# 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
<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2021</td>
<td>01</td>
<td>Initial release</td>
</tr>
<tr>
<td>January 2022</td>
<td>02</td>
<td>Updated for software version 1.1 release</td>
</tr>
<tr>
<td>May 2022</td>
<td>03</td>
<td>Made the following changes for software version 1.2 release:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Removed Ultrastar Serv60+8 content throughout</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added Red Hat Enterprise Linux &amp; CentOS 7.6 to Compatible Operating Systems  (page 8); removed SUSE Linux Enterprise Server (only used for Ultrastar Serv60+8)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added WDCKIT to Required Software  (page 9); removed ipmiutil (only used for Ultrastar Serv60+8);</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added Exporting a Custom Zoning Configuration  (page 80) and Importing a Custom Zoning Configuration (page 85)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added Checking Cable Information (Rear)  (page 48) and Checking Cable Information (IOM) (page 107)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added Checking Background Processes  (page 115)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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)</td>
</tr>
<tr>
<td>December 2022</td>
<td>04</td>
<td>Made the following changes for software version 1.3 release:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated to new branding</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated images and instructions throughout</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated download instructions in Downloading Resource Manager Standard Edition  (page 12)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated installation instructions in Installing Resource Manager Standard Edition for Linux (page 16) to include custom port numbers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added note about Rebuild and Copyback features to Creating a Drive Group / RAID Configuration (page 129)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added Downloading SES PHY Counters  (page 110)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added Starting Patrol Read  (page 117)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added Configuring SMTP  (page 185), Viewing / Downloading Events (page 186), and Downloading Logs (page 188)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added Installing an SSL Certificate  (page 198)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added Download Links for Required Software (page 206)</td>
</tr>
<tr>
<td>Date</td>
<td>Revision</td>
<td>Comment</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>March 2024</td>
<td>05</td>
<td>Made the following changes for software version 1.3.1 release:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added Werkzeug 2.2.2 to [Required Software](page 9) and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[Download Links for Required Software](page 206)</td>
</tr>
</tbody>
</table>
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 guarantees 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 hereeto.

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)](#).
1.1 Resource Manager Standard Edition Overview

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)**.
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).
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).

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).
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.

<table>
<thead>
<tr>
<th>Firmware</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEP</td>
<td>3010-007 or later</td>
</tr>
<tr>
<td>OOBM</td>
<td>3.11 or later</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat® Enterprise Linux® (RHEL)</td>
<td>7.6, 7.9, 8.0, 8.2, 8.3</td>
</tr>
<tr>
<td>CentOS</td>
<td>7.6, 7.9, 8.0, 8.2, 8.3</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>16.04, 18.04, 20.04</td>
</tr>
<tr>
<td>Debian</td>
<td>10.9</td>
</tr>
<tr>
<td>Oracle® Linux</td>
<td>8.2</td>
</tr>
<tr>
<td>Windows Server®</td>
<td>2016, 2019</td>
</tr>
</tbody>
</table>
1.5 Compatible Browsers

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

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome</td>
<td>83.0.4103.97 or newer</td>
</tr>
<tr>
<td>Firefox</td>
<td>68.9.0esr (64-bit) or newer</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
<th>Applicable OSs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache HTTP Server™</td>
<td>2.4.46</td>
<td>Linux only</td>
</tr>
<tr>
<td>Internet Information Services (IIS)</td>
<td>10</td>
<td>Windows only</td>
</tr>
<tr>
<td>URL Rewrite</td>
<td>2.1</td>
<td>Windows only</td>
</tr>
<tr>
<td>Microsoft Application Request Routing</td>
<td>3.0</td>
<td>Windows only</td>
</tr>
<tr>
<td>Python®</td>
<td>3.8.8</td>
<td>Windows &amp; Linux</td>
</tr>
<tr>
<td><strong>Python Modules:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>pip</td>
<td>9.0.1</td>
<td>Windows &amp; Linux</td>
</tr>
<tr>
<td>Flask</td>
<td>2.2.2</td>
<td></td>
</tr>
<tr>
<td>Flask-Cors</td>
<td>3.0.8</td>
<td></td>
</tr>
<tr>
<td>Flask-RESTful</td>
<td>0.3.9</td>
<td></td>
</tr>
<tr>
<td>pymongo</td>
<td>4.2.0</td>
<td></td>
</tr>
<tr>
<td>requests</td>
<td>2.18.4</td>
<td>Windows &amp; Linux</td>
</tr>
<tr>
<td>PyJWT</td>
<td>2.0.1</td>
<td></td>
</tr>
<tr>
<td>json2html</td>
<td>1.3.0</td>
<td></td>
</tr>
<tr>
<td>waitress</td>
<td>2.0.0</td>
<td></td>
</tr>
<tr>
<td>Paste</td>
<td>3.5.0</td>
<td></td>
</tr>
<tr>
<td>pyOpenSSL</td>
<td>22.1.0</td>
<td></td>
</tr>
<tr>
<td>Werkzeug</td>
<td>2.2.2</td>
<td></td>
</tr>
<tr>
<td><strong>Python Modules:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>pywin32</td>
<td>300</td>
<td>Windows only</td>
</tr>
<tr>
<td>psutil</td>
<td>5.8.0</td>
<td></td>
</tr>
<tr>
<td>MongoDB™</td>
<td>4.4</td>
<td>Windows &amp; Linux</td>
</tr>
<tr>
<td>sg_utils</td>
<td>1.42</td>
<td>Windows &amp; Linux</td>
</tr>
</tbody>
</table>
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/](https://portal.wdc.com/s/).
The login page for the Western Digital Business Support Center will be displayed:

