



Western Digital®

User Guide

Resource Manager Standard Edition

Software Version 1.3.1
Document D018-000126-000
Revision 05
March 2024

Table of Contents

Revision History.....

iii

Notices.....

v

Points of Contact.....

vi

Chapter 1. Overview.....

1

Resource Manager Standard Edition Overview.....

2

Supported Platforms.....

8

Required Firmware.....

8

Compatible Operating Systems.....

8

Compatible Browsers.....

9

Required Software.....

9

Third Party Licenses.....

10

Chapter 2. Installation.....

11

Downloading Resource Manager Standard Edition.....

12

Installing Resource Manager Standard Edition for Linux.....

16

Installing Resource Manager Standard Edition for Windows.....

18

Chapter 3. Management.....

29

Accessing Resource Manager Standard Edition.....

30

Dashboard.....

34

Switching Enclosures Using Drop-Down List.....

35

Switching Enclosures Using Icon.....

36

Virtual View.....

39

Internal View.....

39

Front View.....

39

Rear View.....

44

Devices.....

51

Drives.....

51

Zoning.....69

IOM.....94

Sensors.....112

MegaRAID.....115

 Controller.....115

 RAID Configuration.....129

 Logical Drives.....147

 Physical Drives.....169

Alerts.....184

 Configuring Email Notifications.....184

 Configuring SMTP.....185

 Viewing / Downloading Events.....186

 Downloading Logs.....188

Settings.....190

 Adding an Account.....190

 Editing an Account.....193

 Deleting an Account.....196

 Installing an SSL Certificate.....198

Virtual Tour.....203

 Taking a Virtual Tour.....203

Chapter 4. Appendices..... 205

 Download Links for Required Software..... 206

Revision History

Date	Revision	Comment
June 2021	01	Initial release
January 2022	02	Updated for software version 1.1 release
		Made the following changes for software version 1.2 release:
		<ul style="list-style-type: none"> Removed Ultrastar Serv60+8 content throughout Added Red Hat Enterprise Linux & CentOS 7.6 to Compatible Operating Systems (page 8); removed SUSE Linux Enterprise Server (only used for Ultrastar Serv60+8) Added WDCKIT to Required Software (page 9); removed ipmiutil (only used for Ultrastar Serv60+8); Added Updating Drive Firmware, Single Drive (HBA) (page 55), Updating Drive Firmware, Multiple Drives (HBA) (page 62), Updating Drive Firmware, Single Drive (MegaRAID) (page 173), and Updating Drive Firmware, Multiple Drives (MegaRAID) (page 177) Added Exporting a Custom Zoning Configuration (page 80) and Importing a Custom Zoning Configuration (page 85) Added Checking Cable Information (Rear) (page 48) and Checking Cable Information (IOM) (page 107) Added Checking Background Processes (page 115) Added Modifying a Drive Group / RAID Configuration (page 147), Starting a Consistency Check (page 152), Initializing a Logical Drive (page 156), and Erasing a Logical Drive (page 160)
May 2022	03	
		Made the following changes for software version 1.3 release:
		<ul style="list-style-type: none"> Updated to new branding Updated images and instructions throughout Updated download instructions in Downloading Resource Manager Standard Edition (page 12) Updated installation instructions in Installing Resource Manager Standard Edition for Linux (page 16) to include custom port numbers Added note about Rebuild and Copyback features to Creating a Drive Group / RAID Configuration (page 129) Added Downloading SES PHY Counters (page 110) Added Starting Patrol Read (page 117) Added Configuring SMTP (page 185), Viewing / Downloading Events (page 186), and Downloading Logs (page 188) Added Installing an SSL Certificate (page 198) Added Download Links for Required Software (page 206)
December 2022	04	

Date	Revision	Comment
March 2024	05	Made the following changes for software version 1.3.1 release: <ul style="list-style-type: none">Added Werkzeug 2.2.2 to Required Software (page 9) and Download Links for Required Software (page 206)

Notices

Western Digital Technologies, Inc. or its affiliates' (collectively "Western Digital") general policy does not recommend the use of its products in life support applications wherein a failure or malfunction of the product may directly threaten life or injury. Per Western Digital Terms and Conditions of Sale, the user of Western Digital products in life support applications assumes all risk of such use and indemnifies Western Digital against all damages.

This document is for information use only and is subject to change without prior notice. Western Digital assumes no responsibility for any errors that may appear in this document, nor for incidental or consequential damages resulting from the furnishing, performance or use of this material.

Absent a written agreement signed by Western Digital or its authorized representative to the contrary, Western Digital explicitly disclaims any express and implied warranties and indemnities of any kind that may, or could, be associated with this document and related material, and any user of this document or related material agrees to such disclaimer as a precondition to receipt and usage hereof.

Each user of this document or any product referred to herein expressly waives all guaranties and warranties of any kind associated with this document any related materials or such product, whether expressed or implied, including without limitation, any implied warranty of merchantability or fitness for a particular purpose or non-infringement. Each user of this document or any product referred to herein also expressly agrees Western Digital shall not be liable for any incidental, punitive, indirect, special, or consequential damages, including without limitation physical injury or death, property damage, lost data, loss of profits or costs of procurement of substitute goods, technology, or services, arising out of or related to this document, any related materials or any product referred to herein, regardless of whether such damages are based on tort, warranty, contract, or any other legal theory, even if advised of the possibility of such damages.

This document and its contents, including diagrams, schematics, methodology, work product, and intellectual property rights described in, associated with, or implied by this document, are the sole and exclusive property of Western Digital. No intellectual property license, express or implied, is granted by Western Digital associated with the document recipient's receipt, access and/or use of this document or the products referred to herein; Western Digital retains all rights hereto.

Western Digital, the Western Digital design, the Western Digital logo, and Ultrastar are registered trademarks or trademarks of Western Digital Corporation or its affiliates in the US and/or other countries. Apache HTTP Server is either a registered trademark or trademark of the Apache Software Foundation in the United States and/or other countries. Chrome is a trademark of Google LLC. Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries. MegaRAID is among the trademarks of Broadcom. MongoDB is a trademark of MongoDB, Inc. Oracle is a registered trademark of Oracle and/or its affiliates. "Python" is a trademark or registered trademark of the Python Software Foundation. Red Hat Enterprise Linux is a registered trademark of Red Hat, Inc. in the U.S. and other countries. All other marks are the property of their respective owners. Not all products are available in all regions of the world. Pictures shown may vary from actual products. Product specifications subject to change without notice.

Western Digital
5601 Great Oaks Parkway
San Jose, CA 95119

© 2024 Western Digital Corporation or its affiliates. All Rights Reserved.

Points of Contact

For further assistance with a Western Digital product, contact Western Digital Datacenter Platforms technical support. Please be prepared to provide the following information, as applicable: part number (P/N), serial number (S/N), product name and/or model number, software version, and a brief description of the issue.

Website:

<https://portal.wdc.com/s/>

Email:

enterprisesupport@wdc.com

UK Import Representation Contact

Western Digital UK Limited

PO Box 471
Leatherhead KT22 2LU
UK

Telephone: +44 1372 366000

EU Import Representation Contact

Western Digital EU Limited

PO Box 13379
Swords, Co
Dublin, Ireland



Overview

In This Chapter:

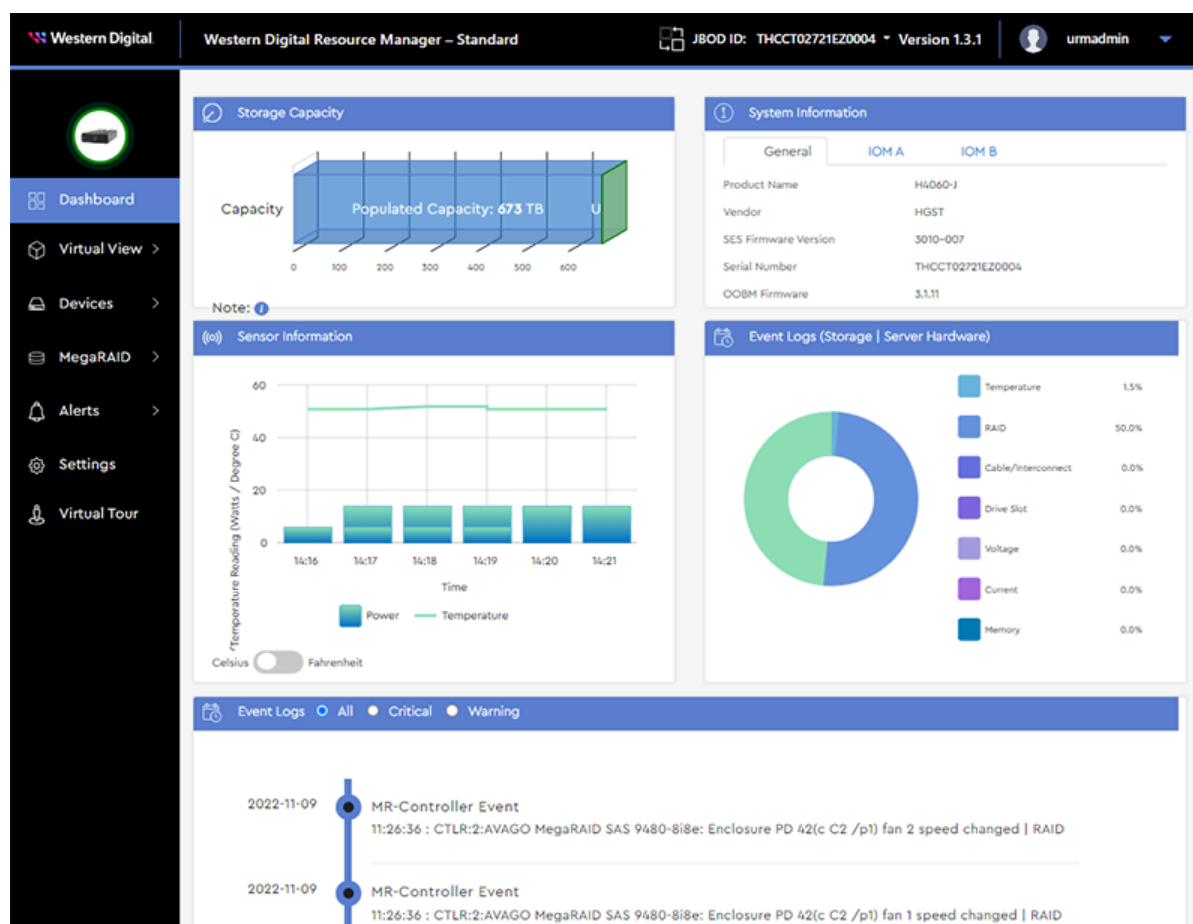
- Resource Manager Standard Edition Overview.....	2
- Supported Platforms.....	8
- Required Firmware.....	8
- Compatible Operating Systems.....	8
- Compatible Browsers.....	9
- Required Software.....	9
- Third Party Licenses.....	10

1.1 Resource Manager Standard Edition Overview

Resource Manager Standard Edition is an in-band monitoring and management application for Western Digital storage platforms. It runs on the host operating system (Windows® or Linux®), using a RESTful interface to present a real-time status of the platform's storage health and management controls to the browser in the form of an intuitive GUI.

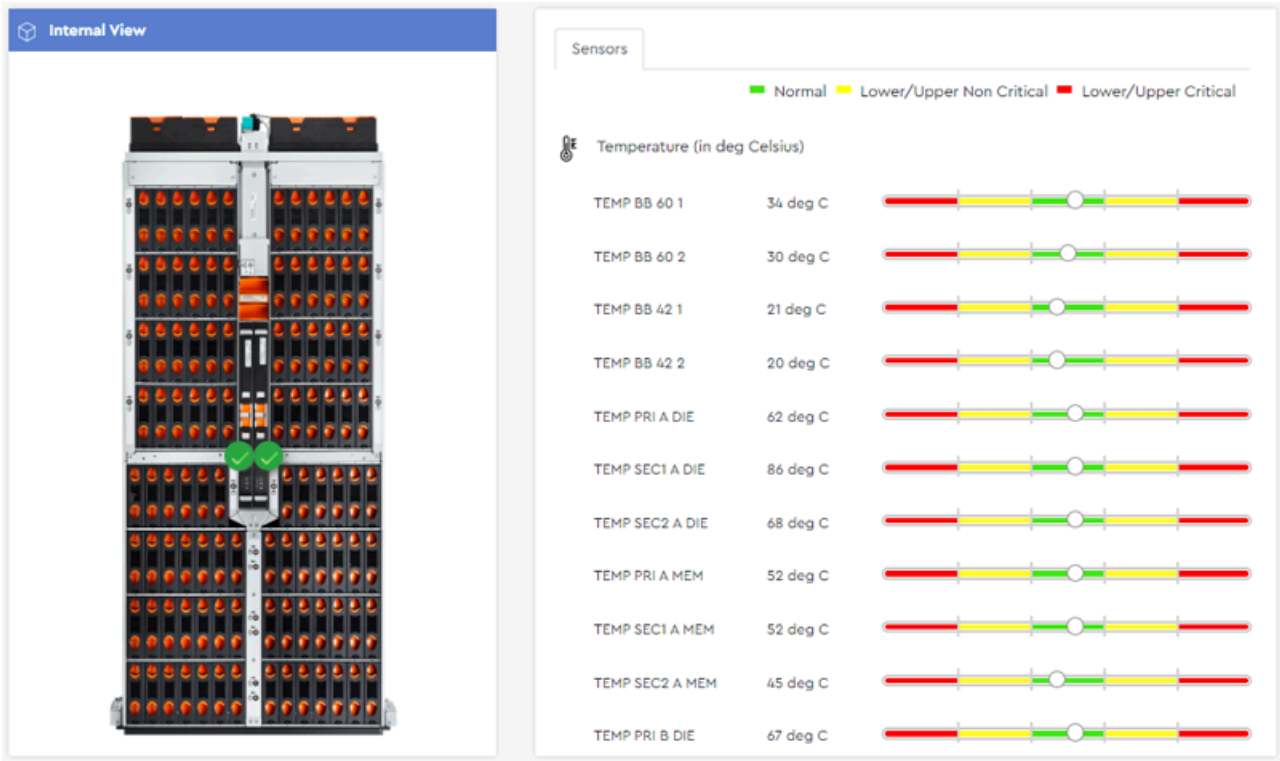
Dashboard

The dashboard is a consolidated monitoring page displaying the most critical enclosure data, such as populated/unpopulated storage capacity, system information, IOM information, the last 10 minutes of sensor readings, and events. For more information, see [Dashboard \(page 34\)](#).



Virtual View

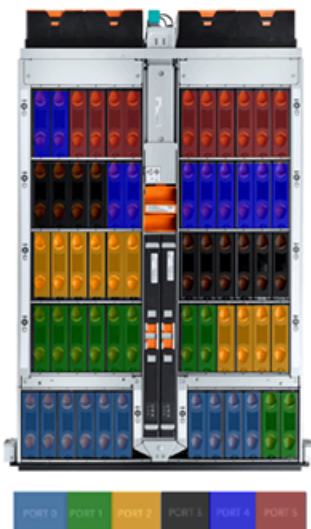
The **Virtual View** section provides real-time health status and sensor information for the components visible or accessible from different perspectives, such as drives, system fans, IOMs, and PSUs. Front and rear views also provide enclosure LED management controls. For more information, see [Virtual View \(page 39\)](#).



Devices

The **Devices** section provides information about the enclosure's sensors and major components, as well as management controls for drives, zoning, and IOM(s). If drives are managed through an HBA, or a MegaRAID controller in JBOD mode, the **Devices** section also provides drive LED management controls. For more information, see [Devices \(page 51\)](#).

Drive Zones



Zoning

Current Status

Disabled

Zoning Configuration

Configuration 1

Import Configuration

Import

Configuration 1

Enable

zone A

Color Code

port0

slot0

slot1

slot2

slot3

slot4

slot5

slot6

slot7

slot8

slot9

zone B

zone C

zone D

MegaRAID

The **MegaRAID** section provides information about all MegaRAID controllers detected in the host, and management controls for drive identification LEDs, grouping drives, assigning RAID levels, and allocating capacity to logical drives. For more information, see [MegaRAID \(page 115\)](#).

Logical Drives

enclosure_66enclosure_124

ConfigureController IDAVAGO MegaRAID SAS 9480-8i8e

Important Note: 2 Background processess running. [Click here](#) to view

Total Logical drives: 9Total Global hot spare: 2

Drive Group	RAID Level	Physical Drives	Logical Drives	Hot Spares	Capacity	Utilization	Action
> DG0	RAID 0	2	4	0	14.553 TB	100%	...
> DG1	RAID 5	4	4	0	16.374 TB	100%	...
✓ DG2	RAID 5	5	1	0	36.382 TB	100%	...

Enc ID	Slot ID	Device ID	Drive Type	Interface	Serial number	Capacity
66	56	18	HDD	SAS	VCG1M55M	9.096 TB
66	29	33	HDD	SAS	8DG3L9ED	10.914 TB
66	55	45	HDD	SAS	VCG16GAN	9.096 TB
124	2	68	HDD	SAS	9JG1G8DG	12.733 TB

Logical drive

- LD NameVD1
- LD ID8
- Capacity36.365 TB
- Stripe Size256KB
- PolicyRA | WB | DIO

Alerts

The **Alerts** section provides information and controls for setting up email notifications, configuring SMTP settings, checking event logs, and downloading SES firmware and system log files. For more information, see [Alerts \(page 184\)](#).

Email Configuration

Configure emails to send the updates to one or more users.

Email Notification Settings

Notify me for ☒ All ☐ Critical ☐ Warning

Add Email for Notification

Email Address 1

Add more Emails

Save

User Settings

The **Settings** section allows configuration of user account details such as IDs, roles, email addresses, and passwords. For more information, see [Settings \(page 190\)](#).

Settings

User Settings

SSL Certificate

Search

+ Add User

Edit

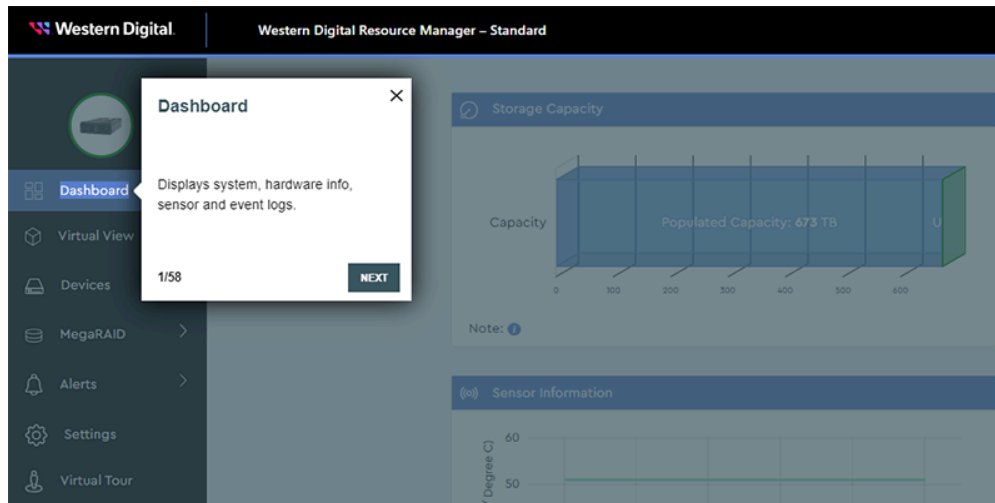
Delete

Serial Number	User ID	User Role	Mail	User Created Time	Last Logged Time
1	urmadmin	admin	admin@wdc.com	09/12/2022, 05:26:22	11/11/2022, 16:46:43
2	test1	user	firstname.lastname@company.com	11/11/2022, 15:02:39	N/A
3	test2	user	firstname.lastname@company.com	11/11/2022, 15:03:09	N/A

1

Virtual Tour

The **Virtual Tour** section guides users through the Resource Manager Standard Edition graphical interface, providing tooltip explanations of menu options and page sections. For more information, see [Virtual Tour \(page 203\)](#).



1.2 Supported Platforms

The Resource Manager Standard Edition application supports storage management of the following platforms.

- Ultrastar® Data102
- Ultrastar Data60



Note: For supported hardware components, please refer to your platform's *Compatibility Matrix* and the Resource Manager Standard Edition *Release Notes*. Unless otherwise noted, the Resource Manager Standard Edition is compatible with each platform's supported components.

1.3 Required Firmware

Supported platforms require the following firmware versions for compatibility with the Resource Manager Standard Edition application.

Firmware	Version
SEP	3010-007 or later
OOBM	3.111 or later

1.4 Compatible Operating Systems

The server must be running one of the following operating systems in order to host the Resource Manager Standard Edition application.

Operating System	Version
Red Hat® Enterprise Linux® (RHEL)	7.6, 7.9, 8.0, 8.2, 8.3
CentOS	7.6, 7.9, 8.0, 8.2, 8.3
Ubuntu	16.04, 18.04, 20.04
Debian	10.9
Oracle® Linux	8.2
Windows Server®	2016, 2019

1.5 Compatible Browsers

The host server requires one of the following browsers to run the Resource Manager Standard Edition application.

Browser	Version
Chrome	83.0.4103.97 or newer
Firefox	68.9.0esr (64-bit) or newer

1.6 Required Software

The following software (listed versions or later) must be installed on the host server for it to run the Resource Manager Standard Edition application.

Software	Version	Applicable OSs
Apache HTTP Server™	2.4.46	Linux only
Internet Information Services (IIS)	10	Windows only
URL Rewrite	2.1	Windows only
Microsoft Application Request Routing	3.0	Windows only
Python®	3.8.8	Windows & Linux
Python Modules:		
pip	9.0.1	
Flask	2.2.2	
Flask-Cors	3.0.8	
Flask-RESTful	0.3.9	
pymongo	4.2.0	
requests	2.18.4	Windows & Linux
PyJWT	2.0.1	
json2html	1.3.0	
waitress	2.0.0	
Paste	3.5.0	
pyOpenSSL	22.1.0	
Werkzeug	2.2.2	
Python Modules:		
pywin32	300	Windows only
psutil	5.8.0	
MongoDB™	4.4	Windows & Linux
sg_utils	1.42	Windows & Linux

Linux Installation Notes



Important: If `python3.8` is already installed, but the `python3 --version` command returns a version number different from `3.8.x`, do the following to activate the `python3.8.x` version: Run the `which python3.8` command to get the location path where `python3.8` is installed. Copy the path from the command output and use it to set the symbolic links in `/usr/bin/`.

Windows Installation Notes



Important: `Python38`, `Python38\Scripts`, and `sg3_util` will not be added to the system PATH environment variable by default; please add them manually.



Important: After installing `pywin32` using `pip install`, from a command prompt, change directory to `Python\Python38\Scripts\`; the exact path may vary depending on the location where Python is installed on your operating system. Then run the following command:

```
python pywin32_postinstall.py -install
```

1.7 Third Party Licenses

This product may include or use open source software subject to open source licenses. If required by the applicable open source license, Western Digital may provide the open source code to you on request either electronically or on a physical storage medium for a charge covering the cost of performing such distribution, which may include the cost of media, shipping, and handling.

For open source licensing information, please visit <https://www.westerndigital.com/company/innovation/open-source/product-compliance>.



Installation

In This Chapter:

- Downloading Resource Manager Standard Edition.....12
- Installing Resource Manager Standard Edition for Linux.....16
- Installing Resource Manager Standard Edition for Windows.....18

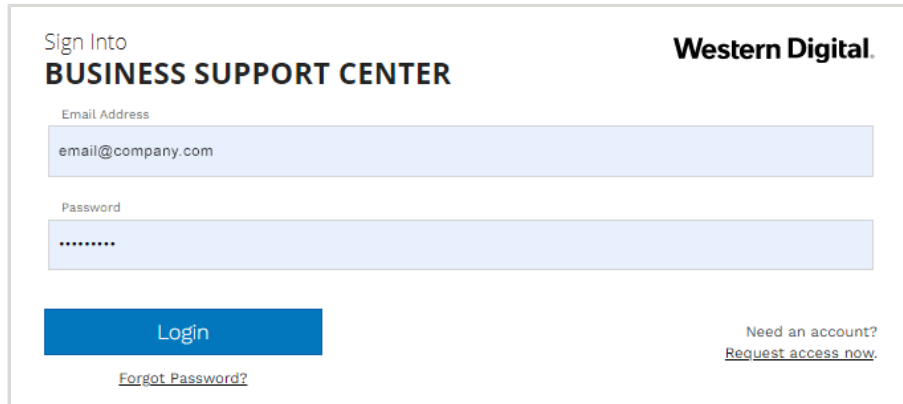
2.1 Downloading Resource Manager Standard Edition

This procedure provides instructions for downloading the Resource Manager Standard Edition application and documentation from the Western Digital Business Support Center.

Step 1: Open a web browser and navigate to: <https://portal.wdc.com/s/>.

The login page for the **Western Digital Business Support Center** will be displayed:

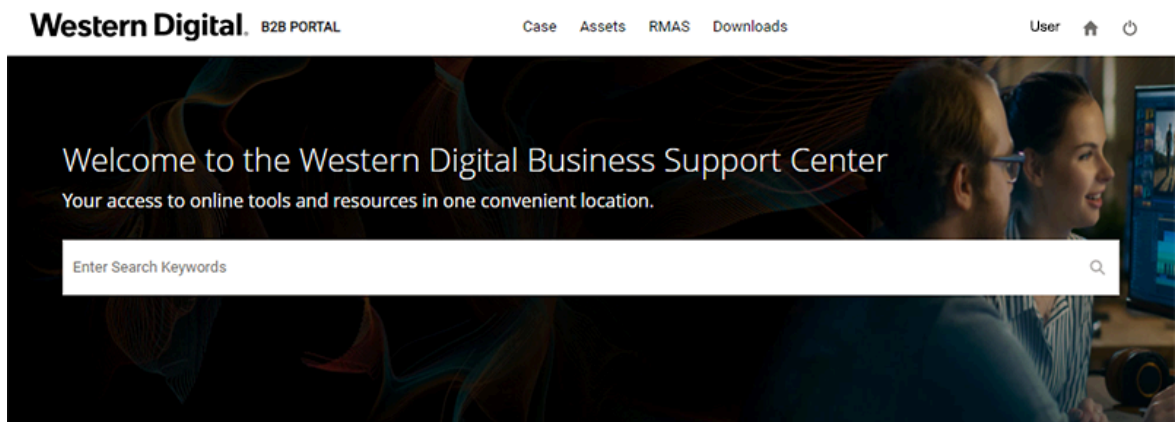
Figure 8: Login Page

The image shows the login page of the Western Digital Business Support Center. It features a header with the Western Digital logo and the text "Sign Into BUSINESS SUPPORT CENTER". Below the header are two input fields: "Email Address" with the placeholder text "email@company.com" and "Password" with masked characters "*****". A blue "Login" button is positioned below the password field. To the right of the login button, there is a link that says "Need an account? Request access now." and a link below the login button that says "Forgot Password?".

Step 2: Enter a valid email address and password into the **Email Address** and **Password** fields. Then click the **Login** button.

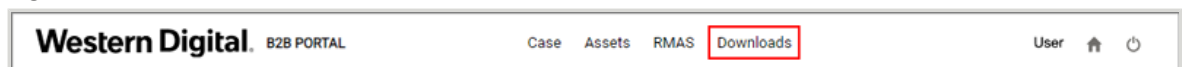
The **Western Digital B2B Portal** page will be displayed:

Figure 9: Western Digital B2B Portal



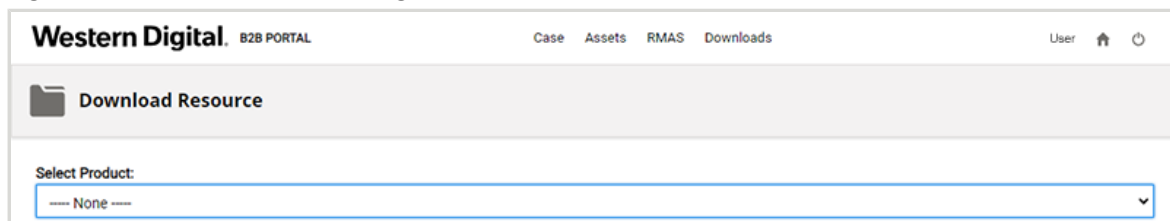
Step 3: Click **Downloads** at the top of the page:

Figure 10: Downloads Link



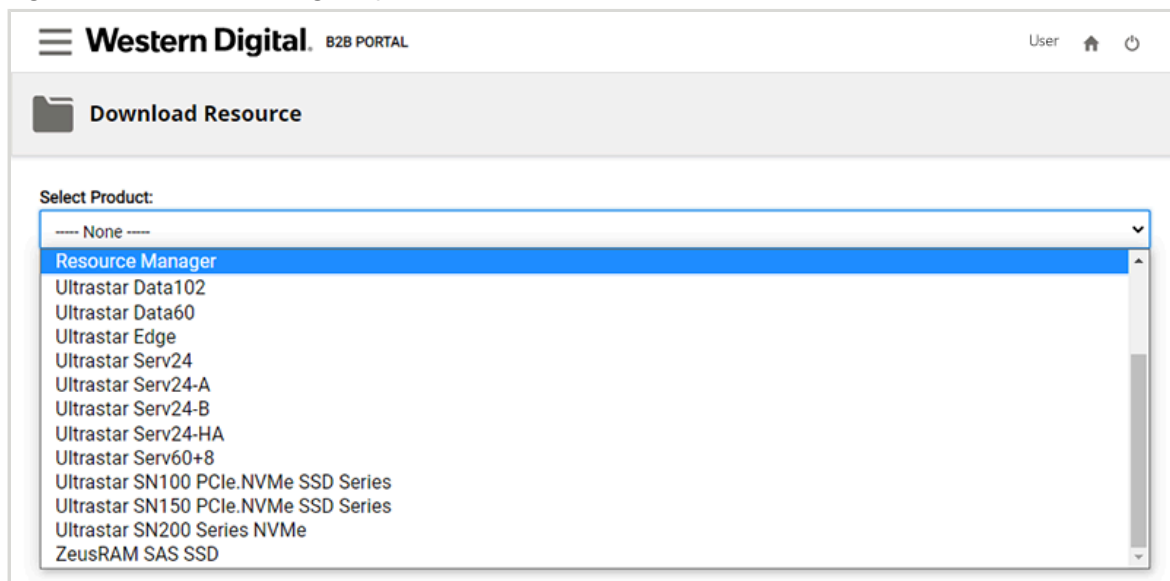
The **Download Resource** page will be displayed:

Figure 11: Download Resource Page



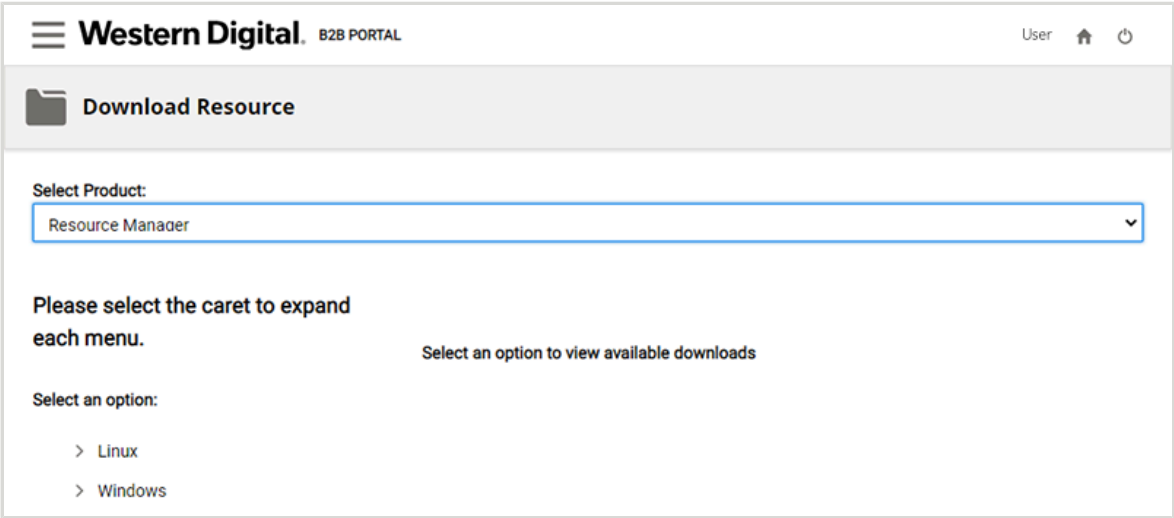
Step 4: Use the **Select Product** drop-down list to select the **Resource Manager** option:

Figure 12: Resource Manager Option



An operating system selection list will appear:

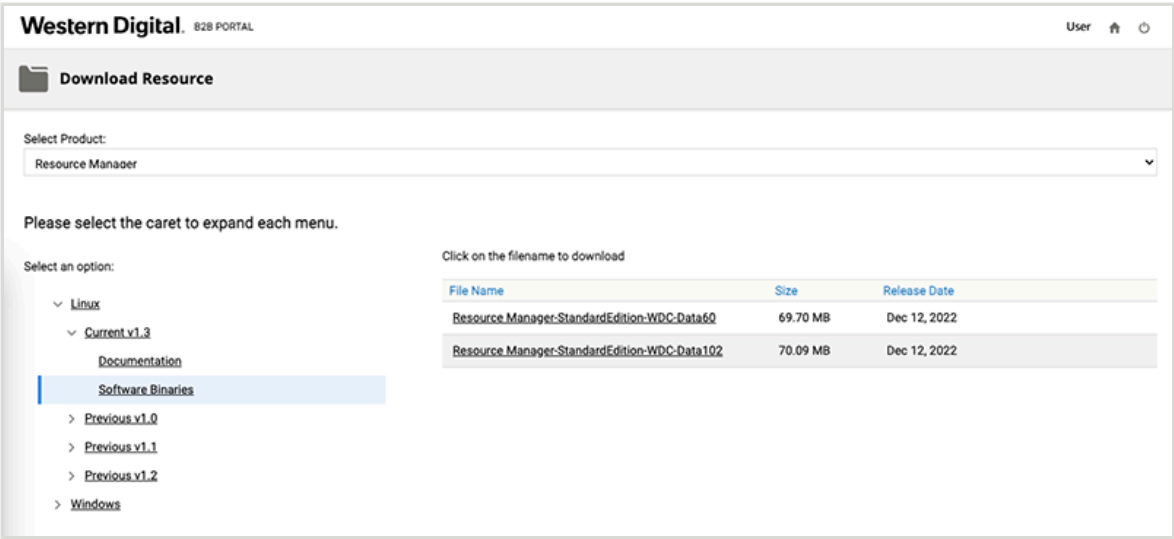
Figure 13: Operating System Selection List



- Step 5:** Under **Select an option**, use the arrows to select all of the following:
- a. Your operating system
 - b. The current version of Resource Manager Standard Edition
 - c. The **Software Binaries** option

The software binary files for supported platforms will be displayed on the right:

Figure 14: Software Binaries



- Step 6:** Click on the filename to download the binary file for your platform.

Step 7: Unzip/extract the archive file to the desired directory on the host server.

The following example shows the unzipped/extracted file structure and contents of **all** binary file options:

```
.
├── Linux
│   ├── WDC-Data102
│   │   ├── inbandmgmt.zip
│   │   ├── libstorelib.so
│   │   ├── libstorelib.so.07
│   │   ├── libstorelib.so.07.1105.0100.0000
│   │   ├── rm_ssl_debian.conf
│   │   ├── rm_ssl_fedora.conf
│   │   ├── usmd.service
│   │   ├── usm_gui.zip
│   │   ├── WDC-Data102-installer.sh
│   │   ├── WDC-Data102-uninstall.sh
│   │   ├── wdckit-raid_2.14.0.0_amd64.deb
│   │   ├── wdckit-raid-2.14.0.0.x86_64.rpm
│   │   ├── wddcs-x86_64-3.0.8.0.deb
│   │   ├── wddcs-x86_64-3.0.8.0.rpm
│   │   └── WD-ResourceManager-License.txt
│   └── WDC-Data60
│       ├── inbandmgmt.zip
│       ├── libstorelib.so
│       ├── libstorelib.so.07
│       ├── libstorelib.so.07.1105.0100.0000
│       ├── rm_ssl_debian.conf
│       ├── rm_ssl_fedora.conf
│       ├── usmd.service
│       ├── usm_gui.zip
│       ├── WDC-Data60-installer.sh
│       ├── WDC-Data60-uninstall.sh
│       ├── wdckit-raid_2.14.0.0_amd64.deb
│       ├── wdckit-raid-2.14.0.0.x86_64.rpm
│       ├── wddcs-x86_64-3.0.8.0.deb
│       ├── wddcs-x86_64-3.0.8.0.rpm
│       └── WD-ResourceManager-License.txt
└── Windows
    ├── WDC-Data102
    │   └── Resource Manager-StandardEdition-WDC-Data102.exe
    └── WDC-Data60
        └── Resource Manager-StandardEdition-WDC-Data60.exe
```

2.2 Installing Resource Manager Standard Edition for Linux

This procedure provides instructions for installing the Resource Manager Standard Edition application on a Linux operating system.

Before you begin:

- **Ensure all required software has been installed.** See [Required Software \(page 9\)](#) for details.
- Complete the instructions for [Downloading Resource Manager Standard Edition \(page 12\)](#).
- Resource Manager Standard Edition uses HTTP ports 80 and 8080 on the host operating system. If a firewall is enabled on the host, ensure that these TCP ports are open before installing the product.
- All commands in this procedure should be executed with sudo privileges.

Step 1: From a command terminal on the host server, navigate to the appropriate unzipped/extracted directory for your platform:

- Linux/WDC-Data102/
- Linux/WDC-Data60/

Step 2: Run the installation script for your platform:

- `# ./WDC-Data102-installer.sh`
- `# ./WDC-Data60-installer.sh`

Step 3: When prompted, review the end-user license agreement. Then enter `y` to accept it:

```
Do you agree All License Agreement Terms and Conditions?(y/n)y
```

The installation script will check for pre-requisites and update or install as needed, along with installing the Resource Manager Standard Edition. You will then be prompted for a Web Server port number:

```
Pre-requisites check start for Western Digital Resource Manager.
Python version 3.8.12 is already installed. Requirement satisfied.
sg_utils version 2.07 is already installed. Requirement satisfied.
Flask version 2.2.2 is already installed. Requirement satisfied.
Pre-requisites check end for Western Digital Resource Manager.
Verifying... ##### [100%]
Preparing... ##### [100%]
Updating / installing...
  1:wddcs-3.0.8.0-1 ##### [100%]
Verifying... ##### [100%]
Preparing... ##### [100%]
Updating / installing...
  1:wdckit-raid-2.14.0.0-1 ##### [100%]
Please enter custom Web Server port number or press ENTER to continue with
default 8080 :
```



Note: The output text in your terminal may differ from this example.

2.2 Installing Resource Manager Standard Edition for Linux

Step 4: As prompted, either enter a custom port number for the Web Server, or press `ENTER` to continue with the default port of 8080.

You will then be prompted for a Resource Manager Service port number:

```
Please enter custom Resource Manager Service port number or press ENTER to
continue with default 8081 :
```

Step 5: As prompted, either enter a custom port number for the Resource Manager Service, or press `ENTER` to continue with the default port of 8081.

You will be notified that the installation is now complete:

```
Installation completed.
```

Step 6: After the installation is finished, use the `systemctl` command with the `status` option to check the status of the web server and verify that the application is running:

```
# systemctl status usmd
usmd.service - Western Digital Resource Manager Web Application HTTP server
(running in port 8080)
   Loaded: loaded (/etc/systemd/system/usmd.service; static; vendor preset:
   enabled)
   Active: active (running) since Thu 2020-12-31 11:28:26 IST; 1h 18min ago
 Main PID: 35459 (python3)
    Tasks: 7 (limit: 7372)
   CGroup: /system.slice/usmd.service
           |-- 2650 /bin/sh -c wdds /dev/sg2 show handles
           |-- 2651 wddcs /dev/sg2 show handles
           |--19819 /usr/bin/python3 /opt/usm/inbandmgmt/middleware/main.py
```

Result: The Resource Manager Standard Edition application is now installed.

What to do next: Proceed to [Accessing Resource Manager Standard Edition \(page 30\)](#).

2.3 Installing Resource Manager Standard Edition for Windows

This procedure provides instructions for installing Resource Manager Standard Edition on a Windows operating system.

Before you begin:

- **Ensure all required software has been installed.** See [Required Software \(page 9\)](#) for details.
- Complete the instructions for [Downloading Resource Manager Standard Edition \(page 12\)](#).
- Resource Manager Standard Edition uses HTTP ports 80 and 8080 on the host operating system. If a firewall is enabled on the host, ensure that these TCP ports are open before installing the product.

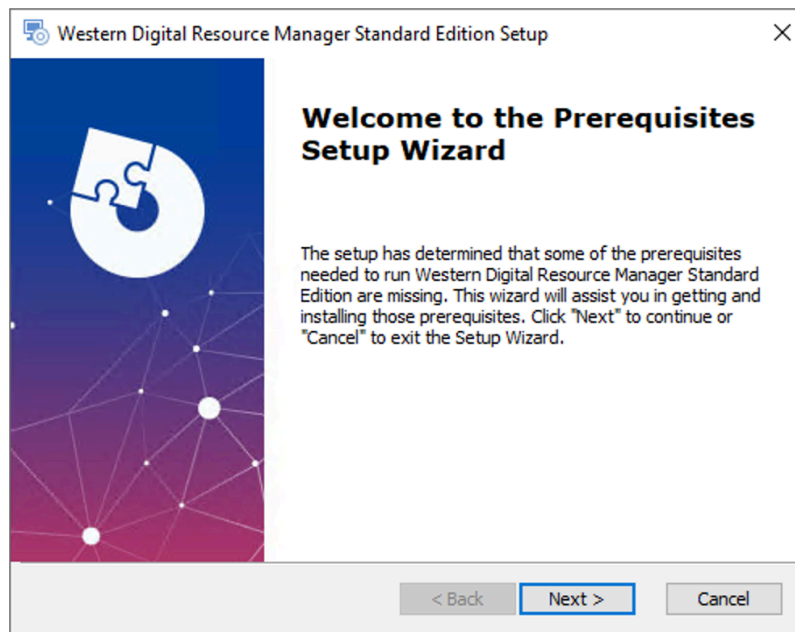
Step 1: On the host server, navigate to the appropriate unzipped/extracted directory for your platform:

- Windows\WDC-Data102\
- Windows\WDC-Data60\

Step 2: Run the Resource Manager Standard Edition application file for your platform:

- Resource Manager-StandardEdition-WDC-Data102.exe
- Resource Manager-StandardEdition-WDC-Data60.exe

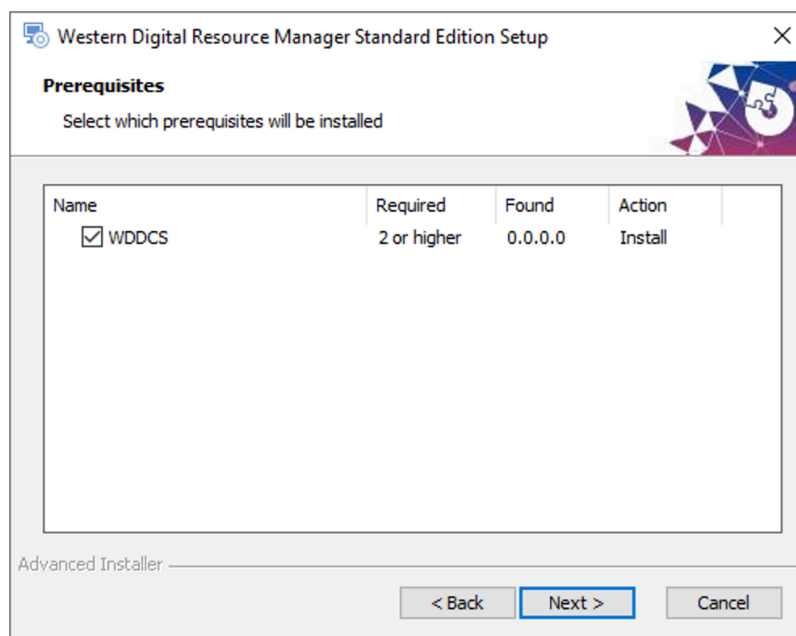
This will launch the Resource Manager Standard Edition setup wizard. The setup wizard will check for installed prerequisite WD software and lead the user through one of three different paths, depending on what it finds.



Step 3: Click **Next >**.

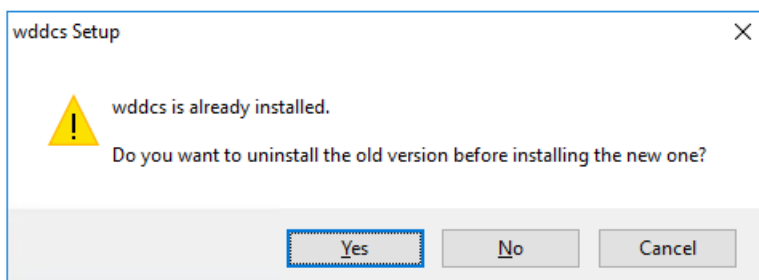
The **Prerequisites** window will be displayed, listing the required software and version, the version currently installed (if applicable), and the required action:

2.3 Installing Resource Manager Standard Edition for Windows



- **Path 1:** If a current version of the WDDCS Tool is installed, click to remove the checkmark next to **WDDCS**. Then click **Next >**. The Resource Manager Standard Edition setup wizard will be displayed to begin the installation process. Proceed to [Installing Resource Manager Standard Edition \(page 26\)](#) for further instructions.
- **Path 2:** If the WDDCS Tool is not installed, click **Next >**. The **wddcs Setup** wizard will be launched to install the current version. Proceed to [Installing the WDDCS Tool \(page 23\)](#) for further instructions.
- **Path 3:** If an old version of the WDDCS Tool is installed, click **Next >**. The **wddcs Setup** wizard will be launched to uninstall the old version and install the current version. Proceed to [Uninstalling the WDDCS Tool \(page 19\)](#) for further instructions.

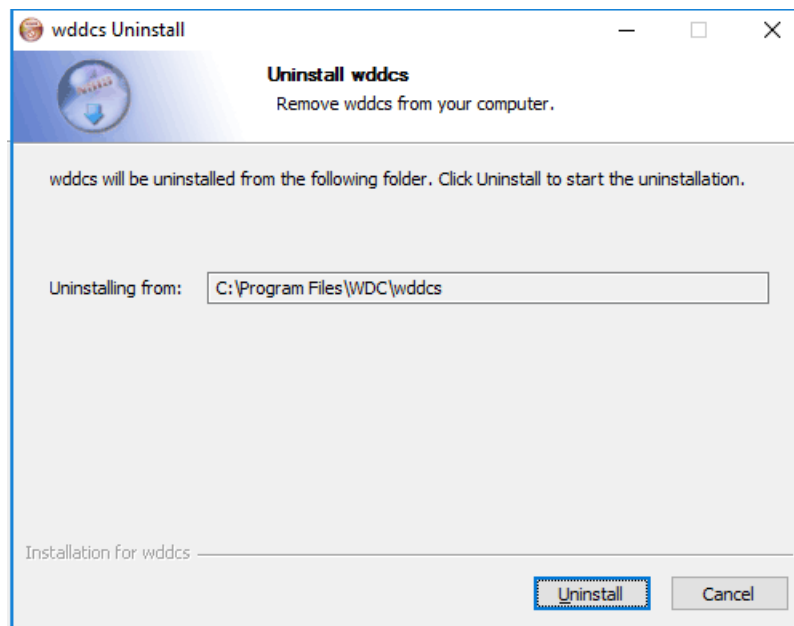
Uninstalling the WDDCS Tool



Step 4: Click **Yes** to confirm the uninstallation.

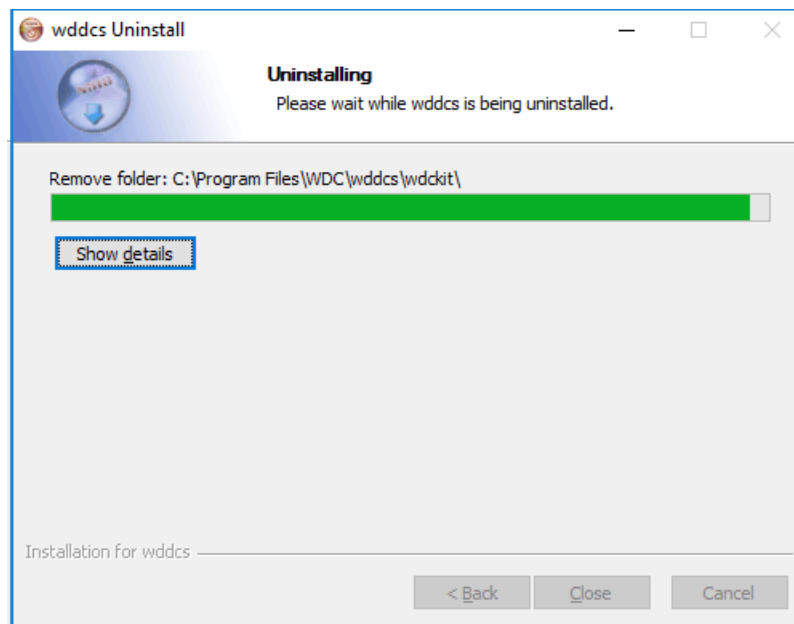
The **Uninstall wddcs** window will be displayed, showing from which directory the old version will be uninstalled.

2.3 Installing Resource Manager Standard Edition for Windows



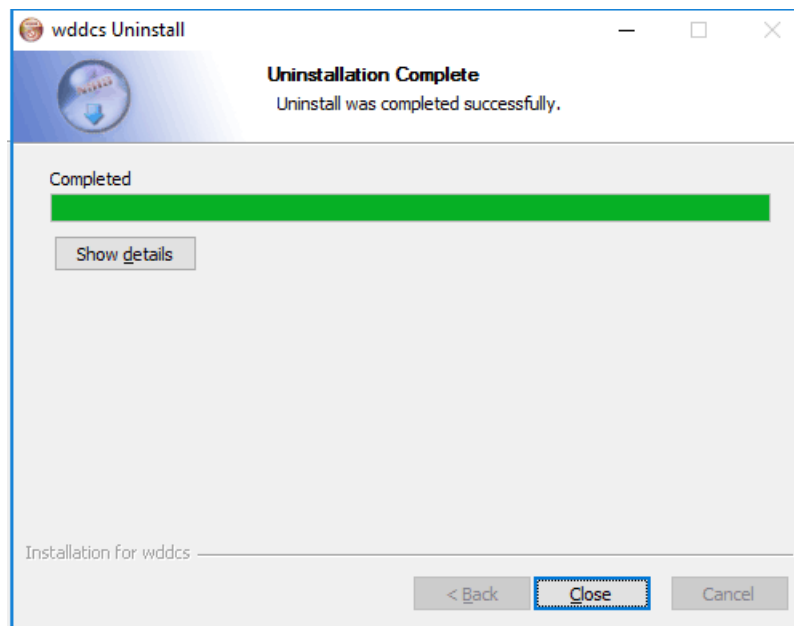
Step 5: Click **Uninstall**.

The **wddcs Uninstall** window will update, showing that the WDDCS Tool is being uninstalled:



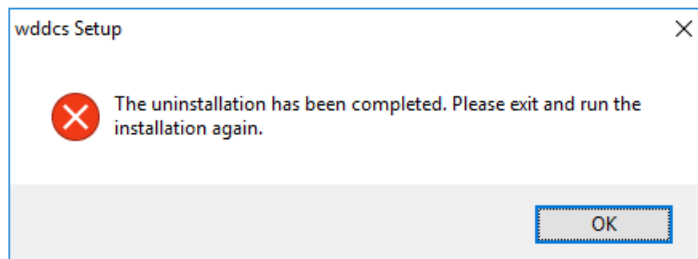
After a few seconds, the **wddcs Uninstall** window will update again, showing that the uninstallation is complete:

2.3 Installing Resource Manager Standard Edition for Windows



Step 6: Click **Close**.

The **wddcs Setup** window will reappear, prompting the user to exit and run the installation again:



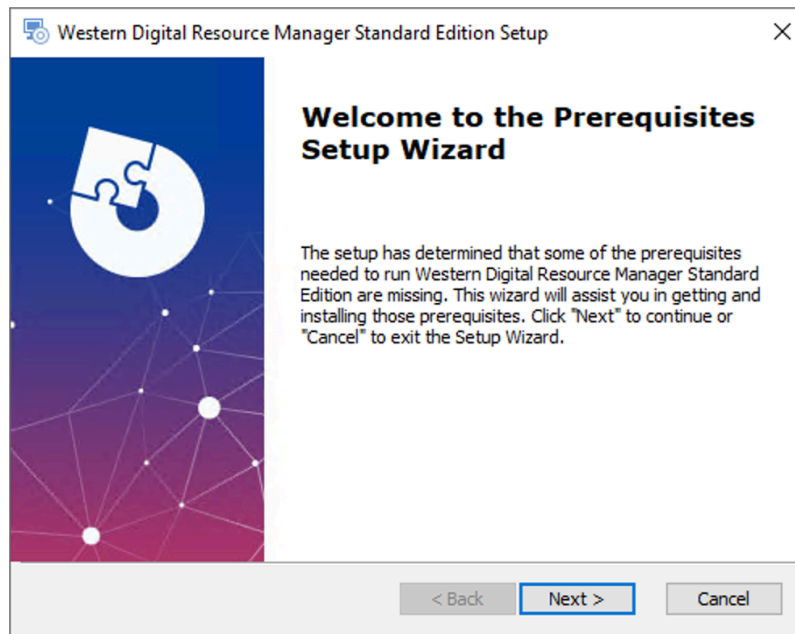
Step 7: Click **OK** to exit the **wddcs Setup** window.

Step 8: Close all setup windows for the Resource Manager Standard Edition.

Step 9: Reopen the Resource Manager Standard Edition application (.exe) file again.

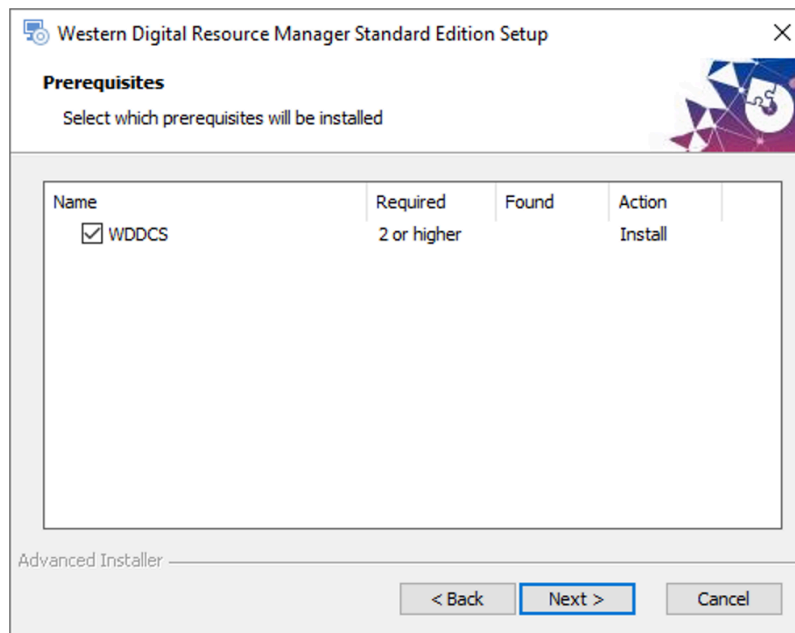
The welcome prerequisites window will be displayed:

2.3 Installing Resource Manager Standard Edition for Windows



Step 10: Click **Next >**.

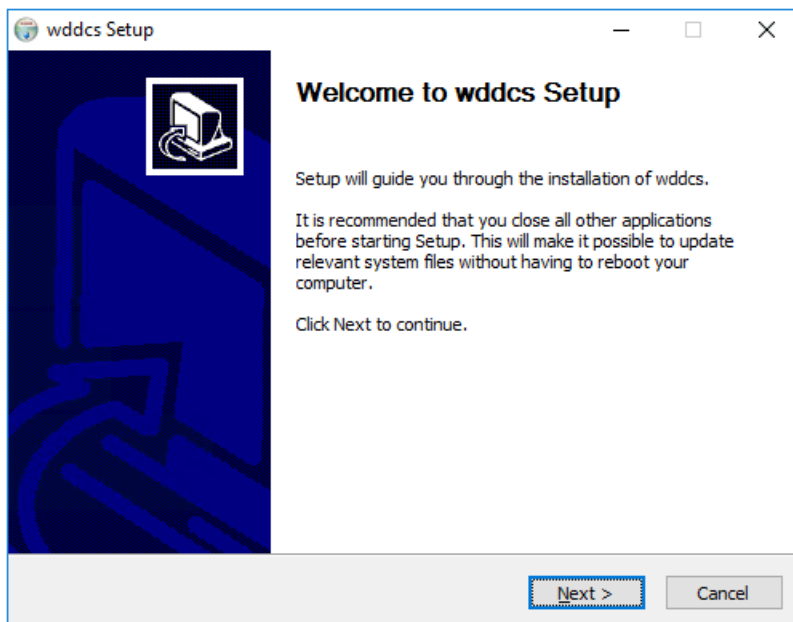
The **Prerequisites** window will update, showing the required version of the WDDCS Tool to be installed:



Step 11: Click **Next >**.

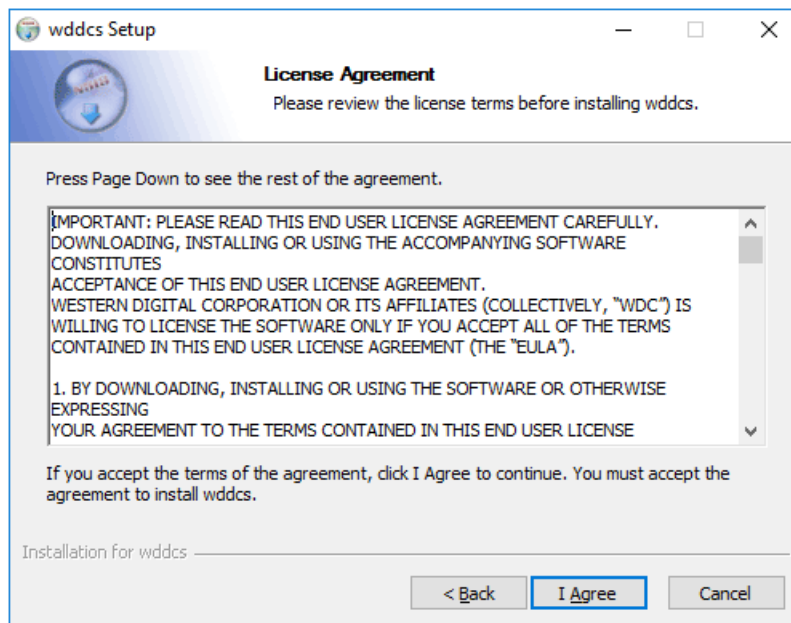
The **wddcs Setup** wizard will be launched.

Installing the WDDCS Tool



Step 12: Click **Next >**.

