Spectra Logic BlackPearl Object Gateway

User Guide

SpectraLogic.com

Copyright

Notices

Except as expressly stated herein, Spectra Logic Corporation makes its products and associated documentation on an "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, BOTH OF WHICH ARE EXPRESSLY DISCLAIMED. In no event shall Spectra Logic be liable for any loss of profits, loss of business, loss of use or data, interruption of business, or for indirect, special, incidental or consequential damages of any kind, even if Spectra Logic has been advised of the possibility of such damages arising from any defect or error.

Information furnished in this manual is believed to be accurate and reliable. However, no responsibility is assumed by Spectra Logic for its use. Due to continuing research and development, Spectra Logic may revise this publication from time to time without notice, and reserves the right to change any product specification at any time without notice.

Trademarks

Part Number

90990093 Revision AF

Revision History

Revision	Date	Description
Z	April 2023	Updated for the BlackPearl OS 5.6 release.
AA	October 2023	Updated for the BlackPearl OS 5.7 release.
AB	February 2024	Updated for the BlackPearl Gen3 H series chassis and BlackPearl OS 5.7.3.
AC	December 2024	Updated for the BlackPearl OS 5.7.6 release.
AD	April 2025	Updated for the BlackPearl Gen 3 F Series chassis and BlackPearl OS 5.8.
AE	September 2025	Updated for the BlackPearl OS 5.8.2 release and the Gen3 H 3310 chassis.
AF	January 2026	Updated for the BlackPearl OS 5.9 release.

Note: To make sure you have the most current version of this guide, see the Spectra Logic Technical Support portal at *support.spectralogic.com/documentations/user-guides/*.

End User License Agreement

1. READ CAREFULLY

YOU SHOULD READ THE FOLLOWING TERMS AND CONDITIONS BEFORE ACCEPTING THIS END-USER LICENSE AGREEMENT ("EULA"). THIS EULA IS A LEGAL AGREEMENT BETWEEN YOUR ORGANIZATION, THE END USER, AND SPECTRA LOGIC CORPORATION ("SPECTRA") FOR THE SPECTRA SOFTWARE PRODUCT WHICH INCLUDES COMPUTER SOFTWARE AND MAY INCLUDE ASSOCIATED MEDIA, PRINTED MEDIA, AND "ONLINE" OR ELECTRONIC DOCUMENTATION (COLLECTIVELY, "SOFTWARE PRODUCT"). BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE PRODUCT, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MAY NOT INSTALL, COPY, DOWNLOAD OR USE THE SOFTWARE PRODUCT. YOU AGREE THAT YOUR USE OF THE SOFTWARE ACKNOWLEDGES THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

2. OWNERSHIP

It is understood and agreed that Spectra Logic Corporation, a Delaware corporation with offices at 6285 Lookout Road, Boulder, CO 80301 ("Licensor") is the owner of all right, title and interest to the Software Product, regardless of the media or form of the original download, whether by the World Wide Web, disk or otherwise. You, as licensee ("Licensee") through your downloading, installing, copying or use of this product do not acquire any ownership rights to the Software Product.

3. GENERAL

The Software Product is licensed, not sold, to you by Spectra for use only under the terms of this EULA. The Software Product is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The rights granted herein are limited to Spectra's and its licensors' intellectual property rights in the Software Product and do not include any other patents or intellectual property rights. The terms of this EULA will govern any software upgrades provided by Spectra that replace and/or supplement the original Software Product, unless such upgrade is accompanied by a separate license in which case the terms of that license will govern.

4. SOFTWARE PRODUCT

The Software Product, as used in this EULA, means, collectively and/or as applicable:

- Related explanatory written materials and instructions, and any other possible documentation related thereto ("Documentation"); and
- Upgrades, modified versions, updates, additions and copies of the Software Product (the "Upgrades"), if any, licensed to by Spectra under this EULA.
- The Software Product package;
- Any and all contents, components, attachments, software, media, and code with which this Agreement is provided and delivered;
- Any and all images, photographs, art, art work, clip art, fonts or other artistic works (the "Art Work");

5. GRANT OF LICENSE AND RESTRICTIONS

A. Spectra grants you a non-exclusive, non-transferable End-User license right to install the Software Product solely for the purpose for which it was created.

B. Unless provided otherwise in the Documentation or by prior express written consent of Spectra, you shall not display, modify, reproduce and distribute any Art Work, or portion(s) thereof, included with or relating to the Software Product, if any. Any such authorized display, modification, reproduction and distribution shall be in full accord with this EULA. Under no circumstances will your use, display, modification, reproduction and distribution of the Art Work give you any Intellectual Property or Proprietary Rights of the Art Work. All rights, title, and interest belong solely to Spectra.

C. Except for the initial loading of the Software Product, you shall not, without Spectra's express written consent:

- Copy or reproduce the Software Product; or
- Modify, adapt, or create derivative works based on the Software Product or any accompanying materials.

6. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

A. Spectra will provide you with support services related to the Software Product ("Support"). Such Support will be provided in accordance with the Spectra Master Support Agreement, available for download and viewing on the Spectra Corporate Web site. Use of Support is governed by this EULA and Spectra's Master Support Agreement.

B. Any supplemental software, code, content, or media provided to you in the course of Support shall be considered part of the Software Product and subject to the terms and conditions of this EULA.

C. Spectra retains all right, title, and interest in and to the Software Product, and any rights not granted to you herein are reserved by Spectra. You hereby expressly agree not to extract information, reverse engineer, disassemble, decompile, or translate the Software Product, or otherwise attempt to derive the source code of the Software, except to the extent allowed under any applicable law. In the event that such activities are permitted by applicable law, any information you, or your authorized agent, discover shall be promptly disclosed to Spectra and shall be deemed the confidential information of Spectra.

D. You shall not modify, sublicense, assign, or transfer the Software Product or any rights under this EULA, except as expressly provided in this EULA. Any attempt to sublicense, assign, or transfer any of the rights, duties, or obligations will be void.

E. You may permanently transfer all of your rights under this EULA, provided you retain no copies. The other party must agree to accept the terms and conditions of the EULA.

7. ALL RESERVED

All rights not expressly granted herein are reserved by Spectra.

8. TERM

A. This License is effective until terminated. Licensee may terminate it at any time by destroying the Software Product with all copies, full or partial, and removing all of its component parts.

B. Your rights under this EULA will terminate automatically without notice from Spectra if you fail to comply with any term(s) or condition(s) of this EULA. In such event, no notice shall be required by Spectra to effect such termination.

C. Upon termination of this EULA, you shall cease all use of the Software Product and destroy all copies, full or partial, together with all backup copies, modifications, printed or written materials, and merged portions in any form and remove all component parts of the Software Product.

9. INTELLECTUAL PROPERTY RIGHTS

A. Spectra shall retain all right, title, and interest in the Software Product and to any modifications or improvements made thereto, and any upgrades, updates or Documentation provided to End User. End User will not obtain any rights in the Software Product, its updates, upgrades, and Documentation, as a result of its responsibilities hereunder.

B. End User acknowledges Spectra's exclusive rights in the Software Product and that the Software Product is unique and original to Spectra and that Spectra is owner thereof. Unless otherwise permitted by law, End User shall not, at any time during or after the effective Term of the Agreement, dispute or contest, directly or indirectly, Spectra's exclusive right and title to the Software Product or the validity thereof.

10. U.S. GOVERNMENT END USERS

The Software Product and related documentation are "Commercial Items," as that term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable. The Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other End Users pursuant to the terms and conditions herein. Unpublished rights reserved under the copyright laws of the United States.

11. EXPORT LAW ASSURANCES

You may not use or otherwise export or re-export the Software Product except as authorized by United States law and the laws of the jurisdiction in which the Software Product was obtained. In particular, but without limitation, the Software Product may not be exported or re-exported (a) into (or to a nation or resident of) any U.S. embargoed countries or (b) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Department of Commerce Denied Persons List or Entity List. By installing or using any component of the Software Product, you represent and warrant that you are not located in, under control of, or a national or resident of any such country or on any such list.

12. DISCLAIMER OF WARRANTIES

YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT USE OF THE SOFTWARE PRODUCT IS AT YOUR SOLE RISK AND THAT THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY AND EFFORT IS WITH YOU. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AND EXCEPT AS MAY BE STATED IN THE SPECTRA MASTER SERVICE AGREEMENT, THE SOFTWARE PRODUCT IS PROVIDED "AS IS," WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND SPECTRA AND SPECTRA'S AFFILIATES (COLLECTIVELY REFERRED TO AS "SPECTRA" FOR THE PURPOSES OF SECTIONS 12 AND 13) HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE SOFTWARE PRODUCT, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, OF SATISFACTORY QUALITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF ACCURACY, OF QUIET ENJOYMENT, AND NON-INFRINGEMENT OF THIRD-PARTY RIGHTS. SPECTRA DOES NOT WARRANT AGAINST INTERFERENCE WITH YOUR ENJOYMENT OF THE SOFTWARE PRODUCT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE PRODUCT WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION OF THE SOFTWARE PRODUCT WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE SOFTWARE PRODUCT WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY SPECTRA OR A SPECTRA AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATION ON APPLICABLE STATUTORY RIGHTS OF A CONSUMER, SO THE ABOVE EXCLUSION AND LIMITATIONS MAY NOT APPLY TO YOU.

13. LIMITATION OF LIABILITY

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL SPECTRA, ITS AFFILIATES OR LICENSEES, BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT OR THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, EVEN IF SPECTRA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, SPECTRA'S ENTIRE LIABILITY UNDER ANY PROVISION OF THIS EULA SHALL BE LIMITED TO THE AMOUNT ACTUALLY PAID BY YOU FOR THE SOFTWARE PRODUCT; PROVIDED HOWEVER, IF YOU HAVE ENTERED INTO A MASTER SUPPORT AGREEMENT, SPECTRA'S ENTIRE LIABILITY REGARDING SUPPORT SERVICES SHALL BE GOVERNED BY THE TERMS OF THAT AGREEMENT. BECAUSE SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

14. CONTROLLING LAW AND SEVERABILITY

This EULA will be governed by and construed in accordance with the laws of the State of Colorado, as applied to agreements entered into and to be performed entirely within Colorado between Colorado residents. This EULA shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. If for any reason a court of competent jurisdiction finds any provision, or portion thereof, to be unenforceable, the remainder of this EULA shall continue in full force and effect.

SYSTEM BIOS

Resetting the system BIOS when not authorized by Spectra Logic Technical Support invalidates the system configuration. Spectra Logic reserves the right to charge for time and materials to reconfigure and recertify the system.

Contacting Spectra Logic

To Obtain General Information	
Spectra Logic Website: *spectralogic.com*	
United States Headquarters	**European Office**
Spectra Logic Corporation 6285 Lookout Road Boulder, CO 80301 USA **Phone:** 1.800.833.1132 or 1.303.449.6400 **International:** 1.303.449.6400 **Fax:** 1.303.939.8844	Spectra Logic Europe Ltd. 329 Doncastle Road Bracknell Berks, RG12 8PE United Kingdom **Phone:** 44 (0) 870.112.2150 **Fax:** 44 (0) 870.112.2175
Spectra Logic Technical Support	
Technical Support Portal: *support.spectralogic.com*	
United States and Canada **Phone:** **Toll free US and Canada:**1.800.227.4637 **International:** 1.303.449.0160	**Europe, Middle East, Africa** **Phone:** 44 (0) 870.112.2185 **Deutsch Sprechende Kunden** **Phone:** 49 (0) 6028.9796.507
Additional international numbers available at *support.spectralogic.com/home* **If you have a Spectra Logic Portal account, please log in for country-specific numbers at** *support.spectralogic.com/support-contact-info*	
Spectra Logic Sales	
Website: *shop.spectralogic.com*	
United States and Canada **Phone:** 1.800.833.1132 or 1.303.449.6400 **Fax:** 1.303.939.8844 **Email:** sales@spectralogic.com	**Europe** **Phone:** 44 (0) 870.112.2150 **Fax:** 44 (0) 870.112.2175 **Email:** eurosales@spectralogic.com
To Obtain Documentation	
support.spectralogic.com/documentations	

Table of Contents

ABOUT THIS GUIDE

This guide describes how to configure, monitor, and maintain the Spectra® BlackPearl® Object Gateway master node, which is referred to as the *master node* in these instructions.

This guide also describes the Spectra 44-bay expansion node, the 96-bay expansion node, the 77-bay expansion node, and the 107-bay expansion node which are referred to as *expansion nodes* in these instructions. The expansion nodes are used in conjunction with the master node and cannot be used as a stand-alone product.

When instructions in this guide apply to both the BlackPearl Object Gateway master node and expansion nodes, *the system* is used to refer to both.

INTENDED AUDIENCE

This guide is intended for data center administrators and operators who maintain and operate file storage systems. The information in this guide assumes a familiarity with computing terminology and with network connectivity protocols such as SAS, Fibre Channel, and Ethernet. If your BlackPearl Object Gateway installation includes a tape library, knowledge of tape-based backup systems and how to use the library is required. You also need to be familiar with installing, configuring, and using data file storage and data management software.

DISCONTINUED COMPONENTS

To view information about discontinued components of the BlackPearl Object Gateway, log into the Support portal (see Access the Technical Support Portal on page 395), and navigate to **Documentation > Product Life Cycle Information**.

BLACKPEARL USER INTERFACE SCREENS

The BlackPearl user interface changes as new features are added or other modifications are made between software revisions. Therefore, the screens you see in the BlackPearl user interface may differ from those shown in this guide.

Related Information

This section contains information about this document and other documents related to the Spectra BlackPearl Object Gateway.

Typographical Conventions

This document uses the following conventions to highlight important information:

⚠	**WARNING**	Read text marked by the "Warning" icon for information you must know to avoid personal injury.
⚠	**CAUTION**	Read text marked by the "Caution" icon for information you must know to avoid damaging the hardware or losing data.
⚠	**IMPORTANT**	Read text marked by the "Important" icon for information that helps you complete a procedure or avoid extra steps.

Note: Read text marked with "Note" for additional information or suggestions about the current topic.

Related Publications

For additional information about the Spectra BlackPearl Object Gateway and the DS3 interface, refer to the publications listed in this section.

Spectra BlackPearl Object Gateway

The following documents related to the Spectra BlackPearl Object Gateway are available on the Support Portal website at *support.spectralogic.com*, and from the Documentation screen in the BlackPearl user interface.

- The *Spectra BlackPearl Site Preparation Guide* provides important information that you should know before installing a BlackPearl Object Gateway in your storage environment.
- The *Spectra BlackPearl Rack Mounting Instructions Guide* provides detailed instructions for installing a Gen1 BlackPearl Object Gateway in a standard rack.
- The *Spectra BlackPearl Network Setup Tips* document provides helpful instructions for troubleshooting common connectivity problems.
- The *Spectra BlackPearl DS3 API Reference* provides information on understanding and using the DS3 API.

The following documents are available after logging into your Support portal account at: *support.spectralogic.com*.

- The *Spectra BlackPearl Release Notes and Documentation Updates* provide the most up-to-date information about the BlackPearl Object Gateway, including information about the latest software releases and documentation updates.
- The *Spectra 96-Bay Chassis Drive Replacement Guide* provides instructions for replacing a failed data drive in the 96-bay expansion node.
- The *Spectra 96-Bay Chassis Fan Replacement Guide* provides instructions for replacing a failed fan in the 96-bay expansion node.
- The *Spectra 96-Bay Chassis Power Supply Replacement Guide* provides instructions for replacing a failed power supply in the 96-bay expansion node.
- The *Spectra 96-Bay Chassis I/O Module Replacement Guide* provides instructions for replacing a failed I/O module in the 96-bay expansion node.
- The *Spectra 107-Bay Expansion Node FRU Guide* provides instructions for replacing fans, power supplies, drives, and SAS expanders in the 77-bay and 107-bay expansion node.
- The *Spectra BlackPearl H-Series Chassis Part Replacement Guide* provides instructions for replacing parts in the Spectra BlackPearl H-series chassis.

Spectra Logic Software User Guides

The guides for this section are for other Spectra Logic products that use the BlackPearl Object Gateway as a core component.

- *Spectra Vail User Guide*
- *Spectra StorCycle User Guide*
- *Spectra Rio MediaEngine User Guide*

Tape Library User Guides

Spectra Logic Tape Libraries

User Guides for Spectra Logic tape libraries are posted on the Support Portal website at: *support.spectralogic.com/documentations/user-guides*.

ONLINE RESOURCES

Online BlackPearl User Guide

The BlackPearl User Guide is available in an online format located at: *https://support.spectralogic.com/blackpearl/BlackPearlOnlineHelp.htm*

WHAT'S NEW

BlackPearl OS 5.9 brings with it the following changes and improvements:

Redesigned User Interface

The BlackPearl user interface is completely overhauled with a new graphic style and optimized for greater usability and ease of information access.

Configurable Maximum Concurrent Job Value

Using API commands, you are now able to configure the maximum concurrent number of jobs up to the new limit of 500,000 jobs. Additionally, the default maximum number of concurrent jobs is increased to 40,000.

⚠ **IMPORTANT** If you have changed the number of concurrent jobs, the changed value is overwritten with the new 40,000 default value. Contact Spectra Logic Technical Support for assistance in restoring the previously configured value.

New API Commands

Commands to control the maximum concurrent jobs, view Advanced Bucket Management configuration, and view enhanced information about a specified tape cartridge have been added or modified. Additionally, API changes have been made to support LTO-10 tape drives, capacity reporting information for tape libraries, and filtering tapes lists by bucket, partition, or storage domain.

Configurable ZFS Record Size

You are now able to configure the ZFS record size using the BlackPearl user interface, CLI, and API commands. This setting determines how data is divided and stored on disk. In general, larger values increase performance at the cost of increased storage space requirements.

Improved Performance with Arctic Blue Expansion Nodes

Performance is improved for systems configured with multiple, separate, Arctic Blue (96-drive) expansion nodes. The BlackPearl Object Gateway now processes data storage operations to multiple expansion nodes simultaneously.

Improved Messaging and Logging

The BlackPearl Object Gateway is upgraded to proved better messaging and logging when various system events occur.

CIFS Advanced Parameter Updates

The BlackPearl Object Gateway now accepts the colon character (:) as part of the name of an advanced parameter for CIFS shares, allowing for a greater number of parameter types to be used.

Chapter 1 - Product Overview

This chapter provides an overview of the Spectra Logic BlackPearl Object Gateway features and components.

OVERVIEW

The BlackPearl Object Gateway allows data to move seamlessly into tape storage in a way not previously possible. It enables users to deploy a tier of deep storage that is cost effective, easy to manage, and scalable to exabytes of data.

FEATURES

The BlackPearl Object Gateway includes the following features:

Advanced Bucket Management

The BlackPearl Advanced Bucket Management (ABM) feature automates many aspects of deep storage including policy based multiple copies on diverse media types without the need for expensive middleware to operate the libraries and stream data to tape drives.

Attack Hardening

The BlackPearl Object Gateway provides safeguards to protect against outside threats to your data. These features are critical to maintaining control of data in the case of ransomware attacks. Immutable data snapshots, generated by trigger or on a configurable schedule, allow you to restore your data to a moment in time before the attack.

BlackPearl User Interface

The BlackPearl user interface is used to perform configuration and management tasks on the BlackPearl Object Gateway. It also lets you monitor the hardware and view system messages. The BlackPearl user interface also provides monitoring and control of some aspects of an attached Spectra Logic tape library.

DS3 Interface

The DS3 interface is a data transport and communication interface that allows software clients to direct and manage “bulk” storage read or write operations of data objects. This feature allows for bulk object storage operations with tape for accessibility at the lowest cost media option.

Easy Network-Based Administration

The BlackPearl Object Gateway can be configured over an Ethernet network using a standard web browser.

Integration with a Spectra Logic Tape Library

Fibre Channel and SAS HBAs can be installed to provide connectivity to a Spectra Logic tape library using LTO or TS11*xx* technology drives.

Intelligent Object Management

With IOM, the BlackPearl Object Gateway is capable of self-healing files present on the Gateway, as well as automatically compacting data stored on tape, and provides an easy migration path from one type of storage to another. IOM also allows multiple object versioning and data pre-staging from tape to disk, and improves tape library performance by reducing the number of cartridge mounts.

LTFS Format

The BlackPearl Object Gateway with a supported tape library, writes data on tape in the open Linear Tape File System® (LTFS) format to ensure you are always able to access it.

Mirrored Boot Drives

The operating system is hosted on two mirrored drives.

Multi-Factor Authentication

The BlackPearl Object Gateway offers multi-factor authentication, which enhances the security of your BlackPearl Object Gateway by using an authenticator app to confirm the identity of any user trying to log in to the BlackPearl user interface. This prevents unauthorized access to the system even if the user credentials needed to access the system are compromised.

Rack-Mount Hardware

The BlackPearl chassis are designed to mount in a standard 4-post, 19-inch (48.3 cm) rack using just 2U (3.5 inches, 8.9 cm) or 4U (7 inches, 17.8 cm) of rack space, depending on the size of the Gateway. Rack-mounting hardware is included with each BlackPearl Object Gateway.

RAID-Protected Data Drives

The base BlackPearl Object Gateway includes solid-state drives which store the system database, and spinning disk drives or solid-state drives which provide the Gateway’s caching capacity. The drives are grouped into volumes with double-parity protection and data integrity verification to protect against data corruption.

Replicated Configuration

The BlackPearl Object Gateway has mirrored system drives and replicates the data on the system drives to all data pools. If one or both boot drives fail, the Gateway recovers automatically when replacement boot drives are installed.

Redundant Hardware

The Gateway features N+1 redundant power supplies and data drives that are hot-swappable for uninterrupted operation. Any data drives not configured in a storage pool act as global spares. A spare becomes active if a drive in a storage pool fails.

Optional Network Attached Storage Features

Volume Snapshots

Volume Snapshots are images of a volume’s configuration and data makeup as they were when the snapshot was generated. Snapshots are immutable and cannot be overwritten or altered. This protects against any data deletions, encryption, revision, alterations, or appendments. Restoring to triggered or time-based snapshots allow you to go “back in time” and restore the volume to the state it was in when the snapshot was created.

Snapshot Change Threshold

The BlackPearlObjectGateway allows you to set a threshold for the amount of data in a snapshot that changes before a user is notified. Changes to the size of a snapshot may be caused by a ransomware attack

File Sharing Connectivity for Major Operating Systems

The Network File System (NFS) and Common Internet File System (CIFS) protocols provide connectivity to most major operating systems, including Microsoft® Windows®, macOS®, UNIX®, and Linux®. Solid state disk drives may be installed in your system to improve NFS performance.

Data Replication

You can select to replicate data from the NAS volumes on the BlackPearl Object Gateway to one or more NAS replication targets.

Network File Interface

The NFI service (Network File Interface) automatically transfers files from the NAS volumes on the Gateway to BlackPearl managed object storage on the same Gateway or on a remote BlackPearl Object Gateway.

Metadata Performance Drives

Metadata Performance Drives increase performance when searching metadata, restoring small files, and in deduplication operations. These drives are dedicated to storing metadata information about all objects on the pool and are useful if you search many files before restoring them.

Write Performance Drives

The BlackPearl Object Gateway supports even numbers of solid state drives as Write Performance drives. The drives increase write speed to shared NFS volumes on the system.

Optional Hardware Features

HotPair

Two BlackPearl master nodes, a Gen2 X Series or Gen3 master node with two server modules can be connected to multiple expansion nodes in a failover configuration. One master node acts as the primary controller, and the other acts as the secondary. In the event that the secondary controller detects a failure of the primary controller, it automatically takes over to provide uninterrupted operation, without administrative intervention.

44-Bay Expansion Node

For Gen1 master nodes, the BlackPearl 44-bay expansion node accommodates up to 44 disk drives with an active bezel, and 45 disk drives with a passive bezel. Up to eight 44-bay expansion nodes can be connected to a BlackPearl 4U master node, which allows the Gateway to use the 44-bay expansion nodes as storage domain targets. Up to two 44-bay expansion nodes can be connected to a BlackPearl 2U master node.

96-Bay Expansion Node

The 96-bay expansion node accommodates up to 96 disk drives with an active or passive bezel. Up to nine 96-bay expansion nodes can be connected to a BlackPearl 4U master node, which allows the master node to use the 96-bay expansion nodes as storage domain targets. Up to two 96-bay expansion nodes can be connected to a BlackPearl 2U master node.

Note: Depending on the power requirements of the drives installed in the 96-bay expansion node, some configurations do not support up to 96 drives.

77-Bay and 107-Bay Expansion Nodes

The 77-bay and 107-bay expansion nodes accommodate up to 77 or 107 disk drives, respectively, with an active or passive bezel, to use for storage domain targets.

- Up to nine 77-bay and 107-bays expansion nodes can be connected to a Gen2 S or V Series, or a Gen3, master node.
- Up to eight 77-bay and 107-bay expansion nodes can be connected to a Gen1 S or P Series 4U master node or a Gen2 BlackPearl X Series master node.
- Up to two 77-bay and 107-bay expansion nodes can be connected to a Gen1 V Series 2U master node.

Networking Interfaces

Gen3 Chassis

The BlackPearl Gen3 chassis offer Ethernet HBA in 10/25 Gbps or 40/100 Gbps speeds for the data connection. The management interface uses a 1 Gbps Ethernet port.

Gen2 Chassis

1 Gigabit Ethernet

For the Gen2 X Series chassis includes an onboard 1 Gigabit Ethernet port to access the BlackPearl User Interface.

For the Gen2 V Series chassis, two onboard 1 Gigabit copper ports (10GBase-T) provide Ethernet connectivity for the Gateway with one dedicated port used to access the BlackPearl user interface.

10GBase-T Ethernet Connectivity

For the Gen2 S Series chassis, two onboard 10 Gigabit copper ports (10GBase-T) provide Ethernet connectivity for the Gateway with one dedicated port used to access the BlackPearl user interface.

Optionally, the Gen2 S and V series may include a two-port 10GBase-T network interface card to provide a data connections between hosts and the BlackPearl Object.

25 Gigabit Ethernet

For Gen2 S and V Series chassis, an optional dual port, 25 Gigabit Ethernet (25 GigE) network interface card can be installed to provide high-speed data connections between hosts and the BlackPearl Object Gateway.

100 Gigabit Ethernet

For Gen2 X Series chassis, a dual port, 100 Gigabit Ethernet (100 GigE) network interface card is installed to provide Ethernet connectivity for the Gateway.

1 Gigabit IPMI

For all Gen2 Chassis, a 1 Gigabit Ethernet port provides access to the system IPMI interface. On the Gen2 X series, the IPMI port is integrated with the BlackPearl management port.

Gen1 Chassis

10GBase-T Ethernet Connectivity

Two onboard 10 gigabit copper ports (10GBase-T) provide Ethernet connectivity for the Gateway with one dedicated port used to access the BlackPearl user interface.

10GBase-T Ethernet

An optional dual port, 10 gigabit copper (10GBase-T) network interface card can be installed to provide high-speed data connections between hosts and the BlackPearl Object Gateway.

10 Gigabit Ethernet

A dual port, 10 Gigabit Ethernet (10 GigE) network interface card is installed to provide high-speed data connections between hosts and the BlackPearl Object Gateway.

40 Gigabit Ethernet

An optional dual port, 40 Gigabit Ethernet (40 GigE) network interface card can be installed to provide high-speed data connections between hosts and the BlackPearl Object Gateway.

COMPONENTS

The following sections show the locations of and briefly describe the BlackPearl Object Gateway's major front and rear panel components.

Front Bezel

All BlackPearl chassis include a front bezel, which is attached with magnets.

Note: For the 77-bay, 96-bay and 107-bay expansion node, the bezel is permanently attached.

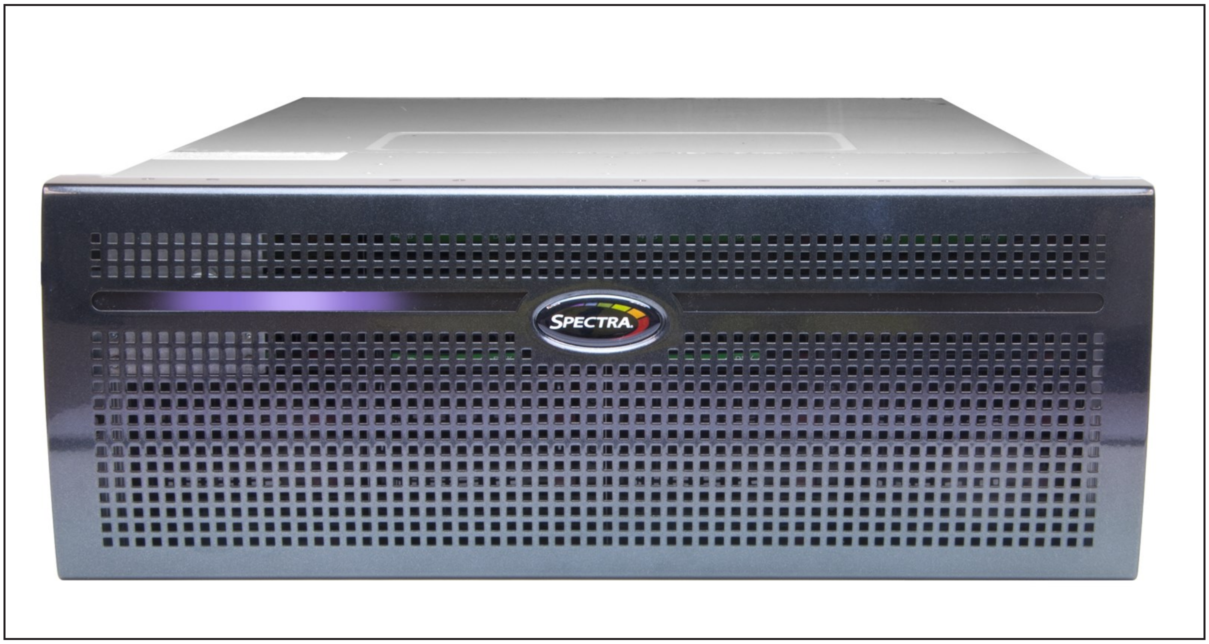


Figure 1 A 4U BlackPearl chassis with front bezel and visual status beacon.

In most cases, the front bezel includes a visual status beacon light bar which provides status information for the Gateway. See Monitor the Gateway Hardware on page 246 for information about the status indicated by each visual status beacon color/pattern.

Gen3 F Series

Front View

Figure 2 shows the components on the front of the Gen3 F Series BlackPearl Object Gateway with the front bezel removed.

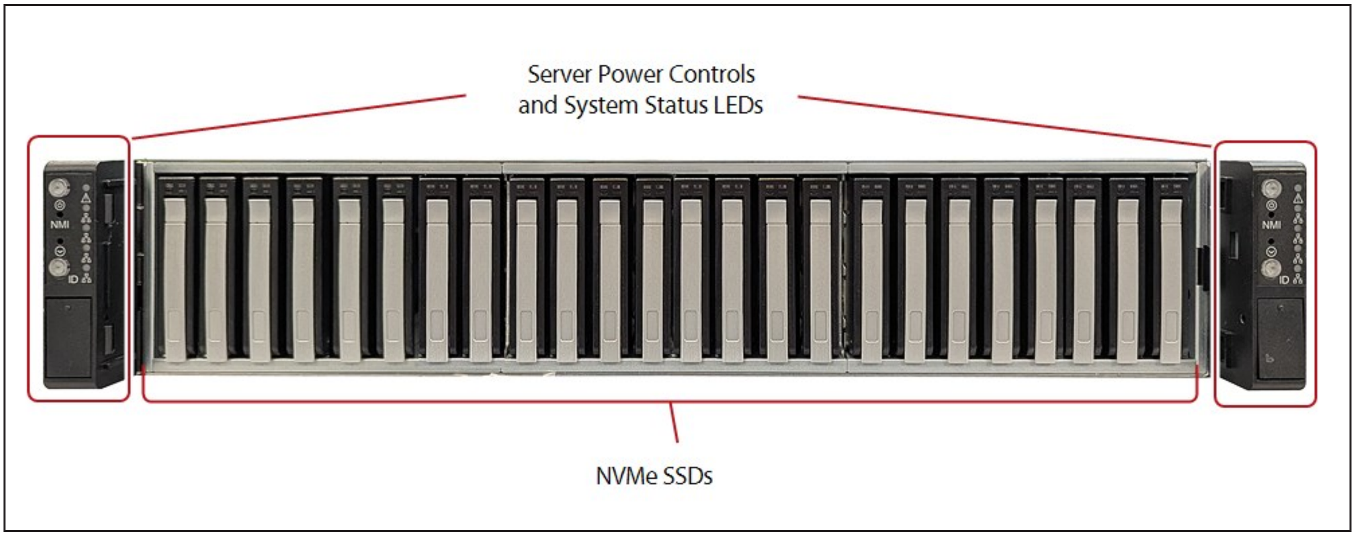


Figure 2 The front view of the Gen3 F Series BlackPearl Object Gateway (front bezel removed).

Component	Description
Sever power controls	Power controls for each of the two installed server modules. The lower module uses the power controls on the left-hand side. The upper module (optional) uses the power controls on the right-hand side.
System status LEDs	The status LEDs indicate power status, server status, and the link status of motherboard Ethernet ports.
Data drives	The base Gen3 F Series BlackPearl Object Gateway supports up to 24 high-performance NVMe drives mounted on individual drive sleds. The drive sleds slide into bays in the front of the chassis and lock in place. The front of each drive sled has a handle for removing the sled.
Data drive status LEDs	Two blue LEDs display drive status: • The left blue LED indicates drive activity. • The right red LED indicates a drive error.
Empty drive sleds	Empty drive sleds are installed in the unused drive bays to prevent contaminants from entering the enclosure and to maintain proper air flow. Ensure each empty drive sled has a 'drive blank' installed in the sled for proper airflow and cooling.

Rear View

Figure 3 shows the major components on the rear of the Gen3 F series BlackPearl Object Gateway.

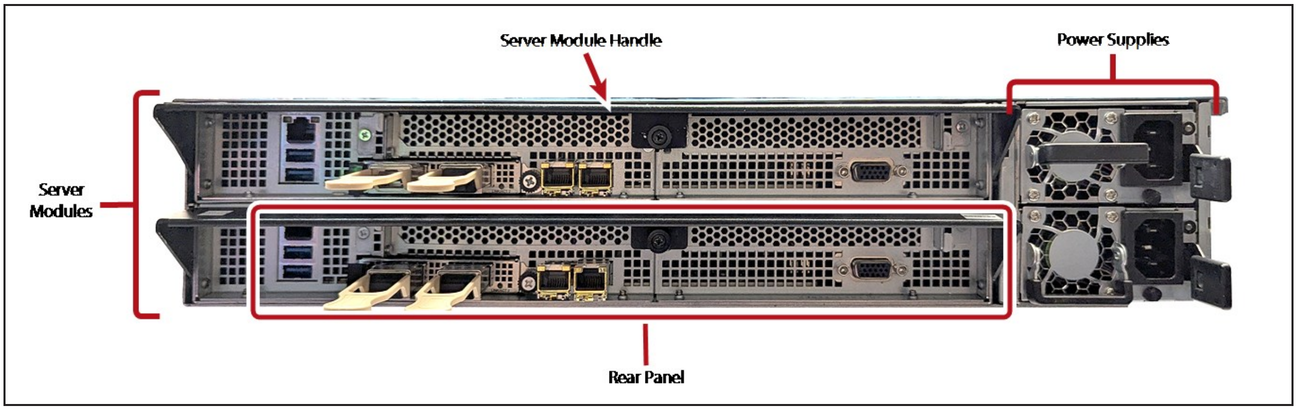


Figure 3 The rear view of the Gen3 F Series BlackPearl Object Gateway.

Component	Description
Sever module	The BlackPearl Gen3 F series chassis supports up to two server modules. The bottom module is always installed. The top module is only installed in a HotPair configuration.
Rear panel	The rear panel of the Gen3 F Series BlackPearl server module allows for Ethernet, Fibre Channel, SAS, USB, IPMI, and other connections. See Rear Panel on the next page for a detailed description.
Power modules	The Gen3 F Series BlackPearl Object Gateway includes two power modules. Each power module has active current sharing and supports N+1 redundancy. • Each power supply has its own AC power connector. • Each power supply has a bi-color LEDs to indicate power to the power module and status of the power module. • Not lit - Neither power module has AC power. • Amber solid - The power module experienced a critical event and shut down or the power cord is unplugged. • Green solid - The power module is on and OK.
Server module handle	The sever handle is used to install or uninstall the server module. When not in use, a thumbscrew locks the handle in place.

