rebuilt to restore full redundancy to a virtual drive.
- **Unconfigured Bad** – A disk drive that is not a part of an array and is known to be bad. This state is typically assigned to a drive that has `Failed` , but is no longer part of a configured virtual drive, because it has been replaced by a spare drive.

  On hot-plug, or discovery during startup, if the firmware cannot communicate with a drive, or drive initialization fails, the drive is marked `Unconfigured Bad` . A hot-plugged drive might continue to be in the `Unconfigured Bad` state, if it had `Failed` previously. The firmware can be configured to remember the `Failed` drive information.
- **Shield state** – The shield state is an interim state of a physical drive for diagnostic operations. The results of the diagnostic tests determine if the physical drive is good or bad. If any of the diagnostic tests fail, the physical drive transitions to a bad state (FAILED or UNCONF BAD).
- **Foreign** – While importing disks from a different RAID controller (foreign metadata), the physical disk is marked as Foreign until the configuration on the disks is added to the existing configuration on the controller.

  Foreign is not actually a drive state, it indicates that a drive is derived from another configuration. The foreign drives typically remain in an Unconfigured Good state until they are imported into the current configuration. A Foreign drive is any disk that has a disk data format (DDF) configuration record and is not a part of the current set of configured disks. Even if the disk is removed from the current configuration, it is still considered Foreign until it is imported. A Foreign drive cannot be configured as a part of a virtual drive or a hot spare unless the Foreign configuration on the drive has been explicitly cleared by the user.

  Users migrating the volumes from an old controller to a new controller must ensure that all the controller settings and NVDATA settings that they had earlier on the old controller are present in the new controller because if incompatible settings are found, the foreign import of the drive might fail.
- **Spare** – A disk drive that is configured as a hot spare. If the spare is not activated, the status light emitting diode (LED) state corresponds to `Online` .
- **Copyback** – A disk drive serving as a Copyback destination drive. The drive’s state transitions to Online when the Copyback operation completes and the source drive transitions to an unconfigured good or bad drive.
- **Offline** – A disk drive that is still part of a configured volume, but is not active now. This state is used to represent a configured drive for which the data is not valid. This state can occur as a transition state, or because of any action performed by the user.
- **Just a Bunch of Disks (JBOD)** – Drives that are marked JBOD cannot be part of any configuration because they are stand-alone drives that are exposed to the operating system. Because the operating system and/or applications manage these drives through the controller, it is not appropriate for the firmware to perform RAID operations on JBOD drives. To include a JBOD drive in a RAID configuration, its state must be transitioned to Unconfigured Good. If users enable the JBOD support, the firmware marks new drives as JBOD unless the drive contains a valid DDF record.

Viewing Drive Properties

Select a drive from an array in the Controller dashboard to view its properties.

Figure 39: Drive Properties

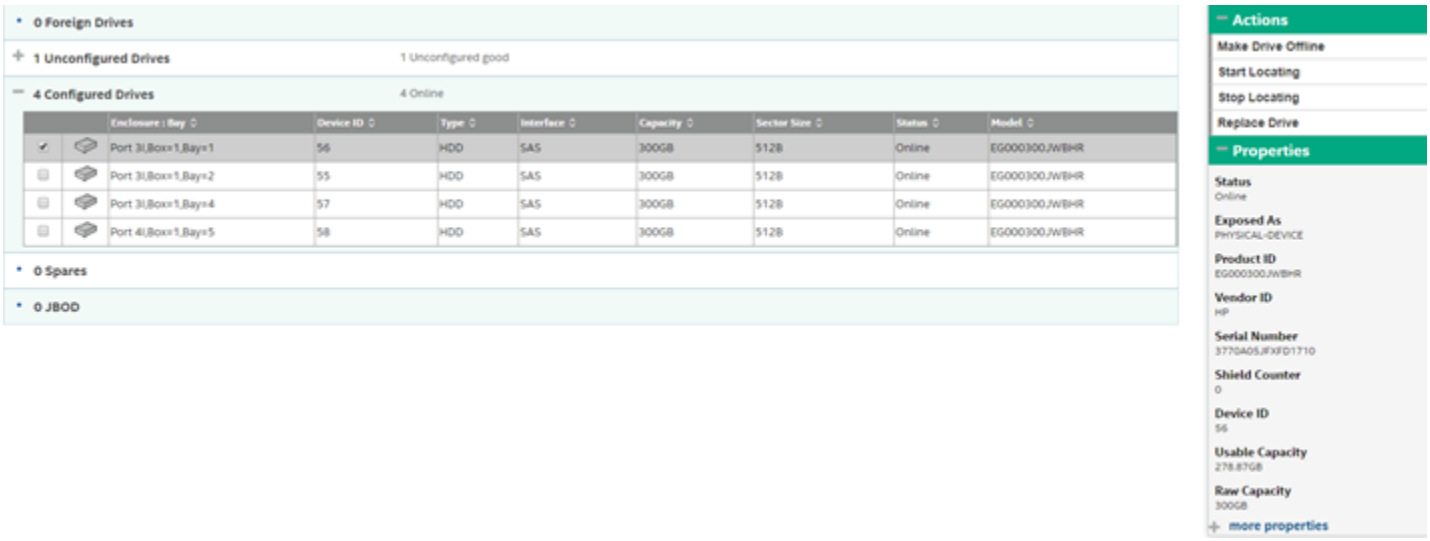


Table 11: Drive Properties

Property	Description
Status	The current status of the drive.
Exposed As	To differentiate the drives, the drives are exposed as one of the following: • JBOD • PHYSICAL-DEVICE
Product ID	The product ID of the drive.
Vendor ID	The ID assigned to the drive by the vendor.
Serial Number	The serial number of the drive.
Shield Counter	The shield counter value.
Device ID	The device ID of the drive that is assigned by the manufacturer.
Usable Capacity	The usable storage capacity, based on the RAID level used.
Raw Capacity	The actual full capacity of the drive before any coercion mode is applied to reduce the capacity.
General Properties	
SAS Address 0	The World Wide Name (WWN) for the drive.
SAS Address 1	The WWN for the drive.
Negotiated Link Speed	The negotiated link speed for data transfer to and from the drive.
Drive Speed	The speed of the drive.
Temperature	The temperature of the drive.
Revision Level	The revision level of the drive's firmware.
Power Status	The power status displays the following status: • **On** – when a drive is spun up.
Native Command Queueing	Indicates if the Native Command Queueing (NCQ) function is enabled. NCQ enables the drive to queue the I/O requests and reorder them for efficiency.
Sector Size	The size of the sector of the drive. The possible options are 4 KB or 512 KB.
Enclosure Properties	

Property	Description
Enclosure ID	The ID of the enclosure in which the drive is located.
Enclosure Location	The port number of the enclosure to which the drive is connected.

Start and Stop Locating a Drive

If the drives are in a disk enclosure, you can identify them by making their LEDs blink. Perform the following steps to identify the drives:

1. Navigate to the drive on the Controller dashboard, and select the drive you want to identify such as, Unconfigured Good drive, Online drive, Configured drive, and so on.
2. Select **Actions** > **Start Locating**.
   The corresponding LED on the drive starts blinking.
3. To stop the LED from blinking, select **Actions** > **Stop Locating**.

Making a Drive Offline

Perform the following steps to make a drive offline.

> **ATTENTION**
> After you perform this procedure, all of the data on the drive will be lost.

1. Navigate to the Controller Dashboard, click an array name (for example, **Array_1**).
   Click the  icon corresponding to an array to display its contents.
   The volumes and drives associated with the selected array appear.
2. Click the **Drive** tab, and select the drive that you want to make offline.
3. Select **Actions** > **Make Drive Offline**.
   A confirmation message appears.
4. Select **Confirm** and click **Yes, Make Drive Offline** to make the selected drive `Offline`.

Making a Drive Online

You can change the state of a drive to online. In an online state, the drive works normally and is a part of a configured volume.

> **ATTENTION**
> When transitioning a drive to an online state manually or forcefully, you lose data on the drive. When adding a drive to an existing volume or replacing a drive in an existing volume, you must manually start the rebuild process, if the rebuild does not automatically start. When the rebuild process is completed, the drive automatically transitions to an online state.