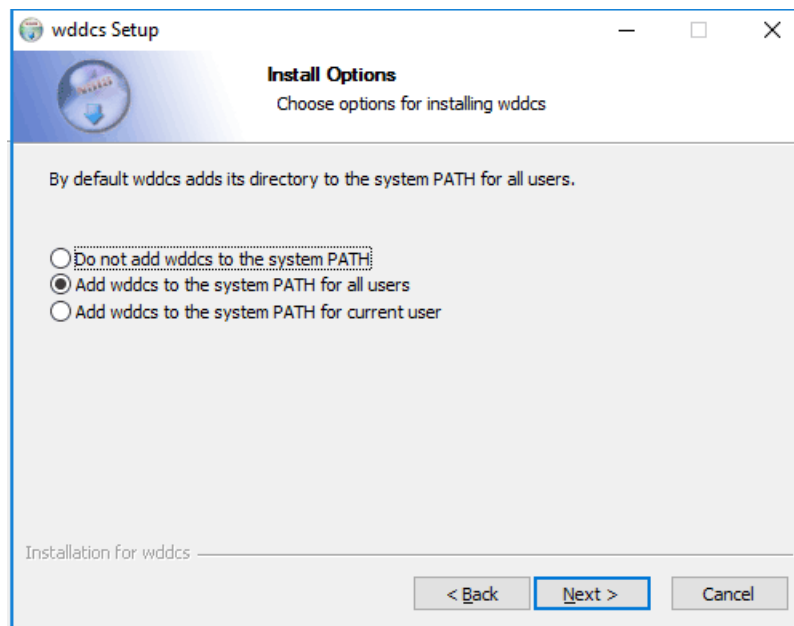
The **wddcs Setup** window will update, showing the WDDCS Tool **License Agreement**:



Step 13: Read through the license agreement and click **I Agree**.

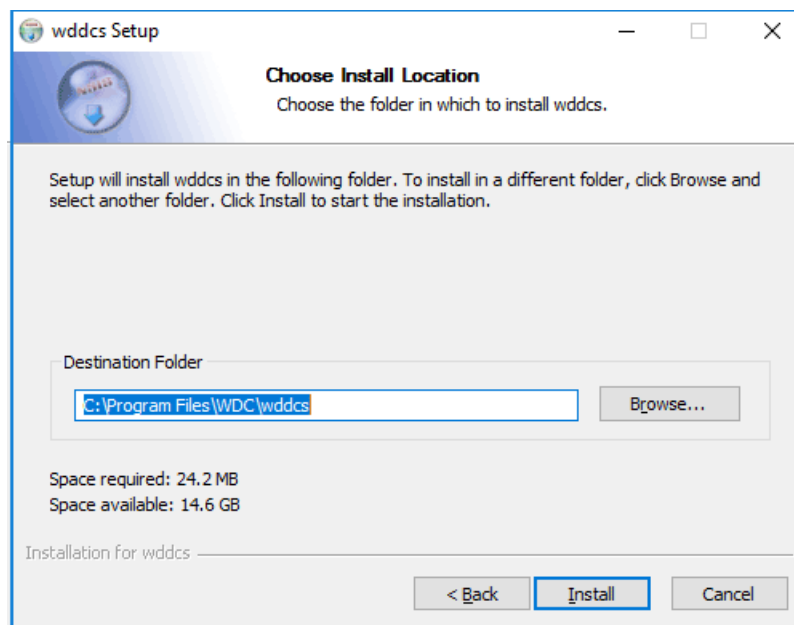
The **wddcs Setup** window will update, prompting the user to choose a system PATH option. The **Add wddcs to the system PATH for all users** option is selected by default:

2.3 Installing Resource Manager Standard Edition for Windows



Step 14 : Click **Next >**.

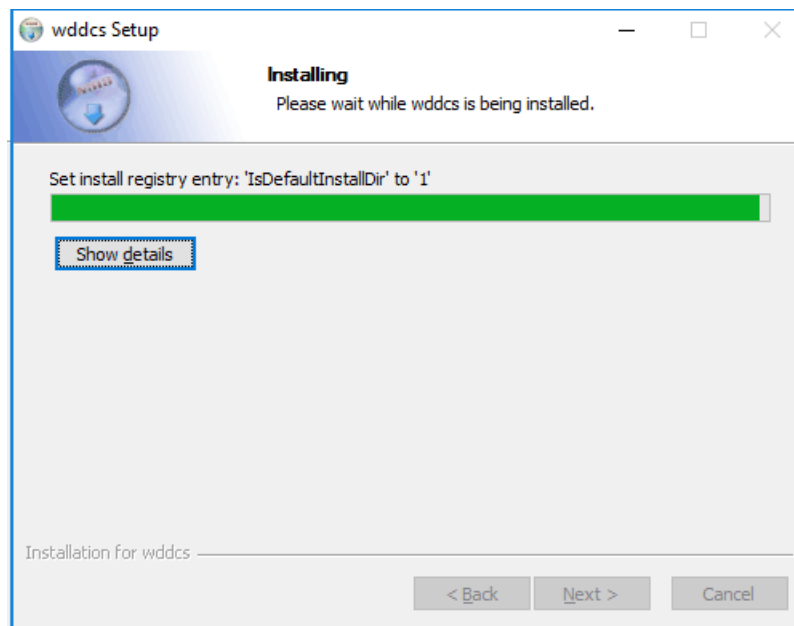
The **wddcs Setup** window will update, prompting the user to accept the default installation directory or choose another:



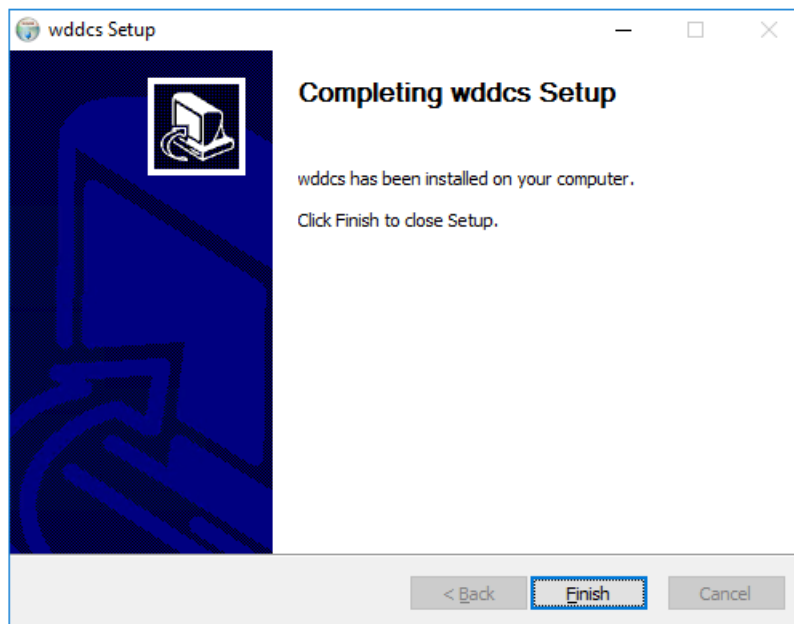
Step 15 : Click **Install**.

The **wddcs Setup** window will update, showing the installation progress:

2.3 Installing Resource Manager Standard Edition for Windows



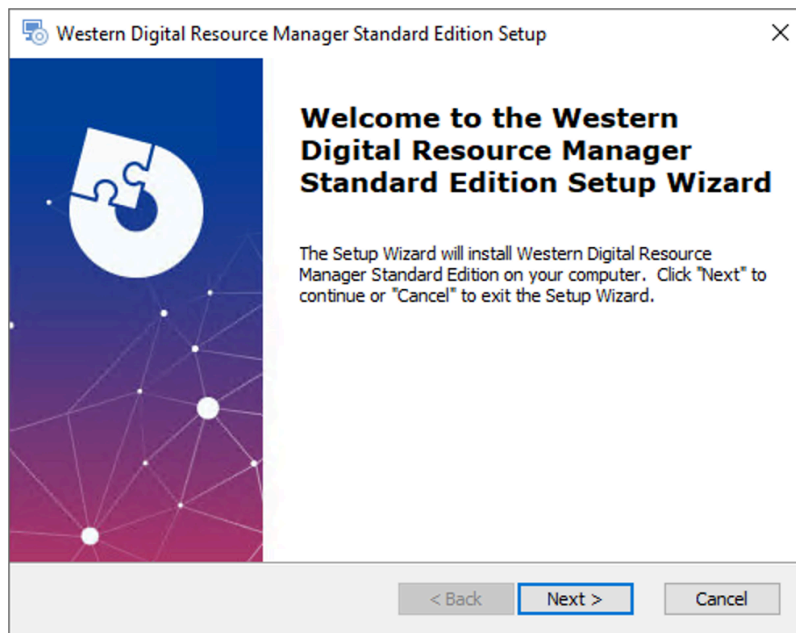
After a few seconds, the **wddcs Setup** window will update again, showing that the installation is complete:



Step 16: Click **Finish**.

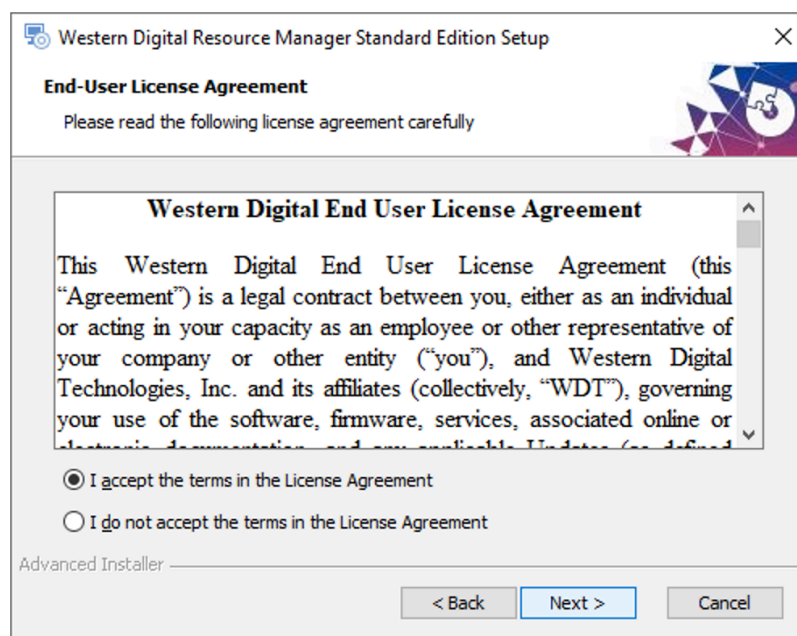
The Resource Manager Standard Edition setup wizard will be displayed again.

Installing Resource Manager Standard Edition



Step 17: Click **Next >**.

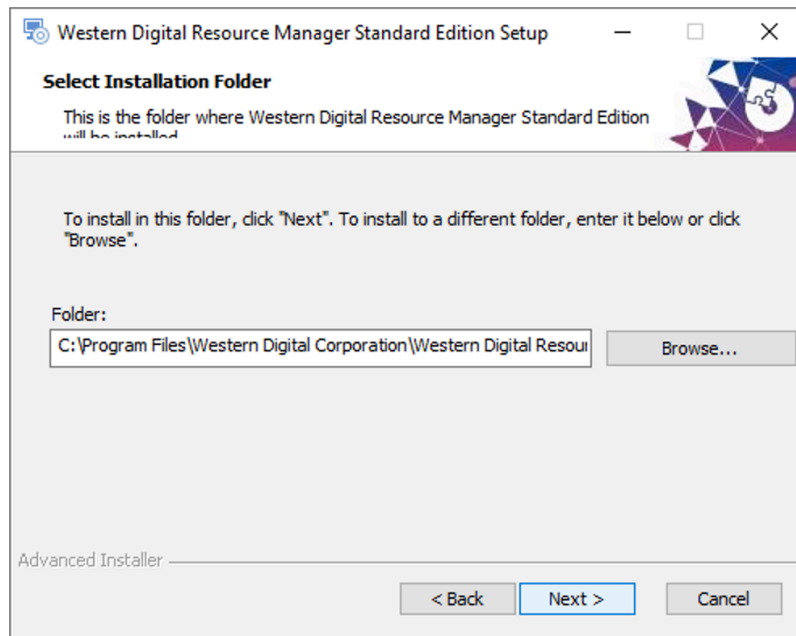
The Resource Manager Standard Edition **End-User License Agreement** window will be displayed.



Step 18: Read through the end-user license agreement, click the radio button for **I accept the terms in the License Agreement**, and click **Next >**.

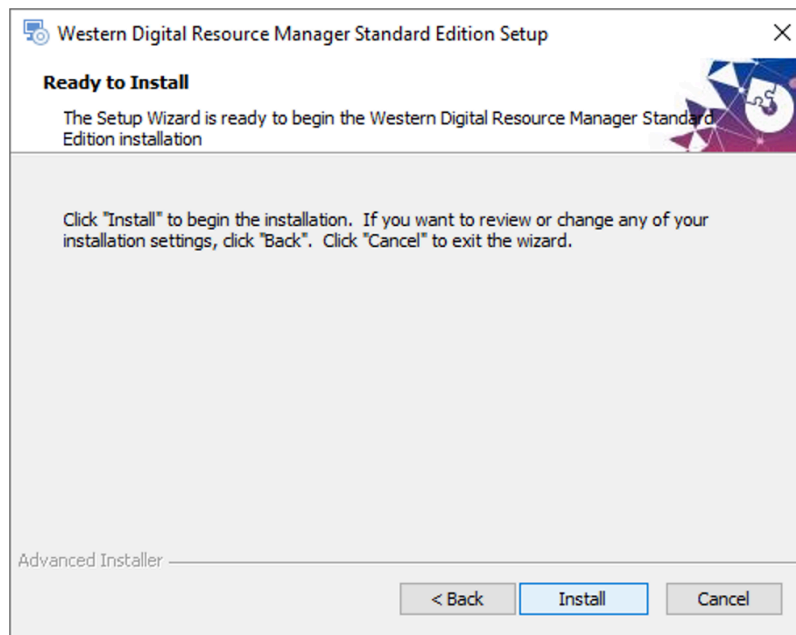
The **Select Installation Folder** window will be displayed:

2.3 Installing Resource Manager Standard Edition for Windows



Step 19: Either keep the default installation folder or click **Browse...** to select a different installation folder. Then click **Next >**.

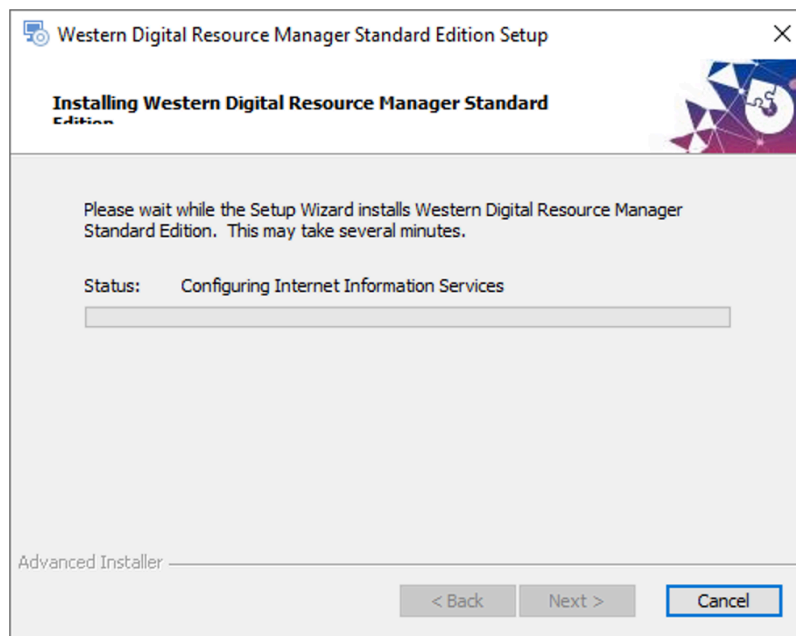
The **Ready To Install** window will be displayed:



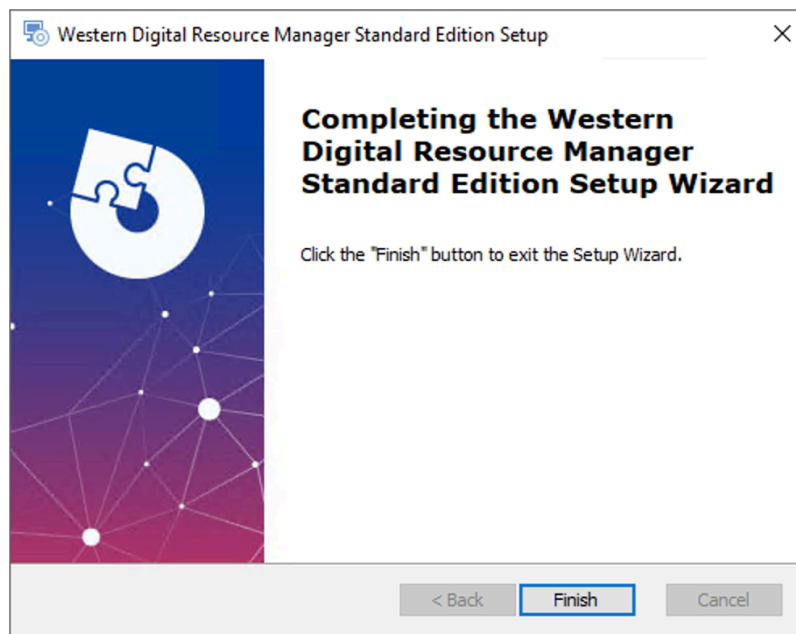
Step 20: Click **Install**.

The **Installing Western Digital Resource Manager Standard Edition** window will be displayed, showing the status of the installation:

2.3 Installing Resource Manager Standard Edition for Windows



When the installation is complete, the setup wizard will proceed to a completion window:



Step 21: Click **Finish** to exit the setup wizard.

Result: The Resource Manager Standard Edition application is now installed.

What to do next: Proceed to [Accessing Resource Manager Standard Edition \(page 30\)](#).



Management

In This Chapter:

- Accessing Resource Manager Standard Edition..... 30
- Dashboard..... 34
- Virtual View..... 39
- Devices..... 51
- MegaRAID..... 115
- Alerts..... 184
- Settings..... 190
- Virtual Tour..... 203

3.1 Accessing Resource Manager Standard Edition

This procedure provides instructions for logging in to the Resource Manager Standard Edition application.

Step 1: Open a browser and navigate to the appropriate address for the host operating system:

- For Linux – `https://<server_ip>/#/`
- For Windows – `https://<server_ip>/unifiedapp/`



Note: Replace `<server_ip>` with the IP address of the server hosting the Resource Manager Standard Edition software.

The login page will appear:

Figure 36: Login Page

Western Digital

WESTERN DIGITAL RESOURCE MANAGER – STANDARD

Sign In

User ID

Enter User ID

Password

Enter Password

☐ Show Password

Sign In

Western Digital Resource Manager – Standard.

Monitoring and Management Capabilities for Western Digital platforms.

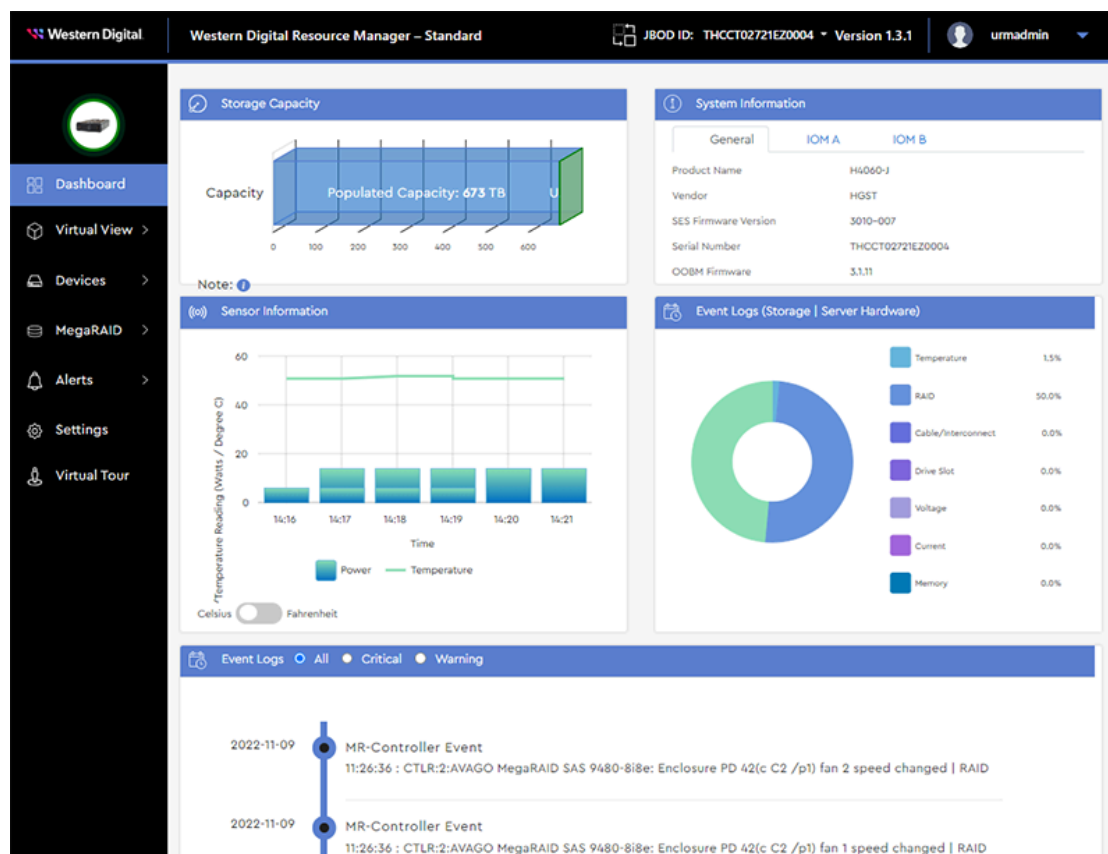
Step 2: Enter a valid username and password into the **User ID** and **Password** fields. Then click the **Sign In** button.



Note: The default username/password is urmadmin/admin@123.

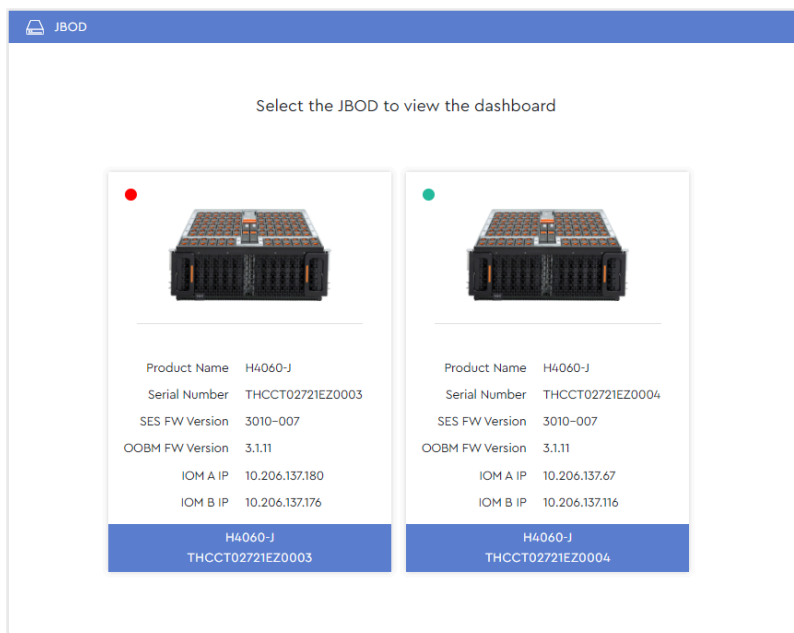
- a. If the host server is connected to a **single** enclosure, that enclosure's dashboard will appear:

Figure 37: Enclosure Dashboard



- b. If the host server is connected to **multiple** enclosures, the **JBOD** selection page will appear:

Figure 38: JBOD Selection Page



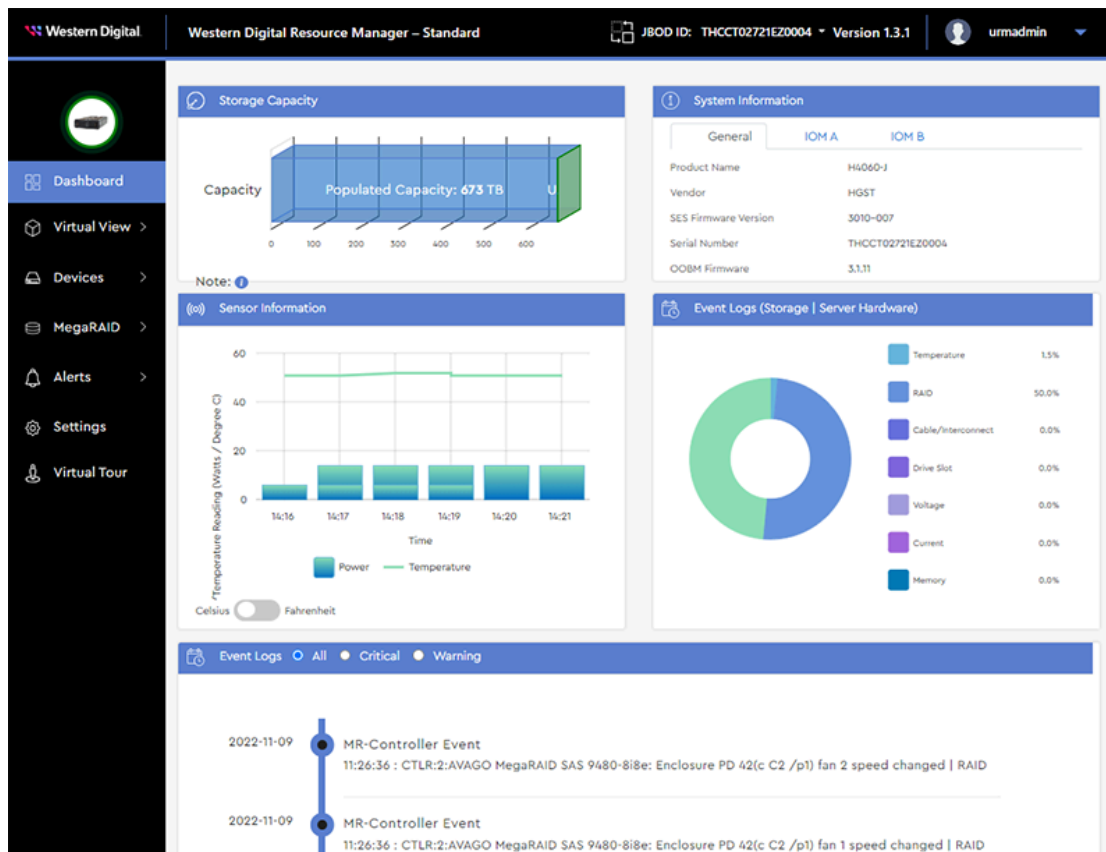
Note: The colored dot in the upper-left corner of each JBOD section indicates the health of the enclosure. The dot will also provide a tooltip explanation of the health status when hovered over:

- **Green** – OK
- **Amber** – WARNING
- **Red** – CRITICAL

- c. Click to select the desired enclosure from the available options. Then click the **Go to Dashboard** button.

That enclosure's dashboard will appear:

Figure 39: Enclosure Dashboard

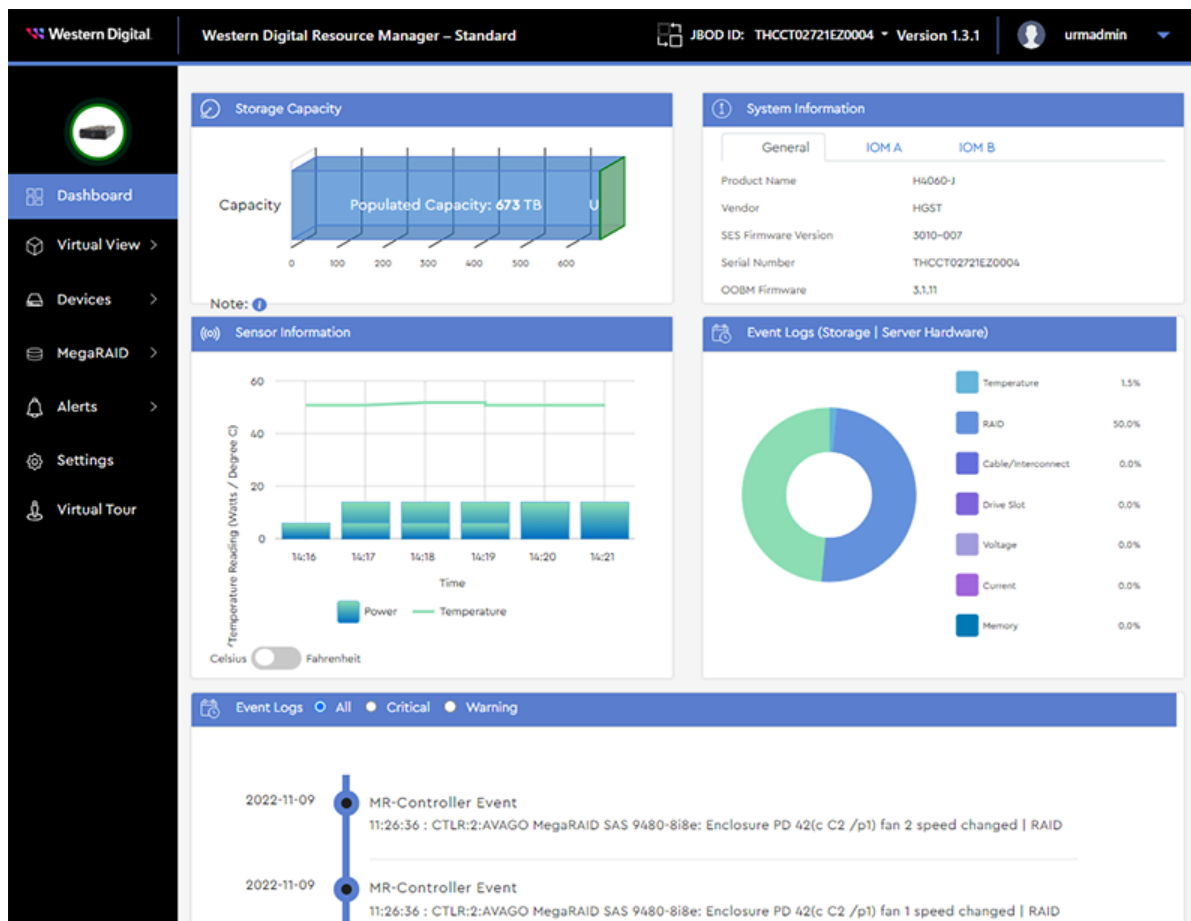


Result: You are now logged in to the desired enclosure using the Resource Manager Standard Edition application.

What to do next: Proceed with management of the enclosure.

3.2 Dashboard

The **Dashboard** is a consolidated monitoring page displaying the most critical enclosure data, such as populated/unpopulated storage capacity, system information (serial number, SEP & OOBM FW versions), IOM information (MAC & IP addresses), and the last 10 minutes of sensor readings (refreshed approximately every 60 seconds). Events are displayed in a categorized pie chart as well as a chronological list, filterable by severity.



Note: If the enclosure is connected to a non-RAID HBA, the **Storage Capacity** section displays unpopulated capacity based on the highest capacity drive model supported by the platform, while populated capacity is based on the capacity of the drives installed. For example, the Ultrastar Data60 supports up to sixty (60) 20TB drives¹, for a total of 1200TB of unpopulated capacity. If thirty (30) slots are populated with 20TB drives, the populated capacity would be 600TB, and the unpopulated capacity would also be 600TB. Hovering over the graph will produce a tooltip that shows the number of populated and unpopulated drive slots.

1. One terabyte (TB) is equal to one trillion bytes. Actual user capacity may be less due to operating environment.



Note: For non-RAID HBAs, the controller firmware doesn't report raw capacity. The Resource Manager Standard Edition calculation is based on data received from StorLIB.



Note: If the enclosure is connected to a MegaRAID controller, the populated capacity will be the total capacity of all Logical Drives; unpopulated capacity will be the remaining Physical Drives capacity available for configuring a RAID.

3.2.1 Switching Enclosures Using Drop-Down List

When the host server is connected to multiple enclosures, selecting a specific enclosure can be accomplished during or after login. This procedure provides instructions for selecting a different enclosure after login, using the drop-down list.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

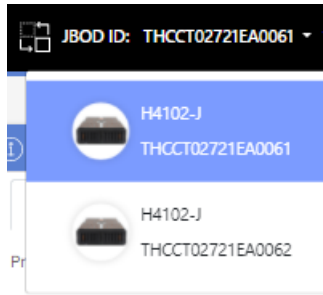
Step 1: At the top of the dashboard, click the drop-down list next to the current enclosure's ID:

Figure 41: Enclosure ID Drop-Down List



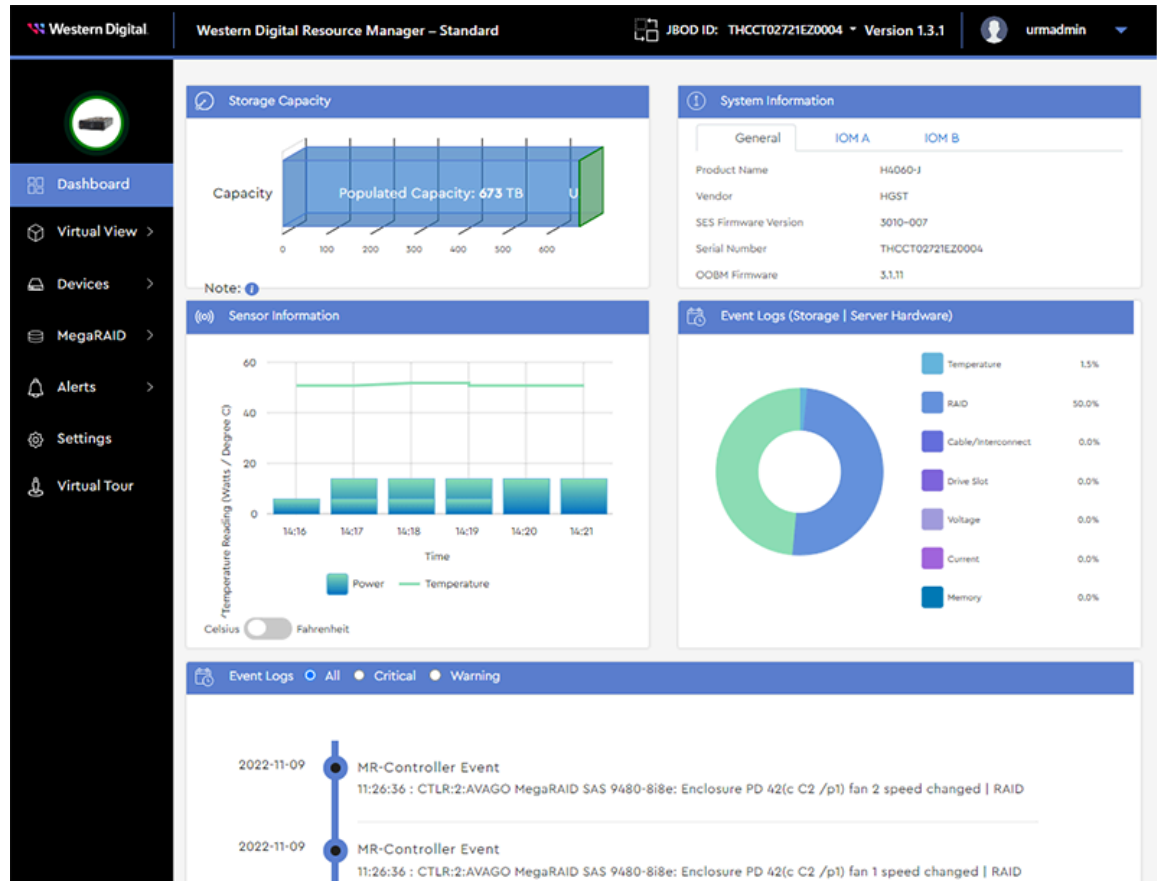
The enclosures attached to the host will be presented in a list format, with the currently-selected enclosure highlighted:

Figure 42: Enclosure Options



Step 2: Click to select another enclosure from the list. That enclosure's dashboard will appear:

Figure 43: Other Enclosure's Dashboard



Result: A different enclosure has now been selected using the drop-down list.

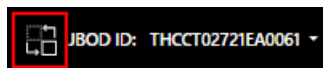
3.2.2 Switching Enclosures Using Icon

When the host server is connected to multiple enclosures, selecting a specific enclosure can be done during or after login. This procedure provides instructions for selecting a different enclosure after login using the change-enclosure icon.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

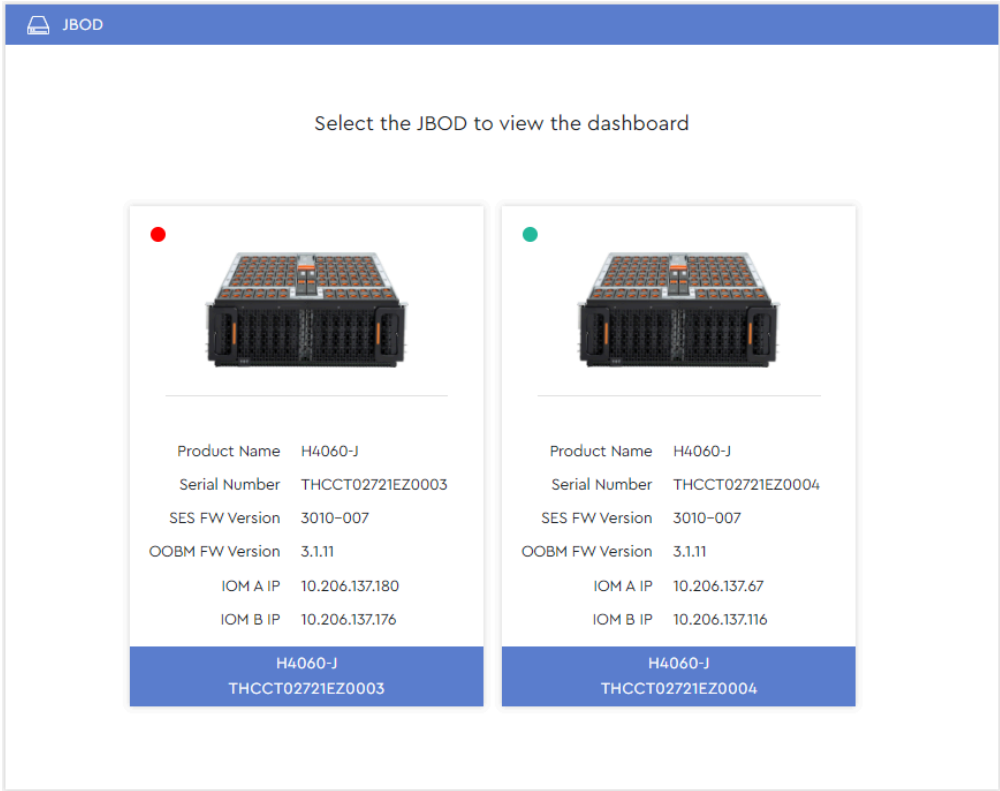
Step 1: At the top of the dashboard, click the change-enclosure icon:

Figure 44: Change-Enclosure Icon



The JBOD selection page will appear (the same one used during login):

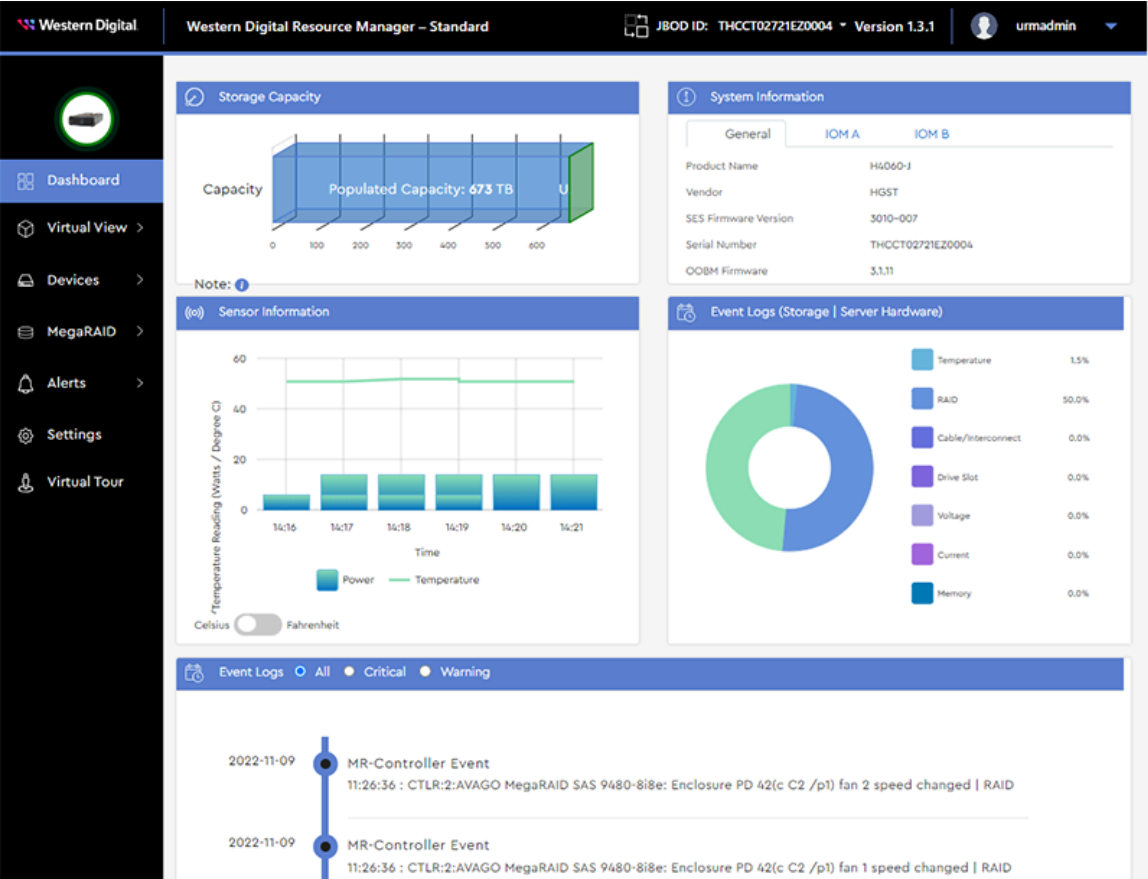
Figure 45: JBOD Selection Page



Step 2: Click to select a different enclosure from the available options. Then click the **Go to Dashboard** button.

That enclosure's dashboard will appear:

Figure 46: Other Enclosure's Dashboard



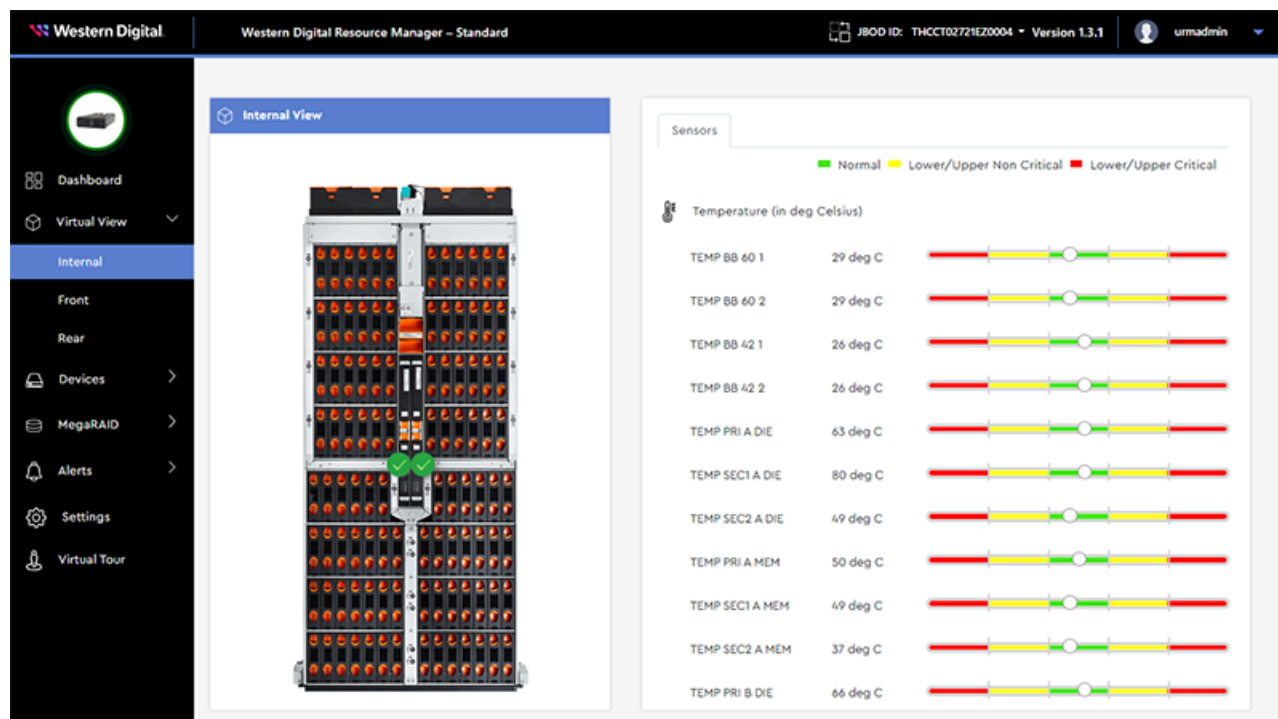
Result: A different enclosure has now been selected using the change-enclosure icon.

3.3 Virtual View

The **Virtual View** section provides real-time health status and sensor information for the components visible or accessible from different perspectives, such as drives, system fans, IOMs, and PSUs. Front and rear views also provide enclosure LED management controls.

3.3.1 Internal View

The **Internal View** displays IOM health status and temperature readings of baseboard and expander sensors.

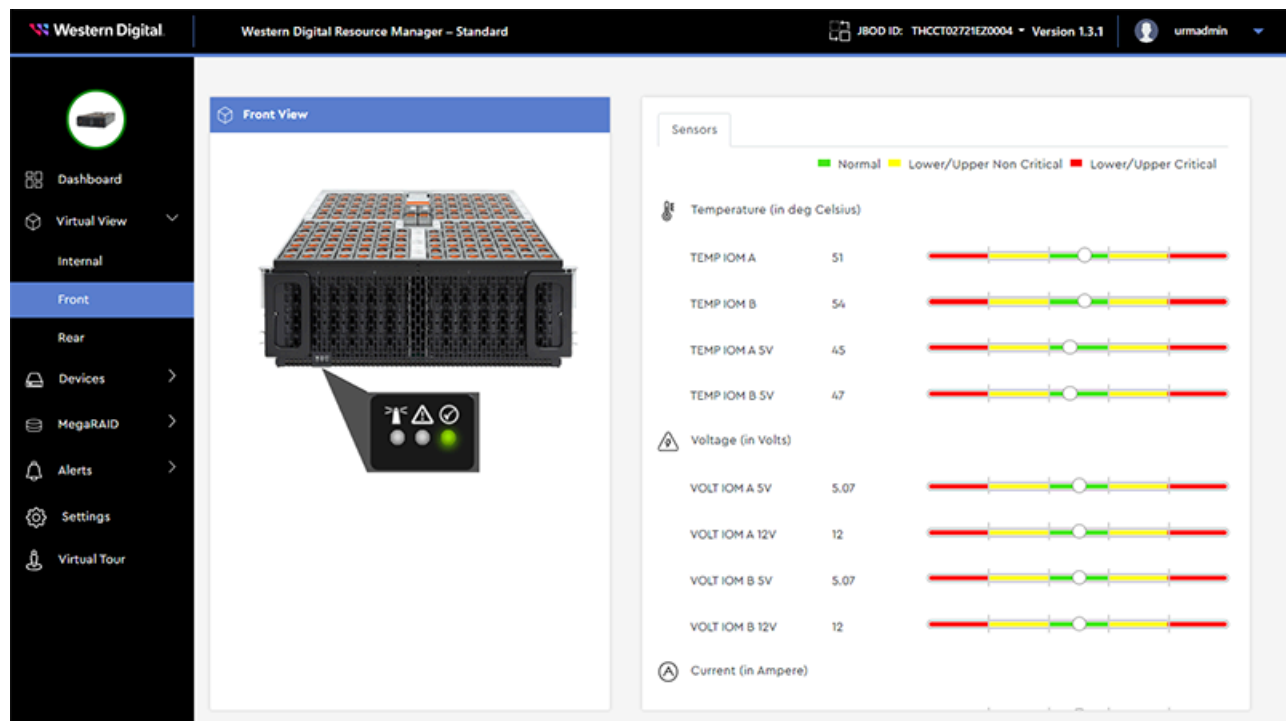


3.3.2 Front View

The **Front View** displays the temperature, voltage, and current readings of IOM sensors, as well as enclosure identification, fault, and power status LEDs.



Note: The enclosure identification LED image also functions as a control; it can be used to toggle on/off the enclosure's physical identification LED.



3.3.2.1 Enabling / Disabling Enclosure Identification LEDs (Front)

This procedure provides instructions for enabling (illuminating) and/or disabling the enclosure's identification LEDs from the **Front** virtual view page.

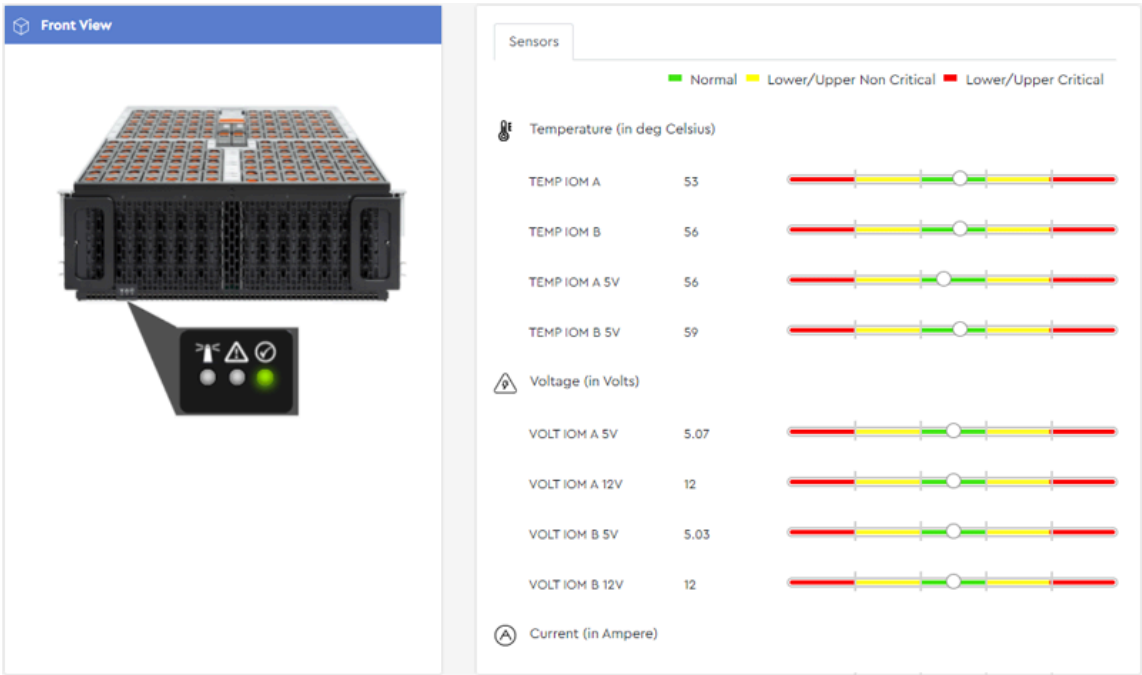
Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Enabling the Enclosure's Identification LEDs

Step 1: From the navigation bar, select **Virtual View** > **Front**.

The **Front** virtual view page will be displayed:

Figure 49: Front View



Step 2: The **Front View** image on the left will display the status of the enclosure's Identification, Fault, and Power LEDs.

Figure 50: Front View LEDs



Step 3: Hovering your cursor over the Identification LED will produce a tooltip, indicating its current status and that it can be clicked to enable the LED.

Figure 51: Identification LED Tooltip



Step 4: As instructed, click the Identification LED.

The blue LED will illuminate to show that the physical enclosure LEDs (both front and rear) have been enabled.

Figure 52: Identification LEDs Enabled



Disabling the Enclosure's Identification LEDs

Step 5: Click the blue Identification LED to disable it.

The LED will turn off to show that the physical enclosure LEDs (front and rear) have been disabled.

Figure 53: Identification LEDs Disabled



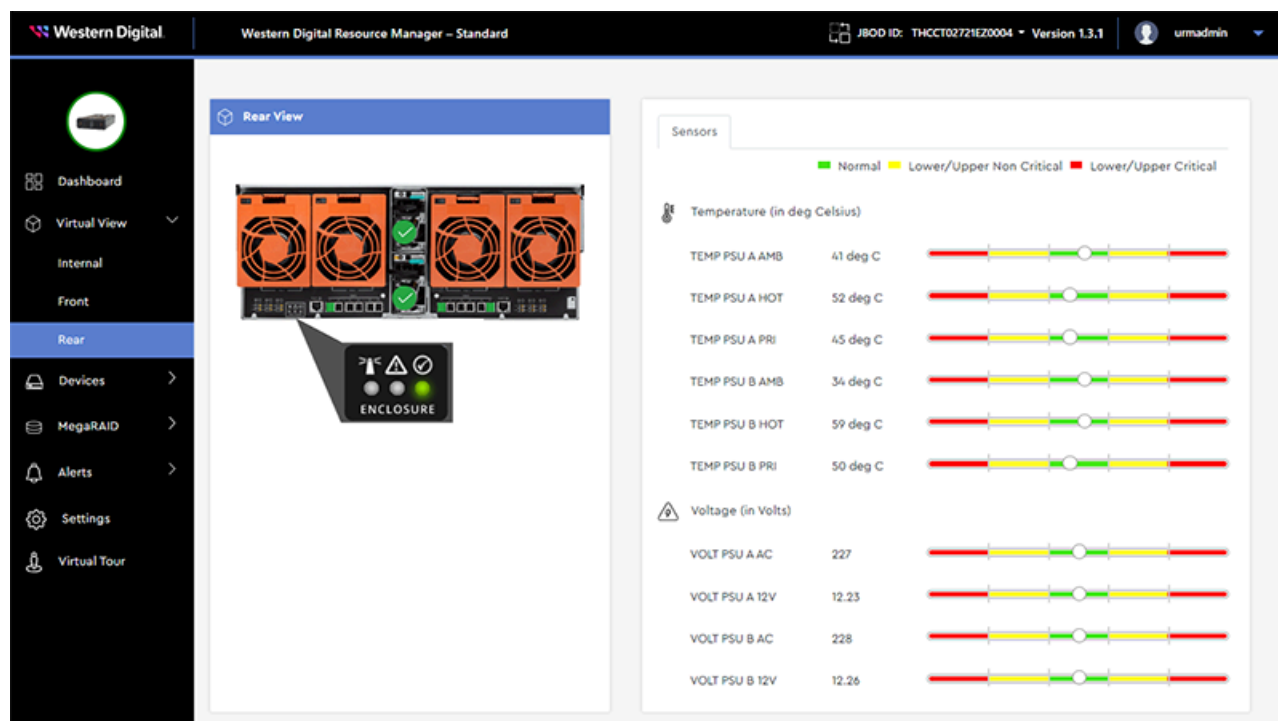
Result: The enclosure's identification LEDs have now been enabled and/or disabled.

3.3.3 Rear View

The **Rear View** displays PSU health status and temperature, voltage, and current readings of PSU sensors, as well as enclosure identification, fault, and power status LEDs.



Note: The enclosure identification LED image also functions as a control; it can be used to toggle on/off the enclosure's physical identification LED.



3.3.3.1 Enabling / Disabling Enclosure Identification LEDs (Rear)

This procedure provides instructions for enabling (illuminating) and/or disabling the enclosure's identification LEDs from the **Rear** virtual view page.

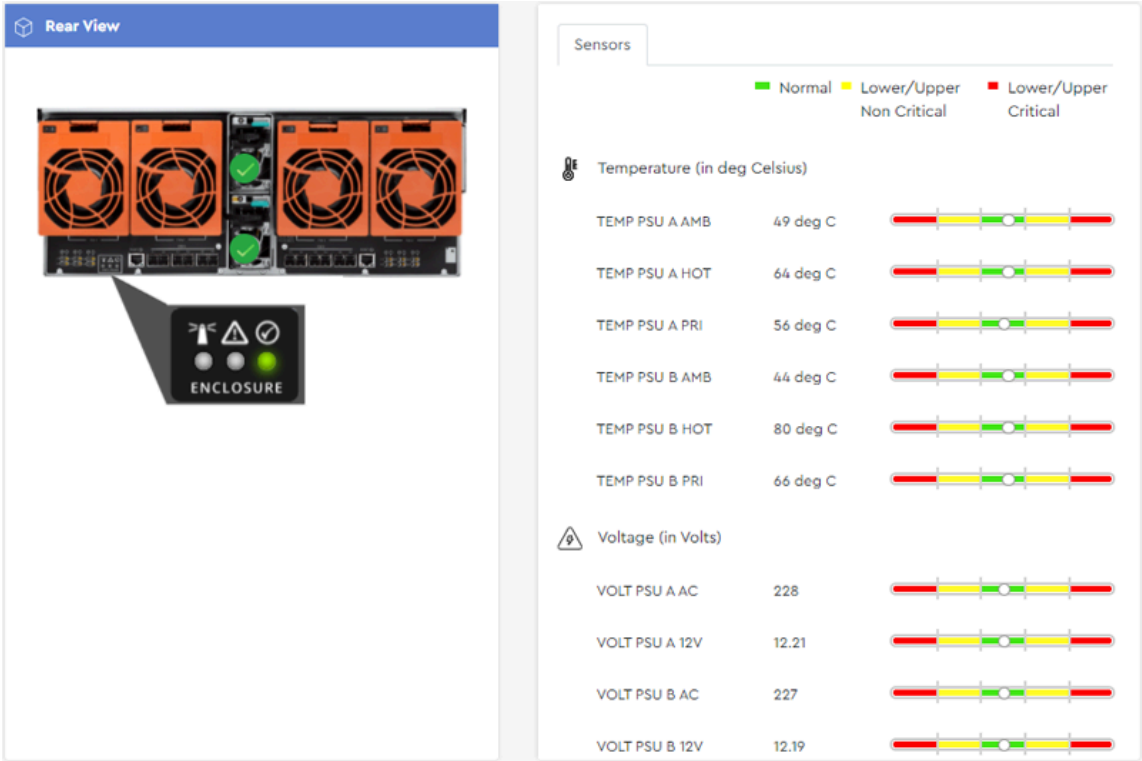
Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Enabling the Enclosure's Identification LEDs

Step 1: From the navigation bar, select **Virtual View** > **Rear**.

The **Rear** virtual view page will be displayed:

Figure 55: Rear View



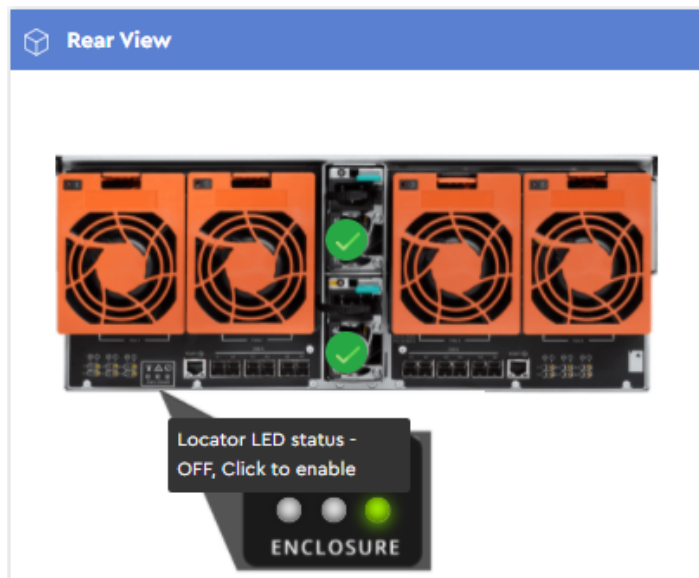
Step 2: The **Rear View** image on the left will display the status of the enclosure's Identification, Fault, and Power LEDs.