*Figure 8: Login Page*

**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:
2. Installation

2.1 Downloading Resource Manager Standard Edition

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

An operating system selection list will appear:
2. Installation

2.1 Downloading Resource Manager Standard Edition

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:

![Operating System Selection List](image)

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

![Software Binaries](image)
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.
sq_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.

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

![Uninstall wddcs window](image)

**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.
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:

```plaintext
wddcs Setup

 GDPR Violation Warning
The uninstallation has been completed. Please exit and run the installation again.

OK
```

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


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.
2. Installation

2.3 Installing Resource Manager Standard Edition for Windows

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:
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.
2.3 Installing Resource Manager Standard Edition for Windows

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:

![Ready To Install Window]

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*
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 drives\(^1\), 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.
3. Management
3.2 Dashboard

**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:
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.


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

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


Enabling the Enclosure’s Identification LEDs

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

The Front virtual view page will be displayed:
Step 2: The **Front View** image on the left will display the status of the enclosure’s Identification, Fault, and Power LEDs.

*Figure 49: Front View*

*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.

![Identification LED Tooltip](image)

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.
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.
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.


Enabling the Enclosure’s Identification LEDs

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

The Rear virtual view page will be displayed:
Step 2: The **Rear View** image on the left will display the status of the enclosure’s Identification, Fault, and Power 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:
**Step 2:** The *Rear View* image on the left will display the status of the enclosure's I/O ports.

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

- **Black** – Not installed
3. Management
3.3 Virtual View

- **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*

   ![Drives Page Image]

**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:
3. Management

3.4 Devices

Step 3: Click the Actions tab.

The Actions tab will be displayed:

![Figure 66: Actions Tab](image)

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

![Figure 67: Locate Link](image)

A dialogue box will appear, prompting the user to confirm enabling the drive's identification LED:
Step 5: Click the **OK** button. A success notification will appear at the top of the page:

**Figure 69: Success Notification**

![Success Notification](image)

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

**Disabling a Drive Identification LED**

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

**Figure 70: Stop Locating Link**

![Stop Locating Link](image)
Step 7: Click the OK button.
A success notification will appear at the top of the page:

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

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

*Figure 75: 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:
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.
**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.
After the firmware is uploaded, a success notification will appear at the top of the page:

**Figure 80: Success Notification**

- **Success**: File uploaded successfully. Click on the Upgrade button to continue

**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:
3. Management
3.4 Devices

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.


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

The **Actions** tab will be displayed:
3. Management
3.4 Devices

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

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:

![Choose Button](image)

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

![Figure 89: Upload Firmware](image)

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

![Figure 90: Upgrade Button](image)

A notification will appear on the page during the upgrade:
When the upgrade is finished, a success notification will be displayed:

**Figure 92: Upgrade Success**

<table>
<thead>
<tr>
<th>Drive Slots</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot 37</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>Slot 38</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>Slot 39</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>Slot 41</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>Slot 50</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>Slot 46</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

**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

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.