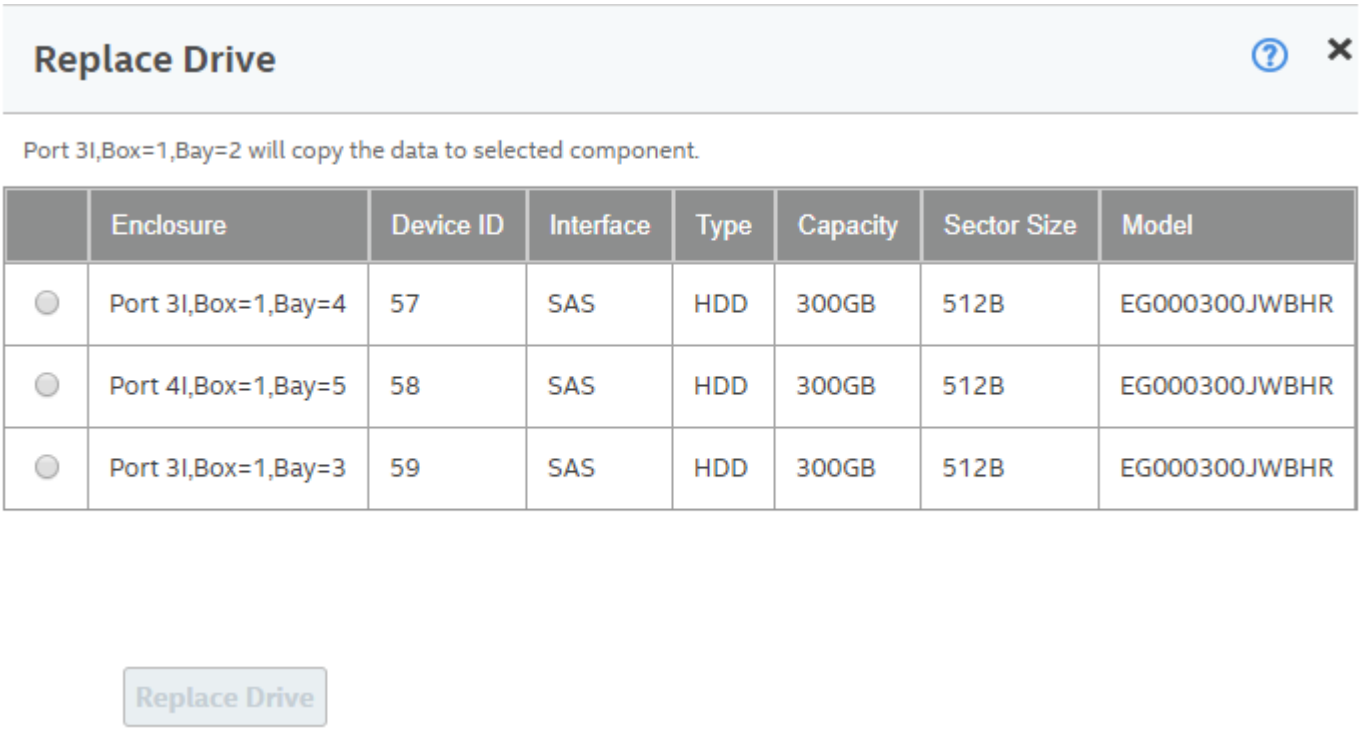
1. Navigate to the Controller Dashboard, click an array name (for example, **Array_1**).
   Click the  icon corresponding to an array to display its contents.
   The volumes and drives that are associated with the selected array appear.
2. Click the **Drive** tab, and select the offline drive that you want to make online.
3. Select **Actions** > **Make Drive Online**.
   The drive status changes to `Online`.

Replacing a Drive

You might want to replace a drive if the drive shows signs of failing. Before you start this operation, be sure that an available unconfigured good replacement drive is available. The replacement drive must have at least as much capacity as the drive you are replacing. Perform the following steps to replace a drive.

ATTENTION
Make sure to back up the data on the drive before you replace it.

1. Navigate to the Controller dashboard, click a array name (for example, **Array_1**). Click the icon corresponding to a array to display its contents.
   The volumes and drives associated with the selected array appear.
2. Click the **Drive** tab, and select a drive which you want to replace.
3. Select **Actions** > **Replace Drive**.
   The **Replace Drive** dialog appears.
   Figure 40: Replace Drive



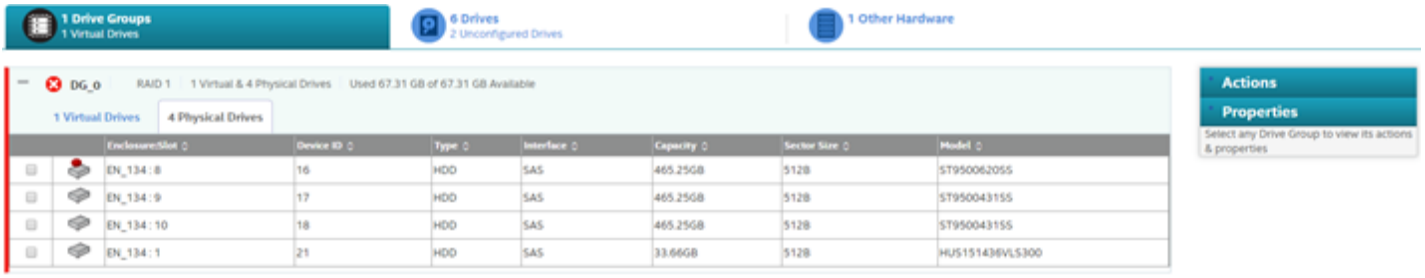
4. Select a replacement drive and click **Replace Drive**.
   A confirmation message appears.
5. Select **Confirm** and click **Yes, Replace Drive** to proceed with the replace operation.
   The drive is replaced and the data is copied to the selected component.

Marking a Drive as a Missing Drive

If a drive is currently part of a redundant configuration and if the drive is displaying signs of failure, you can mark the drive as missing and start rebuilding data on that drive.

1. Navigate to the Controller dashboard and select **Arrays**.
2. Click an array name (for example, **Array_1**).
3. Click the icon that corresponds to an array to display its contents.
   The volumes and physical drives associated with the selected array appear.
4. Click the **Physical Drive** tab, and select a drive which you want to mark as missing.
5. Select **Actions** > **Mark Drive Offline**.
   A confirmation dialog appears.
6. Select **Confirm** and click **Yes, Mark Drive Offline** to proceed towards marking the drive offline.
   The drive is marked as offline as shown in the following figure.

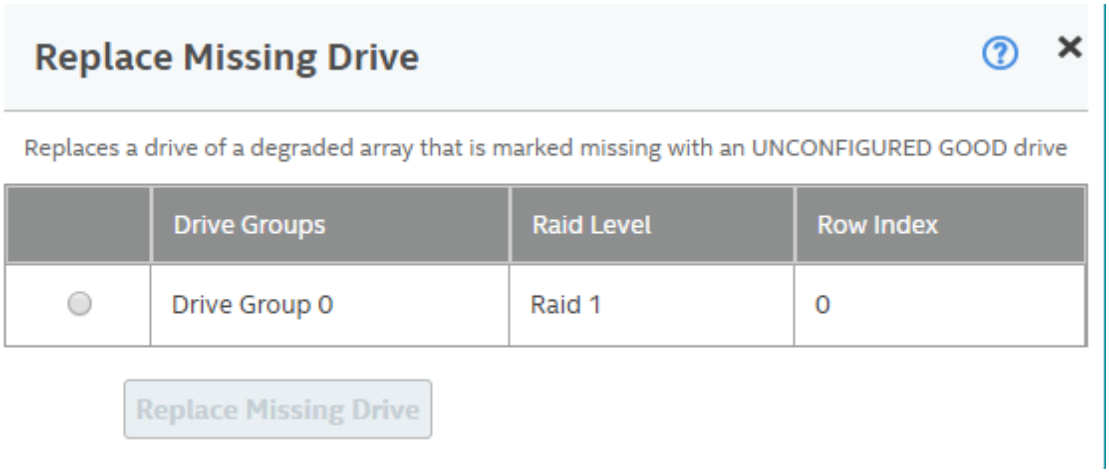
   Figure 41: Mark Drive Offline Dialog



7. Navigate to the **Drives** tab and expand the **Configured Drives** section to see the drives that are offline.
8. Select a drive whose status is offline and go to **Actions** > **Mark Drive as Missing**.
9. Navigate to the **Drives** tab.
10. Select an Unconfigured Good drive from the list of Unconfigured Good drives, and go to **Actions** > **More Actions** > **Replace Missing Drive**.

    The **Replace Missing Drive** dialog appears.

Figure 42: Replace Missing Drive Dialog



11. Select the drive and click **Replace Missing Drive**.
12. Navigate to the **Arrays** tab and select a new drive.
13. Click **Actions** > **More Actions** > **Start Rebuild**.