Figure 56: Rear View LEDs



Step 3: Hovering your cursor over the Identification LED will produce a tooltip, indicating its current status and that it can be clicked to enable the LED.

Figure 57: Identification LED Tooltip



Step 4: As instructed, click the Identification LED.

The blue LED will illuminate to show that the physical enclosure LEDs (both front and rear) have been enabled.

Figure 58: Identification LEDs Enabled



Disabling the Enclosure's Identification LEDs

Step 5: Click the blue Identification LED to disable it.

The LED will turn off to show that the physical enclosure LEDs (front and rear) have been disabled.

Figure 59: Identification LEDs Disabled



Result: The enclosure's identification LEDs have now been enabled and/or disabled.

3.3.3.2 Checking Cable Information (Rear)

This procedure provides instructions for checking summary information about attached cables from the **Rear** virtual view page.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

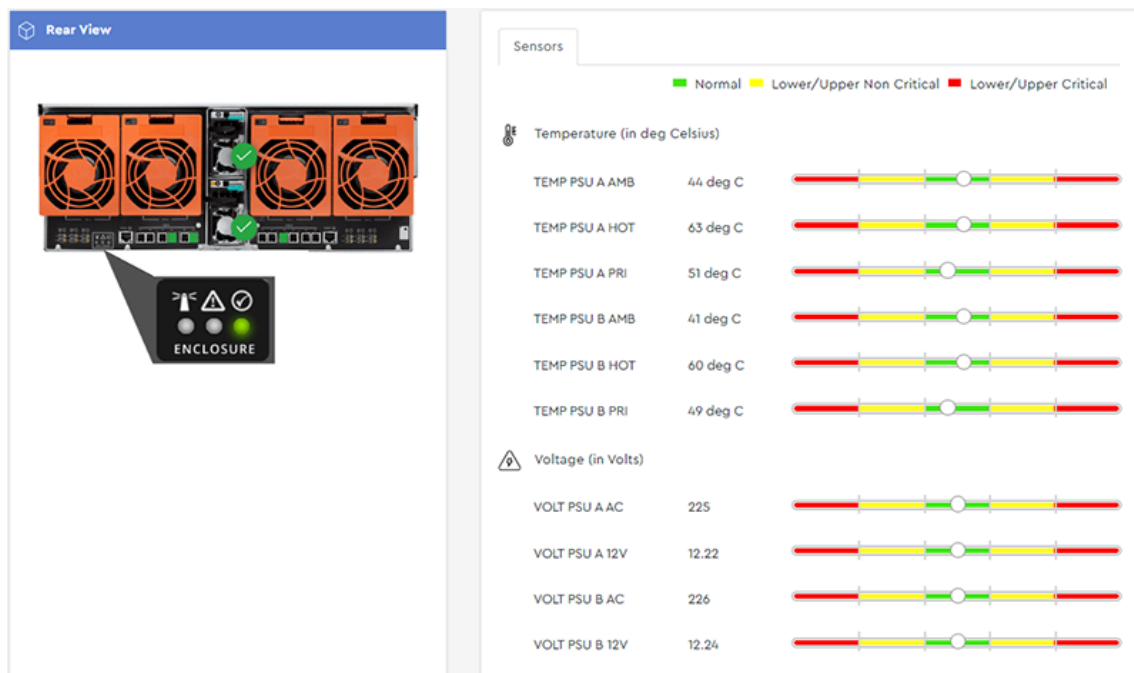


Note: To view detailed information about attached cables, see [Checking Cable Information \(IOM\) \(page 107\)](#).

Step 1: From the navigation bar, select **Virtual View > Rear**.

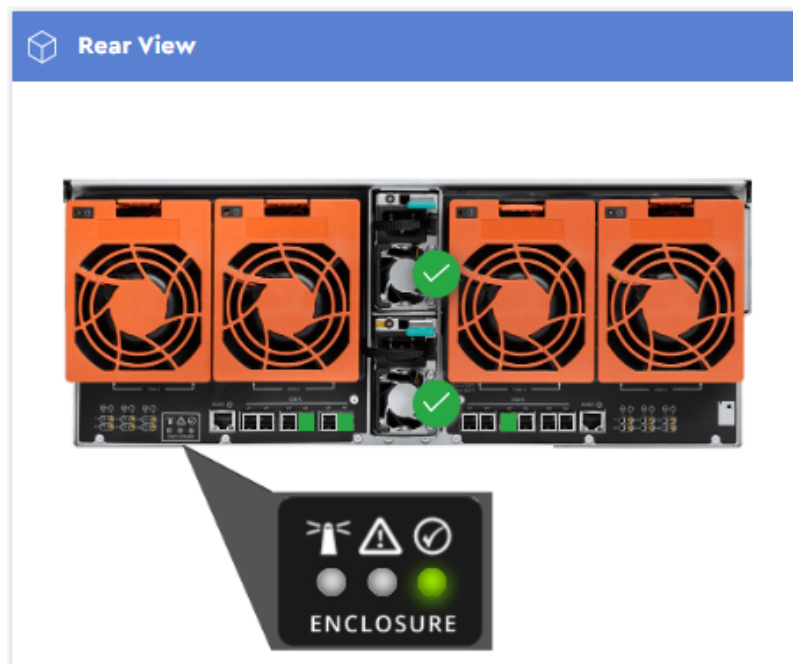
The **Rear** virtual view page will be displayed:

Figure 60: Rear View



Step 2: The **Rear View** image on the left will display the status of the enclosure's I/O ports.

Figure 61: Rear View I/O Ports



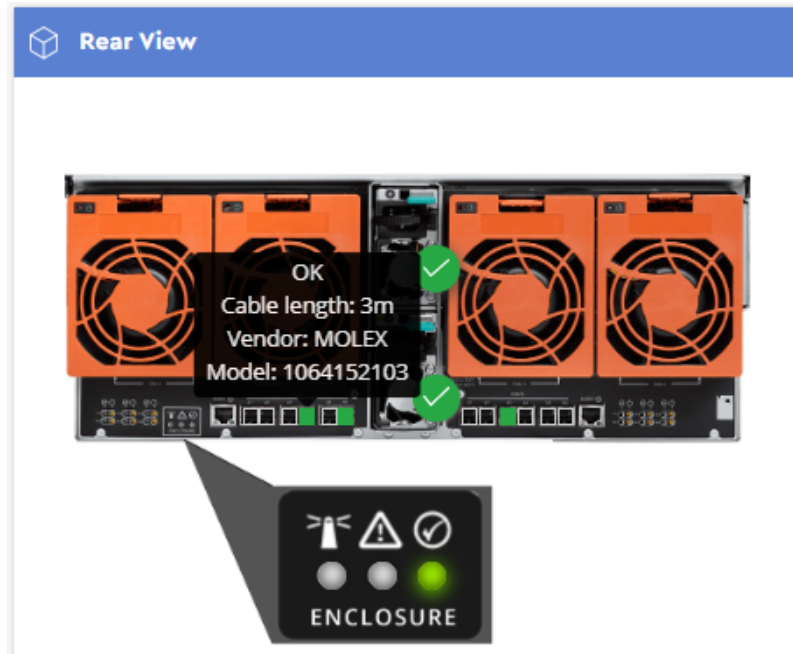
The ports will be highlighted as follows to indicate their cable attachment/health status:

- **Black** – Not installed

- **Green** – OK
- **Amber** – Non-Critical / Warning
- **Red** – Critical

Step 3: Hover your cursor over a port to view a tooltip, indicating the attached cable's health, length, manufacturer, and model.

Figure 62: Cable Tooltip



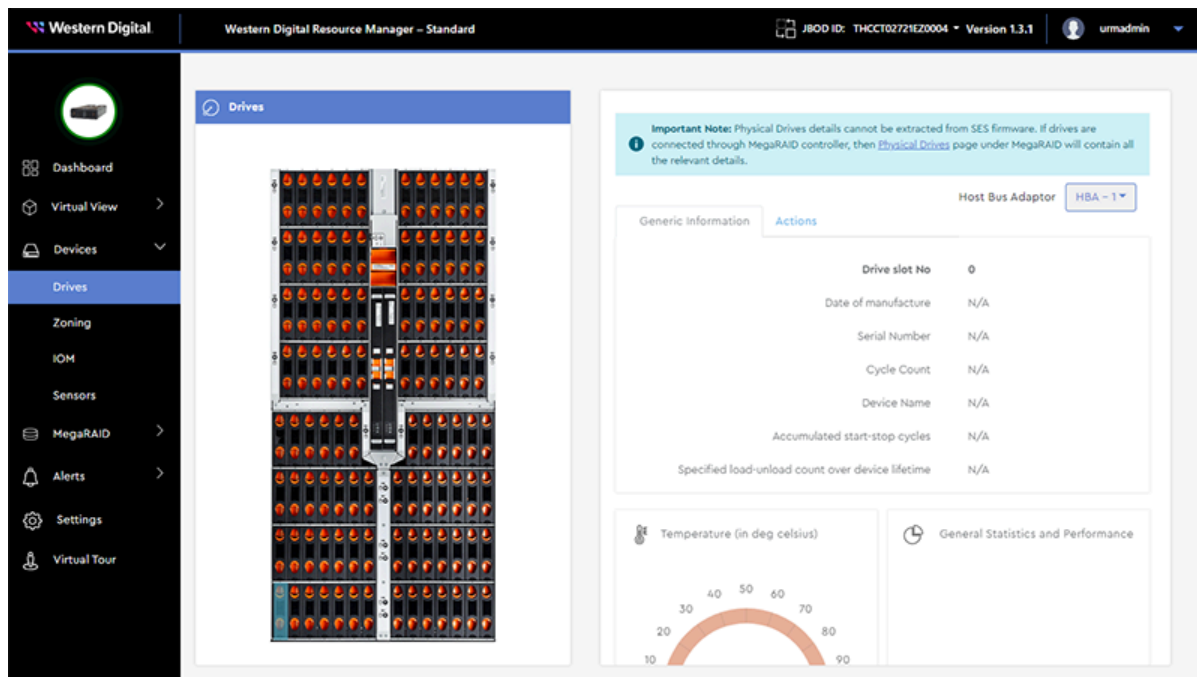
Result: Summary information about attached cables has now been viewed.

3.4 Devices

The **Devices** section provides information about the enclosure's sensors and major components, as well as management controls for drives, zoning, and IOM(s). If drives are managed through an HBA, or a MegaRAID controller in JBOD mode, the **Devices** section also provides drive LED management controls.

3.4.1 Drives

The **Drives** page provides an at-a-glance status of all drives in the enclosure, as well as general information, sensor data, and performance statistics for any specific drive.



Note: If a MegaRAID controller is detected in the host, drive details will **not** be available in this section of the Resource Manager Standard Edition. Instead, see [Physical Drives \(page 169\)](#) in the **MegaRAID** section.

3.4.1.1 Enabling / Disabling a Drive Identification LED (HBA)

This procedure provides instructions for enabling (illuminating) and/or disabling a drive's identification LED when the drive is managed through an HBA.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.



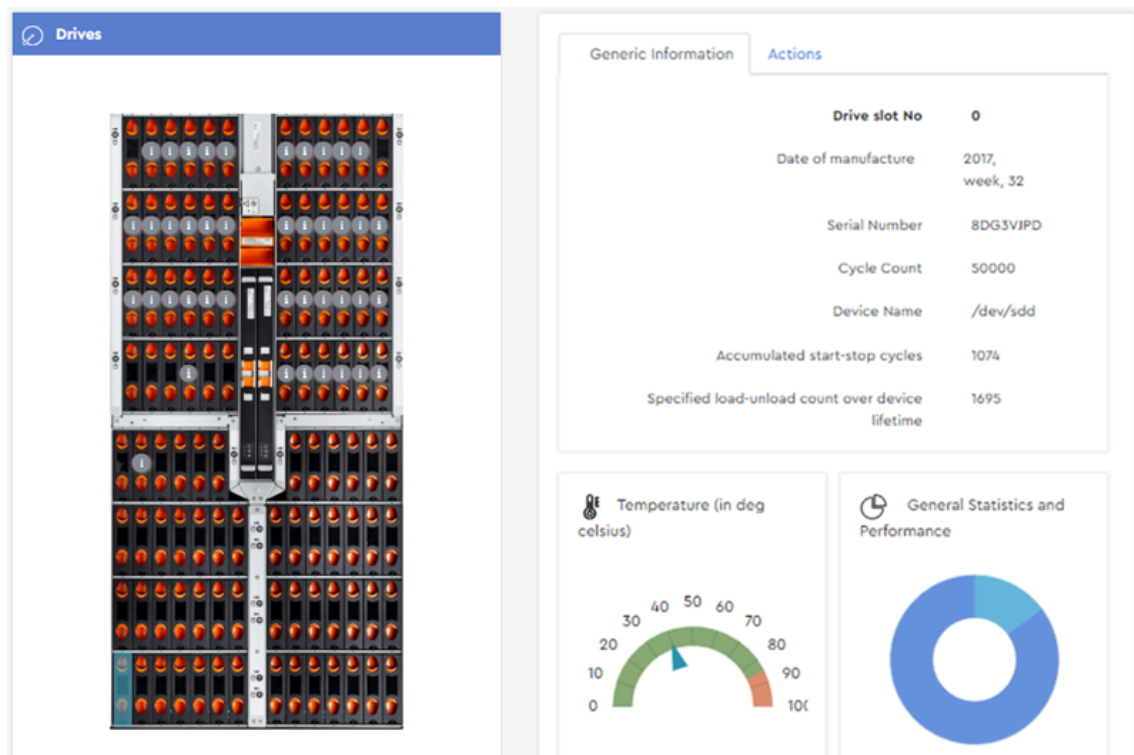
Note: To enable/disable a drive's LED through a MegaRAID controller, see [Enabling / Disabling a Drive Identification LED \(MegaRAID\) \(page 169\)](#).

Enabling a Drive Identification LED

Step 1: From the navigation bar, select **Devices** > **Drives**.

The **Drives** page will be displayed:

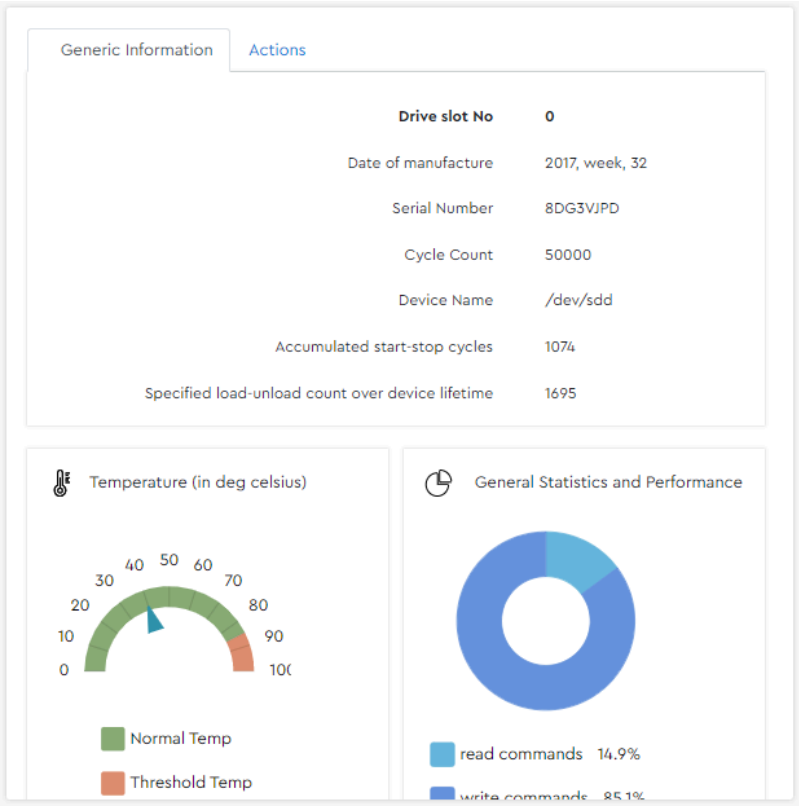
Figure 64: Drives Page



Step 2: From the **Drives** image on the left, click to select a drive slot.

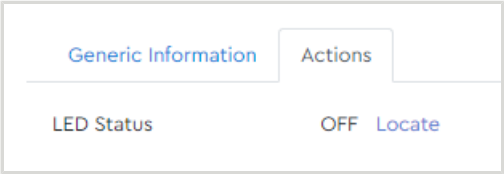
The **Generic Information** tab will display the available information about the drive installed in the selected slot:

Figure 65: Generic Information Tab



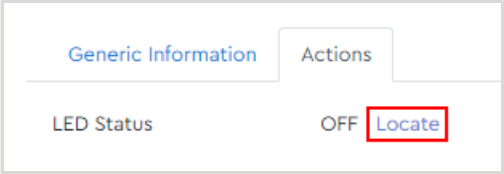
Step 3: Click the **Actions** tab.
The **Actions** tab will be displayed:

Figure 66: Actions Tab



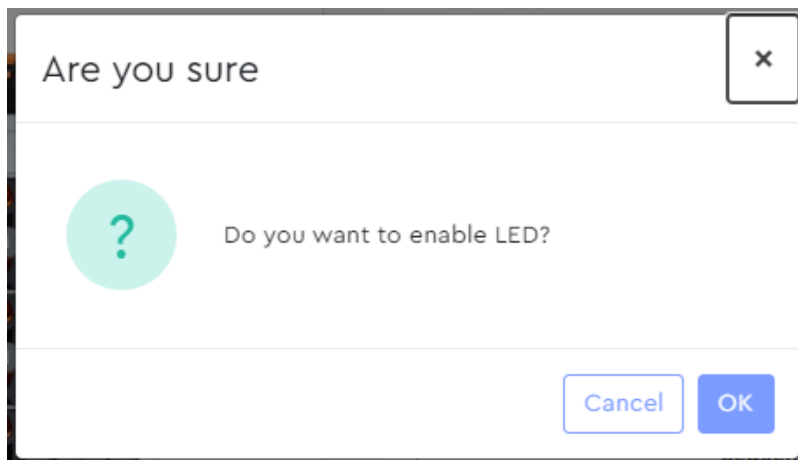
Step 4: In the **LED Status** section, click the **Locate** link.

Figure 67: Locate Link



A dialogue box will appear, prompting the user to confirm enabling the drive's identification LED:

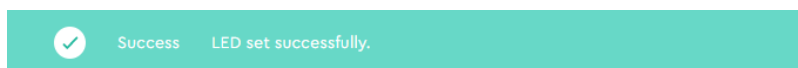
Figure 68: Confirm Enabling LED



Step 5: Click the **OK** button.

A success notification will appear at the top of the page:

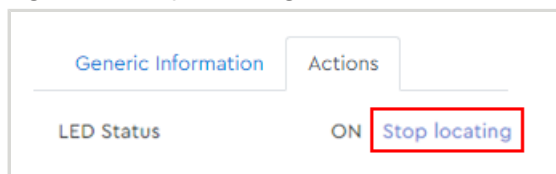
Figure 69: Success Notification



Disabling a Drive Identification LED

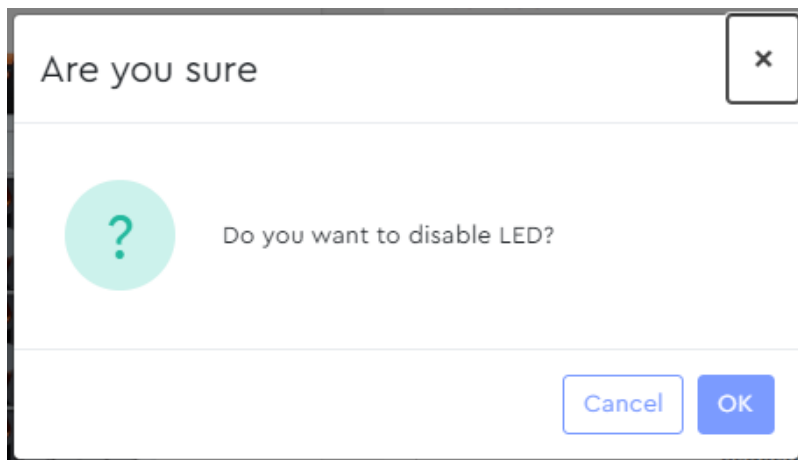
Step 6: In the **LED Status** section, click the **Stop Locating** link.

Figure 70: Stop Locating Link



A dialogue box will appear, prompting the user to confirm disabling the drive's identification LED:

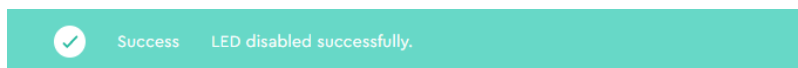
Figure 71: Confirm Disabling LED



Step 7: Click the **OK** button.

A success notification will appear at the top of the page:

Figure 72: Success Notification



Result: The selected drive's identification LED has now been enabled and/or disabled.

3.4.1.2 Updating Drive Firmware, Single Drive (HBA)

This procedure provides instructions for updating firmware on a single drive, when the drive is managed through an HBA.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

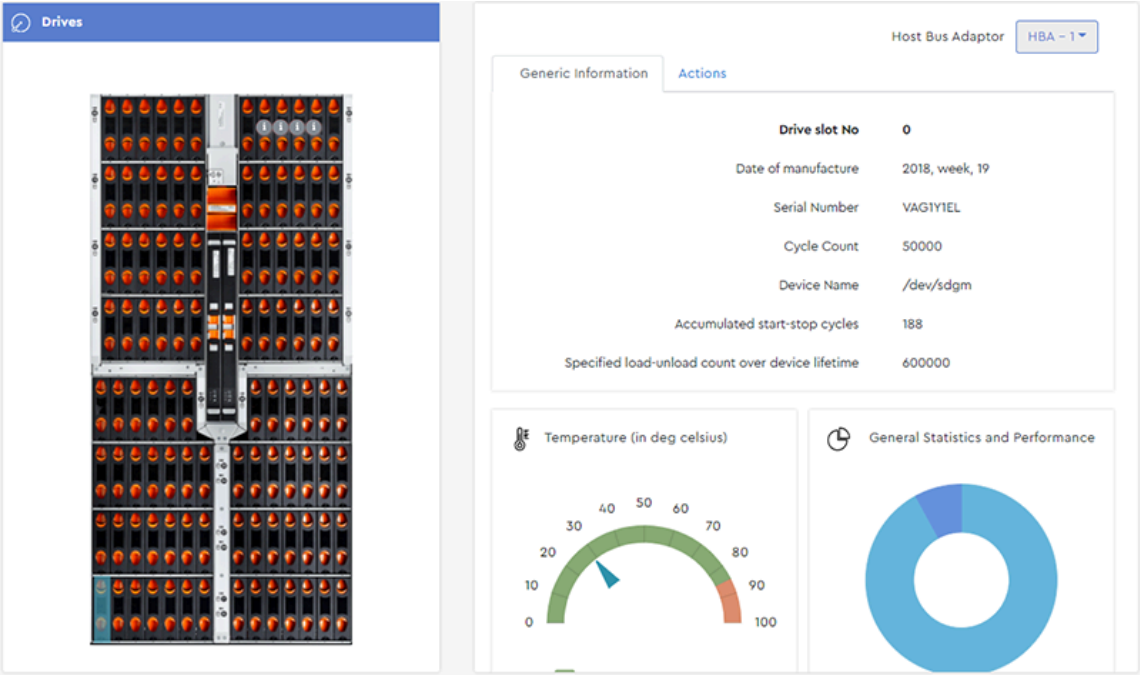


Note: To update a single drive's firmware through a MegaRAID controller, see [Updating Drive Firmware, Single Drive \(MegaRAID\) \(page 173\)](#).

Step 1: From the navigation bar, select **Devices > Drives**.

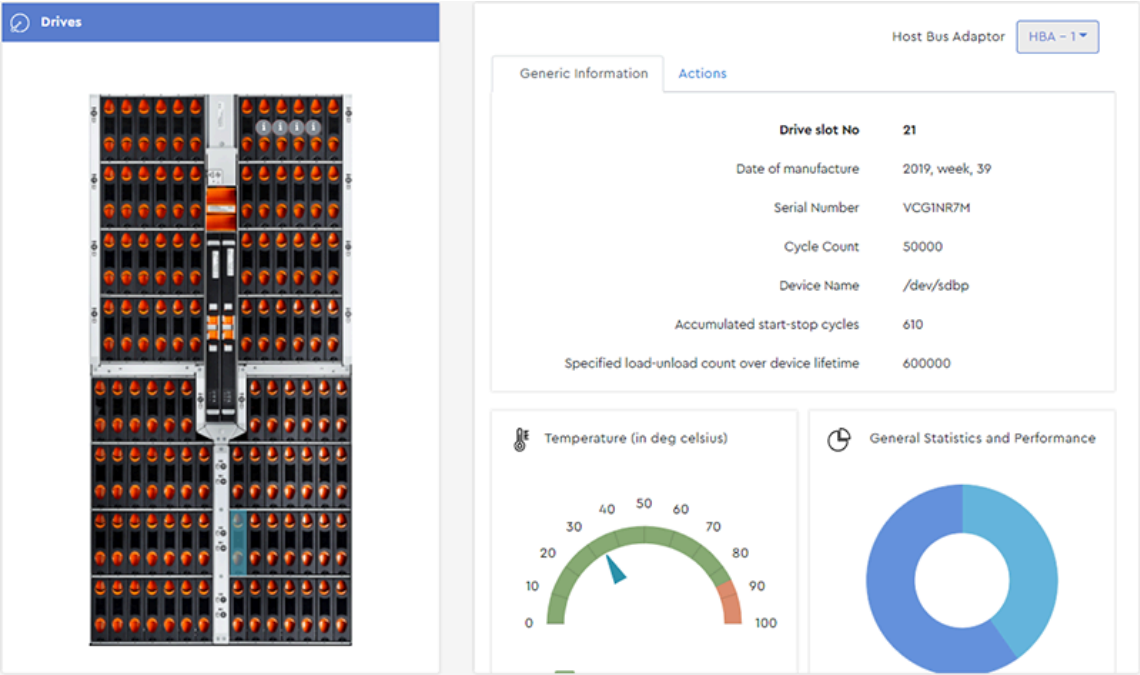
The **Drives** page will be displayed:

Figure 73: Drives Page



- Step 2:** From the **Drives** section on the left, click to select a drive slot.
- The drive will be highlighted, and the **Generic Information** tab on the right will display details about the drive installed in that slot:

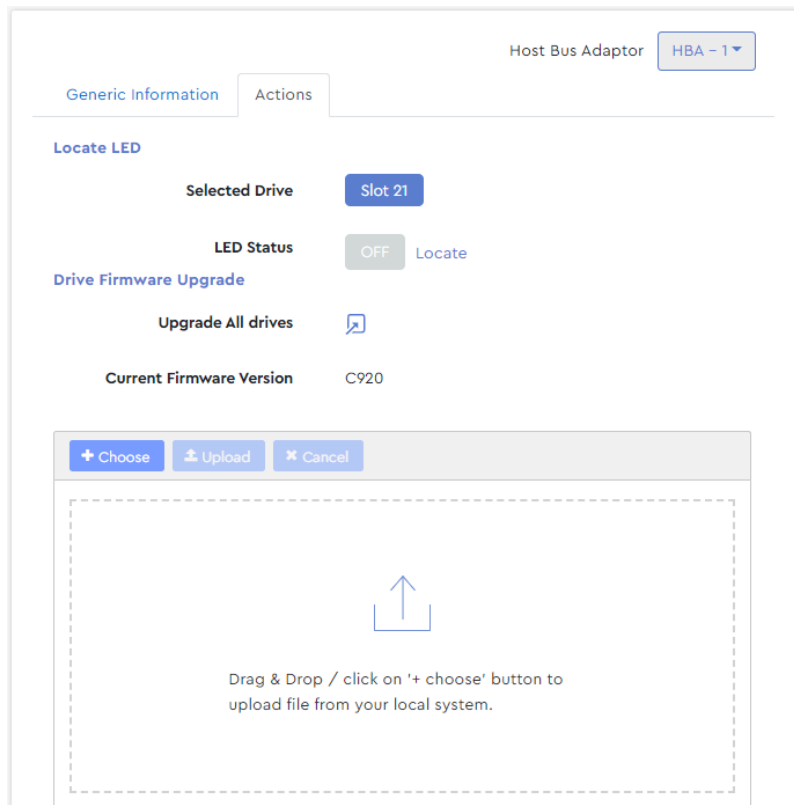
Figure 74: Selected Slot



Step 3: Click the **Actions** tab.

The **Actions** section will appear, displaying information about the installed drive and available actions:

Figure 75: Actions Section



The screenshot shows a web interface with a 'Host Bus Adaptor' dropdown set to 'HBA - 1'. Below this are two tabs: 'Generic Information' and 'Actions', with 'Actions' being the active tab. The 'Actions' section contains several controls:

- Locate LED**: A section with a 'Selected Drive' dropdown set to 'Slot 21' and an 'LED Status' toggle set to 'OFF'. A 'Locate' button is next to the toggle.
- Drive Firmware Upgrade**: A section with an 'Upgrade All drives' button featuring a document icon.
- Current Firmware Version**: A label showing 'C920'.

Below these controls is a file upload area with three buttons: '+ Choose', 'Upload', and 'Cancel'. A dashed box contains an upward arrow icon and the text: 'Drag & Drop / click on '+ choose' button to upload file from your local system.'

Take note of the **Current Firmware Version** for this drive, as this will be used to confirm a successful update at the end of this procedure:

Figure 76: Current Firmware Version

The screenshot shows a web-based management interface. At the top right, there is a 'Host Bus Adaptor' dropdown menu set to 'HBA - 1'. Below this, there are two tabs: 'Generic Information' and 'Actions'. The 'Generic Information' tab is active. Under the 'Locate LED' section, there is a 'Selected Drive' dropdown set to 'Slot 21' and an 'LED Status' toggle set to 'OFF' with a 'Locate' button next to it. Below this is the 'Drive Firmware Upgrade' section, which includes an 'Upgrade All drives' button with a document icon. A red rectangle highlights the 'Current Firmware Version' field, which displays 'C920'. At the bottom, there is a file upload area with buttons for '+ Choose', 'Upload', and 'Cancel'. Below these buttons is a dashed box containing an upward arrow icon and the text: 'Drag & Drop / click on '+ choose' button to upload file from your local system.'

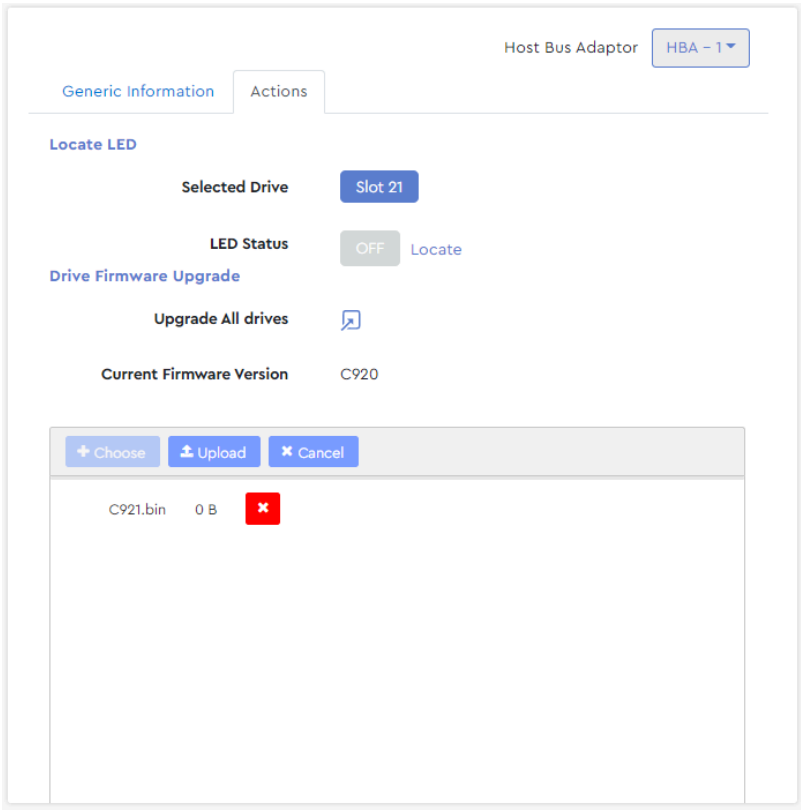
Step 4: Either drag & drop the drive firmware file onto the **Drag & Drop** section, or click the **Choose** button, which will open your operating system's file browser and allow you to browse and select the firmware file.

Figure 77: Choose Button

The screenshot displays a web-based management interface. At the top right, there is a 'Host Bus Adaptor' dropdown menu set to 'HBA - 1'. Below this, there are two tabs: 'Generic Information' and 'Actions', with 'Actions' being the active tab. The 'Actions' tab contains several sections: 'Locate LED' with a 'Selected Drive' dropdown set to 'Slot 21' and an 'LED Status' toggle set to 'OFF' with a 'Locate' link; 'Drive Firmware Upgrade' with an 'Upgrade All drives' button; and 'Current Firmware Version' showing 'C920'. At the bottom of the 'Actions' tab, there is a file upload section with three buttons: '+ Choose' (highlighted with a red box), 'Upload', and 'Cancel'. Below these buttons is a large dashed rectangular area containing an upward-pointing arrow icon and the text: 'Drag & Drop / click on '+ choose' button to upload file from your local system.'

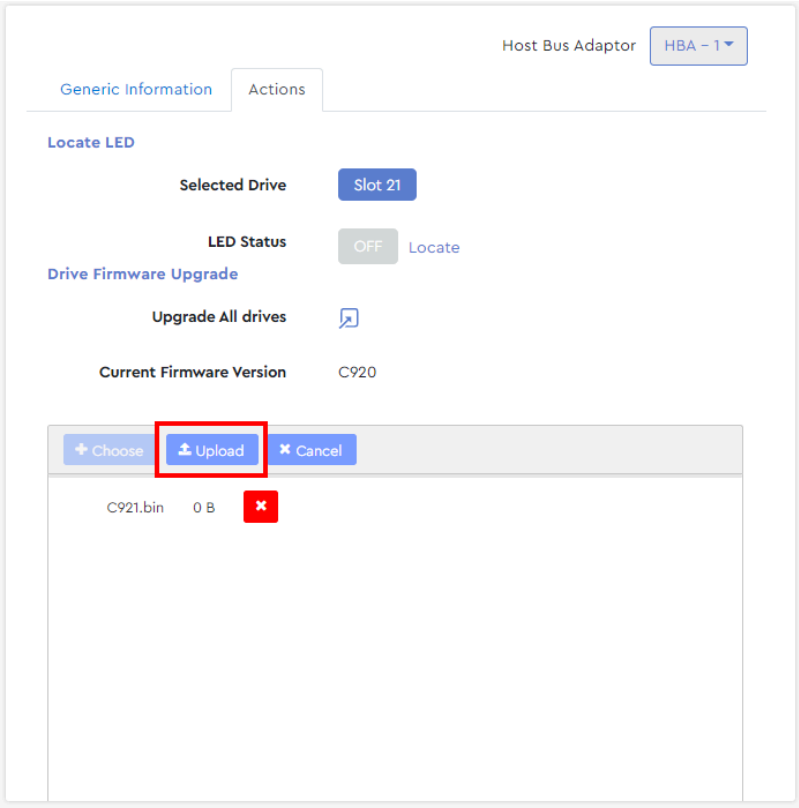
Step 5: Once selected, the drive firmware file will appear in the **Drag & Drop** section.

Figure 78: Firmware File Selected



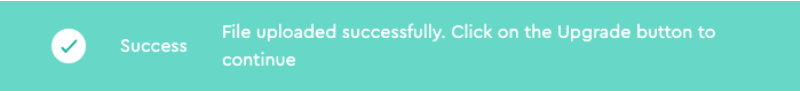
Step 6: Click the **Upload** button to upload the firmware to the drive.

Figure 79: Upload Firmware



After the firmware is uploaded, a success notification will appear at the top of the page:

Figure 80: Success Notification



Step 7: As prompted, click the **Upgrade** button to upgrade the firmware:

Figure 81: Upgrade Button



Step 8: After the firmware has been updated, compare the **Current Firmware Version** to the version noted at the beginning of this procedure:

Figure 82: Updated Firmware

Result: The drive's firmware has now been updated.

3.4.1.3 Updating Drive Firmware, Multiple Drives (HBA)

This procedure provides instructions for updating firmware on multiple drives (of the same drive model), when those drives are managed through an HBA.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

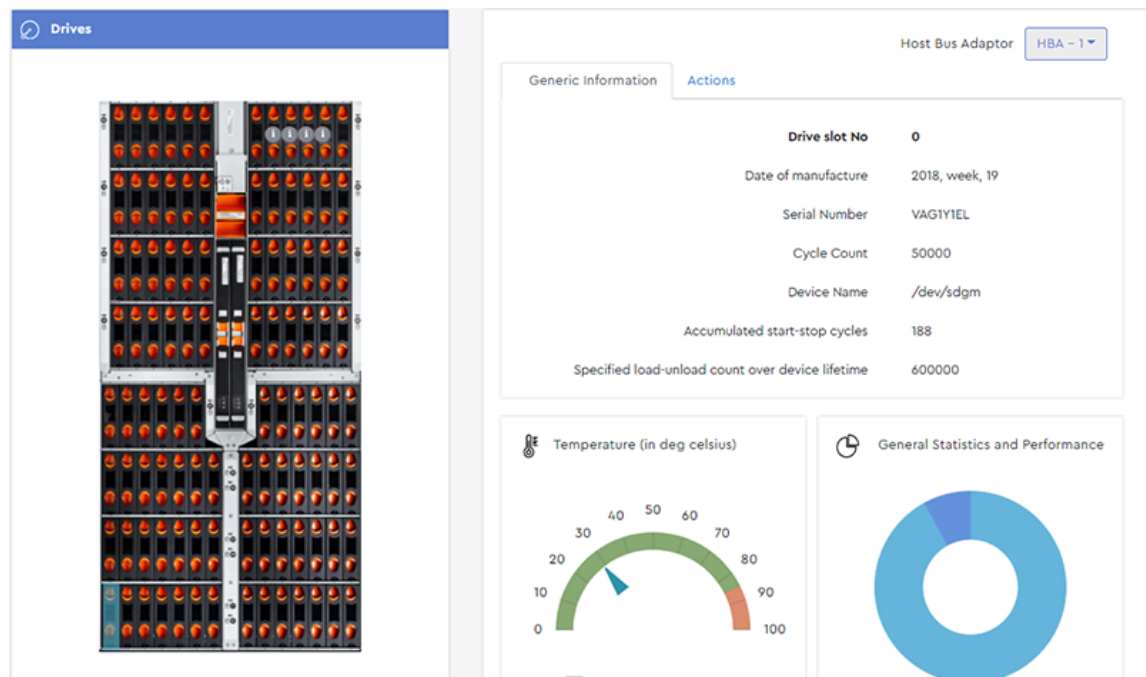


Note: To update firmware on multiple drives through a MegaRAID controller, see [Updating Drive Firmware, Multiple Drives \(MegaRAID\) \(page 177\)](#).

Step 1: From the navigation bar, select **Devices > Drives**.

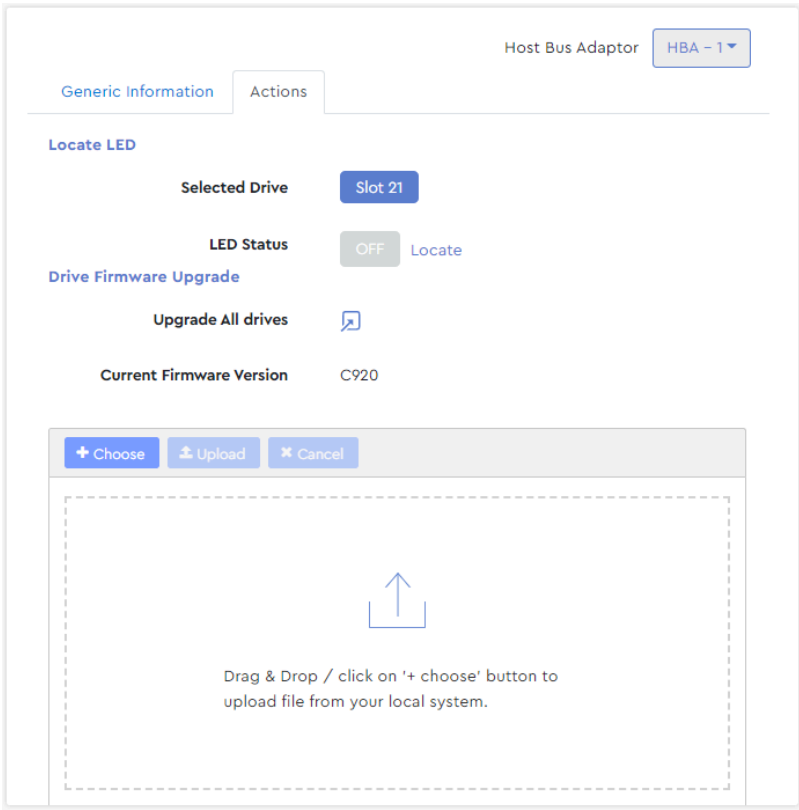
The **Drives** page will be displayed:

Figure 83: Drives Page



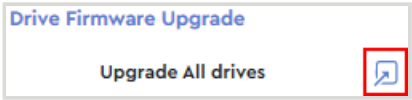
- Step 2:** On the right-hand side of the page, click the **Actions** tab.
The **Actions** tab will be displayed:

Figure 84: Actions Tab



Step 3: In the **Drive Firmware Upgrade** section, click the **Upgrade All drives** icon:

Figure 85: Upgrade All Drives



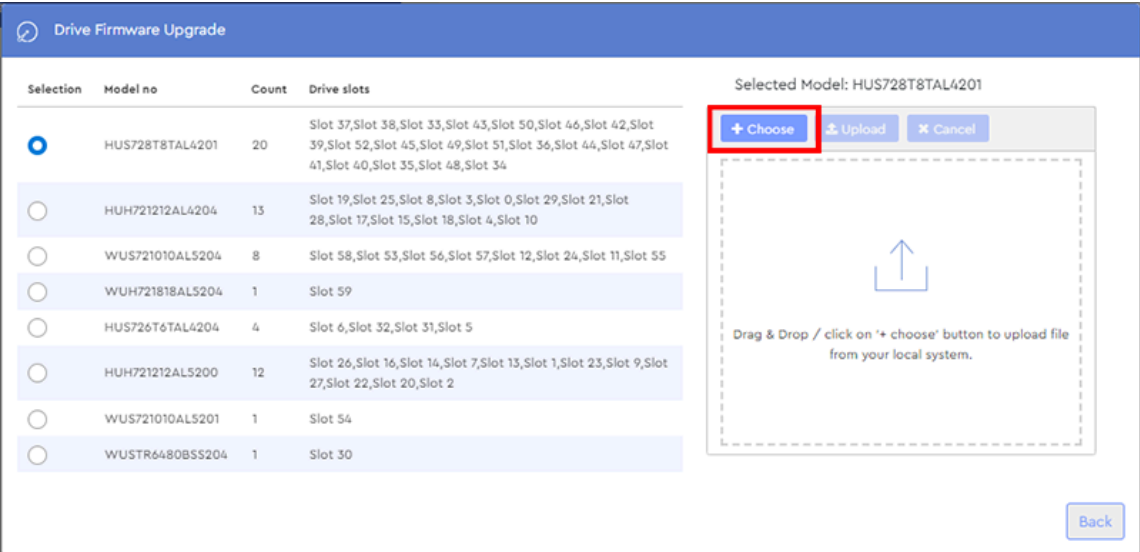
A **Drive Firmware Upgrade** window will appear, displaying a list of installed drive models, the quantity of each model, and the slot numbers where they are installed.

Figure 86: Drive Firmware Upgrade



Step 4: Click one of the radio buttons in the **Selection** column to select a drive model (and the associated drives). Then click the **Choose** button:

Figure 87: Choose Button



This will open your operating system's file browser and allow you to locate and select the firmware file.

Step 5: Once selected, the drive firmware file will appear in the **Drag & Drop** section:

Figure 88: Firmware File Selected



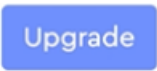
Step 6: Click the **Upload** button to upload the firmware to the drives.

Figure 89: Upload Firmware



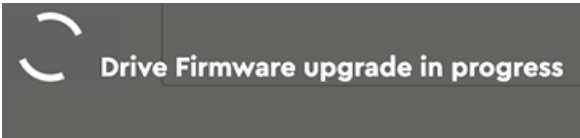
Step 7: After the firmware is uploaded, click the **Upgrade** button to upgrade the firmware:

Figure 90: Upgrade Button



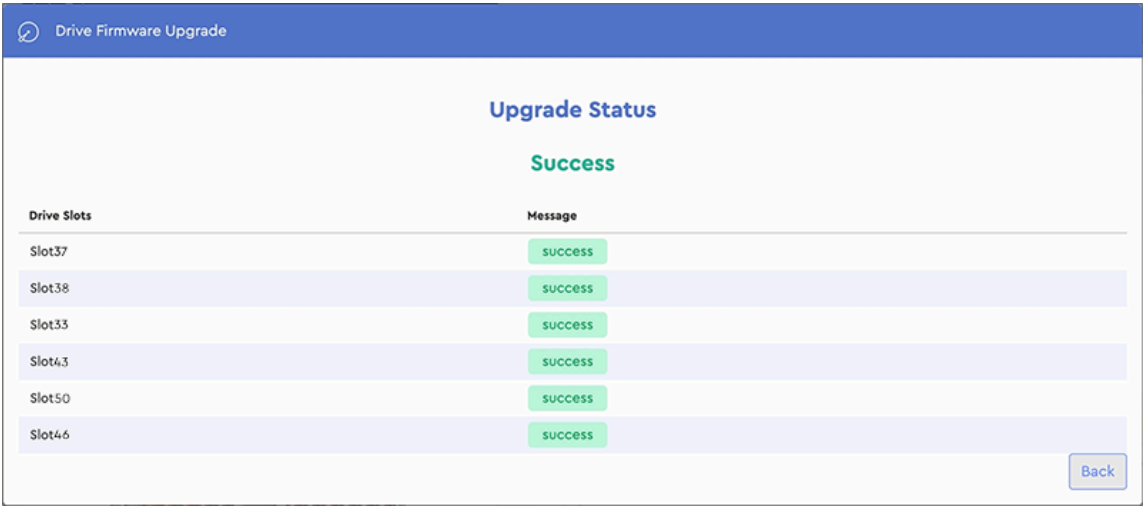
A notification will appear on the page during the upgrade:

Figure 91: Upgrade In Progress



When the upgrade is finished, a success notification will be displayed:

Figure 92: Upgrade Success



- Step 8:** Click the **Back** button, return to the **Actions** tab, and select one of the slots that was included in the group.
- Step 9:** Review the **Current Firmware Version** to verify that it matches the uploaded drive firmware:

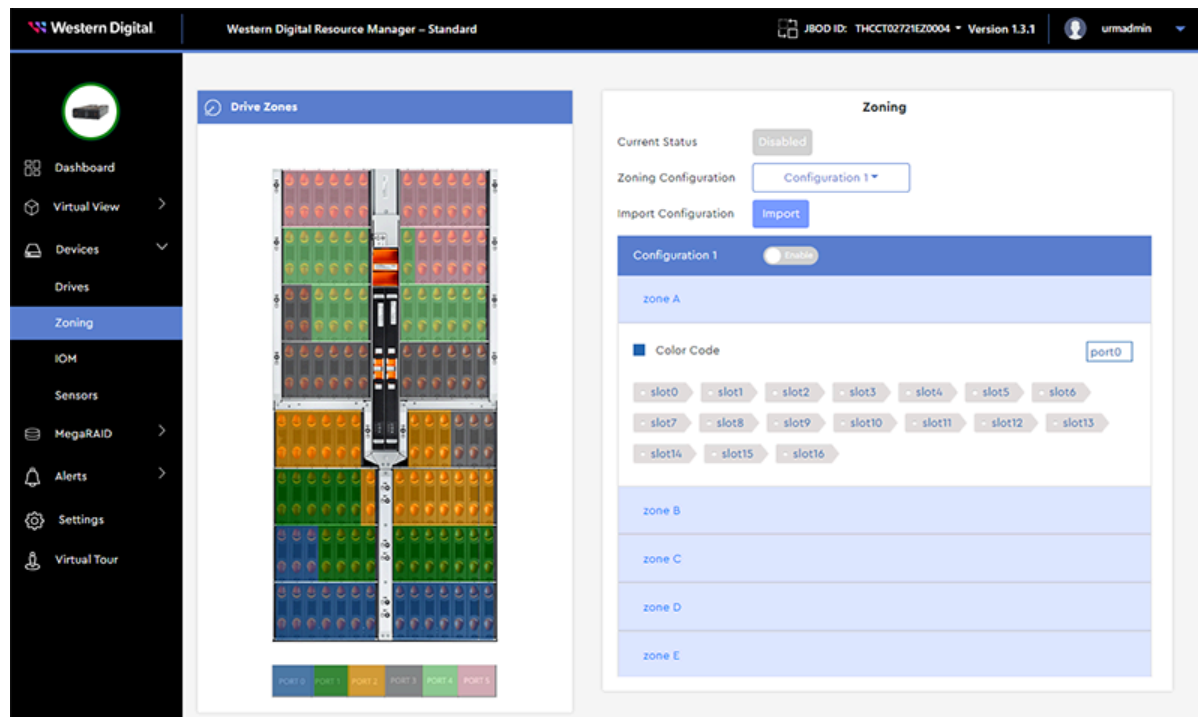
Figure 93: Current Firmware Version

The screenshot displays a web interface for managing storage devices. At the top right, a dropdown menu for 'Host Bus Adaptor' is set to 'HBA - 1'. Below this, there are two tabs: 'Generic Information' and 'Actions'. The 'Generic Information' tab is active, showing details for 'Slot 21'. The 'LED Status' is 'OFF', with a 'Locate' button next to it. Under the 'Drive Firmware Upgrade' section, there is a button for 'Upgrade All drives' and a red-bordered box highlighting the 'Current Firmware Version' as 'C921'. At the bottom, there is a file upload area with buttons for '+ Choose', 'Upload', and 'Cancel'. A dashed box contains an upward arrow icon and the text: 'Drag & Drop / click on '+ choose' button to upload file from your local system.'

Result: The drives' firmware has now been updated.

3.4.2 Zoning

The **Zoning** page provides controls for configuring drive zones. Select a predefined zoning configuration, or group specific drives to create your own. Custom configurations can be imported or exported in JSON or Hjson formats. File-based configurations are stored on the enclosure's baseboard, making them persistent through power cycles. See your platform's User Guide for more information about file-based zoning.



3.4.2.1 Selecting a Predefined Zoning Configuration

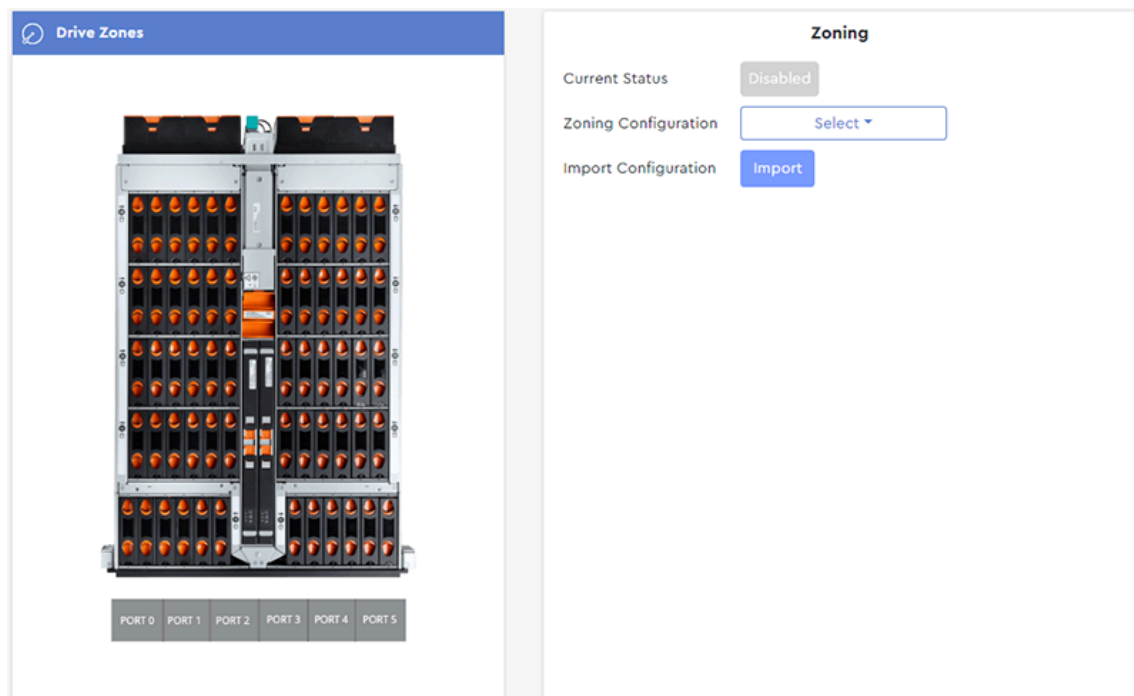
This procedure provides instructions for selecting and enabling a predefined drive zoning configuration using the Resource Manager Standard Edition application.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **Devices > Zoning**.

The zoning page will be displayed:

Figure 95: Zoning Page



Note: The enclosure image on the zoning page will depend on your platform model. This example shows the Ultrastar Data60.

Step 2: From the **Zoning Configuration** drop-down list, select **Configuration 1, 2, or 3**:

Figure 96: Zoning Configuration Drop-Down List

Zoning

Current Status

Disabled

Zoning Configuration

Select ▾

Import Configuration

Configuration 1

Configuration 2

Configuration 3

Custom Configuration



Note: See the *Predefined Zoning Configurations* section of your platform's *User Guide* for a detailed explanation of each predefined zoning configuration.

The **Zoning** section will display the details for the selected configuration:

Figure 97: Configuration Details

Drive Zones

Zoning

Current Status

Disabled

Zoning Configuration

Configuration 1 ▾

Import Configuration

Import

Configuration 1

Enable

zone A

Color Code

port0

slot0

slot1

slot2

slot3

slot4

slot5

slot6

slot7

slot8

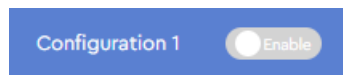
slot9

zone B

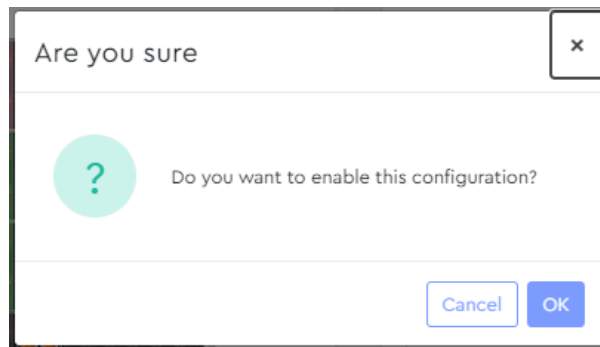
zone C

zone D

Step 3: Click the toggle switch next to the configuration name to enable the configuration.

Figure 98: Configuration Toggle Switch

A dialogue box will appear, prompting the user to confirm the configuration:

Figure 99: Confirm Configuration Dialogue Box

Step 4: Click the **OK** button to enable the configuration.

Result: The selected zoning configuration is now enabled.

3.4.2.2 Creating a Custom Zoning Configuration

This procedure provides instructions for creating and enabling a custom drive zoning configuration using the Resource Manager Standard Edition application.

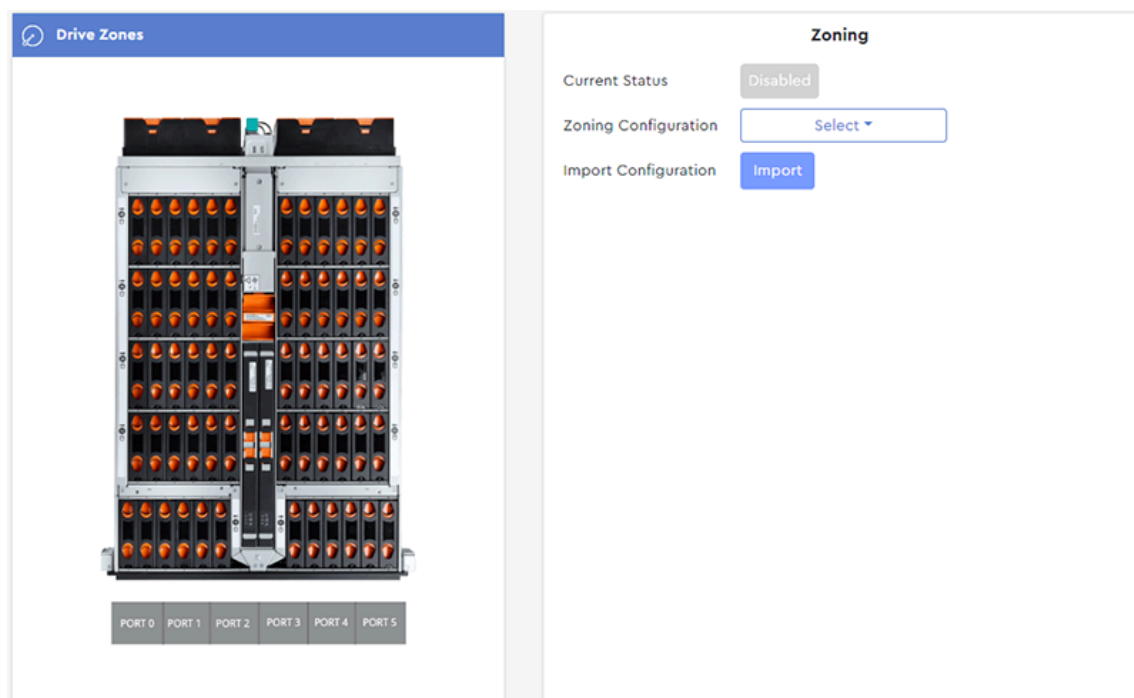
Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Creating a Custom Zoning Configuration

Step 1: From the navigation bar, select **Devices > Zoning**.

The zoning page will be displayed:

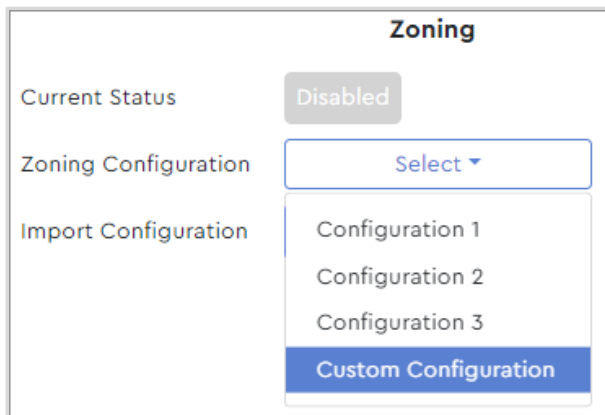
Figure 100: Zoning Page



Note: The enclosure image on the zoning page will depend on your platform model. This example shows the Ultrastar Data60.