Rear Panel

Figure 4 shows the components on the rear panel of the Gen3 F Series BlackPearl master node.

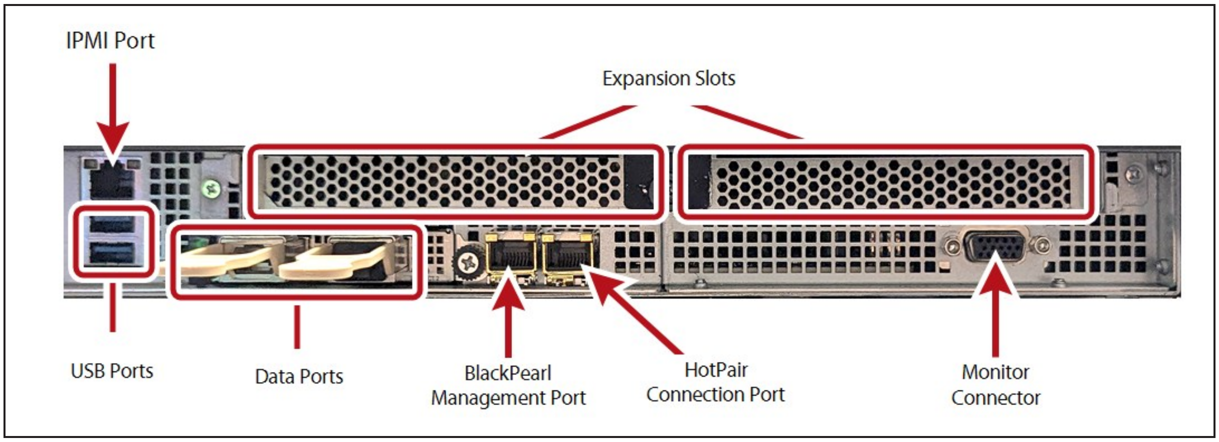


Figure 4 The Gen3 F Series BlackPearl rear panel components.

Component	Description
IPMI management port	See IPMI Configuration on page 434 for information on using IPMI management. The port has two status LEDs: • Activity / Link LED • Off - No Link • Blinking Amber - Data activity • On - Link • Speed LED • Off - Indicates 10 Mbps connection or no link • Amber - Indicates 100 Mbps connection • Green - Indicates 1 Gbps connection
USB ports	Four USB 3.1 Gen 1 Ports are available on the F Series BlackPearl chassis. If necessary, you can use these ports to connect a USB drive, or USB keyboard to the chassis for troubleshooting purposes as directed by Spectra Logic Technical Support.
Data Ports	Two 100 GigE ports provide the data connection to the BlackPearl Object Gateway.
Expansion Slots	Two expansion slots provide support for either SAS or Fibre Channel connections.

Component	Description
BlackPearl management port	The BlackPearl management port is used to connect to a browser-based user interface to configure, manage, and monitor the BlackPearl Object Gateway. The BlackPearl management port cannot be used for data transfer.
HotPair Connection port	The HotPair connection port is only used in a HotPair configuration.
Monitor connector	If necessary, you can connect a monitor to the VGA connector on the chassis for troubleshooting purposes. Only connect a monitor for initial configuration of the BlackPearl management port, or as directed by Spectra Logic Technical Support.

Internal Components

The following table describes the internal field replaceable components in the server module.

Internal Component	Description
Boot drives	Two NVMe M.2 boot drives provide high performance storage for the operating system and BlackPearl user interface. The NVMe M.2 boot drives are connected to the motherboard and are not hot-swappable.
Expansion slots and optional interface cards	The expansion slots accommodate optional interface cards to provide additional connectivity. • The Gen3 F series optionally includes: • Up to two optional four-port 12 GB SAS cards provide connectivity to SAS drives in a Spectra Logic or supported tape library, or provide connectivity for up to eight 77-bay and 107-bay expansion nodes. • Up to two optional four-port 16 GB or 32 GB Fibre Channel cards provides connectivity to Fibre Channel tape drives in a Spectra Logic or supported tape library.

Gen3 H Series

Note: Except where noted, the information in this section applies to both the Gen 3 H 3310 and Gen 3 H 3300 series chassis.

Front View

Figure 5 shows the components on the front of the Gen3 H Series BlackPearl Object Gateway with the front bezel removed.

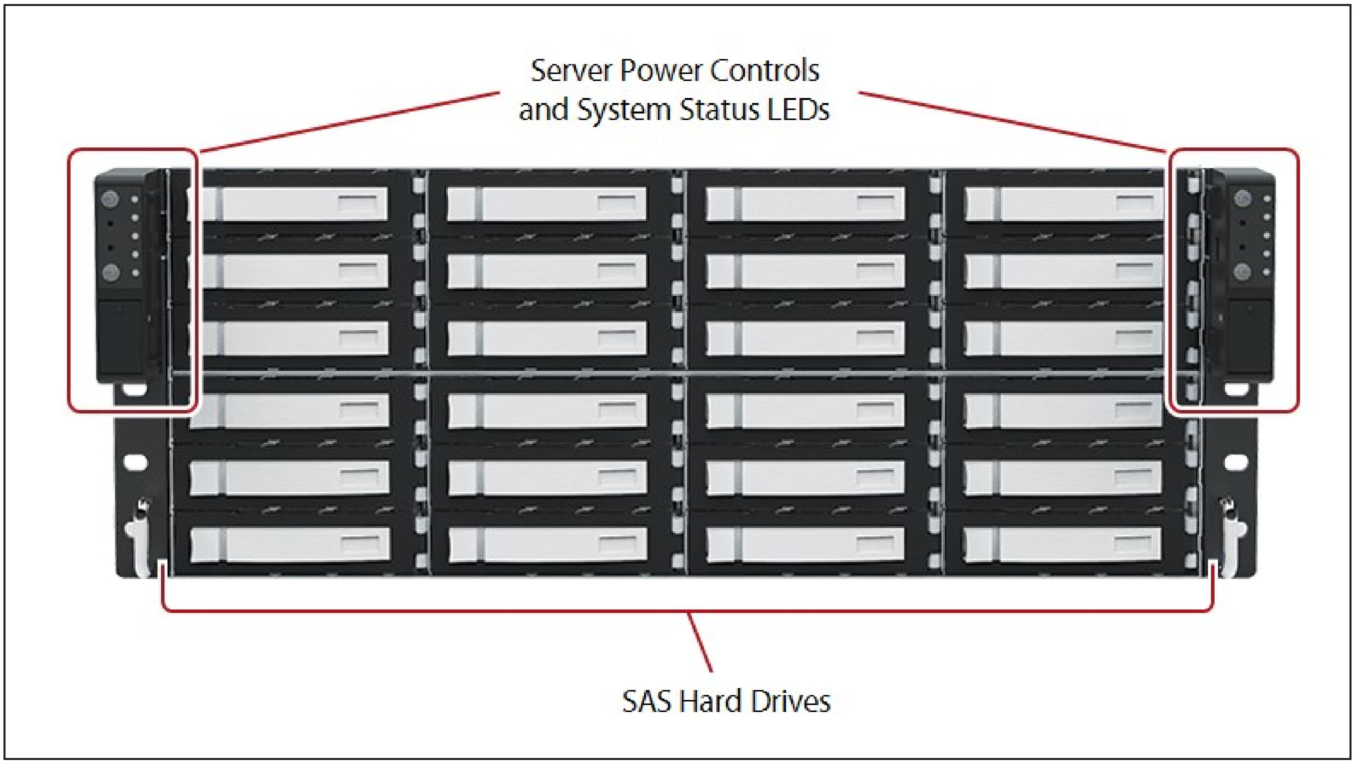


Figure 5 The front view of the Gen3 H Series BlackPearl Object Gateway (front bezel removed).

Component	Description
Sever power controls	Power controls for each of the two installed server modules. The lower module uses the power controls on the left-hand side. The upper module (optional) uses the power controls on the right-hand side.
System status LEDs	The status LEDs indicate power status, server status, and the link status of motherboard Ethernet ports. **Note:** The LEDs are not visible with the bezel installed.
Data drives	The base Gen3 H Series BlackPearl Object Gateway supports up to 24 high-performance SAS hard drives (HDDs) mounted on individual drive sleds.

Component	Description
	The drive sleds slide into bays in the front of the chassis and lock in place. The front of each drive sled has a handle for removing the sled.
Data drive status LEDs	Two blue LEDs display drive status: • The upper LED indicates drive activity. • The lower LED indicated a drive error. **Note:** The LEDs are not visible with the bezel installed.
Empty drive sleds	Empty drive sleds are installed in the unused drive bays to prevent contaminants from entering the enclosure and to maintain proper air flow. Ensure each empty drive sled has a 'drive blank' installed in the sled for proper airflow and cooling.

Rear View

Figure 6 shows the major components on the rear of the Gen3 H BlackPearl Object Gateway.

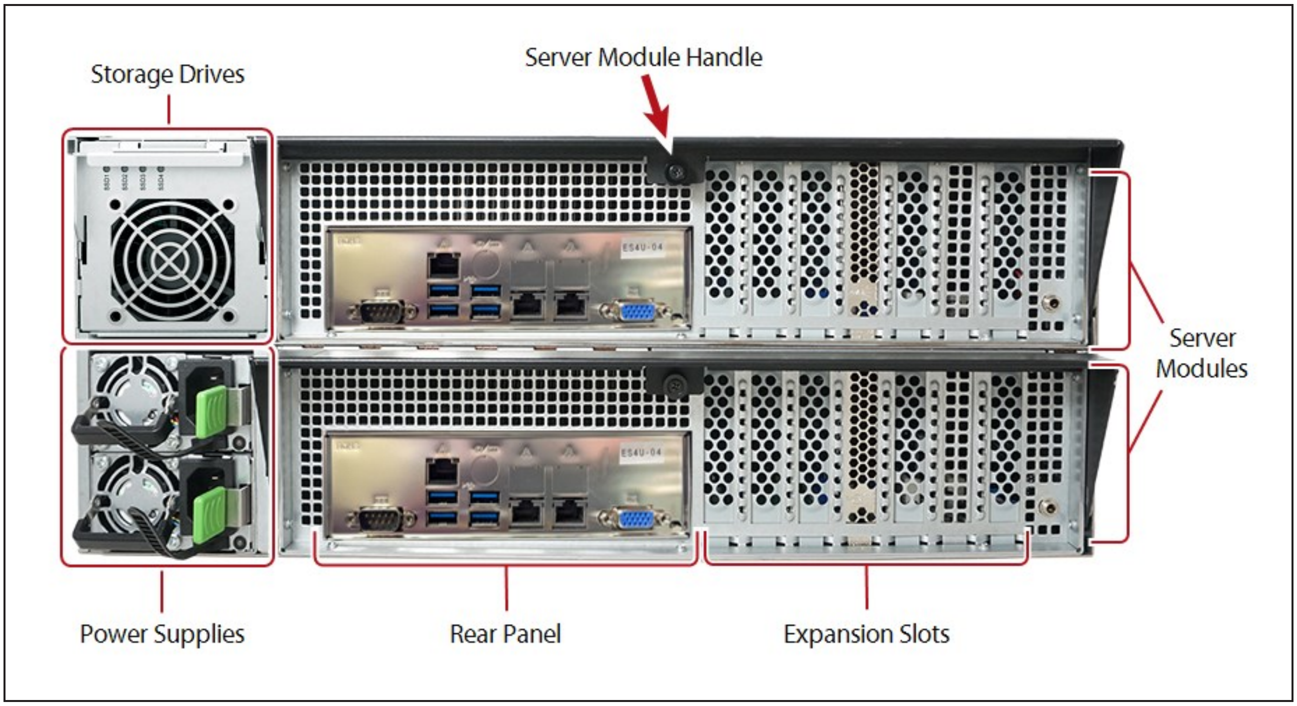


Figure 6 The rear view of the Gen3 H Series BlackPearl Object Gateway.

Component	Description
Sever module	The BlackPearl Gen3 H chassis supports up to two server modules. The bottom module is always installed. The top module is only installed in a HotPair configuration.

Component	Description
Rear panel	The rear panel of the Gen3 H Series BlackPearl master node allows for Ethernet, Fibre Channel, SAS, USB, IPMI, and other connections. See Rear Panel on the next pagefor a detailed description.
Storage drives	The Gen 3 H Series supports up to four NVMe drives in the rear of the chassis for the BlackPearl database, special allocation, metadata performance, and ZIL. **Note:** The Gen 3 H 3310 Series supports two additional NVMe drives mounted inside the chassis.
Expansion slots	The expansion slots in the Gen3 H series chassis allows for Ethernet, SAS, and Fibre Channel connections using optional HBA modules.
Power modules	The Gen3 H Series BlackPearl Object Gateway includes two power modules. Each power module has active current sharing and supports N+1 redundancy. • Each power supply has its own AC power connector. • Each power supply has a bi-color LEDs to indicate power to the power module and status of the power module. • Not lit - Neither power module has AC power. • Amber solid - The power module experienced a critical event and shut down or the power cord is unplugged. • Green solid - The power module is on and OK.
Server module handle	The sever handle is used to install or uninstall the server module. When not in use, a thumbscrew locks the handle in place.

Internal Components

The following table describes the internal field replaceable components in the server module.

Internal Component	Description
Boot drives	Two NVMe M.2 boot drives provide high performance storage for the operating system and BlackPearl user interface. The NVMe M.2 boot drives are connected to the motherboard and are not hot-swappable.
Storage drives	The Gen 3 H 3310 Series supports two NVMe drives mounted inside the chassis for the BlackPearl database, special allocation, metadata performance, and ZIL.
Midplane board	• The H 3300 Series chassis features a SAS 3 midplane board.

Internal Component	Description
	• The H 3310 Series chassis features a SAS 4 midplane board.
Expansion slots and optional interface cards	The expansion slots accommodate optional interface cards to provide additional connectivity. • The Gen3 H series includes a two port 1 GigE card to provide data connection between hosts and the BlackPearl Object Gateway. • The Gen3 H series optionally includes: • One optional dual port 25 GigE HBAs using either 10 Gbps or 25 Gbps SFPs. Ports of the same type can be aggregated for better performance. • One optional dual port 100 GigE HBAs using either 40 Gbps or 100 Gbps SFPs. Ports of the same type can be aggregated for better performance. • Up to five optional four-port 12 GB SAS cards provide connectivity to SAS drives in a Spectra Logic or supported tape library, or provide connectivity for up to eight 77-bay and 107-bay expansion nodes. • Up to five optional four-port 16 GB or 32 GB Fibre Channel cards provides connectivity to Fibre Channel tape drives in a Spectra Logic or supported tape library.

Rear Panel

Figure 7 shows the components on the rear panel of the Gen3 H Series BlackPearl master node.

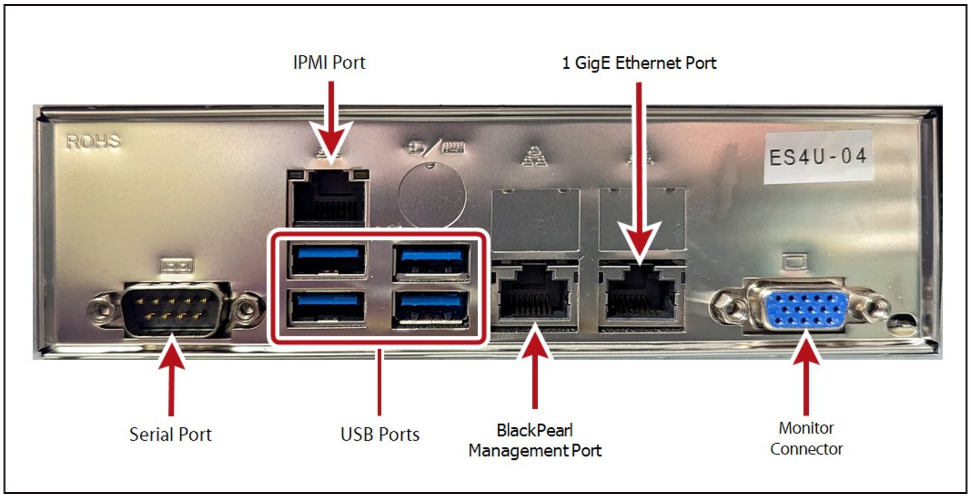


Figure 7 The Gen3 H Series BlackPearl rear panel components.

Component	Description
Monitor connector	If necessary, you can connect a monitor to the VGA connector on the chassis for troubleshooting purposes. Only connect a monitor for initial configuration of the BlackPearl management port, or as directed by Spectra Logic Technical Support.
Serial port	The serial port is only used in a HotPair configuration.
IPMI management port	See IPMI Configuration on page 434 for information on using IPMI management. The port has two status LEDs: • Activity / Link LED • Off - No Link • Blinking Amber - Data activity • On - Link • Speed LED • Off - Indicates 10 Mbps connection or no link • Amber - Indicates 100 Mbps connection • Green - Indicates 1 Gbps connection
USB ports	Four USB 3.1 Gen 1 Ports are available on the H Series BlackPearl chassis. If necessary, you can use these ports to connect a USB drive, or USB keyboard to the chassis for troubleshooting purposes as directed by Spectra Logic Technical Support.
1 Gigabit Ethernet ports	The Gen 3 H Series BlackPearl Object Gateways include two 10GBase-T ports. The left 1 Gigabit port is dedicated as the BlackPearl management port and cannot be used for data transfer. The right 1 Gigabit port can be used for network connectivity tests on a 1 Gigabit network but is not sufficient for normal data storage operations. Each port has two status LEDs: • Activity / Link LED • Off - No Link • Blinking Yellow - Data activity • On - Link • Speed LED • Off - Indicates 10 Mbps connection or no link • Amber - Indicates 100 Mbps connection • Green - Indicates 1 Gbps connection

Component	Description
BlackPearl management port	The BlackPearl management port is used to connect to a browser-based user interface to configure, manage, and monitor the BlackPearl Object Gateway. The BlackPearl management port cannot be used for data transfer.

Gen2 X Series

Front View

Figure 8 shows the components on the front of the Gen2 X Series BlackPearl Object Gateway with the front bezel removed.

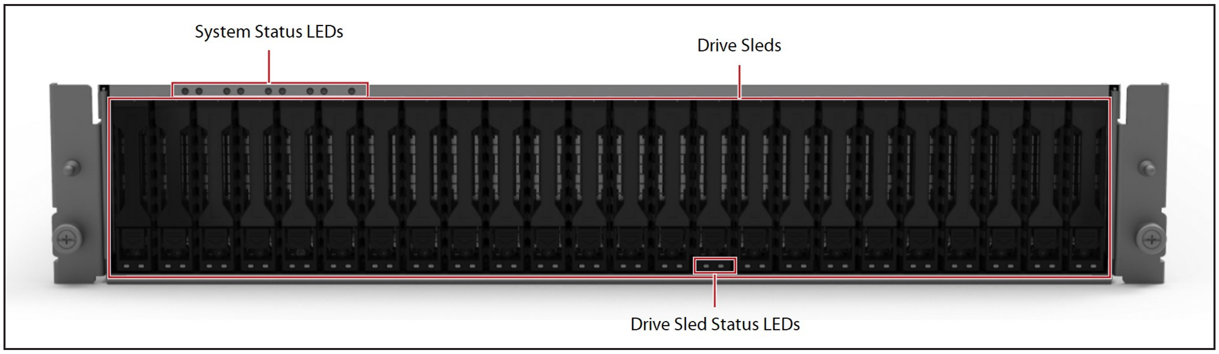


Figure 8 The front view of the Gen2 X Series BlackPearl Object Gateway (front bezel removed).

Component	Description
System status LEDs	The status LEDs indicate power status, fan status, server status, and chassis status. See Monitor the Gateway Hardware on page 246 for more information. **Note:** The LEDs are not visible with the bezel installed.
Data drives	The base Gen2 X Series BlackPearl Object Gateway includes two 1.6 TB high-performance solid-state drives (SSDs) for database storage and four 6.4 TB high-performance solid-state drives for the object cache. Up to 18 additional drives can be added for a total of 24 drives. The drive sleds slide into bays in the front of the chassis and lock in place. The front of each drive sled has a handle for removing the sled and a latch for locking the drive sled in place.
Data drive status LEDs	The blue LED indicates the location of the drive for servicing. The green / amber bi-color LED indicates the drive status. • Off - There is no SSD activity. • Green - SSD activity is detected. No faults are detected. • Solid Amber - The SSD experienced a fault and requires a service action. • Amber blinking at 1 Hz - The SSD is attempting to link. • Amber blinking at 2 Hz - The SSD failed to link. **Note:** The LEDs are not visible with the bezel installed.

Component	Description
Empty drive sleds	Empty drive sleds are installed in the unused drive bays to prevent contaminants from entering the enclosure and to maintain proper air flow. Ensure each empty drive sled has a 'drive blank' installed in the sled for proper airflow and cooling.

Rear View

Figure 9 show the major components on the rear of the Gen2 X Series BlackPearl chassis.

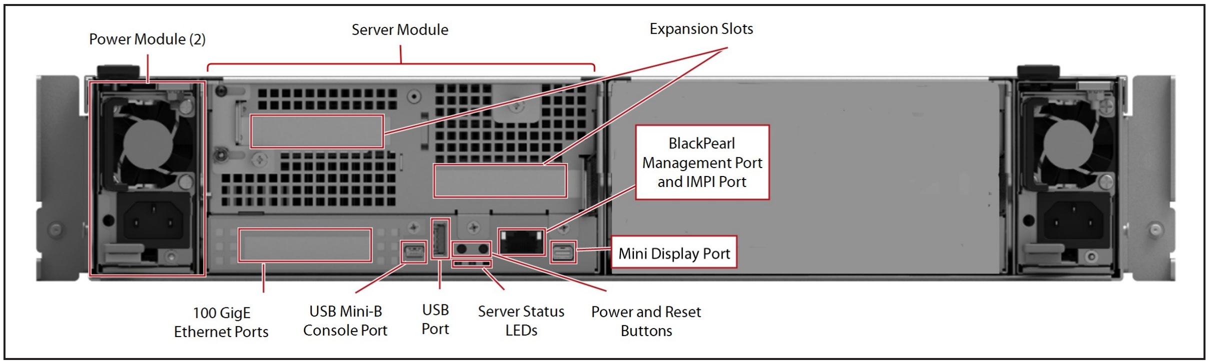


Figure 9 The rear view of the Gen2 X Series BlackPearl Object Gateway.

Component	Description
Power modules	The Gen2 X Series BlackPearl Object Gateway includes two power modules. Each power module has active current sharing and supports N+1 redundancy. • Each power supply has its own AC power connector. • Each power supply has a bi-color LEDs to indicate power to the power module and status of the power module. • Not lit - Neither power module has AC power. • Amber solid - The power module experienced a critical event and shut down or the power cord is unplugged. • Amber blinking - The power module detected hi-temp, hot spot temp, high current, or high-power warning, but continues to operate. • Green solid - The power module is on and OK.

Component	Description
Server status LEDs	The server module has three status LEDs below the server module power and reset buttons. A lit LED indicates the following: • Green - The server module has booted and is operating normally. A service action is not allowed. • Blue solid - The server module is being sent an identify command. • Blue blinking - A service action is allowed. • Amber - A server module fault has been detected.
Server Power and Reset buttons	The chassis powers on when power is connected or when the power button is pressed. Use the user interface, not the power button, to power down the chassis. To power on the chassis, insert a blunt pointed object (such as a paper clip) into the recessed opening to momentarily press the **Power** button. If directed by Spectra Logic Technical Support, use the server **Power** and **Reset** buttons to turn off power to the server module, or reset the server module CPU. Insert a blunt pointed object (such as a paper clip) into the recessed opening to press the **Power** or **Reset** button. • Press the **Power** button momentarily to initiate the normal shut-down sequence or to power on the server module. • Press and hold the **Power** button for 4 or more seconds to immediately power off the server module. • Press the **Reset** button monumentally to reset the power module.
BlackPearl management port and IPMI port	The BlackPearl management port is used to connect to a browser-based user interface to configure, manage, and monitor the Gen2 X Series BlackPearl Object Gateway. The BlackPearl management port cannot be used for data transfer. The port has two status LEDs: • Green - Indicates port activity at 1000 Mb. • Amber - Indicates port activity at 100 Mb. This port is also used to access the system IPMI interface using a separate IP address than the BlackPearl management port.
USB ports	Use these ports to connect a USB drive to the chassis to load configuration keys, or to connect a USB drive, or USB keyboard to the chassis for troubleshooting purposes as directed by Spectra Logic Technical Support. The front bezel connects to the active server module's USB port while in production use.
USB Mini-B port	Provides a serial console connection to a USB serial port to access the BlackPearl management console.
Mini DisplayPort	Provides for a PCIe video connection to the BlackPearl management console.

Internal Components

The following table describes the internal field replaceable components.

Internal Component	Description
Server module	The server module in the Gen2 X Series BlackPearl Object Gateway provides Ethernet, Fibre Channel, SAS, USB, and other connections. A second identically configured server module can be added for HotPair failover.
100 GigE Ethernet ports	The two 100 Gigabit Ethernet (100 GigE) ports are used for data transfer on an Ethernet network.
Expansion slots	The expansion slots accommodate optional interface cards to provide additional connectivity. • Up to two optional four-port SAS card provide connectivity to SAS drives in a Spectra Logic tape library, or provides connectivity for up to eight 77-bay and 107-bay expansion nodes. • Up to two four-port 16 GB or 32 GB Fibre Channel card provides connectivity to four Fibre Channel tape drives in a Spectra Logic or supported tape library.

Gen2 S Series and Gen2 V Series

Front View

Figure 10 shows the components on the front of the Gen2 S Series BlackPearl Object Gateway with the front bezel removed. Figure 11 shows the components on the front of the Gen2 V Series BlackPearl Object Gateway with the front bezel removed.

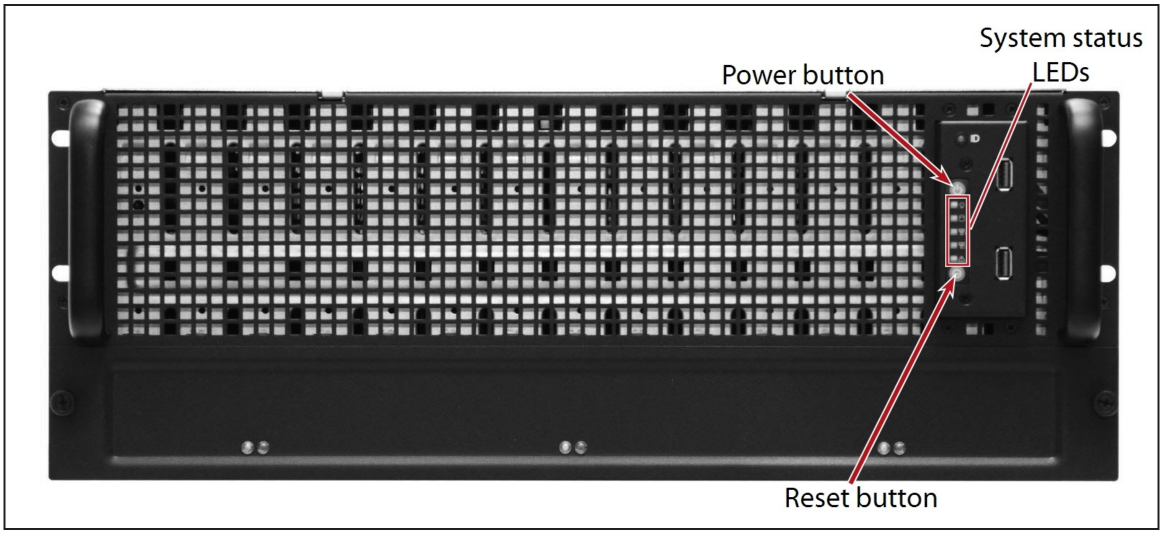


Figure 10 The front view of the Gen2 S Series BlackPearl 4U Gateway (front bezel removed).

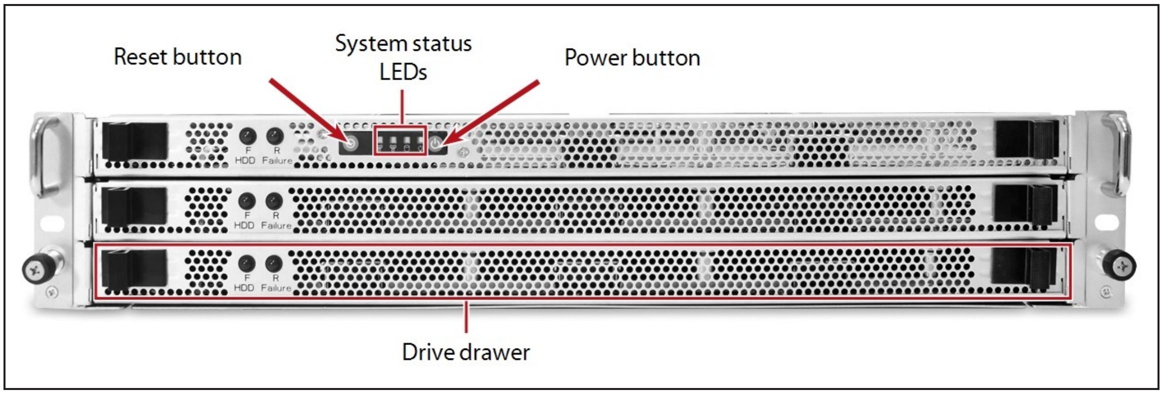


Figure 11 The front view of the Gen2 V Series BlackPearl 2U Gateway (front bezel removed).

Component	Description
Power button ⏻	The chassis powers on when power is connected or when the power button is pressed. Use the user interface, not the power button, to power down the chassis.

Component	Description
Reset button 	Only use the chassis reset button under direction of Spectra Logic Technical Support.
System status LEDs	The status LEDs indicate power status, disk and network activity, as well as hardware faults. See Monitor the Gateway Hardware on page 246 for more information. **Note:** The LEDs are not visible with the bezel installed.
Drive drawers (Gen2 V Series only)	Three drive drawers each contain eight drive bays for up to 24 high-performance disk drives. Depending on your order configuration, the BlackPearl Object Gateway may optionally contain solid state drives to improve NAS write performance. See Features on page 26 for more information.

Rear View

Figure 12 shows the major components on the rear of the Gen2 S BlackPearl Object Gateway. Figure 13 shows the major components on the rear of the Gen2 V Series BlackPearl Object Gateway.

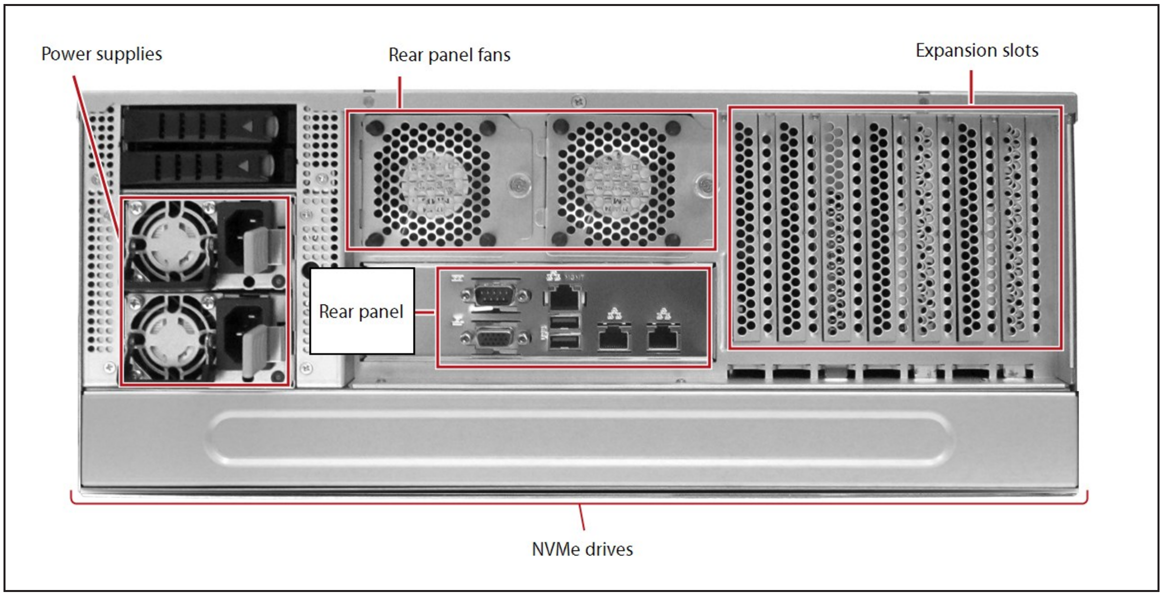


Figure 12 The rear view of the Gen2 S Series BlackPearl 4U Gateway.

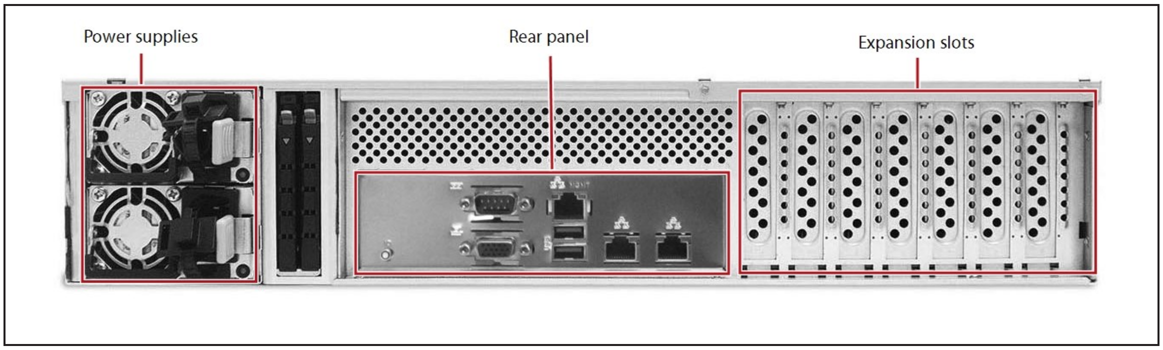


Figure 13 The rear view of the Gen2 V Series BlackPearl 2U Gateway.

Component	Description
Power supplies	The standard BlackPearl Object Gateway configuration includes two power supplies to provide N+1 redundancy and fail-over protection. Each power supply has its own AC power connector.
Rear panel fans (Gen2 S Series only)	Two rear panel fans and four internal fans provide the cooling for the Gen2 S series chassis. The rear panel fans are hot-swappable. The Gen2 V series has three internal fans.

Component	Description
Rear panel	The rear panel of the Gen2 S Series and Gen2 V Series BlackPearl master node allows for Ethernet, Fibre Channel, SAS, USB, and other connections. See Rear Panel on the next pagefor a detailed description.

Internal Components

The following table describes the internal field replaceable components.

Internal Component	Description
Boot drives	Two NVMe boot drives provide high performance storage for the operating system and BlackPearl user interface. The NVMe boot drives are connected to the motherboard and are not hot-swappable.
NVMe SSD drives	The Gen 2 S Series supports up to 10 NVMe drives for the BlackPearl database, special allocation, metadata performance, and ZIL.
Expansion slots and optional interface cards	The expansion slots accommodate optional interface cards to provide additional connectivity. • The Gen2 V series includes a two port 10GBase-T card to provide data connection between hosts and the Gen2 V series. • The Gen2 S series optionally includes a two port 10GBase-T card to provide data connection between hosts and the Gen2 S series. • Up to two optional dual port 25 GigE cards provide a high-speed data connection between hosts and the Gen2 S Series and Gen2 V Series BlackPearl Object Gateway. Ports of the same type can be aggregated for better performance. • Up to three optional four-port SAS cards provide connectivity to SAS drives in a Spectra Logic tape library, or provide connectivity for up to eight 77-bay and 107-bay expansion nodes. • Up to three four-port Fibre Channel card provides connectivity to Fibre Channel tape drives in a Spectra Logic or supported tape library.

Rear Panel

Figure 14 shows the components on the rear panel of the Gen2 S Series and Gen 2 V Series BlackPearl 4U and 2U master nodes.