Replacing a Missing Drive

1. Navigate to the Controller dashboard and select **Drive Groups**.
2. Create a new drive group for any RAID level with two drives.
3. Navigate to the drive group, and mark one of the physical drives from disk group 0 as offline.
4. Select the physical drive that is marked as offline, and click **Mark the drive as missing**.
5. Select **Unconfigured drives**, then select the physical drive, and then **Replace Missing Drive**.
6. Select the drive group where you want to replace the missing physical drive.
7. Click **Ok**.

Assigning Global Spare Drives

A global spare drive replaces a failed drive in any redundant array, as long as the capacity of the global spare drive is equal to or greater than the coerced capacity of the failed drive. Perform the following steps to assign global spare drives.

1. Navigate to the Controller dashboard and click the **Drives** tab.
   All of the associated drives appear.
2. Expand **Unconfigured Drives** and select an unconfigured good drive.
3. Select **Actions** > **More Actions** > **Assign Global Spare Drive**.
   The unconfigured good drive is changed to a global spare drive. The status of the unconfigured good drive appears as a global spare drive in the **Spare Drives** section.

Removing a Global Spare Drive

Perform the following steps to remove a global spare drive.

1. Navigate to the Controller dashboard and click the **Drives** tab.
   All of the associated drives appear.
2. Expand **Spare Drives** and select a spare drive that you want to remove.
3. Select **Actions** > **More Actions** > **Remove Global Spare Drive**.
   The spare drive is removed and is listed in the **Unconfigured Drives** section as an unconfigured good drive.

Assigning Dedicated Spare Drives

Dedicated spare drives provide protection to one or more specified arrays on the controller. If you select an Unconfigured Good drive, you have the option of assigning it as a dedicated spare drive. Perform these steps to assign a dedicated spare drive.

1. Navigate to the Controller dashboard and click the **Drives** tab.
   All of the associated drives appear.
2. Expand **Unconfigured Drives** and select an unconfigured good drive.
3. Select **Actions** > **More Actions** > **Assign Dedicated Spare Drive**.
   The **Arrays** dialog appears.
4. Select an array and click **Add Dedicated Spare Drive**.
   A confirmation message appears.
5. Click **Done**.
   The unconfigured good drive is changed to a dedicated spare drive. The status of the unconfigured good drive appears as a dedicated spare drive in the **Spare Drives** section.

Rebuilding a Drive

If a drive configured as RAID 1, 5, 6, 10, 50, or 60 fails, the firmware automatically rebuilds the data on a spare drive to prevent data loss. The rebuild operation is a fully automatic process. You can monitor the progress of drive rebuilds in the **Background Processes in Progress** window. See Background Operations Support.

Converting an Unconfigured Bad Drive to an Unconfigured Good Drive

Perform the following steps to convert an unconfigured bad drive to an unconfigured good drive.

1. Navigate to the Controller dashboard and click the **Drives** tab.
   All of the associated drives appear.
2. Expand **Unconfigured Drives** and select an unconfigured bad drive.
3. Select **Actions** > **Make Unconfigured Good**.
   A confirmation message appears.
4. Select **Confirm** and click **Yes, Make Unconfigured Good** to proceed with the operation.
   The unconfigured bad drive is changed to an unconfigured good drive. The status of the unconfigured bad drive appears as unconfigured good in the **Unconfigured Drives** section.

Removing a Drive

You might need to remove a non-failed drive that is connected to the controller. Preparing a physical drive for removal spins the drive into a power save mode.

1. Navigate to the Controller dashboard, and click the **Drives** tab.
   All of the associated drives appear.
2. Expand **Unconfigured Drives**, and select a drive that you want to remove.
3. Select **Actions** > **Prepare for Removal**.
   The drive is in the power save mode and is ready for removal.
4. Wait until the drive spins down and then remove it.

   If you do not want to remove the drive, select **Actions** > **Undo Prepare for Removal**.

Make Unconfigured Good Drives and Make JBOD Drives

Unconfigured Good: The drive is unconfigured and hidden from the OS.

JBOD: The drive is exposed to the host OS as a physical drive. The user cannot use a JBOD drive to create a RAID configuration, because it is exposed to the host OS. A JBOD drive has to be converted to Unconfigured Good before creating a RAID configuration on the drive.

> **NOTE**
> The default JBOD behavior for the MR400 controller was changed in firmware 52.26.3-5250 and later versions. See Changing Behavior Modes for details.

Making Unconfigured Good Drives

Perform the following steps to change the status of JBOD drives to Unconfigured Good drives.

1. Navigate to the Controller dashboard and click the **Drives** tab.
   All of the associated drives appear.
2. Expand **JBOD** and select a JBOD drive.
3. Select **Actions** > **Make Unconfigured Good**.
   A confirmation message appears.
4. Select **Confirm** and click **Yes, Make Unconfigured Good** to proceed with the operation.
   The JBOD drive is changed to an unconfigured good drive.

Making a JBOD Drive

Perform these steps to change the status of unconfigured good drives to JBOD drives.

1. Navigate to the Controller dashboard and click the **Drives** tab.
   All of the associated drives appear.
2. Expand **Unconfigured Drives** and select an unconfigured good drive.
3. Select **Actions** > **Make JBOD**.
   The unconfigured good drive is changed to a JBOD drive.

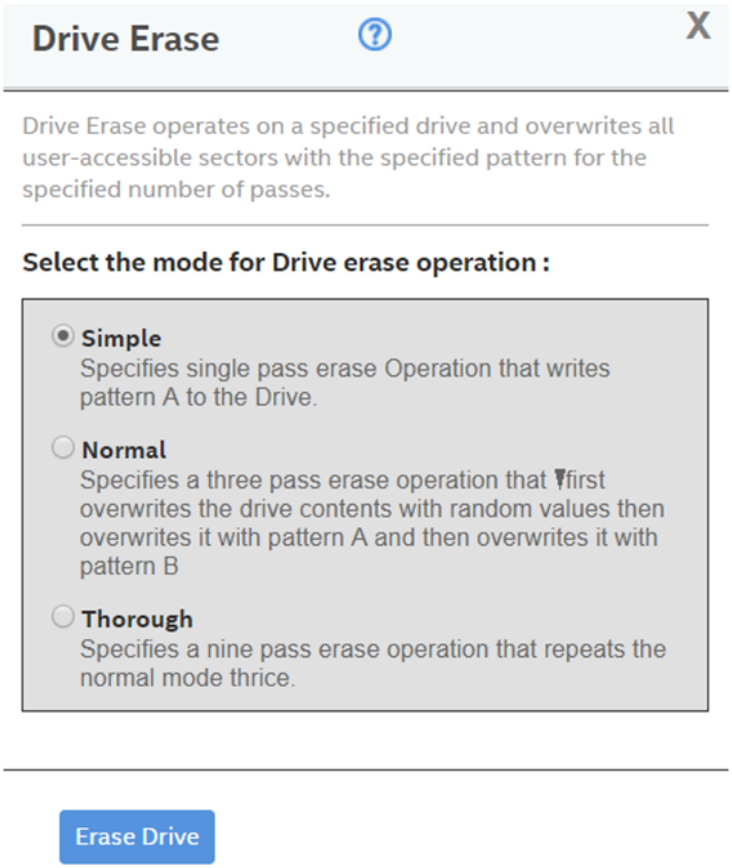
Erasing a Drive

You can erase data on Non SEDs (normal HDDs) by using the **Drive Erase** option. For Non–SEDs, the erase operation consists of a series of write operations to a drive that overwrites every user-accessible sector of the drive with specified

patterns. It can be repeated in multiple passes using different data patterns for enhanced security. The erase operation is performed as a background task. Perform the following steps to erase a drive.

1. Navigate to the Controller dashboard and click the **Drives** tab.
   All of the associated drives appear.
2. Expand **Unconfigured Drives** and select an unconfigured good drive.
3. Select **Actions** > **More Actions** > **Drive Erase**.
   The **Drive Erase** dialog appears.

   Figure 43: Drive Erase Dialog



   The dialog shows the following modes:

   - **Simple**
   - **Normal**
   - **Thorough**

4. Select a mode and click **Erase Drive**.
   A warning message appears asking for your confirmation.
5. Click **Yes, Erase Drive**.
   After the drive erase operation has started, the **Stop Erase** option is enabled in the **Actions** menu. You can monitor the progress of the erase operation. See Background Operations Support.

Erasing a Drive Securely

ATTENTION
The following procedure is applicable only to MR416i-p, MR416i-o, MR416i-a, MR216i-p, MR216i-o, MR216i-a, and MR4048i-o.