Step 2: From the **Zoning Configuration** drop-down list, select **Custom Configuration**:

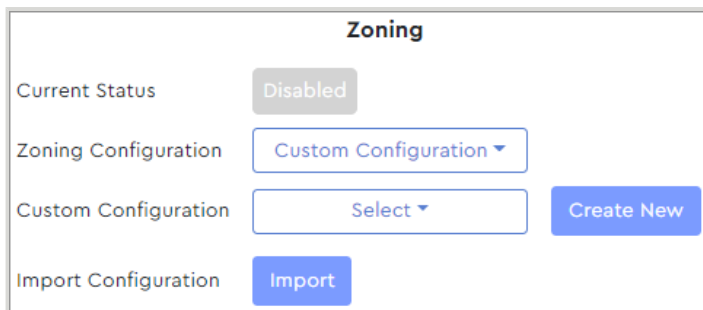
Figure 101: Zoning Configuration Drop-Down List



The image shows a 'Zoning' configuration panel. It has a title 'Zoning' at the top. Below the title, there are three rows of controls. The first row is 'Current Status' with a 'Disabled' button. The second row is 'Zoning Configuration' with a 'Select' dropdown menu. The third row is 'Import Configuration' with a list of options: 'Configuration 1', 'Configuration 2', 'Configuration 3', and 'Custom Configuration'. The 'Custom Configuration' option is highlighted in blue.

A **Create New** button will appear in the **Custom Configuration** section:

Figure 102: Create New Button

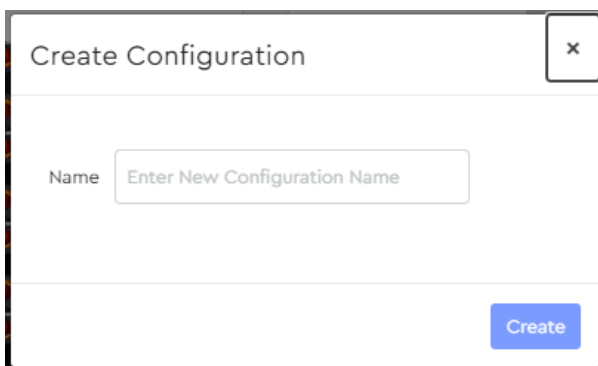


The image shows the 'Zoning' configuration panel with additional controls. The 'Zoning Configuration' dropdown is now set to 'Custom Configuration'. Below it, there is a 'Custom Configuration' section with a 'Select' dropdown and a 'Create New' button. At the bottom, there is an 'Import Configuration' section with an 'Import' button.

Step 3: Click the **Create New** button.

A **Create Configuration** dialogue box will appear:

Figure 103: Create Configuration Dialogue Box



The image shows a 'Create Configuration' dialogue box. It has a title bar with a close button (X). Inside, there is a 'Name' field with a placeholder text 'Enter New Configuration Name'. At the bottom right, there is a 'Create' button.

Step 4: Type a name for the new configuration into the **Name** field, and click the **Create** button.

A new section will appear, with controls for adding zones to the new configuration:

Figure 104: New Configuration

The screenshot shows a web interface for configuring zoning. At the top, the title "Zoning" is centered. Below it, the "Current Status" is "Disabled". The "Zoning Configuration" is set to "Custom Configuration". The "Custom Configuration" is set to "Select". There is a link to "Create New Custom Configuration". The "Import Configuration" section has an "Import" button. Below this is a table with one row labeled "Test1". The "Test1" row has an "Enable" toggle switch and three icons (document, folder, trash). Below the table is a message "Please click add new zone". At the bottom is an "Add New Zone" button.

Zoning

Current Status **Disabled**

Zoning Configuration **Custom Configuration**

Custom Configuration **Select**

[Create New Custom Configuration](#)

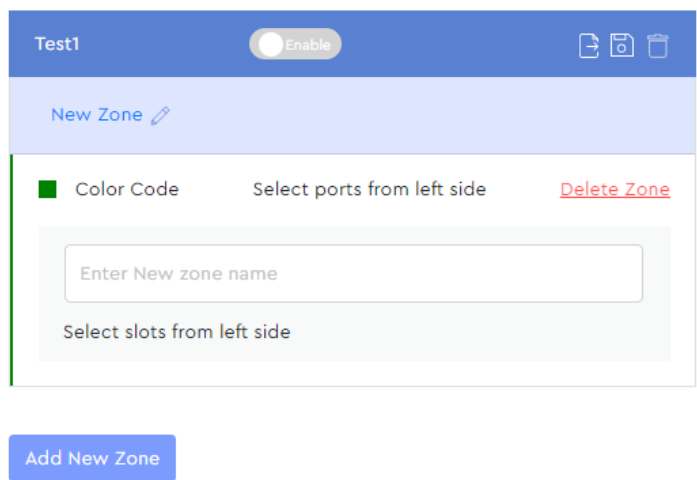
Import Configuration **Import**

Test1	Enable			
Please click add new zone				

Add New Zone

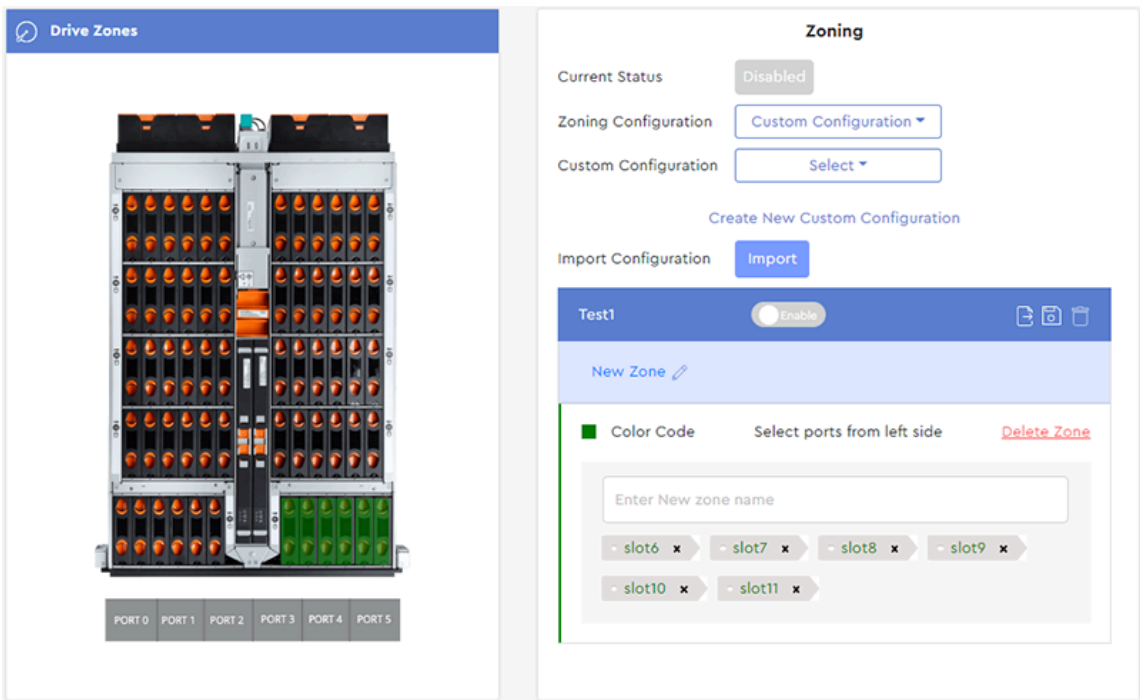
Step 5: As prompted, click the **Add New Zone** button.
A **New Zone** section will be added to the configuration:

Figure 105: New Zone



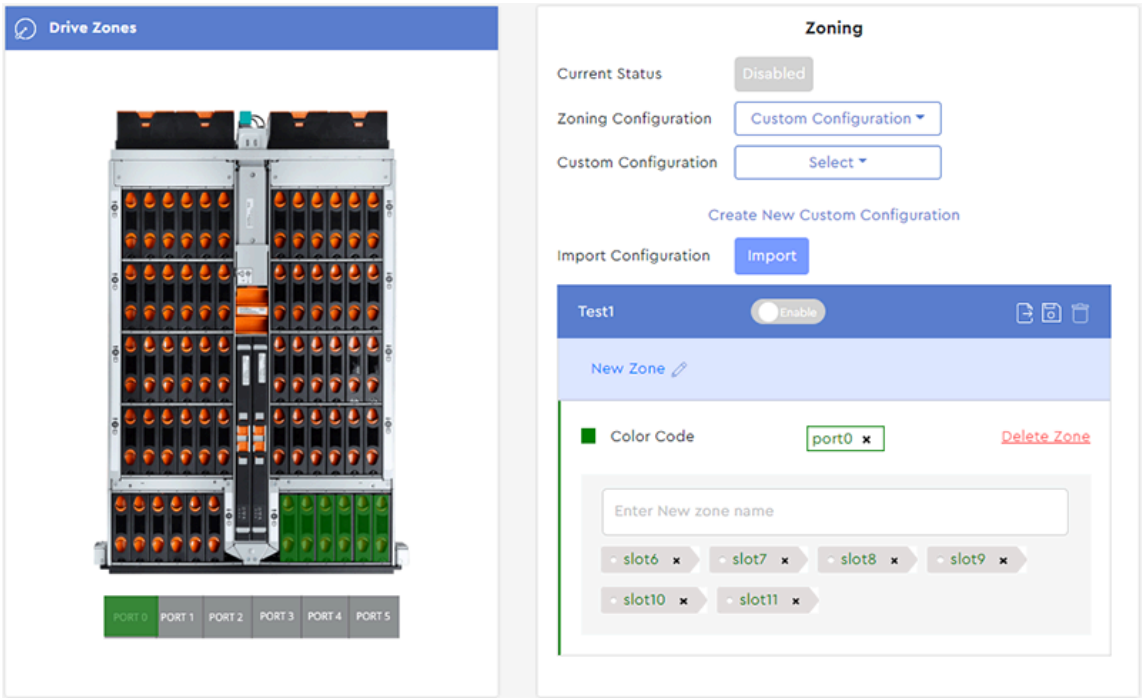
Step 6: From the **Drive Zones** section on the left, click the drive slots to be included in this zone. The slots will be colored to match the pre-selected color for the zone:

Figure 106: Color-Coded Drive Slots



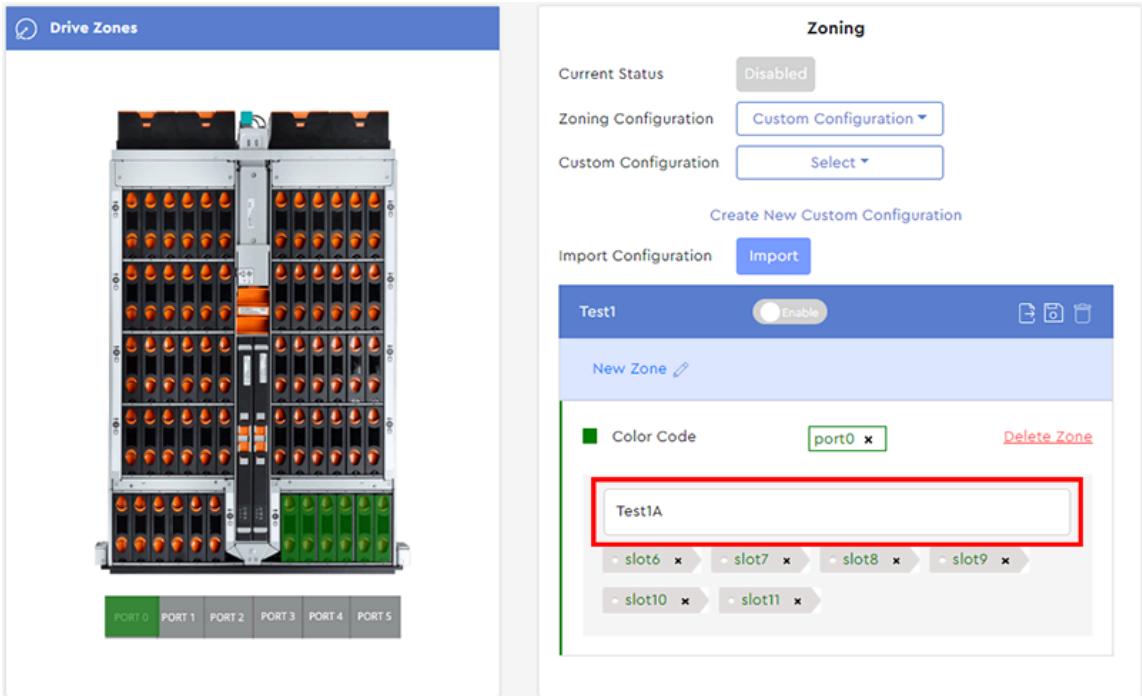
Step 7: At the bottom of the **Drive Zones** section, click a port to assign it to this zone. The port will be color-coded to match the drive slots:

Figure 107: Color-Coded Port



Step 8: Type a name for this new zone into the text field labeled **Enter New zone name**:

Figure 108: Zone Name



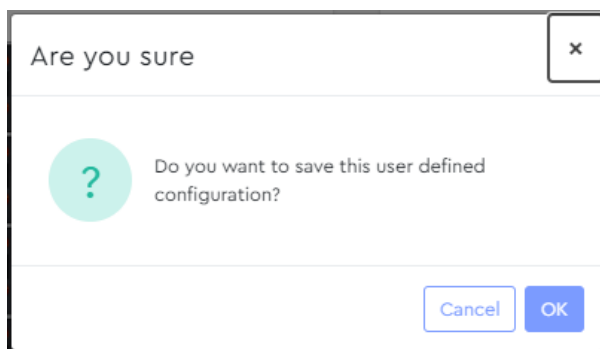
- Step 9:** If needed, repeat these instructions beginning at step 5 (page 75) to create additional zones with associated drive slots and ports.
- Step 10:** When all zones for the new configuration have been created, save the configuration by clicking the **Save** icon in the configuration header:

Figure 109: Save Icon



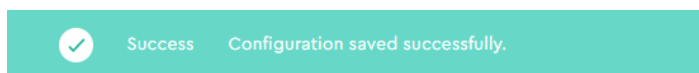
A dialogue box will appear, prompting the user to confirm saving the configuration:

Figure 110: Save Configuration Dialogue Box



- Step 11:** Click the **OK** button to save the configuration.
- A success notification will appear at the top of the page:

Figure 111: Success Message



Note: The new configuration will now be a selectable option from the **Custom Configuration** drop-down list.

Enabling the Custom Zoning Configuration

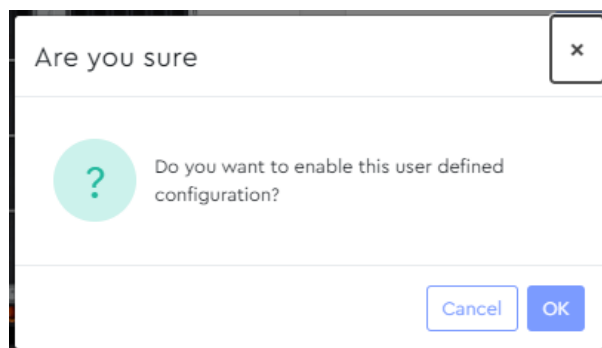
- Step 12:** To enable the newly-created zoning configuration, click the toggle switch next to the configuration name:

Figure 112: Configuration Toggle Switch



A dialogue box will appear, prompting the user to confirm enabling the configuration:

Figure 113: Enable Configuration Dialogue Box



Step 13: Click the **OK** button to enable the zoning configuration.

Result: The custom zoning configuration is now created and enabled.

3.4.2.3 Exporting a Custom Zoning Configuration

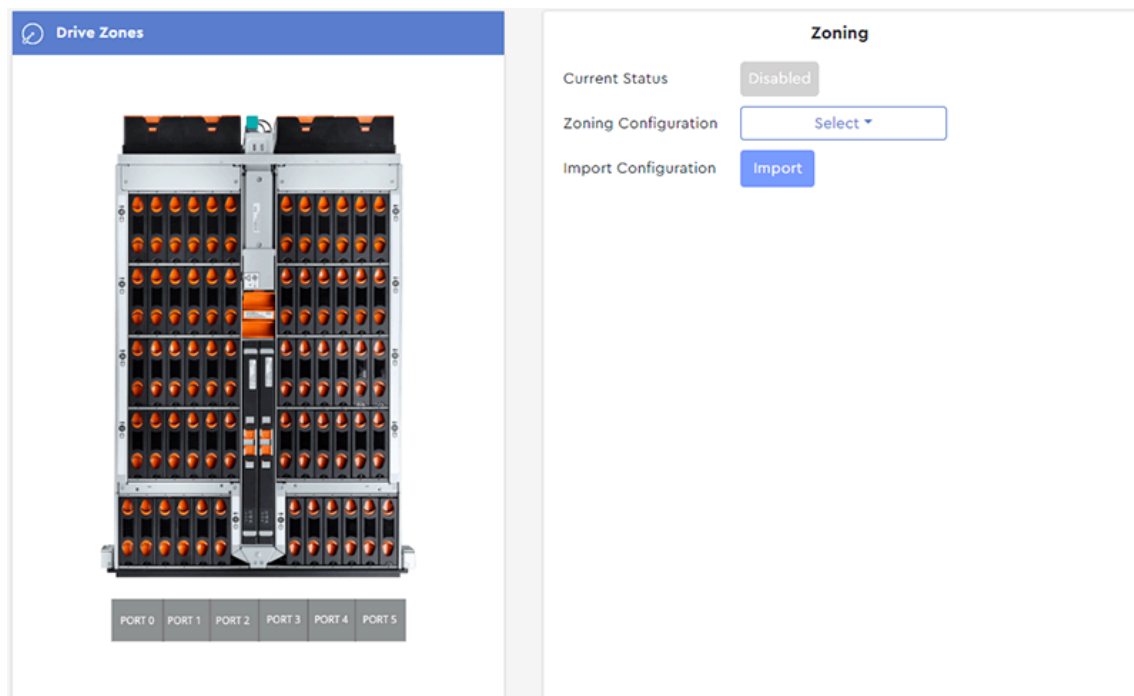
This procedure provides instructions for exporting a **previously-created** custom zoning configuration using the Resource Manager Standard Edition application.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **Devices > Zoning**.

The zoning page will be displayed:

Figure 114: Zoning Page



Note: The enclosure image on the zoning page will depend on your platform model. This example shows the Ultrastar Data60.

Step 2: From the **Zoning Configuration** drop-down list, select **Custom Configuration**:

Figure 115: Zoning Configuration Drop-Down List

Zoning

Current Status

Disabled

Zoning Configuration

Select ▾

Import Configuration

Configuration 1
Configuration 2
Configuration 3
Custom Configuration

A **Custom Configuration** section will appear:

Figure 116: Custom Configuration Section

Zoning

Current Status

Disabled

Zoning Configuration

Custom Configuration ▾

Custom Configuration

Select ▾

Create New

Import Configuration

Import

Step 3: From the **Custom Configuration** drop-down list, select a previously-created custom configuration:

Figure 117: Custom Configuration Drop-Down List

Zoning

Current Status

Disabled

Zoning Configuration

Custom Configuration ▾

Custom Configuration

Select ▾

Create New

Import Configuration

sample
sample_2
Test1

The custom configuration will appear in a new section, locked for editing:

Figure 118: Custom Configuration, Locked

Zoning

Current Status Disabled

Zoning Configuration Custom Configuration ▾

Custom Configuration Test1 ▾ Create New

Import Configuration Import

Test1 Enable 📄 🔍 🗑️

Test1A ✎

■ Color Code port0 x Delete Zone

🔒 Double Click to edit

slot6 x slot7 x slot8 x slot9 x

slot10 x slot11 x

Add New Zone

Step 4: Double-click the configuration to unlock it:

Figure 119: Custom Configuration, Unlocked

The screenshot displays the 'Zoning' configuration page. At the top, the 'Current Status' is 'Disabled'. Below this, the 'Zoning Configuration' is set to 'Custom Configuration'. The 'Custom Configuration' section shows a dropdown menu with 'Test1' selected, a 'Create New' button, and an 'Import' button. The 'Import Configuration' section has an 'Import' button. The main configuration area for 'Test1' includes an 'Enable' toggle, a 'Test1A' label with an edit icon, and a 'Color Code' section with a green box labeled 'port0' and a 'Delete Zone' link. Below this, there are two rows of slot selection buttons: 'slot6', 'slot7', 'slot8', 'slot9' in the first row, and 'slot10', 'slot11' in the second row. An 'Add New Zone' button is at the bottom.

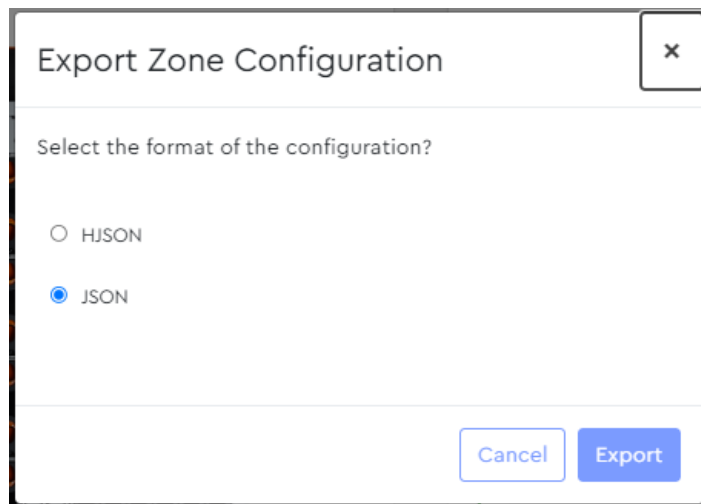
Step 5: Click the **Export** icon in the configuration header to export the configuration:

Figure 120: Export Icon



A dialogue box will appear, prompting the user to confirm exporting the configuration:

Figure 121: Export Configuration Dialogue Box



Step 6: Click the appropriate radio button to select the desired file format, then click the **Export** button. The configuration file will be saved in the `Downloads` directory on both Windows and Linux operating systems.



Note: A datestamp and timestamp will be appended to the filename to indicate when the configuration was exported.

Result: The selected zoning configuration is now exported.

3.4.2.4 Importing a Custom Zoning Configuration

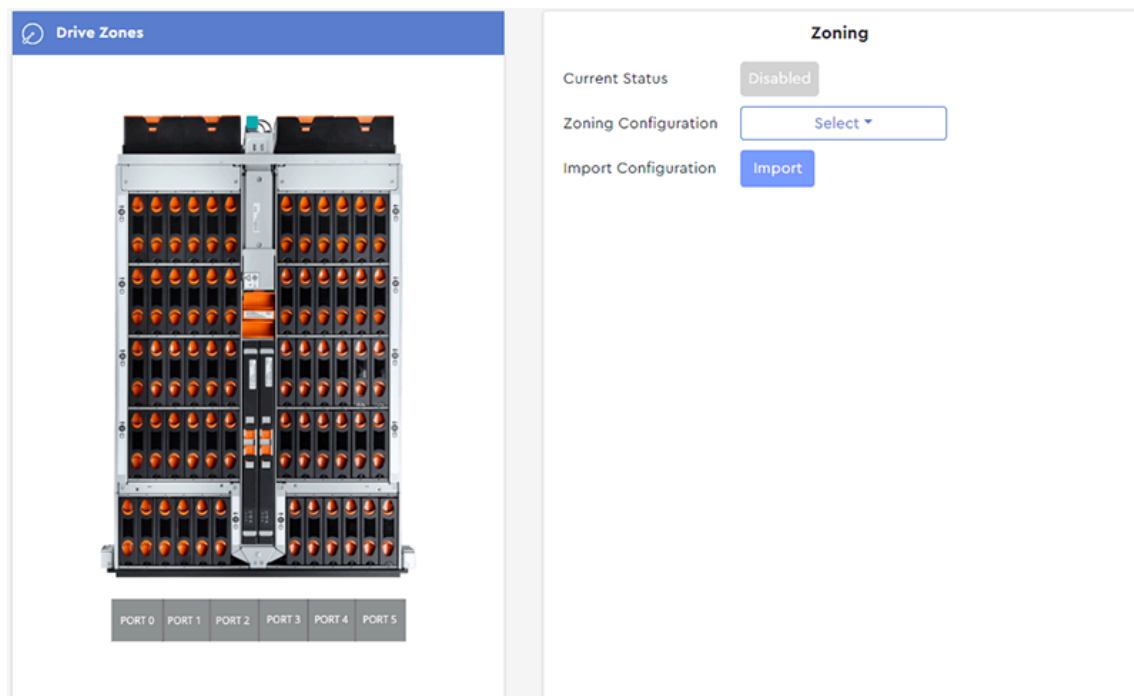
This procedure provides instructions for importing a custom zoning configuration using the Resource Manager Standard Edition application.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **Devices > Zoning**.

The zoning page will be displayed:

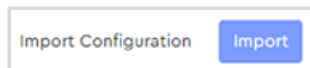
Figure 122: Zoning Page



Note: The enclosure image on the zoning page will depend on your platform model. This example shows the Ultrastar Data60.

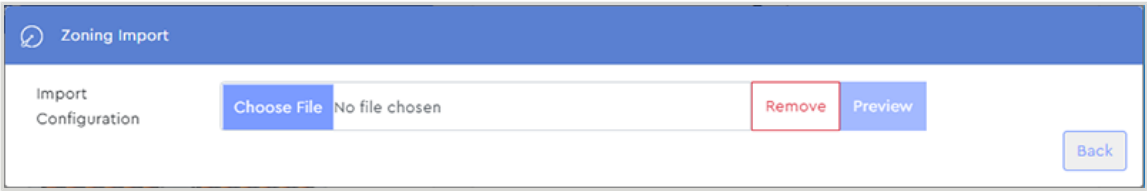
Step 2: In the **Import Configuration** section, click the **Import** button:

Figure 123: Import Button



A **Zoning Import** dialogue box will appear:

Figure 124: Zoning Import Dialogue Box



Step 3: Click the **Choose File** button:

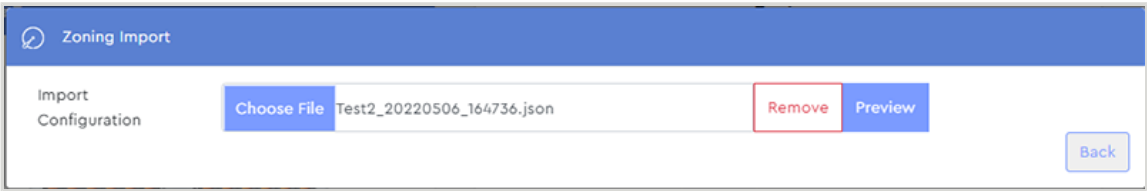
Figure 125: Choose File Button



This will open your operating system's file browser.

Step 4: Browse to the configuration file and select it.
Once selected, the configuration file name will appear in the dialogue box:

Figure 126: Configuration File Selected



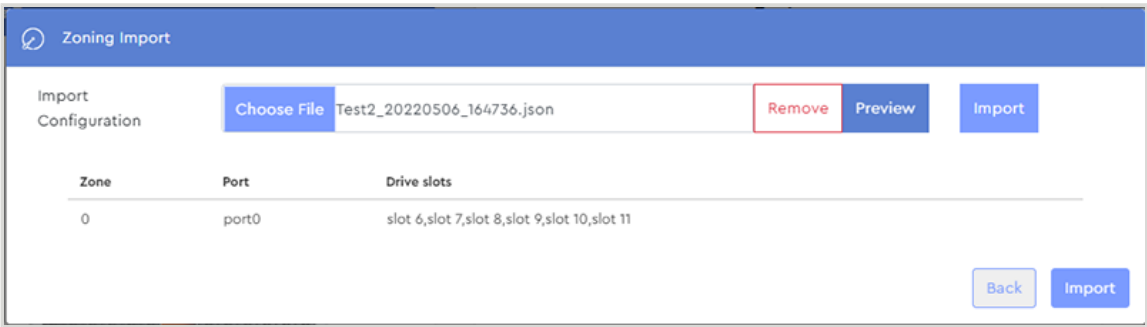
Step 5: Click the **Preview** button:

Figure 127: Preview Button



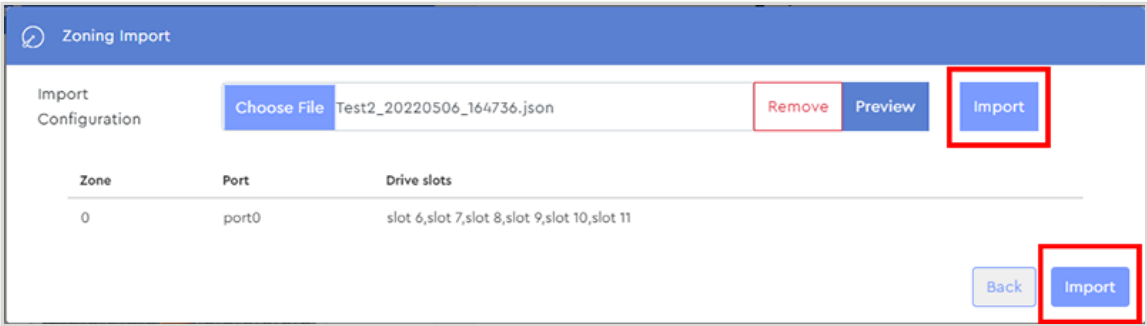
The dialogue box will expand to show a preview of the configuration details:

Figure 128: Imported Configuration Preview



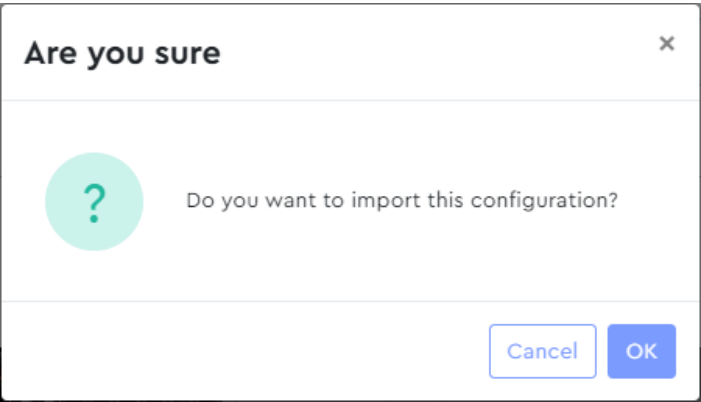
Step 6: Click either of the **Import** buttons to import the zoning configuration.

Figure 129: Import Buttons



A dialogue box will appear, prompting the user to confirm importing the configuration:

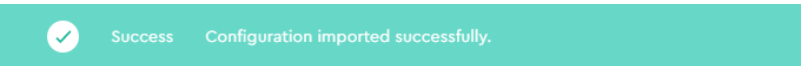
Figure 130: Import Confirmation Dialogue Box



Step 7: Click the **OK** button.

A success notification will appear in the dialogue box:

Figure 131: Success Message



The imported configuration is now a selectable option in the **Custom Configuration** drop-down list:

Figure 132: Selectable Configuration

Zoning

Current Status

Disabled

Zoning Configuration

Custom Configuration ▾

Custom Configuration

Select ▾

Create New

Import Configuration

sample

sample_2

Test1

Test2

Result: The selected zoning configuration is now imported.

3.4.2.5 Selecting a Custom Zoning Configuration

This procedure provides instructions for selecting and enabling a **previously-created** custom zoning configuration using the Resource Manager Standard Edition application. To create a new custom zoning configuration, see [Creating a Custom Zoning Configuration \(page 73\)](#).

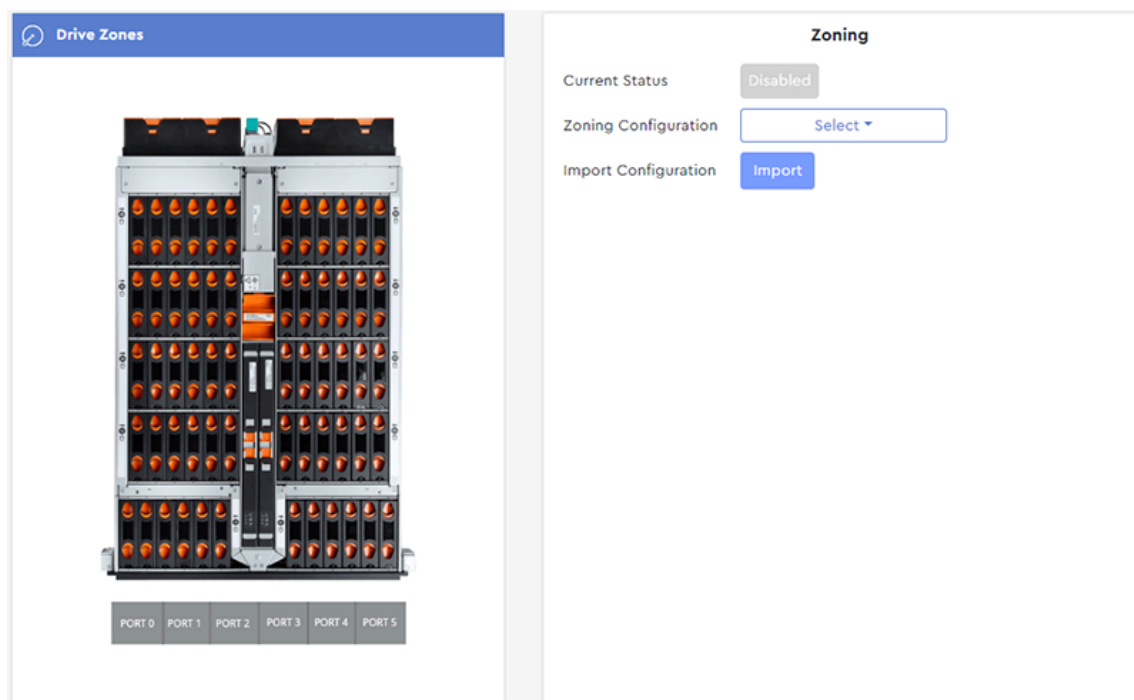
Before you begin:

1. Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.
2. Follow the instructions in [Creating a Custom Zoning Configuration \(page 73\)](#).

Step 1: From the navigation bar, select **Devices > Zoning**.

The zoning page will be displayed:

Figure 133: Zoning Page



Note: The enclosure image on the zoning page will depend on your platform model. This example shows the Ultrastar Data60.

Step 2: From the **Zoning Configuration** drop-down list, select **Custom Configuration**:

Figure 134: Zoning Configuration Drop-Down List

Zoning

Current Status

Disabled

Zoning Configuration

Select ▾

Import Configuration

Configuration 1
Configuration 2
Configuration 3
Custom Configuration

A **Custom Configuration** section will appear:

Figure 135: Custom Configuration Section

Zoning

Current Status

Disabled

Zoning Configuration

Custom Configuration ▾

Custom Configuration

Select ▾

Create New

Import Configuration

Import

Step 3: From the **Custom Configuration** drop-down list, select the previously-created custom configuration:

Figure 136: Custom Configuration Drop-Down List

Zoning

Current Status

Disabled

Zoning Configuration

Custom Configuration ▾

Custom Configuration

Select ▾

Create New

Import Configuration

sample
sample_2
Test1

The custom configuration will appear in a new section, locked for editing:

Figure 137: Custom Configuration, Locked

Zoning

Current Status Disabled

Zoning Configuration Custom Configuration ▾

Custom Configuration Test1 ▾ Create New

Import Configuration Import

Test1 Enable 📄 🔍 🗑️

Test1A ✎

■ Color Code port0 x Delete Zone

🔒 Double Click to edit

slot6 x slot7 x slot8 x slot9 x

slot10 x slot11 x

Add New Zone

Step 4: Double-click the configuration to unlock it:

Figure 138: Custom Configuration, Unlocked

Zoning

Current Status

Disabled

Zoning Configuration

Custom Configuration ▾

Custom Configuration

Test1 ▾

Create New

Import Configuration

Import

Test1

Enable

↩

📄

🗑

Test1A ✎

■

Color Code

port0 ✕

Delete Zone

• slot6 ✕

• slot7 ✕

• slot8 ✕

• slot9 ✕

• slot10 ✕

• slot11 ✕

Add New Zone

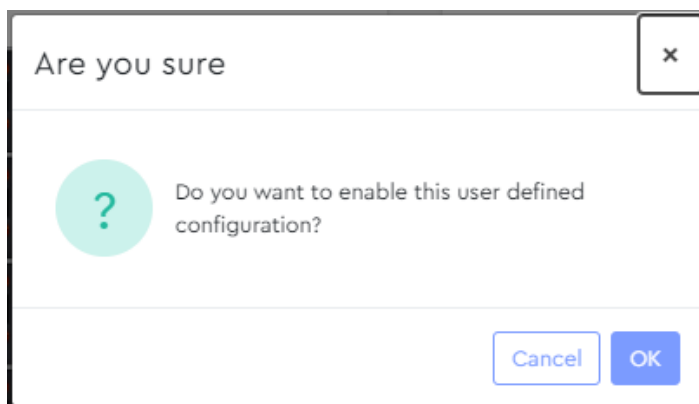
Step 5: Click the toggle switch next to the configuration name to enable the configuration:

Figure 139: Configuration Toggle Switch

Test1

Enable

A dialogue box will appear, prompting the user to confirm the configuration:

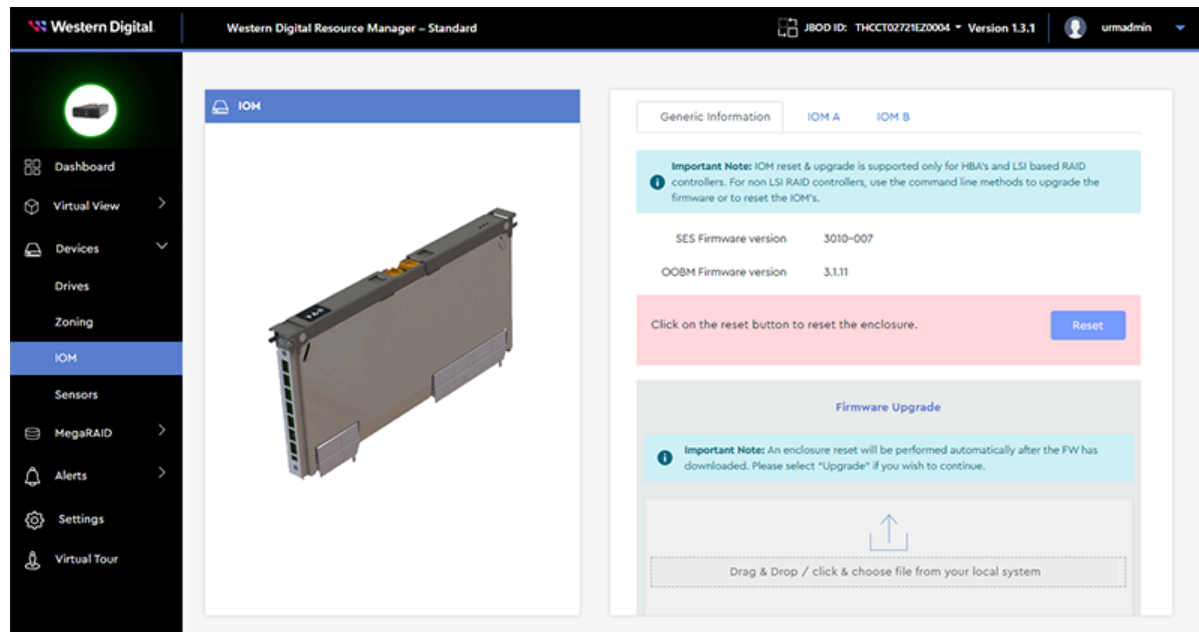
Figure 140: Enable Configuration Dialogue Box

Step 6: Click the **OK** button to enable the configuration.

Result: The selected zoning configuration is now enabled.

3.4.3 IOM

The **IOM** page provides controls for upgrading firmware, resetting the enclosure and/or IOMs, setting the enclosure nickname, and configuring OOBM settings.



3.4.3.1 Upgrading Enclosure Firmware

This procedure provides instructions for upgrading enclosure firmware using the Resource Manager Standard Edition application.

Before you begin:

1. Follow the instructions in your platform's *User Guide* to download new firmware from the support portal and unzip/extract the files to the host server.
2. Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

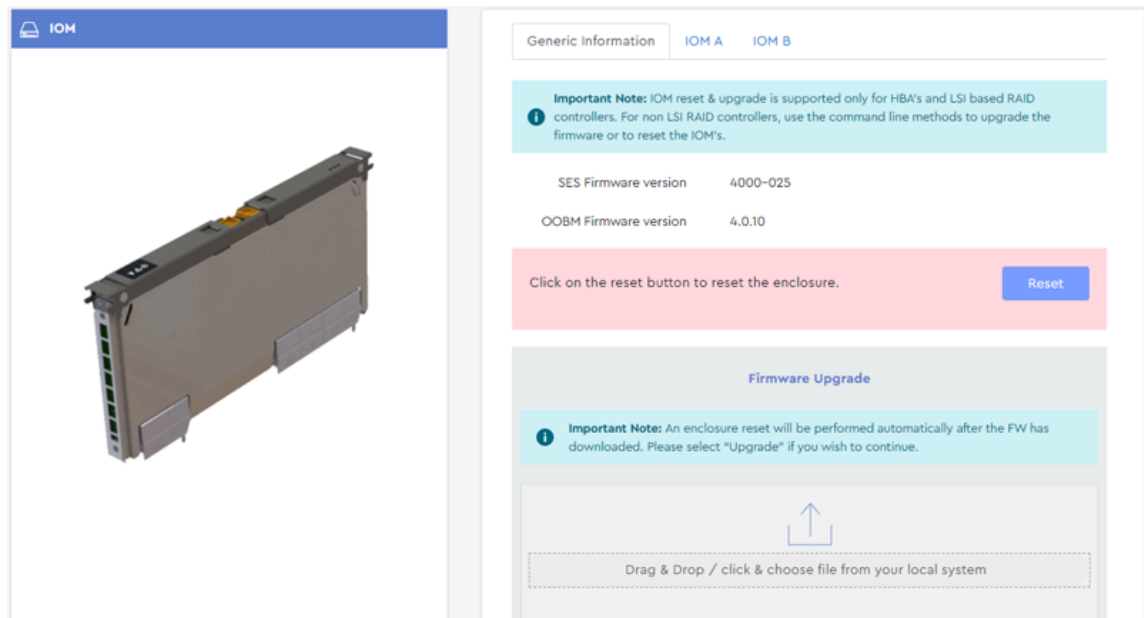


Important: IOM reset & upgrade is supported only for HBAs and LSI-based RAID controllers. For non LSI RAID controllers, use command line methods to upgrade the firmware or to reset the IOM's.

Step 1: From the navigation bar, select **Devices > IOM**.

The **IOM** page will be displayed:

Figure 142: IOM Page



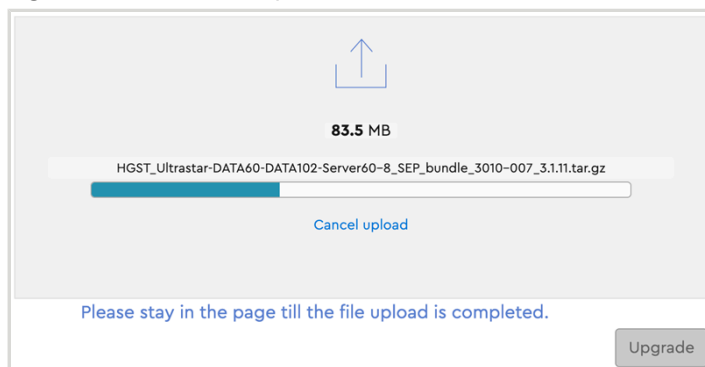
Step 2: On the **Generic Information** tab, take note of the current **OOBM Firmware version** and **SES Firmware version**. These will be used to verify a successful firmware upgrade at the end of this procedure.

Step 3: Drag and drop the previously unzipped/extracted firmware file onto the **Drag & Drop** area.

- a. Alternately, click **Drag & Drop**. This will open your operating system's file explorer. Then navigate to the appropriate directory on the host and select the previously unzipped/extracted firmware file.

An upload status will be displayed, showing the upload progress:

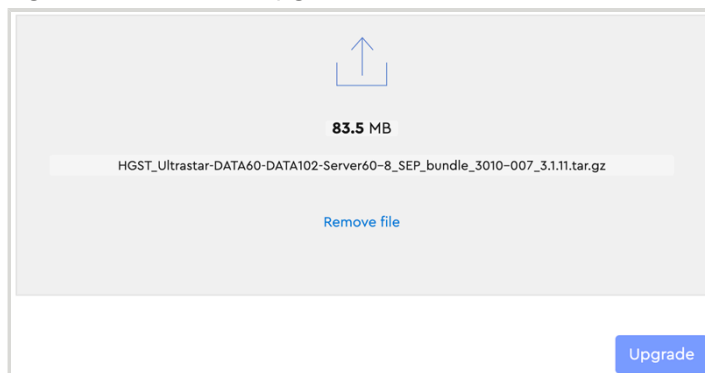
Figure 143: Firmware Upload



Caution: An enclosure reset will be performed automatically after this step!

Step 4: When the firmware file is done uploading, click the **Upgrade** button.

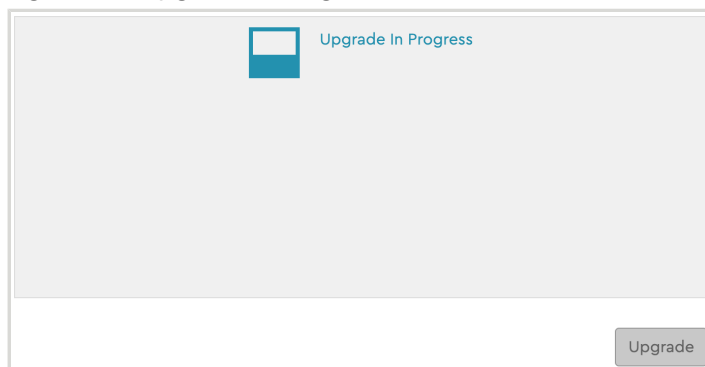
Figure 144: Firmware Upgrade



Important: Due to the firmware image being a .tar.gz file, the enclosure has to unpack and load the firmware onto the respective ICs, which may take up to 15 minutes. Once the **Upgrade** button has been clicked, wait 20 minutes to ensure the enclosure has time to perform this process.

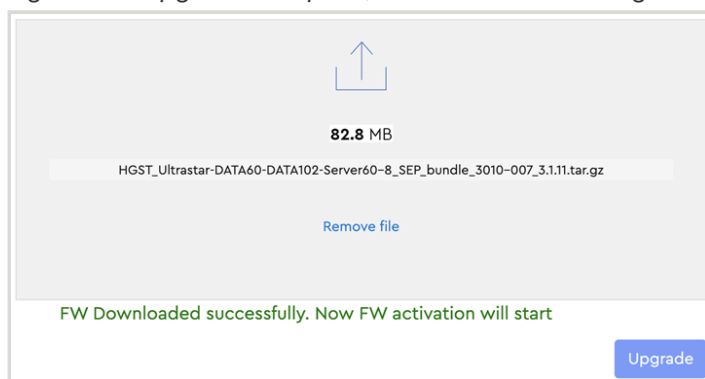
The user is notified that a firmware upgrade is in progress:

Figure 145: Upgrade in Progress



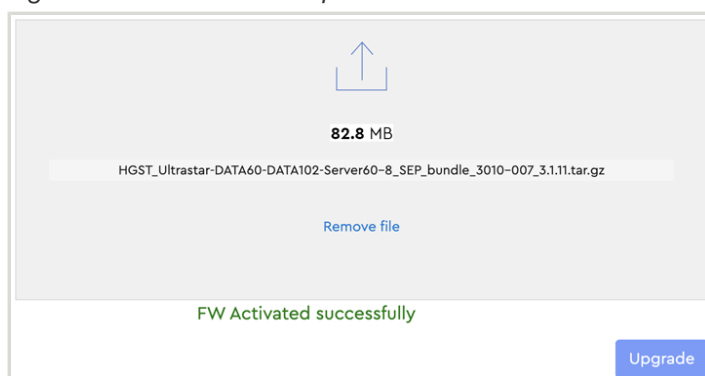
When the upgrade is complete, the user is notified that the firmware will be activated:

Figure 146: Upgrade Complete, FW Activation Starting



When the activation is complete, the user is notified that the activation was successful:

Figure 147: Activation Complete



Step 5: On the **Generic Information** tab, compare the upgraded **OOBM Firmware version** and **SES Firmware Version** to the versions noted prior to the upgrade, and verify that the upgrade was successful.

Result: The enclosure firmware is now upgraded.

3.4.3.2 Resetting the Enclosure

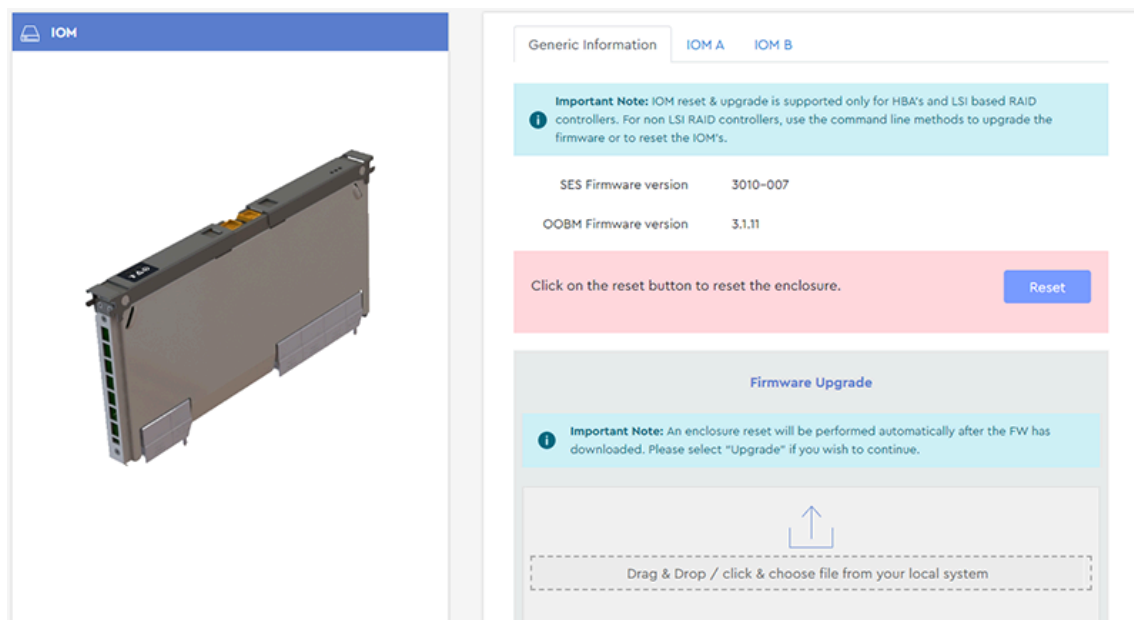
This procedure provides instructions for resetting the enclosure using the Resource Manager Standard Edition application.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **Devices > IOM**.

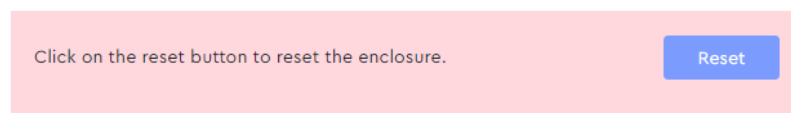
The **IOM** page will be displayed:

Figure 148: IOM Page

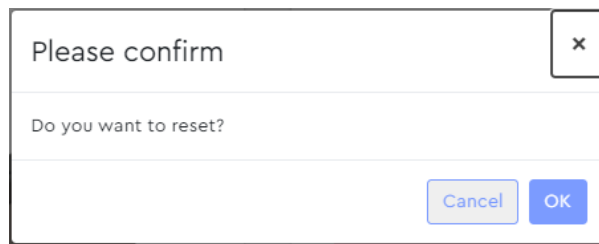


Step 2: On the **Generic Information** tab, click the **Reset** button to reset the enclosure:

Figure 149: Reset Button

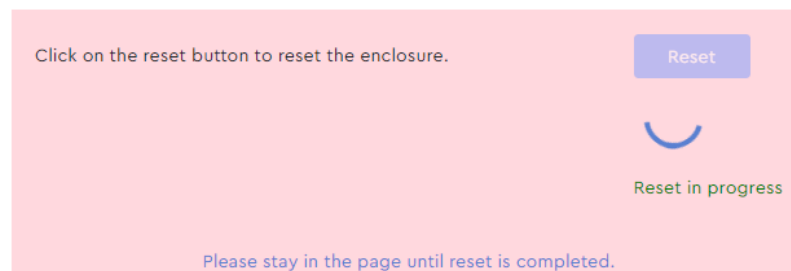


A dialogue box will appear, prompting the user to confirm the reset:

Figure 150: Confirm Reset Dialogue Box

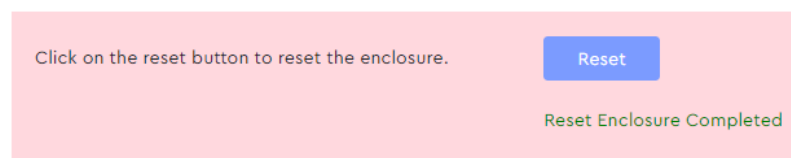
Step 3: Click the **OK** button.

The user will be notified that an enclosure reset is in-progress:

Figure 151: Reset in Progress

Note: Do not navigate away from this page until the enclosure reset is completed.

The user will be notified when the enclosure reset is completed:

Figure 152: Reset Completed

Result: The enclosure has now been reset.

3.4.3.3 Resetting the IOM(s)

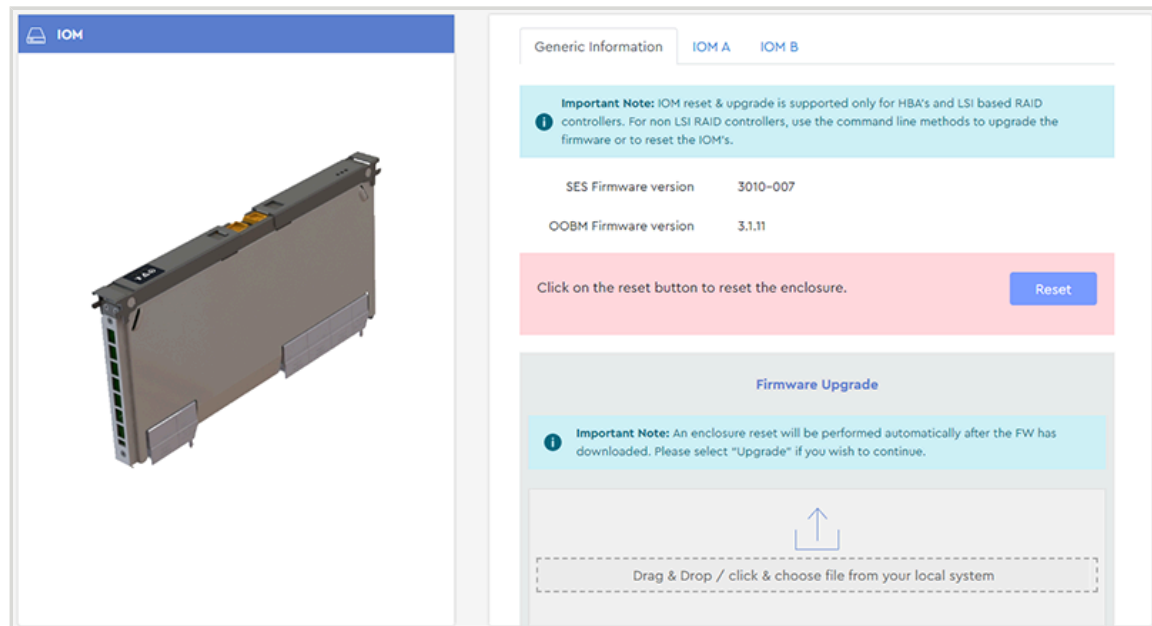
This procedure provides instructions for resetting the IOM(s) using the Resource Manager Standard Edition application.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **Devices > IOM**.

The **IOM** page will be displayed:

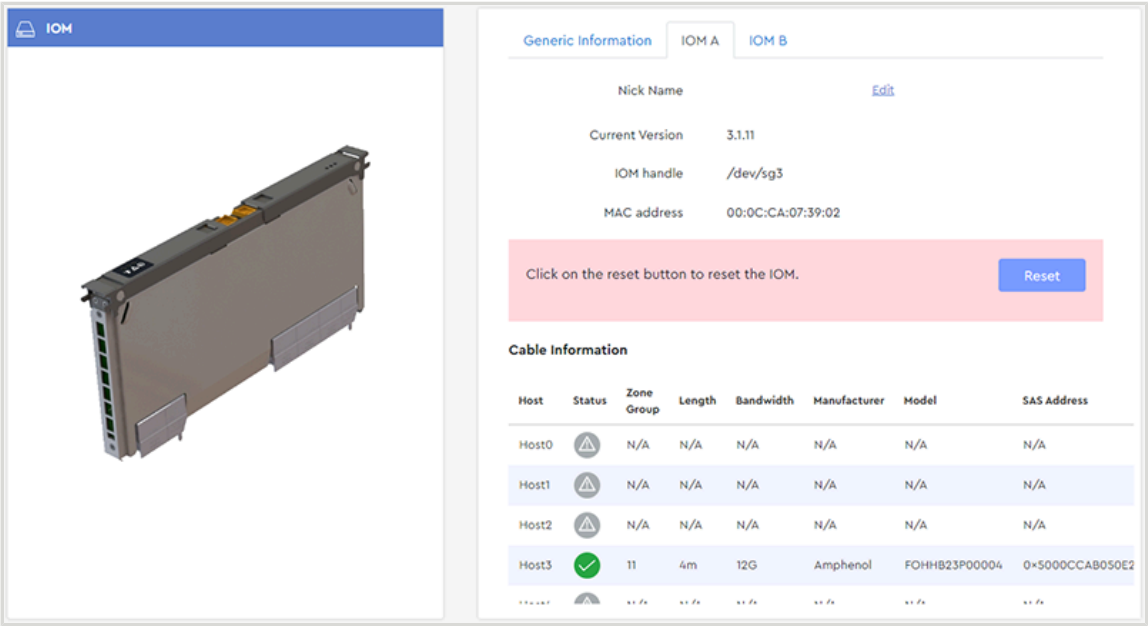
Figure 153: IOM Page



Step 2: Click the **IOM A** or **IOM B** tab.

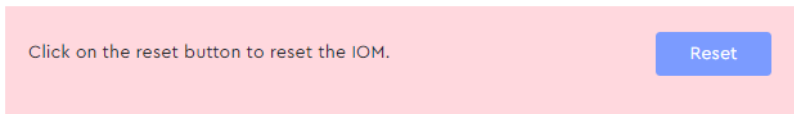
The page for that IOM will be displayed:

Figure 154: IOM A



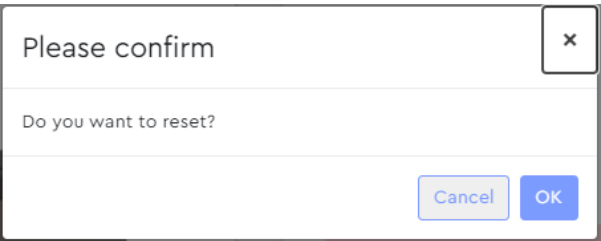
Step 3: Click the **Reset** button to reset the IOM.