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

The zoning page will be displayed:

![Figure 95: Zoning Page](image)

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

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

Step 3: Click the toggle switch next to the configuration name to enable the configuration.
A dialogue box will appear, prompting the user to confirm the configuration:

**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*

![Zoning Page Screenshot]

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

**Figure 102: Create New Button**

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

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

**Figure 103: Create Configuration Dialogue Box**

**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:
Step 5: As prompted, click the **Add New Zone** button.

A **New Zone** section will be added to the configuration:
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:

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


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

The zoning page will be displayed:

![Zoning Page Diagram]

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:
3.4 Devices

A Custom Configuration section will appear:

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

The custom configuration will appear in a new section, locked for editing:
**Step 4:** Double-click the configuration to unlock it:
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:
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:
Step 3: Click the **Choose File** button:

![Choose File Button](image1)

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:

![Configuration File Selected](image2)

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

![Preview Button](image3)

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

![Imported Configuration Preview](image4)

Step 6: Click either of the **Import** buttons to import the zoning configuration.
A dialogue box will appear, prompting the user to confirm importing the configuration:

**Figure 130: Import Confirmation Dialogue Box**

![Dialogue box with confirmation message]

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

A success notification will appear in the dialogue box:

**Figure 131: Success Message**

![Success notification]

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:

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

The custom configuration will appear in a new section, locked for editing:
Step 4: Double-click the configuration to unlock it:
Figure 138: Custom Configuration, Unlocked

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

Figure 139: Configuration Toggle Switch

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

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:
3. Management
3.4 Devices

Figure 143: Firmware Upload

![Firmware Upload](image1)

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

![Firmware Upgrade](image2)

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

**Figure 146: Upgrade Complete, FW Activation Starting**

FW Downloaded successfully. Now FW activation will start

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

**Figure 147: Activation Complete**

FW Activated successfully

**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:
3. Management
3.4 Devices

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](image)

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

The page for that IOM will be displayed:
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

Click on the reset button to reset the IOM.

Please stay in the page until reset is completed.

**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

Click on the reset button to reset the IOM.

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:

![IOM Page](image)

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

**Figure 161: Nickname Field**

![Figure 161: Nickname Field](image)

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**

<table>
<thead>
<tr>
<th>Nick Name</th>
<th>Test10</th>
<th>Edit</th>
<th>Nickname set success</th>
</tr>
</thead>
</table>

**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.


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:
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:

**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:

![IOM Page](image)

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

The page for that IOM will be displayed:
Step 3: Scroll down to the **Cable Information** section to view detailed information about port connectivity status and attached cables.

**Figure 168: Cable Information**

<table>
<thead>
<tr>
<th>Host</th>
<th>Status</th>
<th>Zone Group</th>
<th>Length</th>
<th>Bandwidth</th>
<th>Manufacturer</th>
<th>Model</th>
<th>SAS Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host0</td>
<td></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Host1</td>
<td></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Host2</td>
<td></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Host3</td>
<td></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Host4</td>
<td></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Host5</td>
<td></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Host6</td>
<td></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Cable Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>Host0</td>
</tr>
<tr>
<td>Host1</td>
</tr>
<tr>
<td>Host2</td>
</tr>
<tr>
<td>Host3</td>
</tr>
<tr>
<td>Host4</td>
</tr>
<tr>
<td>Host5</td>
</tr>
</tbody>
</table>

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:
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.
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).


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

The Sensors page will be displayed:

![Sensors Page](image)

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.
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.

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:
3.5 MegaRAID

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.

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:

2. 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:

![MegaRAID Controller Page](image)

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

![Patrol Read Settings](image)

**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

![Confirmation dialog]

Do you want to start patrol read?

- **OK**: Click the OK button.
  A success message will appear, indicating that the Patrol Read scan has started:

Figure 183: Patrol Read Success

![Success message]

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

![Set properties window]

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

The automatic properties will appear:
a. In the **Maximum Physical Drives Allowed** field, enter the maximum number of drives to be scanned simultaneously.

   ![Image](Figure 185: Automatic Patrol Read Properties)

   **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:

   ![Image](Figure 186: Scan Frequency)

   - Hourly
   - Daily
   - Weekly
   - Monthly
   - Continuously

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

3.5 MegaRAID

**Figure 187: Scan Date/Time**

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

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**

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

![Image of Manual Patrol Read Properties](image)

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

![Scan Date/Time](image)

**Figure 191: Scan Date/Time**

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

![Scan Now](image)

**Figure 192: Scan Now**

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

![Manual Patrol Read Drive Groups](image)

**Figure 193: Manual Patrol Read Drive Groups**

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

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

a. 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.