The Instant Secure Erase feature erases data from encrypted drives.

ATTENTION
All data on the drive is lost when you erase it. Before starting this operation, back up any data that you want to keep.

1. Navigate to the Controller dashboard, and click the **Drives** tab.
   All of the associated drives appear.
2. Expand **Unconfigured Drives**, and select an unconfigured good drive.
3. Select **Actions** > **Instant Secure Erase**.
   A confirmation message appears.
4. Select **Confirm** and click **Yes, Securely Erase Drive** to proceed with the operation.
   After the secure erase operation has started, the **Stop Erase** option is enabled in the **Actions** menu. You can monitor the progress of the erase operation. See Background Operations Support.

Sanitizing a Drive

You can erase the data residing on a drive using the **Sanitize** feature. The **Sanitize** option is similar to the *Drive Erase* feature that is already supported by your controller, except that the **Sanitize** option is performed by the drive firmware, whereas the *Drive Erase* feature is performed by the controller firmware.

The Sanitize option is an industry standard SCSI feature. It uses industry standard Sanitize SCSI Block command. The Sanitize operation is constantly monitored the by controller firmware and the drive sanitization progress events are notified to you through Background Operations Support.

ATTENTION
The following procedure is applicable only to P824i-p and newer controllers.

To Sanitize a drive, you must make sure that:

- The selected drive is in an Unconfigured Good state.
- The selected drive is not a JBOD drive.
- The selected drive is not part of any array, dedicated spare drive, or global spare drive.

Sanitize operation is enabled only when no other operation is in progress on the selected drive.

When the Sanitize operation is in progress, you cannot perform any other operation on the drive that is being sanitized.

Perform the following steps to sanitize a drive:

1. Navigate to the Controller dashboard and click the **Drives** tab.
   All of the associated drives appear.
2. Expand **Unconfigured Drives** and choose an unconfigured good drive.
   - You can run drive sanitization on multiple Unconfigured Good drives at the same time.

     However, the Sanitize option is only enabled when the same type of sanitize operation is supported on all the selected drives. For example, on solid state drives (SSDs), **Block Erase** is allowed, and on hard disk drives (HDDs), **Overwrite** is allowed.
   - You cannot run the Sanitize operation on mixed drive types.

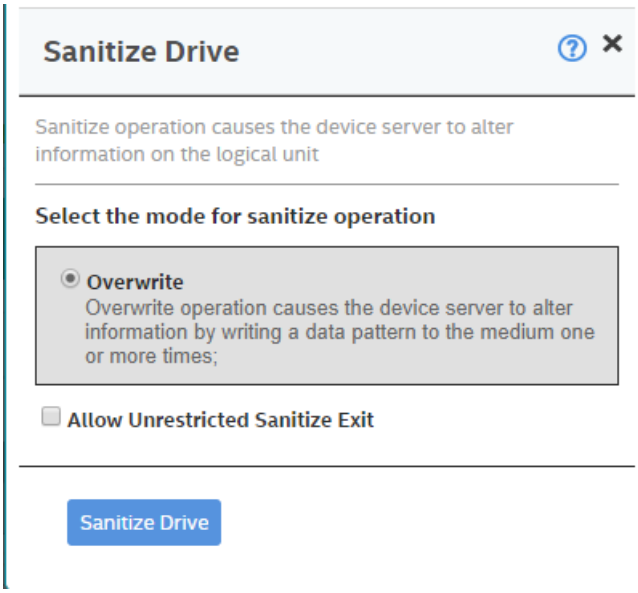
For example, you have selected two drives to run the Sanitize operation; one of them is an SSD and the other one is an HDD. In this scenario, you will not be able to run the Sanitize operation because they are not the same drive type, nor are they of the same sanitize operation type.

3. Select **Actions** > **More Actions** > **Start Sanitize**.

   The **Sanitize Drive** dialog appears.

   NOTE
   After you start the drive sanitize operation, you cannot stop or pause the operation until it is complete.

   Figure 44: Sanitize Dialog



   Depending on the drives you have selected for sanitization (SSDs or HDDs), the following options are available:

   - **Overwrite** – If you have selected HDD, you can sanitize the physical using the Overwrite option.

     This option writes a particular data pattern on the drive one or more times.
   - **Block Erase** – If you have selected SSDs, you can sanitize the drives using the Block Erase option.

     This option sets the physical blocks on the drive to a vendor-specific value.
   - **Allow Unrestricted Sanitize Exit** – If, for some reason, the Sanitize operation fails, the system tries to bring the drive out of the failure mode irrespective of whether you select this check box not.

     However, if this check box is selected, and if the system succeeds in bringing the drive out of the failure mode, the drive is then returned as an Unconfigured Good drive. If you do not select this check box, and if the Sanitize operation fails, the system places the drive in an Unconfigured Bad state.

4. Click **Sanitize Drive**.

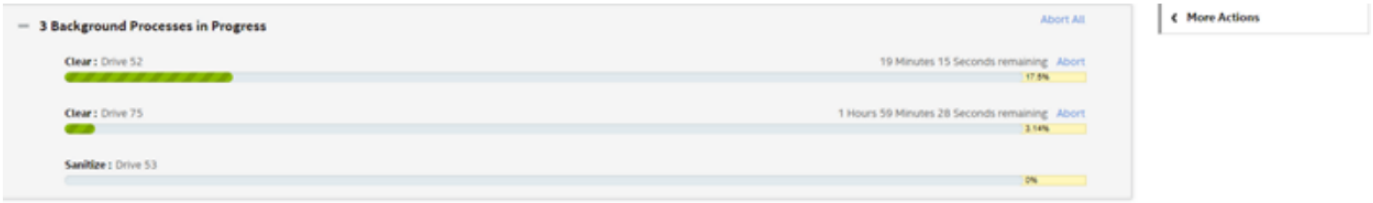
   A confirmation message appears.

5. Click **Yes, Sanitize Drive(s)** to start sanitizing the selected drives.

   You can monitor the progress of the Sanitize operation in the Background Operations section. The status of the drive is also displayed as **Sanitize** until the sanitization operation completes.

   The following figure displays the Background Operations section where the sanitize operation is in progress. The figure also displays the status of the drive that is being sanitized.

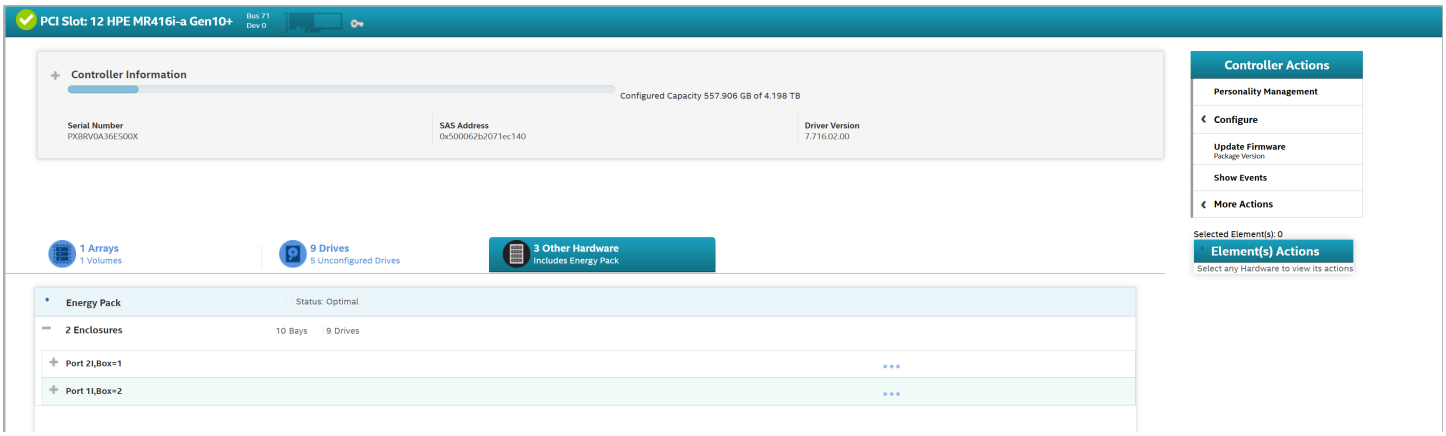
Figure 45: Background Operations and Drive Sanitize Dialog



Managing Hardware Components

When you select the **Other Hardware** tab from the Controller dashboard, the hardware components window appears.