Figure 155: Reset IOM

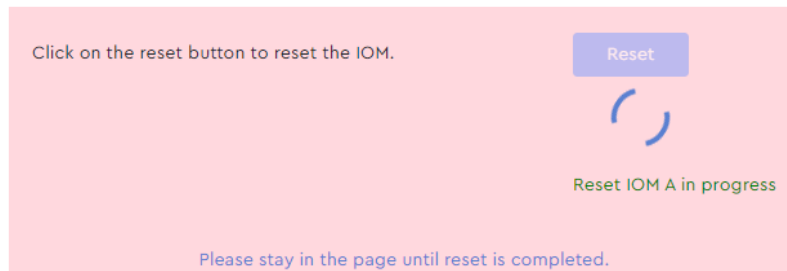


A dialogue box will appear, prompting the user to confirm the reset:

Figure 156: Confirm Reset Dialogue Box

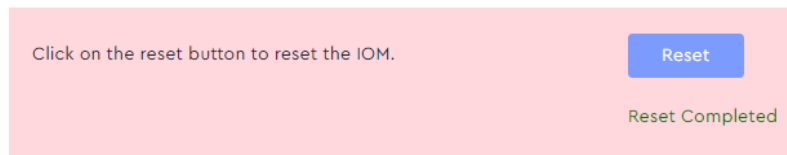


Step 4: Click the **OK** button.
The user will be notified that an IOM reset is in-progress:

Figure 157: Reset in Progress

Note: Do not navigate away from this page until the IOM reset is completed.

When the IOM reset is completed, the user will be notified:

Figure 158: Reset Completed

Result: The IOM(s) have now been reset.

3.4.3.4 Setting the Enclosure Nickname

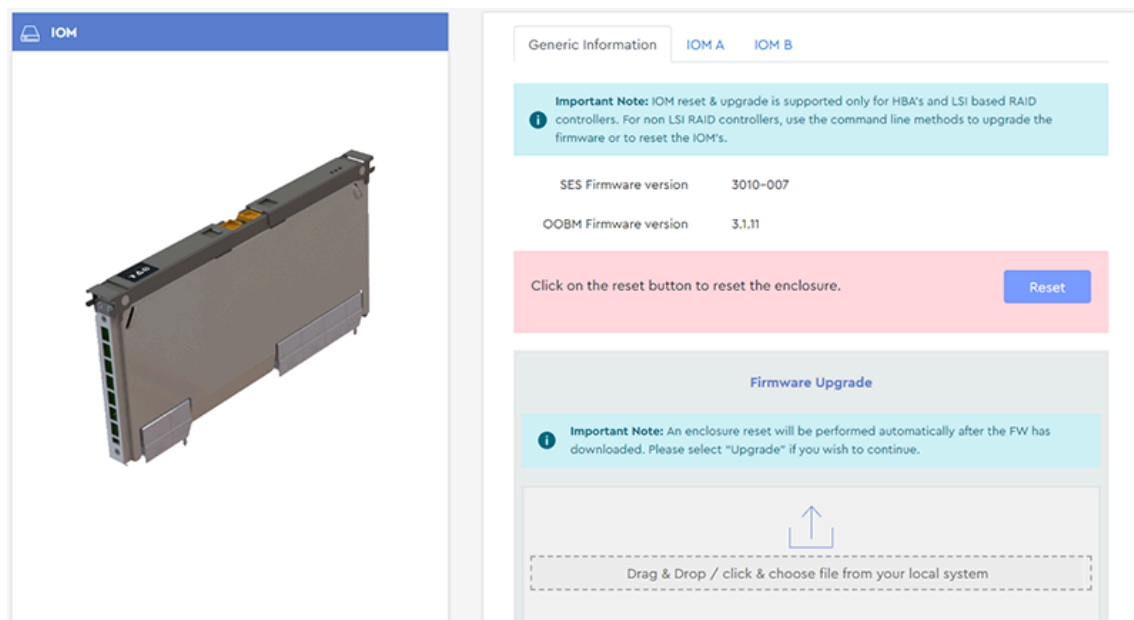
This procedure provides instructions for setting the enclosure nickname using the Resource Manager Standard Edition application.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **Devices > IOM**.

The IOM page will be displayed:

Figure 159: IOM Page



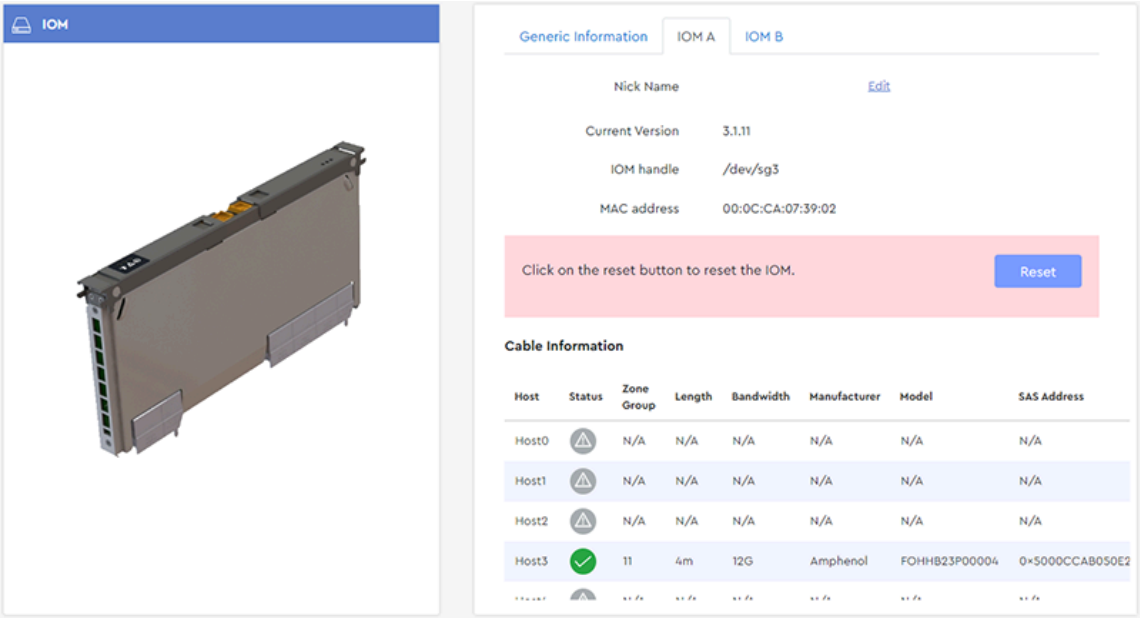
Step 2: Click the **IOM A** or **IOM B** tab.



Note: The enclosure nickname is accessible from either IOM.

The page for that IOM will be displayed:

Figure 160: IOM A



Step 3: Click **Edit** next to the **Nick Name** field.
This turns the enclosure nickname into an editable field:

Figure 161: Nickname Field



Step 4: Enter the desired name for the enclosure into the **Nick Name** field. Then click **Save**.
When the nickname has been saved, the user will be notified:

Figure 162: Nickname Set



Result: The enclosure nickname has now been set.

3.4.3.5 Configuring OOBM Settings

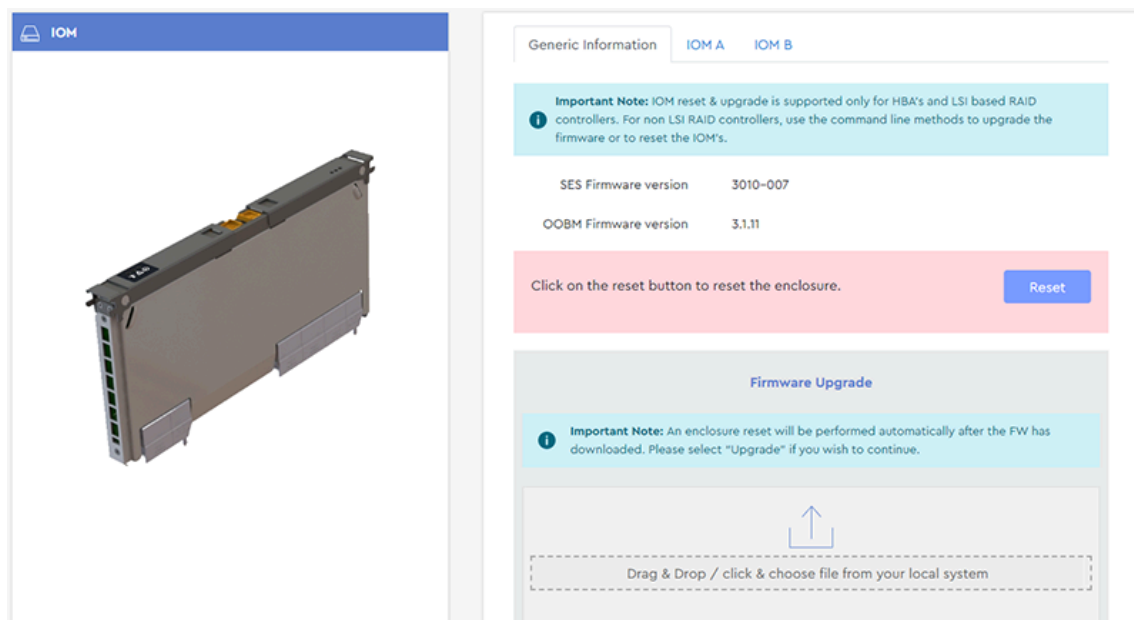
This procedure provides instructions for configuring the Out-of-Band Management settings using the Resource Manager Standard Edition application.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **Devices > IOM**.

The IOM page will be displayed:

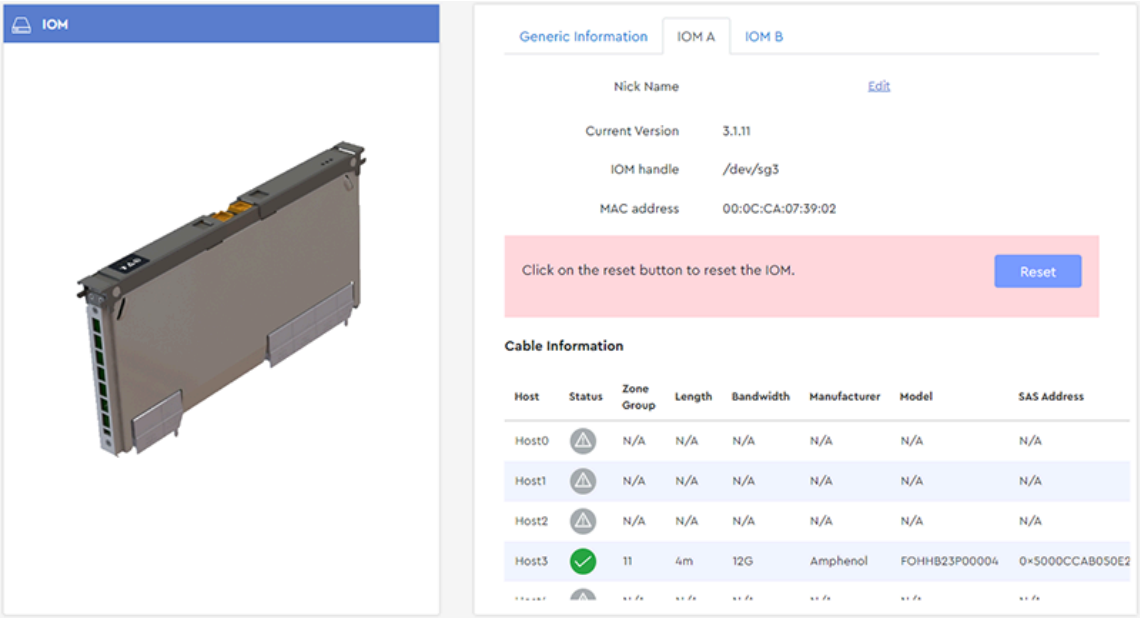
Figure 163: IOM Page



Step 2: Click the **IOM A** or **IOM B** tab.

The page for that IOM will be displayed:

Figure 164: IOM A



- Step 3:** Scroll down to the **OOBM Configuration** section, and select the radio button for either **DHCP** or **Static**.
- Step 4:** If you selected **Static**, enter the desired IP address, netmask, and gateway into the **IP address**, **Netmask**, and **Gateway** fields in the **Add/Edit OOBM Configuration** section.
- Step 5:** Click the **Save** button.

The user will be notified when the OOBM configuration details have been updated:

Figure 165: OOBM Configuration Set



Result: The OOBM configuration details have now been set.

3.4.3.6 Checking Cable Information (IOM)

This procedure provides instructions for checking detailed information about attached cables from the **IOM** device page.

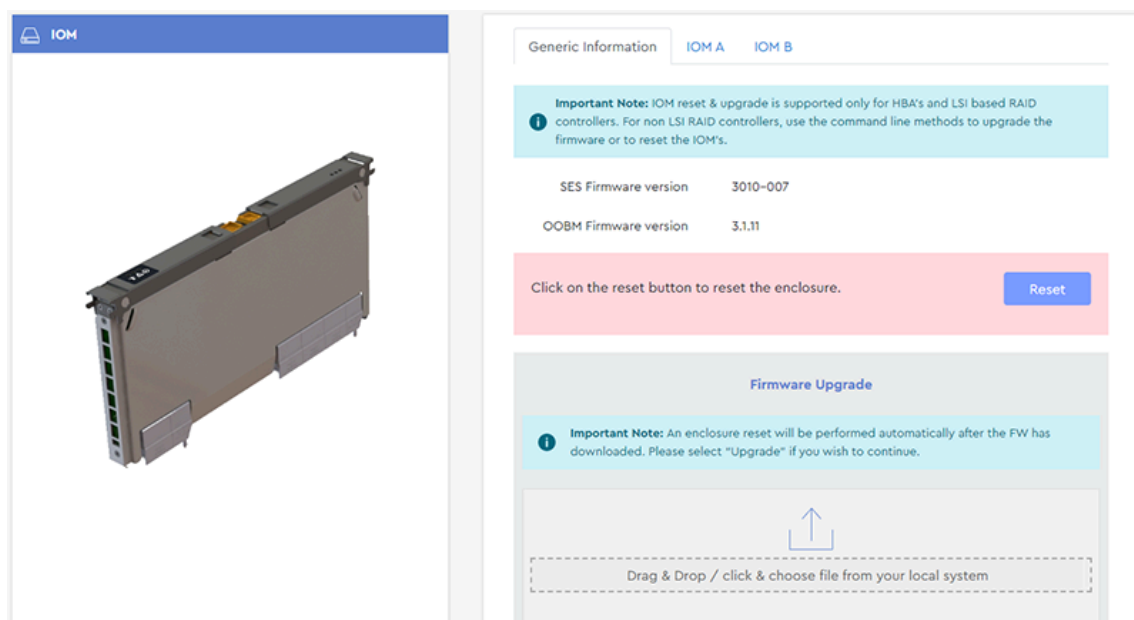
Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.



Note: To view summary information about attached cables, see [Checking Cable Information \(Rear\) \(page 48\)](#).

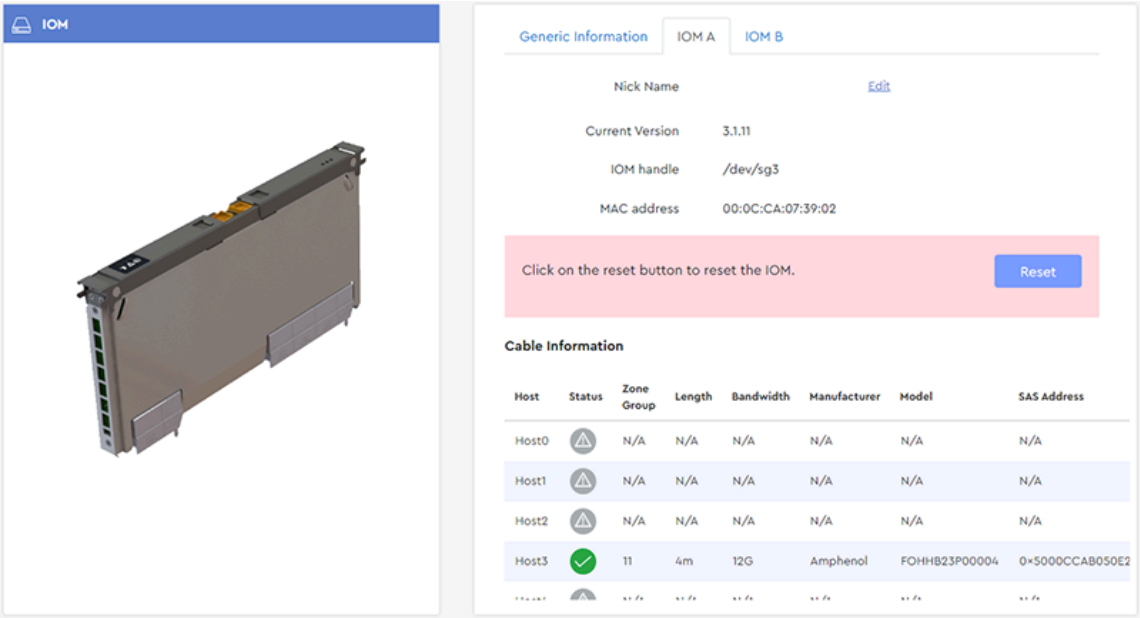
Step 1: From the navigation bar, select **Devices > IOM**.
The **IOM** page will be displayed:

Figure 166: IOM Page



Step 2: Click the **IOM A** or **IOM B** tab.
The page for that IOM will be displayed:

Figure 167: IOM A Tab









Step 3: Scroll down to the **Cable Information** section to view detailed information about port connectivity status and attached cables.

Figure 168: Cable Information

Cable Information							
Host	Status	Zone Group	Length	Bandwidth	Manufacturer	Model	SAS Address
Host0	⚠	N/A	N/A	N/A	N/A	N/A	N/A
Host1	⚠	N/A	N/A	N/A	N/A	N/A	N/A
Host2	⚠	N/A	N/A	N/A	N/A	N/A	N/A
Host3	✓	11	4m	12G	Amphenol	FOHHB23P00004	0x5000CCAB050E2
Host4	⚠	N/A	N/A	N/A	N/A	N/A	N/A
Host5	✓	13	2m	12G	FCI Electronics	10112041-2020LF	0x500062B2060991

Step 4: Hover your cursor over any icon in the **Status** column to view a tooltip, indicating the port connectivity status, cable health, and cable type (passive or active).

Figure 169: Tooltip Explanation of Icons

Cable Information							
Host	Status	Zone Group	Length	Bandwidth	Manufacturer	Model	SAS Address
Host0		N/A	N/A	N/A	N/A	N/A	N/A
Host1		N/A	N/A	N/A	N/A	N/A	N/A
Host2		N/A	N/A	N/A	N/A	N/A	N/A
Host3		11	4m	12G	Amphenol	FOHKB23P00004	0x5000CCAB050E2
Host4		N/A	N/A	N/A	N/A	N/A	N/A
Host5		13	2m	12G	FCI Electronics	10112041-2020LF	0x500062B2060991

Result: Detailed information about attached cables has now been viewed.

3.4.3.7 Downloading SES PHY Counters

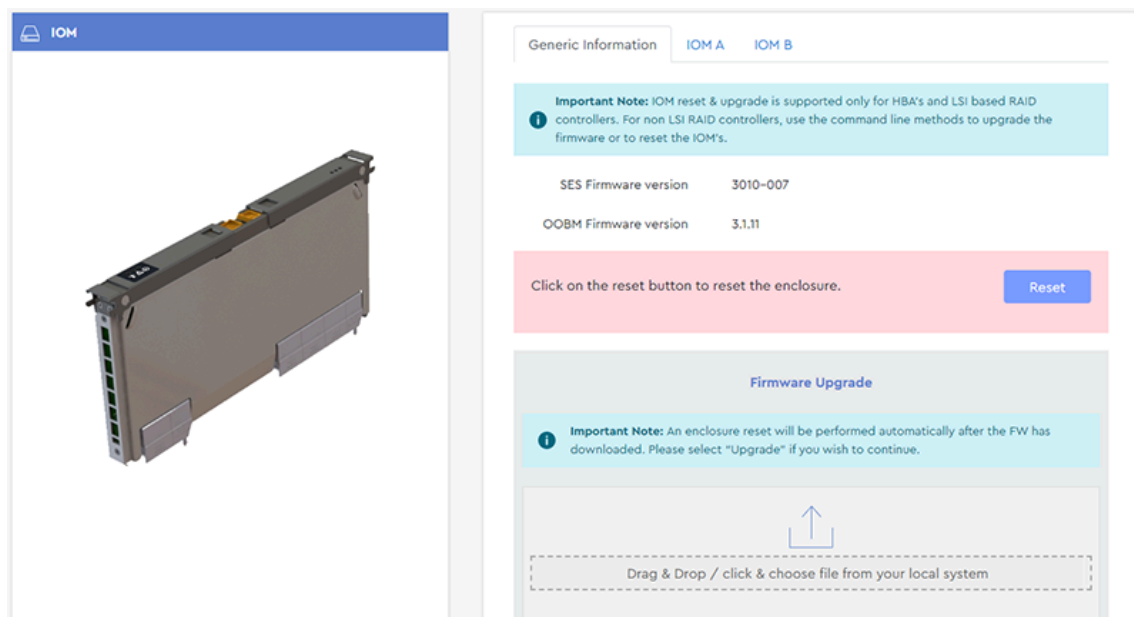
This procedure provides instructions for downloading SES PHY counters.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **Devices > IOM**.

The **IOM** page will be displayed:

Figure 170: IOM Page




Step 2: Click the **IOM A** or **IOM B** tab.

The page for that IOM will be displayed:

Figure 171: IOM A Tab

IOM



Generic InformationIOM A IOM B

Nick Name

Edit

Current Version

3.1.11

IOM handle

/dev/sg3

MAC address

00:0C:CA:07:39:02

Click on the reset button to reset the IOM.

Reset

Cable Information

Host	Status	Zone Group	Length	Bandwidth	Manufacturer	Model	SAS Address
Host0	⚠	N/A	N/A	N/A	N/A	N/A	N/A
Host1	⚠	N/A	N/A	N/A	N/A	N/A	N/A
Host2	⚠	N/A	N/A	N/A	N/A	N/A	N/A
Host3	✅	11	4m	12G	Amphenol	FOHHB23P00004	0+5000CCAB050E2
...	⚠	N/A	N/A	N/A	N/A	N/A	N/A

Step 3: Scroll down to the **SES Phy Counters** section.

Figure 172: SES Phy Counters Section

SES Phy Counters

Download

Step 4: Click the **Download** link to download the SES PHY counters.
A .txt file of the SES PHY counters will appear in the download directory.

Result: The SES PHY counters have now been downloaded.

3.4.4 Sensors

The **Sensors** page provides health status, readings, and limits for all non-discrete sensors in the enclosure.

Western Digital

Western Digital Resource Manager – Standard

JBOD ID: THCCT0272HEZ0004 Version 1.3.1 urmadmin

Dashboard

Virtual View

Devices

Drives

Zoning

IOM

Sensors

MegaRAID

Alerts

Settings

Virtual Tour

Sensors

Fan

Thermal

Voltage

Current

Discrete

#	Status	Sensor ID	Sensor Type	Reading (RPM)	Lower NonCritical	Upper NonCritical	Lower Critical	Upper Critical
1	✓	FAN ENCL 1	Cooling	8880.00	N/A	N/A	N/A	N/A
2	✓	FAN ENCL 2	Cooling	8830.00	N/A	N/A	N/A	N/A
3	✓	FAN ENCL 3	Cooling	8880.00	N/A	N/A	N/A	N/A
4	✓	FAN ENCL 4	Cooling	8860.00	N/A	N/A	N/A	N/A
5	✓	FAN IOM 1	Cooling	20470.00	N/A	N/A	N/A	N/A
6	✓	FAN IOM 2	Cooling	20470.00	N/A	N/A	N/A	N/A
7	✓	FAN PSU A	Cooling	20470.00	N/A	N/A	N/A	N/A
8	✓	FAN PSU B	Cooling	2570.00	N/A	N/A	N/A	N/A

3.4.4.1 Checking Sensors

This procedure provides instructions for checking enclosure sensors using the **Sensors** page of the Resource Manager Standard Edition application. To check sensors using the internal, front, and rear virtual views, see [Virtual View \(page 39\)](#).

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **Devices > Sensors**.

The **Sensors** page will be displayed:

Figure 174: Sensors Page

#	Status	Sensor ID	Sensor Type	Reading (RPM)	Lower NonCritical	Upper NonCritical	Lower Critical	Upper Critical
1	OK	FAN ENCL 1	Cooling	8880.00	N/A	N/A	N/A	N/A
2	OK	FAN ENCL 2	Cooling	8830.00	N/A	N/A	N/A	N/A
3	OK	FAN ENCL 3	Cooling	8880.00	N/A	N/A	N/A	N/A
4	OK	FAN ENCL 4	Cooling	8860.00	N/A	N/A	N/A	N/A
5	OK	FAN IOM 1	Cooling	20470.00	N/A	N/A	N/A	N/A
6	OK	FAN IOM 2	Cooling	20470.00	N/A	N/A	N/A	N/A
7	OK	FAN PSU A	Cooling	20470.00	N/A	N/A	N/A	N/A
8	OK	FAN PSU B	Cooling	2570.00	N/A	N/A	N/A	N/A

Enclosure sensor information is organized into the following tabs by sensor type:

- **Fan** – cooling sensors for enclosure fans, IOM fans, and PSU fans
- **Thermal** – temperature sensors for drive slots, IOMs, baseboard(s), primary and secondary expanders, and PSUs
- **Voltage** – voltage sensors for PSUs and IOMs
- **Current** – current sensors for PSUs and IOMs
- **Discrete** – discrete power supply sensors for PSUs and enclosure cover (door)

Step 2: Click the tab for the desired sensor type. The following image shows the **Voltage** tab.

Sensors								
Fan Thermal Voltage Current Discrete								
#	Status	Sensor ID	Sensor Type	Reading (Volt)	Lower NonCritical	Upper NonCritical	Lower Critical	Upper Critical
1	✓	VOLT PSU A AC	Voltage sensor	228.00	13.5 %	13.5 % (above nominal voltage)	16.5 % (below nominal voltage)	16.5 %
2	✓	VOLT PSU A 12V	Voltage sensor	12.19	7.5 %	5.0 % (above nominal voltage)	10.0 % (below nominal voltage)	10.0 %
3	✓	VOLT PSU B AC	Voltage sensor	227.00	13.5 %	13.5 % (above nominal voltage)	16.5 % (below nominal voltage)	16.5 %
4	✓	VOLT PSU B 12V	Voltage sensor	12.21	7.5 %	5.0 % (above nominal voltage)	10.0 % (below nominal voltage)	10.0 %
5	✓	VOLT IOM A 5V	Voltage sensor	5.07	7.5 %	5.0 % (above nominal voltage)	10.0 % (below nominal voltage)	10.0 %
6	✓	VOLT IOM A 12V	Voltage sensor	12.00	7.5 %	5.0 % (above nominal voltage)	10.0 % (below nominal voltage)	10.0 %
7	✓	VOLT IOM B 5V	Voltage sensor	5.07	7.5 %	5.0 % (above nominal voltage)	10.0 % (below nominal voltage)	10.0 %
8	✓	VOLT IOM B 12V	Voltage sensor	12.00	7.5 %	5.0 % (above nominal voltage)	10.0 % (below nominal voltage)	10.0 %

Step 3: Review the information for the desired sensor(s). Each listing contains the sensor's current reading, upper and lower non-critical limits, upper and lower critical limits, and a status based on the current reading in comparison to the limits.

Step 4: Repeat these steps as needed to check other sensors.

Result: Checking enclosure sensors using the **Sensors** page is now complete.

3.5 MegaRAID

The **MegaRAID** section provides information about all MegaRAID controllers detected in the host, and management controls for drive identification LEDs, grouping drives, assigning RAID levels, and allocating capacity to logical drives.



Note: The **MegaRAID** section will only be visible (accessible) in the navigation bar if Resource Manager Standard Edition detects a MegaRAID controller installed in the host.

3.5.1 Controller

The **Controller** page displays information for the selected MegaRAID controller, as well as controls for switching between JBOD & RAID modes, enabling the controller alarm, resetting firmware, upgrading firmware, and enabling/disabling SES monitoring.

The screenshot shows the Western Digital Resource Manager - Standard interface. The left sidebar contains navigation options: Dashboard, Virtual View, Devices, MegaRAID, Controller (selected), RAID Configuration, Logical Drives, Physical Drives, Alerts, Settings, and Virtual Tour. The main content area is titled 'MegaRAID Controller' and shows the following information:

- Mode:** JBOD (selected) / RAID
- Controller ID:** AVAGO MegaRAID SAS 9480-8i8e
- Background process:** 2 Background process in progress
- Capacity:**
 - used: 94.598 TB
 - Total: 1,209.921 TB
 - Free Space: 7.819%
- Controller Settings:**
 - Health: OK
 - Controller ID: 2
 - Current Mode: RAID
 - FW Package Ver: 51.20.0-4342
 - Alarm: ON
 - SES Monitoring: OFF
- Controller Information:**
 - Serial No: SP91007993
 - Vendor ID: 0x1000
 - Flash Size: 16 MB
 - Sub Vendor ID: 0x1000
 - Device ID: 0x14
 - Driver Version: 07.719.03.00
 - Host Interface: PCIE
- Advanced Properties:**
 - NVRAM Present: Yes
 - NVRAM Size: 128 KB
 - BIOS Version: v7.20.01.0_0x07140000
 - Cache Vault:**
 - Serial Number: 27980
 - Model: CVP405
 - State: Optimal
 - Temperature: 31



Note: Under the **Advanced Properties** section, *N/A* next to **Cache Vault** indicates that the cache vault is not connected.



Caution: Switching between RAID/JBOD modes requires a host reboot and may result in data loss. Please clear all existing configurations before switching modes.

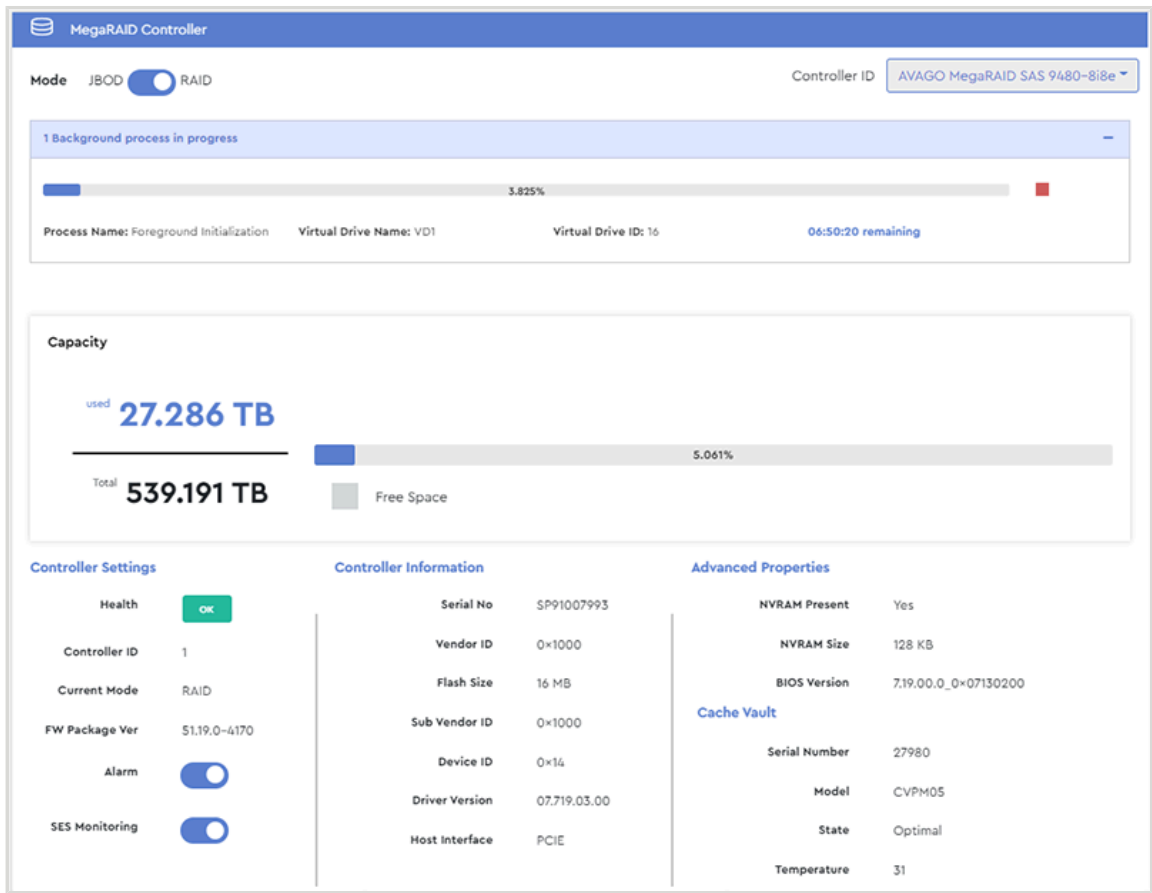
3.5.1.1 Checking Background Processes

This procedure provides instructions for checking the status of background processes.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

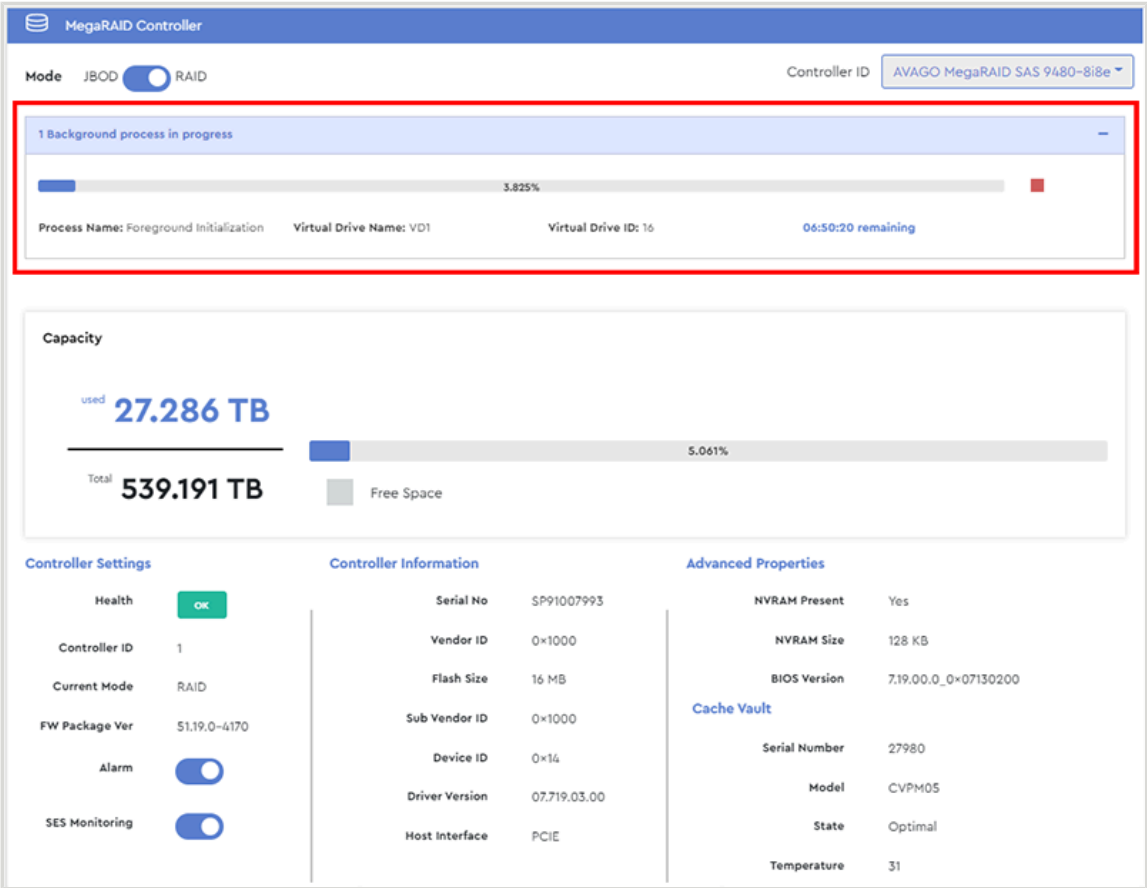
- Step 1:** From the navigation bar, select **MegaRAID > Controller**.
The **MegaRAID Controller** page will be displayed:

Figure 177: MegaRAID Controller Page



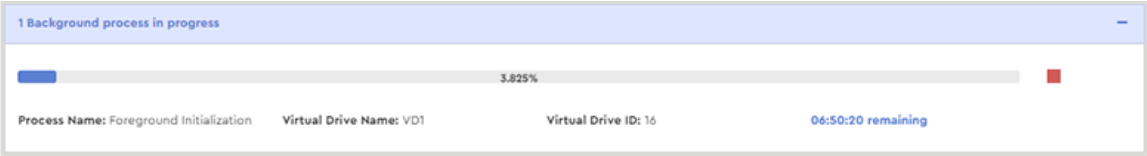
- Step 2:** If any background processes are in progress, they will be listed at the top of the page:

Figure 178: Background Processes



Step 3: Each background process will have its own window displaying its progress percentage, process name, virtual drive name and ID, and the time remaining until completion.

Figure 179: Background Process Details



Result: The status of background processes has now been checked.

3.5.1.2 Starting Patrol Read

This procedure provides instructions for starting or scheduling a Patrol Read, which will scan all drive sectors of one or multiple virtual drive groups to ensure read/write capability.

Before you begin:

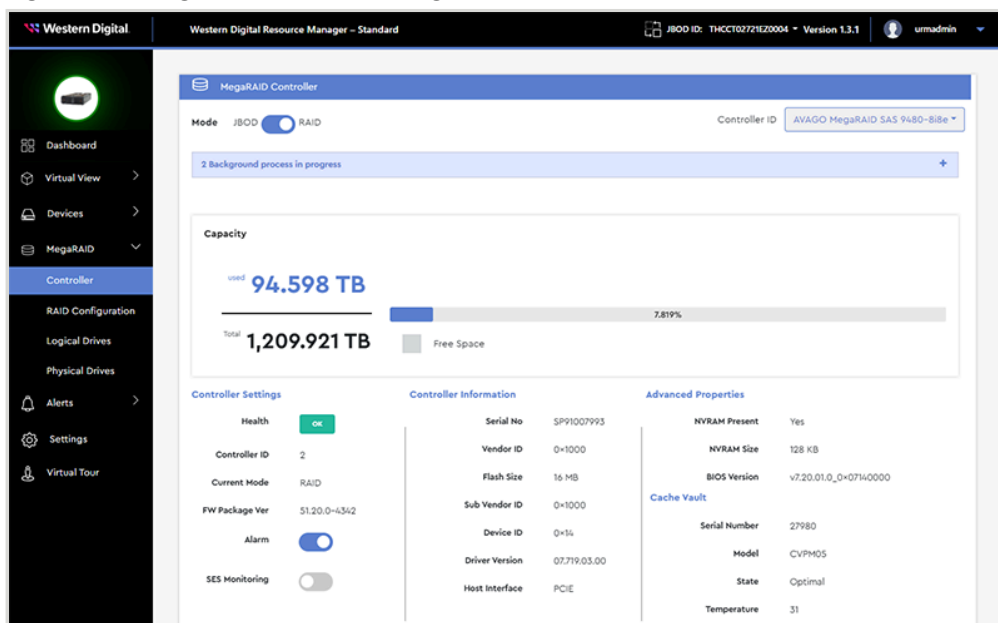
- 1. Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

- Follow the instructions in [Creating a Drive Group / RAID Configuration \(page 129\)](#) to create at least one drive group/RAID configuration.

Step 1: From the navigation bar, select **MegaRAID > Controller**.

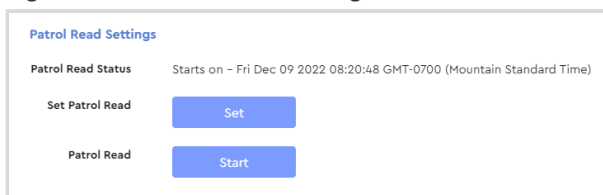
The **MegaRAID Controller** page will be displayed:

Figure 180: MegaRAID Controller Page



Step 2: Scroll down to the **Patrol Read Settings** section.

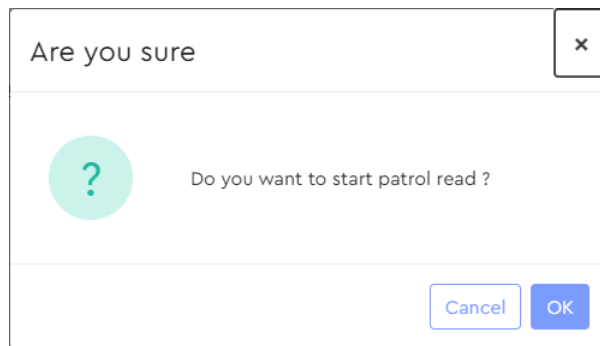
Figure 181: Patrol Read Settings



Step 3: To start a Patrol Read scan immediately using existing settings, click the **Start** button and follow the instructions below. To modify the Patrol Read settings, proceed to step 4 ([page 119](#)).

If you clicked the **Start** button, a confirmation dialog box will appear:

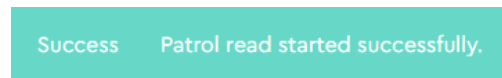
Figure 182: Patrol Read Confirmation



- a. Click the **OK** button.

A success message will appear, indicating that the Patrol Read scan has started:

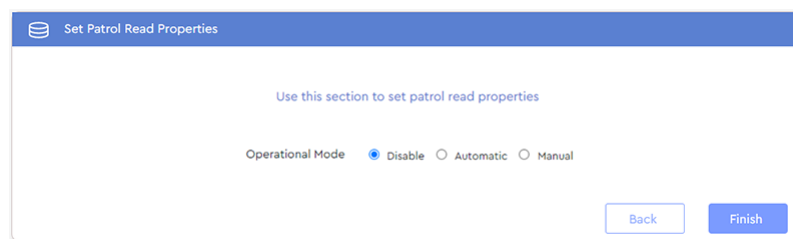
Figure 183: Patrol Read Success



- Step 4:** To modify the Patrol Read properties, click the **Set** button.

The **Set Patrol Read Properties** window will appear:

Figure 184: Set Patrol Read Properties



- Step 5:** To set properties for an automatic scan, select the **Automatic** radio button.

The automatic propterties will appear:

Figure 185: Automatic Patrol Read Properties

Set Patrol Read Properties

Use this section to set patrol read properties

Operational Mode

☐ Disable ☒ Automatic ☐ Manual

Maximum Physical Drives Allowed

10

Schedule Patrol Read

Weekly

12/02/2022 08:20 AM

Start Patrol Read Now

Back

Next

- a. In the **Maximum Physical Drives Allowed** field, enter the maximum number of drives to be scanned simultaneously.



Note: The acceptable range is 1 to 240 drives.

- b. In the **Schedule Patrol Read** section, use the drop-down list to select the frequency of the scan:

Figure 186: Scan Frequency

Weekly

Hourly

Daily

Weekly

Monthly

Continuously

- c. Use the date/time field to select the starting date and time of the scan:

Figure 187: Scan Date/Time

<

December 2022

>

Su	Mo	Tu	We	Th	Fr	Sa
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

^

^

^

08 : 20 AM

v

v

v

12/02/2022 08:20 AM

- d. To start the scan now, click to toggle **Start Patrol Read Now** switch to the **ON** position:

Figure 188: Scan Now

Start Patrol Read Now

- e. When you've made your selections, click the **Next** button.
The available drive groups will appear, and all are selected by default:

Figure 189: Automatic Patrol Read Drive Groups

Set Patrol Read Properties

Select the Drive Group to schedule the patrol read

	<input checked="" type="checkbox"/>	Drive Group	Physical Drives	Logical Drives	Capacity
>	<input checked="" type="checkbox"/>	DG0	3	1	27.286 TB
>	<input checked="" type="checkbox"/>	DG1	6	1	27.286 TB
>	<input checked="" type="checkbox"/>	DG2	2	16	5.458 TB
>	<input checked="" type="checkbox"/>	DG3	2	16	9.095 TB
>	<input checked="" type="checkbox"/>	DG4	2	16	21.827 TB

5 Drive Groups selected. Click finish to save the patrol read properties.

Back

Finish

- f. If needed, use the arrows to expand the drive groups and examine the associated logical drives. Or use the checkboxes to deselect drive groups.
- g. When all your selections have been made, click the **Finish** button.

Step 6: To set properties for a manual scan, select the **Manual** radio button.

Figure 190: Manual Patrol Read Properties

Set Patrol Read Properties

Use this section to set patrol read properties

Operational Mode ☐ Disable ☐ Automatic ☒ Manual

Maximum Physical Drives Allowed

Schedule Patrol Read

Start Patrol Read Now ☐

Back Next

- a. In the **Maximum Physical Drives Allowed** field, enter the maximum number of drives to be scanned simultaneously.



Note: The acceptable range is 1 to 240 drives.

- b. In the **Schedule Patrol Read** section, use the date/time field to select the starting date and time of the scan:

Figure 191: Scan Date/Time

<

December 2022

>

Su	Mo	Tu	We	Th	Fr	Sa
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

^

08 : 20 AM

v

12/02/2022 08:20 AM

- c. To start the scan now, click to toggle **Start Patrol Read Now** switch to the **ON** position:

Figure 192: Scan Now

Start Patrol Read Now

- d. When you've made your selections, click the **Next** button.
The available drive groups will appear, and all are selected by default:

Figure 193: Manual Patrol Read Drive Groups

Set Patrol Read Properties

Select the Drive Group to schedule the patrol read

<input checked="" type="checkbox"/>	Drive Group	Physical Drives	Logical Drives	Capacity
> <input checked="" type="checkbox"/>	DG0	3	1	27.286 TB
> <input checked="" type="checkbox"/>	DG1	6	1	27.286 TB
> <input checked="" type="checkbox"/>	DG2	2	16	5.458 TB
> <input checked="" type="checkbox"/>	DG3	2	16	9.095 TB
> <input checked="" type="checkbox"/>	DG4	2	16	21.827 TB

5 Drive Groups selected. Click finish to save the patrol read properties.

Back

Finish

- e. If needed, use the arrows to expand the drive groups and examine the associated logical drives. Or use the checkboxes to deselect drive groups.
- f. When all your selections have been made, click the **Finish** button.

Step 7: A success message will appear at the top of the screen.

Figure 194: Success Message

Success Patrol read saved successfully.

Result: The Patrol Read process is now set up.

3.5.1.3 Upgrading MegaRAID Controller Firmware

This procedure provides instructions for upgrading MegaRAID controller firmware using the Resource Manager Standard Edition application.

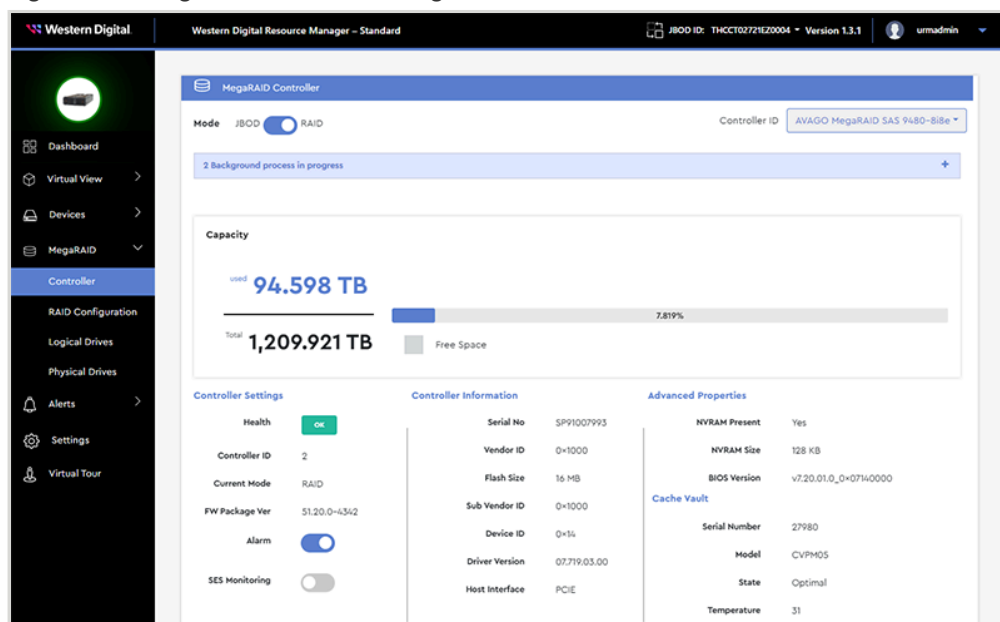
Before you begin:

1. Follow the controller manufacturer's instructions to download new MegaRAID firmware and unzip/extract the files to the host server.
2. Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **MegaRAID > Controller**.

The **MegaRAID Controller** page will be displayed:

Figure 195: MegaRAID Controller Page



Step 2: Scroll down to the **Firmware Upgrade** section, and take note of the **FW Package Ver**. It will be used to verify a successful firmware upgrade at the end of this procedure.

Figure 196: Firmware Package Version

Firmware Upgrade

FW Package Ver 51.19.0-4170

Important Note: MegaRAID controller reset will be performed automatically after the Firmware update is completed.

+ Choose Upload Cancel

Drag & Drop / click on '+ choose' button to upload file from your local system.

- Step 3:** Drag and drop the previously unzipped/extracted firmware file onto the **Drag & Drop** area.
- Alternately, click the **Choose** button. This will open the operating system's file explorer and allow you to navigate to the appropriate directory and select the previously unzipped/extracted firmware file.

Figure 197: Choose Button

Firmware Upgrade

FW Package Ver 51.19.0-4170

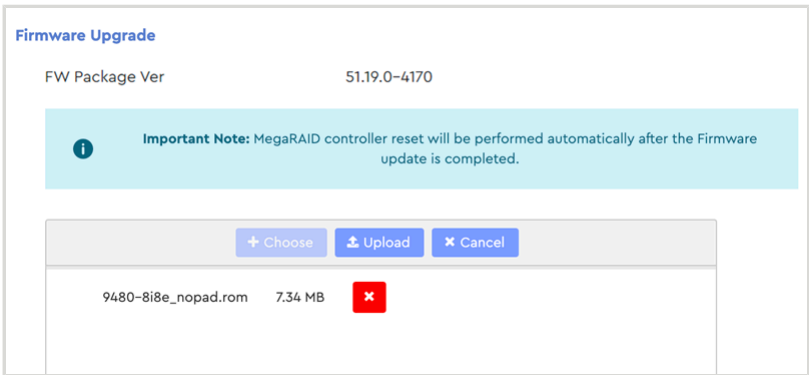
Important Note: MegaRAID controller reset will be performed automatically after the Firmware update is completed.

+ Choose Upload Cancel

Drag & Drop / click on '+ choose' button to upload file from your local system.

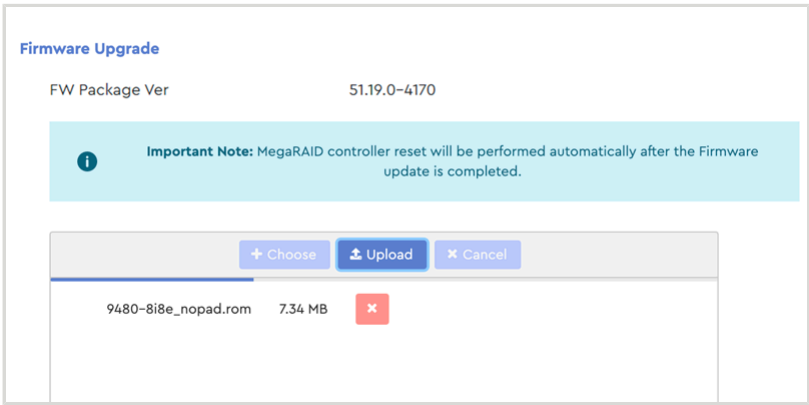
The firmware filename will appear in the upload area:

Figure 198: Firmware Filename



Step 4: Click the **Upload** button.
A progress bar will appear in the upload area:

Figure 199: Upload Progress



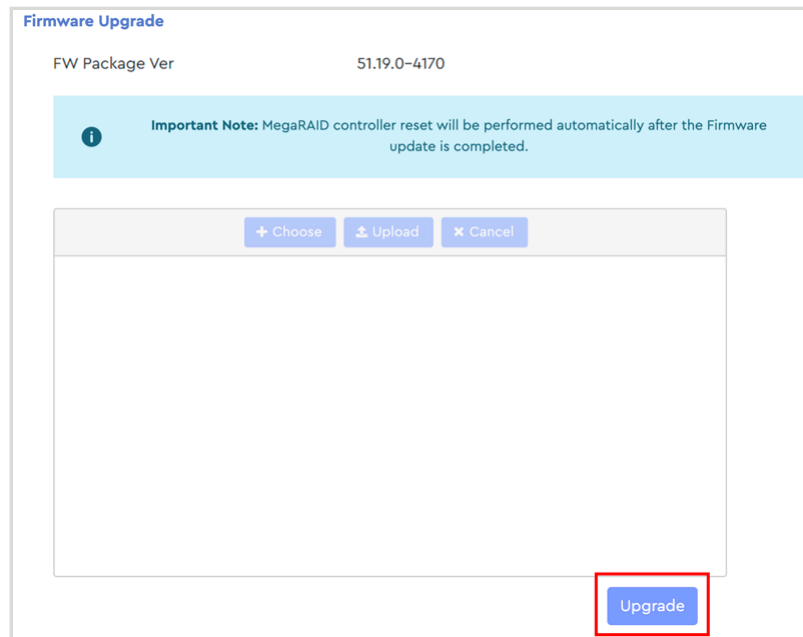
Step 5: When the firmware file is done uploading, a success notification will appear:

Figure 200: Upload Success



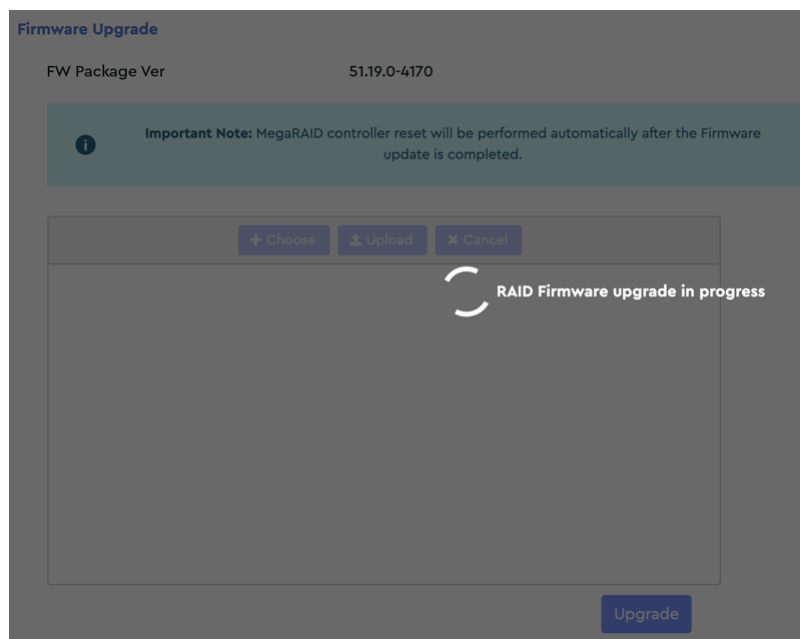
Step 6: As instructed in the success message, click the **Upgrade** button:

Figure 201: Upgrade Button



The page will be overlaid with a progress message:

Figure 202: Upgrade In Progress



When the upgrade is complete, another success message will be displayed:

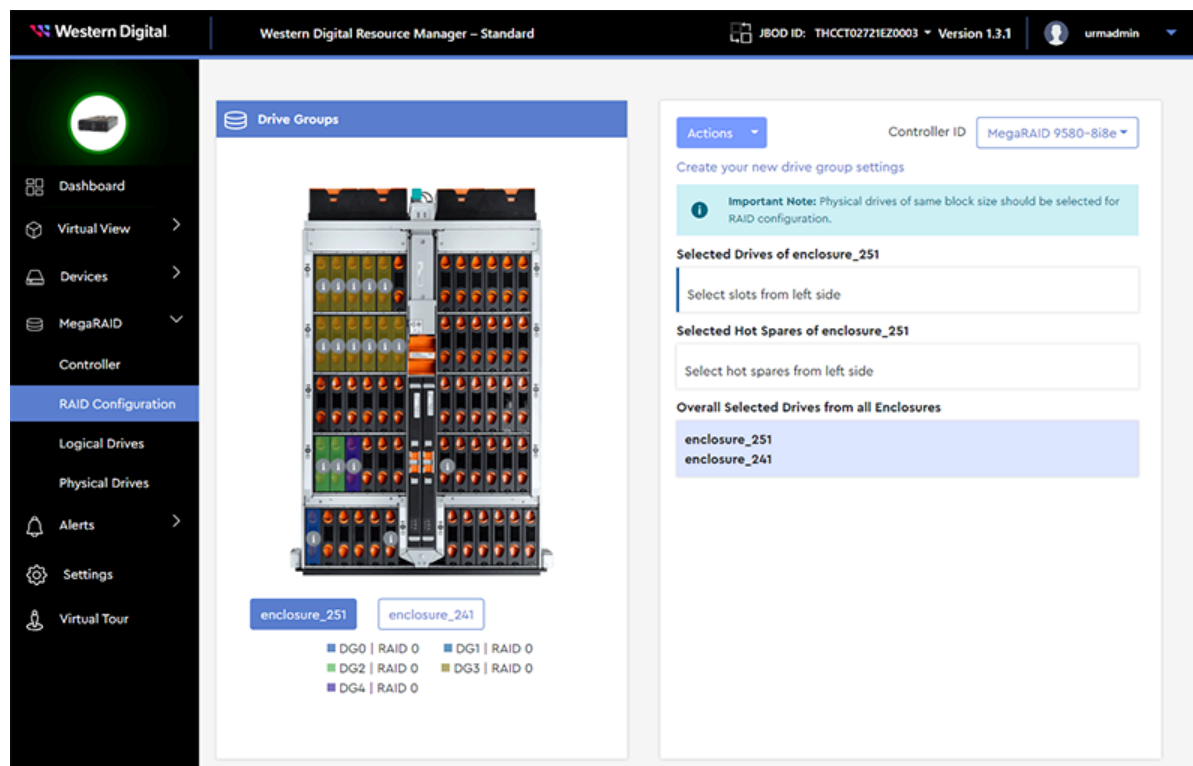
Figure 203: Upgrade Success

Step 7: In the **Firmware Upgrade** section, check the **Current Firmware Version** to ensure that the firmware was upgraded.

Result: The MegaRAID controller firmware is now upgraded.

3.5.2 RAID Configuration

The **RAID Configuration** page displays settings and controls for configuring a RAID.