The firmware filename will appear in the upload area:
Figure 198: Firmware Filename

**Firmware Upgrade**

<table>
<thead>
<tr>
<th>FW Package Ver</th>
<th>51.19.0-4470</th>
</tr>
</thead>
</table>

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

![Firmware Filename](image)

**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

![Upload Success](image)

**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:
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.

![RAID Configuration Page](image)

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:
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**

```
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:
3. Management

3.5 MegaRAID

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.
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 209: Another Enclosure

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 210: Summary of Drives from All Enclosures

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:
### 3.5 MegaRAID

**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.
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**

![Logical Drive Settings](image)

**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.

**Step 10:** If needed, use the **Capacity** field to reduce the capacity allocated to each logical drive.
**Step 11:** From the **Stripe Size** drop-down list, select the stripe size for this RAID.

**Figure 219: Stripe Size**

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 prepares the storage medium for use

- **No Initialization**
  
  The new configuration is not initialized, and the existing data on the drives is not overwritten.

- **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.
### Figure 221: Read Policy

<table>
<thead>
<tr>
<th>Initialization</th>
<th>A controller attribute indicating the current Read Policy mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Initialization</td>
<td></td>
</tr>
<tr>
<td>Read Policy</td>
<td></td>
</tr>
<tr>
<td>Read Ahead</td>
<td></td>
</tr>
<tr>
<td>Write Policy</td>
<td></td>
</tr>
<tr>
<td>Write Back</td>
<td></td>
</tr>
<tr>
<td>IO Policy</td>
<td></td>
</tr>
<tr>
<td>Direct IO</td>
<td></td>
</tr>
<tr>
<td>Disk Cache Policy</td>
<td></td>
</tr>
<tr>
<td>Disabled</td>
<td></td>
</tr>
</tbody>
</table>

- **No Read Ahead**
  - In No Read Ahead mode, read ahead capability is disabled.

- **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.

### Figure 222: Write Policy

<table>
<thead>
<tr>
<th>Initialization</th>
<th>A controller attribute indicating the current Write Policy mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Initialization</td>
<td></td>
</tr>
<tr>
<td>Read Policy</td>
<td></td>
</tr>
<tr>
<td>Read Ahead</td>
<td></td>
</tr>
<tr>
<td>Write Policy</td>
<td></td>
</tr>
<tr>
<td>Write Back</td>
<td></td>
</tr>
<tr>
<td>IO Policy</td>
<td></td>
</tr>
<tr>
<td>Direct IO</td>
<td></td>
</tr>
<tr>
<td>Disk Cache Policy</td>
<td></td>
</tr>
<tr>
<td>Disabled</td>
<td></td>
</tr>
</tbody>
</table>

- **Write Through**
  - This mode provides for cache data protection upon power failure. **Note:** It may result in slower performance.

- **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.

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

The details of the RAID configuration will be replaced by a colored square, representing the logical drive:
Figure 226: Logical Drive

![Logical Drive](image)

**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

![Create Drive Group](image)

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

Figure 228: Confirm Creating Logical Drive

![Confirm Creating Logical Drive](image)

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

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

Figure 229: Success Notification

![Success Notification](image)

**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:
3.5 MegaRAID

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 232: Confirm Clearing All Configurations**

Are you sure

Clear config will delete all the logical drives and erase data associated with all the logical drives. Do you want to clear configuration?

[OK] [Cancel]

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

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

**Figure 233: Success Notification**

[Success] Clear configuration successful.

**Result:** All RAID configurations have now been cleared.
Step 2: From the **Actions** drop-down list, select the **Foreign Configuration** option.

A dialogue box will be displayed, prompting the user to either clear or import all foreign configurations:
Step 3: Click the **Import** button.

The dialogue box notifies the user that importing has started:

![Figure 237: Importing Foreign Configurations](image)

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


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

The RAID Configuration page will be displayed:
Step 2: From the **Actions** drop-down list, select the **Foreign Configuration** option.

A dialogue box will be displayed, prompting the user to either 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*

**Are you sure**

Clear config will delete all the logical drives and erase data associated with all the logical drives. Do you want to clear configuration?

[Cancel] [OK]

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

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

3.5.3.1 Modifying a Drive Group / RAID Configuration

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


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

A Drive Groups - Reconstruction page will be displayed, allowing modifications to the drive group:
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:
b. To remove a drive slot from the group, click its x:

![Figure 249: Remove Selected Drives](image)

- **Selected Drives**

- **Overall Selected Drives from all Enclosures**

- **RAID Level** drop-down list:

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

![RAID Reconstruction Confirmation](image)

**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:

![Background Process Notification](image)