Figure 46: Other Hardware Window



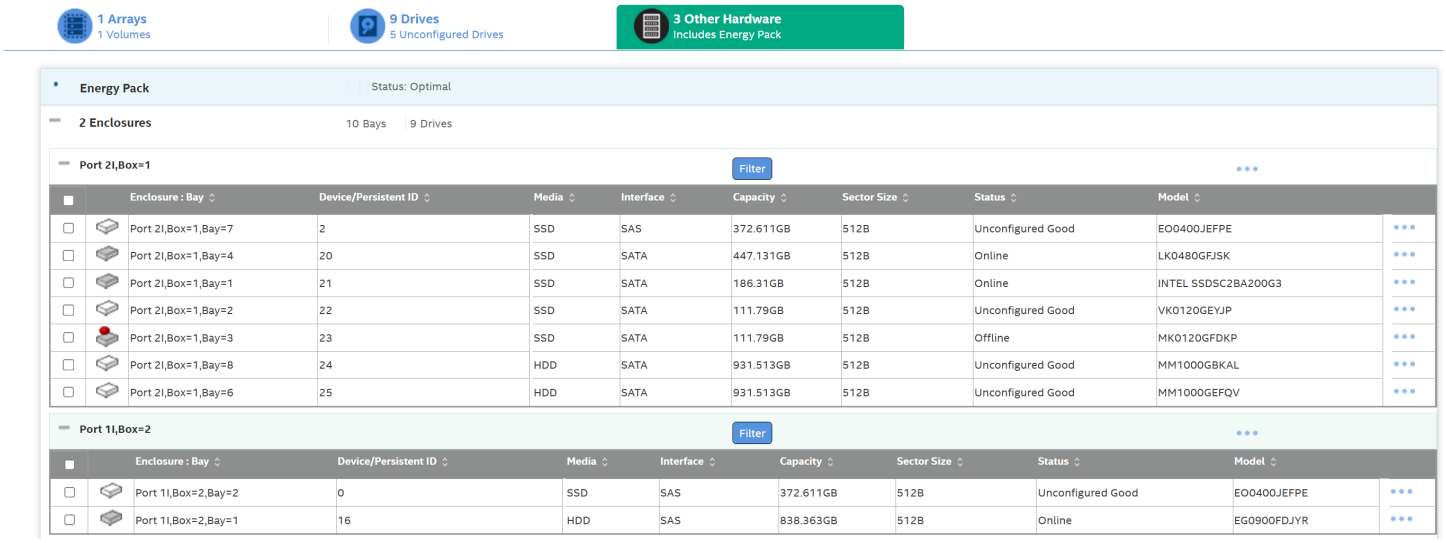
Monitoring the HPE Smart Storage Energy Pack

When the application is running, you can monitor the status of the HPE Smart Storage Energy Pack.

Also, if the HPE Smart Storage Energy Pack is in an Optimal state, **WriteCache Policy** is enabled. If the HPE Smart Storage Energy Pack is in not in an optimal state, **WriteCache Policy** is disabled.

To view the **WriteCache Policy** status, go to the **Array** tab, select an **Array**, then select a **Volume**. The **WriteCache Policy** status is displayed under the **Properties** section, as shown in the following figure.

Figure 47: WriteCache Policy Window



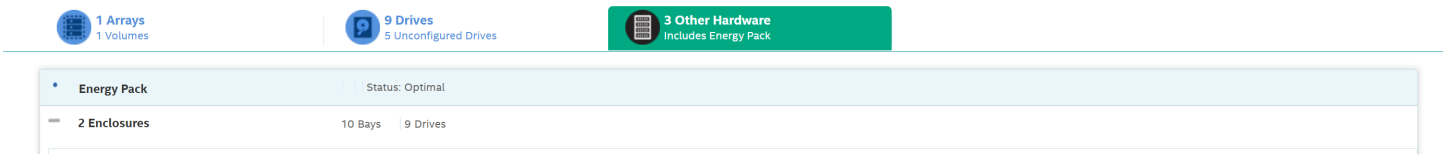
Monitoring Enclosures

When the HPE MR Storage Administrator application is running, you can monitor the status of all of the enclosures connected to the controllers in the server.

Viewing Enclosure Properties

From the **Other Hardware** tab, under **Enclosures**, select **Box** to view its properties.

Figure 48: Enclosure Properties Window



If you have selected multiple volumes or multiple drives, click the icon (Expand button) to perform actions such as starting a consistency check and so on. This action is applicable for all the scenarios where you have selected multiple volumes or multiple drives and are performing certain actions through the **Actions** dialog.

Table 12: Enclosure Properties

Property	Description
Name	Indicates the name of the enclosure.
Bay count	Indicates the number of bays.
Location	Indicates the location of the enclosure.

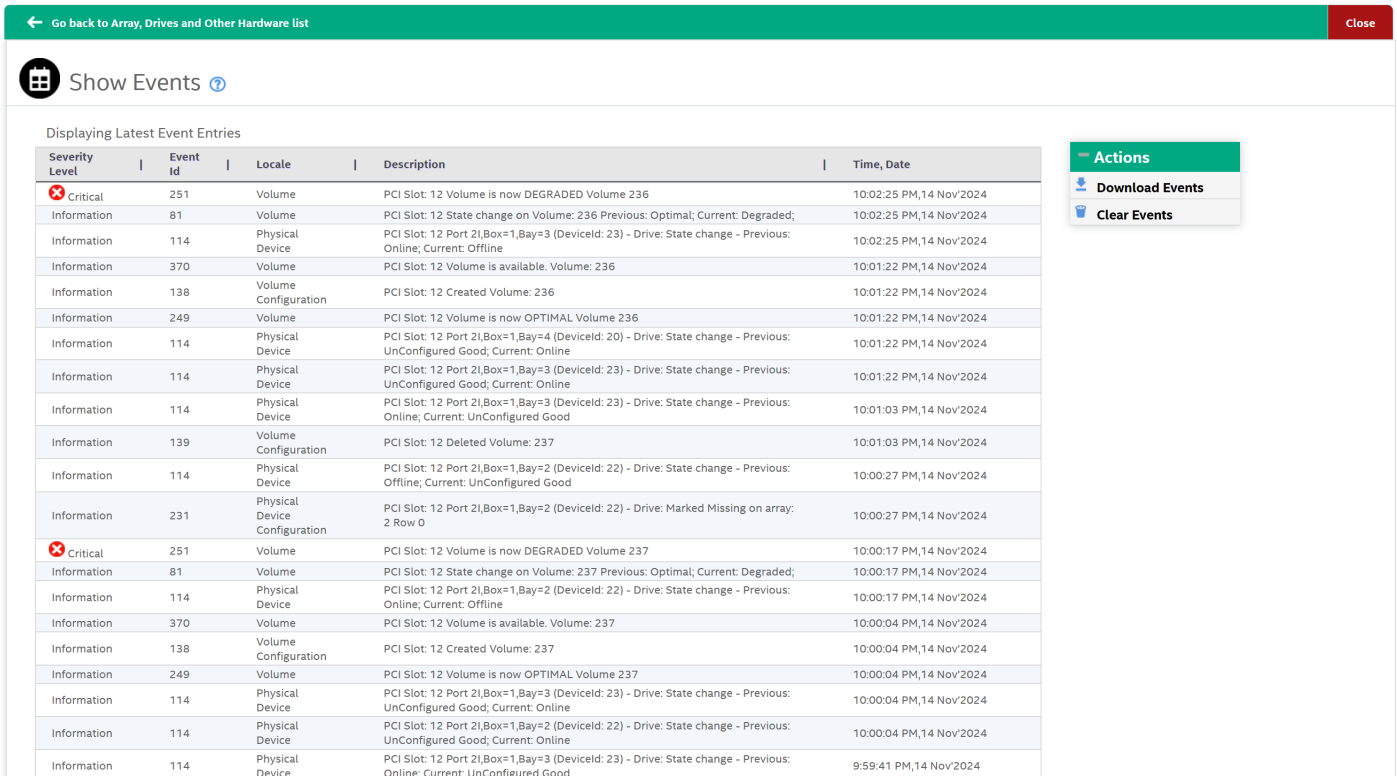
Viewing Event Logs

The application monitors the activity and performance of the server and all the controllers cards attached to it. Perform the following steps to view the event logs.

1. Select **More Actions** > **View Event Log** on the Server or Controller dashboard.

   The **View Event Log** window appears that displays a list of events. Each entry has an event ID, a severity level that indicates the severity of the event, a date and time entry, and a brief description of the event. The event logs are sorted by date and time in the chronological order.