3.5.2.1 Creating a Drive Group / RAID Configuration

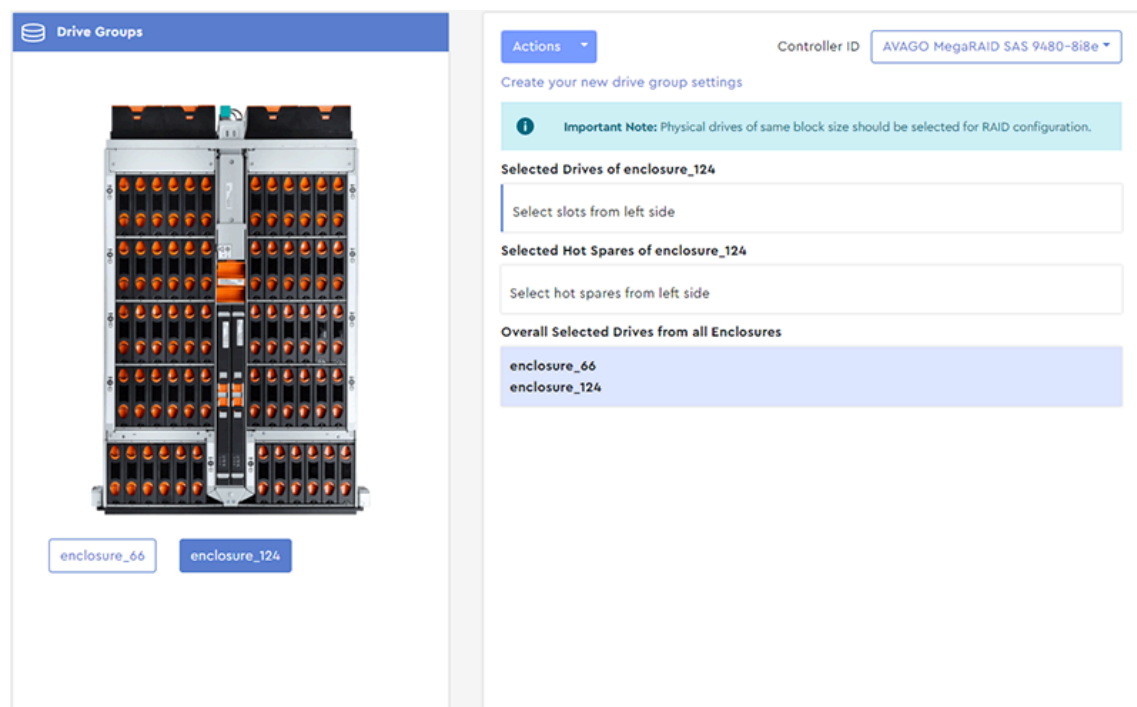
This procedure provides instructions for creating a drive group and configuring a RAID.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **MegaRAID > RAID Configuration**.

The **RAID Configuration** page will be displayed:


Figure 205: RAID Configuration Page



The screenshot shows the RAID Configuration Page. On the left, under the 'Drive Groups' tab, there is a visual representation of two server enclosures, 'enclosure_66' and 'enclosure_124', each with multiple drive slots. On the right, the 'Actions' dropdown is set to 'Controller ID' with the value 'AVAGO MegaRAID SAS 9480-8i8e'. Below this, a section titled 'Create your new drive group settings' contains an 'Important Note' about selecting drives of the same block size. The 'Selected Drives of enclosure_124' section has a text input field labeled 'Select slots from left side'. The 'Selected Hot Spares of enclosure_124' section also has a text input field labeled 'Select hot spares from left side'. The 'Overall Selected Drives from all Enclosures' section shows a list with 'enclosure_66' and 'enclosure_124' selected.

Step 2: In the **Selected Drives** section, click the field labeled **Select slots from left side**.
The drive group will be assigned a color, displayed on the left side of the field:

Figure 206: Selected Drives Field



A close-up of the 'Selected Drives' section, showing a text input field with the placeholder text 'Select slots from left side'.

Step 3: From the **Drive Groups** image on the left, click to select which drive slots will be included in the drive group.



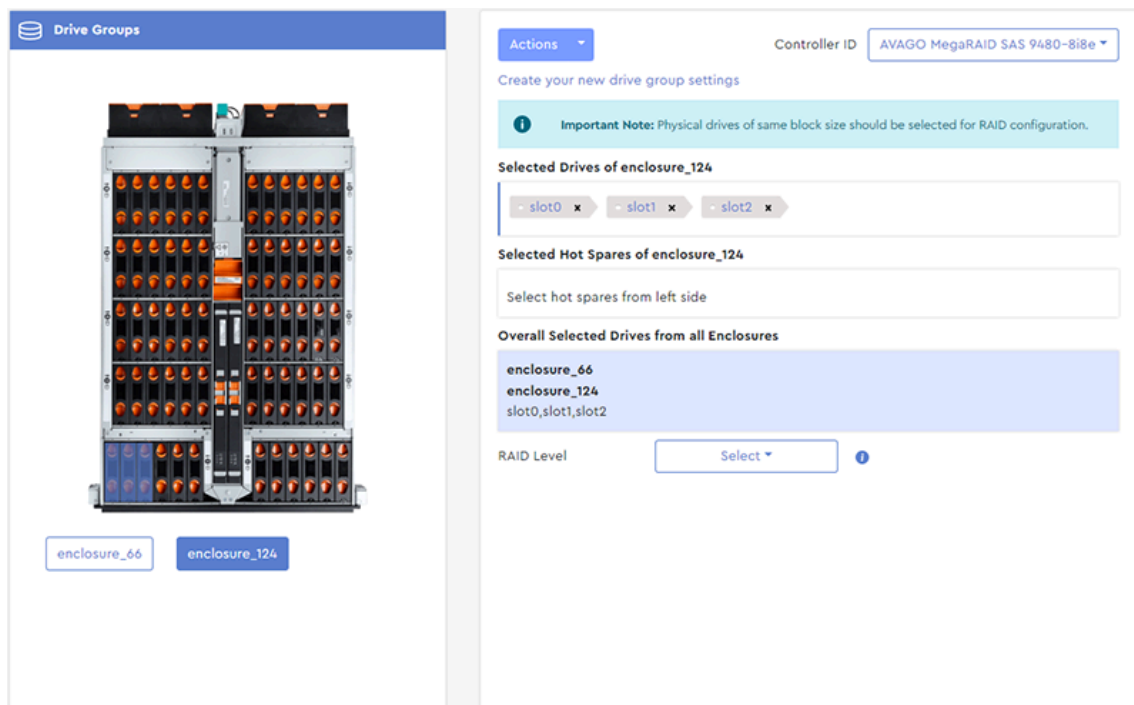
Important: As noted on the RAID Configuration page, all drives in a drive group must have the same block size (512B or 4K). Hovering over a drive slot will produce a tooltip that includes the block size for the drive installed in that slot.



Note: The maximum number of physical drives in a RAID10 drive group is sixteen (16). For all other RAID levels, the maximum number of physical drives in a drive group is thirty-two (32).

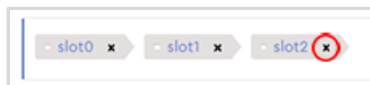
The drive slots will be color-coded, and the slot numbers will appear in the **Selected Drives** field:

Figure 207: Selected Drives



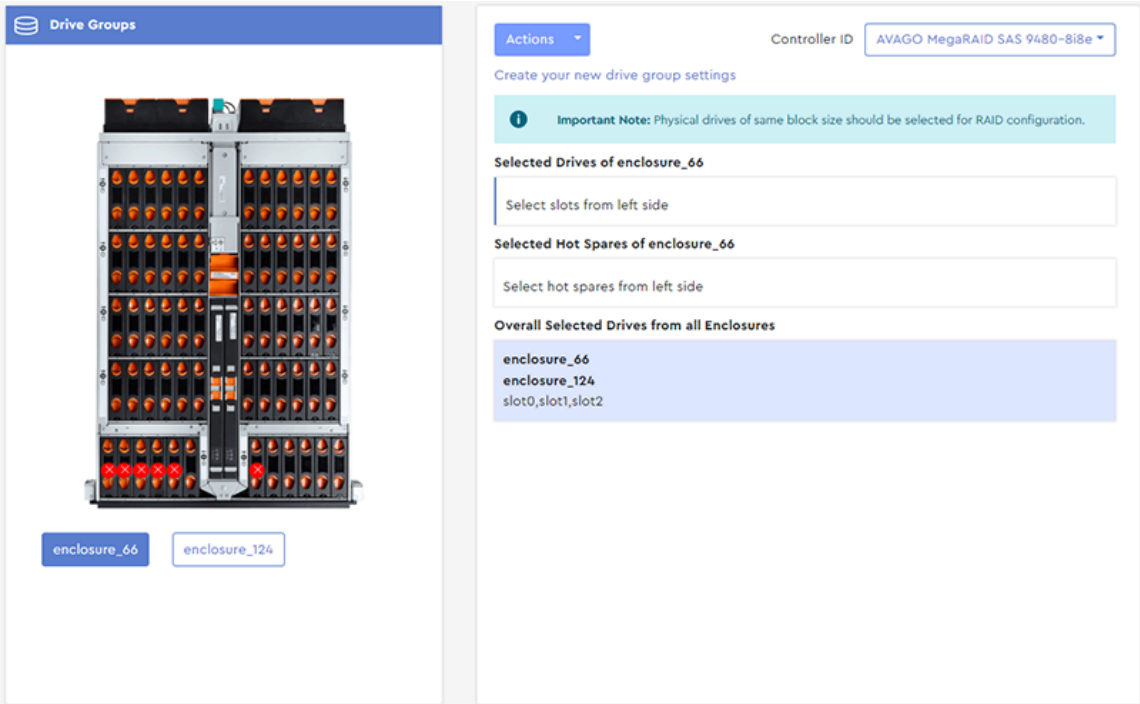
- a. To remove any drive slot from the drive group, click its **x**:

Figure 208: Remove Selected Drives



Step 4: To add drive slots from another enclosure, click that enclosure's button at the bottom of the **Drive Groups** section on the left. The image will update to show the other enclosure.

Figure 209: Another Enclosure



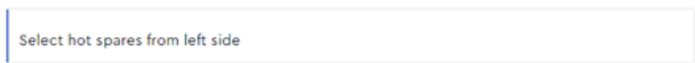
Step 5: Click to select additional drive slots and add them to the drive group. A summary of the drive slots and associated enclosures will be provided in the **Overall Selected Drives from all Enclosures** section.

Figure 210: Summary of Drives from All Enclosures



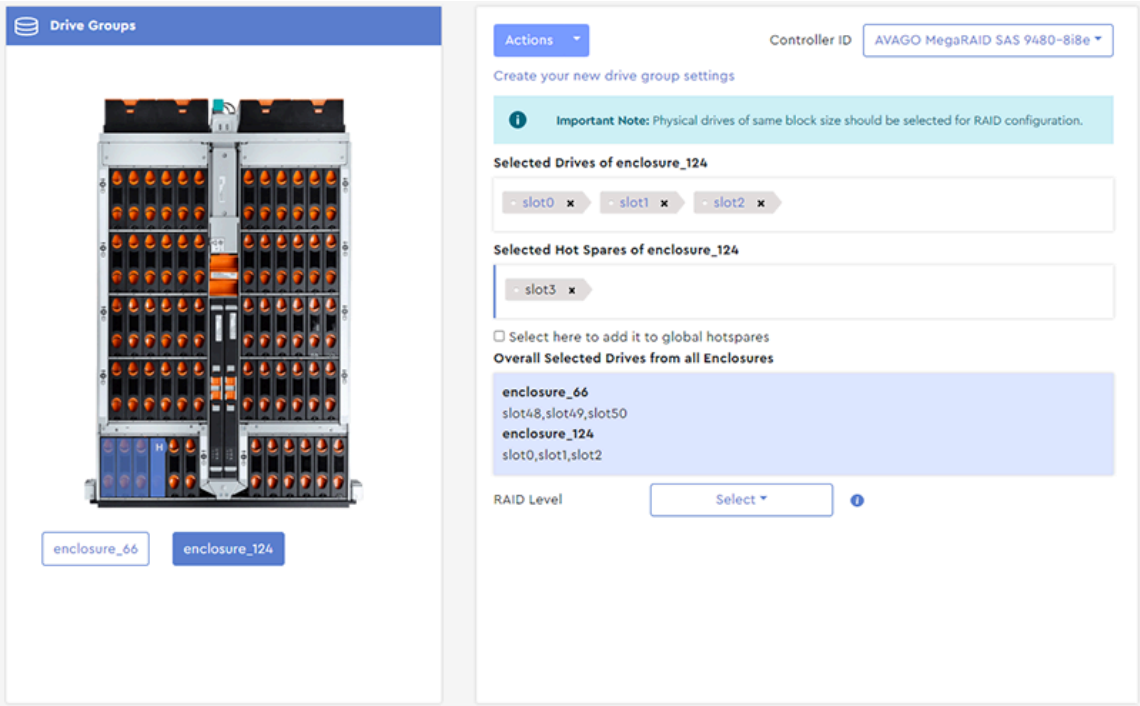
Step 6: In the **Selected Hot Spares** section, click the field labeled **Select hot spares from left side**. The **Selected Hot Spares** field will be highlighted:

Figure 211: Selected Hot Spares Field



Step 7: From the **Drive Groups** image on the left, click to select which drive slots will function as hot spares for the drive group. The drives slots will be color-coded, and the slot numbers will appear in the **Selected Hot Spares** field:

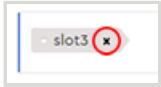
Figure 212: Selected Hot Spares



Important: Resource Manager Standard Edition includes advanced RAID features such as Rebuild and Copyback. If a drive within a drive group fails, the Rebuild feature will detect the failure and automatically rebuild the drive group using the designated hot spare. When the failing drive is replaced, the Copyback feature will automatically detect the good drive and copy back any data from the hotspare to the new drive. With the drive group fully intact, the hotspare will then return to its original function as a hotspare.

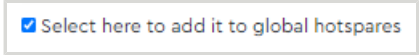
- a. To remove a drive slot from the hot spares group, click its **x**:

Figure 213: Remove Selected Hot Spares




- b. By default, the selected drive will be a dedicated hot spare for this drive group. To make the selected drive a global hot spare, click the checkbox:

Figure 214: Add To Global Hot Spares



Step 8: From the **RAID Level** drop-down list, select the RAID level for this drive group.

Figure 215: Select RAID Level



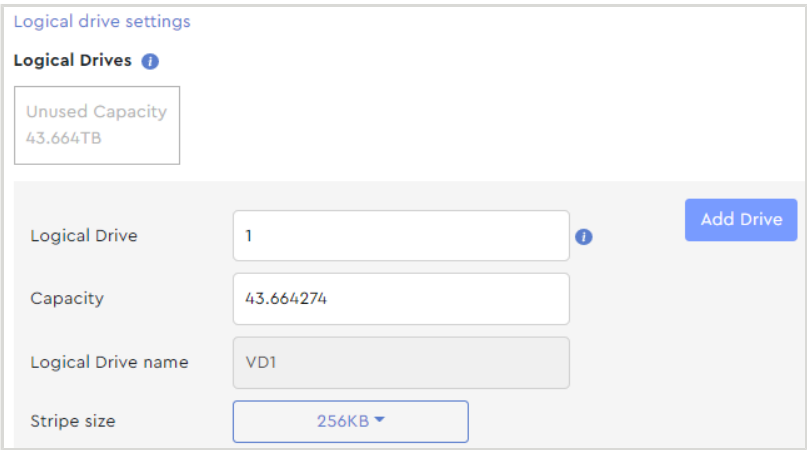
The screenshot shows a web interface for selecting a RAID level. On the left, there is a label "RAID Level". To its right is a blue button with the text "Select" and a downward arrow. A dropdown menu is open below the button, displaying a list of RAID levels: RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50, and RAID 60. An information icon (i) is located to the right of the "Select" button.



Note: Only valid options will be displayed in the drop-down list.

When a RAID level is selected, a **Logical Drive Settings** section will appear, displaying information about the RAID and controls for additional configuration:

Figure 216: Logical Drive Settings



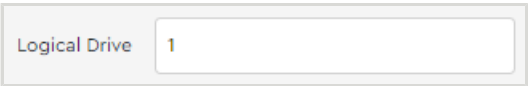
The screenshot shows the "Logical drive settings" section. At the top, it says "Logical drive settings" with a sub-header "Logical Drives" and an information icon. Below this, a box displays "Unused Capacity 43,664TB". The main area contains four input fields: "Logical Drive" with the value "1", "Capacity" with the value "43,664,274", "Logical Drive name" with the value "VD1", and "Stripe size" with a dropdown menu showing "256KB". An "Add Drive" button is located to the right of the "Logical Drive" field.

Step 9: In the **Logical Drive** field, select the **quantity** of logical drives to be created from the available capacity of the physical drive group.



Note: By default, the total unused capacity will be divided equally among the selected quantity of logical drives. The maximum quantity of logical drives is sixteen (16) per drive group.

Figure 217: Logical Drive Field



The screenshot shows a close-up of the "Logical Drive" field. It consists of a label "Logical Drive" and a text input box containing the number "1".

Step 10: If needed, use the **Capacity** field to reduce the capacity allocated to each logical drive.

Figure 218: Capacity Field

Capacity	43.664274
----------	-----------

Step 11: From the **Stripe Size** drop-down list, select the stripe size for this RAID.

Figure 219: Stripe Size

Stripe size	256KB ▾
Policy	
Initialization No Initialization	<input checked="" type="radio"/> No Initialization
	<input type="radio"/> Fast Initialization



Note: Only valid options will be displayed in the drop-down list.

Step 12: In the **Policy** section, select a category from the left column, and choose the associated policy from the list in the right column.

Figure 220: Initialization

Initialization No Initialization	Initialization prepares the storage medium for use <input checked="" type="radio"/> No Initialization The new configuration is not initialized, and the existing data on the drives is not Over written.
Read Policy Read Ahead	<input type="radio"/> Fast Initialization The Firmware erases the first and last 8 MB of the data area of the virtual drive by writing 0x00 to wipe out any remains of Master boot record (MBR) or partition tables. This operation is extremely fast, so the virtual drive is almost instantly accessible to the user.
Write Policy Write Back	
IO Policy Direct IO	
Disk Cache Policy Disabled	

Figure 221: Read Policy

Initialization No Initialization	A controller attribute indicating the current Read Policy mode <input type="radio"/> No Read Ahead In No Read Ahead mode, read ahead capability is disabled. <input checked="" type="radio"/> Read Ahead Read ahead capability allows the controller to read sequentially ahead of requested data and to store the additional data in cache memory, anticipating that the data will be needed soon. This process speeds up reads for sequential data, but there is little improvement occurs when accessing random data.
Read Policy Read Ahead	
Write Policy Write Back	
IO Policy Direct IO	
Disk Cache Policy Disabled	

Figure 222: Write Policy

Initialization No Initialization	A controller attribute indicating the current Write Policy mode <input type="radio"/> Write Through This mode provides for cache data protection upon power failure. Note: It may result in slower performance. <input checked="" type="radio"/> Write Back This option provides a good balance between data protection and performance as the controller switches between Write back and write through depending on Energy Pack status. Note: Write Back caching is enabled when the battery backup unit is installed and charged. Write Through is enabled when battery is not installed / charge is low / battery fails / during battery relearn cycle. <input type="radio"/> Always Write Back This mode provides optimal performance. Note: Data loss will occur if there is power failure along with cache Energy Pack is not installed, or the Energy Pack has failed or discharged.
Read Policy Read Ahead	
Write Policy Write Back	
IO Policy Direct IO	
Disk Cache Policy Disabled	

Figure 223: IO Policy

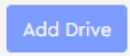
Initialization No Initialization	<p>The IO policy applies to reads on a specific virtual drive. It does not affect the read ahead cache.</p> <p><input checked="" type="radio"/> Direct IO</p> <p>In Direct I/O mode, reads are not buffered in cache memory. Data is transferred to the cache and the host concurrently. If the same data block is read again, it comes from cache memory. This option is the default setting.</p> <p><input type="radio"/> Cached IO</p> <p>In Cached I/O mode, all reads are buffered in cache memory.</p>
Read Policy Read Ahead	
Write Policy Write Back	
IO Policy Direct IO	
Disk Cache Policy Disabled	

Figure 224: Disk Cache Policy

Initialization No Initialization	<p>Specify the drive cache policy.</p> <p><input type="radio"/> Unchanged</p> <p>Leave the current drive cache policy as is.</p> <p><input type="radio"/> Enabled</p> <p>Enable the drive cache.</p> <p><input checked="" type="radio"/> Disabled</p> <p>Disable the drive cache.</p>
Read Policy Read Ahead	
Write Policy Write Back	
IO Policy Direct IO	
Disk Cache Policy Disabled	

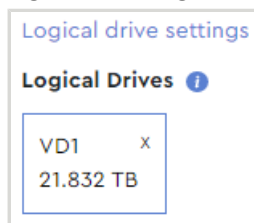
Step 13: After all RAID configuration selections have been made, click the **Add Drive** button.

Figure 225: Add Drive Button



The details of the RAID configuration will be replaced by a colored square, representing the logical drive:

Figure 226: Logical Drive



- a. To edit the details of the logical drive, click the square.
- b. To delete the logical drive, click the **x** in the upper-right corner.

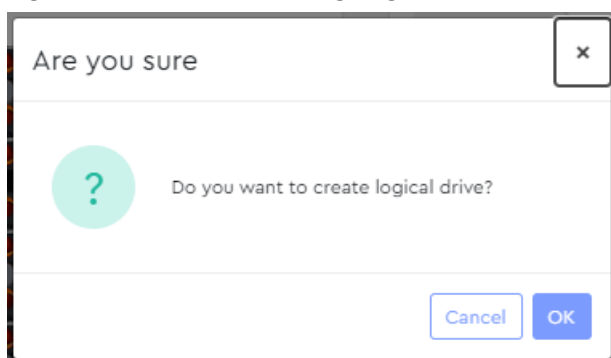
Step 14: Click the **Create Drive Group** button at the bottom of the **Logical Drive Settings** section.

Figure 227: Create Drive Group Button



A dialogue box will appear, prompting the user to confirm creating the logical drive:

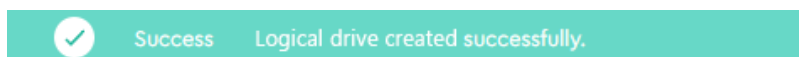
Figure 228: Confirm Creating Logical Drive



Step 15: Click the **OK** button.

A success notification will appear at the top of the page:

Figure 229: Success Notification



Result: The RAID is now created and will appear as a drive group in [Logical Drives \(page 147\)](#).

3.5.2.2 Clearing All RAID Configurations

This procedure provides instructions for clearing **all** RAID configurations from a MegaRAID controller.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

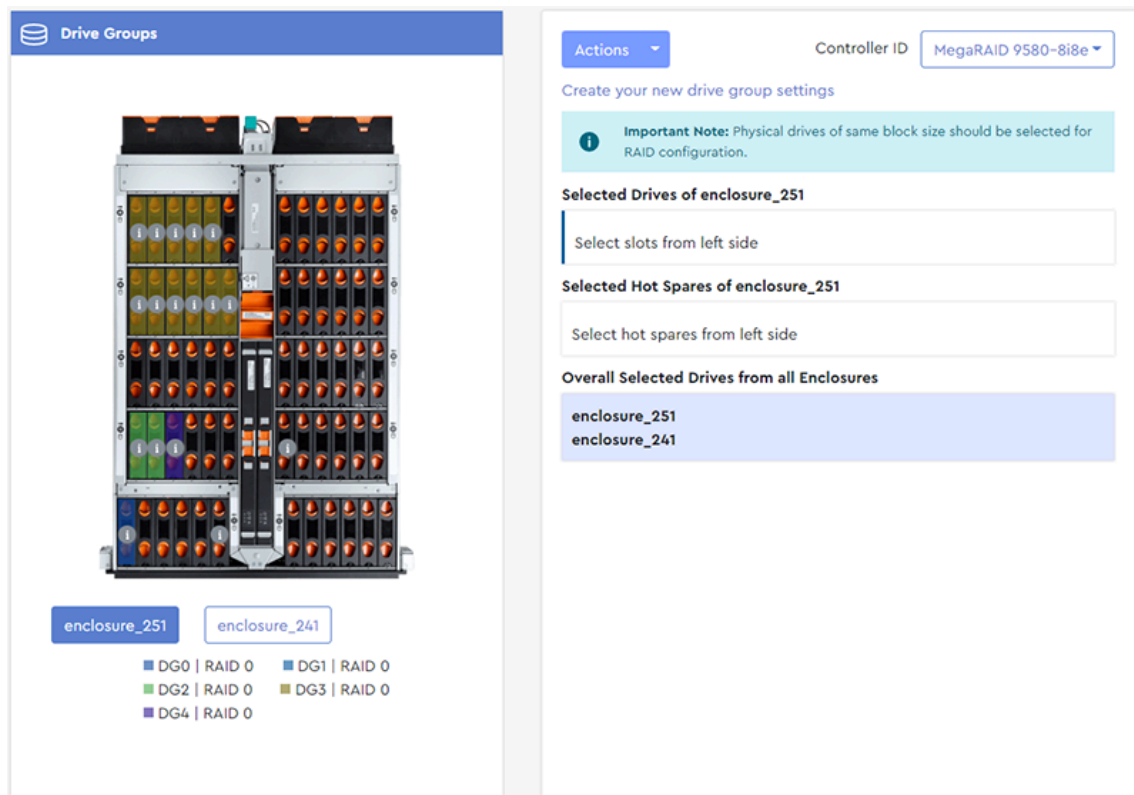


Note: To delete only **one** configuration, see [Deleting a Logical Drive \(page 165\)](#).

Step 1: From the navigation bar, select **MegaRAID > RAID Configuration**.

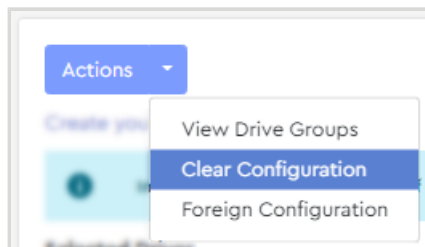
The **RAID Configuration** page will be displayed:

Figure 230: RAID Configuration Page

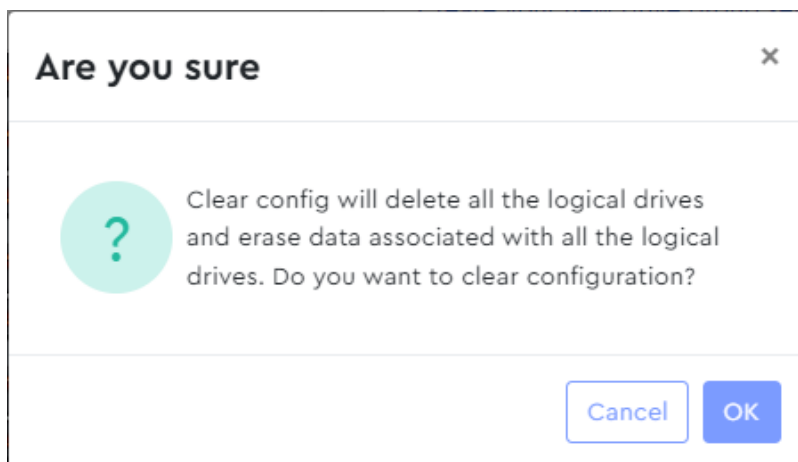


Step 2: From the **Actions** drop-down list, select the **Clear Configuration** option.

Figure 231: Clear Configuration



A dialogue box will be displayed, prompting the user to confirm clearing all RAID configurations:

Figure 232: Confirm Clearing All Configurations

Step 3: Click the **OK** button.

A success notification will appear at the top of the page:

Figure 233: Success Notification

Result: All RAID configurations have now been cleared.

3.5.2.3 Importing Foreign Configurations

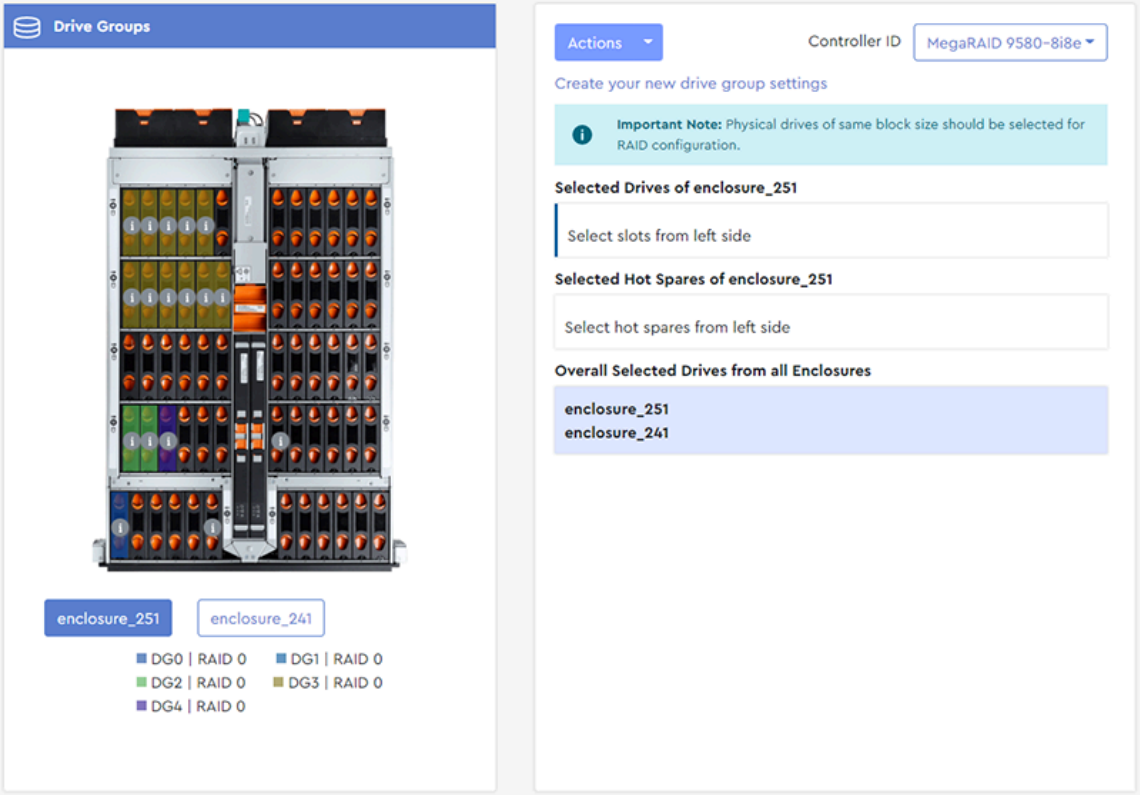
This procedure provides instructions for importing foreign RAID configurations—configurations that already exist on replacement drives.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **MegaRAID > RAID Configuration**.

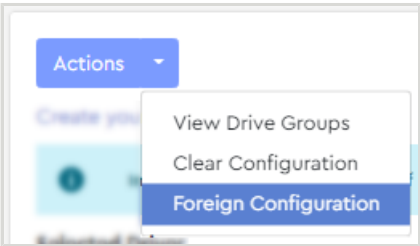
The **RAID Configuration** page will be displayed:

Figure 234: RAID Configuration Page

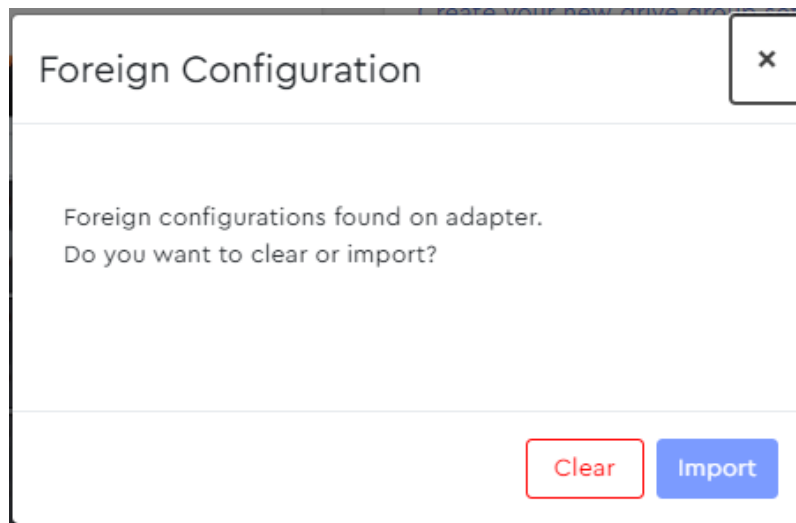


Step 2: From the **Actions** drop-down list, select the **Foreign Configuration** option.

Figure 235: Foreign Configuration

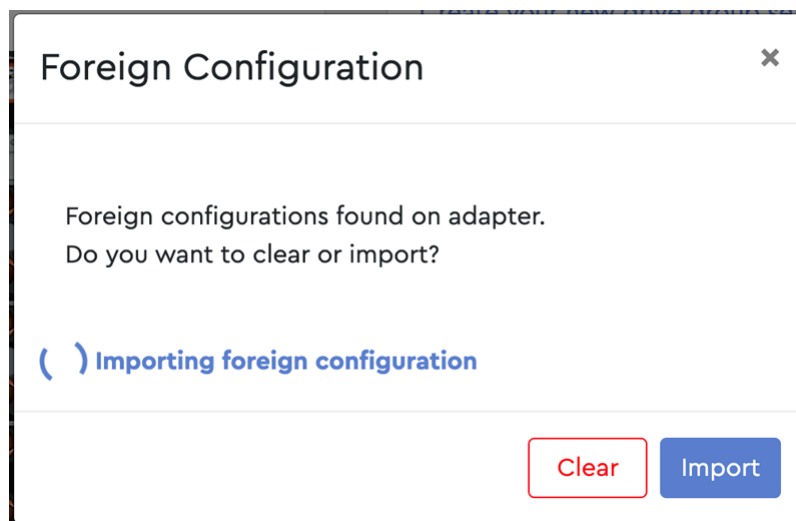


A dialogue box will be displayed, prompting the user to either clear or import all foreign configurations:

Figure 236: Clear or Import All Foreign Configurations

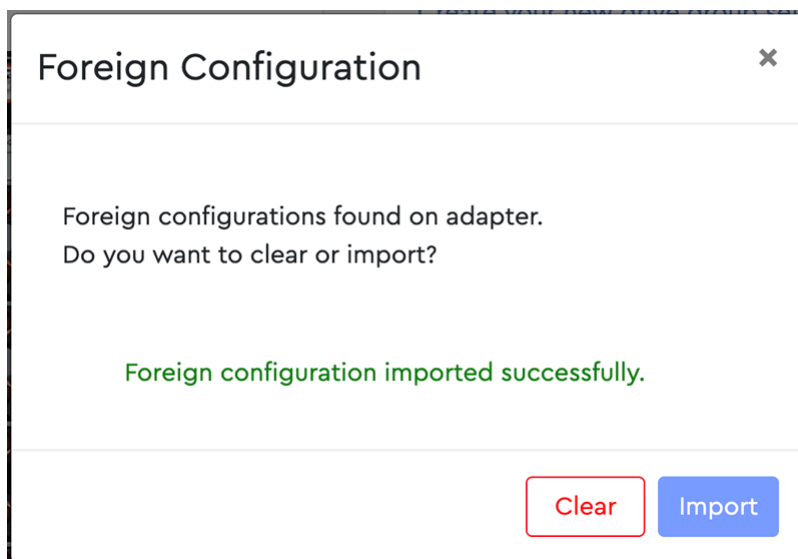
Step 3: Click the **Import** button.

The dialog box notifies the user that importing has started:

Figure 237: Importing Foreign Configurations

When the import is finished, a success message will be displayed:

Figure 238: Import Success



Result: The foreign configurations have now been imported.

3.5.2.4 Clearing Foreign Configurations

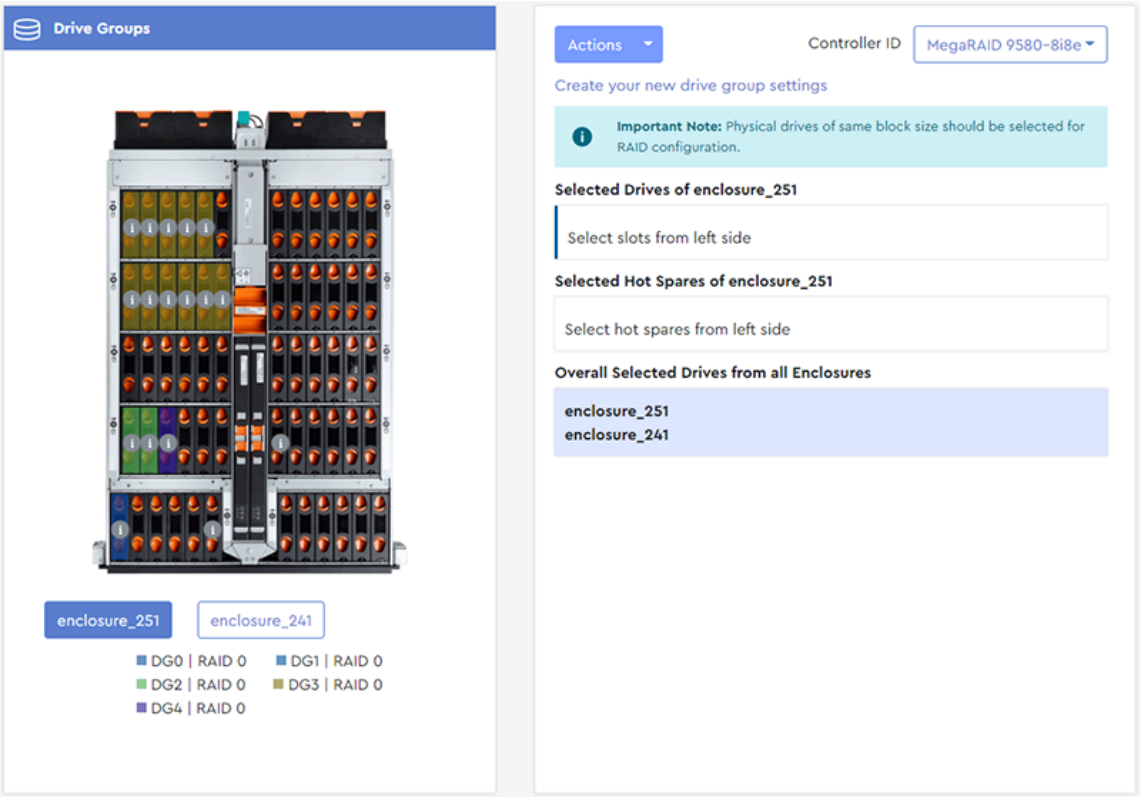
This procedure provides instructions for clearing foreign RAID configurations—configurations that already exist on replacement drives.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **MegaRAID > RAID Configuration**.

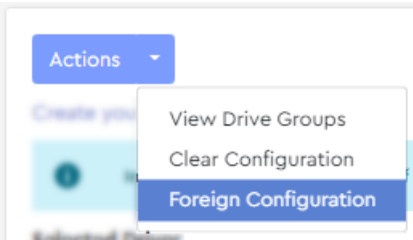
The **RAID Configuration** page will be displayed:

Figure 239: RAID Configuration Page



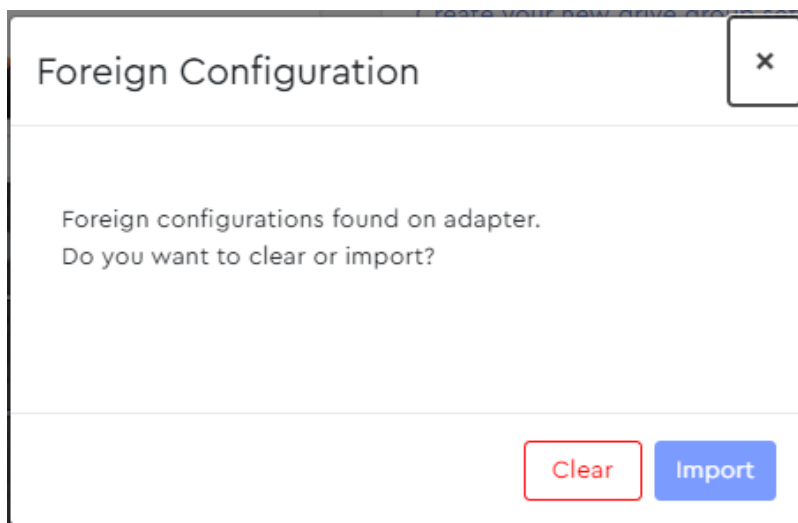
Step 2: From the **Actions** drop-down list, select the **Foreign Configuration** option.

Figure 240: Foreign Configuration



A dialogue box will be displayed, prompting the user to either clear or import all foreign configurations:

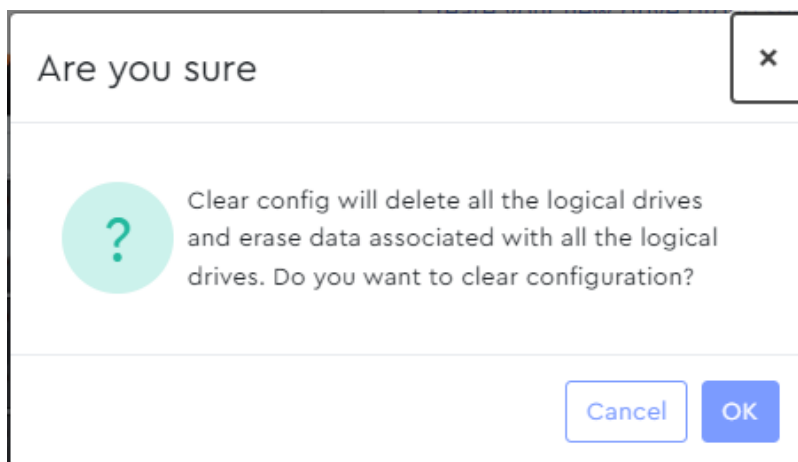
Figure 241: Clear or Import All Foreign Configurations



Step 3: Click the **Clear** button.

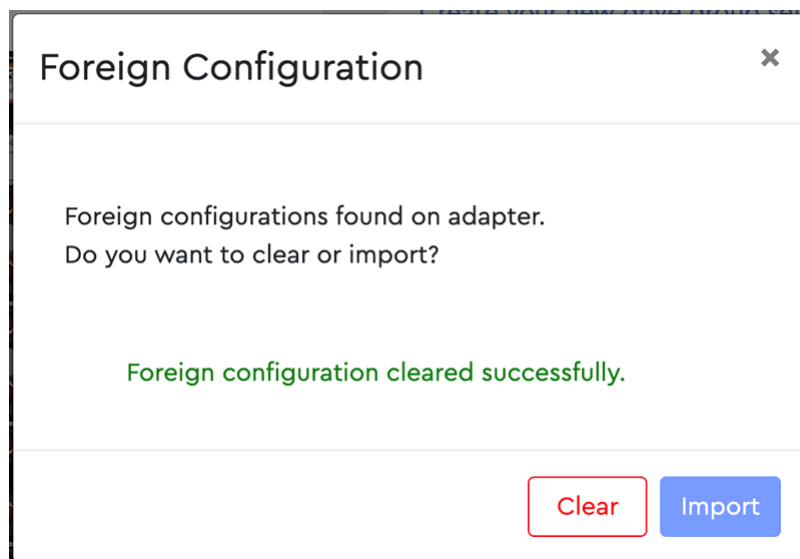
The dialogue box prompts the user to confirm the request:

Figure 242: Confirm Clear



Step 4: Click the **OK** button.

When the foreign configurations have been cleared, a success message will be displayed:

Figure 243: Clear Success

Result: The foreign configurations have now been cleared.

3.5.3 Logical Drives

The **Logical Drives** page displays information about the logical drives being managed through the selected MegaRAID controller.

Western Digital Resource Manager - Standard

JBOD ID: THCCT0272HEZ0004 • Version 1.3.1 • uradmin

Logical Drives

Configure Controller ID: AVAGO MegaRAID SAS 9480-8i8e

Important Note: 2 Background processes running. [Click here](#) to view

Total Logical drives: 9 Total Global hot spare: 2

Drive Group	RAID Level	Physical Drives	Logical Drives	Hot Spares	Capacity	Utilization	Action
DG0	RAID 0	2	4	0	14.553 TB	100%	...
DG1	RAID 5	4	4	0	16.376 TB	100%	...
DG2	RAID 5	5	1	0	36.382 TB	100%	...

Enc ID	Slot ID	Device ID	Drive Type	Interface	Serial number	Capacity
66	56	18	HDD	SAS	VCG1M5SM	9.096 TB
66	29	33	HDD	SAS	8DG3L9ED	10.914 TB
66	55	45	HDD	SAS	VCG16GAN	9.096 TB
124	2	68	HDD	SAS	9JG1G8DG	12.733 TB

Logical drive

LD Name: VD1
LD ID: 8
Capacity: 36.365 TB
Stripe Size: 256KB
Policy: RA | WB | DIO

3.5.3.1 Modifying a Drive Group / RAID Configuration

This procedure provides instructions for modifying a drive group / RAID configuration.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

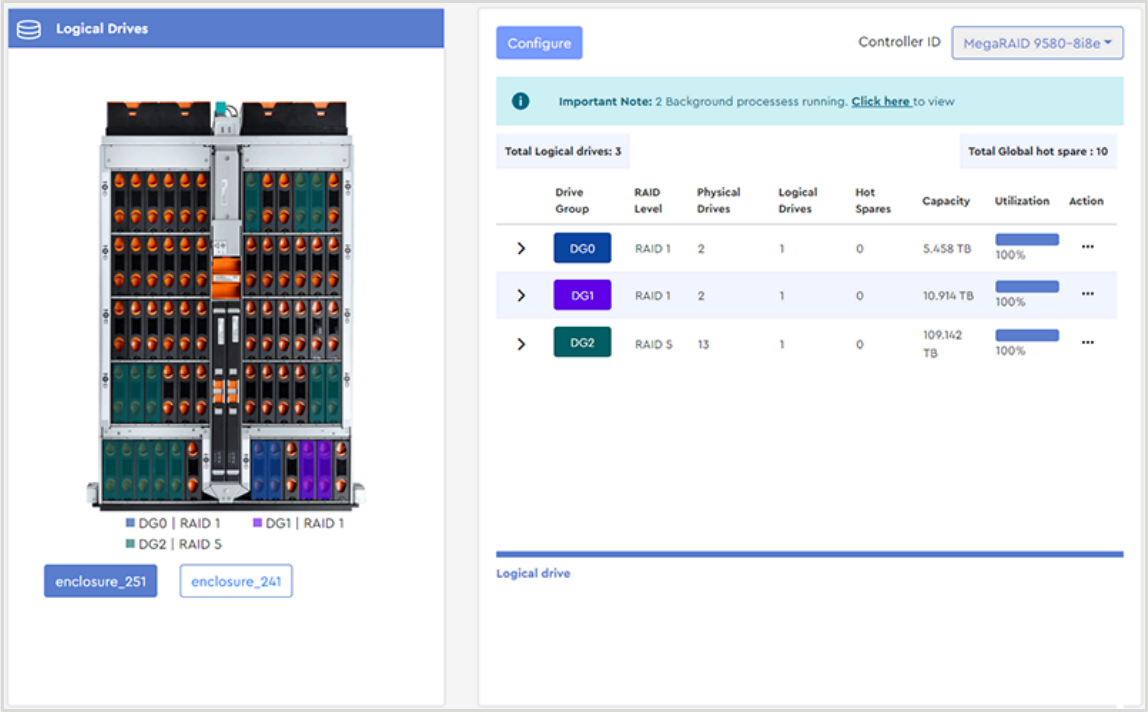


Note: This procedure assumes that the drive group / RAID configuration was previously created. See [Creating a Drive Group / RAID Configuration \(page 129\)](#) for more information.

Step 1: From the navigation bar, select **MegaRAID > Logical Drives**.

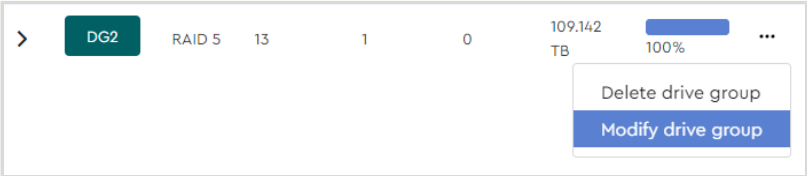
The **Logical Drives** page will be displayed:

Figure 245: Logical Drives Page



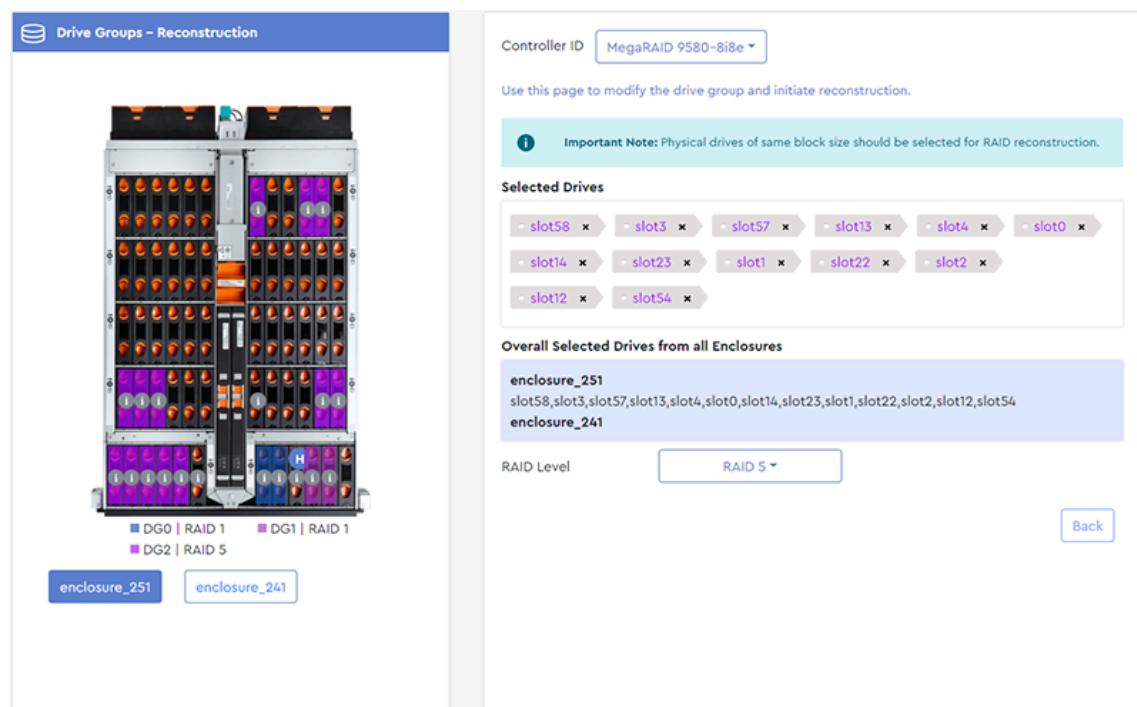
Step 2: From the right column, click the elipsis menu (...) for the drive group to be modified, and select the **Modify drive group** option:

Figure 246: Modify Drive Group



A **Drive Groups - Reconstruction** page will be displayed, allowing modifications to the drive group:

Figure 247: Drive Groups - Reconstruction



Step 3: Modify the drive group by adding drives, deleting drives, or selecting a different RAID level.

- a. To add drives, click to select additional slots from the **Drive Groups - Reconstruction** image on the left.



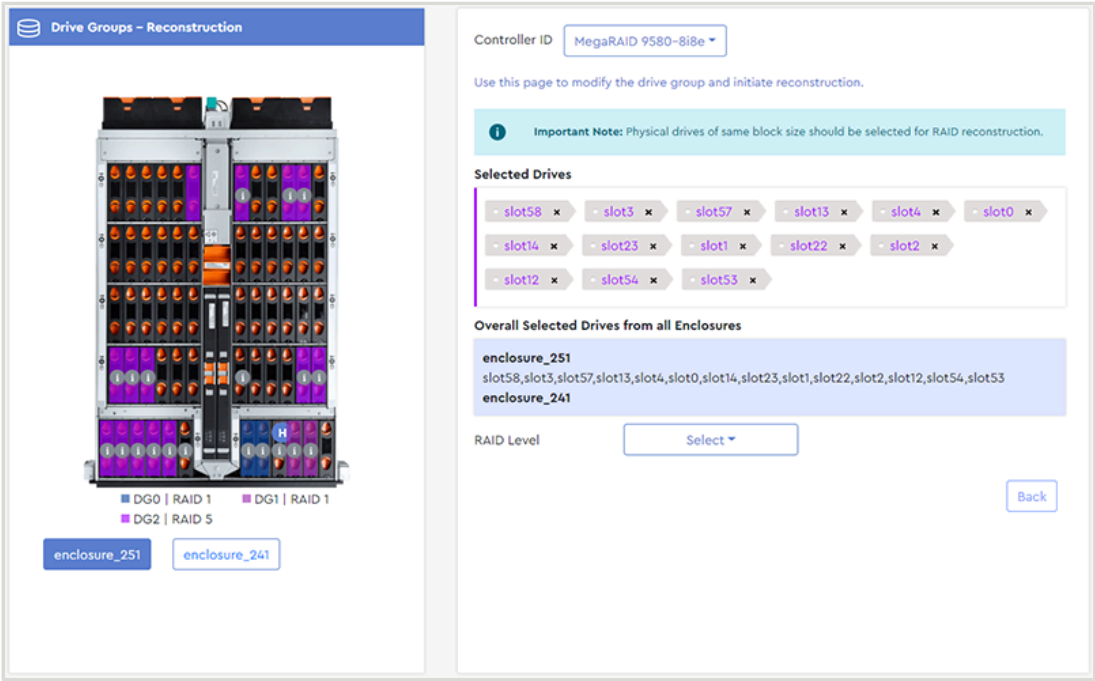
Important: As noted on the RAID Configuration page, all drives in a drive group must have the same block size (512B or 4K). Hovering over a drive slot will produce a tooltip that includes the block size for the drive installed in that slot.



Note: The maximum number of physical drives in a RAID10 drive group is sixteen (16). For all other RAID levels, the maximum number of physical drives in a drive group is thirty-two (32).

The drive slots will be color-coded, and the slot numbers will appear in the **Selected Drives** field:

Figure 248: Added Drives



- b. To remove a drive slot from the group, click its **x**:

Figure 249: Remove Selected Drives



- c. To select a different RAID level, use the **RAID Level** drop-down list:

Figure 250: Select RAID Level



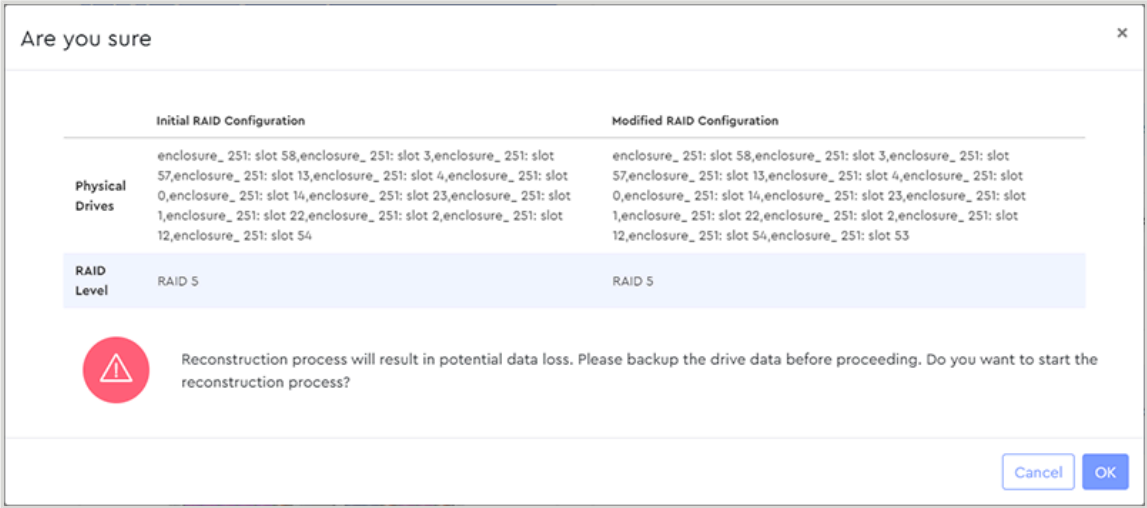
A **Modify Drive Group** button will be displayed:

Figure 251: Modify Drive Group



- Step 4:** Click the **Modify Drive Group** button.
- A dialogue box will appear, displaying the details of the **Initial RAID Configuration** and the **Modified RAID Configuration**:

Figure 252: RAID Reconstruction Confirmation



- Step 5:** Click the **OK** button to start the RAID reconstruction process.
- The user will be notified of the foreground reconstruction operations:

Figure 253: Initiating Logical Drive Reconstruction

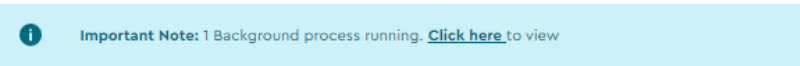


Figure 254: Fetching RAID List



When the foreground operations are complete, a background process notification will be displayed on the **Logical Drives** page:

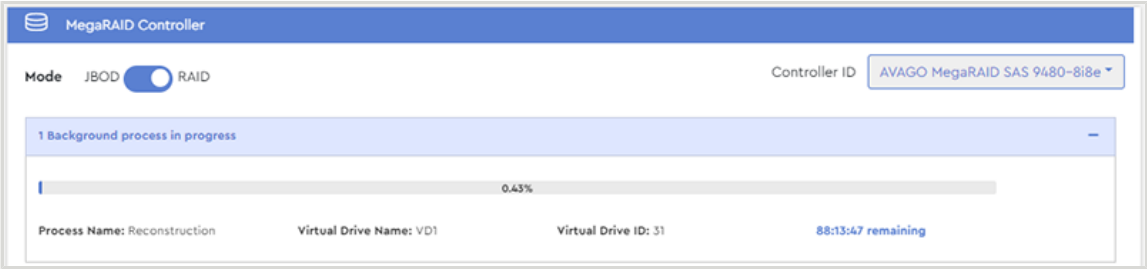
Figure 255: Background Process Notification



- Step 6:** To check the progress of the background reconstruction, click the text in the notification message:

The user will be redirected to the **MegaRAID Controller** page, where the reconstruction progress is displayed:

Figure 256: Background Process Notification



Result: When the Reconstruction background process reaches 100%, the drive group modification will be complete.