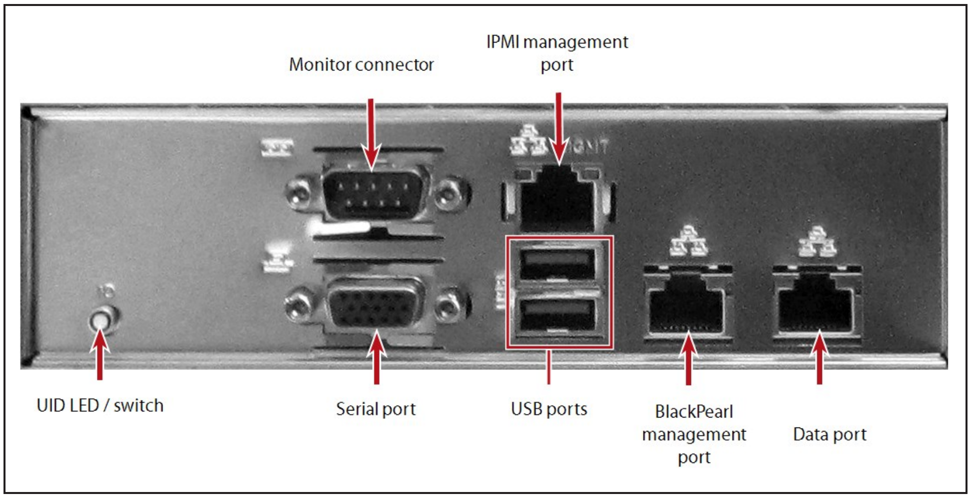


Figure 14 Gen2 S Series and Gen 2 V Series BlackPearl rear panel components.

Component	Description
UID LED / switch	Pressing the unit ID LED / switch displays a flashing blue pattern on the visual status beacon (see Monitor the Gateway Hardware on page 246) and the UID LED on the back of the chassis to make finding the chassis easier when moving between the front and rear of the rack.
Monitor connector	If necessary, you can connect a monitor to the VGA connector on the chassis for troubleshooting purposes. Only connect a monitor for initial configuration of the BlackPearl management port, or as directed by Spectra Logic Technical Support.
Serial port	The serial port is only used in a HotPair configuration.

Component	Description
IPMI management port	See IPMI Configuration on page 434 for information on using IPMI management. The port has two status LEDs: • Activity / Link LED • Off - No Link • Blinking Amber - Data activity • On - Link • Speed LED • Off - Indicates 10 Mbps connection or no link • Amber - Indicates 100 Mbps connection • Green - Indicates 1 Gbps connection
USB ports	Two USB 3.1 Gen 1 Ports are available on both the V Series and the S Series BlackPearl chassis. The S Series chassis also has one USB 3.1 Gen 2 Port (not shown). If necessary, you can use these ports to connect a USB drive, or USB keyboard to the chassis for troubleshooting purposes as directed by Spectra Logic Technical Support. The front bezel connects to one of the USB ports while in production use.
1 Gigabit Ethernet ports	The Gen 2 V Series BlackPearl Object Gateways include two 10GBase-T ports. The left 1 Gigabit port is dedicated as the BlackPearl management port and cannot be used for data transfer. The right 1 Gigabit port can be used for network connectivity on a 1 Gigabit network. Each port has two status LEDs: • Activity / Link LED • Off - No Link • Blinking Yellow - Data activity • On - Link • Speed LED • Off - Indicates 10 Mbps connection or no link • Amber - Indicates 100 Mbps connection • Green - Indicates 1 Gbps connection **Note:** An optional 10GBase-T Ethernet card can be added for improved data transfer.

Component	Description
10GBase-T Ethernet ports	The Gen2 S Series BlackPearl Object Gateways include two 10GBase-T ports. The left 10GBase-T port is dedicated as the BlackPearl management port and cannot be used for data transfer. The right 10GBase-T port can be used for network connectivity on a 10GBase-T network. Each port has two status LEDs: • Activity / Link LED • Off - No Link • Blinking Yellow - Data activity • On - Link • Speed LED • Off - Indicates 1 Gbps or 100 Mbps connection, or no link • On - Indicates 10 Gbps connection **Notes:** • The 10GBase-T ports auto-negotiate down to 1 Gbps or 100 Mbps. • Optional Ethernet cards can be added for data transfer.
BlackPearl management port	The BlackPearl management port is used to connect to a browser-based user interface to configure, manage, and monitor the BlackPearl Object Gateway. The BlackPearl management port cannot be used for data transfer.

77-Bay and 107-Bay Expansion Nodes

Front View

Figure 15 shows the major components on the front of the 77-bay and 107-bay expansion nodes. There are no components or status indicators visible on the front of the 77-bay and 107-bay expansion nodes with the front bezel is attached.

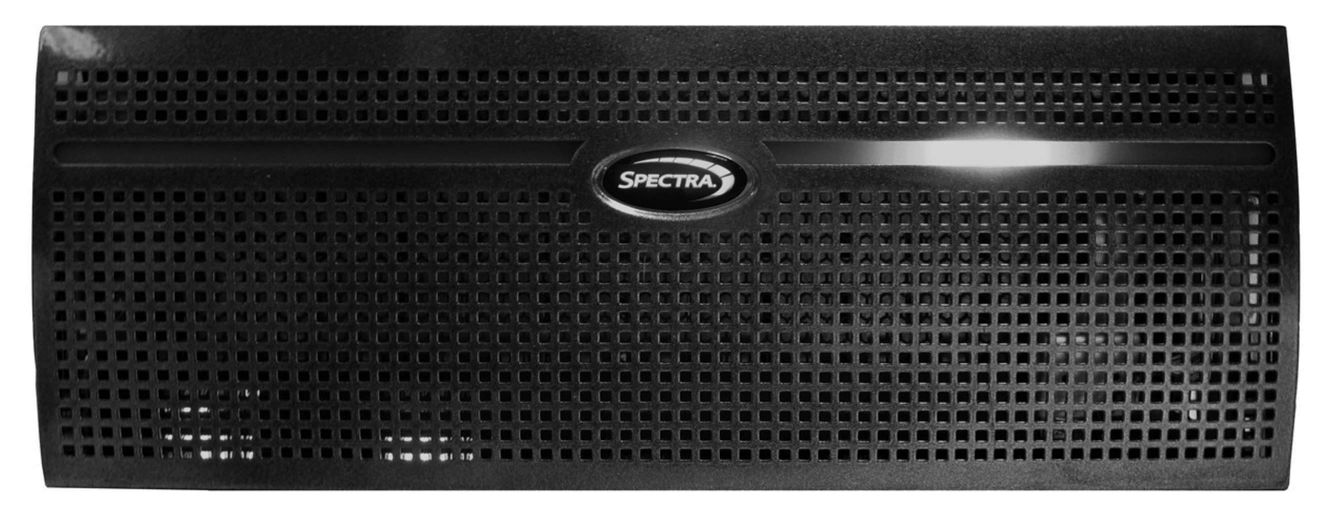


Figure 15 The front view of the 77-bay and 107-bay expansion nodes.

Internal Components

The following table describes the internal field replaceable components.

Internal Component	Description
Data drives	The 77-bay and 107-bay expansion nodes supports up to 77 or 107 enterprise disk drives, respectively. Disk drives are mounted on individual drive sleds in the chassis. The drive sleds slide into bays in the top of the enclosure and lock in place.

Rear View

Figure 16 shows the major components on the rear of the 77-bay and 107-bay expansion nodes.

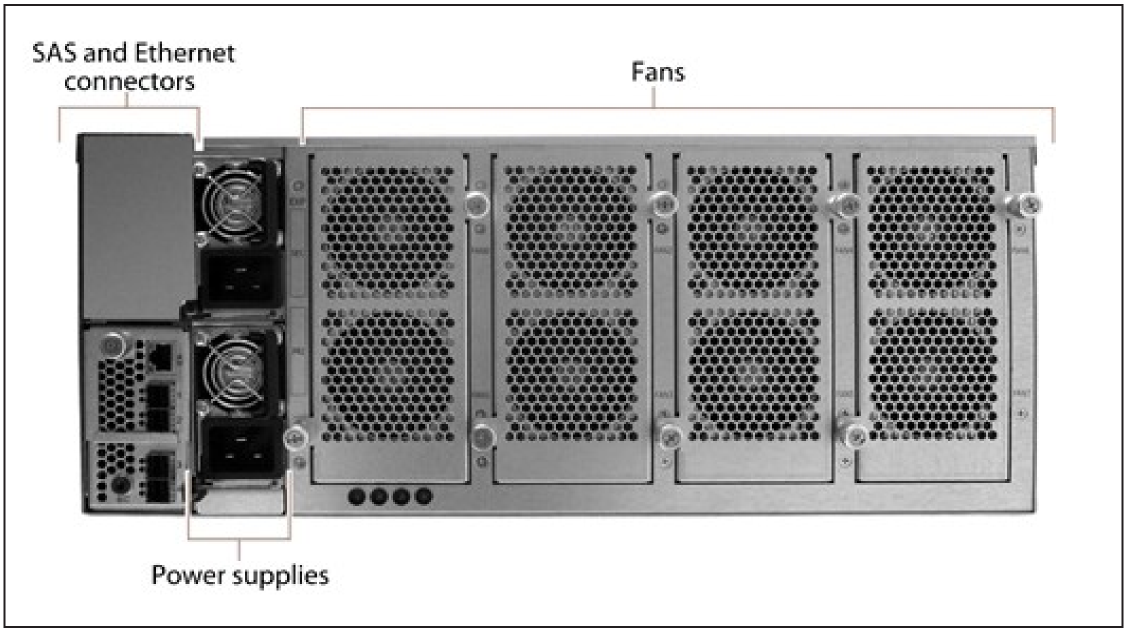


Figure 16 The rear view of the 77-bay and 107-bay expansion nodes.

Component	Description
SAS and Ethernet connectors	The rear panel of the 77-bay and 107-bay expansion nodes have one or two expander panels which include one Ethernet port and four SAS ports used to connect the 77-bay or 107-bay expansion node to a BlackPearl master node.
Fans	Eight hot-swappable fans, in banks of two, provide the cooling for the 77-bay and 107-bay expansion nodes.
Power supplies	The 77-bay and 107-bay expansion nodes includes two power supplies to provide N+1 redundancy and fail-over protection. • Each power supply has its own AC power connector. • Each power supply has a single LED that lights to indicate when the power is on and functioning normally.

Gen1 S Series, Gen1 P Series, and Gen1 V Series

Front View

Figure 17 shows the components on the front of the Gen1 S Series or Gen1 P Series BlackPearl Object Gateway. All information is the same for the Gen1 S Series and Gen1 P Series unless specified. Figure 18 shows the components on the front of the Gen1 V Series BlackPearl Object Gateway with the front bezels removed.

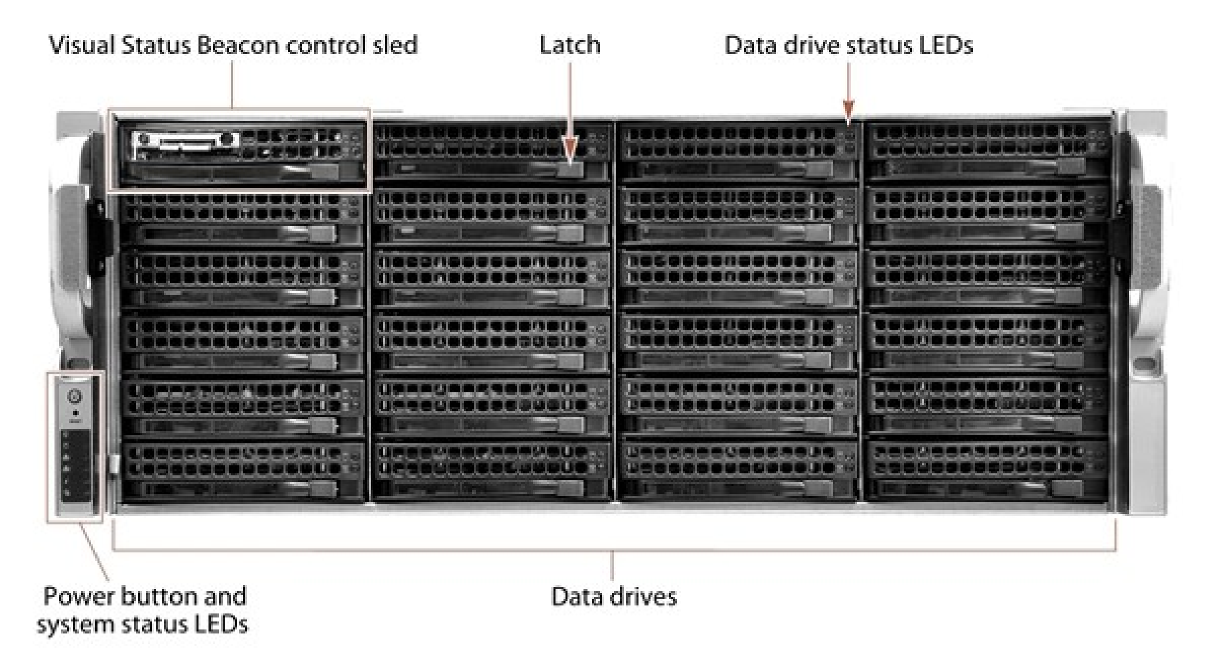

Visual Status Beacon control sled
Latch
Data drive status LEDs
Power button and system status LEDs
Data drives

Figure 17 The front view of the Gen1 S and P Series BlackPearl 4U master node (front bezel removed).

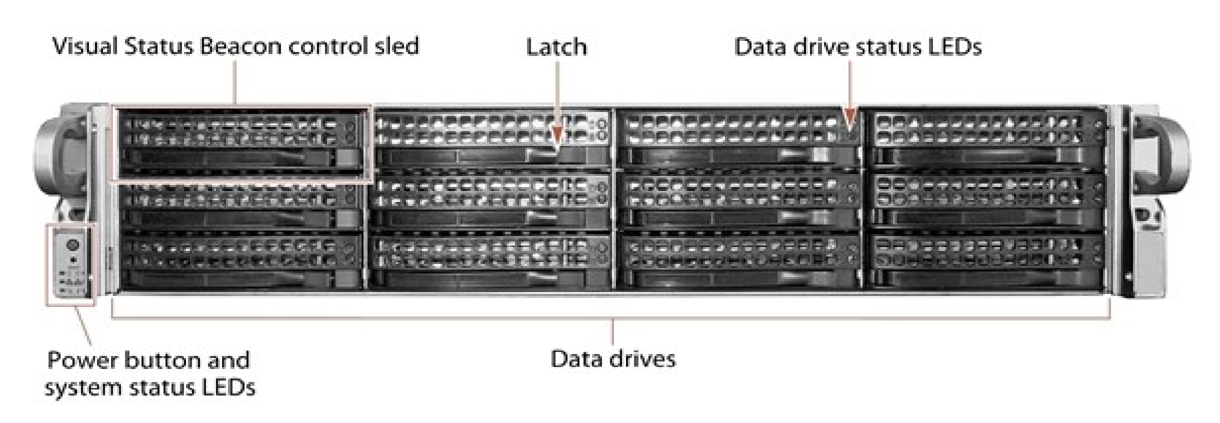

Visual Status Beacon control sled
Latch
Data drive status LEDs
Power button and system status LEDs
Data drives

Figure 18 The front view of the Gen1 V Series BlackPearl 2U master node (front bezel removed).

Component	Description
Visual Status Beacon control sled	The drive sled in the upper left corner of the front of the chassis provides control for the Visual Status Beacon. A disk drive cannot be installed in this position.
Power button	The chassis powers on when power is connected or when the power button is pressed. Use the user interface, not the power button, to power down the chassis.
System status LEDs	The status LEDs indicate power status, disk and network activity, as well as hardware faults. See Monitor the Gateway Hardware on page 246 for more information. **Note:** The LEDs are not visible with the bezel installed.
Data drives	The base BlackPearl Gen 1 S Series master node includes one high-performance solid-state drive, and five spinning-disk drives mounted on individual drive sleds in the front of the chassis. An additional 16 drives can be installed in the front of the chassis. The BlackPearl Gen 1 V Series master node includes ten spinning-disk drives and two high-performance solid-state drives in the front of the chassis. The drive sleds slide into bays in BlackPearl chassis and lock in place. The front of each drive sled has a handle for removing the sled from the chassis and a latch for locking the drive sled in place.
Data drive status LEDs	Two LEDs on each drive sled indicate the status of the drive. One LED is for drive status while the other shows drive activity. **Note:** The LEDs are not visible with the bezel installed.
Empty drive sleds	Empty drive sleds are installed in the unused drive bays to prevent contaminants from entering the enclosure and to maintain proper air flow.

Rear View

Figure 19 shows the major components on the rear of the Gen1 S or Gen1 P Series BlackPearl master node. All information is the same for the Gen1 S Series and Gen1 P Series unless specified. Figure 20 shows the major components of the Gen1 V Series BlackPearl master node chassis.

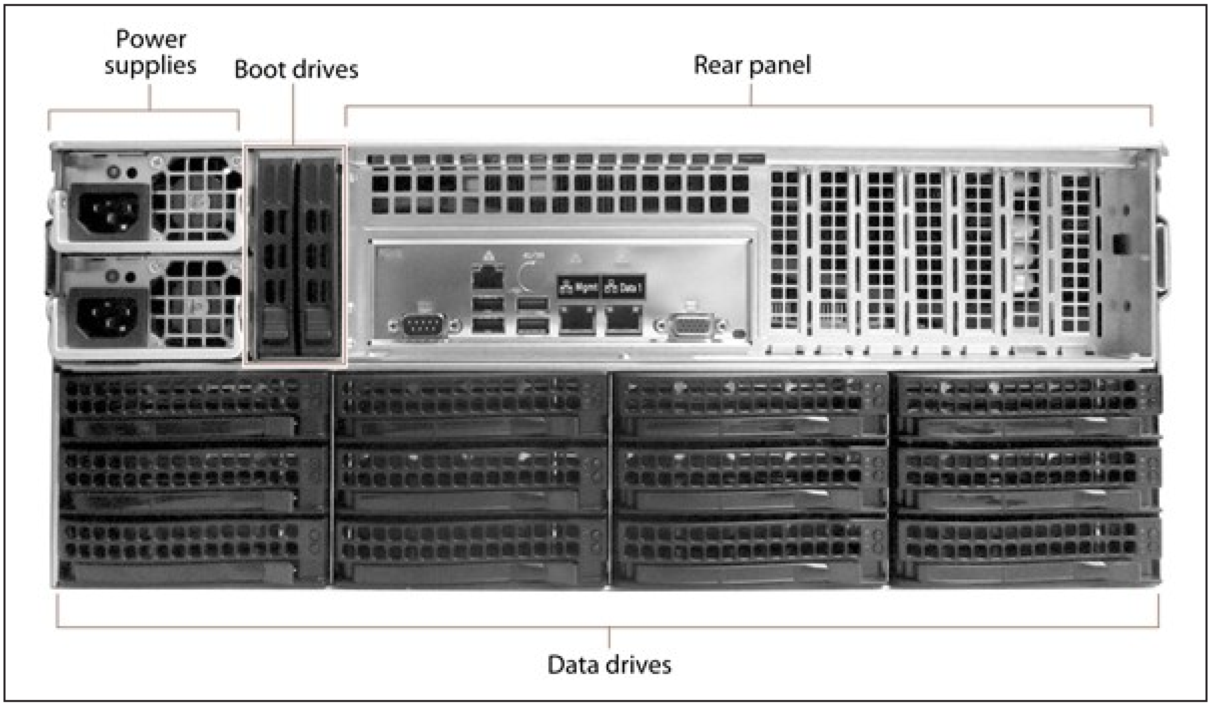


Figure 19 The rear view of the Gen1 S Series BlackPearl 4U master node.

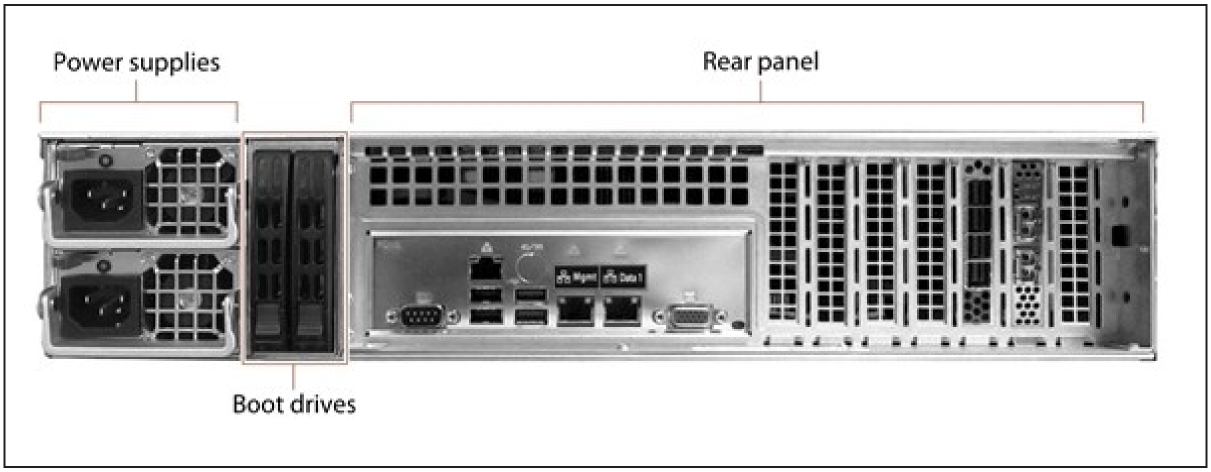


Figure 20 The rear view of the Gen1 V Series BlackPearl 2U master node.

Component	Description
Power supplies	The standard BlackPearl Object Gateway configuration includes two power supplies to provide N+1 redundancy and fail-over protection. • Each power supply has its own AC power connector. • Each power supply has a single LED that lights to indicate when the power is on and functioning normally.
Rear panel	The rear panel of the Gen1 S Series BlackPearl Object Gateway allows for Ethernet, Fibre Channel, SAS, USB, and other connections. See Rear Panel on the next page for a detailed description.
Boot drives	The boot drives provide storage for the operating system and BlackPearl user interface. The boot drives in the BlackPearl Object Gateway are hot swappable which allows for uninterrupted operation during replacement.
Data drives (BlackPearl 4U master node only)	The base Gen1 S Series BlackPearl 4U master node includes one high-performance solid-state drive, and five spinning-disk drives mounted on individual drive sleds in the rear of the chassis. Additional drives are installed in the front of the chassis. The drive sleds slide into bays in the BlackPearl chassis and lock in place. The front of each drive sled has a handle for removing the sled from the chassis and a latch for locking the drive sled in place. **Note:** The Gen1 S Series BlackPearl 2U master node does not have data drives in the rear of the chassis.
Empty drive sleds (BlackPearl 4U master node only)	Empty drive sleds are installed in the unused drive bays to prevent contaminants from entering the enclosure and to maintain proper air flow.

Rear Panel

Figure 21 shows the components on the rear panel of the BlackPearl 4U and 2U Gen1 S Series chassis.

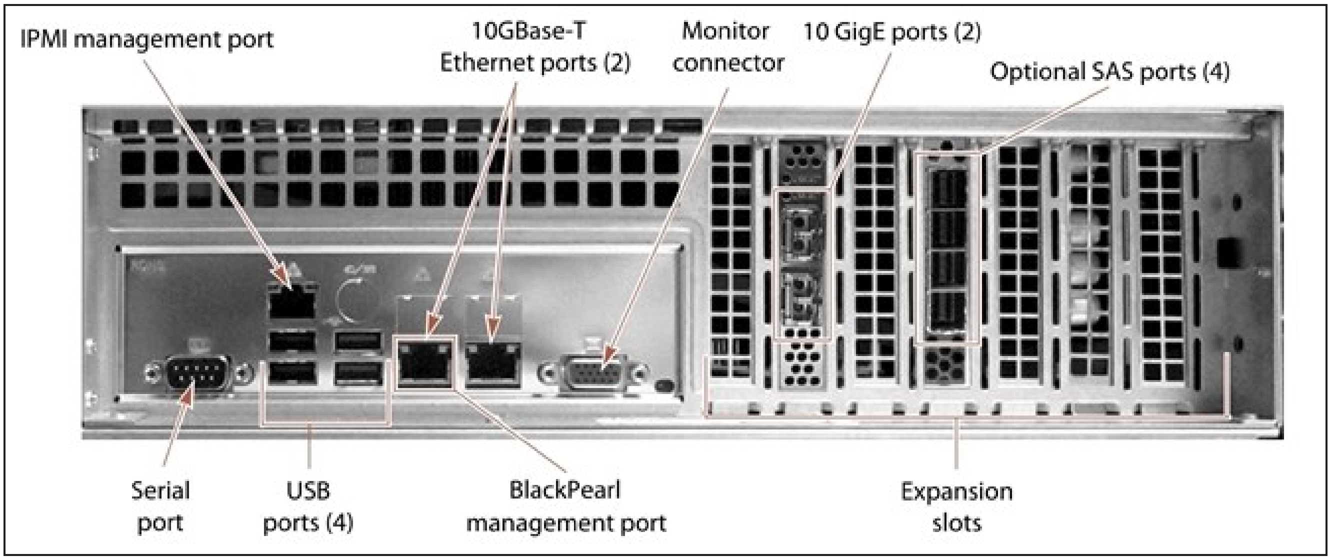


Figure 21 The Gen1 S Series BlackPearl rear panel components.

Component	Description
IPMI management port	See IPMI Configuration on page 434 for information on using IPMI management.
10GBase-T Ethernet ports	The Gen1 S Series BlackPearl master node includes two 10GBase-T ports. One of the 10GBase-T ports can be used for network connectivity on a 10GBase-T network. The left port of the two 10GBase-T ports is dedicated as the BlackPearl management port and cannot be used for data transfer. **Notes:** • The 10GBase-T ports auto-negotiate down to 1000Base-T. • Spectra Logic recommends using 40 GigE ports or the 10 GigE ports for data transfer to ensure maximum performance.
Monitor connector	If necessary, you can connect a monitor to the SVGA connector on the BlackPearl master node for troubleshooting purposes. Only connect a monitor for initial configuration of the BlackPearl management port, or as directed by Spectra Logic Technical Support.

Component	Description
10 GigE ports	The two 10 Gigabit Ethernet (10 GigE) ports can be used for network connectivity on a 10 GigE network. A Gateway can contain different types of network interface cards, but can only use one card at a time. **Note:** Unless your BlackPearl Object Gateway includes a 40 GigE card or a 10GBase-T card, Spectra Logic recommends using the 10 GigE ports for data transfer to ensure maximum performance.
Expansion slots and optional interface cards	The expansion slots accommodate optional interface cards to provide additional connectivity. • An optional 40 GigE or 10GBase-T Ethernet network interface card can be used to provide a high-speed data connection between hosts and the Gen1 Series S BlackPearl Object Gateway. Ports of the same type can be aggregated for better performance. • Optional two-port SAS cards each provide connectivity to SAS drives in a Spectra Logic tape library, or provides connectivity for up to one 44-bay expansion nodes, or up to two 77-bay, 96-bay, or 107-bay expansion nodes. • Optional four-port SAS cards each provide connectivity to SAS drives in a Spectra Logic tape library, or provides connectivity for up to two 44-bay expansion nodes, or up to four 77-bay, 96-bay, or 107-bay expansion nodes. • Optional two- or four-port Fibre Channel cards provide connectivity to Fibre Channel tape drives in a Spectra Logic or supported tape library. Each port connects to one drive.
BlackPearl management port	The BlackPearl management port is used to connect to a browser-based user interface to configure, manage, and monitor the Gen1 S Series BlackPearl Object Gateway. The BlackPearl management port cannot be used for data transfer.
USB ports	If necessary, you can use these ports to connect a USB drive, or USB keyboard to the chassis for troubleshooting purposes. Only connect a USB drive or keyboard as directed by Spectra Logic Technical Support.
Serial port	The serial port is only used in a HotPair configuration.

44-Bay Expansion Node

Front View

Figure 22 shows the major components on the front of the 44-bay expansion node.

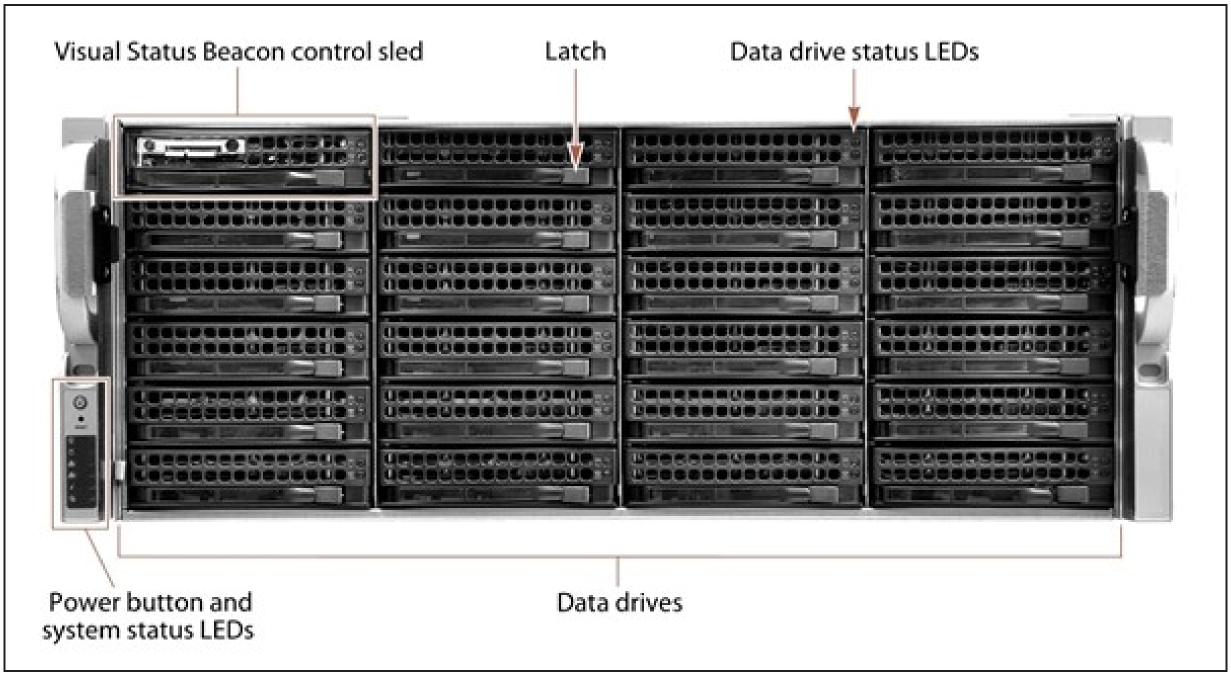

Visual Status Beacon control sled
Latch
Data drive status LEDs
Power button and system status LEDs
Data drives

Figure 22 The front view of the 44-bay expansion node (front bezel removed).

Component	Description
Visual Status Beacon control sled	If the expansion node uses an active bezel, the drive sled in the upper left corner of the front of the expansion node provides control for the Visual Status Beacon. A disk drive cannot be installed in this position.
Power button	The power button powers on the AC power for the 44-bay expansion node. Use the user interface, not the power button, to power down the BlackPearl Object Gateway, including the expansion node.
System status LEDs	The status LEDs indicate power status, disk and network activity, as well as hardware faults. See Monitor the Gateway Hardware on page 246 for more information.
Data drives	The front of the 44-bay expansion node supports up to 23 enterprise disk drives, mounted on individual drive sleds in the front of the chassis. The drive sleds slide into bays in the front of the enclosure and lock in place. The front of each drive sled has a handle for removing the sled from the chassis and a latch for locking the drive sled in place.

Component	Description
Data drive status LEDs	Two LEDs on each drive sled indicate the status of the drive. One LED is for drive status while the other shows drive activity.
Empty drive sleds	When fewer than the maximum number of drives are installed, empty drive sleds are installed in the unused drive bays to prevent contaminants from entering the enclosure and to maintain proper air flow.

Rear View

Figure 23 shows the major components on the rear of the 44-bay expansion node.

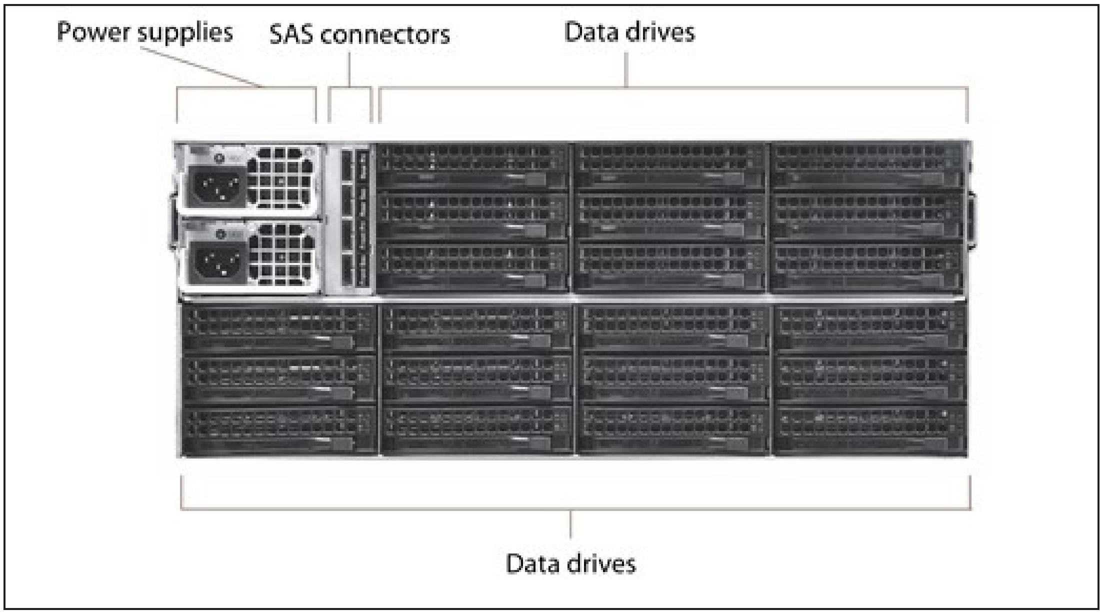


Figure 23 The rear view of the 44-bay expansion node.

Component	Description
Power supplies	The 44-bay expansion node includes two power supplies to provide N+1 redundancy and fail-over protection. • Each power supply has its own AC power connector. • Each power supply has a single LED that lights to indicate when the power is on and functioning normally.
SAS connectors	The rear panel of the 44-bay expansion node has four SAS ports used to connect an expansion node to a master node. Two ports are for primary connections and two ports are for secondary connections. Labels next to each port identify if the port is a primary or secondary connection.
Data drives	Up to 21 data drives can be installed in the rear of the expansion node.
Empty drive sleds	When fewer than the maximum number of drives are installed, empty drive sleds are installed in the unused drive bays to prevent contaminants from entering the enclosure and to maintain proper air flow.

96-Bay Expansion Node

Front View

Figure 24 shows the major components on the front of the 96-bay expansion node. There are no components or status indicators on the front of the 96-bay expansion node.

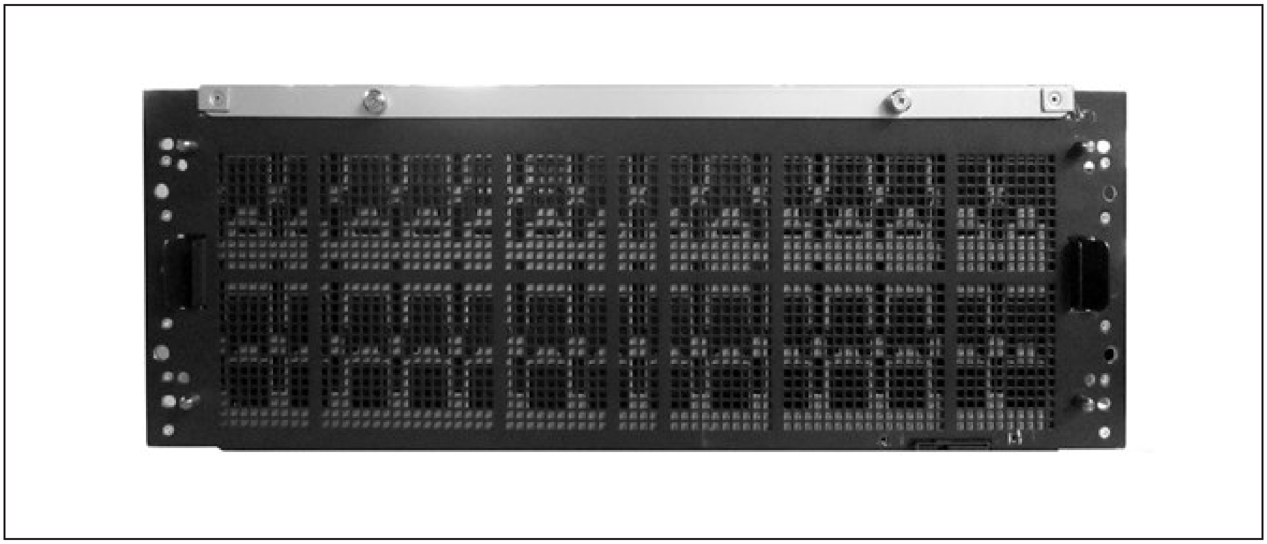


Figure 24 The front view of the 96-bay expansion node (front bezel removed).