   Figure 49: View Event Log Window



Severity Level	Event Id	Locale	Description	Time, Date
Critical	251	Volume	PCI Slot: 12 Volume is now DEGRADED Volume 236	10:02:25 PM,14 Nov'2024
Information	81	Volume	PCI Slot: 12 State change on Volume: 236 Previous: Optimal; Current: Degraded;	10:02:25 PM,14 Nov'2024
Information	114	Physical Device	PCI Slot: 12 Port 2I,Box=1,Bay=3 (DeviceId: 23) - Drive: State change - Previous: Online; Current: Offline	10:02:25 PM,14 Nov'2024
Information	370	Volume	PCI Slot: 12 Volume is available. Volume: 236	10:01:22 PM,14 Nov'2024
Information	138	Volume Configuration	PCI Slot: 12 Created Volume: 236	10:01:22 PM,14 Nov'2024
Information	249	Volume	PCI Slot: 12 Volume is now OPTIMAL Volume 236	10:01:22 PM,14 Nov'2024
Information	114	Physical Device	PCI Slot: 12 Port 2I,Box=1,Bay=4 (DeviceId: 20) - Drive: State change - Previous: UnConfigured Good; Current: Online	10:01:22 PM,14 Nov'2024
Information	114	Physical Device	PCI Slot: 12 Port 2I,Box=1,Bay=3 (DeviceId: 23) - Drive: State change - Previous: UnConfigured Good; Current: Online	10:01:22 PM,14 Nov'2024
Information	114	Physical Device	PCI Slot: 12 Port 2I,Box=1,Bay=3 (DeviceId: 23) - Drive: State change - Previous: Online; Current: UnConfigured Good	10:01:03 PM,14 Nov'2024
Information	139	Volume Configuration	PCI Slot: 12 Deleted Volume: 237	10:01:03 PM,14 Nov'2024
Information	114	Physical Device	PCI Slot: 12 Port 2I,Box=1,Bay=2 (DeviceId: 22) - Drive: State change - Previous: Offline; Current: UnConfigured Good	10:00:27 PM,14 Nov'2024
Information	231	Physical Device Configuration	PCI Slot: 12 Port 2I,Box=1,Bay=2 (DeviceId: 22) - Drive: Marked Missing on array: 2 Row 0	10:00:27 PM,14 Nov'2024
Critical	251	Volume	PCI Slot: 12 Volume is now DEGRADED Volume 237	10:00:17 PM,14 Nov'2024
Information	81	Volume	PCI Slot: 12 State change on Volume: 237 Previous: Optimal; Current: Degraded;	10:00:17 PM,14 Nov'2024
Information	114	Physical Device	PCI Slot: 12 Port 2I,Box=1,Bay=2 (DeviceId: 22) - Drive: State change - Previous: Online; Current: Offline	10:00:17 PM,14 Nov'2024
Information	370	Volume	PCI Slot: 12 Volume is available. Volume: 237	10:00:04 PM,14 Nov'2024
Information	138	Volume Configuration	PCI Slot: 12 Created Volume: 237	10:00:04 PM,14 Nov'2024
Information	249	Volume	PCI Slot: 12 Volume is now OPTIMAL Volume 237	10:00:04 PM,14 Nov'2024
Information	114	Physical Device	PCI Slot: 12 Port 2I,Box=1,Bay=3 (DeviceId: 23) - Drive: State change - Previous: UnConfigured Good; Current: Online	10:00:04 PM,14 Nov'2024
Information	114	Physical Device	PCI Slot: 12 Port 2I,Box=1,Bay=2 (DeviceId: 22) - Drive: State change - Previous: UnConfigured Good; Current: Online	10:00:04 PM,14 Nov'2024
Information	114	Physical Device	PCI Slot: 12 Port 2I,Box=1,Bay=3 (DeviceId: 23) - Drive: State change - Previous: Online; Current: UnConfigured Good	9:59:41 PM,14 Nov'2024

2. (Optional) – Click **Load More** to view more events in the same page.

Downloading Logs

To download the event logs, navigate to the **View Event Log** window, then click **Download Log** to download the event log file.

Clearing the Event Logs

Perform the following steps to clear the event logs.

1. Click **Clear Log** in the **View Event Log** window.

   A confirmation dialog appears.

2. Select **Confirm**, and click **Yes, Clear Log**.
   The event logs are cleared.

Known Issues and Workarounds

The following is a list of known issues and workarounds.

- **Issue**: The desktop shortcut is linked with a batch file. If the Windows User Account Control (UAC) is enabled, the privilege escalation prompt is not presented for users who have administrative privileges, but not administrator resulting in access denied message.
  Workaround: Enter the LSA URL, `localhost:port` directly into the browser
- **Issue**: The event API length for the serial number field is 10 characters. Only 10 characters are displayed in the event data for the PD serial number.
  Workaround: None.
- **Issue**: When heavy I/Os are active, MRSA may be slow and the user may see stale data.
  Workaround: Refresh the browser or restart the MRSA service to retrieve the updated data.
- **Issue**: When the user enables or disables a controller, the controller is not loaded or unloaded in MRSA by default.
  Workaround: Restart the MRSA service to retrieve the updated controller list.
- **Issue**: A repurposed event occurs.
  Workaround: Restart the MRSA service.
- **Issue**: Only the GUI is branded per HPE terminologies. Downloaded files are not branded.
  Workaround: None.
- **Issue**: Light Weight Agent only allows two Snapdump files to be downloaded at a time.
  Workaround: None.
- **Issue**: An IR/IT firmware downgrade is not supported from one phase to another phase due to limitations in underlying layers.
  Workaround: None.
- **Issue**: MRSA does not detect all the controllers in a HyperV Environment when the controller passthrough is enabled or disabled.
  Workaround: Restart the MRSA service to reload and update the library.
- **Issue**: MRSA may be inaccessible after a successful firmware update while I/O's are occurring.
  Workaround: Restart the MRSA services.
- **Issue**: MRSA may hang when downloading support logs on multiple clients.
  Workaround: Restart the MRSA services. Collect logs from one client at a time during non-heavy IO or drive/ blackplane operations.

  NOTE
  Downloading the support log is available only for admin users.
- **Issue**: Allows the *Guest* user to log in when the *Guest* user is disabled through the **User Accounts**.
  Workaround:

  1. Open the Command Prompt.
  2. Enter `lusrmgr.msc`.
  3. Select **Users**, then **Guest**.
  4. Right-click on the **Guest User**, and select the Properties option.
  5. Select the check box, **Account is Disabled**, if not already selected.
- **Issue**: The server response of IPv4 and IPv6 addresses groups are intermixed in the presence of multi NIC cards.
  Workaround: None.
- **Issue**: When an auto rebuild is enabled, multiclick PD actions are not updated properly.
  Workaround: Manually refresh the page.
- **Issue**: Google Chrome may not position popup windows correctly.

Workaround: None.
Version: 61.0.3163.100 and later

- **Issue**: When using Mozilla FireFox, do not save the user name and password, or click the user name text box to enable saving.
  Workaround: None.
- **Issue**: Operations performed during an online controller reset fail.
  Workaround: Do not perform any operation in MRSA during an online controller reset.
- **Issue**: Zoom operations.
  Workaround: Do not zoom operations on a browser until the monitor resolution is low.
- **Issue**: Performing any action (for example, Configuration) from the Server summary page, then manually refreshing the page causes the user to be redirected to the initially selected Action page.
  Workaround: Do not perform a manual refresh.
- **Issue**: Converting a JBOD PD from JBOD to UG causes the application to display different action menu names. MRSA displays it as **Make unconfigured good**.
- **Issue**: If the same dedicated spare is assigned to multiple drive groups, you may see inconsistency in the Element Count and DHSP Element selection check boxes on the Controller page.
- **Issue**: In MegaRAID, when the patrol read is running at the physical drive level, it is a controller level operation. Each individual physical drive patrol read progress bar will not disappear after completing 100%.
  Workaround: Wait for all of the physical drive progress bars to complete. Once all of the physical drive progress bars have reached 100%, they disappear.
- **Issue**: During installation or uninstallation, the publisher can show as unknown on the **User Account Control** message box.
- **Issue**: MRSA does not allow the physical drive to be selected from non-spanned volumes or spanned volumes.
- **Issue**: The **Modify** option for the existing `setup.exe` does not work.
  Workaround: Uninstall and reinstall the build instead of using the **Modify** option.

Multi-Selection Threshold Physical Drives

While selecting physical drives, you can only select up to 32 PDs.

If you want to select more than 32 PDs, perform the following steps:

1. Navigate to the directory `\LSIStorageAuthority\server\html\files`
2. Open the `Configfile.json` file.
3. In the `Configfile.json` file, search for the `maxVDs` field.
   The `maxVDs` field is set by default to a value of `32` to accept 32 PDs.
4. Modify this value to `64` .
5. Clear your browser's history.