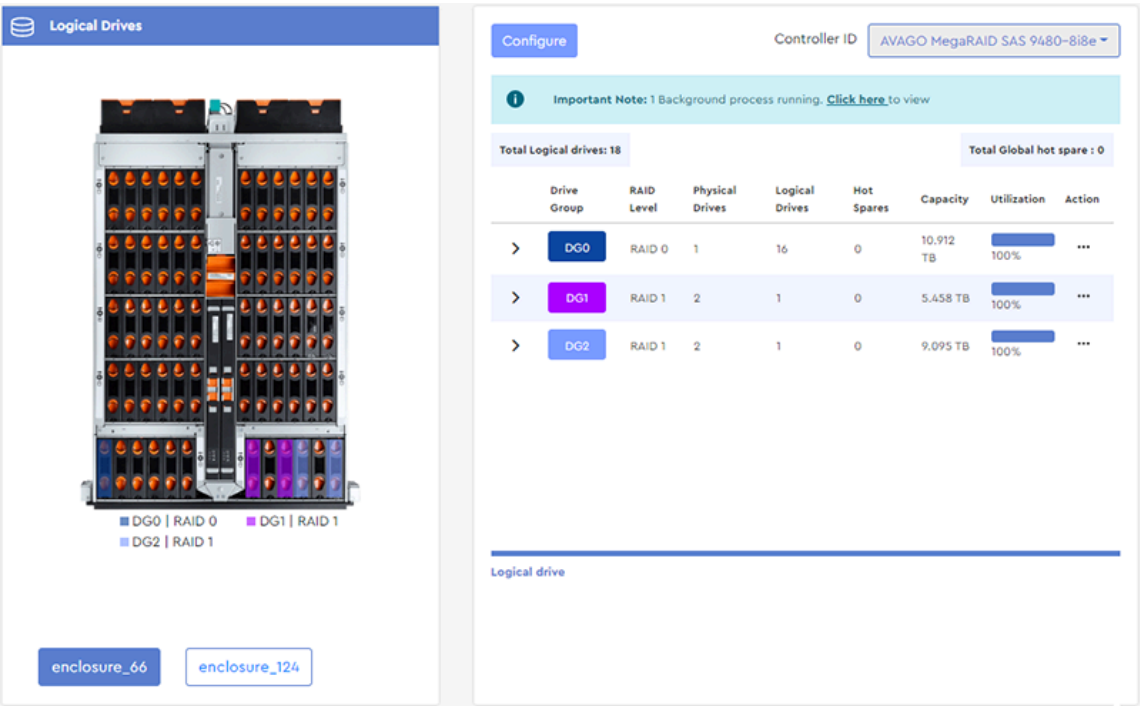
3.5.3.2 Starting a Consistency Check

This procedure provides instructions for starting a consistency check on a logical drive.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

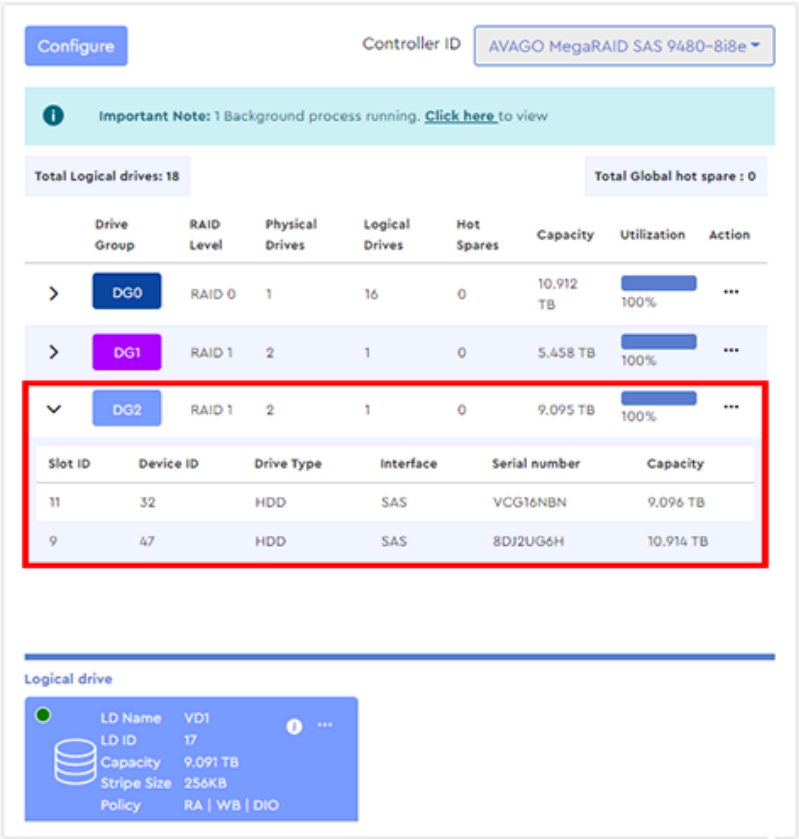
- Step 1:** From the navigation bar, select **MegaRAID > Logical Drives**.
The **Logical Drives** page will be displayed:

Figure 257: Logical Drives Page



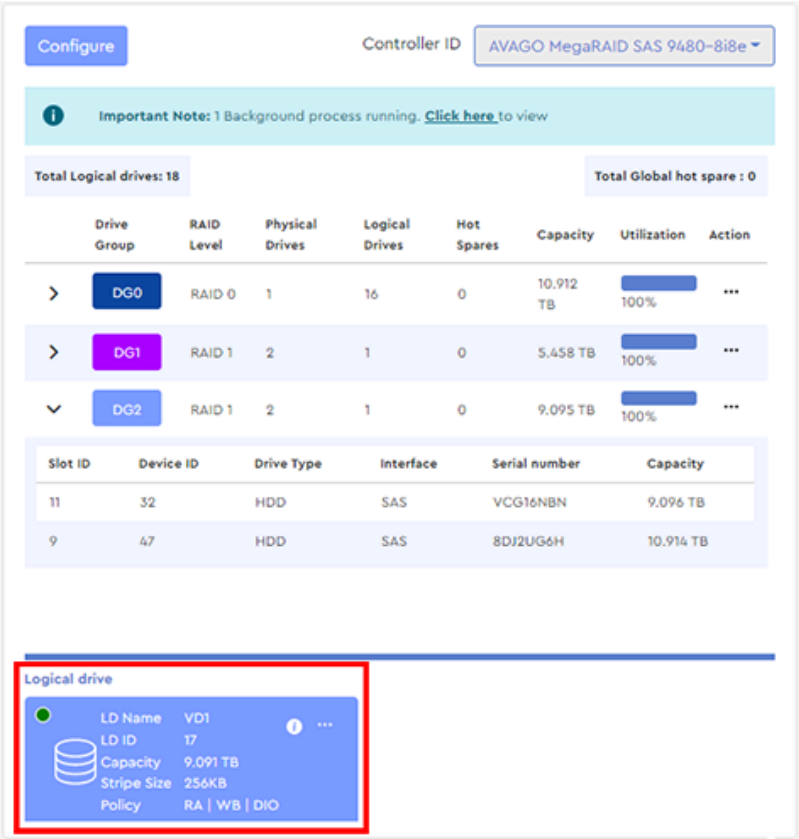
Step 2: From the right column, select a drive group to expand its details:

Figure 258: Drive Group Details



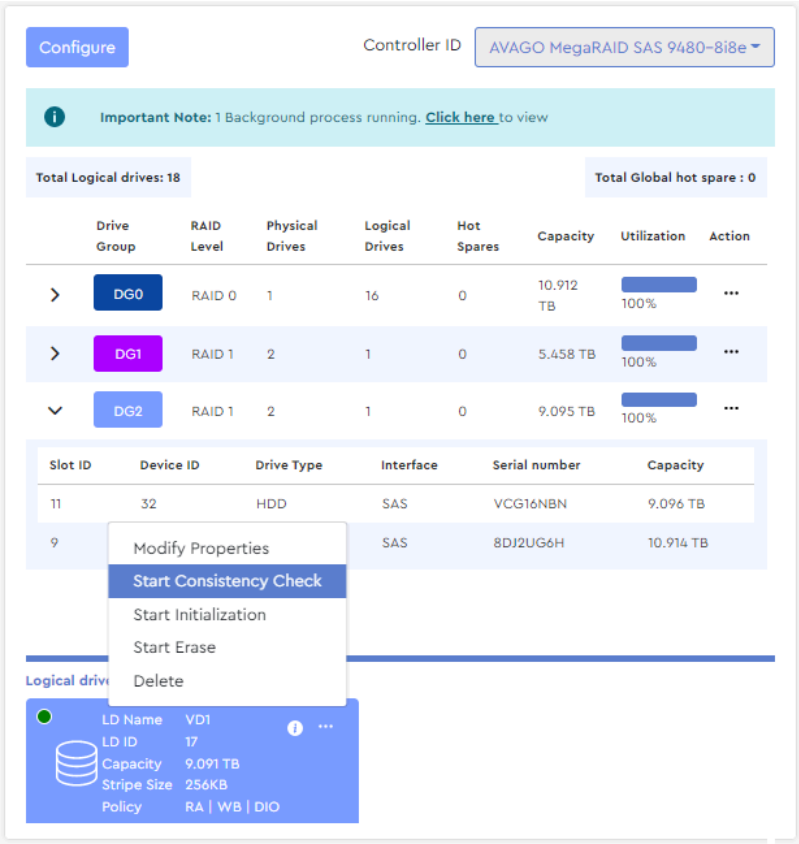
At the bottom of the column, the logical drive(s) for that group will be displayed:

Figure 259: Logical Drive Details



Step 3: Click the ellipsis (...) for the logical drive, and select the **Start Consistency Check** option.

Figure 260: Start Consistency Check



A dialogue box will appear, prompting the user to confirm the consistency check. The message will differ, depending whether or not the logical drive has been initialized:

Figure 261: Confirmation, Not Initialized

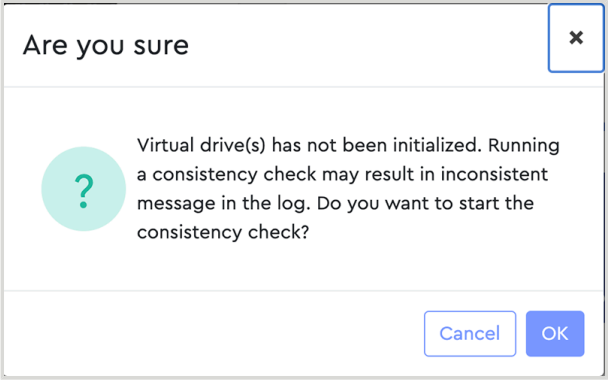
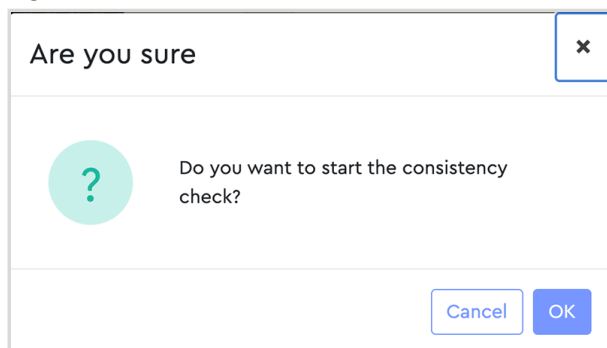


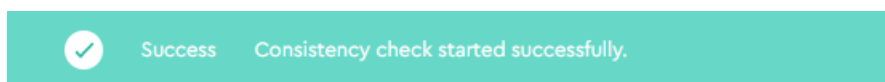
Figure 262: Confirmation, Initialized



Step 4: Click the **OK** button.

A success notification will appear at the top of the page:

Figure 263: Success Notification



Result: The consistency check has now been started. To check the progress, see [Checking Background Processes \(page 115\)](#).

3.5.3.3 Initializing a Logical Drive

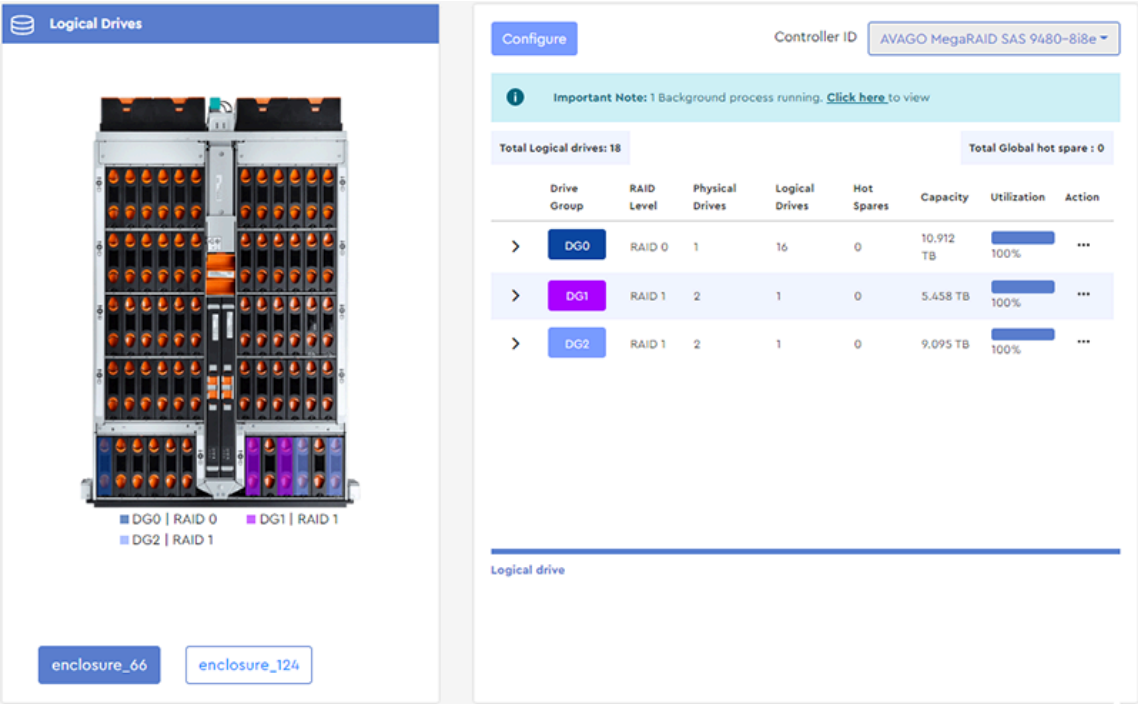
This procedure provides instructions for starting initialization of a logical drive.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **MegaRAID > Logical Drives**.

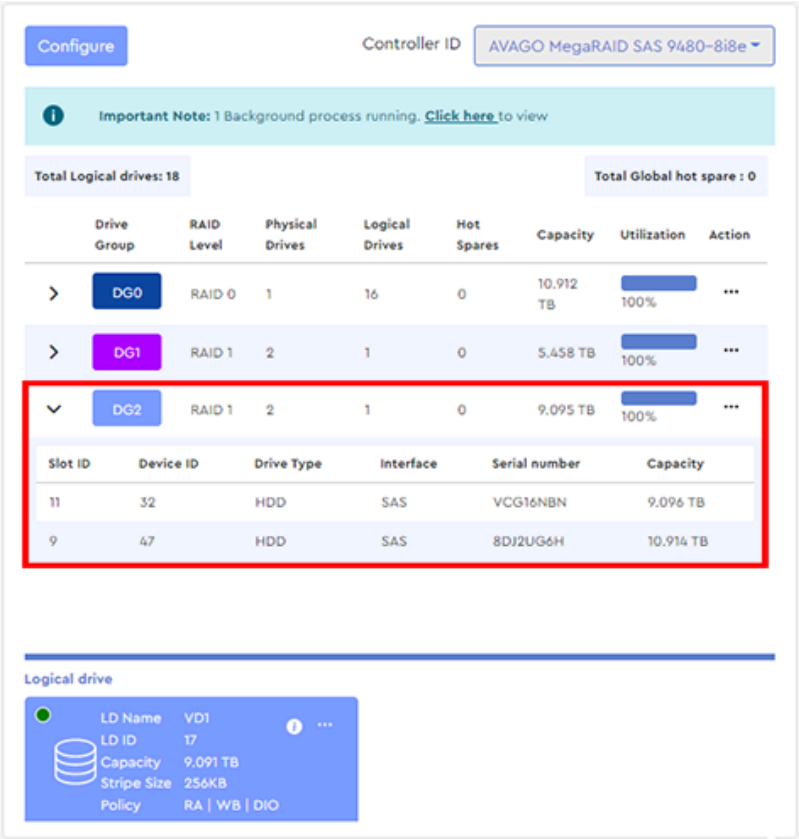
The **Logical Drives** page will be displayed:

Figure 264: Logical Drives Page



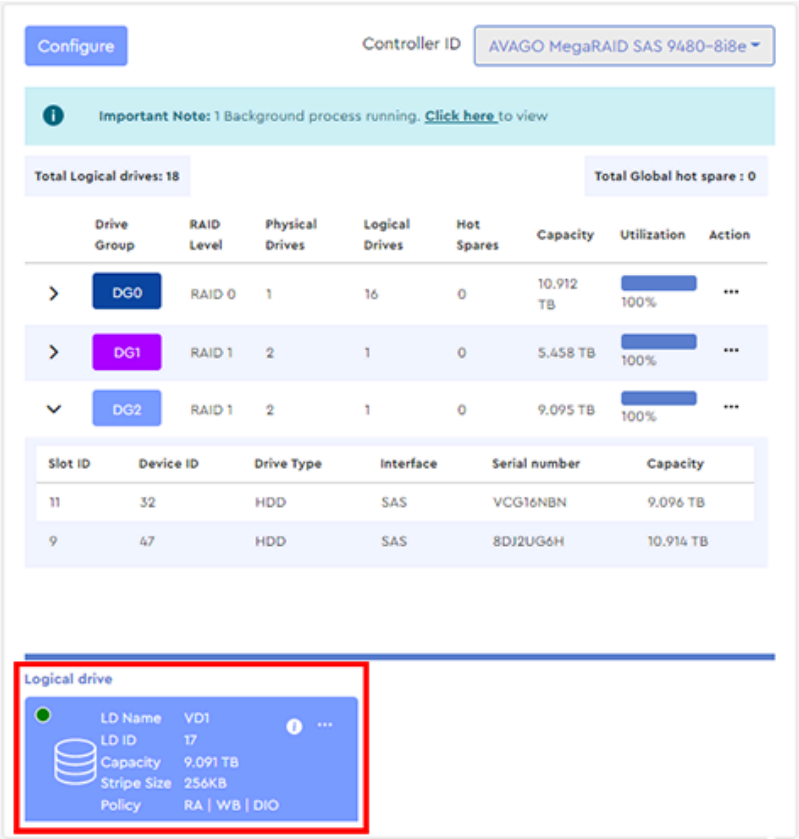
Step 2: From the right column, select a drive group to expand its details:

Figure 265: Drive Group Details



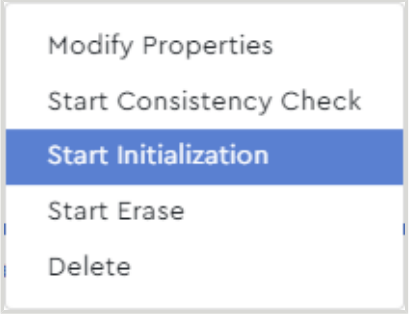
At the bottom of the column, the logical drive(s) for that group will be displayed:

Figure 266: Logical Drive Details



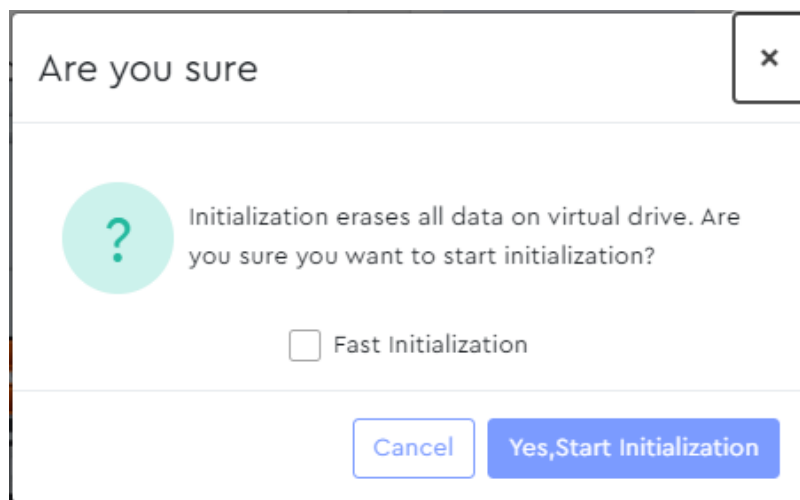
Step 3: Click the ellipsis (...) for the logical drive, and select the **Start Initialization** option.

Figure 267: Start Initialization



A dialogue box will appear, prompting the user to confirm the initialization. If needed, click the checkbox to select **Fast Initialization** instead of the default full initialization:

Figure 268: Confirm Initialization

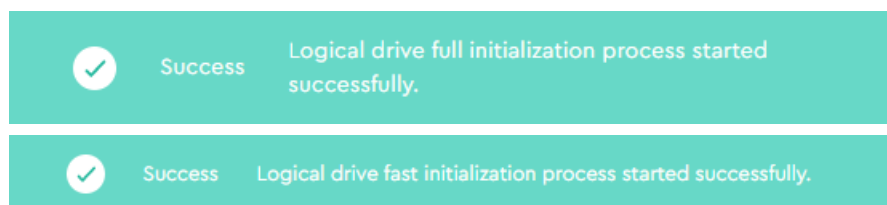


Step 4: The default is a full initialization (foreground process) of the virtual drive. If a fast initialization (background process) is needed, click the checkbox for **Fast Initialization**, which will initialize the first 8MB and the last 8MB on the virtual drive.

Step 5: Click the **Yes, Start Initialization** button.

A success notification will appear at the top of the page. The message will depend on whether you chose a full or fast initialization:

Figure 269: Start Initialization Success



Result: The initialization of the logical drive has now been started. To check the progress, see [Checking Background Processes \(page 115\)](#)

3.5.3.4 Erasing a Logical Drive

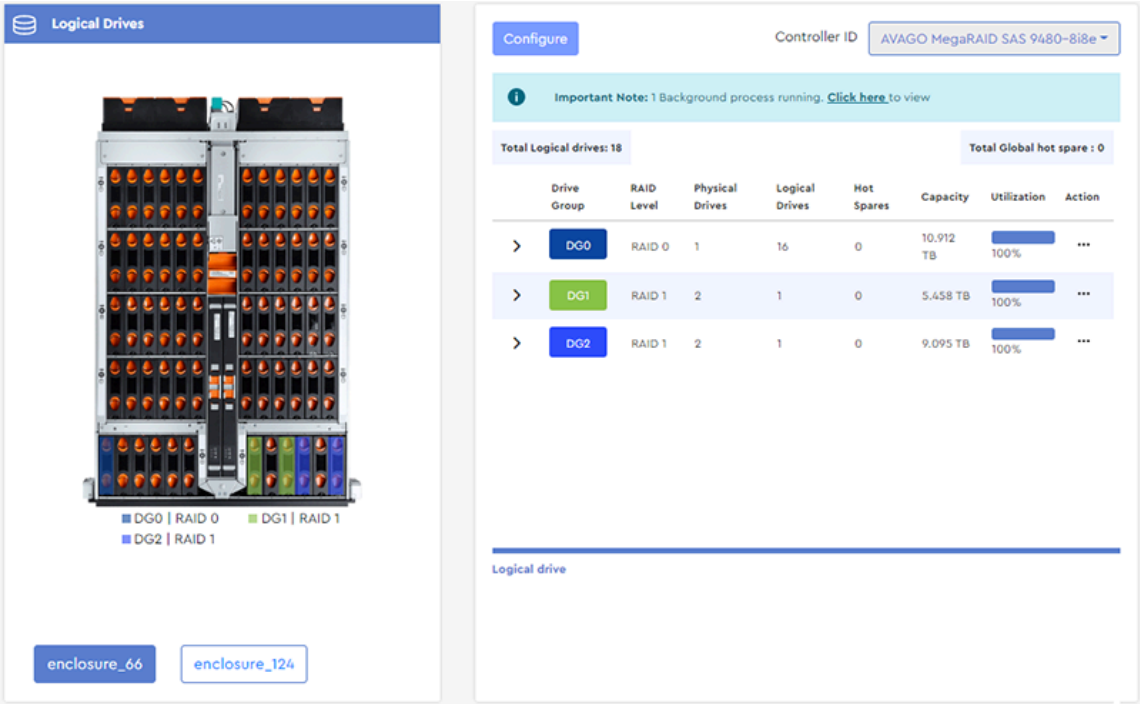
This procedure provides instructions for erasing a logical drive.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **MegaRAID > Logical Drives**.

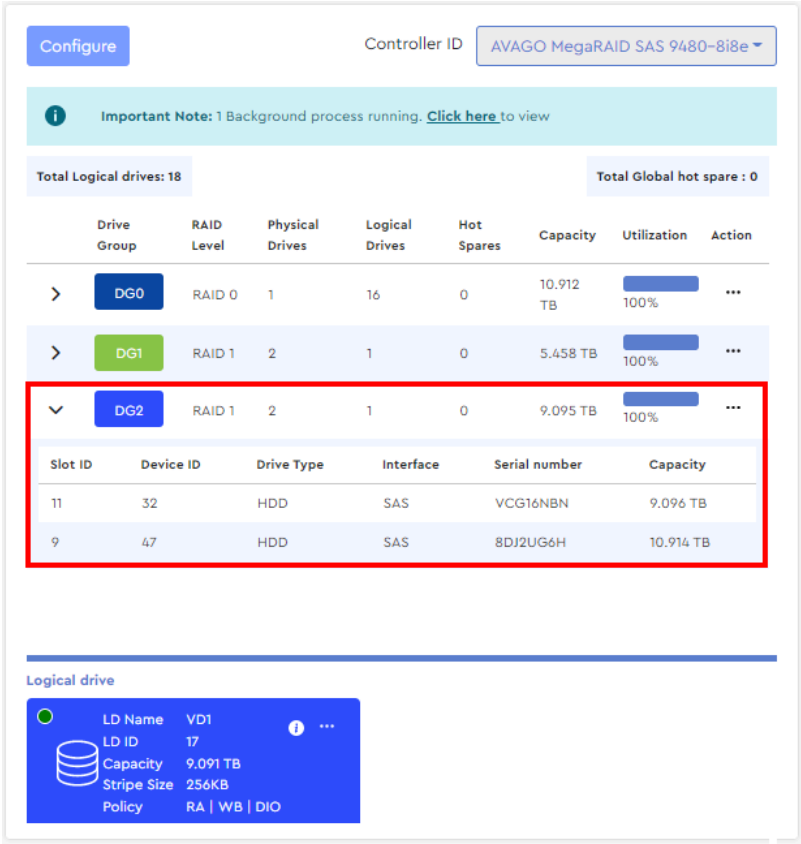
The **Logical Drives** page will be displayed:

Figure 270: Logical Drives Page



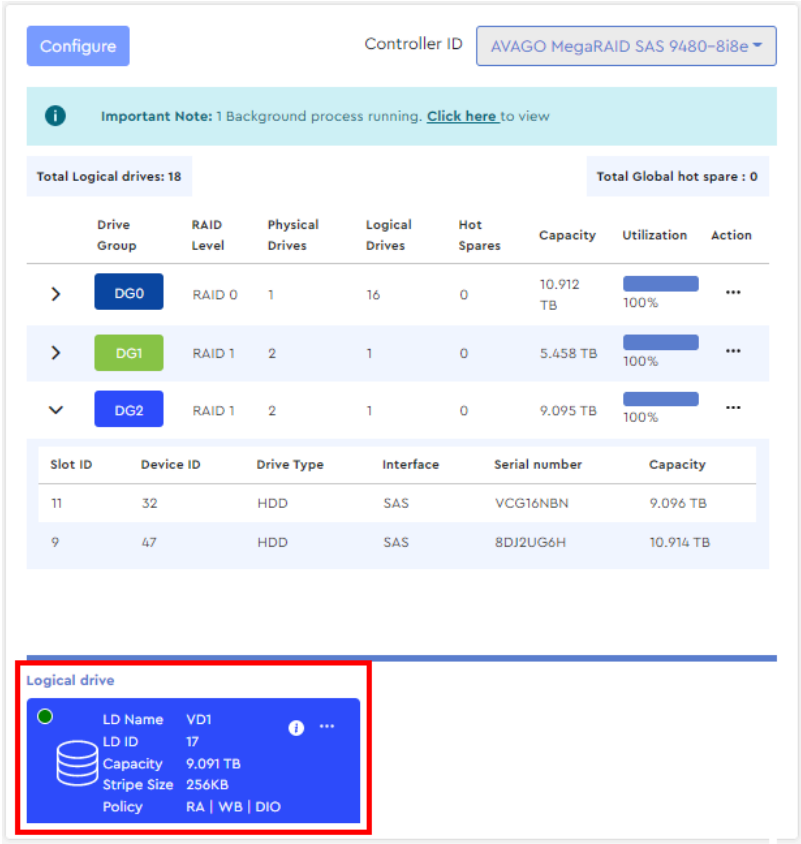
Step 2: From the right column, select a drive group to expand its details:

Figure 271: Drive Group Details



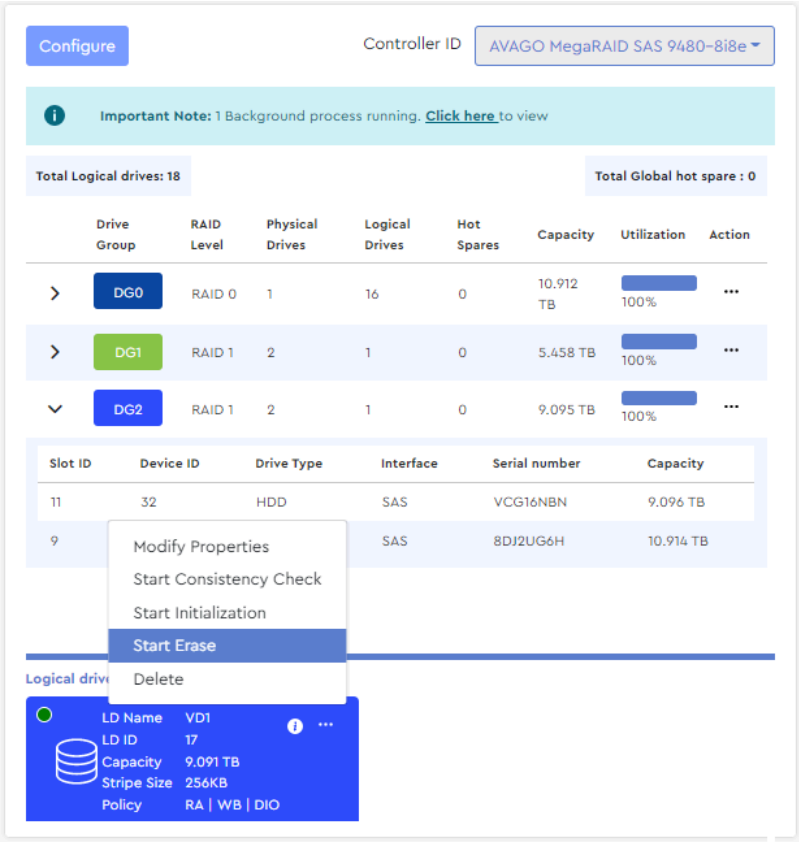
At the bottom of the column, the logical drive(s) for that group will be displayed:

Figure 272: Logical Drive Details



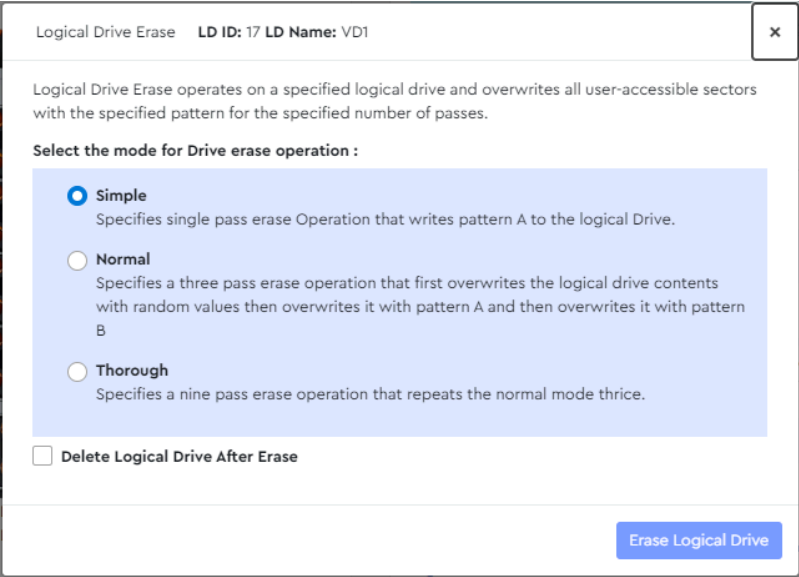
Step 3: Click the ellipsis (...) for the logical drive, and select the **Start Erase** option:

Figure 273: Start Erase



A dialogue box will appear, prompting the user to select an erase option:

Figure 274: Erase Options



Step 4: Click the appropriate radio button to select **Simple**, **Normal**, or **Thorough** erase. If needed, select the checkbox next to **Delete Logical Drive After Erase**. Then click the **Erase Logical Drive** button.

A success notification will appear at the bottom of the dialogue box:

Figure 275: Success Notification

Logical drive erase started successfully.

Result: The erase process has now been started. To check the progress, see [Checking Background Processes \(page 115\)](#).

3.5.3.5 Deleting a Logical Drive

This procedure provides instructions for deleting a logical drive (including its RAID configuration) from a MegaRAID controller.

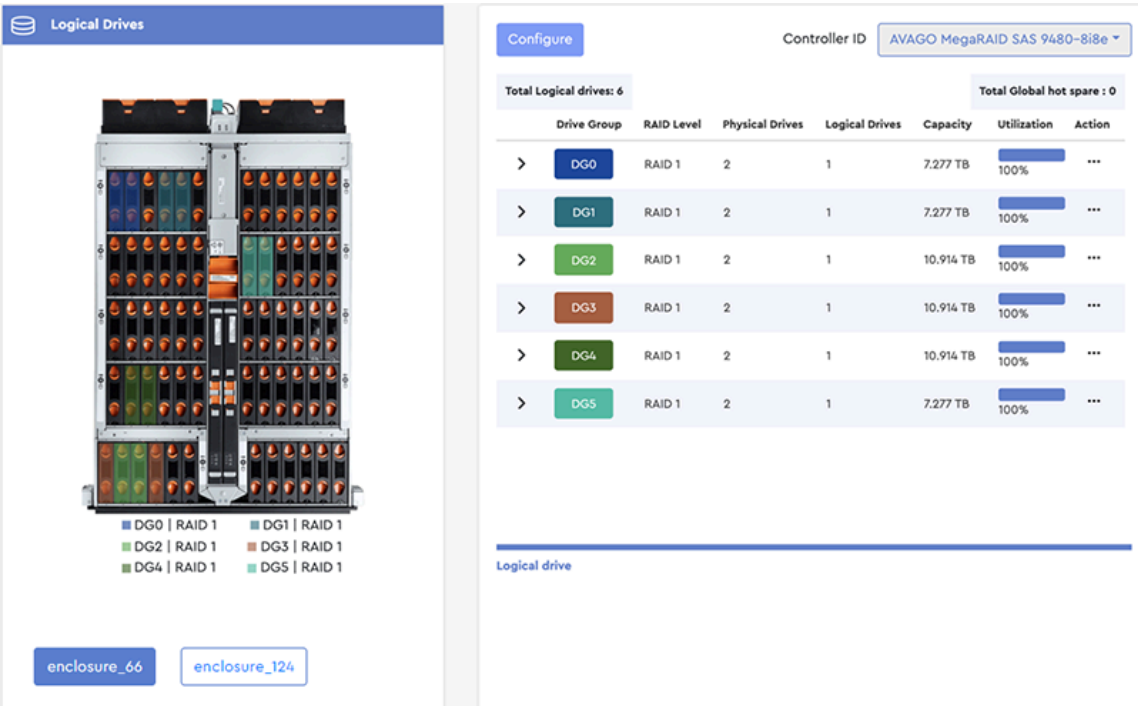
Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.



Note: To delete **all** RAID configurations, see [Clearing All RAID Configurations \(page 138\)](#).

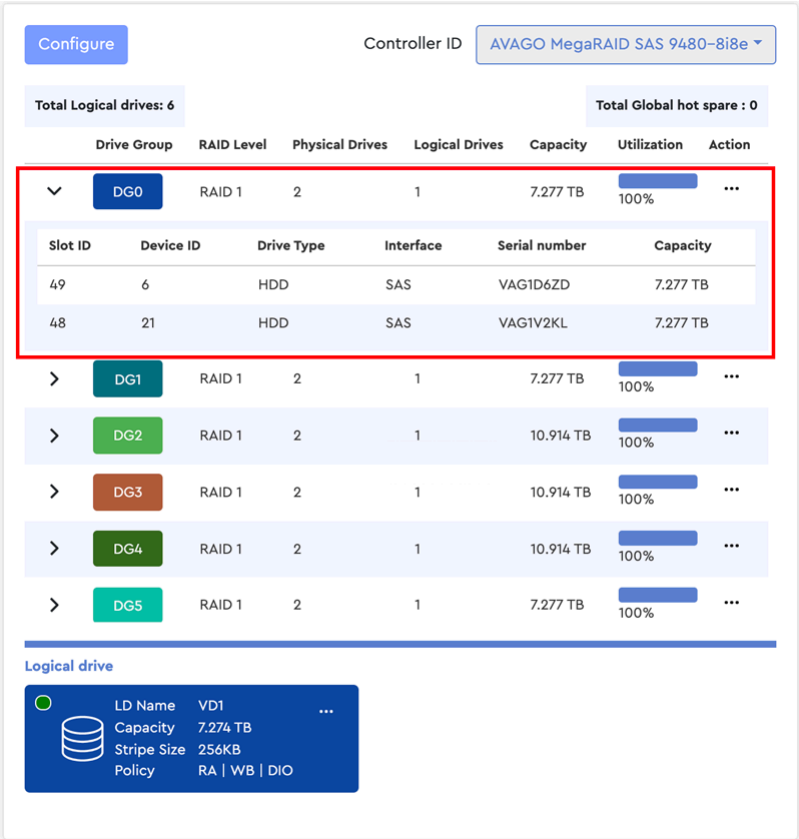
Step 1: From the navigation bar, select **MegaRAID > Logical Drives**.
The **Logical Drives** page will be displayed:

Figure 276: Logical Drives Page



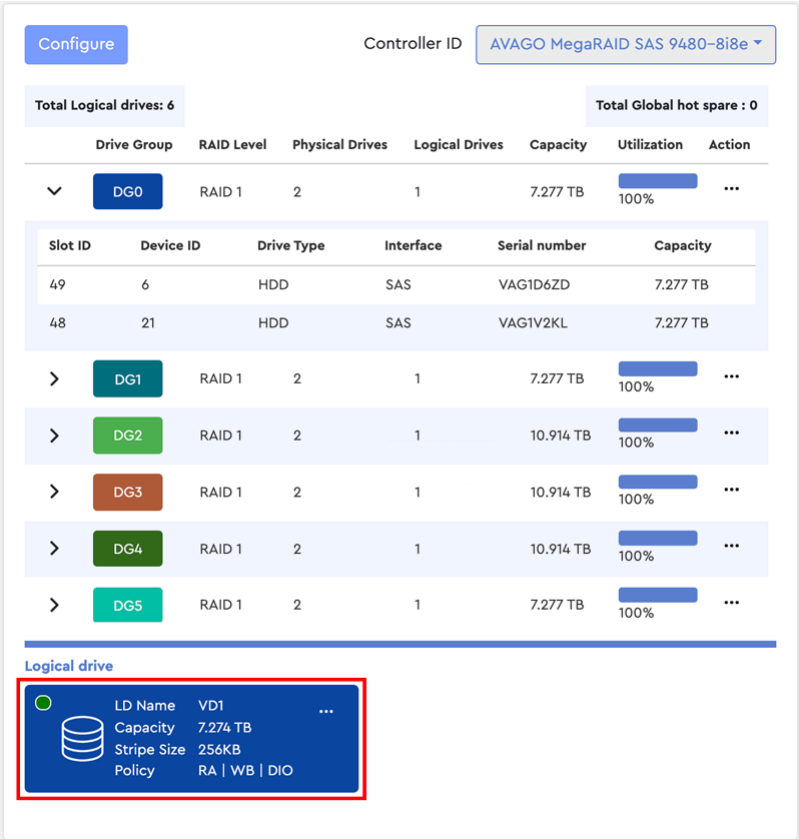
Step 2: From the right column, select a drive group to expand its details:

Figure 277: Drive Group Details



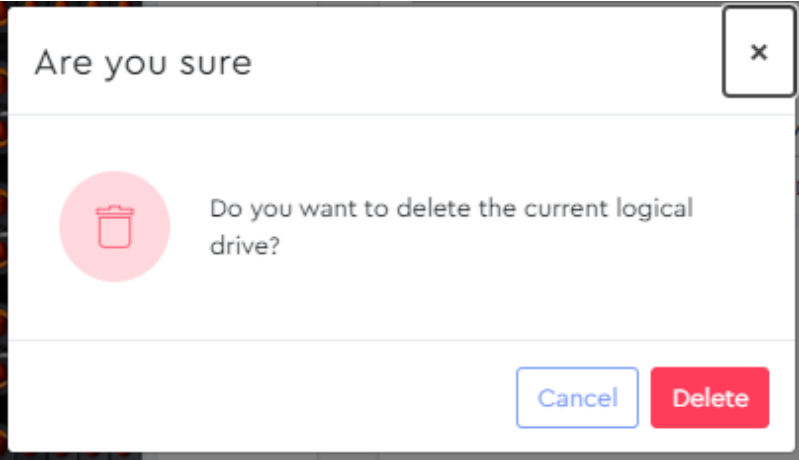
At the bottom of the column, the logical drive(s) for that group will be displayed:

Figure 278: Logical Drive Details



Step 3: Click the ellipsis (...) for the logical drive, and select the **Delete** option.
A dialogue box will appear, prompting the user to confirm deleting the logical drive:

Figure 279: Confirm Deleting Logical Drive



Step 4: Click the **Delete** button.
A success notification will appear at the top of the page:

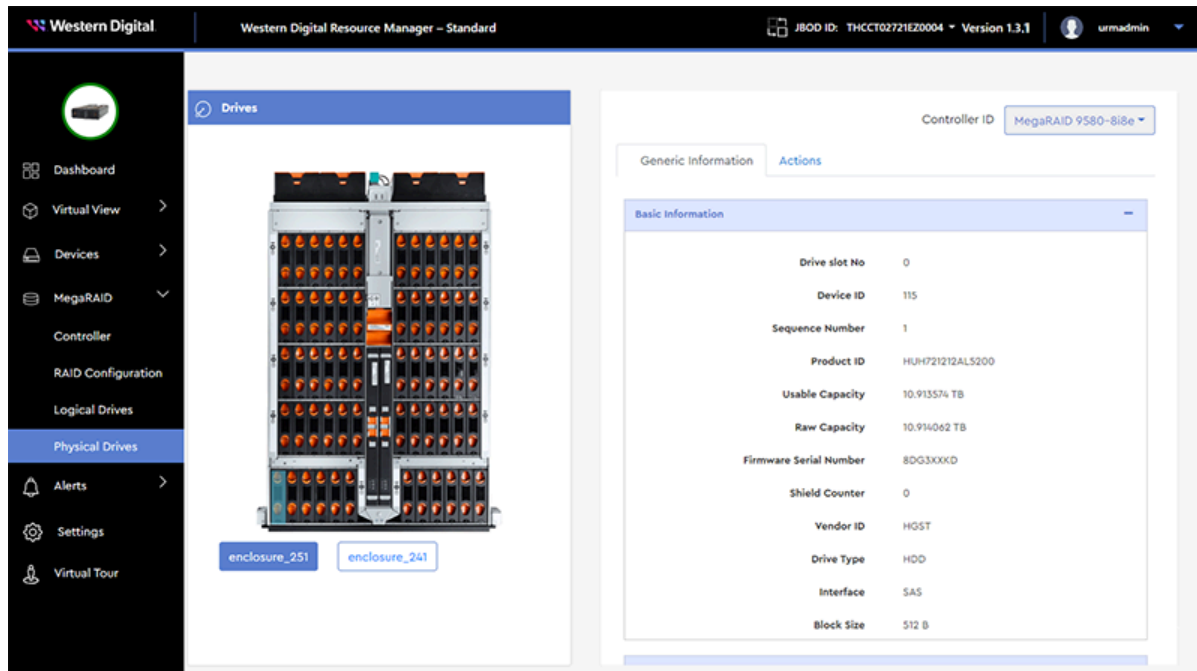
Figure 280: Success Notification



Result: The logical drive (along with its RAID configuration) has now been deleted.

3.5.4 Physical Drives

The **Physical Drives** page displays detailed information about the physical drives being managed through the selected MegaRAID controller.



3.5.4.1 Enabling / Disabling a Drive Identification LED (MegaRAID)

This procedure provides instructions for enabling (illuminating) and/or disabling a drive's identification LED when the drive is managed through a MegaRAID controller.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.



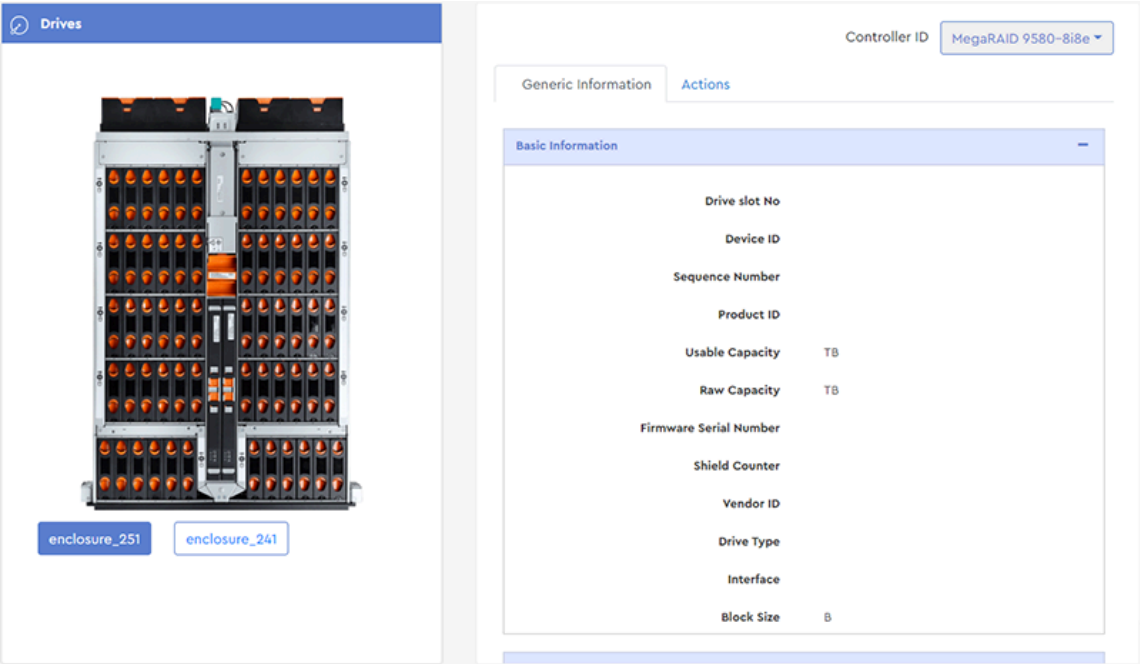
Note: To enable/disable a drive's LED through an HBA, see [Enabling / Disabling a Drive Identification LED \(HBA\) \(page 51\)](#).

Enabling a Drive Identification LED

Step 1: From the navigation bar, select **MegaRAID > Physical Drives**.

The **Physical Drives** page will be displayed:

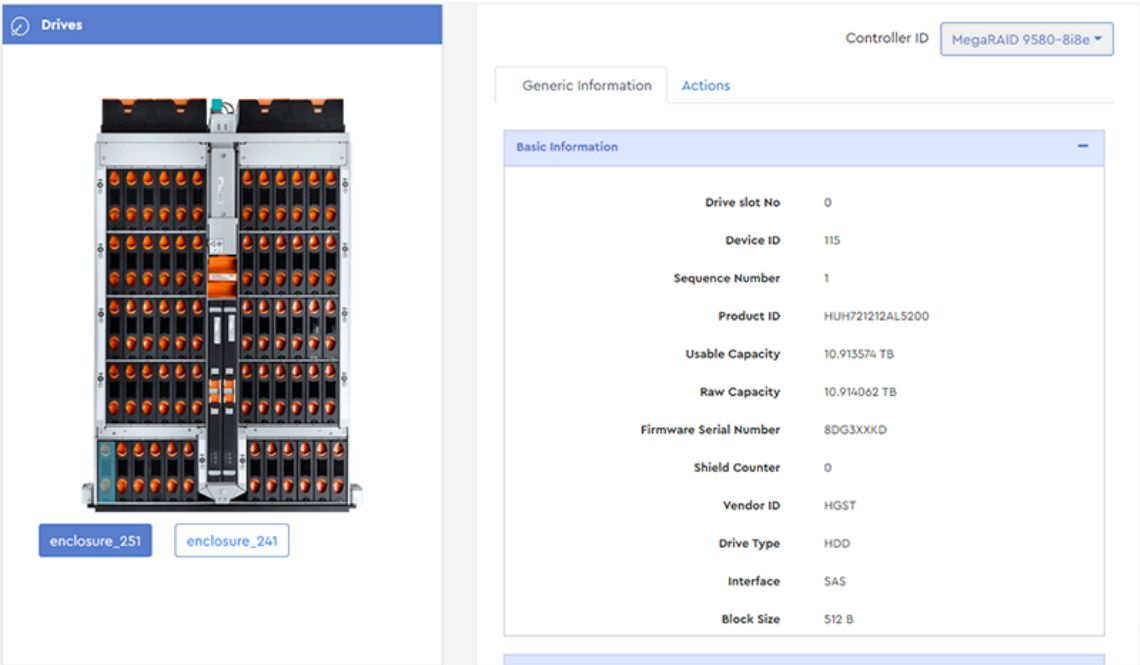
Figure 282: Physical Drives Page



Step 2: From the **Drives** image on the left, click to select a drive slot.

The **Generic Information** tab on the right will display the available information about the drive installed in the selected slot.

Figure 283: Generic Information



Step 3: Click the **Actions** tab.
The actions tab will be displayed:

Figure 284: Actions Tab



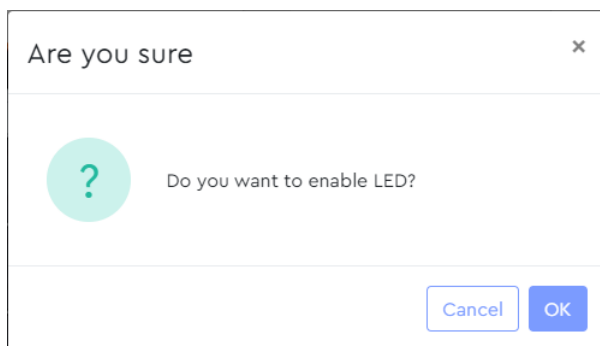
Step 4: In the **LED Status** section, click the **Locate** link.

Figure 285: Locate Link



A dialogue box will appear, prompting the user to confirm enabling the drive's identification LED:

Figure 286: Confirm Enabling LED



Step 5: Click the **OK** button.

A success notification will appear at the top of the page:

Figure 287: Success Notification



Disabling a Drive Identification LED

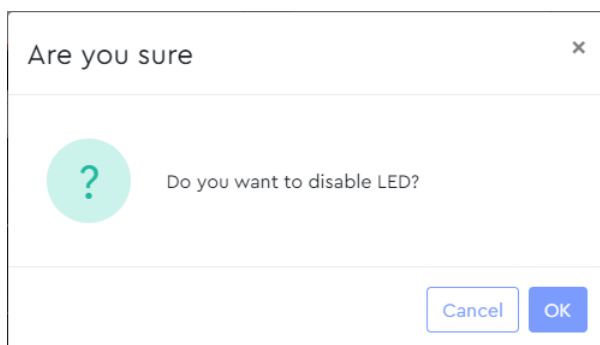
Step 6: In the **LED Status** section, click the **Stop Locating** link.

Figure 288: Stop Locating Link



A dialogue box will appear, prompting the user to confirm disabling the drive's identification LED:

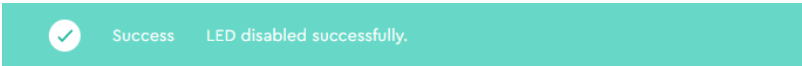
Figure 289: Confirm Disabling LED



Step 7: Click the **OK** button.

A success notification will appear at the top of the page:

Figure 290: Success Notification



Result: The selected drive's identification LED has now been enabled and/or disabled.

3.5.4.2 Updating Drive Firmware, Single Drive (MegaRAID)

This procedure provides instructions for updating firmware on a single drive, when that drive is managed through a MegaRAID controller.

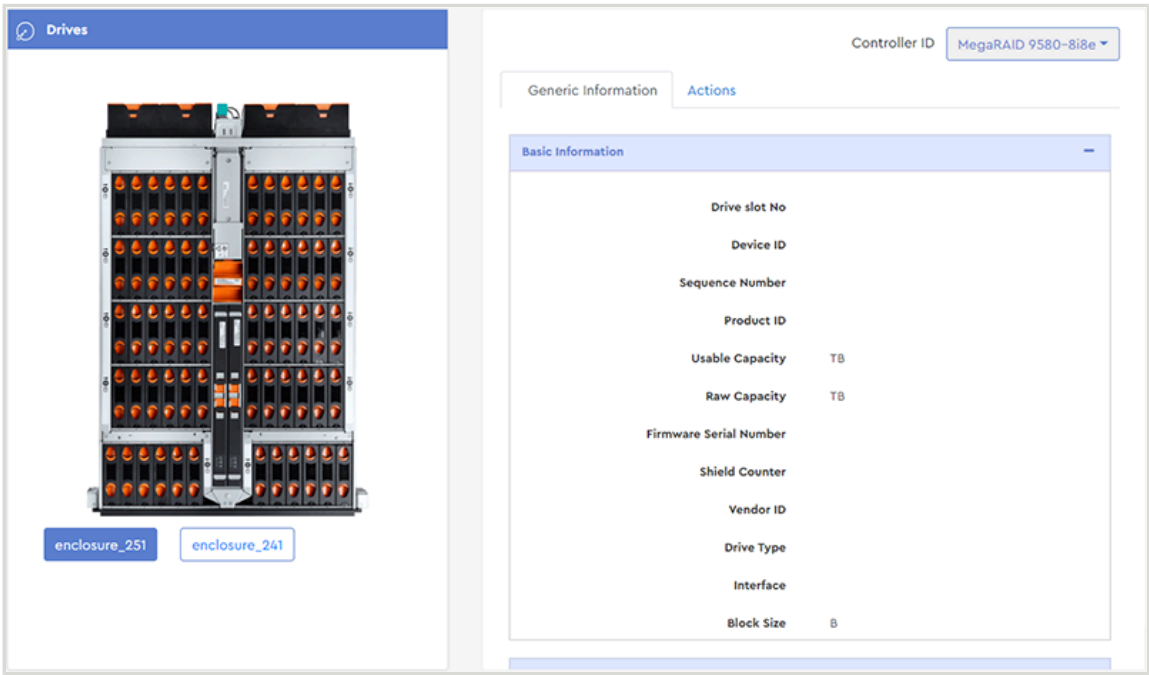
Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.



Note: To update a single drive's firmware through an HBA, see [Updating Drive Firmware, Single Drive \(HBA\) \(page 55\)](#).

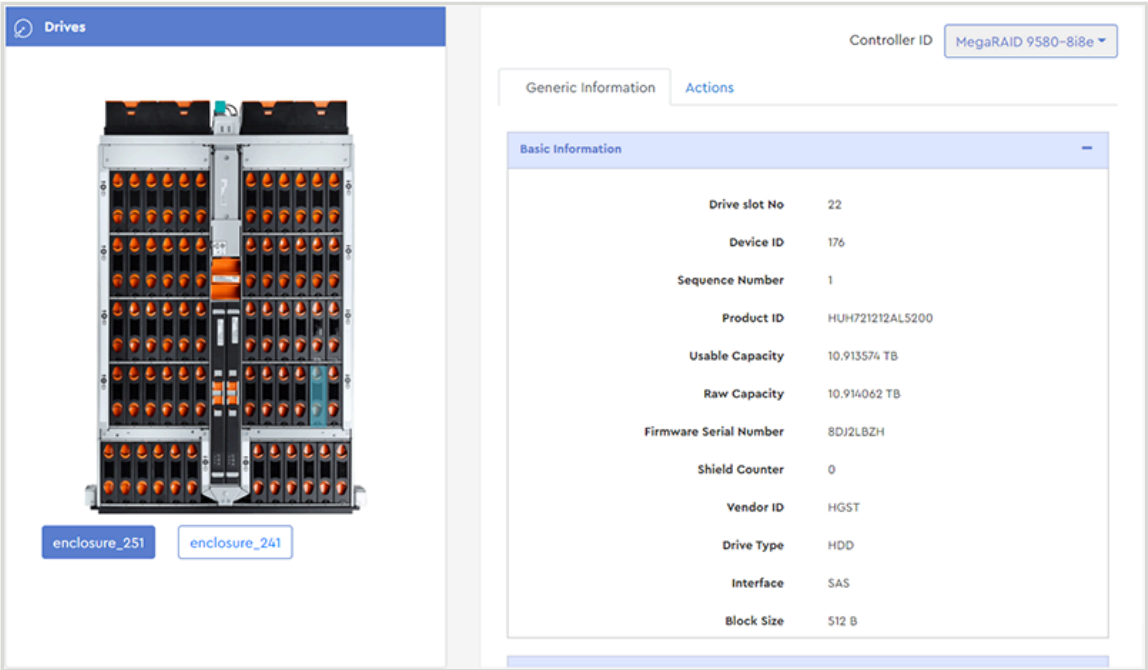
Step 1: From the navigation bar, select **MegaRAID > Physical Drives**.
The **Physical Drives** page will be displayed:

Figure 291: Physical Drives Page



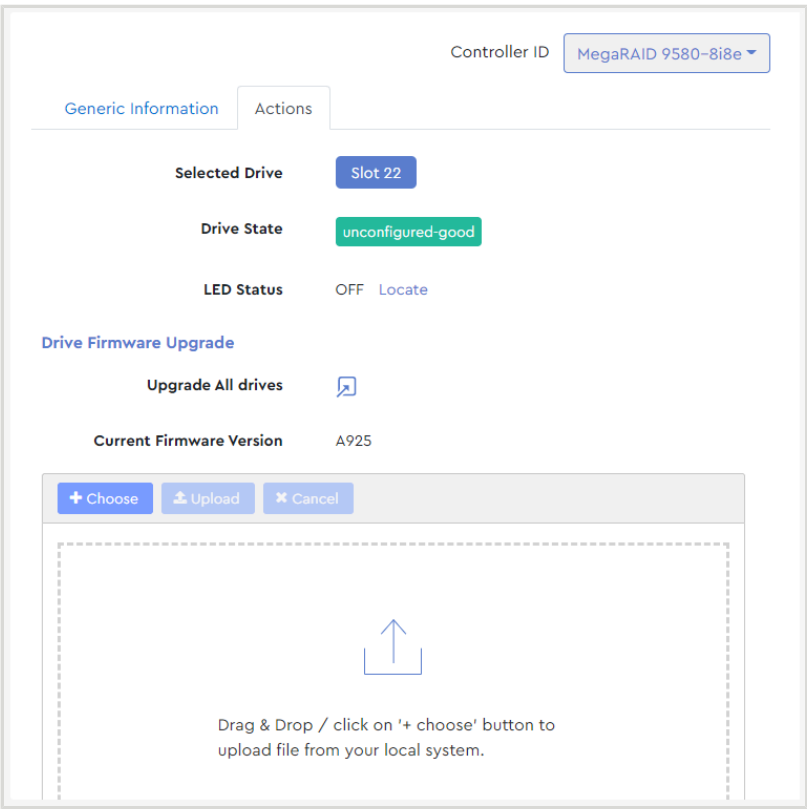
Step 2: From the **Drives** section on the left, click to select a drive slot.
The drive will be highlighted, and **Generic Information** tab on the right will display the available information about the drive installed in the selected slot:

Figure 292: Generic Information



- Step 3:** Click the **Actions** tab.
- The **Actions** tab will display information about the installed drive and available actions:

Figure 293: Actions Section



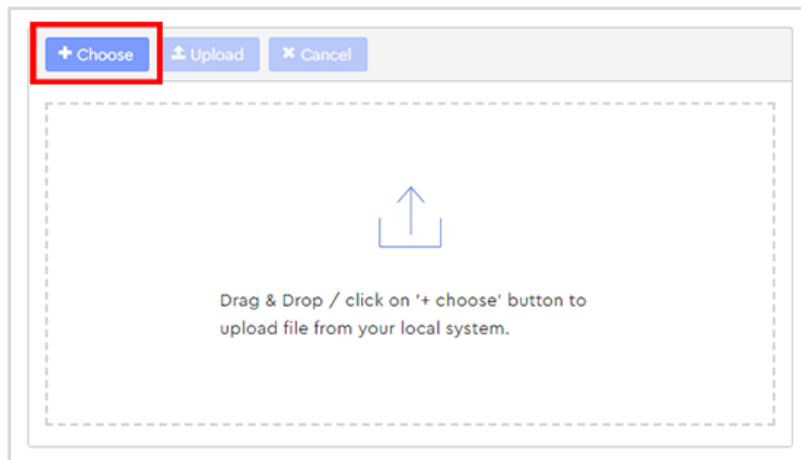
Take note of the **Current Firmware Version** for this drive, as this will be used to confirm a successful update at the end of this procedure:

Figure 294: Current Firmware Version



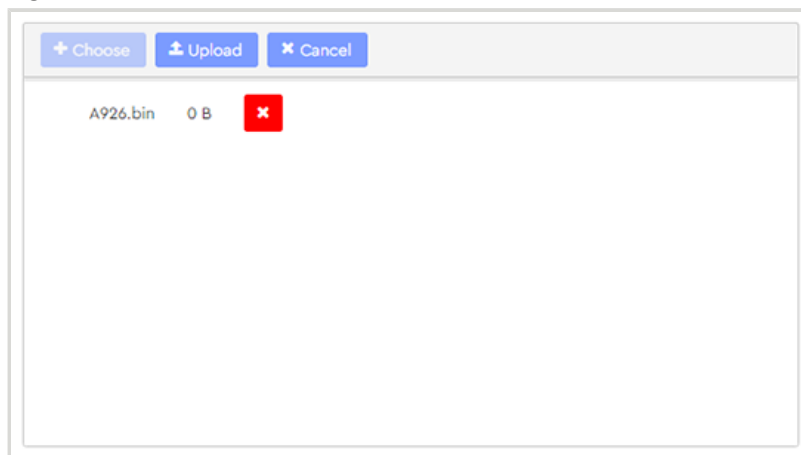
Step 4: Either drag & drop a drive firmware file onto the **Drag & Drop** section, or click the **Choose** button, which will open your operating system's file browser and allow you to browse and select the firmware file.