Internal Components

The following table describes the internal field replaceable components.

Internal Component	Description
Data drives	The 96-bay expansion node supports up to 96 enterprise disk drives, mounted on individual drive sleds in the chassis. The drive sleds slide into bays in the top of the enclosure and lock in place.

Rear View

Figure 25 shows the major components on the rear of the 96-bay expansion node.

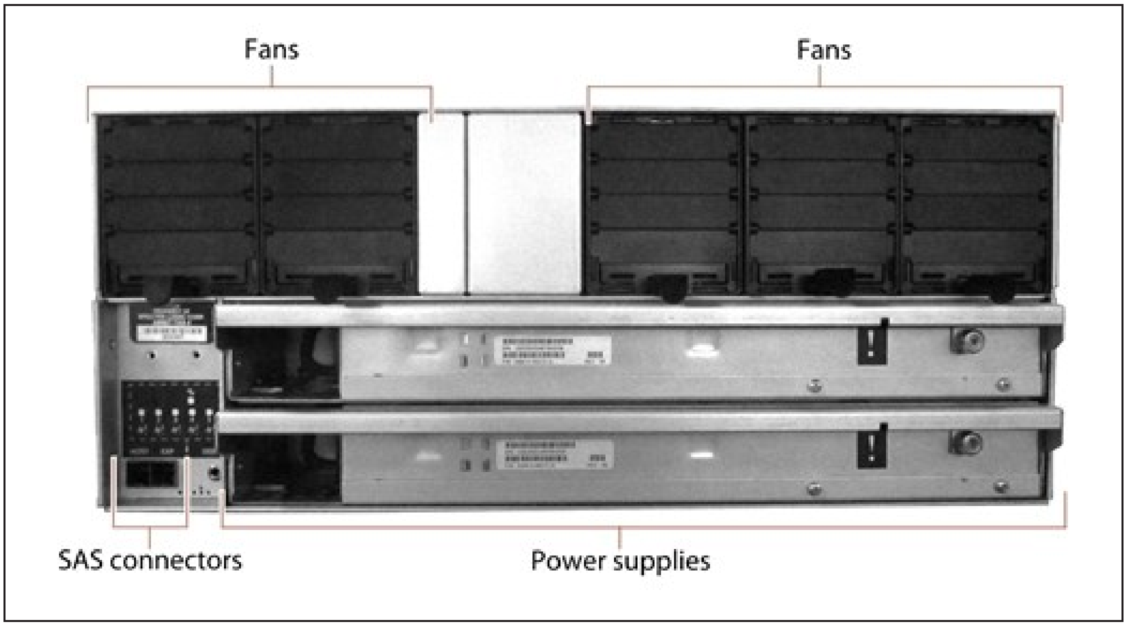


Figure 25 The rear view of the 96-bay expansion node.

Component	Description
Fans	Five hot-swappable fans provide the cooling for the 96-bay expansion node.
Power supplies	The 96-bay expansion node includes two power supplies to provide N+1 redundancy and fail-over protection. • Each power supply has its own AC power connector. • Each power supply has a single LED that lights to indicate when the power is on and functioning normally.
SAS connectors	The rear panel of the 96-bay expansion node has two SAS ports used to connect an expansion node to BlackPearl master node.

CHAPTER 2 - CONFIGURING INITIAL SETTINGS

This chapter describes the initial setup of the Spectra BlackPearl Object Gateway, necessary for operation in your environment.

Before You Begin

If your BlackPearl Object Gateway was installed by Spectra Logic Professional Services the steps in this section are complete. They are provided here for reference. See Next Steps on page 87 to begin using your BlackPearl Object Gateway.

Rackmount the Chassis

If desired, rackmount the chassis. Use the appropriate resource below:

- For a Gen3 H series or F Series, contact Spectra Logic Technical Support for instructions.
- For a Gen2 X, S, or V Series see the *BlackPearl Quick Start Guide*.
- For a Gen1 P, S, or V Series, see the *Spectra BlackPearl Rackmount Installation Guide*.

Install Drives

After you rackmount the chassis, you may need to install the drives that shipped with your BlackPearl Object Gateway. Use one of the sections below to install the drives.

- Install a Drive in a Gen3 H Series Chassis on page 273
- Install a Drive in a Gen2 S Series Chassis on page 280.
- Install a Drive in a Gen2 V Series Chassis on page 281
- Install a Drive in a Gen2 X Series Chassis on page 282

Connect Ethernet Cables

Before proceeding with the below sections, you must connect Ethernet cables to the management and data ports on the BlackPearl Object Gateway rear panel. See one of the following for the location of the Ethernet ports on the rear of the master node:

- For a Gen3 F Series see Rear Panel on page 35.
- For a Gen3 H Series see Rear Panel on page 40.
- For a Gen2 X Series see Rear View on page 44.
- For a Gen2 S or V Series see Rear Panel on page 51.
- For a Gen1 P, S, or V Series, see Rear Panel on page 60.

POWER ON THE GATEWAY

Use the instructions in this section to power on a BlackPearl Object Gateway, and optionally, a 44-bay, 77-bay, 96-bay, or 107-bay expansion node. During the power-on sequence, the BlackPearl Object Gateway initializes all of its installed components and starts the BlackPearl web server.

1. If your BlackPearl configuration includes one or more expansion nodes, power on the expansion nodes first. If you do not have any expansion nodes, skip to Step 2 on page 70.

- To power on a 77-bay, 96-bay, or 107-bay expansion node, connect power cables to the power supplies on the rear of the expansion node chassis (see Figure 16 on page 55 and Figure 25 on page 66), then plug the power cables into power outlets near the chassis. The expansion node immediately powers on. Wait approximately four minutes while the expansion node initializes before powering on the BlackPearl master node.
- To power on a 44-bay expansion node, remove the front bezel and then gently press the power button on the front panel. Wait approximately four minutes while the expansion node initializes before powering on the BlackPearl master node.

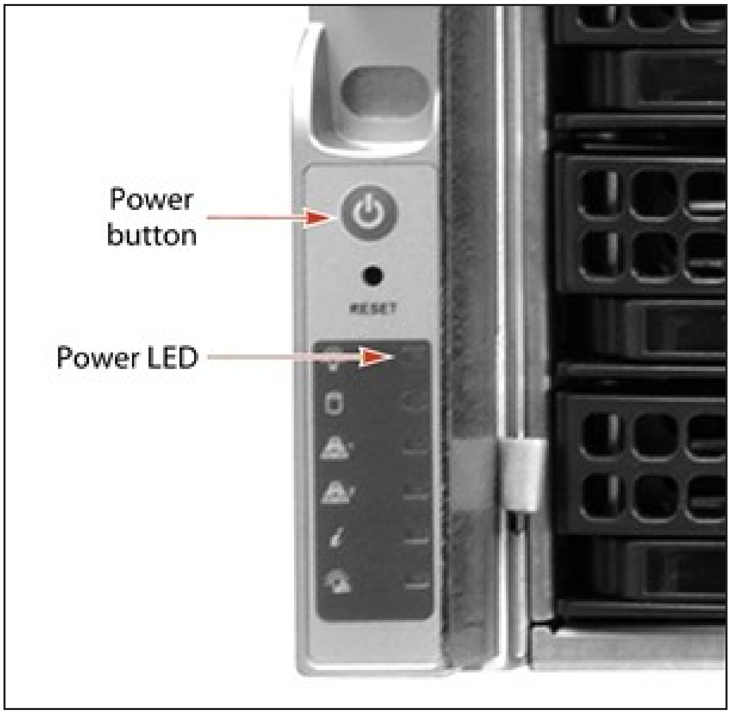


Figure 26 Press the power button (Gen 1 shown).

2. To power on a BlackPearl master node, connect power cables to the power supplies on the rear of the master node chassis. See one of the following for the location of the power supply connectors on the rear of the master node:
   - For a Gen3 F Series see Rear Panel on page 35.
   - For a Gen3 H Series see Rear Panel on page 40.
   - For a Gen2 X Series see Rear View on page 44.
   - For a Gen2 S or V Series see Rear Panel on page 51.
   - For a Gen1 P, S, or V Series, see Rear Panel on page 60.
3. Plug the power cables into power outlets near the chassis. Wait while the BlackPearl Object Gateway completes its power-on sequence, which takes approximately 5 to 10 minutes, depending on the configuration.

Note: Do not use the front panel power button to power down the Gateway. See Reboot or Shut Down a BlackPearl Object Gateway on page 267.

Configure the BlackPearl Management Port

IMPORTANT You must connect Ethernet cables as described in Connect Ethernet Cables on page 68 before either proceeding with the steps below.

The default IP address for the BlackPearl management port is set to **10.0.0.2**, with a netmask of **255.255.255.0**.

- If you do not want to change the default management port IP address, skip to Log Into the BlackPearl User Interface on page 74.
- If your network is already using this IP address, or you want to configure a different IP address for the management port:
  - Use the BlackPearl console to configure the management port IP address. See the instructions below.
  - Use the 10.0.0.2 IP address to log into the BlackPearl user interface and then change the IP address. Skip to Log Into the BlackPearl User Interface on page 74, then use the instructions in Configure Network Connections on page 107

Note: If you cannot use one of the methods above to change the Management port IP address, see Resolve a BlackPearl Management Port IP Address Conflict on page 430 for an alternate method.

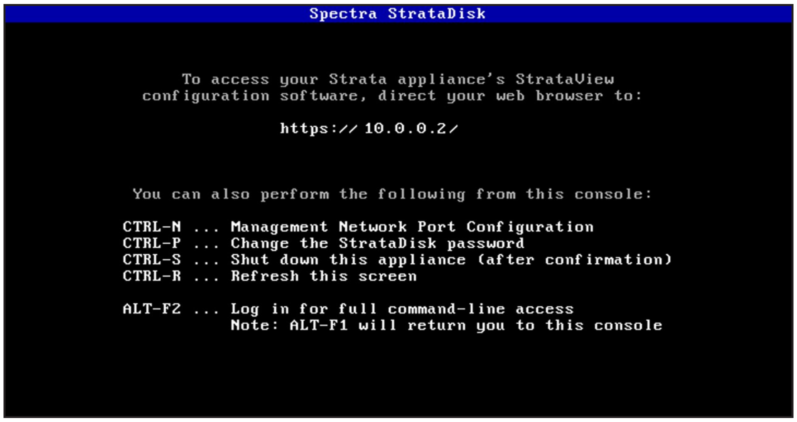
1. Connect a monitor and USB keyboard or KVM switch to the rear of the BlackPearl Object Gateway.

Note: The Gen2 X Series chassis has a mini DisplayPort connection for the monitor. The other chassis have a VGA connection.

See one of the following for the location of the monitor and USB ports on the rear of the master node:

- For a Gen3 F Series see Rear Panel on page 35.
- For a Gen3 H Series see Rear Panel on page 40.
- For a Gen2 X Series see Rear View on page 44.
- For a Gen2 S or V Series see Rear Panel on page 51.
- For a Gen1 P, S, or V Series, see Rear Panel on page 60.

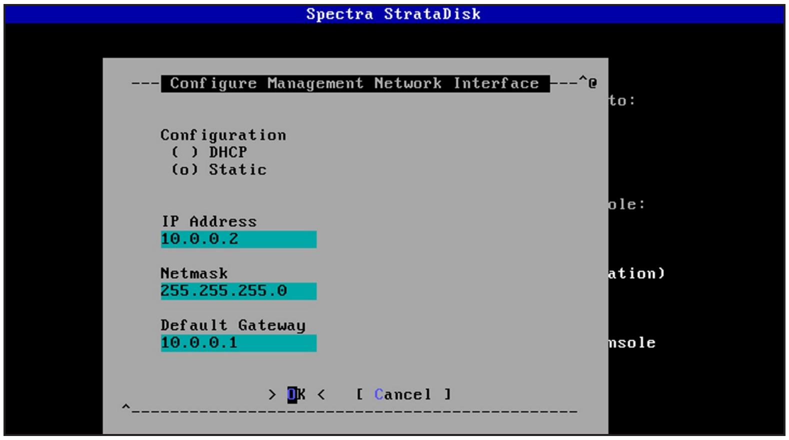
The Console screen displays.



```
                    Spectra StrataDisk

         To access your Strata appliance's StrataView
      configuration software, direct your web browser to:

                   https:// 10.0.0.2/


      You can also perform the following from this console:

     CTRL-N ... Management Network Port Configuration
     CTRL-P ... Change the StrataDisk password
     CTRL-S ... Shut down this appliance (after confirmation)
     CTRL-R ... Refresh this screen

     ALT-F2 ... Log in for full command-line access
                Note: ALT-F1 will return you to this console
```

Figure 27 The Console screen.

2. Press **CTRL-N**. The Configure Management Network Interface screen displays.



```
                    Spectra StrataDisk

  ---Configure Management Network Interface---^@
                                                   to:

       Configuration
        ( ) DHCP
        (o) Static

                                                   ole:
       IP Address
       10.0.0.2

       Netmask                                     ation)
       255.255.255.0

       Default Gateway                             nsole
       10.0.0.1

                   > OK <    [ Cancel ]
  ^-----------------------------------------------
```

Figure 28 The Configure Management Network Interface screen.

3. Select either **DHCP** or **Static** as the addressing method.

   If you select static addressing, enter the following information:

   - **IP Address**—Enter a valid IPv4 address.
   - **Netmask**—Enter the subnet mask.
   - **Default Gateway**—Enter the default network gateway.

4. Select **OK**. The console screen displays showing the new IP address.

Note: If the new IP address does not display, you may need to manually refresh the console screen by pressing **CTRL-R**.

5. You are now able to connect to the BlackPearl user interface with the IP address displayed in Step 4.

6. Disconnect the monitor and USB keyboard from the BlackPearl Object Gateway.

Log Into the BlackPearl User Interface

Use the following instructions to log into the BlackPearl user interface.

Notes:
- There is no limit to the number of users who can log in to the user interface. Spectra Logic recommends only one person use the interface at a time to avoid conflicting operations.
- To log into the BlackPearl user interface on a system that is configured to use Multi-Factor Authentication, see Multi-Factor Authentication on page 185.

1. Using a standard web browser, enter the IP address for the BlackPearl management port configured in Configure the BlackPearl Management Port on page 71.

Note: The BlackPearl user interface uses a secure connection.

2. If necessary, resolve the security certificate warning for the BlackPearl user interface.

   The BlackPearl Object Gateway ships with non-signed SSL certificates for both the data and management ports. When using the shipped certificates, you must pass a security check every time you attempt to access the management port to view the BlackPearl user interface, or when you attempt to transfer data using the data port.

Notes:
- The absence of the certificate does not affect functionality.
- If desired, you can install signed, trusted SSL certificates for your data and management ports so that you no longer need to pass the security check when accessing these ports. See Configure Certificates on page 92.

3. Enter the primary administrator username and password. The fields are case sensitive.
   - The default username is **Administrator**.
   - The default password is the serial number of the master node. Find the serial number on the sticker positioned on the top of the chassis, on the right-hand side, toward the front. The serial number is indicated by the letters "SN" on the sticker.

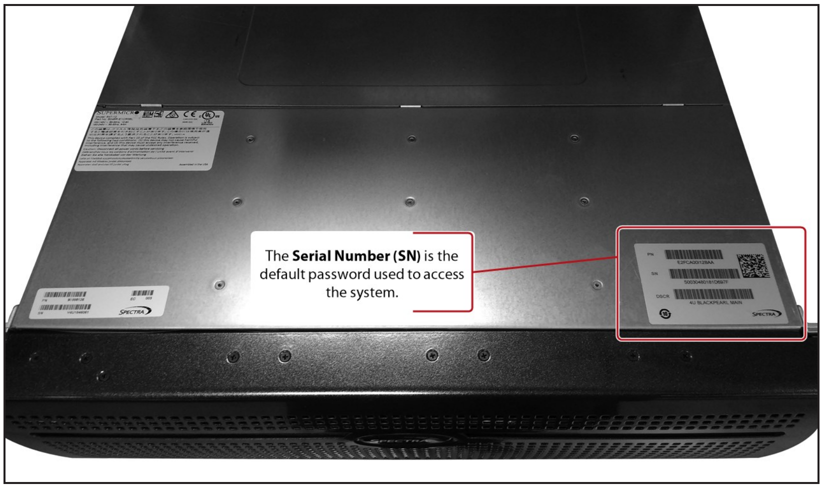
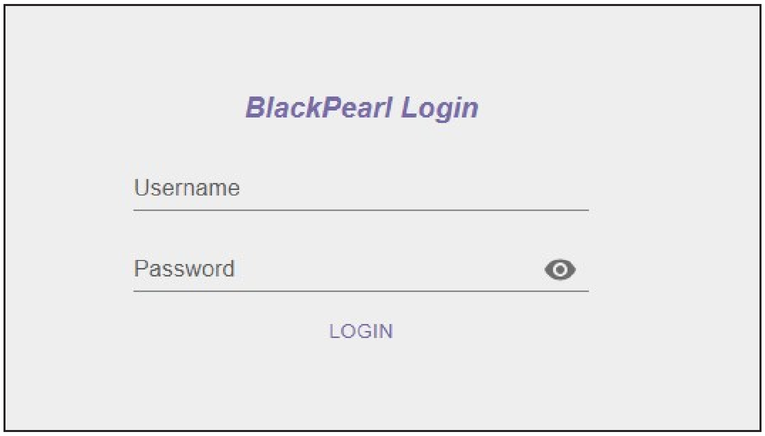

The **Serial Number (SN)** is the default password used to access the system.

Figure 29 The BlackPearl serial number sticker.



BlackPearl Login

Username

Password

LOGIN

Figure 30 The BlackPearl Login screen.

4. Click **Login** to log in.

Note: Spectra Logic recommends that you change the default password for the primary administrator (see Configure Users on page 203).

CONFIGURE THE DATA CONNECTION

This section describes using the BlackPearl user interface to configure one or more data connections for the BlackPearl Object Gateway. The configuration steps are the same for all standard and optional port types.

Notes:

- You can configure link aggregation for better performance.
- While different types of Ethernet network interface cards can be installed in the same BlackPearl Object Gateway, only one type port can be used in each link aggregation configuration.
- You can only use the BlackPearl management port to access the BlackPearl user interface. You cannot use this port for data transfer.

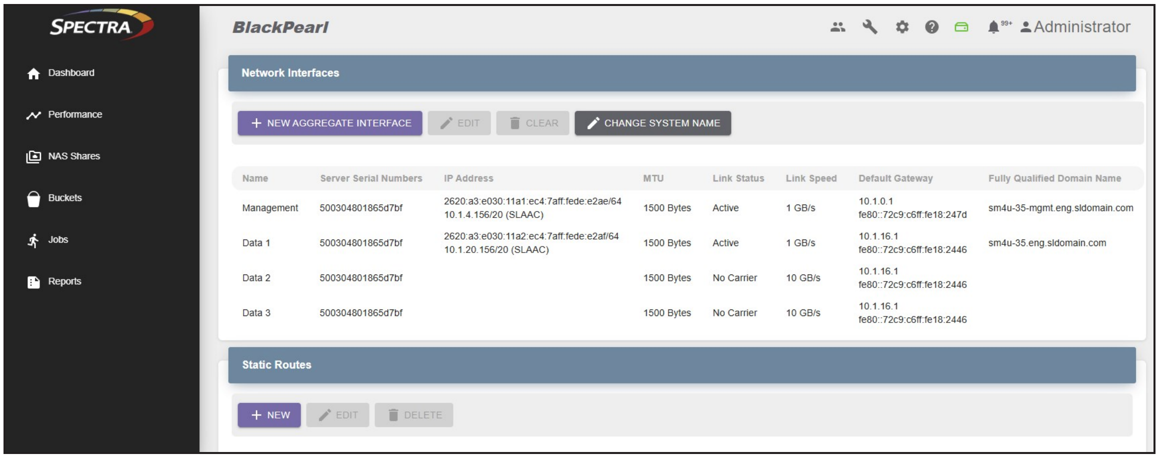
Configure an Aggregate Port Data Connection

Link aggregation uses multiple Ethernet ports, configured with a single MAC address, to improve data transfer speeds. See Networking Best Practices on page 89 for more information.

IMPORTANT The network switch connected to the BlackPearl Object Gateway must be configured for Level 3 LACP in order to support an aggregate data connection on the BlackPearl Object Gateway.

Use the following instructions to configure an aggregate port data connection.

1. Use the toolbar in the upper-right to select **Configuration (wrench) > Network**.

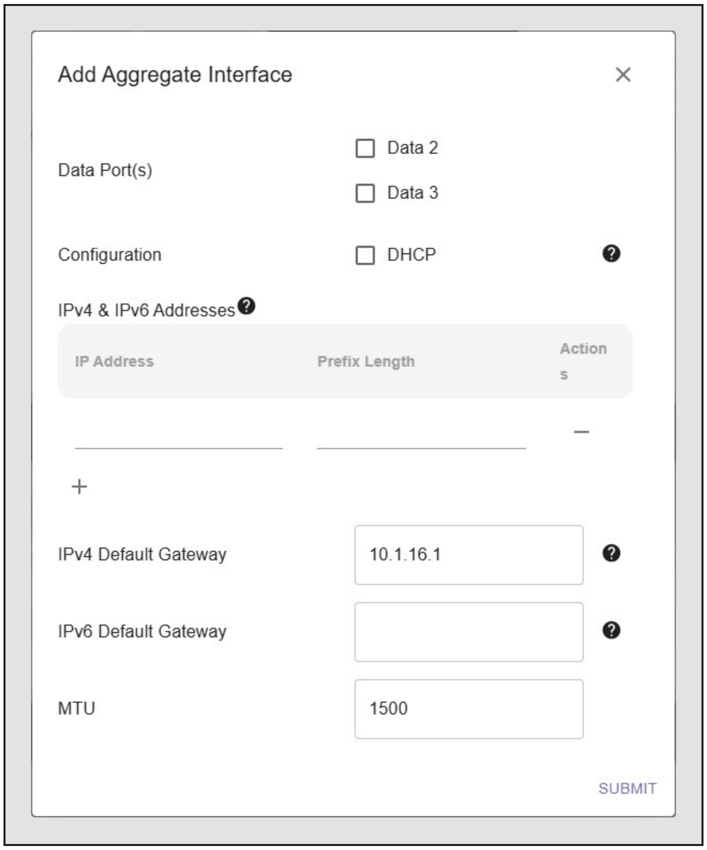


Name	Server Serial Numbers	IP Address	MTU	Link Status	Link Speed	Default Gateway	Fully Qualified Domain Name
Management	500304801865d7bf	2620:a3:e030:11a1:ec4:7aff:fede:e2ae/64 10.1.4.156/20 (SLAAC)	1500 Bytes	Active	1 GB/s	10.1.0.1 fe80::72c9:c6ff:fe18:247d	sm4u-35-mgmt.eng.sldomain.com
Data 1	500304801865d7bf	2620:a3:e030:11a2:ec4:7aff:fede:e2af/64 10.1.20.156/20 (SLAAC)	1500 Bytes	Active	1 GB/s	10.1.16.1 fe80::72c9:c6ff:fe18:2446	sm4u-35.eng.sldomain.com
Data 2	500304801865d7bf		1500 Bytes	No Carrier	10 GB/s	10.1.16.1 fe80::72c9:c6ff:fe18:2446	
Data 3	500304801865d7bf		1500 Bytes	No Carrier	10 GB/s	10.1.16.1 fe80::72c9:c6ff:fe18:2446	

Figure 31 The Network screen.

2. Click **New Aggregate Interface**. The New Aggregate Interface dialog box displays.

Note: Depending on your hardware configuration, the New Aggregate Interface dialog box may look different than what is shown below.



Add Aggregate Interface ×

Data Port(s) □ Data 2 □ Data 3

Configuration □ DHCP

IPv4 & IPv6 Addresses

IP Address	Prefix Length	Actions
		–

+

IPv4 Default Gateway: 10.1.16.1

IPv6 Default Gateway:

MTU: 1500

SUBMIT

Figure 32 The Add Aggregate Interface dialog box.

3. Select the **Data Port(s)** you want to configure into an aggregate data interface.

Note: Only one type of port can be used in an aggregation. For example, you cannot use both 10 GigE and 40 GigE ports in the same link aggregation.

4. Select the **DHCP** checkbox to configure the Gateway to automatically acquire an IPv4 address using DHCP. This setting does not apply to IPv6.

5. To configure a static IP address enter the following information:

   - **IP Address**—Enter a valid IPv4 or IPv6 address.
   - **Prefix Length**—Enter the subnet mask.

Notes:

- You cannot enter an IPv4 address if you selected DHCP in Step 4.
- If desired, you can enter multiple IP and prefix lengths assigned to the data port. Use the **+** button to configure additional IP and Netmask addresses. You can configure a maximum of 16 aliases.

6. If applicable, enter the **IPv4 Default Gateway**.

Notes:
- If you selected DHCP in Step 4, this option is unavailable.
- The Gateway entered for the last configured IPv4 connection sets the default Gateway for the BlackPearl Object Gateway.

7. If applicable, enter the **IPv6 Default Gateway**.

Notes:
- The gateway entered for the last configured IPv6 connection sets the default gateway for the BlackPearl Object Gateway.
- The IPv6 Gateway does not need to be configured when the BlackPearl Object Gateway is connected to a SLACC network.

8. Change the **MTU** (Maximum Transmission Unit) value, if desired. If you set the MTU value to something other than 1500, ensure that your switch configuration supports larger MTU settings, as well as all the hosts on the network.
9. Click **Submit**.

Configure a Single Port Data Connection

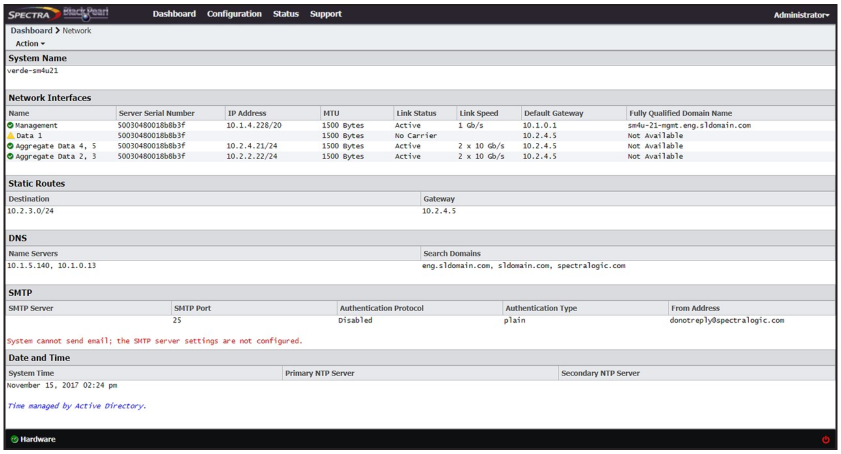
Use the following instructions to configure a single port data connection.

To configure a single data port connection, you must access the legacy user interface used in BlackPearl OS 5.8.x and earlier. Functionality to configure a single port data connection will be added to a later version of the BlackPearl OS.

1. Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with "/legacy". For example:

   https://*ipaddress*/legacy

2. Use the toolbar in the upper-right to select **Configuration > Network**. The Network screen displays with information about the network connections of the Gateway.



System Name

verde-sm4u21

Network Interfaces

Name	Server Serial Number	IP Address	MTU	Link Status	Link Speed	Default Gateway	Fully Qualified Domain Name
✓ Management	50030480018b8b3f	10.1.4.228/20	1500 Bytes	Active	1 Gb/s	10.1.0.1	sm4u-21-mgmt.eng.sldomain.com
⚠ Data 1	50030480018b8b3f		1500 Bytes	No Carrier		10.2.4.5	Not Available
✓ Aggregate Data 4, 5	50030480018b8b3f	10.2.4.21/24	1500 Bytes	Active	2 x 10 Gb/s	10.2.4.5	Not Available
✓ Aggregate Data 2, 3	50030480018b8b3f	10.2.2.22/24	1500 Bytes	Active	2 x 10 Gb/s	10.2.4.5	Not Available

Static Routes

Destination	Gateway
10.2.3.0/24	10.2.4.5

DNS

Name Servers	Search Domains
10.1.5.140, 10.1.0.13	eng.sldomain.com, sldomain.com, spectralogic.com

SMTP

SMTP Server	SMTP Port	Authentication Protocol	Authentication Type	From Address
	25	Disabled	plain	donotreply@spectralogic.com

System cannot send email; the SMTP server settings are not configured.

Date and Time

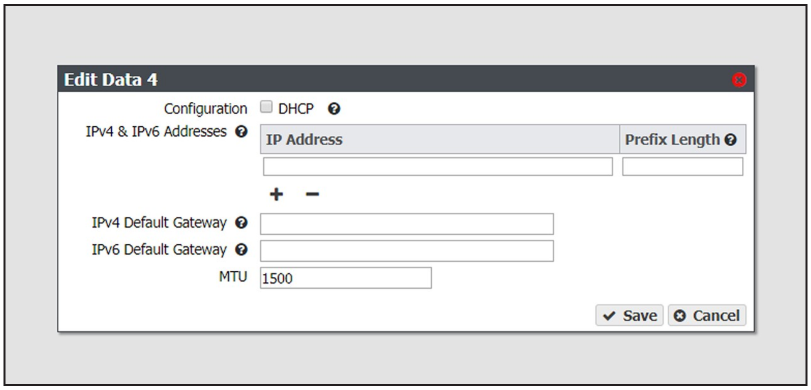
System Time	Primary NTP Server	Secondary NTP Server
November 15, 2017 02:24 pm		

Time managed by Active Directory.

Figure 33 The Network screen.

3. Select the Data # row and select **Action > Edit** from the menu bar. The Edit Data # dialog box displays.

Note: Depending on your hardware configuration, the Edit Data # dialog box may look different than what is shown below.



Edit Data 4

Configuration ☐ DHCP

IPv4 & IPv6 Addresses

IP Address	Prefix Length

IPv4 Default Gateway

IPv6 Default Gateway

MTU 1500

Figure 34 The Edit Data # dialog box.

4. Select the **DHCP** checkbox to configure the Gateway to automatically acquire an IPv4 address using DHCP. This setting does not apply to IPv6.

5. To configure a static IP address, click the **+** button and enter the following information:

   - **IP Address**—Enter a valid IPv4 or IPv6 address.

   Note: You cannot enter an IPv4 address if you selected DHCP.

   - **Prefix Length**—Enter the subnet mask.

   Note: If desired, you can enter **Aliases**, multiple IP and prefix lengths assigned to the data port. Use the **+** button to configure additional IP and Netmask addresses. You can configure a maximum of 16 aliases.

6. If applicable, enter the **IPv4 Default Gateway**.

   Notes:
   - If you selected DHCP, this option is unavailable.
   - The gateway entered for the last configured IPv4 connection sets the default gateway for the BlackPearl Object Gateway.

7. If applicable, enter the **IPv6 Default Gateway**.

   Notes:
   - The gateway entered for the last configured IPv6 connection sets the default gateway for the BlackPearl Object Gateway.
   - The IPv6 Gateway does not need to be configured when the BlackPearl Object Gateway is connected to a SLACC network.

8. Change the **MTU** (Maximum Transmission Unit) value, if desired. If you set the MTU value to something other than 1500, ensure that your switch configuration supports larger MTU settings, as well as all the hosts on the network.

9. Click **Save**.

Configure a Static Route

The BlackPearl Object Gateway only supports communication with one default gateway. When configuring a BlackPearl Object Gateway with multiple data connections, each connection communicates via the gateway entered when the connection was configured. The gateway entered for the last configured connection sets the default gateway for the BlackPearl Object Gateway.

When configuring a Gateway with multiple data connections, if each data connection only communicates with its own network, a static route is not required. When an additional network or external network is only available from one, but not all, of the data connections configured on the BlackPearl Object Gateway, a static route is required in order for the Gateway to communicate to the additional network.

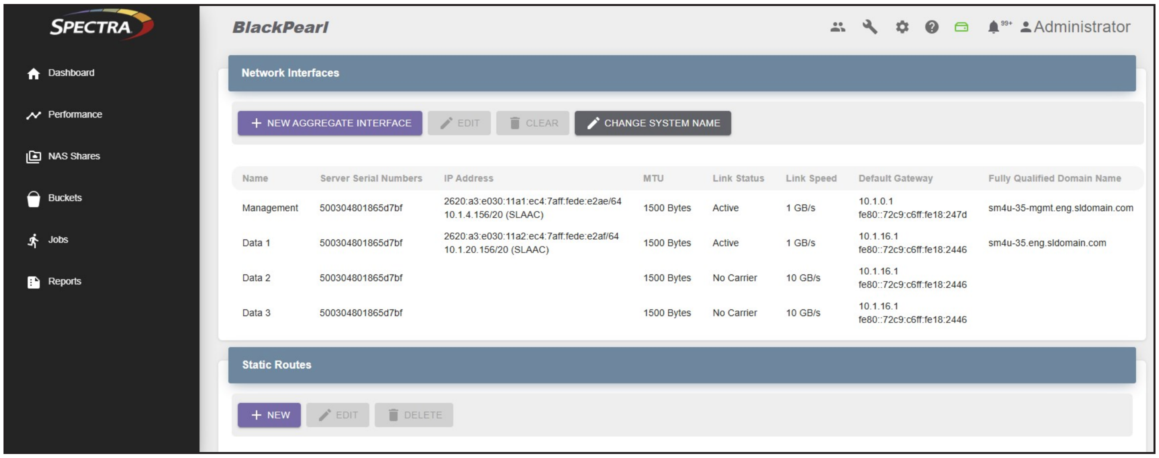
For example, if one data connection is on the 10.2.2.x network and another connection is on the 10.2.4.x network, when the 10.2.3.x network is connected externally to the 10.2.4.x network, a static route must be configured on the BlackPearl Object Gateway to route communication with the 10.2.3.x network through the data connection on the 10.2.4.x network.

After creating the static route to the isolated network, you must create additional static routes to each specific host computer on the isolated network. If the BlackPearl Object Gateway receives a request from an IP address that is not configured to a static route, then the request is sent to the default gateway. If the default gateway is not connected to the IP address for isolation reasons, the request fails.

Note: Static routes are only used with IPv4 addresses.

Use the instructions in this section to configure a static route.

1. Use the toolbar in the upper-right to select **Configuration (wrench) > Network**.



Name	Server Serial Numbers	IP Address	MTU	Link Status	Link Speed	Default Gateway	Fully Qualified Domain Name
Management	500304801865d7bf	2620:a3:e030:11a1:ec4:7aff:fede:e2ae/64 10.1.4.156/20 (SLAAC)	1500 Bytes	Active	1 GB/s	10.1.0.1 fe80::72c9:c6ff:fe18:247d	sm4u-35-mgmt.eng.sldomain.com
Data 1	500304801865d7bf	2620:a3:e030:11a2:ec4:7aff:fede:e2af/64 10.1.20.156/20 (SLAAC)	1500 Bytes	Active	1 GB/s	10.1.16.1 fe80::72c9:c6ff:fe18:2446	sm4u-35.eng.sldomain.com
Data 2	500304801865d7bf		1500 Bytes	No Carrier	10 GB/s	10.1.16.1 fe80::72c9:c6ff:fe18:2446	
Data 3	500304801865d7bf		1500 Bytes	No Carrier	10 GB/s	10.1.16.1 fe80::72c9:c6ff:fe18:2446	

Figure 35 The Network screen.