Now, you can select more than 32 PDs, up to a maximum of 64 PDs.

Support and Other Resources

Accessing Hewlett Packard Enterprise Support

For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

http://www.hpe.com/assistance

To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

http://www.hpe.com/support/hpesc

Information to collect:

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing Updates

Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.

To download product updates:

Hewlett Packard Enterprise Support Center

www.hpe.com/support/hpesc

Hewlett Packard Enterprise Support Center: Software downloads

www.hpe.com/support/downloads

My HPE Software Center

www.hpe.com/support/softwaredepot

To subscribe to eNewsletters and alerts:

www.hpe.com/support/e-updates

To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page:

www.hpe.com/support/AccessToSupportMaterials

> **NOTE**
>
> Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Customer Self Repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website: www.hpe.com/support/selfrepair

Remote Support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

- **HPE Get Connected**
  www.hpe.com/services/getconnected
- **HPE Proactive Care Services**
  www.hpe.com/services/proactivecare
- **HPE Proactive Care Service: Supported Products List**
  www.hpe.com/services/proactivecaresupportedproducts
  HPE Proactive Care Advanced Service: Supported Products List
  www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care Customer Information

- **Proactive Care Central**
- **Proactive Care Service Activation**
  www.hpe.com/services/proactivecarecentralgetstarted

Warranty Information

To view the warranty for your product or to view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products* reference document, go to the Enterprise Safety and Compliance website:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional warranty information

- **HPE ProLiant and x86 Servers and Options**
  www.hpe.com/support/ProLiantServers-Warranties
- **HPE Enterprise Servers**
  www.hpe.com/support/EnterpriseServers-Warranties
- **HPE Storage Products**
  www.hpe.com/support/Storage-Warranties
  HPE Networking Products
  www.hpe.com/support/Networking-Warranties

Regulatory Information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, includingRoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

Documentation Feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Glossary

This glossary defines the terms used in this document.

access policy A volume property indicating what kind of access is allowed for a particular volume. The possible values are *Read/Write*, *Read Only*, or *Blocked*.

array A group of drives attached to a RAID controller on which one or more volumes can be created. All volumes in the array use all of the drives in the array.

BIOS Basic Input/Output System. The computer BIOS is stored on a flash memory chip. The BIOS controls communications between the microprocessor and peripheral devices, such as the keyboard and the video controller, and miscellaneous functions, such as system messages.

cache Fast memory that holds recently accessed data. Use of cache memory speeds subsequent access to the same data. When data is read from or written to main memory, a copy is also saved in cache memory with the associated main memory address. The cache memory software monitors the addresses of subsequent reads to see if the required data is already stored in cache memory. If it is already in cache memory (a cache hit), it is read from cache memory immediately and the main memory read is aborted (or not started). If the data is not cached (a cache miss), it is fetched from main memory and saved in cache memory.

caching The process of using a high speed memory buffer to speed up a computer system's overall read/write performance. The cache can be accessed at a higher speed than a drive subsystem. To improve read performance, the cache usually contains the most recently accessed data, as well as data from adjacent drive sectors. To improve write performance, the cache can temporarily store data in accordance with its write back policies.

capacity A property that indicates the amount of storage space on a drive or volume.

coerced capacity A drive property indicating the capacity to which a drive has been coerced (forced) to make it compatible with other drives that are nominally the same capacity. For example, a 4-GB drive from one manufacturer might be 4196 MB, and a 4-GB from another manufacturer might be 4128 MB. These drives could be coerced to a usable capacity of 4088 MB each for use in a array in a storage configuration.

coercion mode A controller property indicating the capacity to which drives of nominally identical capacity are coerced (forced) to make them usable in a storage configuration.

consistency check An operation that verifies that all stripes in a volume with a redundant RAID level are consistent and that automatically fixes any errors. For RAID 1 arrays, this operation verifies correct mirrored data for each stripe.

consistency check rate The rate at which consistency check operations are run on a computer system.

controller A chip that controls the transfer of data between the microprocessor and memory or between the microprocessor and a peripheral device such as a drive. HPE Smart Array P824i-p MR Gen10 Controllers perform RAID functions such as striping and mirroring to provide data protection.

copyback The procedure used to copy data from a source drive of a volume to a destination drive that is not a part of the volume. The copyback operation is often used to create or restore a specific physical configuration for a array (for example, a specific arrangement of array members on the device I/O buses). The copyback operation can be run automatically or manually.

Typically, a drive fails or is expected to fail, and the data is rebuilt on a spare drive. The failed drive is replaced with a new drive. Then the data is copied from the spare drive to the new drive, and the spare drive reverts from a rebuild drive to its original spare drive status. The copyback operation runs as a background activity, and the volume is still available online to the host.

current write policy	A volume property that indicates whether the volume currently supports Write Back mode or Write Through mode. • In Write Back mode, the controller sends a data transfer completion signal to the host when the controller cache has received all of the data in a transaction. • In Write Through mode, the controller sends a data transfer completion signal to the host when the drive subsystem has received all of the data in a transaction.
device ID	A controller or drive property indicating the manufacturer-assigned device ID.
DDF	Data disk format.
drive type	A drive property indicating the characteristics of the drive.
fast initialization	A mode of initialization that quickly writes zeros to the first and last sectors of the volume. This allows you to immediately start writing data to the volume while the initialization is running in the background.
fault tolerance	The capability of the drive subsystem to undergo a single drive failure per array without compromising data integrity and processing capability. HPE Smart Array MR Controllers provide fault tolerance through redundant arrays in RAID levels 1, 5, 6, 10, 50, and 60. They also support spare drive drives and the auto-rebuild feature.
firmware	Software stored in read-only memory (ROM) or programmable ROM (PROM). Firmware is often responsible for the behavior of a system when it is first turned on. A typical example would be a monitor program in a system that loads the full operating system from a drive or from a network, then passes control to the operating system.
formatting	The process of writing a specific value to all data fields on a drive, to map out unreadable or bad sectors. Because most drives are formatted when manufactured, formatting is usually done only if a drive generates many media errors.
FS	File system.
GUI	Graphical user interface.
HPE Smart Storage Energy Pack	Refers to a energy pack backup unit.
JBOD	Just a bunch of disks. JBOD generally refers to a collection of hard disks that are directly managed by the host. JBOD is an alternative to using a RAID configuration. Rather than configuring a storage array to use a RAID level, the disks within the array are treated as independent disks.
initialization	The process of writing zeros to the data fields of a volume and, in fault-tolerant RAID levels, generating the corresponding parity to put the volume in a Ready state. Initialization erases all previous data on the drives. Arrays will work without initializing, but they can fail a consistency check because the parity fields have not been generated.
IO policy	A volume property indicating whether Cached I/O or Direct I/O is being used. In Cached I/O mode, all reads are buffered in cache memory. In Direct I/O mode, reads are not buffered in cache memory. Data is transferred to cache and the host concurrently. If the same data block is read again, it comes from cache memory. (The IO Policy applies to reads on a specific volume. It does not affect the read ahead cache.)
load-balancing	A method of spreading work between two or more computers, network links, CPUs, drives, or other resources. Load balancing maximizes resource use, throughput, or response time.
LDF	Logical disk format.
mirroring	The process of providing complete data redundancy with two drives by maintaining an exact copy of one drive's data on the second drive. If one drive fails, the contents of the other drive can be used to maintain the integrity of the system and to rebuild the failed drive.
multipathing	The firmware provides support for detecting and using multiple paths from the HPE Smart Array P824i-p MR Gen10 Controllers to the SAS devices that are in enclosures. Devices connected to enclosures have multiple paths to them. With redundant paths to the same port of a device, if one path fails, another path can be used to communicate between the controller and the device. Using multiple paths with load balancing, instead of a single path, can increase reliability through redundancy.