Figure 295: Choose Button



Step 5: Once selected, the drive firmware file will appear in the **Drag & Drop** section.

Figure 296: Firmware File Selected



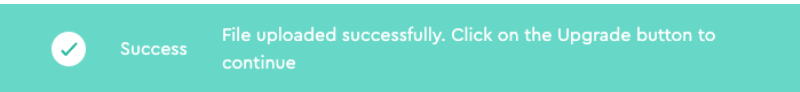
Step 6: Click the **Upload** button to upload the firmware to the drive.

Figure 297: Upload Firmware



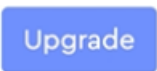
After the firmware is uploaded, a success notification will appear at the top of the page:

Figure 298: Success Notification



Step 7: As prompted, click the **Upgrade** button to upgrade the firmware:

Figure 299: Upgrade Button



Step 8: After the firmware has been updated, compare the **Current Firmware Version** to the version noted at the beginning of this procedure:

Figure 300: Updated Firmware



Result: The drive's firmware has now been updated.

3.5.4.3 Updating Drive Firmware, Multiple Drives (MegaRAID)

This procedure provides instructions for updating firmware on multiple drives (of the same drive model), when those drives are managed through a MegaRAID controller.

Before you begin: Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

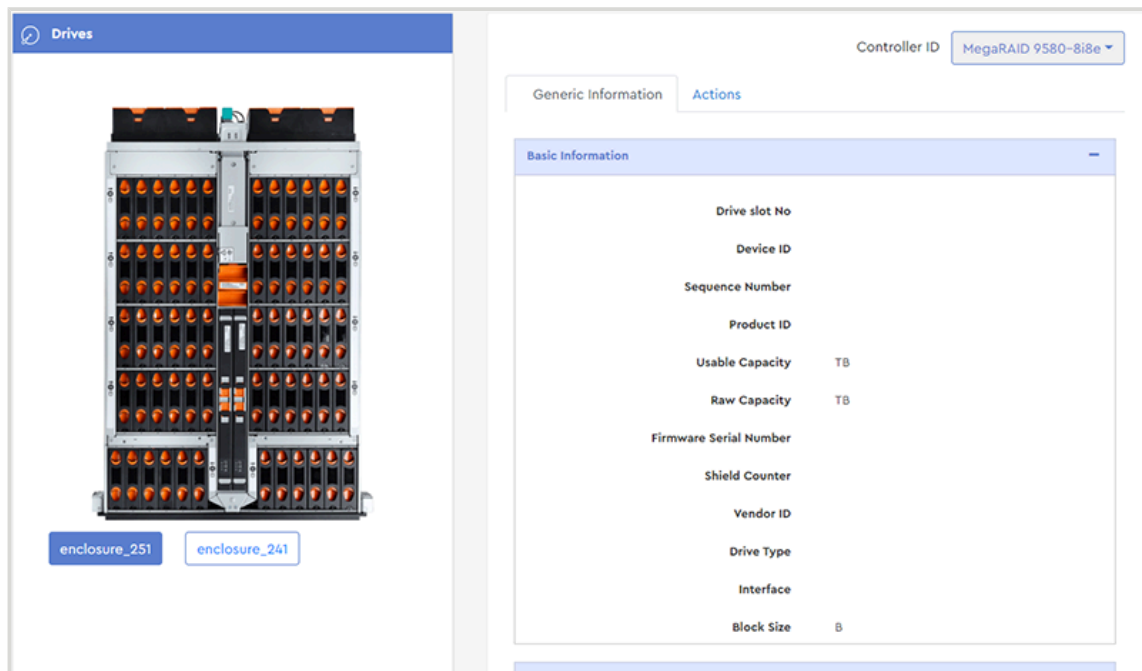


Note: To update firmware on multiple drives through an HBA, see [Updating Drive Firmware, Multiple Drives \(HBA\) \(page 62\)](#).

Step 1: From the navigation bar, select **MegaRAID > Physical Drives**.

The **Physical Drives** page will be displayed:

Figure 301: Physical Drives Page



Step 2: On the right-hand side of the page, click the **Actions** tab.

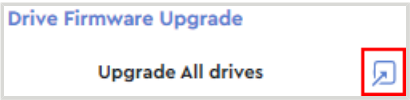
The **Actions** tab will be displayed:

Figure 302: Actions Tab



Step 3: In the **Drive Firmware Upgrade** section, click the **Upgrade All drives** icon:

Figure 303: Upgrade All Drives



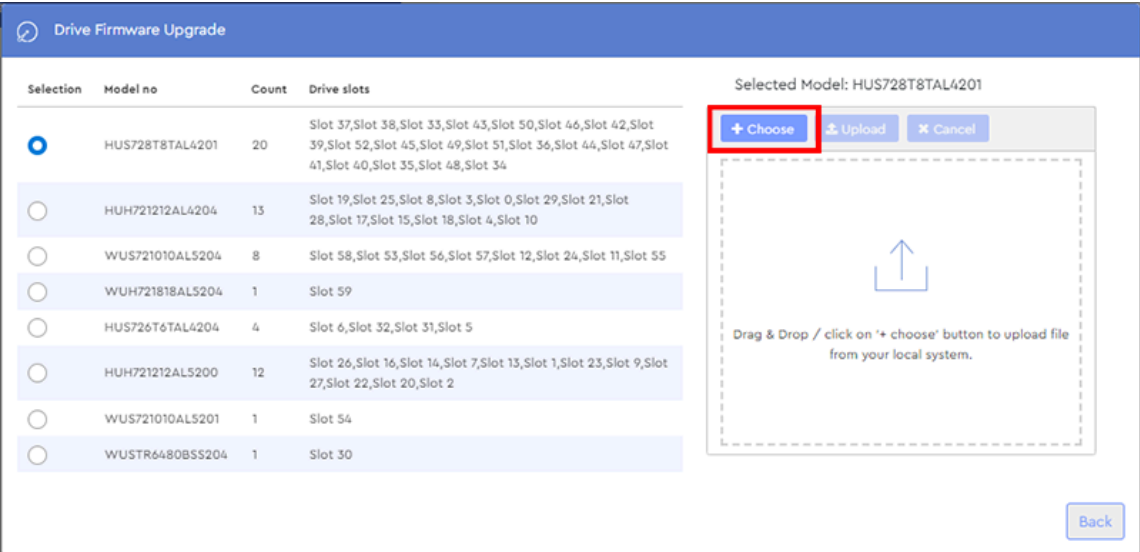
A **Drive Firmware Upgrade** window will appear, displaying a list of installed drive models, the quantity of each model, and the slot numbers where they are installed.

Figure 304: Drive Firmware Upgrade



Step 4: Click one of the radio buttons in the **Selection** column to select a drive model (and the associated drives). Then click the **Choose** button:

Figure 305: Choose Button



This will open your operating system's file browser and allow you to locate and select the firmware file.

Step 5: Once selected, the drive firmware file will appear in the **Drag & Drop** section:

Figure 306: Firmware File Selected



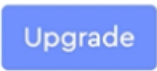
Step 6: Click the **Upload** button to upload the firmware to the selected drives.

Figure 307: Upload Firmware



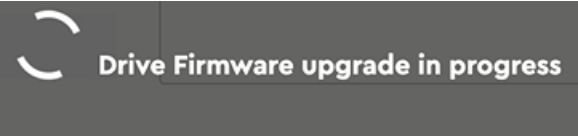
Step 7: After the firmware is uploaded, click the **Upgrade** button to upgrade the firmware:

Figure 308: Upgrade Button



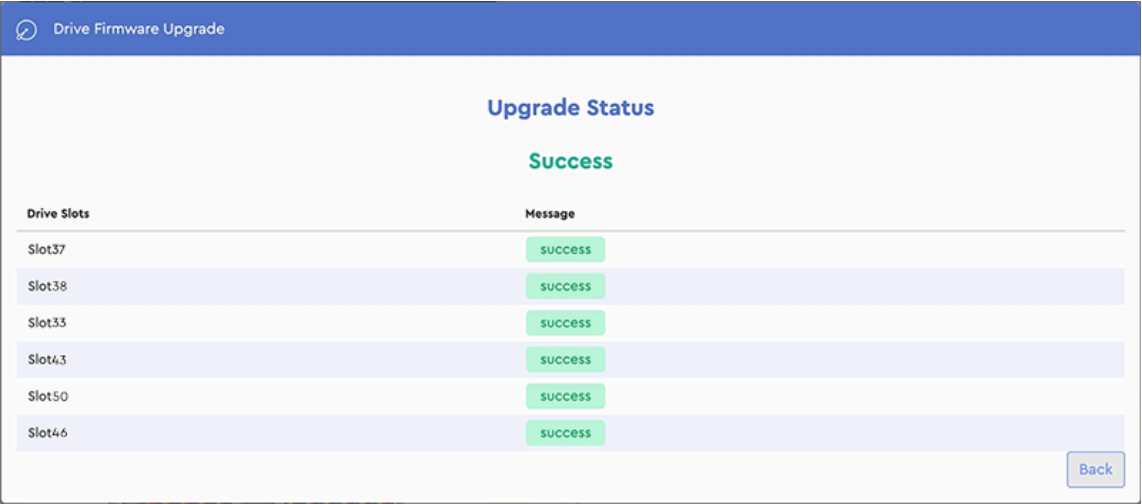
A notification will appear on the page during the upgrade:

Figure 309: Upgrade In Progress



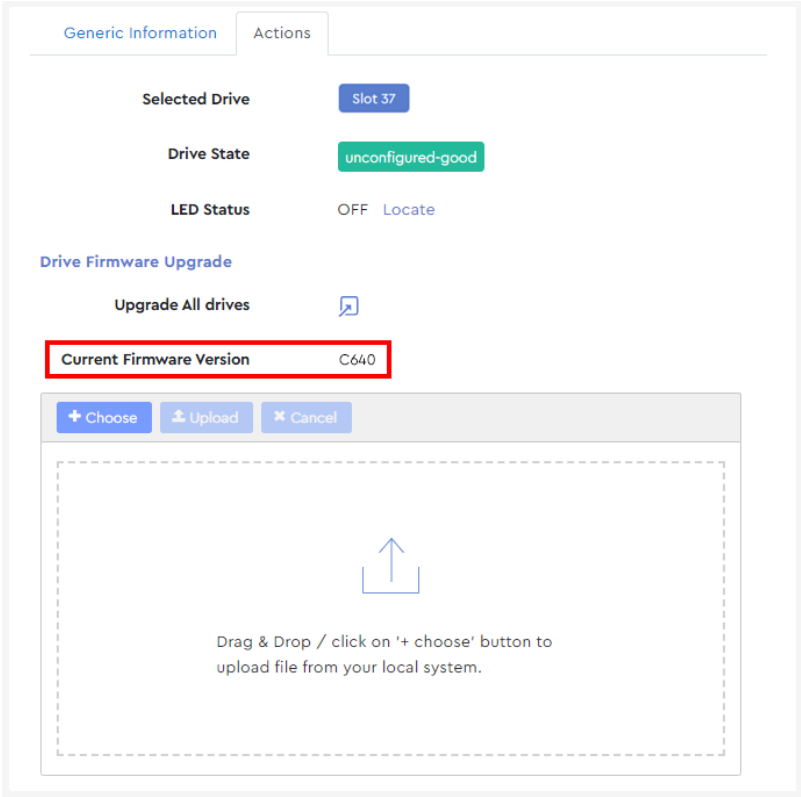
When the upgrade is finished, a success notification will be displayed:

Figure 310: Upgrade Success



- Step 8:** Click the **Back** button, return to the **Actions** tab, and select one of the slots that was included in the group.
- Step 9:** Review the **Current Firmware Version** to verify that it matches the uploaded drive firmware:

Figure 311: Current Firmware Version



Result: The drives' firmware has now been updated.

3.6 Alerts

The **Alerts** section provides information and controls for setting up email notifications, configuring SMTP settings, checking event logs, and downloading SES firmware and system log files.

3.6.1 Configuring Email Notifications

This procedure provides instructions for setting up email notifications for enclosure events. To configure the SMTP settings that will be used when notifications are sent, see [Configuring SMTP \(page 185\)](#).

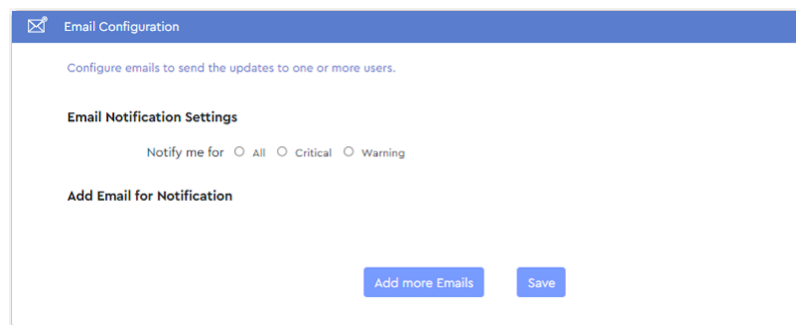
Before you begin:

1. Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **Alerts > Email configuration**.

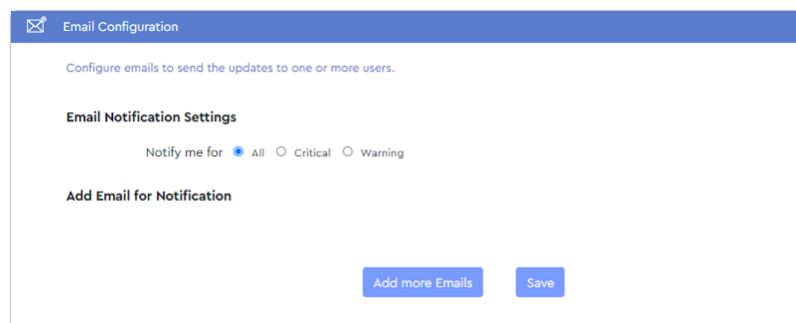
The **Email Configuration** page will be displayed:

Figure 312: Email Configuration Page



Step 2: In the **Email Notification Settings** section, click the radio button to be notified for **All**, **Critical**, or **Warning** events.

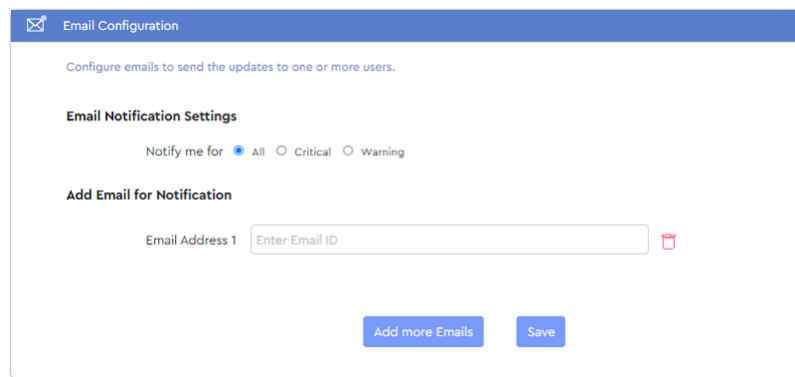
Figure 313: Email Notification Settings



Step 3: In the **Add Email for Notification** section, click the **Add more Emails** button.

An email address field will appear:

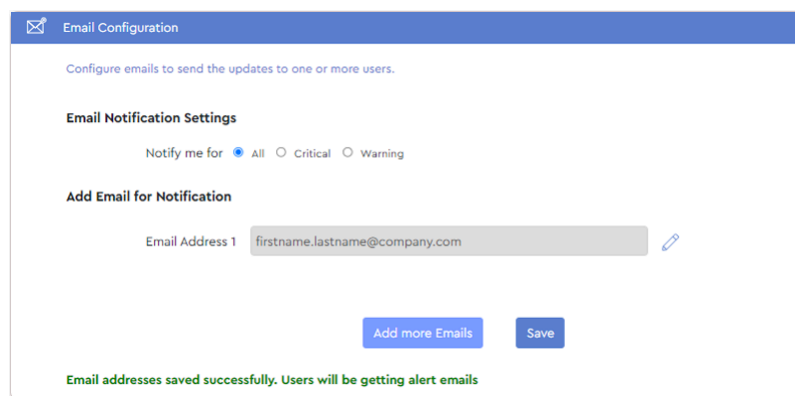
Figure 314: Email Address Field



The screenshot shows the 'Email Configuration' page. At the top, there's a header with an envelope icon and the title 'Email Configuration'. Below it, a subtitle reads 'Configure emails to send the updates to one or more users.' The main section is titled 'Email Notification Settings' and contains a 'Notify me for' section with three radio buttons: 'All' (selected), 'Critical', and 'Warning'. Below this is the 'Add Email for Notification' section, which includes a label 'Email Address 1' and a text input field containing the placeholder text 'Enter Email ID'. To the right of the input field is a red trash icon. At the bottom of the form are two blue buttons: 'Add more Emails' and 'Save'.

Step 4: Type a valid email address into the field and click the **Save** button.
A confirmation message will be displayed at the bottom of the **Email Configuration** page:

Figure 315: Email Address Saved



This screenshot shows the 'Email Configuration' page after an email address has been saved. The 'Email Address 1' field now contains the text 'firstname.lastname@company.com' and has a blue edit icon to its right. The 'Add more Emails' and 'Save' buttons remain at the bottom. A green confirmation message at the bottom of the page reads: 'Email addresses saved successfully. Users will be getting alert emails'.

Step 5: Repeat these steps as needed to send alerts to additional email addresses.

Result: Email notifications for enclosure events have now been configured.

3.6.2 Configuring SMTP

This procedure provides instructions for configuring the SMTP (Simple Mail Text Protocol) settings to be used when Resource Manager Standard Edition sends email alerts. For more information on configuring email notifications themselves, see [Configuring Email Notifications \(page 184\)](#).

Before you begin:

1. Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **Alerts > SMTP configuration**.

The **SMTP Configurations** page will be displayed:

Figure 316: SMTP Configuration Page

SMTP Configurations

The following SMTP mail server settings allows Resource Manager application to send emails

From Email Address

From Name

SMTP Host or IP

SMTP server port number

SMTP User

SMTP Password

Type of Encryption ☒ None ☐ SSL ☐ TLS

StartTLS enable ☐

Step 2: Enter the appropriate information (Email Address, Sender Name, etc.) in the text fields, and if needed, select the type of encryption using the radio buttons.

Step 3: Click the **Save** button to save the configuration.

Result: SMTP has now been configured.

3.6.3 Viewing / Downloading Events

This procedure provides instructions for viewing and downloading enclosure events.

Before you begin:

1. Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **Alerts > Events**.

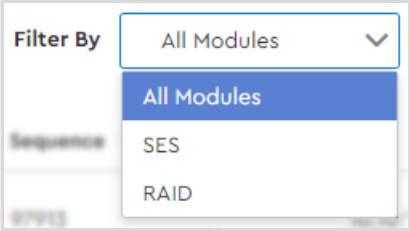
The **Events** page will be displayed:

Figure 317: Events Page

Sequence	Date	Time	Module	Event	Severity	Group	Description
97913	2022-11-16	16:10:17	RAID	MR-Controller Event	Information	RAID	CTLR:1:MegaRAID 9580-8i8e: PD 20(e0x9/s55) Inquiry info: Info- WDC WUS721010AL5204 VCG1P2N 10 TB
97912	2022-11-16	16:10:17	RAID	MR-Controller Event	Information	RAID	CTLR:1:MegaRAID 9580-8i8e: Inserted: PD 20(e0x9/s55) Info: encIPd-f9, scsiType=0, portMap=10, sasAddr=5000cca0b00319e2
97911	2022-11-16	16:10:17	RAID	MR-Controller Event	Information	RAID	CTLR:1:MegaRAID 9580-8i8e: Inserted: PD 20(e0x9/s55)
97910	2022-11-16	16:10:17	RAID	MR-Controller Event	Information	RAID	CTLR:1:MegaRAID 9580-8i8e: PD 1f(e0x8/s26) Inquiry info: Info- HGST HUH721212AL5200 8D13H66H 12 TB
97909	2022-11-16	16:10:17	RAID	MR-Controller Event	Information	RAID	CTLR:1:MegaRAID 9580-8i8e: Inserted: PD 1f(e0x8/s26) Info: encIPd-f8, scsiType=0, portMap=10, sasAddr=5000cca2537714b9,5000cca2537714ba
97908	2022-11-16	16:10:17	RAID	MR-Controller Event	Information	RAID	CTLR:1:MegaRAID 9580-8i8e: Inserted: PD 1f(e0x8/s26)
97907	2022-11-16	16:10:17	RAID	MR-Controller Event	Information	RAID	CTLR:1:MegaRAID 9580-8i8e: PD 1e(e0x9/s9) Inquiry info: Info- HGST HUH721212AL4204 8DG3U1YD 12 TB
97906	2022-11-16	16:10:17	RAID	MR-Controller Event	Information	RAID	CTLR:1:MegaRAID 9580-8i8e: Inserted: PD 1e(e0x9/s9) Info: encIPd-f9, scsiType=0, portMap=10, sasAddr=5000cca25306ecc9,5000cca25306ecca
97905	2022-11-16	16:10:17	RAID	MR-Controller Event	Information	RAID	CTLR:1:MegaRAID 9580-8i8e: Inserted: PD 1e(e0x9/s9)
97904	2022-11-16	16:10:17	RAID	MR-Controller Event	Information	RAID	CTLR:1:MegaRAID 9580-8i8e: PD 1d(e0x8/s25) Inquiry info: Info- HGST HUH721212AL4204 8DGN1GEH 12 TB

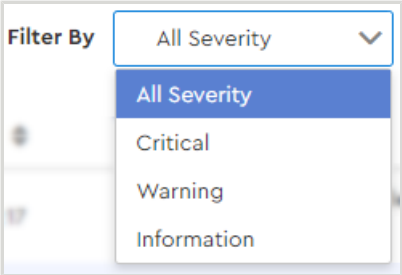
Step 2: If needed, use the **Modules** drop-down to filter the list for SES or RAID events.

Figure 318: Modules Drop-Down



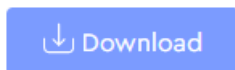
Step 3: If needed, use the **Severity** drop-down to filter the list for Critical, Warning, or Information events.

Figure 319: Severity Drop-Down



Step 4: If needed, click the **Download** button to download a PDF copy of the events list.

Figure 320: Events Download Button



Result: Enclosure events have now been viewed / downloaded.

3.6.4 Downloading Logs

This procedure provides instructions for downloading enclosure logs.

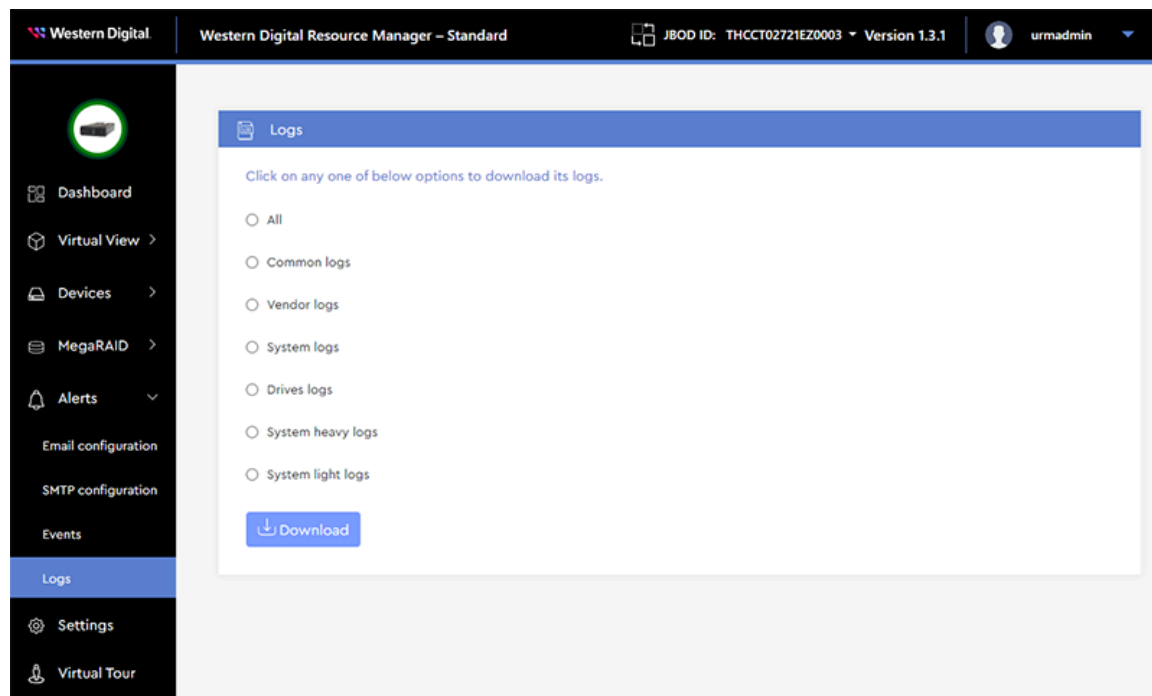
Before you begin:

1. Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **Alerts > Logs**.

The **Logs** page will be displayed:

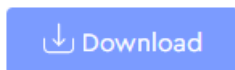
Figure 321: Logs Page



Step 2: Use the radio buttons to select the type of logs to be downloaded (choose one).

Step 3: Click the **Download** button to download an archive file of the logs.

Figure 322: Logs Download Button



Result: Enclosure logs have now been downloaded.

3.7 Settings

The **Settings** section allows configuration of user account details such as IDs, roles, email addresses, and passwords.

3.7.1 Adding an Account

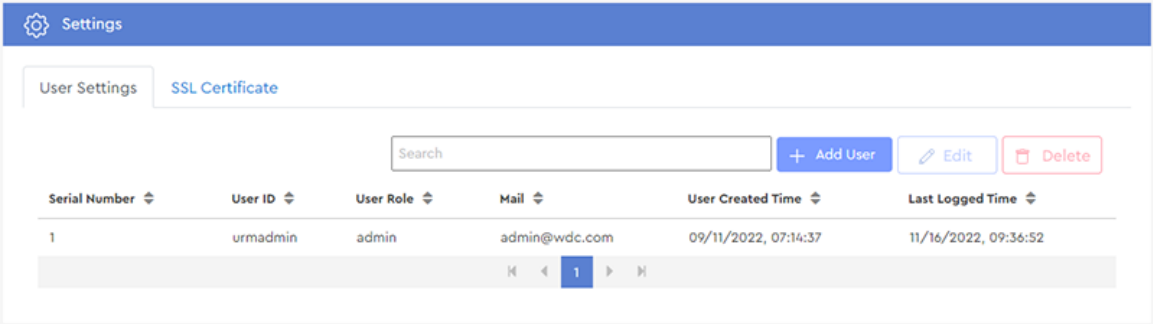
This procedure provides instructions for adding a user or admin account.

Before you begin:

- 1. Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **Settings**.
The **Settings** page will be displayed:

Figure 323: Settings Page



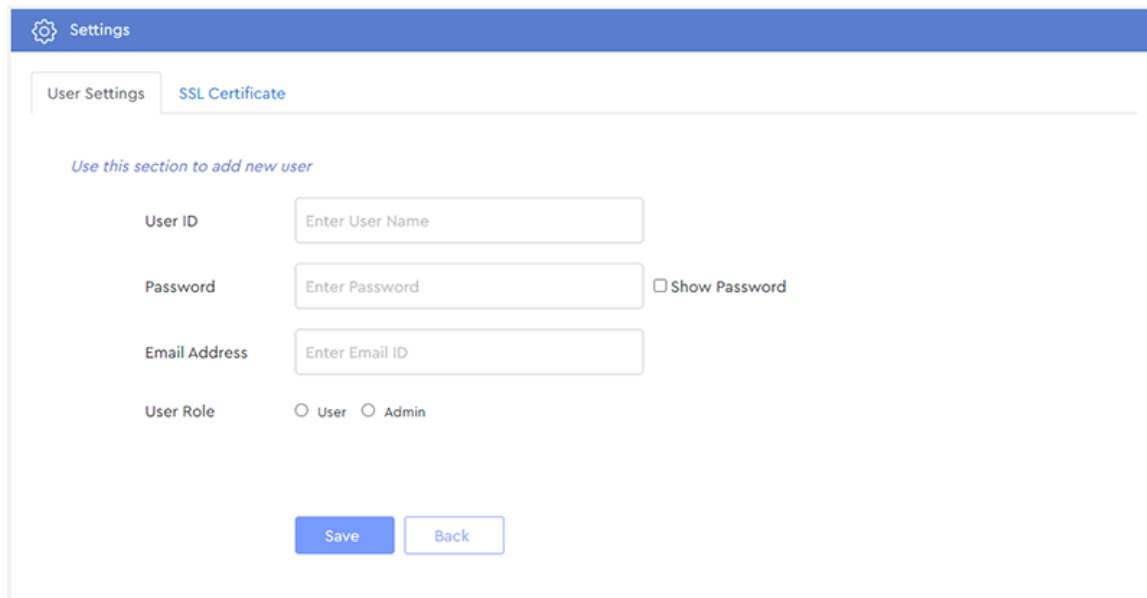
Step 2: From the **User Settings** tab, click the **Add User** button:

Figure 324: Add User Button



The user settings for the new account will be displayed:

Figure 325: User Settings for New Account



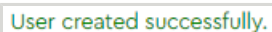
The screenshot shows a web interface for adding a new user. At the top is a blue header bar with a gear icon and the word "Settings". Below this is a tabbed interface with "User Settings" selected and "SSL Certificate" as an alternative tab. A blue instruction text reads "Use this section to add new user". The form contains four fields: "User ID" with a placeholder "Enter User Name", "Password" with a placeholder "Enter Password" and a "Show Password" checkbox, "Email Address" with a placeholder "Enter Email ID", and "User Role" with radio buttons for "User" and "Admin". At the bottom are "Save" and "Back" buttons.

Step 3: Complete all the fields to assign a **User ID**, **Password**, **Email Address**, and **User Role** for the account.

Step 4: Click the **Save** button.

A success message will be displayed:

Figure 326: Success Message



User created successfully.

Step 5: Click the **Back** button to return to the **Settings** page.

Figure 327: Back Button



Back

Step 6: On the **Settings** page, verify that the new account appears in the accounts list.

Figure 328: Accounts List

Settings

User Settings

SSL Certificate

Search

+ Add User

Edit

Delete

Serial Number	User ID	User Role	Mail	User Created Time	Last Logged Time
1	urmadmin	admin	admin@wdc.com	09/11/2022, 07:14:37	11/16/2022, 09:36:52
2	test1	user	firstname.lastname@company.com	11/16/2022, 09:56:44	N/A

1

Result: The new account has now been added.

3.7.2 Editing an Account

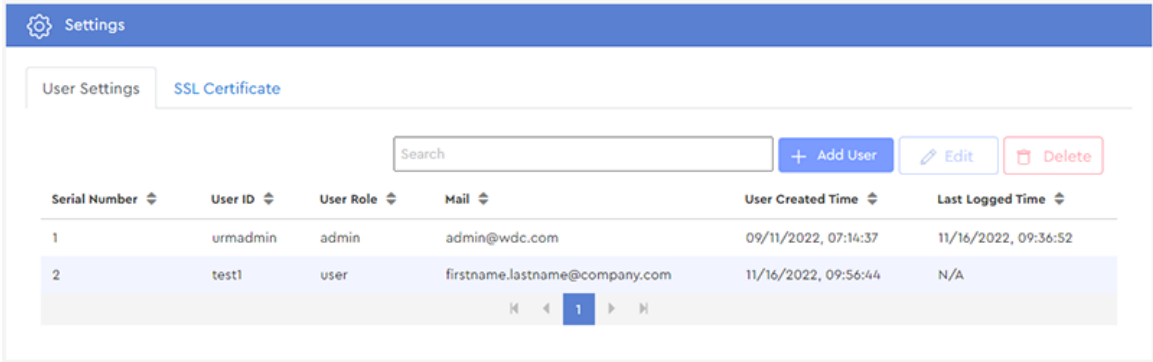
This procedure provides instructions for editing a user or admin account.

Before you begin:

- 1. Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **Settings**.
The **Settings** page will be displayed:

Figure 329: Settings Page



Step 2: Click the row of an existing account to select it. Then click the **Edit** button:

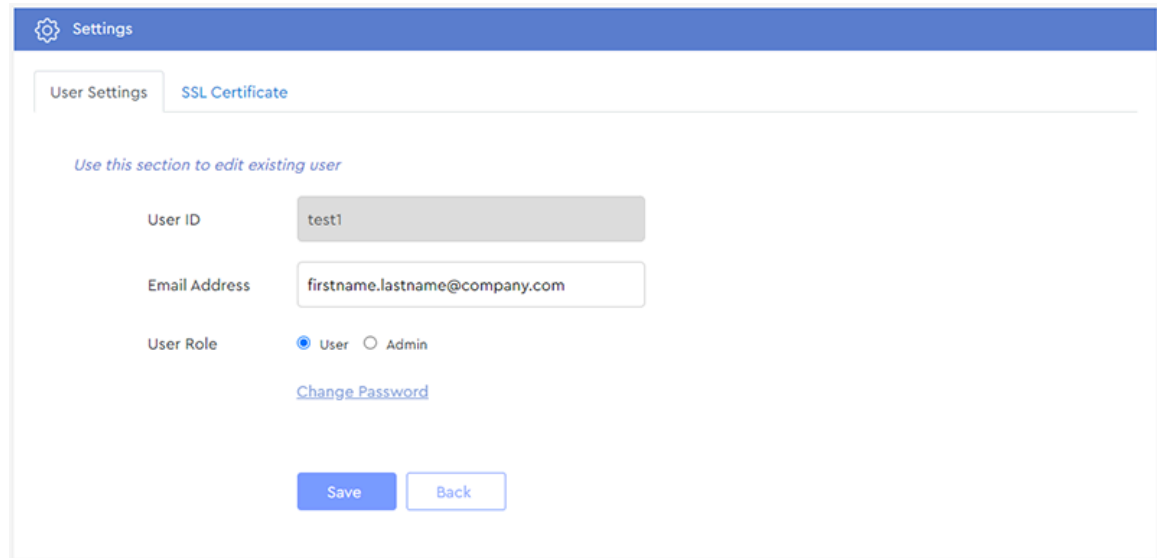
Figure 330: Edit Button



Note: The first account (urmadmin) is a default account and cannot be edited or deleted.

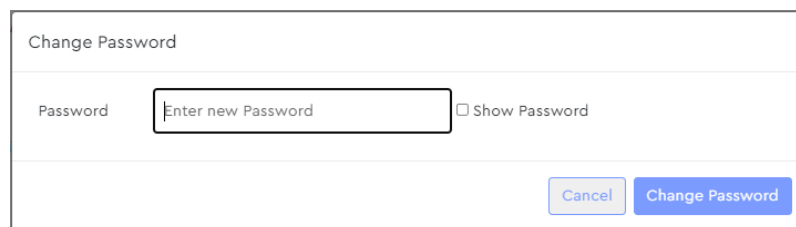
The settings for that account will be displayed:

Figure 331: Account Settings



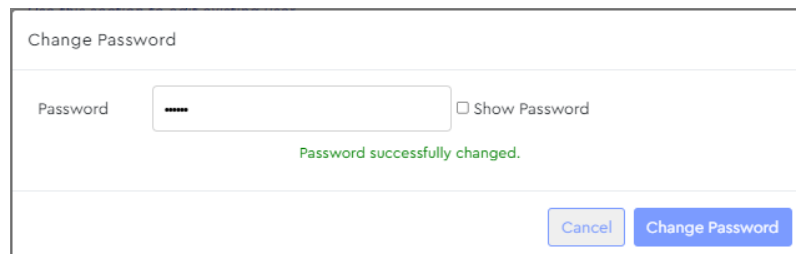
Step 3: Enter a new **Email Address**, change the **User Role**, or click **Change Password** to modify the account password.

- a. If you clicked **Change Password**, a **Change Password** dialogue box will be displayed:



- b. Enter a new password into the **Password** field and click the **Change Password** button.
The user will be notified that the password was successfully changed:

Figure 333: Password Changed Successfully



- c. Click outside of the **Change Password** dialogue box to return to the **Settings** page for the account.

Step 4: When all modifications have been made, click the **Save** button.

The user will be notified that the edits were saved:

Figure 334: User Data Saved

The screenshot shows a web interface for user management. At the top, there's a blue header with a gear icon and the word 'Settings'. Below this, there are two tabs: 'User Settings' and 'SSL Certificate'. The 'User Settings' tab is selected. Underneath the tabs, there's a blue instruction: 'Use this section to edit existing user'. The form contains three main sections: 'User ID' with a text input field containing 'test1'; 'Email Address' with a text input field containing 'firstname.lastname@company.com'; and 'User Role' with two radio buttons, 'User' (which is selected) and 'Admin'. Below these fields is a blue link that says 'Change Password'. A green message 'User data saved successfully.' is displayed. At the bottom of the form are two buttons: a blue 'Save' button and a white 'Back' button with a blue border.

Step 5: Click the **Back** button to return to the **User Settings** page, showing the list of accounts.

Result: The account has now been edited.

3.7.3 Deleting an Account

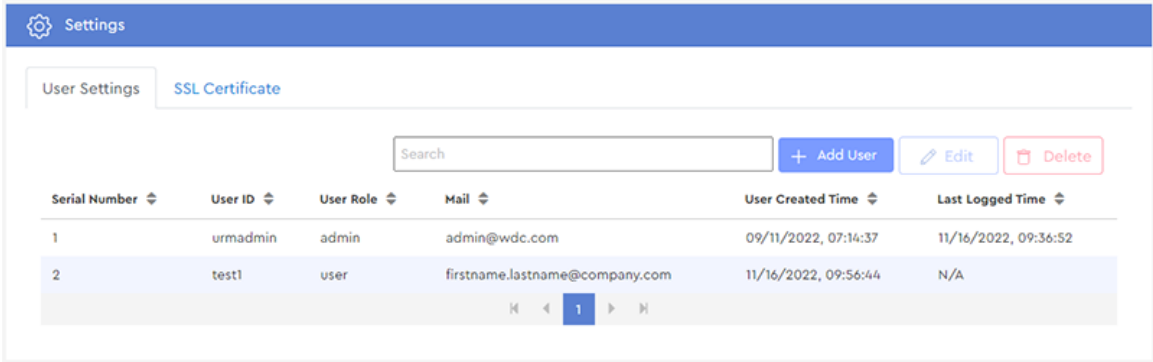
This procedure provides instructions for deleting a user or admin account.

Before you begin:

- 1. Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

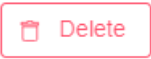
Step 1: From the navigation bar, select **Settings**.
The **Settings** page will be displayed:

Figure 335: Settings Page



Step 2: Click the row of an existing account to select it. Then click the **Delete** button:

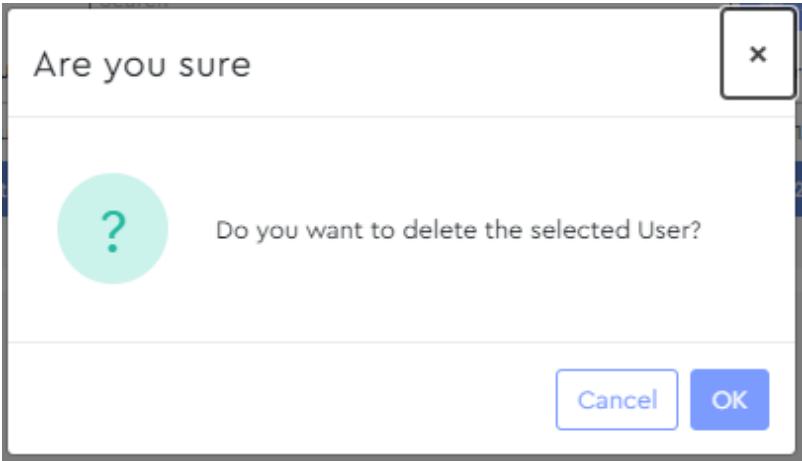
Figure 336: Delete Button



Note: The first account (urmadmin) is a default account and cannot be edited or deleted.

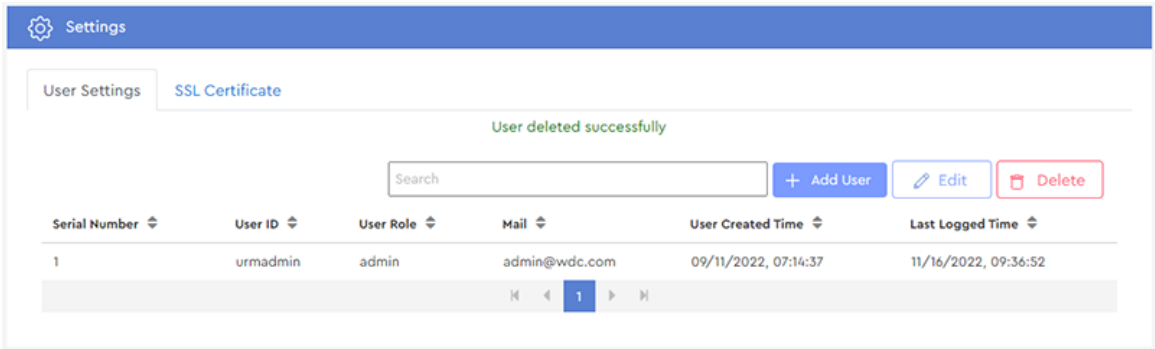
A dialogue box will appear, prompting the user to confirm the deletion:

Figure 337: Confirm Deletion Dialogue Box



Step 3: Click the **OK** button.
The account will be deleted, and the user will be notified of the successful deletion:

Figure 338: Successful Deletion



Result: The account has now been deleted.

3.7.4 Installing an SSL Certificate

This procedure provides instructions for installing an SSL certificate.

Before you begin:

1. Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

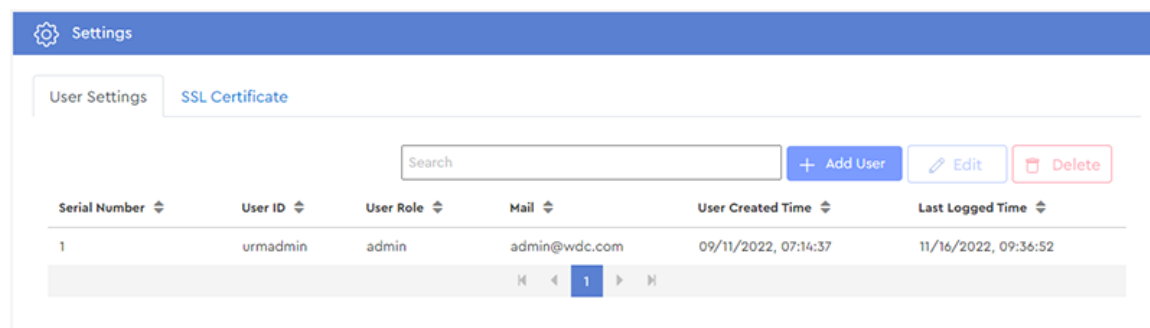


Note: Supported file types are .key, .crt, and .pem.

Step 1: From the navigation bar, select **Settings**.

The **Settings** page will be displayed:

Figure 339: Settings Page



Step 2: Click the **SSL Certificate** tab.

The **SSL Certificate** settings will be displayed:

Figure 340: SSL Certificate Settings

Settings

User SettingsSSL Certificate

SSL Certificate on this Host machine

+ Install New Certificate

Country	US
State	CA
Locality	San Jose
Organization	Western Digital Corporation
Unit	WDC
Common Name	WDC
Valid From	19/Oct/2022, 07:29:01+00:00
Valid Till	19/Oct/2023, 07:29:01+00:00
Expired	false

Step 3: Click the **Install New Certificate** button.

Figure 341: Install New Certificate Button

+ Install New Certificate

The **SSL Settings** section will update to allow selection of a certificate:

Figure 342: SSL Certificate Selection

Settings

User SettingsSSL Certificate

SSL Certificate on this Host machine

Private Key

Choose File

No file chosen

Upload

Back

Step 4: Click the **Private Key Choose File** button, navigate to the Private Key file on the host, and select it.

Figure 343: Choose File Button



The selected filename will appear in the **Private Key** field:

Figure 344: Private Key Selected



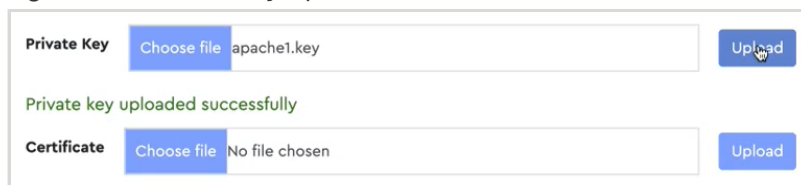
Step 5: Click the **Private Key Upload** button to upload the selected Private Key to the enclosure.

Figure 345: Upload Button



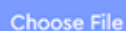
A success message will be displayed, and a **Certificate** field will appear:

Figure 346: Private Key Uploaded



Step 6: Click the **Certificate Choose File** button, navigate to the Certificate file on the host, and select it.

Figure 347: Choose File Button



The selected filename will appear in the **Certificate** field:

Figure 348: Certificate Selected



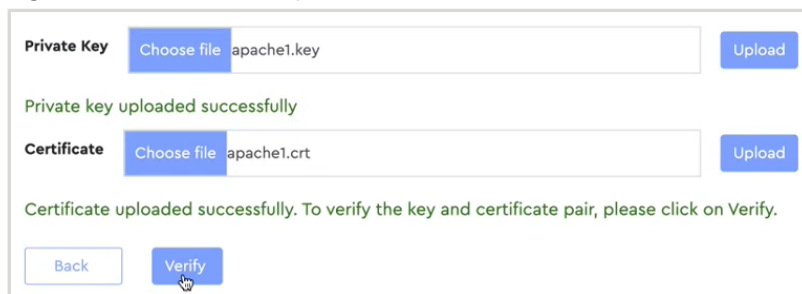
Step 7: Click the **Certificate Upload** button to upload the selected Private Key to the enclosure.

Figure 349: Upload Button



A success message will be displayed, and a **Verify** button will appear:

Figure 350: Certificate Uploaded



The screenshot shows a web interface for uploading certificates. It has two sections: 'Private Key' and 'Certificate'. Each section has a 'Choose file' button and an 'Upload' button. The 'Private Key' section shows 'apache1.key' and a green message 'Private key uploaded successfully'. The 'Certificate' section shows 'apache1.crt' and a green message 'Certificate uploaded successfully. To verify the key and certificate pair, please click on Verify.' At the bottom, there are 'Back' and 'Verify' buttons.

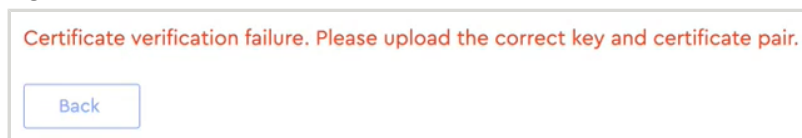
Step 8: Click the **Verify** button to validate the contents and compatibility of the Private Key and Certificate pair.

Figure 351: Verify Button



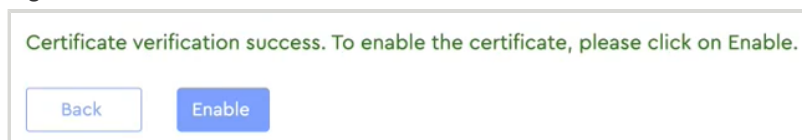
If the verification fails, a failure message will be displayed:

Figure 352: Verification Failure



If the verification passes, a success message will be displayed:

Figure 353: Verification Success



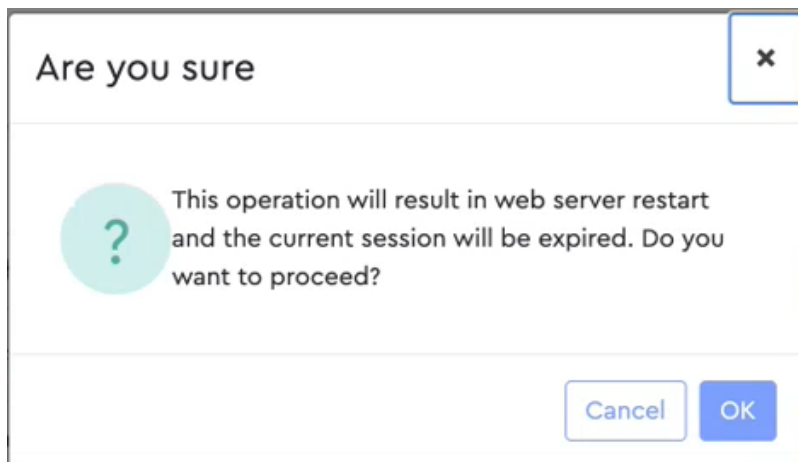
Step 9: After successful verification of the Private Key and Certificate pair, click the **Enable** button.

Figure 354: Enable Button



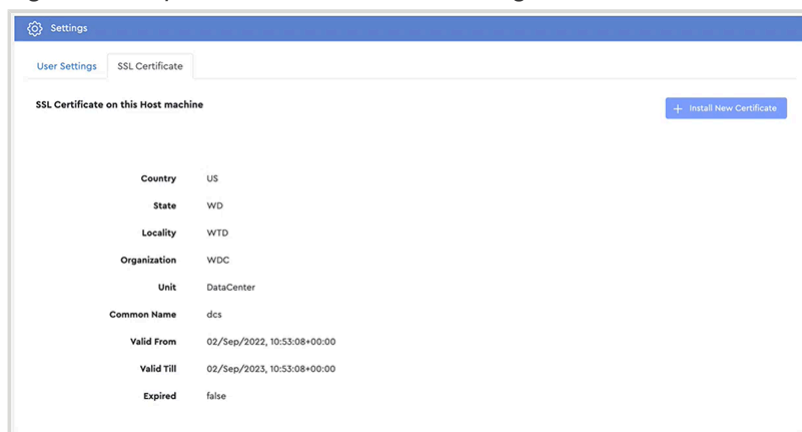
A confirmation dialog box will appear:

Figure 355: Enable Confirmation



- Step 10:** Click the **OK** button to restart the web server and apply the Private Key and Certificate pair. When the web server has restarted, the login screen will appear.
- Step 11:** Log back in to the Resource Manager Standard Edition application. If needed, see [Accessing Resource Manager Standard Edition \(page 30\)](#) for login instructions.
- Step 12:** From the navigation bar, select **Settings > SSL Certificate** and view the updated SSL Certificate settings.

Figure 356: Updated SSL Certificate Settings



Result: The SSL certificate has now been installed.

3.8 Virtual Tour

The **Virtual Tour** section guides users through the Resource Manager Standard Edition graphical interface, providing tooltip explanations of menu options and page sections.

3.8.1 Taking a Virtual Tour

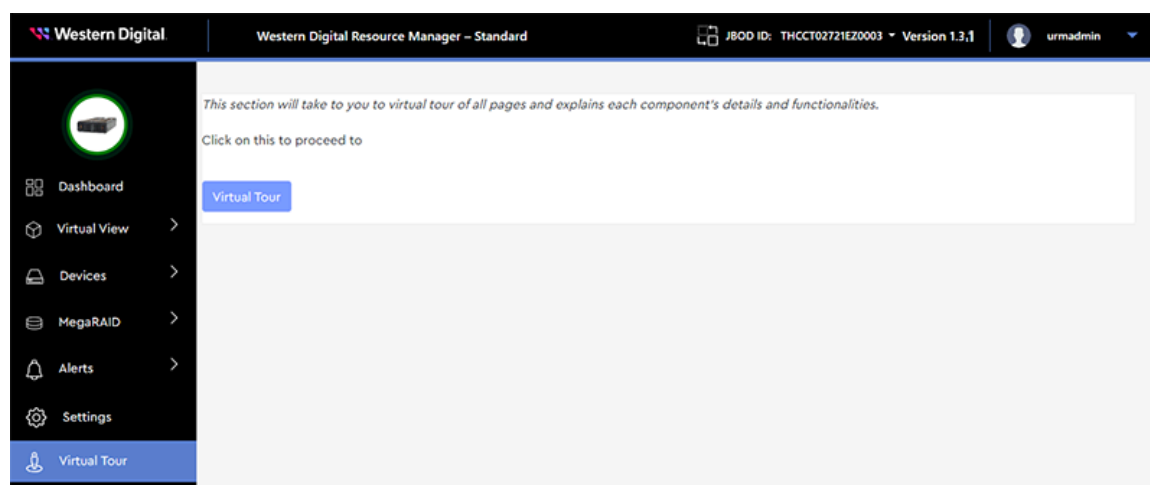
This procedure provides instructions for taking a virtual tour of the Resource Manager Standard Edition graphical user interface (GUI).

Before you begin:

1. Follow the instructions in [Accessing Resource Manager Standard Edition \(page 30\)](#) to log into the Resource Manager Standard Edition application.

Step 1: From the navigation bar, select **Virtual Tour**.

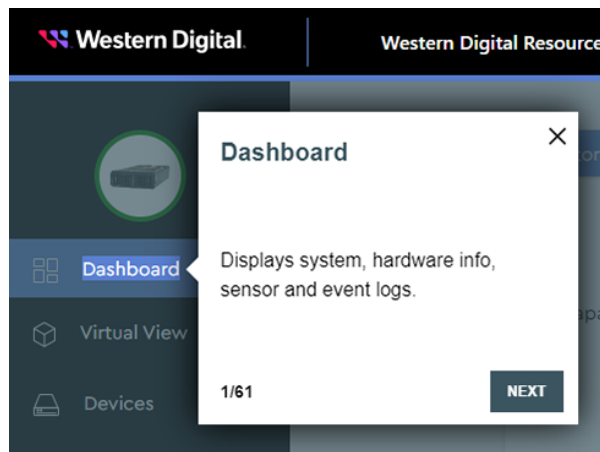
The **Virtual Tour** page will be displayed:



Step 2: Click the **Virtual Tour** button.

A message is displayed, explaining the function of a section of the GUI.

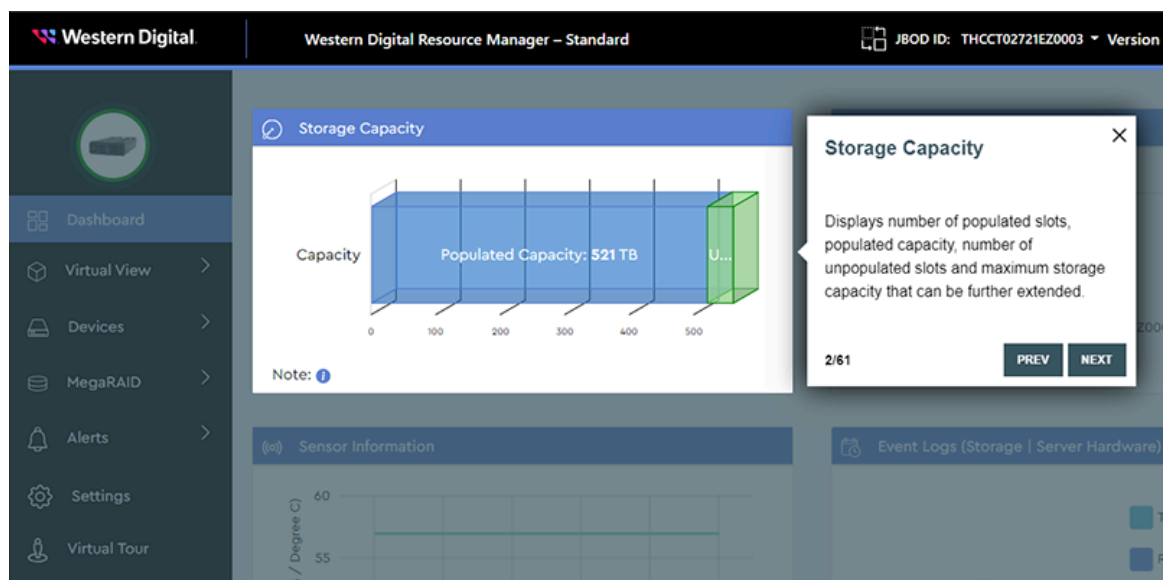
Figure 358: Explanation Message



Step 3: Click the **NEXT** button to move forward through each explanation of the Resource Manager Standard Edition application.

Step 4: Click the **PREV** button to go back to a previous explanation.

Figure 359: PREV and NEXT Buttons



Note: To exit the virtual tour at any time, click the **X** in the upper-right corner of any message box.

Result: The virtual tour is now complete.



Appendices

In This Chapter:

- Download Links for Required Software..... 206

4.1 Download Links for Required Software

The following tables provide download links and notes for the software that must be installed on the host server for it to run the Resource Manager Standard Edition application.



Note: The download links in this section were valid at the time of publication. However, these resources are not maintained by Western Digital and may become invalid at a later date.

Table 6: Required Software

Software	Version	Applicable OSs	Download Link / Notes
Apache HTTP Server™	2.4.46	Linux only	https://httpd.apache.org/download.cgi
Internet Information Services (IIS)	10	Windows only	https://www.microsoft.com/en-us/download/details.aspx?id=48264
URL Rewrite	2.1	Windows only	https://www.iis.net/downloads/microsoft/url-rewrite
Microsoft Application Request Routing	3.0	Windows only	https://www.iis.net/downloads/microsoft/application-request-routing
MongoDB™	4.4	Windows & Linux	Linux: https://fastdl.mongodb.org/windows/mongodb-windows-x86_64-4.4.3-signed.msi Windows: https://fastdl.mongodb.org/windows/mongodb-windows-x86_64-4.4.3-signed.msi
sg_utils	1.42	Windows & Linux	https://sg.danny.cz/sg/sg3_utils.html
Python®	3.8.8	Windows & Linux	Linux: https://www.python.org/downloads/release/python-388/ Installation steps can be found at: https://docs.python-guide.org/starting/install3/linux/ Windows: https://www.python.org/ftp/python/3.8.8/python-3.8.8-amd64.exe

Table 7: Python Modules

Module	Version	Applicable OSs	Notes
pip	9.0.1	Windows & Linux	Included with Python installation
Flask	2.2.2		<pre>pip3 install <module>==<version></pre>
Flask-Cors	3.0.8		
Flask-RESTful	0.3.9		
pymongo	4.2.0		
requests	2.18.4		
PyJWT	2.0.1		
json2html	1.3.0		
waitress	2.0.0		
Paste	3.5.0		
pyOpenSSL	22.1.0		
Werkzeug	2.2.2		
pywin32	300	Windows only	
psutil	5.8.0		