2. In the Static Routes pane, click **New**. The Add Static Route dialog box displays.

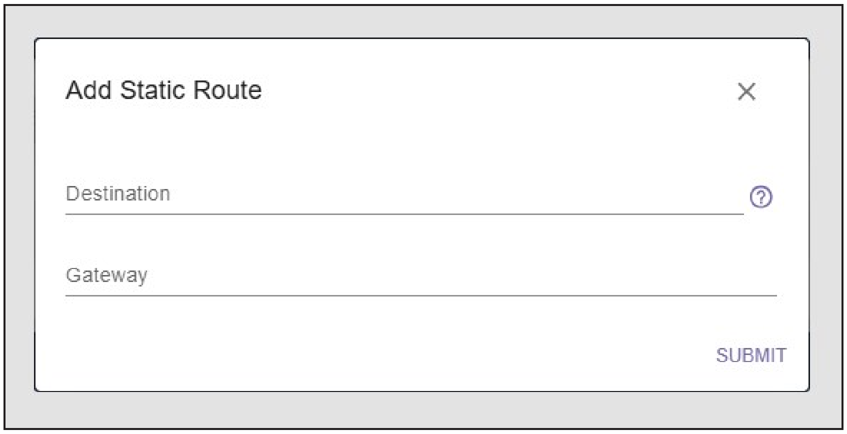

Add Static Route

Figure 36 The Add Static Route dialog box.

3. In the **Destination** field, enter either an IPv4 host address or network address that you want to access through the data connection.
4. Enter the network **Gateway** of the data connection used to communicate with the isolated network.
5. Click **Create**.
6. Repeat for **each** host computer on the isolated network.

CREATE A USER

Use the instructions in this section to create users, which act as Amazon compatible S3 users when interacting with the BlackPearl Object Gateway through a DS3 SDK (Software Development Kit) client, the DS3 API, or the Vail Application. Each user has a unique Amazon compatible S3 Access ID and Secret Key.

Note: The "Administrator" user is created automatically and assigned all permissions.

Description of User Permissions

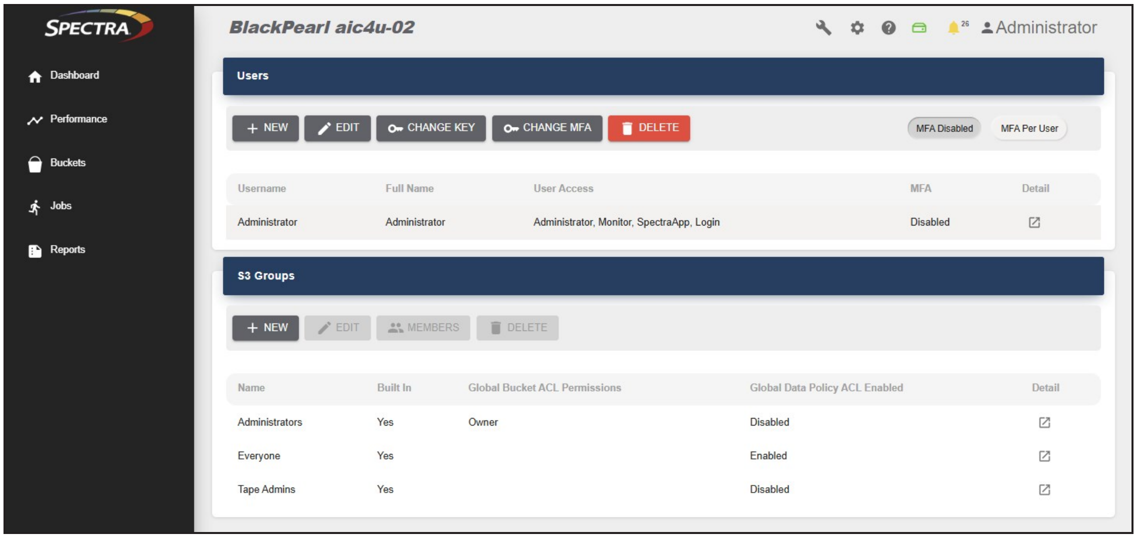
There are five different types of users permissions in the BlackPearl user interface: Administrator, monitor, login, CIFS, and SpectraApp. Use the table below for a description of the user permission types.

Permission	Description
Administrator	A user with the Administrator permission has full control over all user interface functions. A primary Administrator account is created by default using the name "Administrator", and is automatically assigned all permissions. The default password is the serial number of the master node. Find the serial number on the sticker positioned on the top of the chassis, on the right-hand side, toward the front (see Figure 29 on page 74). **Note:** Spectra Logic recommends changing the password for the primary Administrator account. See Configure Users on page 203.
Monitor	A user with Monitor permission can access the BlackPearl user interface but cannot use any functions of the user interface other than exporting tapes, creating a manual snapshot of a volume, or marking a volume read only. This account is useful if you need to view the status jobs or any other aspect of the user interface, but do not have access to an account with administrator permission. **Note:** A user with the monitor permission can open any menu or function and attempt to edit settings, but these changes are ignored when the user attempts to save the changes.
Login	A user with Login permission is able to log into the BlackPearl user interface. **Notes:** • Administrator and Monitor users must also have Login permission in order to log in to the BlackPearl user interface. • The SpectraApp user requires Login permission in order to load the embedded dashboard into an external Spectra software application.

Permission	Description
CIFS User	A user with CIFS permission is able to access CIFS shares in a Windows workgroup environment.
SpectraApp	A user with SpectraApp permission is required to load the BlackPearl embedded dashboard in to the Spectra Vail, StorCycle, or RioBroker applications. See the documentation for your Spectra software application for instructions on loading the embedded dashboard. **Notes:** • A user with Administrator permission is required to create, edit, or delete a SpectraApp user. • The SpectraApp user requires Login permission in order to load the embedded dashboard into an external Spectra software application.

Create a User

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.

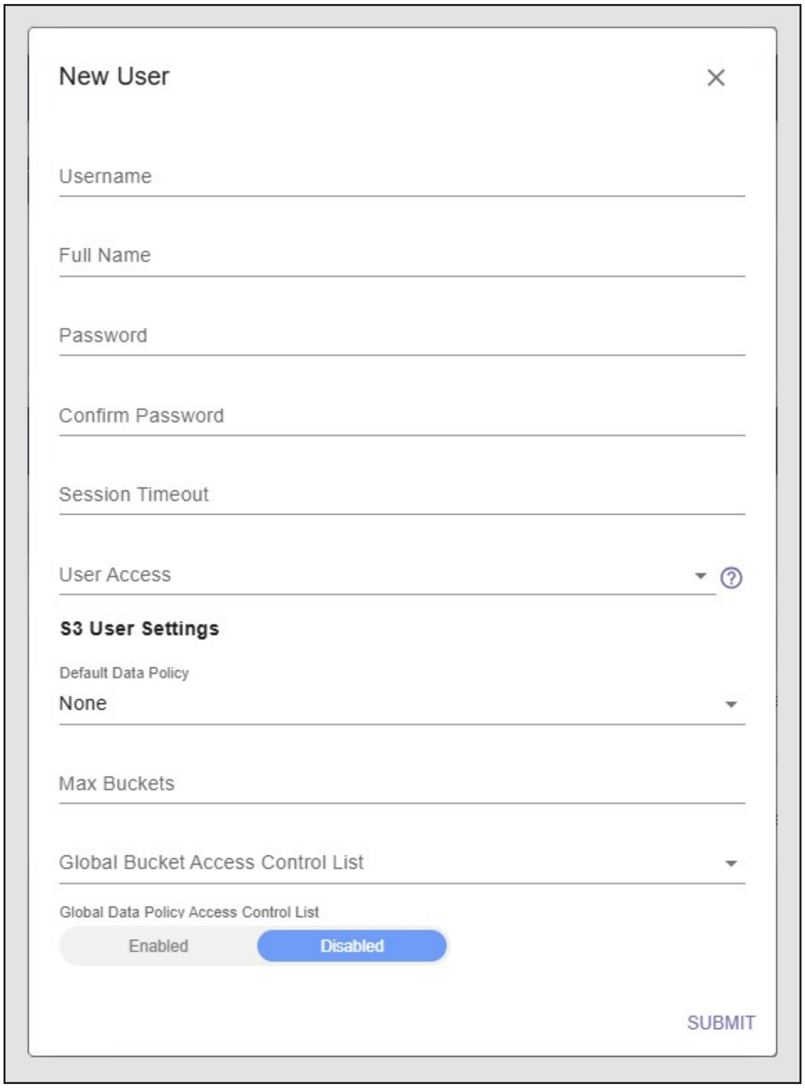


Username	Full Name	User Access	MFA	Detail
Administrator	Administrator	Administrator, Monitor, SpectraApp, Login	Disabled	

Name	Built In	Global Bucket ACL Permissions	Global Data Policy ACL Enabled	Detail
Administrators	Yes	Owner	Disabled	
Everyone	Yes		Enabled	
Tape Admins	Yes		Disabled	

Figure 37 The Users screen.

2. Click **New**. The New User dialog box displays.



Default Data Policy
None

Global Data Policy Access Control List
Disabled

Figure 38 The New User dialog box.

3. Enter the desired **Username** for the user. The Username cannot contain capital letters or spaces and is limited to 16 characters. The Username is used to identify the user in the DS3 environment.

4. Enter the user's **Full Name**.

5. Enter and confirm the desired **Password** for the user.

6. If desired, enter the value for the **Session Timeout** in minutes. This value cannot exceed 999 minutes.

7. Use the **User Access** drop-down menu to select one or more permissions for the user. See Description of User Permissions on page 82 for information on each level of user access permission.

Note: Administrator and Monitor users must also select **Login** in order to log in to the BlackPearl user interface.

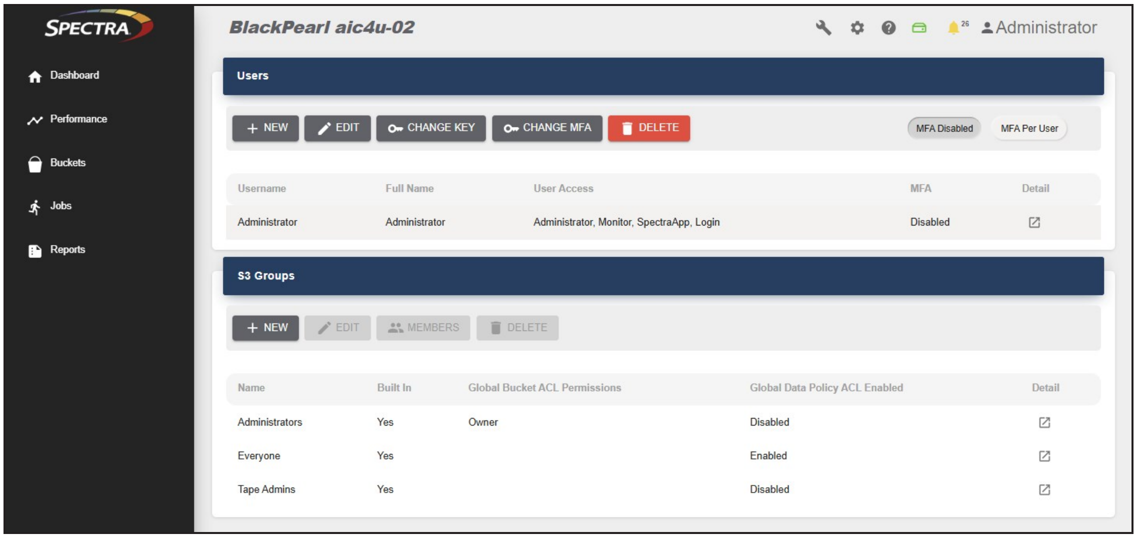
8. Use the **Default Data Policy** drop-down list to select a data policy for the user. If specified, the Gateway uses the selected data policy for all buckets created by the user, unless a different policy is specified during bucket creation.
9. Enter a value for the **Max Buckets** the user is allowed to create.
10. Use the **Global Bucket Access Control List** drop-down menu to select access options for the user. These options give or deny permission for the user being created to perform the action described in the table below, for all buckets present on the Gateway, as well as any buckets created at a future date.

Name	Description
List	The user can see the bucket and can list the objects in a bucket.
Read	The user can get objects and create GET jobs.
Write	The user can put objects and create PUT jobs.
Delete	The user can delete objects, but cannot delete the bucket.
Job	The user can modify or cancel jobs created by other users. The user can also see the details of jobs created by other users. **Note:** All users can view all jobs, but by default, only the initiator of the job can see the full details of a job.
Owner	The user receives full access to all buckets, including all permissions listed above.

11. Use the **Global Data Policy Access Control List** slider to select one of the following:
    - **Enable** - allow the user access to any data policy created on the Gateway.
    - **Disable** - the user is only able to access data policies created by the user.
12. Click **Submit** to create the new user. The Gateway generates a unique Amazon compatible S3 Access ID and Secret Key for the user.

VIEW AMAZON COMPATIBLE S3 CREDENTIALS

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.

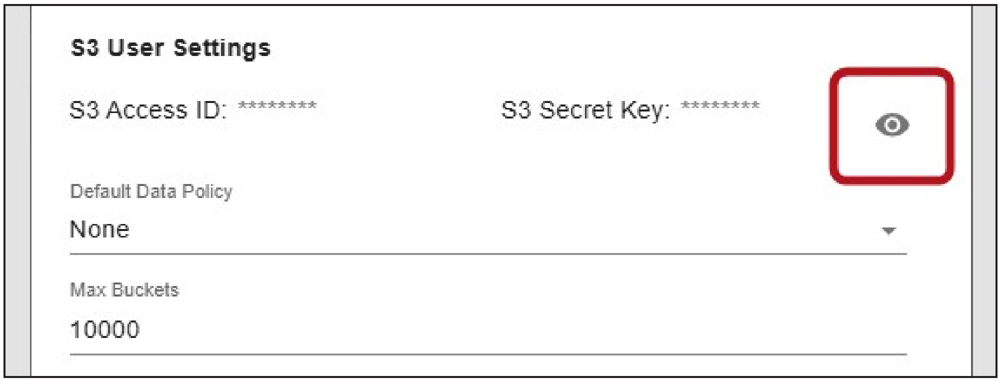


Username	Full Name	User Access	MFA	Detail
Administrator	Administrator	Administrator, Monitor, SpectraApp, Login	Disabled	↗

Name	Built In	Global Bucket ACL Permissions	Global Data Policy ACL Enabled	Detail
Administrators	Yes	Owner	Disabled	↗
Everyone	Yes		Enabled	↗
Tape Admins	Yes		Disabled	↗

Figure 39 The Users screen.

2. Select the user for which you want to view S3 credentials and click **Edit**. The Edit User dialog box displays.



S3 User Settings

S3 Access ID: *********

S3 Secret Key: *********

Default Data Policy

None

Max Buckets

10000

Figure 40 The Edit User dialog box - S3 User Settings.

3. Click the **eye icon** to display the credentials. Click the **eye icon** again to hide the credentials.

NEXT STEPS

The BlackPearl Object Gateway now has the necessary components configured to begin designing your storage architecture. Continue with one of the following:

- To configure SSL certificates see Configure Certificates on page 92.
- To configure DNS, SMTP, system time, and hostname, see Configure Network Settings on page 94.
- To configure object storage settings, see Configuring Object Storage on page 110.
- To configure NAS settings, see Configuring Network Attached Storage on page 152

CHAPTER 3 - CONFIGURING NETWORK SETTINGS

This chapter describes using the BlackPearl user interface to configure networking for the Spectra BlackPearl Object Gateway.

NETWORKING BEST PRACTICES

The basic steps for configuring the management and data ports for access to your network are simple and straight-forward. However, each network environment is unique and may require some additional troubleshooting in order to properly connect to the BlackPearl Object Gateway and utilize the Ethernet interfaces correctly.

Note: The BlackPearl management port is separate from the data ports. The management port and data ports have their own default routes.

Configuration Method

Use the BlackPearl management interface or the command line interface to configure the management and data ports. Do not attempt to access the Gateway directly and use the root console to modify interfaces. The management and command line interfaces are tightly integrated with the base operating system and configure additional features based on network changes.

Supported Network Connectivity

The following configurations are supported for the data path:

Recommended:

- A single logical connection using a network interface card. Use either one physical port, or two ports in link aggregation. For information on supported connection speeds, see Specifications on page 438.

Not Recommended:

- Single gigabit logical connection utilizing one of the on-board motherboard ports and a Category 5e Ethernet cable.

MTU Settings

The BlackPearl Object Gatewaysupports MTU values of 1500-9000. If you configure the MTU value to something other than the 1500 default value, make sure that your switch configuration and all the hosts on the network support the larger MTU settings, to avoid an impact on performance.

Link Aggregation

If link aggregation is configured for the BlackPearl Object Gateway, then network switches must support link aggregation to aggregate or “trunk” the data ports together to provide higher bandwidth to the Gateway.

Network switches must support link aggregation using LACP (Link Aggregation Control Protocol), and hash the destination IP addresses. Typically you must manually configure LACP on the switch ports.

- If you **are** using link aggregation, the switch must be configured **to use** LACP on those ports.
- If you **are not** using link aggregation, the switch must be configured **to not use** LACP on those ports.

Network switches use different methods of routing traffic from hosts to NAS servers. For example, some switches route traffic based on both the MAC address and the IP address.

- Using DHCP link aggregation, the BlackPearl Object Gateway presents only one MAC address and one IP address.
- Using static link aggregation, the BlackPearl Object Gateway presents only one MAC address, but can have up to 16 IP addresses aliased to the MAC address.

Link Aggregation Port Utilization

The network switch rotates data transfers among the physical ports on the BlackPearl Object Gateway in order to achieve the highest throughput possible.

If only a single host is connected to the BlackPearl Object Gateway through a link aggregation connection, the measured performance is lower than the potential maximum transfer rate because only one physical port of the two port link aggregation is being utilized by the switch.

If a single share is configured with two different IP addresses, when two separate hosts begin data transfers, the resulting throughput is approximately twice that of a single host connection.

Note: You may need to configure more than two IP addresses on the BlackPearl Object Gateway to force the switch hashing algorithm to utilize all physical ports to maximize performance.

Network Connectivity Tools

Ping

The ping command uses a request-response mechanism to verify connectivity to a remote network node. For example, to verify the connectivity from the switch to the BlackPearl Object Gateway at IP address 192.168.2.10, run the command shown below from the switch command line or client:

```
ping 192.168.2.10
```

All ICMP Echo requests should receive replies including information about the round trip time it took to receive the response. If the request times out, see Cannot Ping the BlackPearl Object Gateway on the next page.

Note: A response of 0 msec means that the time was less than 1 ms.

Traceroute

You can use the traceroute command to not only verify connectivity to a remote network node, but to track the responses from intermediate nodes as well.

For example, for a BlackPearl Object Gateway at IP address 192.168.2.10, run the command shown below:

```
traceroute 192.168.2.10
```

The output of the command shows a numbered list indicating the number of hops encountered when tracing the packet from the switch to the BlackPearl Object Gateway. If the command fails to reach the BlackPearl Object Gateway, see Cannot Ping the BlackPearl Object Gateway below.

Troubleshooting

No Port Link LED Light

When the management and data ports are configured correctly and attached to the network, the link lights on the network ports should be illuminated on both the BlackPearl Object Gateway and the network switch. If the port lights are not illuminated:

- Make sure that cables are connected. Verify you are using the correct cable type and connectors. This is especially critical for connections utilizing SFPs.
- Check the port configuration on the network switch. The BlackPearl Object Gateway only supports auto-negotiation. Make sure the switch is configured to match speeds on both ends of the connection.
- Verify that the switch ports are not administratively disabled. Consult the switch *User Guide* for information.

Cannot Ping the BlackPearl Object Gateway

When the network ports are configured correctly, you should be able to ping the BlackPearl Object Gateway from your network. If you cannot ping the BlackPearl Object Gateway:

- Check the LACP settings on the switch.
  - If you **are** using link aggregation, the switch must be configured **to use** LACP on those ports.
  - If you **are not** using link aggregation, the switch must be configured **to not use** LACP on those ports.
- Check the VLAN (Virtual Local Area Network) settings on the switch. Ensure that the ports are assigned to the correct VLAN.

Configure Certificates

The BlackPearl Object Gateway ships with non-signed SSL certificates for both the data and management ports on the Gateway. Because the certificates are not signed, you must pass a security check every time you attempt to access the management port to view the BlackPearl user interface, or when you attempt to transfer data using the data port.

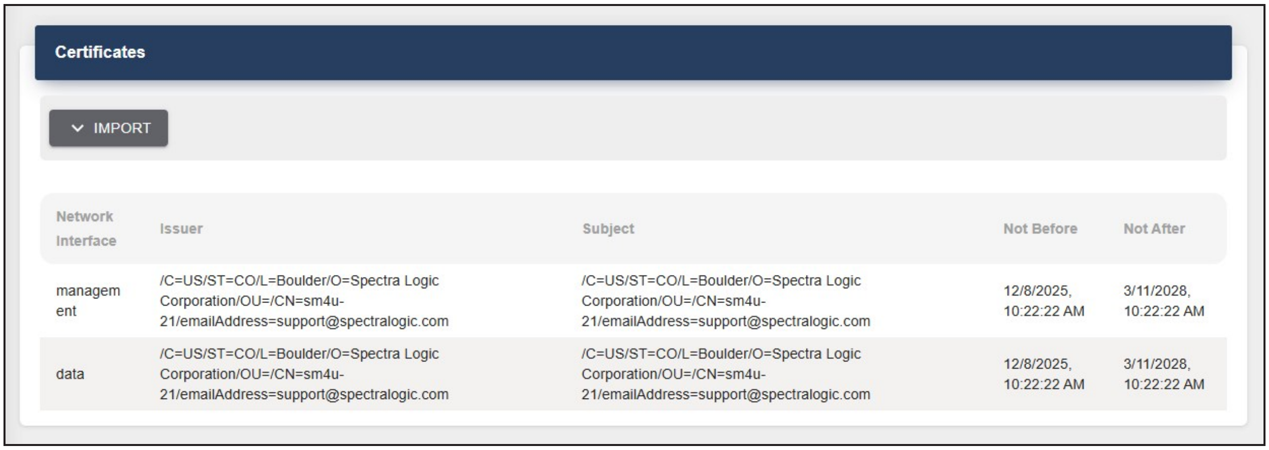
If desired, you can install signed, trusted SSL certificates for your data and management ports so that you no longer need to pass the security check when accessing these ports.

IMPORTANT Starting with BlackPearl OS 5.6, the TLS version is updated to 1.3. Existing certificates using TLS 1.2 must be updated to use the new protocol version.

The BlackPearl Object Gateway accepts intermediate (chain) SSL certificates, and accepts RSA, DSA, and ECC certificates. The BlackPearl Object Gateway accepts both encrypted and non-encrypted certificates.

Use the instructions in this section to install an SSL certificate.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Certificates**. The Certificates screen displays.



Network Interface	Issuer	Subject	Not Before	Not After
management	/C=US/ST=CO/L=Boulder/O=Spectra Logic Corporation/OU=/CN=sm4u-21/emailAddress=support@spectralogic.com	/C=US/ST=CO/L=Boulder/O=Spectra Logic Corporation/OU=/CN=sm4u-21/emailAddress=support@spectralogic.com	12/8/2025, 10:22:22 AM	3/11/2028, 10:22:22 AM
data	/C=US/ST=CO/L=Boulder/O=Spectra Logic Corporation/OU=/CN=sm4u-21/emailAddress=support@spectralogic.com	/C=US/ST=CO/L=Boulder/O=Spectra Logic Corporation/OU=/CN=sm4u-21/emailAddress=support@spectralogic.com	12/8/2025, 10:22:22 AM	3/11/2028, 10:22:22 AM

Figure 41 The Certificates screen.

2. Select either the **Management** or **Data** row, depending on for which port you want to import a new SSL certificate.

3. Click **Import**. The Import Certificate dialog box displays.

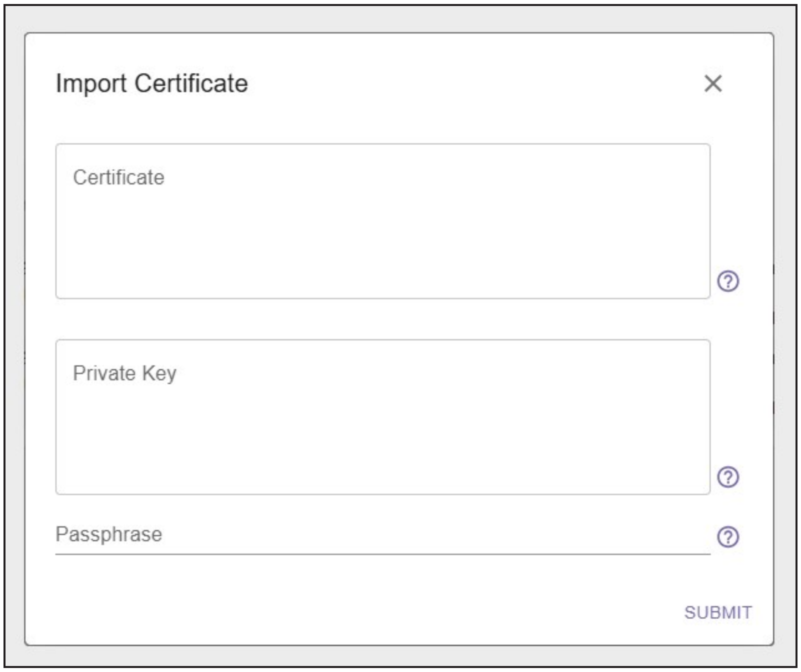


Figure 42 The Import Certificate dialog box.

4. From your source SSL certificate file, copy the Certificate portion of the file and paste the contents into the **Certificate** entry box.

Note: The certificate must be in PEM format.

5. From your source SSL certificate file, copy the Private Key portion of the file and paste the contents into the **Private Key** entry box.

Note: The private key must be in PEM format.

6. If necessary, enter the **Passphrase**. The Passphrase is used to encrypt the private key.
7. Click **Submit**.

CONFIGURE NETWORK SETTINGS

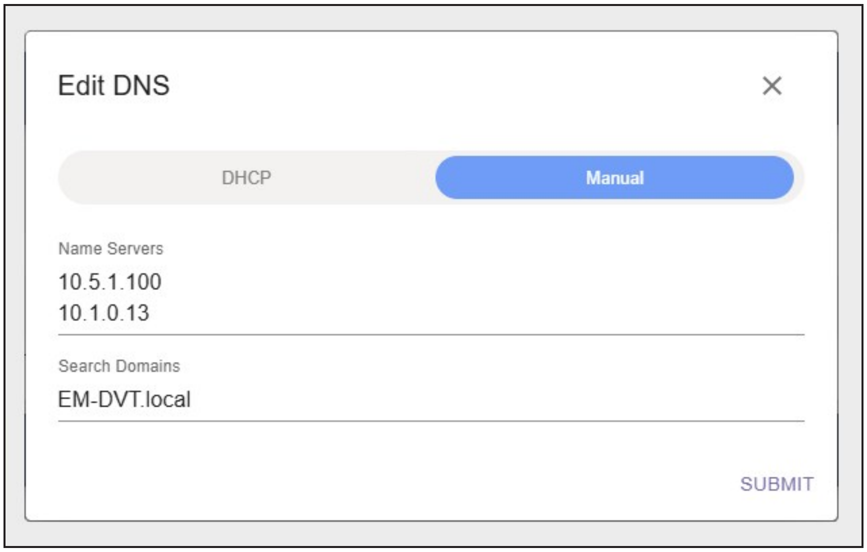
You can use the BlackPearl user interface to edit DNS and SNMP settings, set the system date and time, and set the system hostname.

Configure DNS Settings

The DNS settings on the BlackPearl Object Gateway are used to allow domain name lookup on the Gateway.

Use the following instructions to enter DNS information on the Gateway.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Network**.
2. In the DNS pane, click **Edit**. The Edit DNS dialog box displays.



Edit DNS

Name Servers
10.5.1.100
10.1.0.13

Search Domains
EM-DVT.local

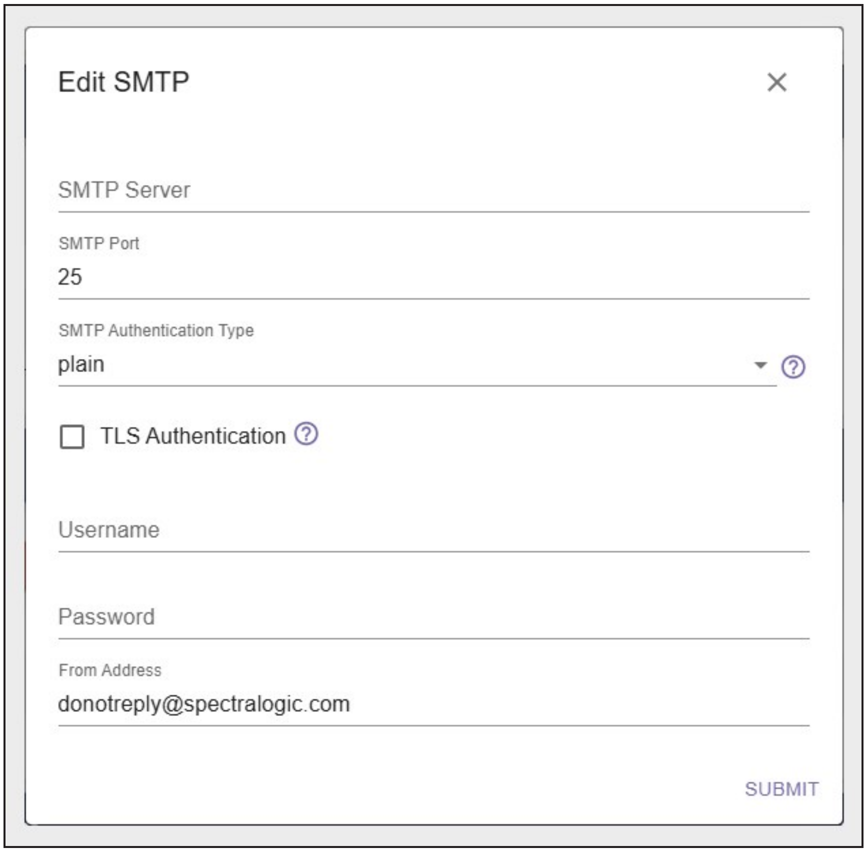
Figure 43 The Edit DNS dialog box.

3. Use the slider to select one of the following:
   - **DHCP** - The Gateway determines the address of name servers and search domains automatically.
   - **Manual** - Enter information for name servers and search domains manually.
4. If you selected **Manual**, enter the following information:
   a. Enter the IP address of one or more name servers in the **Name Servers** field.
   b. Enter the URL of one or more search domains in the **Search Domains** field.
5. Click **Submit**.

Configure SMTP Settings

Use the SMTP settings to associate the BlackPearl Object Gateway with a mail server. The Gateway uses this SMTP server to send emails whenever AutoSupport Logs (ASLs) or certain severites of messages are generated.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Network**.
2. In the SMTP pane, click **Edit**. The Edit SMTP dialog box displays.



Edit SMTP

SMTP Server

SMTP Port: 25

SMTP Authentication Type: plain

□ TLS Authentication

Username

Password

From Address: donotreply@spectralogic.com

Figure 44 The Edit SMTP dialog box.

3. Enter the **SMTP Server** and **SMTP Port** information.
4. Use the **SMTP Authentication Type** drop-down menu to select the authentication required by your SMTP server.
5. If your SMTP server uses TLS (Transport Layer Security) authentication, select the **TLS Authentication** checkbox and enter the required **Username** and **Password** information.
6. Enter an email address in the **From Address** field. This is the email address that displays as the sender whenever the Gateway generates an email. This email address should uniquely identify the BlackPearl Object Gateway to assist in troubleshooting and be recognized by the SMTP server as a valid domain address.
7. Click **Submit**.

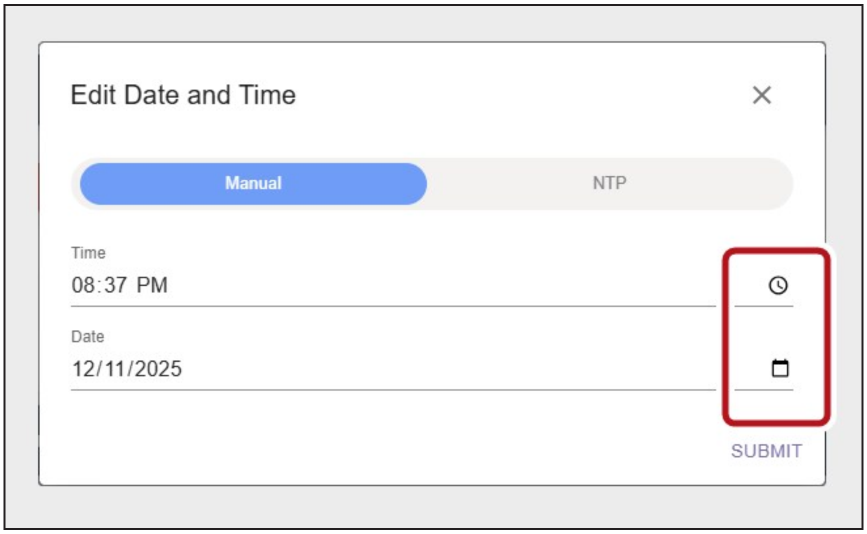
Configure Date and Time

The date and time can be set manually or using NTP (Network Time Protocol). The NTP settings are used to accurately control the current time on the BlackPearl Object Gateway.

Note: If you plan to join an Active Directory domain, you must configure the BlackPearl Object Gateway to use NTP. If the system time and the Active Directory time are more than 5 minutes apart, joining the domain fails.

Use the following instructions to configure the date and time on the Gateway.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Network**.
2. In the Date and Time pane, click **Edit**. The Edit Date and Time dialog box displays.



Edit Date and Time

Time
08:37 PM

Date
12/11/2025

Figure 45 The Edit Date and Time dialog box.

3. Use the slider to select **Manual** or **NTP**.
   - If you select **Manual**:
     a. Enter the current time in the **Time** field. Enter 12-hour time values and include AM or PM. Alternatively, click the clock icon and select the desired time.
     b. Enter values in the **Date** field. Alternatively, click the calendar icon and select the desired date.
   - If you select **NTP** (not shown):
     a. Enter the NTP server information for the **Primary NTP Server**.
     b. If desired, enter the NTP server information for the **Secondary NTP Server**.
4. Click **Submit**.

Change the System Name

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Network**.
2. In the Network Interfaces pane, click **Change System Name**. The Change System Name dialog box displays (not pictured).
3. Enter the desired **System Name** for the Gateway. The Gateway only allows letters, numbers, and the hyphen character (-) in the system name.

Notes:

- The system name cannot be only numbers.
- The hyphen character is only allowed when the system name uses a delimiter.
- The first section of the system name, up to a delimiter (for example, a period) cannot be longer than 15 characters:

  Valid - BlackPearl.domain.com

  Invalid - BlackPearlGateway.domain.com

4. Click **Submit**.

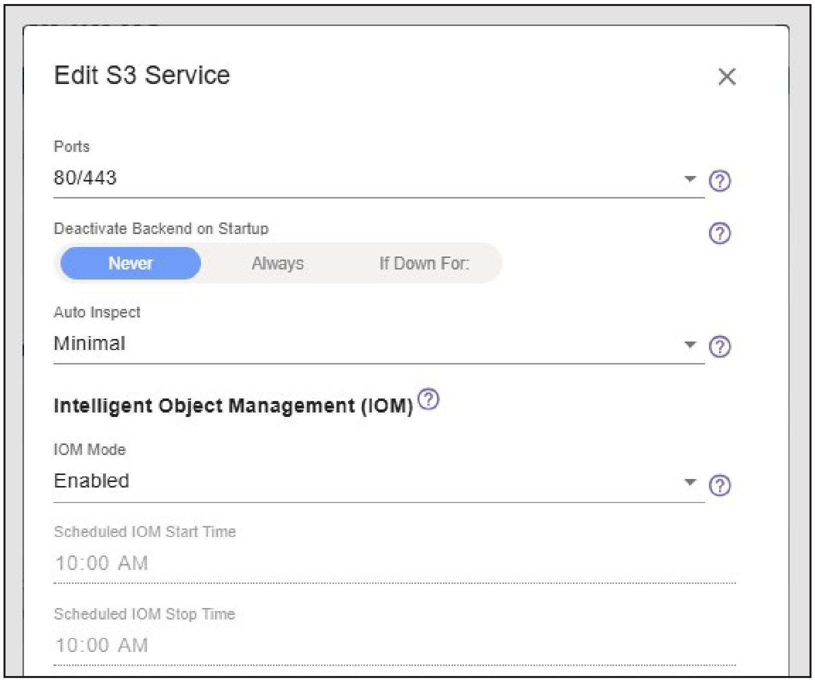
CONFIGURE NETWORKING SERVICES

Use the following instructions to configure Amazon compatible S3, Active Directory, and SNMP networking services on the BlackPearl Object Gateway.