offline	A drive is offline when it is part of a volume but its data is not accessible to the volume.
OS	Operating system.
patrol read	A process that checks the drives in a storage configuration for drive errors that could lead to drive failure and lost data. The patrol read operation can find and sometimes fix any potential problem with drives before host access. This enhances overall system performance because error recovery during a normal I/O operation might not be necessary.
patrol read rate	The user-defined rate at which patrol read operations are run on a computer system.
physical drive or disk (PD)	A disk used to emphasize a contract with virtual disks.
RAID	A group of multiple, independent drives that provide high performance by increasing the number of drives used for saving and accessing data. A RAID array improves input/output (I/O) performance and data availability. The group of drives appears to the host system as a single storage unit or as multiple volumes. Data throughput improves because several drives can be accessed simultaneously. RAID configurations also improve data storage availability and fault tolerance. Redundant RAID levels (RAID levels 1, 5, 6, 10, 50, and 60) provide data protection.
RAID 0	Uses data striping on two or more drives to provide high data throughput, especially for large files in an environment that requires no data redundancy.
RAID 1	Uses data mirroring on pairs of drives so that data written to one drive is simultaneously written to the other drive. RAID 1 works well for small databases or other small applications that require complete data redundancy.
RAID 5	Uses data striping and parity data across three or more drives (distributed parity) to provide high data throughput and data redundancy, especially for applications that require random access.
RAID 6	Uses data striping and parity data across three or more drives (distributed parity) to provide high data throughput and data redundancy, especially for applications that require random access. RAID 6 can survive the failure of two drives.
RAID 10	A combination of RAID 0 and RAID 1 that uses data striping across two mirrored arrays. It provides high data throughput and complete data redundancy.
RAID 50	A combination of RAID 0 and RAID 5 that uses data striping across two arrays with parity data. It provides high data throughput and complete data redundancy.
RAID 60	A combination of RAID 0 and RAID 6 that uses data striping across two arrays with parity data. It provides high data throughput and complete data redundancy. RAID 60 can survive the failure of two drives in each RAID set in the spanned array.
RAID level	A volume property indicating the RAID level of the volume. HPE Smart Array MR Controllers support RAID levels 0, 1, 5, 6, 10, 50, and 60.
RAID transformation	A feature in RAID subsystems that allows changing a RAID level to another level without powering down the system.
raw capacity	A drive property indicating the actual full capacity of the drive before any coercion mode is applied to reduce the capacity.
read policy	A controller attribute indicating the current Read Policy mode. In Always Read Ahead mode, the controller reads sequentially ahead of requested data and stores the additional data in cache memory, anticipating that the data will be needed soon. This speeds up reads for sequential data, but there is little improvement when accessing random data. In No Read Ahead mode (known as Normal mode in WebBIOS), read ahead capability is disabled.
rebuild	The regeneration of all data to a replacement drive in a redundant volume after a drive failure. A drive rebuild normally occurs without interrupting normal operations on the affected volume, though some degradation of performance of the drive subsystem can occur.
rebuild rate	The percentage of central processing unit (CPU) resources devoted to rebuilding data onto a new drive after a drive in a storage configuration has failed.
reclaim volume	A method of undoing the configuration of a new volume. If you highlight the volume in the **Configuration** wizard and click **Reclaim**, the individual drives are removed from the volume configuration.

redundancy	A property of a storage configuration that prevents data from being lost when one drive fails in the configuration.
redundant configuration	A volume that has redundant data on drives in the array that can be used to rebuild a failed drive. The redundant data can be parity data striped across multiple drives in a array, or it can be a complete mirrored copy of the data stored on a second drive. A redundant configuration protects the data in case a drive fails in the configuration.
SAS	Acronym for Serial-Attached SCSI. SAS is a serial, point-to-point, enterprise-level device interface that leverages the Small Computer System Interface (SCSI) protocol set. The SAS interface provides improved performance, simplified cabling, smaller connectors, lower pin count, and lower power requirements when compared to parallel SCSI.
SATA	Acronym for Serial Advanced Technology Attachment. A physical storage interface standard. SATA is a serial link that provides point-to-point connections between devices. The thinner serial cables allow for better airflow within the system and permit smaller chassis designs.
SCSI device type	A drive property indicating the type of the device, such as drive.
serial no.	A controller property indicating the manufacturer-assigned serial number.
spare drive	A standby drive that can automatically replace a failed drive in a volume and prevent data from being lost. A spare drive can be dedicated to a single redundant array or it can be part of the global spare drive pool for all arrays controlled by the controller. When a drive fails, the application automatically uses a spare drive to replace it and then rebuilds the data from the failed drive to the spare drive. Spare Drives can be used in RAID 1, 5, 6, 10, 50, and 60 storage configurations.
stripe size	A volume property indicating the length of the interleaved data segments that the RAID controller writes across multiple drives, not including parity drives. For example, consider a stripe that contains 64 KB of drive space and has 16 KB of data residing on each drive in the stripe. In this case, the stripe size is 64 KB, and the strip size is 16 KB. The user can select the stripe size.
striping	A technique used to write data across all drives in a volume. Each stripe consists of consecutive volume data addresses that are mapped in fixed-size units to each drive in the volume using a sequential pattern. For example, if the volume includes five drives, the stripe writes data to drives one through five without repeating any of the drives. The amount of space consumed by a stripe is the same on each drive. Striping by itself does not provide data redundancy. Striping in combination with parity does provide data redundancy.
strip size	The portion of a stripe that resides on a single drive in the array.
subvendor ID	A controller property that lists additional vendor ID information about the controller.
transformation	The process of moving volumes and spare drive drives from one controller to another by disconnecting the drives from one controller and attaching them to another one. The firmware on the new controller will detect and retain the volume information on the drives.
transformation rate	The user-defined rate at which an array modification operation is carried out.
URI	Uniform Resource Identifier.
vendor ID	A controller property indicating the vendor-assigned ID number of the controller.
vendor info	A drive property listing the name of the vendor of the drive.
volume	An entity within a SCSI target that executes I/O commands. A storage unit created by a RAID controller from one or more drives. Although a volume can be created from several drives, it is seen by the operating system as a single drive. Depending on the RAID level used, the volume can retain redundant data in case of a drive failure.
volume state	A volume property indicating the condition of the volume. Examples include Optimal and Degraded.
write-back	In Write-Back Caching mode, the controller sends a data transfer completion signal to the host when the controller cache has received all of the data in a drive write transaction. Data is written to the drive subsystem in accordance with policies set up by the controller. These policies include the amount of dirty/clean cache lines, the number of cache lines available, and elapsed time from the last cache flush.

write policy See *Default Write Policy*.

write-through In Write-Through Caching mode, the controller sends a data transfer completion signal to the host when the drive subsystem has received all of the data and has completed the write transaction to the drive.

Revision History

Version 1.10, May 2025

Updated the terminology for virtual drive. Updated Changing Behavior Modes and Make Unconfigured Good Drives and Make JBOD Drives section.

Added Clearing NVRAM.

Version 1.9, February 2025

Updated the terminology for logical drive, hot spare, and OCE. Updated the UNMAP Capability Feature, Managing Arrays, and Make Unconfigured Good Drives and Make JBOD Drives sections.

Added Spin Down, Replacing a Missing Drive, and NVMe Thermal Poll Interval.

Removed CacheCade content.

Version 1.8, January 2024

Updated the Abstract and Support Matrix.

Added Upgrade Requirements, Standalone Installer, Installing the LSI Storage Authority Software on the Microsoft Windows Operating System, Installing the LSI Storage Authority Software on the Linux Operating System, Changing the LSI Storage Authority Application Port Number, Changing the nginx Web Server Port Numbers, and Changing the nginx Read Timeout.

Version 1.7, September 2023

Updated the Making a Drive Online and Known Issues and Workarounds sections.

Added Changing Behavior Modes.

Version 1.6, May 2023

Updated the Using the MegaRAID CacheCade Pro 2.0 Feautre and Known Issues and Workarounds sections.

Added Configuring Different Types of Access.

Version 1.5, October 2022

Updated the Support Matrix, Erasing a Drive Securely, Sanitizing a Drive, Known Issues and Workarounds, and Glossary sections.

Version 1.4, April 2022

Added Known Issues and Workarounds, Marking a Drive as a Missing Drive, Removing a Drive, Erasing a Drive Securely, MegaRAID SafeStore Encryption Services, UNMAP Capability Feature, and Multi-Selection Threshold for Virtual and Physical Drives sections.

Updated Clearing the Configuration, Deleting a Logical Drive, Performing Initial Configuration, Glossary, and Support Matrix sections.

Version 1.3, February 2021

Added new Known Issues and Workarounds, Marking a Drive as a Missing Drive, Removing a Drive, Erasing a Drive Securely, MegaRAID SafeStore Encryption Services, UNMAP Capability Feature, and Multi-Selection Threshold for Virtual and Physical Drives sections.

Updated Clearing the Configuration, Deleting a Logical Drive, Performing Initial Configuration, Glossary, and Support Matrix sections.

Preliminary, Version 1.1, January 2020

Updated the Overview, Server Dashboard, and Configuration sections.

Preliminary, Version 1.0, December 25, 2017

Initial document release.