**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.

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

![Logical Drives Page](image)

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

![Confirmation, Not Initialized Dialogue Box]

Virtual drive(s) has not been initialized. Running a consistency check may result in inconsistent message in the log. Do you want to start the consistency check?
Step 4: Click the OK button. A success notification will appear at the top of the page:

**Figure 263: Success Notification**

- Success: Consistency check started successfully.

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

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

Are you sure

Initialization erases all data on virtual drive. Are you sure you want to start initialization?

[ ] Fast Initialization

[ ] Cancel [ ] Yes, Start 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

Success Logical drive full initialization process started successfully.

Success Logical drive fast initialization process started successfully.

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.


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

The Logical Drives page will be displayed:
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:
Step 3: Click the ellipsis (…) for the logical drive, and select the **Start Erase** option:
A dialogue box will appear, prompting the user to select an erase option:

**Figure 274: Erase Options**

Logical Drive Erase operates on a specified logical drive and overwrites all user-accessible sectors with the specified pattern for the specified number of passes.

Select the mode for Drive erase operation:

- **Simple**
  - Specifies a single pass erase operation that writes pattern A to the logical drive.
- **Normal**
  - Specifies a three pass erase operation that first overwrites the logical drive contents with random values and then overwrites it with pattern A and then overwrites it with pattern B.
- **Thorough**
  - Specifies a nine pass erase operation that repeats the normal mode thrice.

- **Delete Logical Drive After Erase**

  ![Erase Logical Drive Button]
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.


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**

<table>
<thead>
<tr>
<th>Drive Group</th>
<th>RAID Level</th>
<th>Physical Drives</th>
<th>Logical Drives</th>
<th>Capacity</th>
<th>Utilisation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>DG0</td>
<td>RAID 1</td>
<td>2</td>
<td>1</td>
<td>7.277 TB</td>
<td>100%</td>
<td>***</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Slot ID</th>
<th>Device ID</th>
<th>Drive Type</th>
<th>Interface</th>
<th>Serial number</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>49</td>
<td>6</td>
<td>HDD</td>
<td>SAS</td>
<td>VAG1DIZD</td>
<td>7.277 TB</td>
</tr>
<tr>
<td>48</td>
<td>21</td>
<td>HDD</td>
<td>SAS</td>
<td>VAGIV5XL</td>
<td>7.277 TB</td>
</tr>
</tbody>
</table>

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

Are you sure

Do you want to delete the current logical drive?

[Cancel]  [Delete]

Step 4: Click the Delete button.
A success notification will appear at the top of the page:
Result: The logical drive (along with its RAID configuration) has now been deleted.

Figure 280: Success Notification

☑️ Success Logical drive deleted successfully.
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.


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

*Figure 284: Actions Tab*

![Actions Tab](image)

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

*Figure 285: Locate Link*

![Locate Link](image)

A dialogue box will appear, prompting the user to confirm enabling the drive’s identification LED:
Step 5: Click the OK button. A success notification will appear at the top of the page:

---

Disabling a Drive Identification LED

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

---

Step 7: Click the OK button. A success notification will appear at the top of the page:
**Figure 290: Success Notification**

Success   LED disabled successfully.

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

The **Actions** tab will display information about the installed drive and available actions:
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**

![Current Firmware Version](image)

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

Step 6: Click the Upload button to upload the firmware to the drive.
After the firmware is uploaded, a success notification will appear at the top of the page:

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

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

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.


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

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

**Figure 307: Upload Firmware**

![Figure 307: Upload Firmware](image)

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

**Figure 308: Upgrade Button**

![Upgrade Button](image)

A notification will appear on the page during the upgrade:
When the upgrade is finished, a success notification will be displayed:

**Figure 310: Upgrade Success**

<table>
<thead>
<tr>
<th>Drive Slots</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot37</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>Slot38</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>Slot39</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>Slot40</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>Slot50</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>Slot51</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

**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:**


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

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

   ![Email Configuration Page](#)

   **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.

   ![Email Notification Settings](#)

   **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:
3.6 Alerts

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:

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:


Step 1: From the navigation bar, select Alerts > SMTP configuration. The SMTP Configurations page will be displayed:
Figure 316: SMTP Configuration Page

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:


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

The Events page will be displayed:
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.
Result: Enclosure events have now been viewed / downloaded.

3.6.4 Downloading Logs

This procedure provides instructions for downloading enclosure logs.

Before you begin:


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

   The Logs page will be displayed:

   ![Logs Page](image)

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:**


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

   The **Settings** page will be displayed:

   ![Figure 323: Settings Page](image)

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

   ![Figure 324: Add User Button](image)

   The user settings for the new account will be displayed:
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*

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


Step 1: From the navigation bar, select Settings.

The Settings page will be displayed:

![Figure 329: Settings Page](image)

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

![Figure 330: Edit Button](image)

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

The settings for that account will be displayed:
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:

![Change Password Dialogue Box]

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:

![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:
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:


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:
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:


   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**

   ![Settings Page]

Step 2: Click the SSL Certificate tab.

   The SSL Certificate settings will be displayed:
Step 3: Click the **Install New Certificate** button.

![Figure 341: Install New Certificate Button](image)

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

![Figure 342: SSL Certificate Selection](image)

**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

![Choose File Button]

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

Figure 344: Private Key Selected

![Private Key Selected]

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

Figure 345: Upload Button

![Upload Button]

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

Figure 346: Private Key Uploaded

![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

![Choose File Button]

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

Figure 348: Certificate Selected

![Certificate Selected]

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

Figure 349: Upload Button

![Upload Button]

A success message will be displayed, and a **Verify** button will appear:
Step 8: Click the **Verify** button to validate the contents and compatibility of the Private Key and Certificate pair.

*Figure 351: Verify Button*

Verify

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

*Figure 352: Verification Failure*

Certificate verification failure. Please upload the correct key and certificate pair.

Back

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

*Figure 353: Verification Success*

Certificate verification success. To enable the certificate, please click on Enable.

Back Enable

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

*Figure 354: Enable Button*

Enable

A confirmation dialog box will appear:
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 12: From the navigation bar, select Settings > SSL Certificate and view the 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:


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.
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.

Result: The virtual tour is now complete.
Appendices

In This Chapter:
- Download Links for Required Software

...
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

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
<th>Applicable OSs</th>
<th>Download Link / Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache HTTP Server™</td>
<td>2.4.46</td>
<td>Linux only</td>
<td><a href="https://httpd.apache.org/download.cgi">https://httpd.apache.org/download.cgi</a></td>
</tr>
<tr>
<td>URL Rewrite</td>
<td>2.1</td>
<td>Windows only</td>
<td><a href="https://www.iis.net/downloads/microsoft/url-rewrite">https://www.iis.net/downloads/microsoft/url-rewrite</a></td>
</tr>
<tr>
<td>Microsoft Application Request Routing</td>
<td>3.0</td>
<td>Windows only</td>
<td><a href="https://www.iis.net/downloads/microsoft/application-request-routing">https://www.iis.net/downloads/microsoft/application-request-routing</a></td>
</tr>
</tbody>
</table>
| 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

<table>
<thead>
<tr>
<th>Module</th>
<th>Version</th>
<th>Applicable OSs</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>pip</td>
<td>9.0.1</td>
<td></td>
<td>Included with Python installation</td>
</tr>
<tr>
<td>Flask</td>
<td>2.2.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flask-Cors</td>
<td>3.0.8</td>
<td>Windows &amp; Linux</td>
<td></td>
</tr>
<tr>
<td>Flask-RESTful</td>
<td>0.3.9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pymongo</td>
<td>4.2.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>requests</td>
<td>2.18.4</td>
<td>Windows &amp; Linux</td>
<td></td>
</tr>
<tr>
<td>PyJWT</td>
<td>2.0.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>json2html</td>
<td>1.3.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>waitress</td>
<td>2.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paste</td>
<td>3.5.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pyOpenSSL</td>
<td>22.1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Werkzeug</td>
<td>2.2.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pywin32</td>
<td>300</td>
<td>Windows only</td>
<td></td>
</tr>
<tr>
<td>psutil</td>
<td>5.8.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Use `pip3 install <module>=<version>` to install the required software.