For instructions on configuring NAS services, see Configure NFS and CIFS Services on page 168.

Configure the S3 Service

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the S3 pane, click **Edit**. The Edit S3 Service dialog box displays.



Edit S3 Service

Ports
80/443

Deactivate Backend on Startup
Never | Always | If Down For:

Auto Inspect
Minimal

Intelligent Object Management (IOM)

IOM Mode
Enabled

Scheduled IOM Start Time
10:00 AM

Scheduled IOM Stop Time
10:00 AM

Figure 46 The Edit S3 Service dialog box - top half.

3. Use the **Ports** drop-down list, select the pair of ports used for the HTTP and HTTPS connections to the S3 service.
4. Use the **Deactivate Backend on Startup** slider to select one of the following:
   - **Never** - The S3 service is enabled at system startup.
   - **Always** - The S3 service is deactivated at system startup.
   - **If Down For** - The S3 service is enabled at system startup unless the system was down for longer than the value specified in the **If Down For x Minutes** entry field (not shown above). If the time value passes while the system is down, the system clears the auto-activation timeout, and the service must be manually started.

5. Use the **Auto-Inspect** drop-down menu to select a behavior for tape inspections. This setting configures whether tape inspections are scheduled by the Gateway based on a tape's last known state, or each time the BlackPearl is initialized.

Value	Description
Full	Tapes are scheduled for inspection if an inspection is necessary given the tape's current state, as well as every time the BlackPearl Object Gateway is initialized.
Minimal	Tapes are scheduled for inspection if an inspection is necessary given the tape's current state.
Never	Tapes are not automatically scheduled for inspection.

Note: All tapes new to the BlackPearl Object Gateway are inspected regardless of the auto-inspect setting.

6. Use the **IOM Mode** drop-down menu to select the behavior for Intelligent Object Management. Enabling this option allows for automatic object recovery, automatic tape compaction, and data migration at a system-wide level. See Intelligent Object Management (IOM) on page 417 for information on IOM.

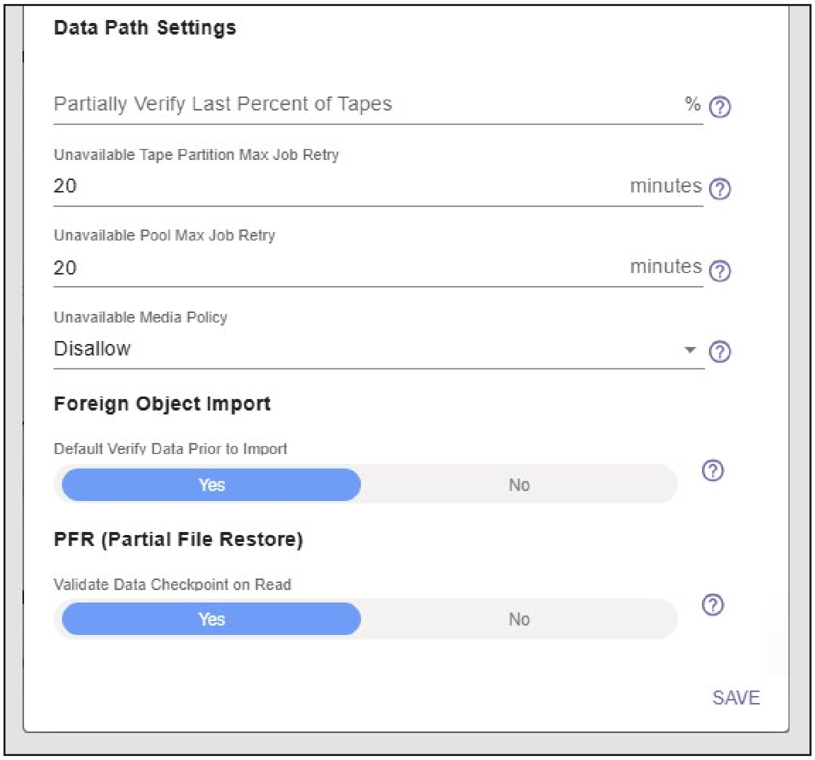
Value	Description
Enabled	The BlackPearl Object Gateway processes IOM operations as needed. If you select this option, the IOM Start Time and IOM Stop Time fields are unavailable.
Scheduled	IOM processes only run during the period between the **Scheduled IOM Start Time** and **Scheduled IOM Stop Time**. **Note:** If you set the start and stop time to the same value, IOM operations do not run.
Disabled	The BlackPearl Object Gateway does not perform any IOM operations.

Notes:

- IOM is enabled by default. Spectra Logic recommends leaving the feature enabled.
- Automatic tape compaction is configured on a per tape partition basis (see Tape Drive Options on page 294 for more information).
- Data migration is initiated manually. See Data Migration on page 311 for more information.
- If this option is currently enabled, when the setting is disabled, any in-progress IOM operations are suspended.

7. Enter a percentage value for **Partially Verify Last Percentage of Tapes**. This setting specifies the percentage of the total reported capacity of the tape cartridge scanned by an automatic or on demand data integrity verification. The Gateway starts the scan at the specified percentage of the tape capacity before the EOD (End of Data) marker, and ends the scan at the EOD marker. For example, if you specify ten percent, the verification process scans the last 250 GB of a 2.5 TB LTO-6 tape cartridge, or the last 600 GB of a 6 TB LTO-7 tape cartridge.

   - Leave the field blank to configure data integrity verification to scan all data present on the tape cartridge.
   - Percentage values of zero and 100 are not supported.
   - See Data Integrity Verification - Tape Media on page 361 for information about on demand tape media data integrity verification.



Data Path Settings

Partially Verify Last Percent of Tapes %

Unavailable Tape Partition Max Job Retry
20 minutes

Unavailable Pool Max Job Retry
20 minutes

Unavailable Media Policy
Disallow

Foreign Object Import

Default Verify Data Prior to Import
Yes No

PFR (Partial File Restore)

Validate Data Checkpoint on Read
Yes No

Figure 47 The Edit S3 Service dialog box - bottom half.

8. Enter a value, in minutes, for **Unavailable Tape Partition Max Job Retry**. This setting specifies the maximum number of minutes that can elapse between the first failed attempt to GET or VERIFY job data (due to a tape partition being offline, in an error state, or deactivated), before a subsequent failure will trigger a retry to process the job data. This only applies to GET or VERIFY jobs.

9. Enter a value, in minutes, for **Unavailable Pool Max Job Retry**. This setting specifies the maximum number of minutes that can elapse between the first failed attempt to GET or VERIFY job data (due to a pool partition being offline, in an error state, or deactivated), before a subsequent failure will trigger a retry to process the job data. This only applies to GET or VERIFY jobs.

10. Use the **Unavailable Media Policy** drop-down menu to select a behavior for when media is unavailable. This setting configures how the Gateway behaves where there are unavailable tape or disk partitions when creating new jobs or retrying to process job data.

Value	Description
Allow	New job requests for unavailable media are allowed and will retry for the duration of the **Unavailable Tape Partition Max Job Retry** or **Unavailable Pool Max Job Retry** setting.
Discouraged	Unavailable partitions can be used, but only if no other media is available.
Disallow	New job requests for unavailable media are not permitted.

11. Use the **Default Verify Data Prior to Import** slider to select one of the following:

    - **Yes** - Selecting this option verifies data on imported tape media before it makes the data available to the Gateway.
    - **No** - Immediately makes imported objects available, and schedules a job with the configured priority to run at a later time. Use the **Default Verify Data After Import Priority** drop-down menu (not shown above) to select a priority for data verifications after import.

12. Use the **Validate Data Checkpoint on Read** slider to select one of the following:

    - **Yes** - When loading a tape cartridge into a tape drive, the BlackPearl Object Gateway verifies that the last tape index and checkpoint location match what is stored in the BlackPearl database before performing any read or write operations. This helps with data integrity if tape verifications are infrequent or not used after data is written.
    - **No** - This option does not verify tape index and checkpoint location when a tape cartridge is loaded, which can save up to 1 to 4 minutes per drive load when restoring data.

13. Click **Save**.

Configure the Active Directory Service

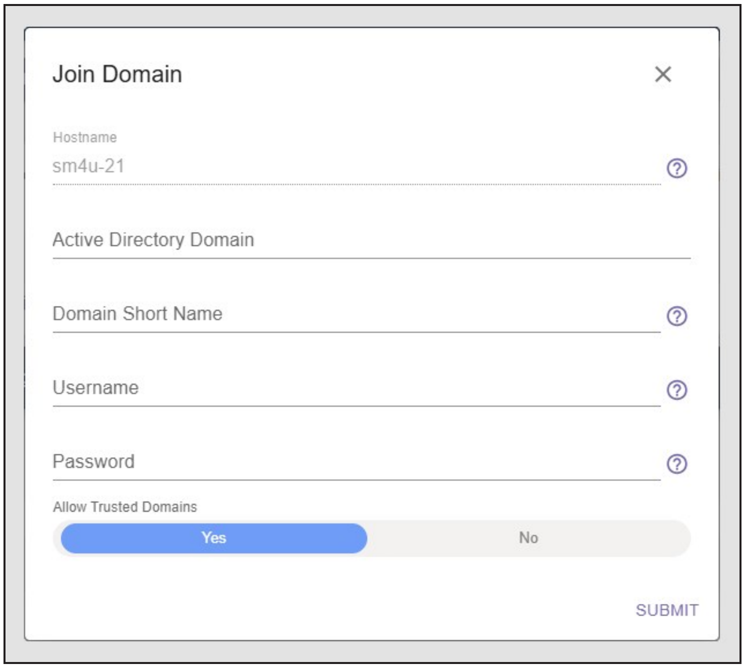
The Active Directory service in the BlackPearl user interface is used to connect the Gateway to a Windows Active Directory domain. Before you can join a domain, you must configure the BlackPearl Object Gateway to use NTP. See Configure Date and Time on page 96.

Note: If the BlackPearl Object Gateway time and the Active Directory domain time are more than 5 minutes apart, joining the domain fails.

Use the instructions in this section to join or leave an Active Directory domain.

Join Domain

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the Active Directory pane, click **Join Domain**. The Join Domain dialog box displays.



Join Domain

Hostname: sm4u-21

Allow Trusted Domains: Yes

Figure 48 The Join Domain dialog box.

3. The **Hostname** identifies the BlackPearl Object Gateway in the Active Directory domain.

Note: The hostname is unavailable and cannot be changed in the Join Domain dialog box. Use the Hardware screen to change the hostname if desired (see Configure Network Connections on page 107).

4. Enter the name of the **Active Directory Domain** you want to join.
5. Optionally, enter the **Domain Short Name** if your domain uses a non-standard workgroup name.

6. Enter the **Username** and **Password** for a user authorized to join the specified domain.

Notes:
- The BlackPearl Object Gateway uses “Pre-Windows 2000” login names for Active Directory users. Login names greater than 20 characters in length, or containing special characters (for example ‘@’) are not able to log into the BlackPearl user interface.
- You must enter the user name and password each time the BlackPearl Object Gateway joins an Active Directory domain. The Gateway does not save this information.

7. Use the **Allow Trusted Domains** slider to select one of the following:
   - **Yes** - Select this option if the Active Directory domain you want to join is a trusted domain.
   - **No** - Select this option if the domain is not a trusted domain.
8. Click **Submit**.

Add Advanced Parameter

Advanced Parameters are used to adjust or set global or share specific Samba parameters. These parameters are mirrored on both the Active Directory and CIFS Service pages.

CAUTION Improperly configuring advanced parameters can expose security vulnerabilities and other serious issues. Advanced parameters should not be configured without a full understanding of the consequences.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the Active Directory pane, click **Add Parameter**.
3. Enter the desired **Parameter Name** and **Parameter Value**.
4. Click **Add**.

Edit Advanced Parameter

CAUTION Improperly configuring advanced parameters can expose security vulnerabilities and other serious issues. Advanced parameters should not be configured without a full understanding of the consequences.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the Active Directory pane, click **Edit Parameter**.
3. Edit the **Parameter Name** and **Parameter Value** as desired.
4. Click **Submit**.

Edit Domain

If desired, you can edit your Active Directory configuration to enable or disable support for trusted domains.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the Active Directory pane, click **Edit Domain**. The Edit Domain confirmation screen displays (not shown).
3. Use the **Allow Trusted Domains** slider to select one of the following:
   - **Yes** - Select this option if the Active Directory domain you want to join is a trusted domain.
   - **No** - Select this option if the domain is not a trusted domain.
4. Click **Submit**.

Delete Advanced Parameter

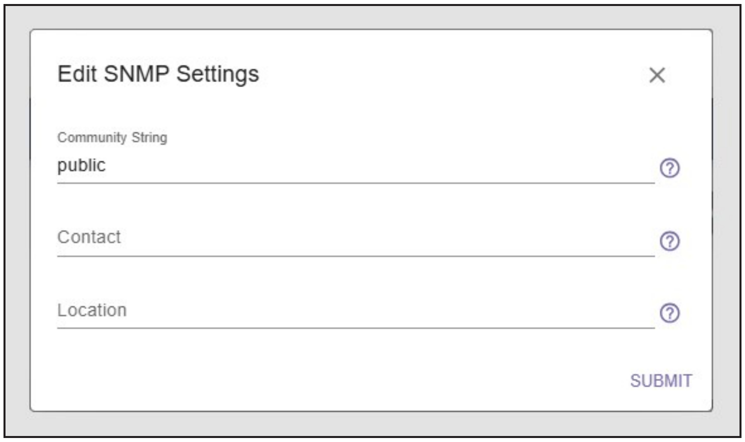
1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the Active Directory pane, click **Delete Parameter**. The Delete Parameter confirmation screen displays (not shown).
3. Click **Delete**.

Leave Domain

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the Active Directory pane, click **Leave Domain**. The Leave Domain confirmation screen displays (not shown).
3. Click **Leave Domain**.

Configure the SNMP Service

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the SNMP pane, click **Edit Settings**. The Edit SNMP Settings dialog box displays.



Edit SNMP Settings

Community String: public

Contact

Location

Figure 49 The Edit SNMP Settings dialog box.

3. If desired, change the value of the **Community String**. Any incoming SNMP queries that use a different community string than the one set here fail. If no community string is specified, then the BlackPearl Object Gateway responds to all SNMP queries.
4. Enter the primary contact for the BlackPearl Object Gateway in the **Contact** field.
5. Enter the physical location of the Gateway in the **Location** field.
6. Click **Submit**.

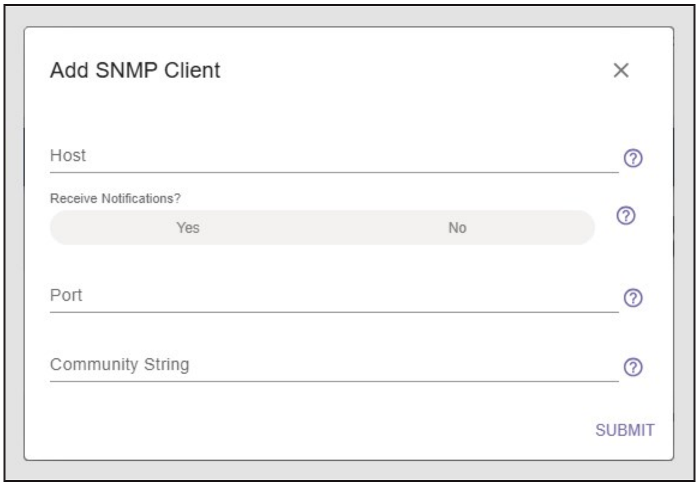
Add SNMP Clients

After configuring the SNMP service, you must add clients to make SNMP queries to the BlackPearl Object Gateway.

Here is how you add an SNMP client:

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.

2. In the SNMP pane, click **Add Client**. The Add SNMP Client dialog box displays.



Add SNMP Client

Host

Receive Notifications?

Yes No

Port

Community String

SUBMIT

Figure 50 The Add SNMP Client dialog box.

3. Enter the host IP address in the **Host** field.
4. Use the **Receive Notifications** slider to select one of the following:
   - **Yes** - The SNMP client receives outgoing notifications/traps.
   - **No** - The client does not receive outgoing notification/traps.
5. Enter the port number to be used for SNMP communication in the **Port** field
6. Enter a community string value in the **Community String** field. This community string is set for each client. The clients monitor SNMP notifications for any that use the string specified here.
7. Click **Submit**.

Download the MIB File

If you want to communicate with the Gateway using SNMP, you must first download the BlackPearl Object MIB (Management Information Base) file, and load the file into a compatible network node manager program, such as HP® OpenView®.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the SNMP pane, click **Download MIB**. Using your web browser, save the file to your local host.
3. Load the file into the network node manager program.
4. You can now use your network node manager program to communicate with the BlackPearl Object Gateway, using the settings configured in Configure Networking Services on page 98.

Configure Network Connections

You can use the BlackPearl user interface to configure the system Ethernet ports and configure static routes.

Note: If configuring a HotPair system, contact Spectra Logic Technical Support for instructions on configuring network connections.

Configure Ethernet Ports

This section describes using the BlackPearl user interface to configure the IP addressing for the Ethernet ports in the BlackPearl Object Gateway. The Gateway may contain a variety of included and optional Ethernet network interface connections.

Notes:

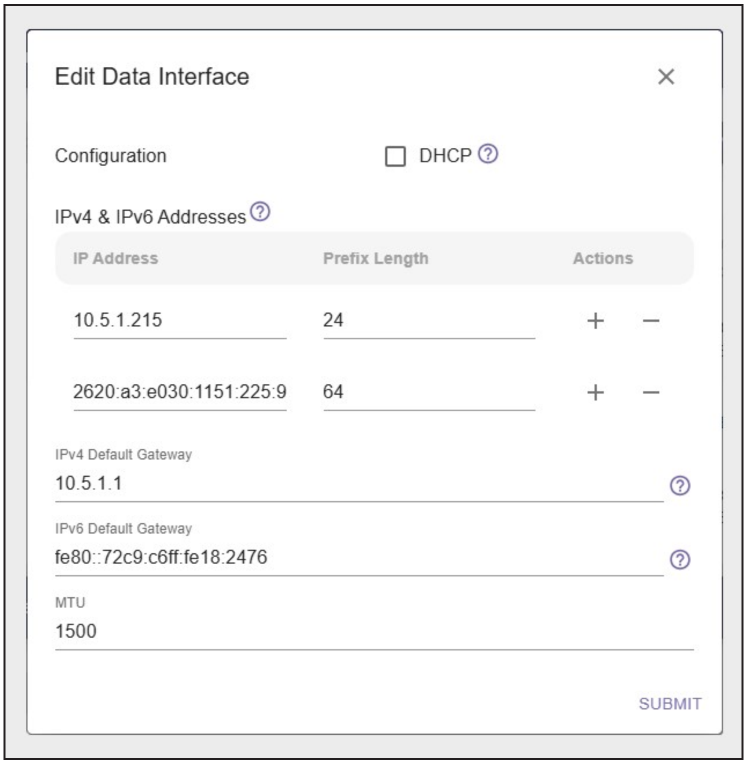
- You can create one or more data connections to the Gateway.
- You can configure link aggregation for better performance.
- While different types of Ethernet network interface cards can be installed in the same BlackPearl Object Gateway, only one type of port can be used in each link aggregation configuration.
- You can only use the BlackPearl management port to access the BlackPearl user interface. You cannot use this port for data transfer.
- The BlackPearl management port is used by external applications to trigger snapshots of NAS volumes.
- The data connection(s) and BlackPearl management port are initially configured in Configuring Initial Settings on page 67. Use the instructions in this section to configure network settings after initial setup is complete.

The next steps depend on if you are configuring the data connection, the management port, or want to delete (clear) a network configuration.

- Configure the Data Connection on page 76
- Configure the Management Port below
- Add a Static Route on page 109
- Clear a Data Port Configuration on page 109

Configure the Management Port

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Network**.
2. In the Network Interfaces pane, select the **Management** row and then click **Edit**. The Edit Data Interface dialog box displays.



Edit Data Interface ✕

Configuration □ DHCP

IPv4 & IPv6 Addresses

IP Address	Prefix Length	Actions
10.5.1.215	24	+ −
2620:a3:e030:1151:225:9	64	+ −

IPv4 Default Gateway: 10.5.1.1

IPv6 Default Gateway: fe80::72c9:c6ff:fe18:2476

MTU: 1500

SUBMIT

Figure 51 The Edit Management dialog box.

3. Select the **DHCP** checkbox to configure the Gateway to automatically acquire an IPv4 address using DHCP. This setting does not apply to IPv6.

IMPORTANT If you select DHCP, you are not able to see the IP address assigned by DHCP before you are logged out of the BlackPearl user interface. Contact your system administrator to determine the DHCP address for the management port.

4. To configure a static IP address, click the **+** button and enter the following information:

- **IP Address**—Enter a valid IPv4 or IPv6 address.

Note: You cannot enter an IPv4 address if you selected DHCP.

- **Prefix Length**—Enter the subnet mask.

Note: If desired, you can enter **Aliases**, multiple IP and prefix lengths assigned to the data port. Use the **+** button to configure additional IP and Netmask addresses. You can configure a maximum of 16 aliases.

5. If applicable, enter the **IPv4 Default Gateway**.

Note: The gateway entered for the last configured IPv4 connection sets the default gateway for the BlackPearl Object Gateway.

6. If applicable, enter the **IPv6 Default Gateway**.

Notes:
- The gateway entered for the last configured IPv6 connection sets the default gateway for the BlackPearl Object Gateway.
- The IPv6 Gateway does not need to be configured when the BlackPearl Object Gateway is connected to a SLACC network.

7. Change the **MTU** value, if desired. If you set the MTU value to something other than 1500, make sure that your switch configuration supports larger MTU settings, as well as all the hosts on the network. Acceptable values are 576 to 65535.

Note: Most networking designs are configured to use a value of 1500 or 9000.

8. Click **Submit**.

Note: When you change the IP address of the BlackPearl management port, you lose your connection to the user interface when you save your changes. To re-establish the connection, enter the new IP address in your browser and log in again.

Add a Static Route

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Network**.
2. In the Static Routes pane, click **New**. The Add Static Route dialog box displays (not shown).
3. If desired, in the **Destination** field, edit the network address that you want to access through the data connection.
4. If desired, edit the network **Gateway** of the data connection used to communicate with the isolated network.
5. Click **Submit**.

Clear a Data Port Configuration

In some cases, it may be useful to delete an existing data port configuration by clearing it. Use the instruction in this section to clear a data port configuration.

Note: The management port cannot be cleared. See Configure the Management Port on page 107 to change the management port settings.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Network**.
2. Select the row of the configuration you want to clear and click **Clear**. A confirmation window displays (not shown).
3. Click **Delete** to clear the Ethernet configuration.

CHAPTER 4 - CONFIGURING OBJECT STORAGE

This chapter provides instructions on how to configure object storage features.

CREATE A TAPE PARTITION

Use the Tape Library User Guides on page 22 for your Spectra Logic or other supported tape library to create a partition. Once the BlackPearl Object Gateway detects a partition on a tape library connected to it, the tape partition is automatically listed on the Buckets screen.

Note: If the BlackPearl Object Gateway is configured to transfer data to tape, make sure the partitions configured for use by the BlackPearl Object Gateway do not contain WORM (Write Once-Read Many) media. The BlackPearl Object Gateway is not compatible with WORM media.

CREATE A DISK POOL

A disk pool groups a set of physical drives together to create a virtual drive that the operating system treats as a single physical drive. There are two types of disk pools:

- **Nearline Storage Disk Pool** - If all drives in the pool are cable of setting an idle timer, Nearline storage disk pools can be configured to spin down after 60 minutes of inactivity, for power savings.
- **Online Storage Disk Pool** - Online storage disk pools remain powered on at all times for fast access to data.

Online and Nearline Storage disk pools use compression with ZFS to allow the BlackPearl Object Gateway to store more data. If the data being written is compressible there is typically in increase with store and restore operations, because less data is transferred to and from the disk drives. The size reduction of transferred files depends on how much the system can compress the data, and may fluctuate.

The data compression process uses CPU cycles to perform the compression. If compression is enabled for non-compressible data, for example JPEG images or movie files that use the H. 264 codec, the compression process may use an excessive number of CPU cycles, slowing the overall performance of the Gateway. This impact is less evident with Gen2 and Gen 3 master nodes.

Note: When viewing the details of an online or nearline storage disk pool, the user interface displays the physically used space on the pool, not the logically used space.

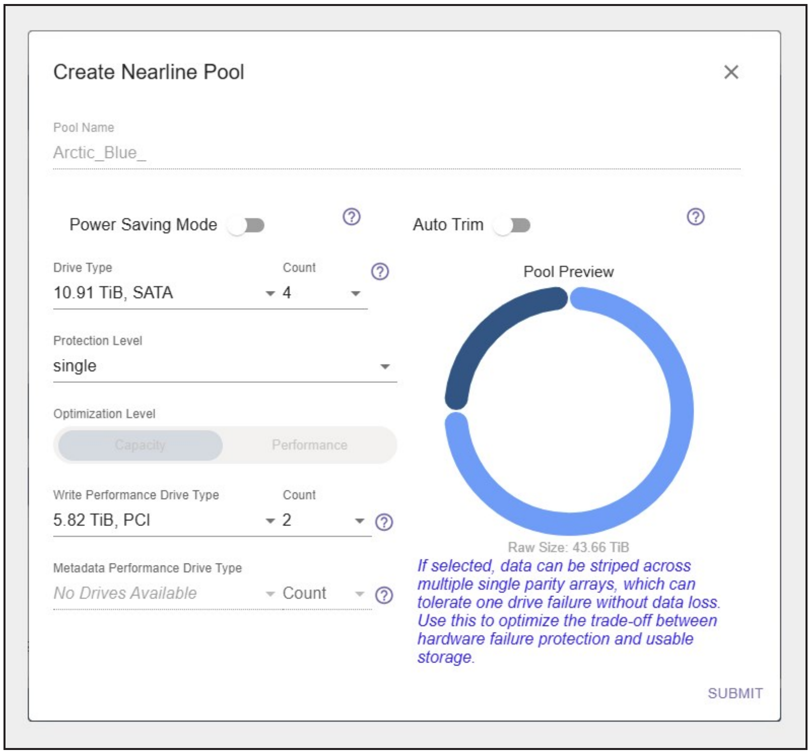
Once a disk pool is created, it can be added to a disk partition.

Create a Nearline Storage Disk Pool

Use the instructions in this section to create a nearline storage disk pool.

Note: Nearline pools created on a 96-bay expansion node have a hard coded capacity utilization limit percentage of 95%.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.
2. In the Disk Pools pane, click **New Nearline Pool**. The Create Nearline Pool dialog box displays.



Create Nearline Pool

Pool Name: Arctic_Blue_

Power Saving Mode: off

Auto Trim: off

Drive Type: 10.91 TiB, SATA — Count: 4

Protection Level: single

Optimization Level: Capacity | Performance

Write Performance Drive Type: 5.82 TiB, PCI — Count: 2

Metadata Performance Drive Type: No Drives Available — Count

Pool Preview

Raw Size: 43.66 TiB

If selected, data can be striped across multiple single parity arrays, which can tolerate one drive failure without data loss. Use this to optimize the trade-off between hardware failure protection and usable storage.

Figure 52 The Create Nearline Pool dialog box.

3. The **Pool Name** is automatically generated. The name is "Arctic_Blue_#" where # is automatically assigned when you create the pool.
4. If desired, use the slider to enable **Power Saving Mode**. This option allows the disk drives in a disk pool to spin down after 60 minutes of inactivity.

Notes:
- This option is only available if all disk drives in the disk pool are capable of power saving mode.
- Spectra Logic recommends leaving Power Saving Mode **disabled**.

5. If desired, use the slider to enable **Auto Trim**. The option automatically removes unused data blocks from SSD and NVMe drives by marking deleted files as immediately ready for reuse, improving drive performance and longevity.

6. Use the **Drive Type** drop-down menu to select the disk drive type to use for the storage pool. Only one drive type can be used in a nearline pool.

Note: Any drive not in a disk pool acts as a global spare. A global spare drive is activated as soon as a drive configured in a disk pool fails.

7. Use the **Count** drop-down menu to select the number of drives of the previously selected type to use in the storage pool. If you plan to optimize the drive for capacity or performance, select an even number of drives.

8. Use the **Protection Level** drop-down menu to select the level of RAID protection to use on the storage pool:

    - **Mirror**—Data is striped across two mirrors. Any detected data corruption is corrected using checksums. This type of RAID offers the best performance for small random reads and writes.
    - **Single**—Data is striped across multiple single-parity arrays, which can tolerate one drive failure without data loss. This type of RAID has faster performance than double- and triple-parity based RAIDs.
    - **Double**—Data is striped across multiple double-parity arrays, which can tolerate two drive failures without data loss. In most cases, double-parity provides the best balance between data protection, performance, and storage capacity.
    - **Triple**—Data is striped across multiple triple-parity arrays, which can tolerate three drive failures without data loss. This type of RAID provides the most data protection.
    - **None**—The pool is not configured to provide data protection. Any drive failure results in data loss.

Note: Spectra Logic does not recommend setting protection to None.

9. Use the **Optimization Level** slider to select one of the following:

    - **Capacity** - The pool has more storage space, but slower performance.
    - **Performance** - The pool is faster at reading and writing data with less overall capacity.

10. Use the **Write Performance Drive Type** drop-down menu to select the disk drive type to use for the write performance drives, which increase write performance when the pool is shared using NFS.

Note: This feature is only intended for storage pools with NFS shares and typically has little impact on CIFS share performance.

11. Use the **Count** drop-down menu to select the number of write performance drives to add to the storage pool.

12. Use the **Metadata Performance Drive Type** drop-down menu to select the disk drive type to use for metadata performance drives, which improve performance for restoring small files, deduplication operations, and when searching metadata.

Note: These drives are permanently part of the storage pool and cannot be removed.

13. Use the **Count** drop-down menu to select the number of metadata performance drives to add to the storage pool.

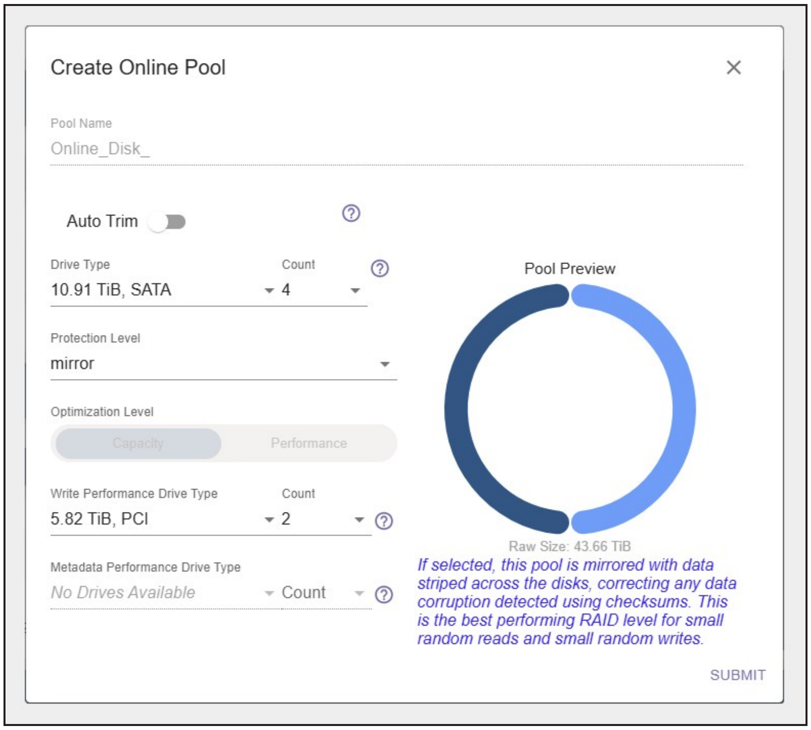
Note: Metadata Performance drives can only be selected in multiples of three.

14. Click **Submit**.

Create an Online Disk Pool

Use the instructions in this section to create an online disk pool.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.
2. In the Disk Pools pane, click **New Online Pool**. The Create Online Pool dialog box displays.



Create Online Pool

Pool Name: Online_Disk_

Auto Trim

Drive Type: 10.91 TiB, SATA — Count: 4

Protection Level: mirror

Optimization Level: Capacity | Performance

Write Performance Drive Type: 5.82 TiB, PCI — Count: 2

Metadata Performance Drive Type: *No Drives Available* — Count

Pool Preview

Raw Size: 43.66 TiB

If selected, this pool is mirrored with data striped across the disks, correcting any data corruption detected using checksums. This is the best performing RAID level for small random reads and small random writes.

SUBMIT

Figure 53 The Create Online Pool dialog box.

3. The **Pool Name** is automatically generated. The name is "Online_Disk_#" where # is automatically assigned when you create the pool.
4. If desired, use the slider to enable **Auto Trim**. The option automatically removes unused data blocks from SSD and NVMe drives by marking deleted files as immediately ready for reuse, improving drive performance and longevity.

5. Use the **Drive Type** drop-down menu to select the disk drive type to use for the storage pool. Only one drive type can be used in an online pool.

Note: Any drive not in a disk pool acts as a global spare. A global spare drive is activated as soon as a drive configured in a disk pool fails.

6. Use the **Count** drop-down menu to select the number of drives of the previously selected type to use in the storage pool. If you plan to optimize the drive for capacity or performance, select an even number of drives.

7. Use the **Protection Level** drop-down menu to select the level of RAID protection to use on the storage pol.

   - **None**—The pool is not configured to provide data protection. Any drive failure results in data loss.

Note: Spectra Logic does not recommend setting protection to None.

   - **Mirror**—Data is striped across two mirrors. Any detected data corruption is corrected using checksums. This type of RAID offers the best performance for small random reads and writes.
   - **Single**—Data is striped across multiple single-parity arrays, which can tolerate one drive failure without data loss. This type of RAID has faster performance than double- and triple-parity based RAIDs.
   - **Double**—Data is striped across multiple double-parity arrays, which can tolerate two drive failures without data loss. In most cases, double-parity provides the best balance between data protection, performance, and storage capacity.
   - **Triple**—Data is striped across multiple triple-parity arrays, which can tolerate three drive failures without data loss. This type of RAID provides the most data protection.

8. Use the **Optimization Level** slider to select one of the following:

   - **Capacity** - The pool has more storage space, but slower performance.
   - **Performance** - The pool is faster at reading and writing data with less overall capacity.

9. Use the **Write Performance Drive Type** drop-down menu to select the disk drive type to use for the write performance drives, which increase write performance when the pool is shared using NFS.

Note: This feature is only intended for storage pools with NFS shares and typically has little impact on CIFS share performance.

10. Use the **Count** drop-down menu to select the number of write performance drives to add to the storage pool.

11. Use the **Metadata Performance Drive Type** drop-down menu to select the disk drive type to use for metadata performance drives, which improve performance for restoring small files, deduplication operations, and when searching metadata.

Notes:

- Metadata Performance drives can only be selected in multiples of three.
- These drives are permanently part of the storage pool and cannot be removed.

12. Use the **Count** drop-down menu to select the number of metadata performance drives to add to the storage pool.

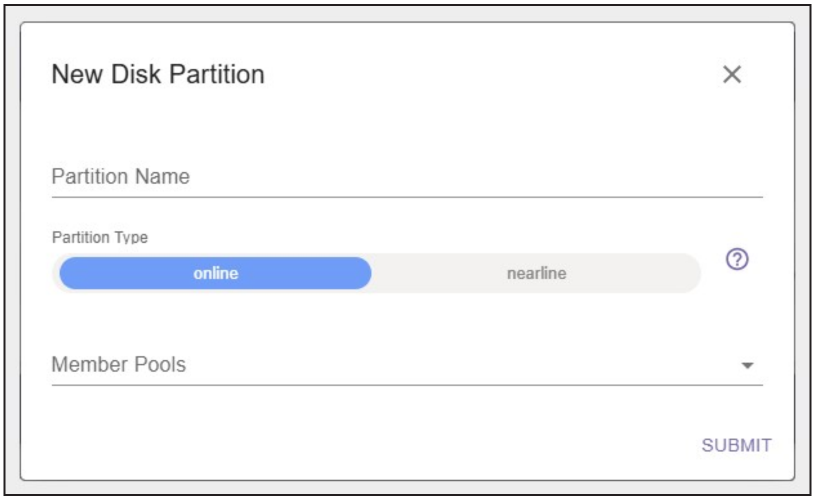
13. Click **Submit**.

CREATE A DISK PARTITION

Disk partitions are collections of one or more disk pools. Disk partitions are specified in storage domains as storage targets.

Use the instructions in this section to create a new disk partition.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.
2. In the Disk Partitions pane, click **New**. The New Disk Partition dialog box displays.



New Disk Partition

Partition Name

Partition Type

Member Pools

Figure 54 The New Disk Partition dialog box.

3. Enter a **Partition Name**.
4. Use **Partition type** the slider to select one of the following:
   - **Online** - uses a disk pool that is always powered on and available for access.
   - **Nearline** - uses a disk pool that can be configured to spin down after 60 minutes of inactivity, for power savings.

Note: You cannot mix different types of disk pools in a disk partition.

5. Use the **Member Pools** drop-down menu to select a disk pool from the list of previously configured disk pools.

Note: It may take up to 1 minute after creating an online or nearline disk pool before it displays in the Member Pools list.

6. If desired, repeat Step 5 to add additional disk pools to the disk partition.
7. Click **Submit**.

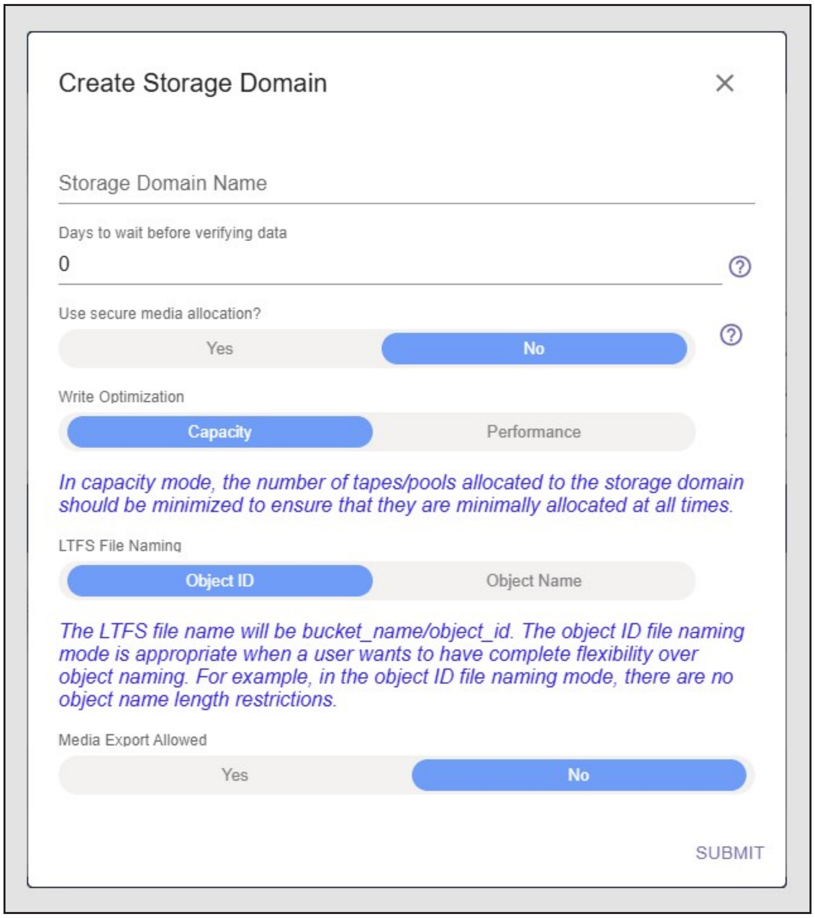
CREATE A STORAGE DOMAIN

A storage domain is a named collection of member data partitions and, when applicable, media type combinations. Storage domains define the possible places where the BlackPearl Object Gateway stores data that is sent to it. Data persistence rules and data policies further define where and for how long to store specific data.

Entire data partition/media type combinations are members of storage domains. When a bucket requires additional capacity, a single disk partition or tape cartridge is allocated out of the members to fulfill the capacity requirement.

Use the instructions in this section to create a new storage domain.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.
2. In the Storage Domains pane, click **New**. The Create Storage Domain dialog box displays.



Create Storage Domain

Storage Domain Name

Days to wait before verifying data: 0

Use secure media allocation? Yes [✓ No]

Write Optimization: [✓ Capacity] Performance

In capacity mode, the number of tapes/pools allocated to the storage domain should be minimized to ensure that they are minimally allocated at all times.

LTFS File Naming: [✓ Object ID] Object Name

The LTFS file name will be bucket_name/object_id. The object ID file naming mode is appropriate when a user wants to have complete flexibility over object naming. For example, in the object ID file naming mode, there are no object name length restrictions.

Media Export Allowed: Yes [✓ No]

Figure 55 The Create Storage Domain dialog box.

3. Enter a **Storage Domain Name**.

4. Enter a value for **Days to wait before verifying data**. The Gateway automatically performs a data integrity verification for all tape media in the storage domain that are unchanged after the specified number of days pass, to ensure the data written to the tape cartridge is still viable. If null, data integrity verification is not performed automatically.

Notes:

- By default, all data on the tape is verified. You can customize the amount of data to be verified in Configure Networking Services on page 98.
- When this verification completes, the **Last Verified** field on the tape details screen is updated.
- While the verification is in progress, client access has priority over the data integrity verification.
- You can also initiate data integrity verification for tape media manually. See Data Integrity Verification - Tape Media on page 361 for more information.
- Disk pools are not subject to automatic data integrity verification. However, you can initiate data integrity verification for disk pools manually. See Data Integrity Verification - Disk Media on page 359 for more information.

5. Use the **Secure Media Allocation** slider to select one of the following:

   - **Yes** - ensures that media allocated to the storage domain always remains in the storage domain. Even if all data on the media is deleted, the media will not be reallocated to another storage domain.
   - **No** - The media will be reallocated to another storage domain if needed.

Note: Secure Media Allocation should only be enabled when, for compliance purposes, the user must be certain which media ever contained any data for the storage domain (usually, to physically destroy the media once the data is no longer needed), or to force rotating through media when new backups are created and old backups are deleted.

6. Use the **Write Optimization** slider to select the optimization used for writes to the storage domain. This setting specifies whether job chunks are written as quickly as possible or across as few pieces of media as possible.

   - **Capacity** - the BlackPearl Object Gateway uses as few tape cartridges or disk pools as possible. The Gateway only allocates a new tape cartridge or disk pool when capacity is needed.
   - **Performance** - the BlackPearl Object Gateway spreads the chunks or aggregations across all available tape drives, or disk pools. The number of tape drives used can be limited by using tape drive reservations.

   The consequence of using performance mode with tape media is that during a restore or GET job, more tape drives and tapes cartridges are required to restore a data set that was initially spread across many tapes. This can drastically reduce overall performance during restores, as the Gateway takes longer to get access to the full data set.

For more information on capacity and performance modes, see Capacity Mode versus Performance Mode on page 421.

IMPORTANT Spectra Logic highly recommends working with Spectra Logic Technical Support, or Spectra Professional Services before using Performance mode.

Note: If the storage domain is assigned to a data policy and "Minimize Spanning" is enabled for the data policy, it overrides the capacity mode vs. performance mode logic for a given job, up to 1 TB in size. Minimize spanning increases the chunk size to 1 TB, and always keeps one chunk on a single tape regardless of write mode. If the job is larger than 1 TB, then multiple chunks are used and the Gateway uses the logic for capacity mode vs performance mode, where different chunks may transfer to different tapes.

7. Use the **LTFS File Naming** slider to configure the naming option for the storage domain. This setting specifies how the Gateway names files when it writes them to tape. This setting only applies to tape media.

   - **Object ID** — LTFS file names use the format {*bucket name*}/{*object id*}, for example bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82. Object names do not need to comply with LTFS file naming rules. The Gateway saves object names as LTFS extended attributes allowing any third party application to reconstruct all the data including the object names.

IMPORTANT If this storage domain is assigned to a data policy that uses versioning, after data is persisted, you cannot change this setting from Object ID to Object Name.

   - **Object Name** — LTFS file names use the format {*bucket name*}/{*object name*}, for example bucket1/video1.mov. Object names must comply with LTFS file naming rules. If the tapes are exported from the BlackPearl Object Gateway and loaded into a non-BlackPearl tape partition, the file names match the object names.

IMPORTANT If you select **Object Name**, you cannot assign this storage domain to a data policy that uses versioning.

Notes:

- The colon character (:) is not allowed in LTFS file names and therefore not allowed in BlackPearl object names.
- The slash character (/) is not allowed in LTFS file names; however, the BlackPearl software can accommodate a slash in the object name and translates it as a directory in the LTFS file system (e.g. directory1/directory2/video1.mov).
- File names with multiple consecutive slash characters (//) are not allowed.
- Directory names have a limit of 255 characters.

- File names have a variable character limit. If you are using English ASCII characters, the limit is 1024 characters. If you are using a graphical language, such as Japanese, the limit is 512 characters.
- Spectra Logic does not recommend the following characters in LTFS file names or BlackPearl object names for reasons of cross-platform compatibility:

  - Asterisk (*)
  - Question mark (?)
  - Question mark (?)
  - Forward slash (/)
  - Backslash (\)
  - Vertical bar / pipe (|)
  - Left curly brace ({)
  - Right curly brace (})
  - Caret (^)
  - Percent character (%)
  - Grave accent / back tick (`)
  - Right square bracket (])
  - Left square bracket ([)
  - Double quotation marks (")
  - Greater Than symbol (>)
  - Less Than symbol (<)
  - Tilde (~)
  - Pound character (#)
  - Control characters such as carriage return (CR) and line feed (LF),
  - Non-printable ASCII characters (128–255 decimal characters)

- Spectra Logic does not recommend accented characters in LTFS file names or BlackPearl object names because LTFS normalizes them before objects are written to tape and there could be conflicts with two objects having the same normalized name.

8. Use the **Media Export Allowed** slider to select one of the following:
   - **Yes** - Enables tape media export options for the storage domain.
   - **No** - Disallows tape media export for the storage domain.

Note: This setting only applies to tape media.

When a tape cartridge export occurs, a message displays in the BlackPearl user interface, and is also emailed to the system administrator. The system administrator **must** be configured to receive emails with both Informational and Warning message severity to be notified when tape media is exported. This allows the administrator to retrieve the tape media when it is exported. Do not leave tape media in the library Entry/Exit port for long periods of time.

See Tape Export Best Practices on page 1 for more information.

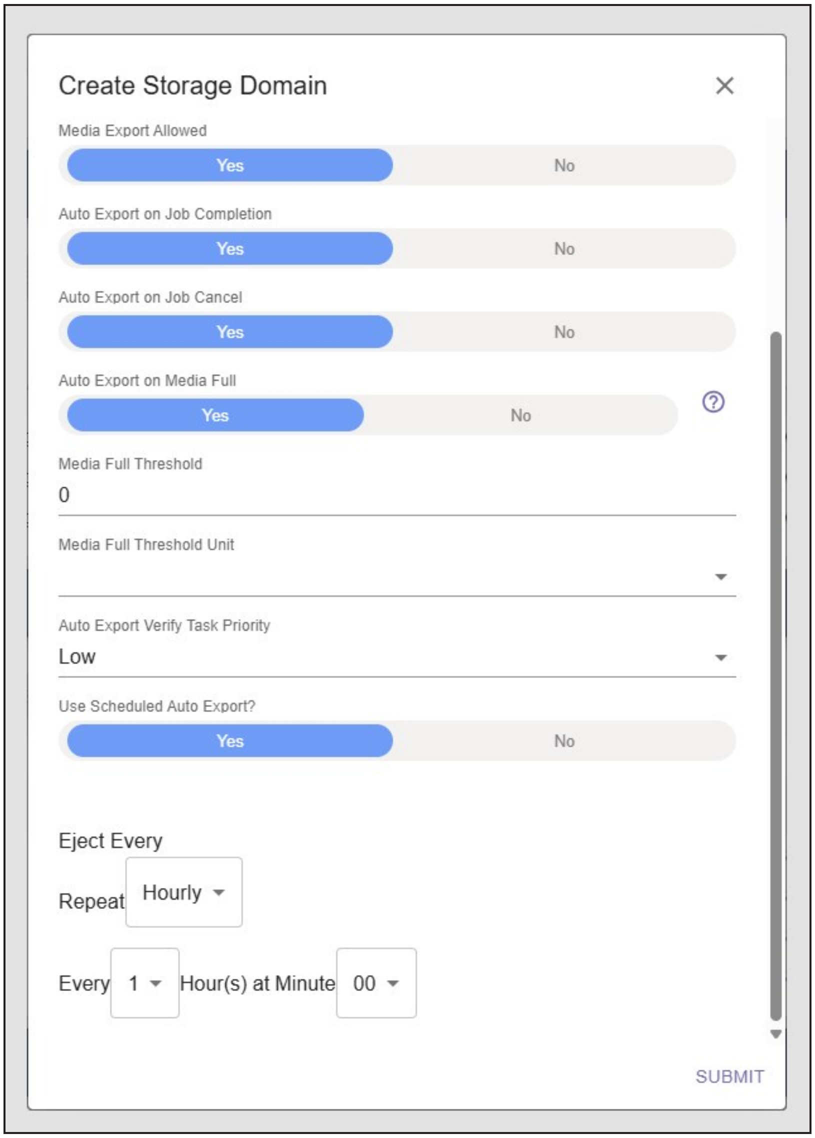
Note: By configuring email alerts, the user is also notified when a GET job is requesting an object from exported tape media, so it can be imported into the library to complete the GET job.

IMPORTANT It is important to not export tape media from the library directly. The BlackPearl Object Gateway controls the movement of media in the library.

9. Do one of the following:

- If you did not enable media export, skip to Step 14 on page 124.
- If you select to allow media export, continue with the following steps:

10. Use the **Auto Export** sliders to configure the behavior for auto exporting media:



Create Storage Domain

Media Export Allowed: Yes

Auto Export on Job Completion: Yes

Auto Export on Job Cancel: Yes

Auto Export on Media Full: Yes

Media Full Threshold: 0

Media Full Threshold Unit:

Auto Export Verify Task Priority: Low

Use Scheduled Auto Export?: Yes

Eject Every

Repeat: Hourly

Every 1 Hour(s) at Minute 00

Figure 56 The Create Storage Domain dialog box with Media Export options displayed.

- **Auto Export on Job Completion** — Enable this option to have the Gateway automatically export tape(s) when a job completes. This option is helpful if you plan to write a single job to tape and want to retrieve the media shortly after the job completes for secure archival or transfer of data to another tape library or BlackPearl Object Gateway.

- **Auto Export on Job Cancel** — Enable this option to have the Gateway automatically export tape(s) when a user cancels a job. This option is helpful if you do not want append the next job to a partially filled tape.
- **Auto Export on Media Full** — Enable this option to have the Gateway automatically export tape(s) when a tape is full. This option is helpful to maximize the amount of data stored on tape media.
  - If you select **Auto Export on Media Full**, you can optionally configure the **Media Full Threshold**, which determines when the Gateway marks a piece of media as full, and queues the piece of media for export.
  - Enter a numerical value of data units for the **Medial Full Threshold**, and use the **Media Full Threshold Unit** drop-down menu to select a data size unit for the threshold value.

11. Use the **Auto Export Verify Task Priority** drop-down menu to select a task priority for tapes to be verified when they are automatically exported. Selecting **None** means that the Gateway does not verify tapes before exporting them.
12. Use the **Scheduled Auto Export** slider to select one of the following:
    - **Yes** - The system automatically exports all tape media on a set schedule. This option is helpful if you need to move all tape media to off-site archival physical storage on a set schedule, regardless of the storage capacity remaining on the tape cartridges.
    - **No** - Tapes are not exported on a schedule and must be manually exported. Skip to Step 14 on page 124.

Note: **Scheduled Auto Export** operates independently from the condition-based auto export options.

For example, if you select to have tape media auto export when full, the Gateway exports a tape cartridge when it meets the media full threshold. Additionally, when the scheduled auto export time is met, the Gateway exports **all** tape cartridges, regardless of whether they have reached the media full threshold.

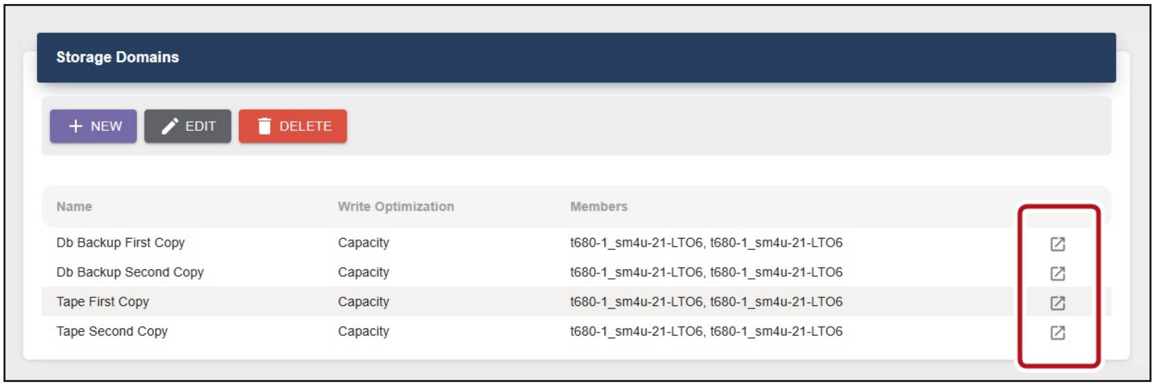
13. Use the **Repeat** drop-down menu to select one of the following:
    - Select **Hourly** and use the **Hours** and **Minute** drop-down menus to select values for **Every _ Hours at Minute _**. These values specify the interval in hours between ejecting tapes, and the number of minutes after the top of the hour when the job starts. For example, if the values are set to 4 and 15, tapes are ejected every four hours, at 15 minutes after the hour.
    - Select **Daily** and enter a value for **Every** to specify the interval, in days, between generating ejecting tapes. Then use the **Hour** and **Minute** drop-down menus to specify the time of day to start the export job.
    - Select **Weekly** and use the **Every** drop-down menu to select one or more day(s) of the week on which to generate a backup. Then use the **Hour** and **Minute** drop-down menus to specify the time of day to start the export job.
14. Click **Submit**.

Add a Storage Domain Member to a Storage Domain

Once a storage domain is created, you must add storage domain members. Entire data partition/media type combinations are members of storage domains. When a bucket requires additional capacity, a single disk partition or tape cartridge is allocated out of the members to fulfill the capacity requirement.

Use the instructions in this section to add a storage domain member to a storage domain.

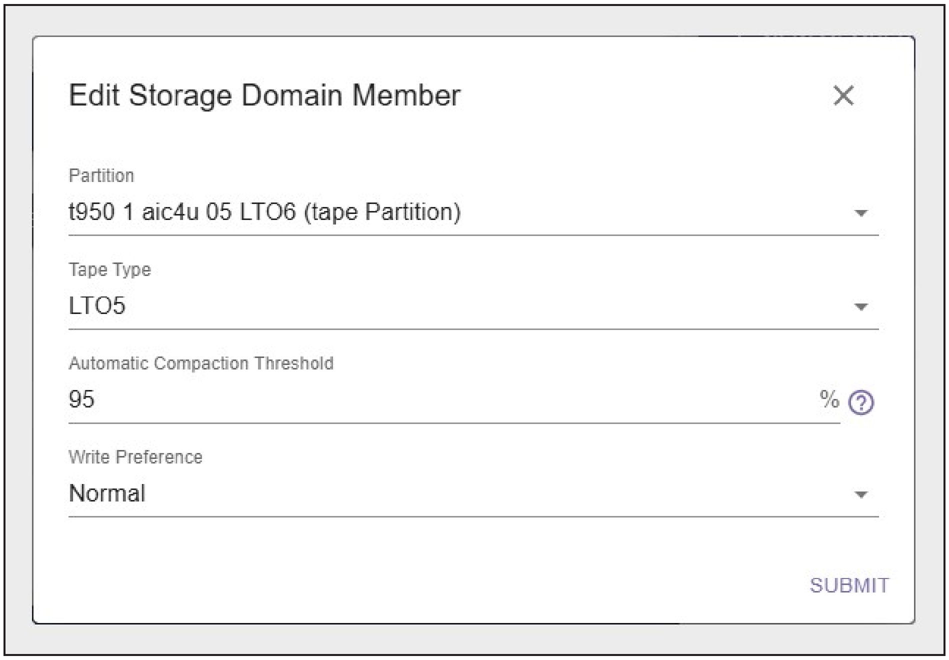
1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.
2. In the Storage Domains pane, click the **Details** button on the row of the storage domain to which you want to add a member.



Name	Write Optimization	Members	
Db Backup First Copy	Capacity	t680-1_sm4u-21-LTO6, t680-1_sm4u-21-LTO6	⧉
Db Backup Second Copy	Capacity	t680-1_sm4u-21-LTO6, t680-1_sm4u-21-LTO6	⧉
Tape First Copy	Capacity	t680-1_sm4u-21-LTO6, t680-1_sm4u-21-LTO6	⧉
Tape Second Copy	Capacity	t680-1_sm4u-21-LTO6, t680-1_sm4u-21-LTO6	⧉

Figure 57 The Buckets Screen - Storage Domain pane - Details button.

3. On the storage domain details screen, click **New Member**. The Edit Storage Domain Member dialog box displays.


Edit Storage Domain Member

Partition
t950 1 aic4u 05 LTO6 (tape Partition)

Tape Type
LTO5

Automatic Compaction Threshold
95 %

Write Preference
Normal

Figure 58 The Edit Storage Domain Member dialog box.

4. Use the **Partition Name** drop-down menu to select a tape or disk partition from the list of previously created partitions.

Note: You cannot add a disk partition to a storage domain that already uses a tape partition, and you cannot add a tape partition to a storage domain that already uses a disk partition.

5. Use the **Tape Type** drop-down menu to select the media type for a tape partition.

Notes:

- You must select the media type that matches the media present in the tape library partition. If the partition contains multiple generations of media, select the highest generation that is present in the library.
- This option does not display if you selected a disk partition in Step 4.

6. Enter a percentage for the **Automatic Compaction Threshold**. Automatic compaction occurs when the percentage of deleted objects on a tape cartridge exceeds this value. The default percentage is 95.

Note: If you selected a disk partition in Step 4, this setting is unavailable.

7. Use the **Write Preference** drop-down menu to select the write preference for this member of the storage domain. This setting determines the preferred usage of the partition when additional capacity is needed. The Gateway uses a partition with **High** write preference before a partition with **Normal** write preference, and so on. Use **Never Select** to indicate that a partition is read-only.

8. Click **Submit**.

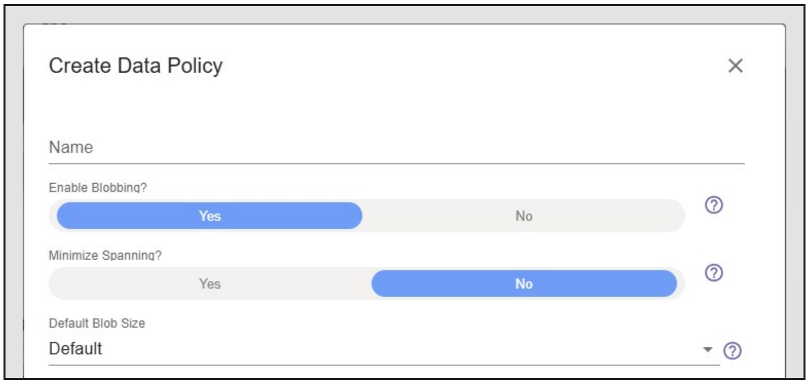
Create a Data Policy

A data policy defines data integrity policies, default job attributes, and persistence and replication rules, which define where data is written and for how long it is kept. A data policy may be used by multiple buckets, but a bucket uses precisely one data policy.

IMPORTANT It is difficult and time consuming to change a data policy once the Gateway writes data to a bucket using the data policy. Make sure that you understand the Advanced Bucket Management concepts and have thoughtfully planned your data policies before you start using the BlackPearlGateway to store data.

Use the instructions in this section to create a new data policy.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.
2. In the Data Policies pane, click **New**. The New Data Policy dialog box displays.



Create Data Policy

Name

Enable Blobbing? Yes / No (Yes selected)

Minimize Spanning? Yes / No (No selected)

Default Blob Size: Default

Figure 59 The Create Data Policy dialog box - Options.

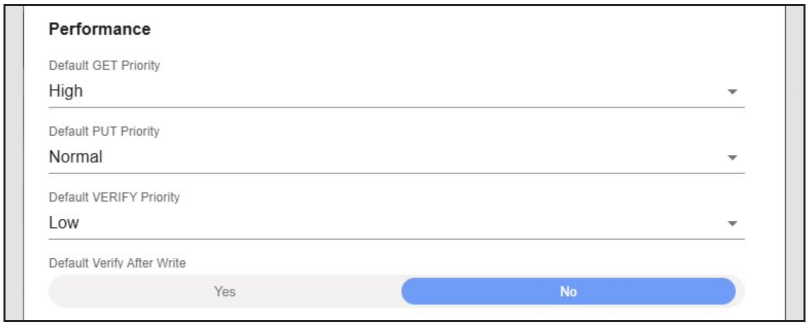
3. Enter a **Data Policy Name** for the new data policy.
4. Use the **Enable Blobbing** slider to select one of the following:
   - Click **Yes** to enable blobbing. When enabled this setting allows an object to be broken into multiple blobs. Blobbing must be enabled to handle objects larger than 1 TB, to use multi-part upload, or to break up an object into multiple blobs.
   - Click **No** to disable blobbing. If disabled, an object must be exactly one blob. Disabling blobbing guarantees that an object will never span multiple tapes or disk pools, since a blob cannot span multiple media.

5. Use the **Minimize Spanning** slider to select one of the following:
    - Click **Yes** to enable minimize spanning. When enabled, the BlackPearl Object Gateway increases the chunk size to 1 TB and always keeps one chunk on a single tape regardless of the capacity/performance write mode configured for the storage domain. For jobs larger than 1 TB, multiple chunks are used for the job and the Gateway uses the configured capacity/performance write mode for the storage domain, where different chucks may transfer to different tapes. Jobs smaller than 1 TB never span media.
    - Click **No** to disable minimize spanning. When disabled, the BlackPearl Object Gateway uses the default chunk size of 64 GiB or 100 GiB (depending on tape media generation). Multiple chunks are used for jobs and may span multiple tapes depending on the configured capacity/performance write mode for the storage domain.

Note: Enabling this option can adversely affect capacity utilization and performance.

6. Use the **Default Blob Size** drop-down menu to set size for when objects are split into multiple blobs. The default size is 64 GB. If you are using a Partial File Restore (PFR) application with the BlackPearl Object Gateway, setting this value to 8 GB may improve performance.

IMPORTANT If you are not using PFR software, Spectra Logic recommends leaving this setting at the default value of 64 GB.



Performance

Default GET Priority: High

Default PUT Priority: Normal

Default VERIFY Priority: Low

Default Verify After Write: Yes [✓ No]

Figure 60 The New Data Policy dialog box - Performance.

7. Select the **Performance** characteristics for the data policy. Each priority determines the resources assigned and the processing order.

IMPORTANT Jobs with priority **Urgent** can use up all of the resources and prevent other jobs from making progress. Use this priority sparingly.

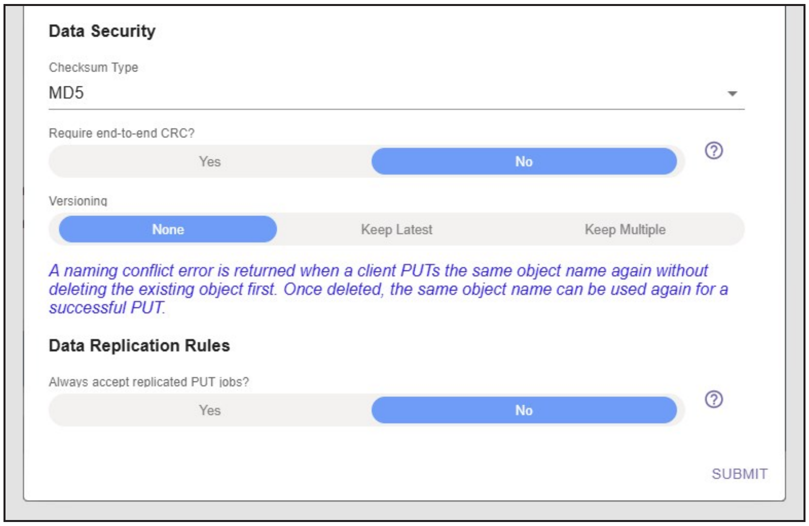
    a. Use the drop-down menu to select the **Default GET Priority**.
    b. Use the drop-down menu to select the **Default PUT Priority**.
    c. Use the drop-down menu to select the **Default VERIFY Priority**.

8. Use the **Default Verify After Write** slider to select of the following:
   - Click **Yes** to enable the feature. When enabled, the BlackPearl Object Gateway always performs a verification of data after it is written.
   - Click **No** to disable the feature. When disabled, a client must specify to verify data after it is written when creating a PUT job.

Notes:
- After the PUT job completes, the tape remains in the drive during data verification.
- Only the data just written by the PUT job is verified.
- Data verification after write uses the checksum type specified in Step 9.
- This verification does not update the **Last Verified** field on the tape details screen.
- Enabling **Default Verify After Write** reduces Gateway write throughput by up to 50%.
- This setting does not apply to replication targets.

9. Use the **Checksum Type** drop-down menu to specify the type of checksum used for data integrity verification, verification after write, and end-to-end CRC.

Notes:
- CRC, MD5, and SHA-512 perform the best for their corresponding cryptographic strengths on the BlackPearl Object Gateway.
- Using SHA-256 and SHA-512 reduces single stream performance and may reduce throughput capabilities of the Gateway.



Data Security

Checksum Type: MD5

Require end-to-end CRC? Yes [✓ No]

Versioning: [✓ None] Keep Latest Keep Multiple

A naming conflict error is returned when a client PUTs the same object name again without deleting the existing object first. Once deleted, the same object name can be used again for a successful PUT.

Data Replication Rules

Always accept replicated PUT jobs? Yes [✓ No]

Figure 61 The New Data Policy dialog box - Data Security.

10. Use the **Require end-to-end CRC** slider to select one of the following:
    - Click **Yes** to enable the feature. When enabled, the BlackPearl Object Gateway enforces that every blob sent to the system include a checksum calculated by the client-side.
    - Click **No** to disable the feature. When disabled, the BlackPearl Object Gateway does not require a client-side checksum.

11. Use the **Versioning** slider to select one of the following:

Option	Description
None	Only one version of an object may exist at any time and the version number of the object is always 1.
Keep Latest	Only one version of the data is available at a time. When a new version of an object is written, the old version is retained until the new version is fully written in compliance with the data policy, and then the old version is deleted. **Note:** The **Keep Latest** setting requires that the PUT job for the earlier version of the object complete before the PUT of the latest version of the object with the same name in order for the PUT job to succeed. **Note:** You cannot assign a Storage Domain configured with the LTFS option set to **Object Name** when using the **Keep Latest** setting.
Keep Multiple Versions	When a new version of an object is written, it is added as the latest version of the object. Any previous versions of the object, up to the value specified in **Number of Versions**, are retained and accessible. **Note:** You cannot assign a Storage Domain configured with the LTFS option set to **Object Name** when using the **Keep Multiple Versions** setting. **IMPORTANT** If you select **Keep Multiple Versions**, you are not able to change this setting after the data policy is created. **CAUTION** If you select **Keep Multiple Versions**, if the PUT of the earlier version is not complete before the PUT of the latest version, the BlackPearlGateway believes the latest version to be the same object as the earlier version and rejects it, and only the earlier version is retained.

12. Use the **Always Accept Replicated PUT Jobs** slider to select one of the following:

- Click **Yes** to enable the feature. When enabled, all PUT jobs using this data policy are created even when one or more replication targets are unavailable, or if there are global issues that would likely prevent the completion of a job.
- Click **No** to disable the feature. When disabled, the system accepts replicated put jobs only if it is currently able to replicate data to the target. If you are not using data replication, click **No**.

IMPORTANT Using this parameter is discouraged, and using it for jobs on both the source and target Gateways at the same time is extremely discouraged. Running jobs on both Gateways when they are not able to communicate with each other can create replication conflicts that must be manually resolved

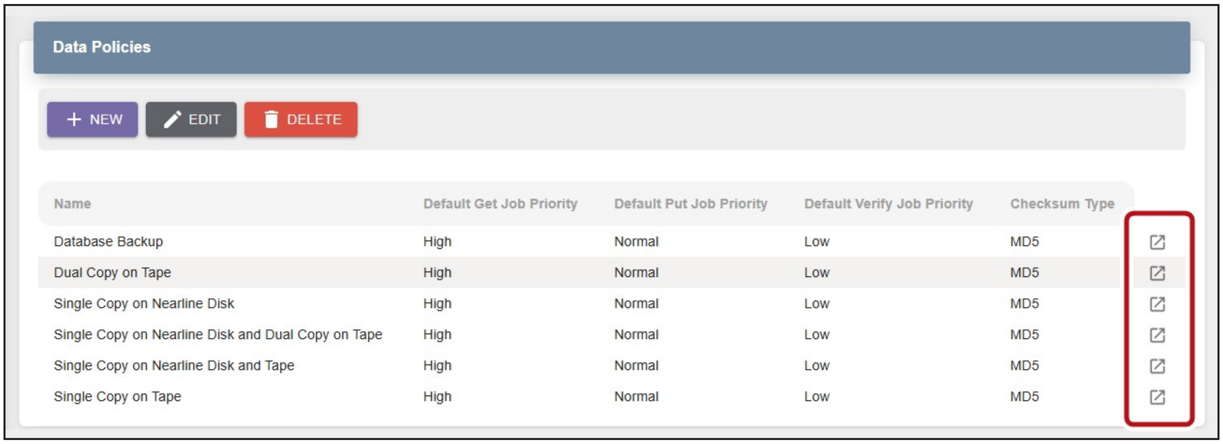
13. Click **Submit**.

Add a Data Persistence Rule to a Data Policy

Once a data policy is created, you must add one or more persistence rules. A persistence rule is either permanent, meaning that data is kept in the specified storage domain at all times, or temporary, meaning that data is kept in the specified storage domain under certain circumstances, and then it can be deleted from that storage domain. A data policy must include at least one permanent persistence rule.

Existing permanent and temporary persistence rules, and replication rules, may be retired so that the rule is not applied for any new incoming data, but will continue to retain data previously written.

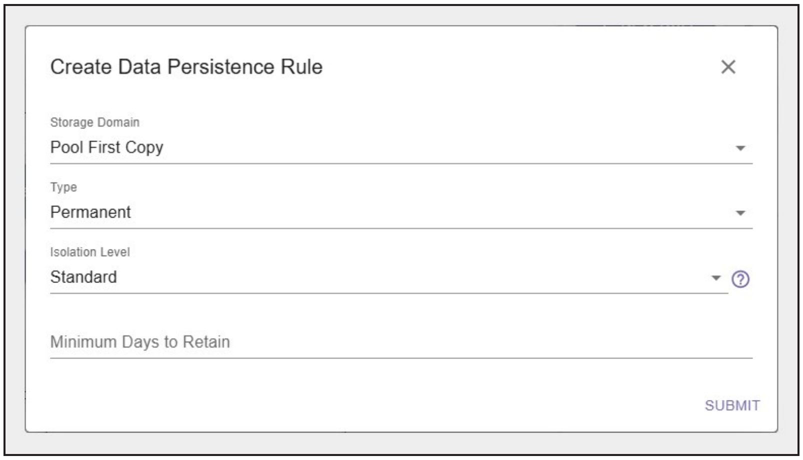
1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.
2. In the Data Policies pane, select the data policy and click the **Details** button.



Name	Default Get Job Priority	Default Put Job Priority	Default Verify Job Priority	Checksum Type
Database Backup	High	Normal	Low	MD5
Dual Copy on Tape	High	Normal	Low	MD5
Single Copy on Nearline Disk	High	Normal	Low	MD5
Single Copy on Nearline Disk and Dual Copy on Tape	High	Normal	Low	MD5
Single Copy on Nearline Disk and Tape	High	Normal	Low	MD5
Single Copy on Tape	High	Normal	Low	MD5

Figure 62 The Buckets Screen - Data Policies pane - Details button.

3. Select **Data Persistence > New Rule**. The Create Data Persistence Rule dialog box displays.



Storage Domain: Pool First Copy

Type: Permanent

Isolation Level: Standard

Minimum Days to Retain

Figure 63 The Create Data Persistence Rule dialog box.

4. Use the **Storage Domain** drop-down menu to select a storage domain from the list of previously created storage domains.

5. Use the **Type** drop-down menu to select whether the data persistence rule to use for the for the storage domain is **Temporary** or **Permanent**.

   - **Temporary** - The data is kept in the specified storage domain under certain circumstances, and then it can be deleted from that storage domain.
   - **Permanent** - The data is kept in the specified storage domain at all times.

Notes:

- The **Temporary** setting cannot be used for a storage domain that targets a tape library.
- When importing data, a **Temporary** persistence rule does not trigger copying data to a disk pool unless the data is staged with IOM (Intelligent Object Management) active and running. See Intelligent Object Management (IOM) on page 417 for information on IOM.
- You cannot create a Data Persistence Rule with a setting of **Retired**. Existing persistence rules can be modified to be retired. See Manage a Data Policy on page 1.

6. Use the **Isolation Level** drop-down menu to select the level of physical isolation required for the storage domain.

   - **Standard** — This allows data from different buckets to reside on the same physical media, and may provide increased performance. This setting is recommended data policies configured to use disk storage.
   - **Bucket Isolated** — Data from different buckets cannot be mixed on the same physical storage media.

Notes:

- The **Standard** isolation level provides the best capacity utilization and overall performance.
- **Bucket Isolated** allocates an entire disk pool to a bucket when needed. Allocating an entire disk pool to a bucket may use up resources quickly and is not recommended.

7. Enter the **Minimum Days to Retain** to specify the minimum number of days the Gateway should retain data written using a temporary persistence rule.

Notes:

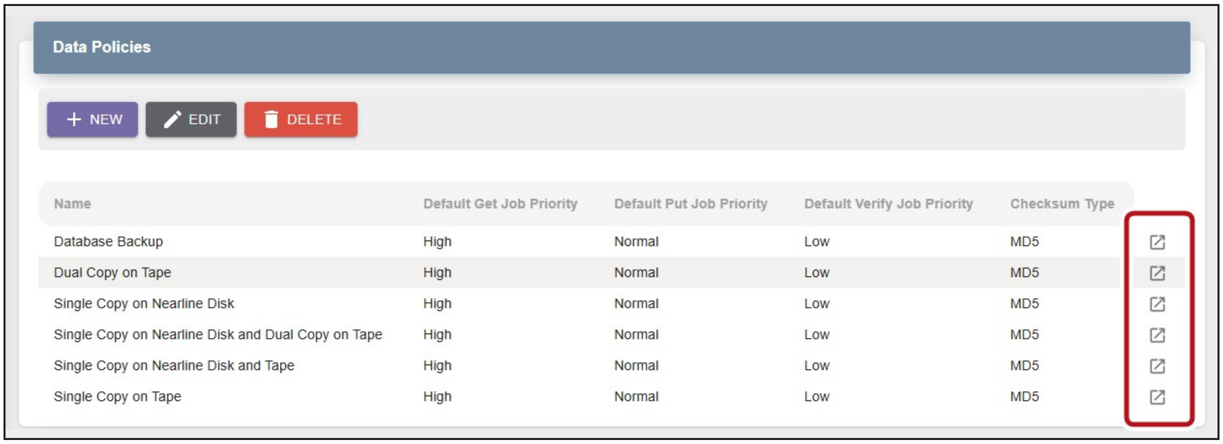
- The **Minimum Days to Retain** for a persistence rule targeting a storage domain using a nearline pool (a 77-bay, 96-bay, or 107-bay expansion node) must be 90 days or greater.
- **Minimum Days to Retain** cannot be specified when using a **Type** of **Permanent**.

8. Click **Submit**.

Create Data Policy ACLs

Use the instruction in this section to create a new data policy ACL for a group or user.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.
2. In the Data Policies pane, select the data policy and click the **Details** button.



Name	Default Get Job Priority	Default Put Job Priority	Default Verify Job Priority	Checksum Type
Database Backup	High	Normal	Low	MD5
Dual Copy on Tape	High	Normal	Low	MD5
Single Copy on Nearline Disk	High	Normal	Low	MD5
Single Copy on Nearline Disk and Dual Copy on Tape	High	Normal	Low	MD5
Single Copy on Nearline Disk and Tape	High	Normal	Low	MD5
Single Copy on Tape	High	Normal	Low	MD5

Figure 64 The Buckets Screen - Data Policies pane - Details button.

3. Click **Access Control List**.
4. Click **Add Group ACL** or **Add User ACL** to add the desired group or user. The Add Access Control List dialog box displays.

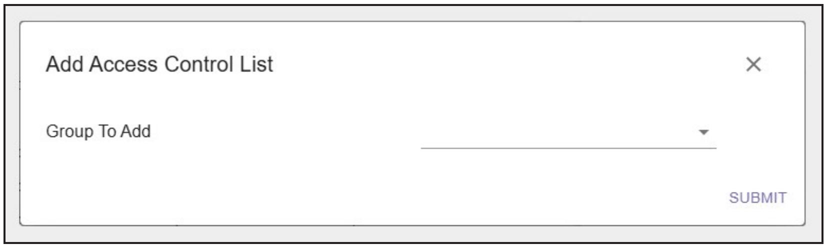


Figure 65 The Add Access Control List dialog box (Group to Add shown).

5. Use the **Group to Add** or **User to Add** drop-down menu to select the group or user to be assigned to the data policy ACL.
6. Click **Submit**.

Add a Data Replication Rule to a Data Policy

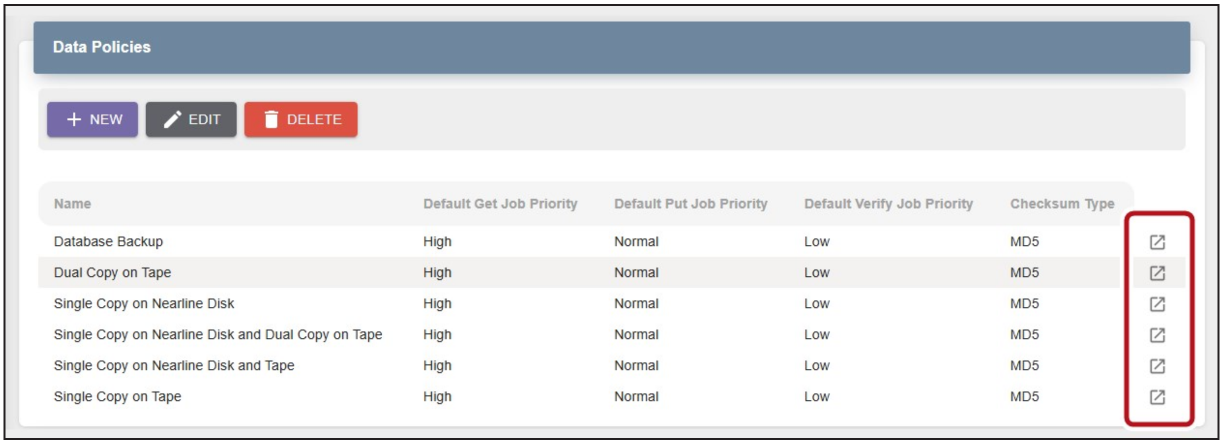
Use the links below to configure the desired data replication rule.

- Add a BlackPearl Data Replication Rule to a Data Policy on the next page
- Add an S3 Data Replication Rule to a Data Policy on page 135
- Add an Azure Data Replication Rule to a Data Policy on page 137

Add a BlackPearl Data Replication Rule to a Data Policy

A BlackPearl replication target must be configured before adding a BlackPearl Data Replication Rule to the data policy. See Create a Replication Target on page 141.

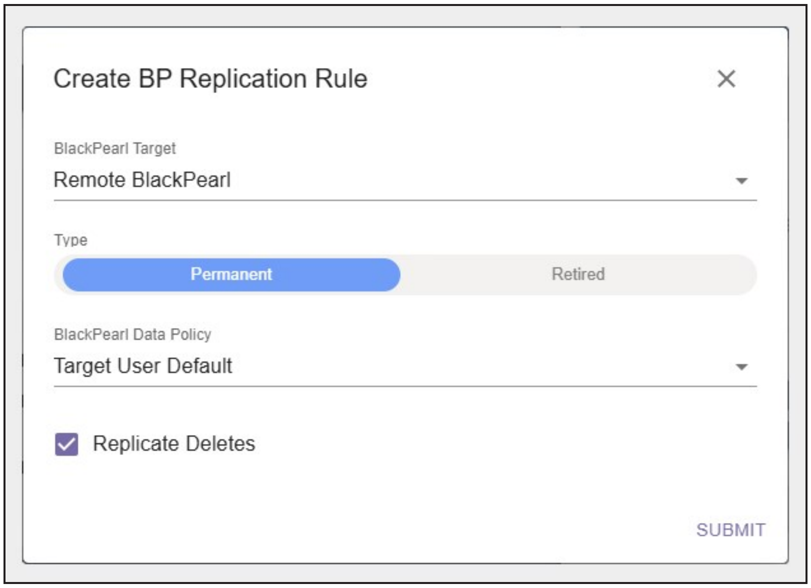
1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.
2. In the Data Policies pane, select the data policy and click the **Details** button.



Name	Default Get Job Priority	Default Put Job Priority	Default Verify Job Priority	Checksum Type	
Database Backup	High	Normal	Low	MD5	↗
Dual Copy on Tape	High	Normal	Low	MD5	↗
Single Copy on Nearline Disk	High	Normal	Low	MD5	↗
Single Copy on Nearline Disk and Dual Copy on Tape	High	Normal	Low	MD5	↗
Single Copy on Nearline Disk and Tape	High	Normal	Low	MD5	↗
Single Copy on Tape	High	Normal	Low	MD5	↗

Figure 66 The Buckets Screen - Data Policies pane - Details button.

3. On the details screen, click **Replication**.
4. In the BlackPearl Data Replication Rules pane, click **Add Rule**. The Create BlackPearl Replication Rule dialog box displays.


Create BP Replication Rule

BlackPearl Target: Remote BlackPearl

Type: Permanent | Retired

BlackPearl Data Policy: Target User Default

☑ Replicate Deletes

Figure 67 The Create BlackPearl Replication Rule dialog box.

5. Use the **BlackPearl Target** drop-down menu to select a replication target from the list of previously created replication targets.

6. Use the **Type** slider to select whether the data persistence rule to use for the for the storage domain is **Permanent** or **Retired**.

Note: You cannot create a replication rule as **Retired**. You can only modify a rule from permanent to retired after the data policy is created.

7. Use the **BlackPearl Data Policy** drop-down menu to select the data policy on the target BlackPearl Object Gateway to use when creating the bucket for replicated data. Alternatively, select **Target User Default** to use the default data policy configured on the target.
8. Select or clear the **Replicate Deletes** checkbox. When selected, any time a replicated file is deleted from the source Gateway, it is also deleted from the target Gateway.

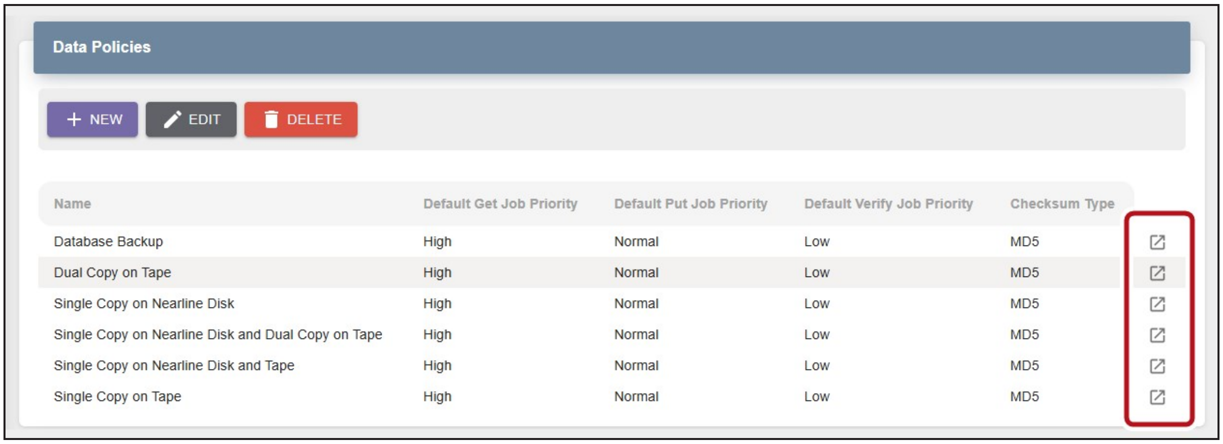
Note: Replicated objects do not immediately delete. Objects are only deleted after running a verify operation on the bucket.

9. Click **Submit**.

Add an S3 Data Replication Rule to a Data Policy

An Amazon S3 replication target must be configured before adding an Amazon S3 Data Replication Rule to the data policy. See Create a Replication Target on page 141.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.
2. In the Data Policies pane, select the data policy and click the **Details** button.

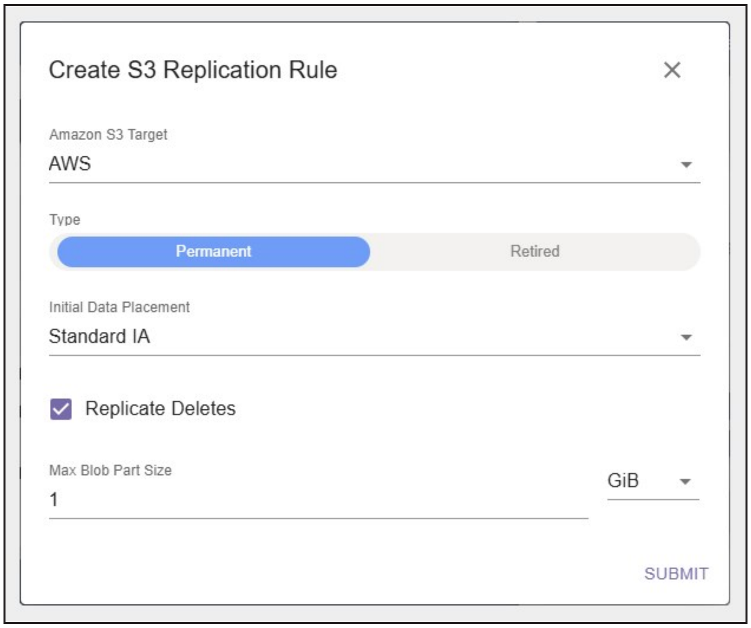


Name	Default Get Job Priority	Default Put Job Priority	Default Verify Job Priority	Checksum Type	
Database Backup	High	Normal	Low	MD5	↗
Dual Copy on Tape	High	Normal	Low	MD5	↗
Single Copy on Nearline Disk	High	Normal	Low	MD5	↗
Single Copy on Nearline Disk and Dual Copy on Tape	High	Normal	Low	MD5	↗
Single Copy on Nearline Disk and Tape	High	Normal	Low	MD5	↗
Single Copy on Tape	High	Normal	Low	MD5	↗

Figure 68 The Buckets Screen - Data Policies pane - Details button.

3. On the details screen, click **Replication**.

4. In the S3 Data Replication Rules pane, click **Add Rule**. The Create S3 Replication Rule dialog box displays.



Create S3 Replication Rule

Amazon S3 Target
AWS

Type
Permanent | Retired

Initial Data Placement
Standard IA

☑ Replicate Deletes

Max Blob Part Size
1 GiB

Figure 69 The Create S3 Replication Rule dialog box.

5. Use the **Amazon S3 Target** drop-down menu to select an Amazon S3 replication target from the list of previously created replication targets.

6. Use the **Type** slider to select whether the data persistence rule to use for the for the storage domain is **Permanent** or **Retired**.

Note: You cannot create a replication rule as **Retired**. You can only modify a rule from permanent to retired after creating the replication rule.

7. Use the **Initial Data Placement** drop-down menu to select the storage class for any objects transferred to the AWS S3 instance.

   - **Standard** — Provides high availability and performance for frequently accessed data.
   - **Reduced Redundancy** — Provides storage of objects on multiple devices across multiple facilities, but does not replicate objects as many times as Amazon S3 standard storage. The lower level of redundancy results in less durability and availability, but also lower storage costs.
   - **Standard IA** (default) — Provides fast access to less frequently accessed data.
   - **Glacier** — Provides secure, long-term archive for rarely accessed data.
   - **Glacier Deep Archive** — Provides a low-cost, secure long-term archive for data that does not require quick retrieval.

Notes:

- The BlackPearlObjectGateway uses "standard" restore for objects archived to Glacier and Glacier Deep Archive storage classes. Restore times are approximately 3-5 hours for Glacier, and 12 hours for Glacier Deep Archive, plus object download time.

- If you are configuring the replication to target a bucket that was previously created using the Amazon AWS interface, you must define a Lifecycle Management Rule in AWS to migrate data from the bucket default tier to the preferred tier, if necessary. Spectra Logic recommends using an immediate (0 days) move rule.

8. Select or clear the **Replicate Deletes** checkbox. When selected, any time a replicated file is deleted from the source Gateway, it is also deleted from the target.
9. If desired, modify the **Max Blob Part Size**. This parameter defines the maximum object part size used when sending data to an Amazon S3 target. Larger blob sizes make public cloud workflows simpler, but may make it more difficult or impossible to reliably transmit blobs. Less reliable network connections to the public cloud require smaller blob sizes. The maximum blob size is 1 TB. The default maximum blob part size is 1 GiB.

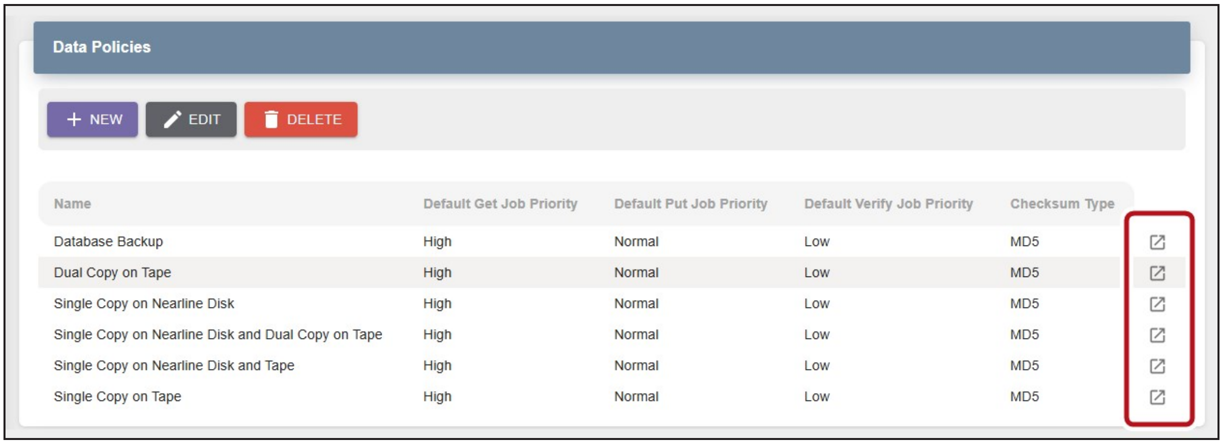
Note: To prevent data transfer failures, it is important that this value not exceed the maximum blob size that the target is able to accept.

10. Click **Submit**.

Add an Azure Data Replication Rule to a Data Policy

A Microsoft Azure replication target must be configured before adding an Azure Data Replication Rule to the data policy. See Create a Replication Target on page 141.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.
2. In the Data Policies pane, select the data policy and click the **Details** button.

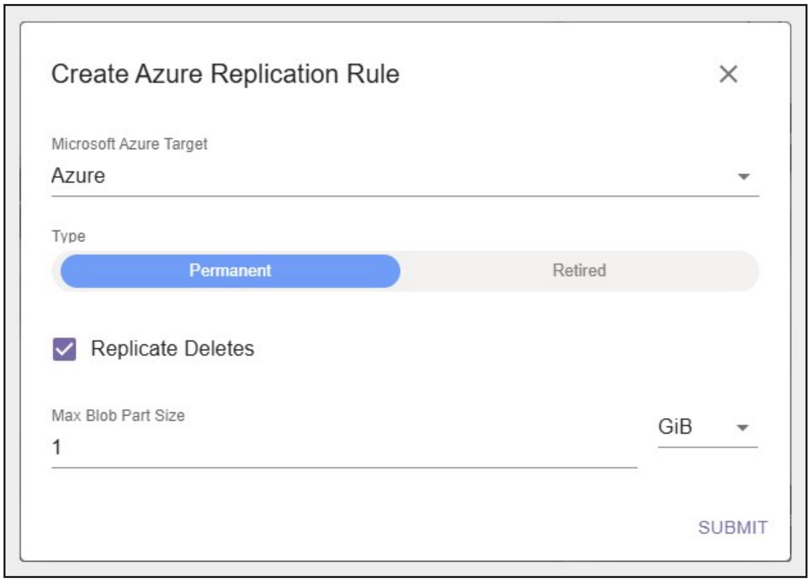


Name	Default Get Job Priority	Default Put Job Priority	Default Verify Job Priority	Checksum Type
Database Backup	High	Normal	Low	MD5
Dual Copy on Tape	High	Normal	Low	MD5
Single Copy on Nearline Disk	High	Normal	Low	MD5
Single Copy on Nearline Disk and Dual Copy on Tape	High	Normal	Low	MD5
Single Copy on Nearline Disk and Tape	High	Normal	Low	MD5
Single Copy on Tape	High	Normal	Low	MD5

Figure 70 The Buckets Screen - Data Policies pane - Details button.

3. On the details screen, click **Replication**.

4. In the Azure Data Replication Rules pane, click **Add Rule**. The Create Azure Replication Rule dialog box displays.



Create Azure Replication Rule

Microsoft Azure Target: Azure

Type: Permanent

☑ Replicate Deletes

Max Blob Part Size: 1 GiB

Figure 71 The Create Azure Replication Rule dialog box.

5. Use the **Microsoft Azure Target** drop-down menu to select a Microsoft Azure replication target from the list of previously created replication targets.

6. Use the **Type** slider to select whether the data persistence rule to use for the for the storage domain is **Permanent** or **Retired**.

Note: You cannot create a replication rule as **Retired**. You can only modify a rule from permanent to retired after creating the replication rule.

7. Select or clear the **Replicate Deletes** checkbox. When selected, any time a replicated file is deleted from the source Gateway, it is also deleted from the target.

Note: Replicated objects do not immediately delete. Objects are only deleted after running a verify operation on the bucket.

8. If desired, modify the **Max Blob Part Size**. This parameter defines the maximum object part size used when sending data to a Microsoft Azure target. Larger blob sizes make public cloud workflows simpler, but may make it more difficult or impossible to reliably transmit blobs. Less reliable network connections to the public cloud require smaller blob sizes. The maximum blob size is 1 TB. The default maximum blob size is 1 GiB.

Note: To prevent data transfer failures, it is important that this value not exceed the maximum blob size that the target is able to accept.

9. Click **Submit**.

CREATE A BUCKET

Buckets are data transfer targets for read and write operations. The Gateway stages data written to it on the cache and optimizes how it writes buckets to storage domains for best performance.

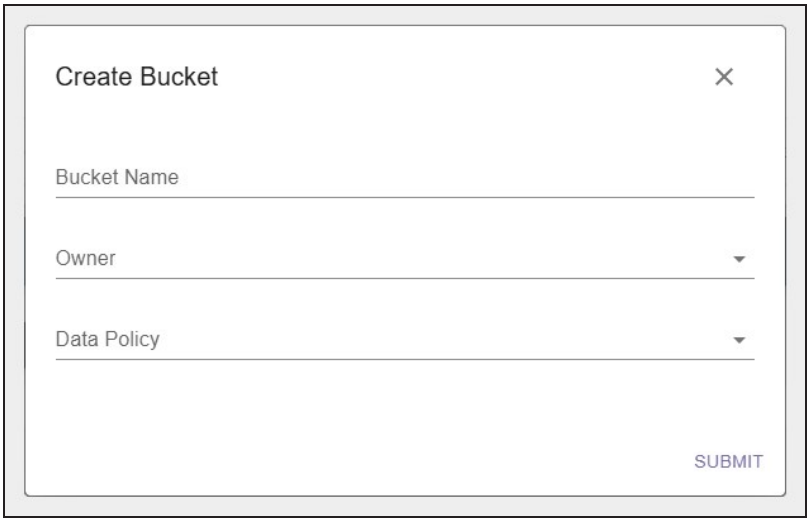
Clients write data to the Gateway using a "bulk PUT" command, and read from the Gateway with a "bulk GET" command. For more information on using these commands see the *Spectra BlackPearl DS3 API Reference*.

Note: Buckets can also be created using a DS3 client, the DS3 API, or by using the BlackPearl embedded dashboard in the Spectra Vail, StorCycle, or Rio MediaEngine software applications.

IMPORTANT If you are creating a bucket that is to be used in a BlackPearl replication configuration, you must create the bucket on the source Gateway and the target Gateway using identical names, or replication fails.

Use the instructions in this section to configure a bucket.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.
2. In the Buckets pane, click **Create**. The Create Bucket dialog box displays.



Create Bucket

Bucket Name

Owner

Data Policy

Figure 72 The Create Bucket dialog box.

3. Enter a **Bucket Name**.

IMPORTANT	When creating a bucket for use with an Amazon S3 or Microsoft Azure replication target, the bucket name must adhere to the cloud target naming requirements. The BlackPearlGateway attempts to create the bucket on the replication target using the name entered in Step 3 with the appended Cloud Bucket Prefix and Suffix, if applicable. If the bucket name is incompatible with the naming requirements of the cloud target provider, bucket creation fails and an error message displays.

Notes:

- The bucket name can only contain letters, numbers, the period (.), dash (-), and underscore (_) characters.
- The bucket name cannot exceed 63 characters.

4. Use the **Owner** drop-down menu to select a user as the owner of the bucket from the list of users already created on the Gateway.
5. Use the **Data Policy** drop-down menu to select a data policy for the bucket from the list of previously created data policies on the Gateway. The bucket uses this data policy when transferring data.
6. Click **Submit**.

Create a Replication Target

Replication targets allow you to configure the BlackPearl Object Gateway to automatically replicate data to another BlackPearl Object Gateway, or to the Azure or Amazon S3 clouds.

Note: The instructions below describe configuring a target that is later associated with a data policy. For instructions on creating NAS replication, see Configure NAS Replication on page 169.

Create a BlackPearl Target

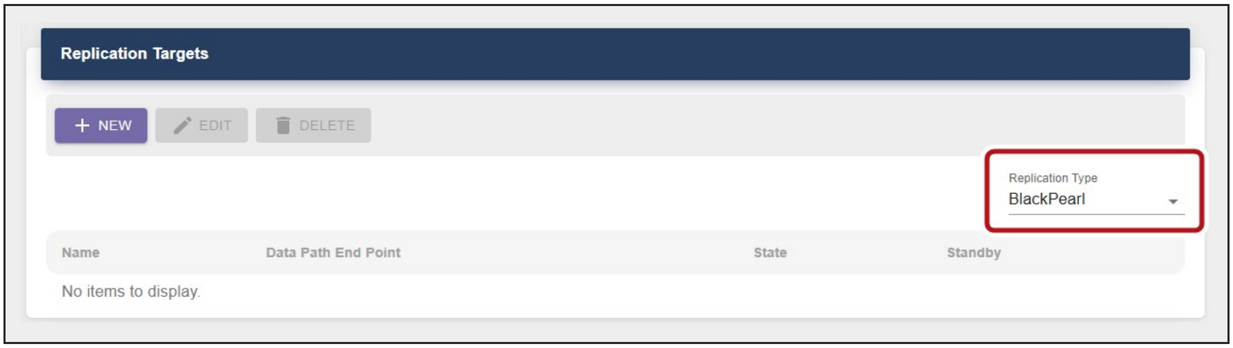
Configuring a BlackPearl target allows a data policy on one BlackPearl Object Gateway to replicate data to a second Gateway. With replication enabled, as soon as data is PUT to the cache of the source Gateway it begins replicating to the target Gateway. Storing multiple copies of the same data on different BlackPearl Object Gateways provides enhanced data security and disaster recovery if the source Gateway fails.

- If data is sent to a data policy that is not configured for replication, the data is not replicated to the target Gateway.
- When you delete data from the source Gateway, you can optionally specify to have the data deleted from the target Gateway as well.
- If the source BlackPearl Object Gateway uses object versioning but the target BlackPearl Object Gateway does not, when an object is deleted on the source Gateway, the delete is replicated to the target Gateway. However, when IOM validates the data on the two Gateways, it detects that the object still exists on the source Gateway, and self-heals the object on the target Gateway again.

IMPORTANT Spectra Logic recommends using the same versioning settings on both the source and target BlackPearl Gateways.

Use the instructions in this section to configure a BlackPearl target.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.
2. In the Data Policies pane, use the **Replication Type** drop-down menu to select **BlackPearl**.



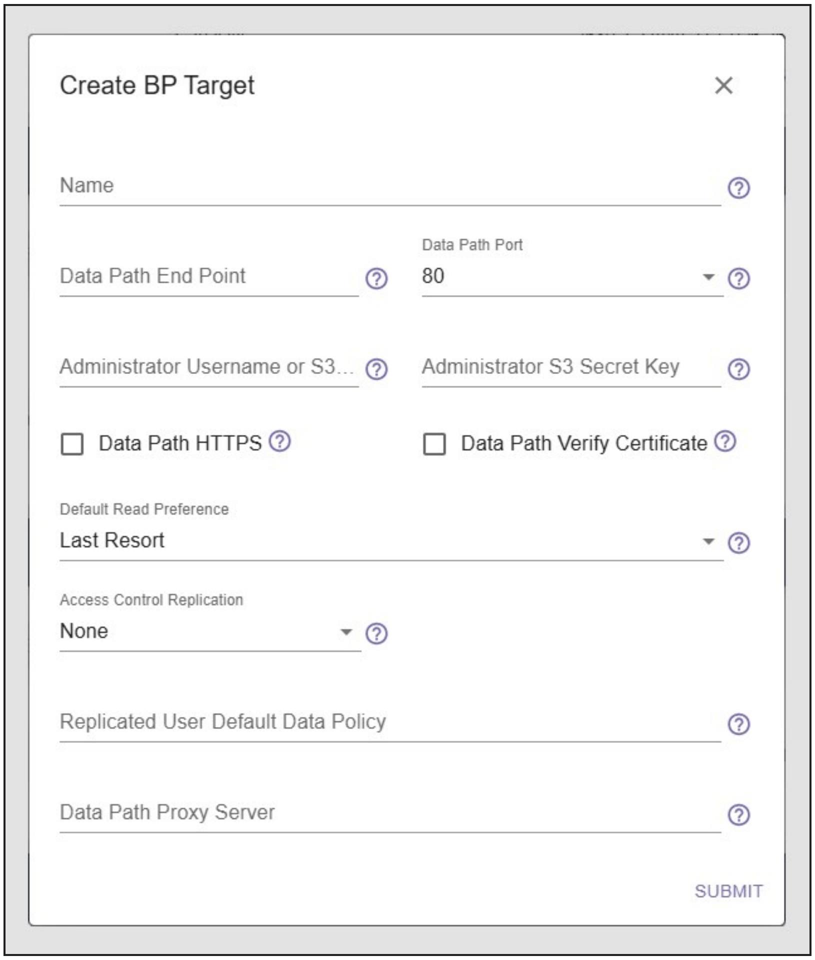
Replication Type: BlackPearl

Name	Data Path End Point	State	Standby

No items to display.

Figure 73 The Buckets Screen - Replication Targets pane - Replication Type menu.

3. In the Data Policies pane, click **New**. The Create BlackPearl Target dialog box displays.


Create BP Target
×
Name
Data Path End Point
Administrator Username or S3...
Administrator S3 Secret Key
☐ Data Path HTTPS
☐ Data Path Verify Certificate
Replicated User Default Data Policy
Data Path Proxy Server
SUBMIT

Data Path Port: 80

Default Read Preference: Last Resort

Access Control Replication: None

Figure 74 The Create BlackPearl Target dialog box.

4. Enter a **Name** for the BlackPearl target.

5. Enter the system name of the target Gateway, or the IP address of the target Gateway's data port, as the **Data Path End Point**.

Note: Do not use the IP address of the target Gateway's management port.

6. Use the **Data Path Port** drop-down menu to select a value for the port on which the target Gateway's S3 service is running.

Note: Port selections for secure transfer (443/8443) are displayed if you enable Data Path HTTPS in Step 9 below.

7. Enter the username or S3 Access ID of a user with administrator privileges on the target Gateway in the **Administrator Username or S3 Access ID** field.

Note: Administrator credentials are used to configure and maintain the source/target relationship. They are not used for user driven replication operations.

8. Enter the **Administrator S3 Secret Key** of the user you entered in Step 7.

9. Select the **Data Path HTTPS** checkbox to enable secure data transfer with the BlackPearl target. When this option is selected, the Data Path Port setting automatically changes to 443. Repeat Step 6 if you want to change the data path port to 8443.

IMPORTANT Using HTTPS for data transfer greatly impacts data transfer speed. Spectra Logic recommends leaving this disabled if it is not required for your data storage environment.

10. If desired, select **Data Path Verify Certificate** to fully validate the SSL certificate of the BlackPearl target. If the certificate is does not pass validation, it is not trusted.

IMPORTANT Do not enable this option if the BlackPearl target uses the default self-signed SSL certificate.

11. Use the **Default Read Preference** drop-down menu to configure the behavior when the system cannot read from the target. Data is normally read from the source Gateway whenever possible. This setting controls when data is read from the target Gateway if the source Gateway is not available.

Name	Description
Last Resort	The source Gateway only reads data from the target Gateway if the source Gateway cannot read from any of its own data partitions.
Minimum Latency	The source Gateway reads the data from the data partition with the least latency no matter if it is connected to the source Gateway or the target Gateway. For example, if the source Gateway only has the data on tape and the target Gateway has the data on pool, the data is read from the target pool. **Note:** Only use MINIMUM LATENCY when the network between the source and target is very inexpensive.
After Online Pool	The source Gateway only reads data from the target Gateway if the source Gateway cannot read from an online pool.
After Nearline Pool	The source Gateway only reads data from the target Gateway if the source Gateway cannot read from a nearline pool.
After Non-Ejectable Tape	The source Gateway only reads data from the target Gateway if the source Gateway cannot read from secure media.
Never	Data is never read from the target Gateway.

12. Use the **Access Control Replication** drop-down menu to configure the behavior of replicating access control information.

Name	Description
None	No access control information is replicated to the BlackPearl target. **Note:** The Administrator secret key on both the source and target BlackPearl Object Gateways must be identical when setting Access Control Replication to **None**.
Users	User creation, modification, and deletion is replicated to the BlackPearl target.

13. If you selected Users in Step 12, you can optionally enter the name of a data policy previously configured on the target Gateway to use as the **Replicated User Default Data Policy**. If configured, the Gateway uses this target data policy as the default data policy for any users replicated to the target.

14. Optionally, enter the IP address of the **Data Path Proxy Server**. If configured, the source Gateway uses the specified proxy to connect to the target Gateway.

15. Click **Submit**.

Create an Amazon S3 Target

Configuring an Amazon S3 target allows a data policy on the BlackPearl Object Gateway to replicate data to the Amazon S3 cloud. With replication enabled, as soon as data is PUT to the cache of the source Gateway it begins replication to the Amazon S3 cloud.

Note: Only Amazon Web Services (AWS) S3 is qualified as an Amazon S3 target. Other S3 services have not been tested.

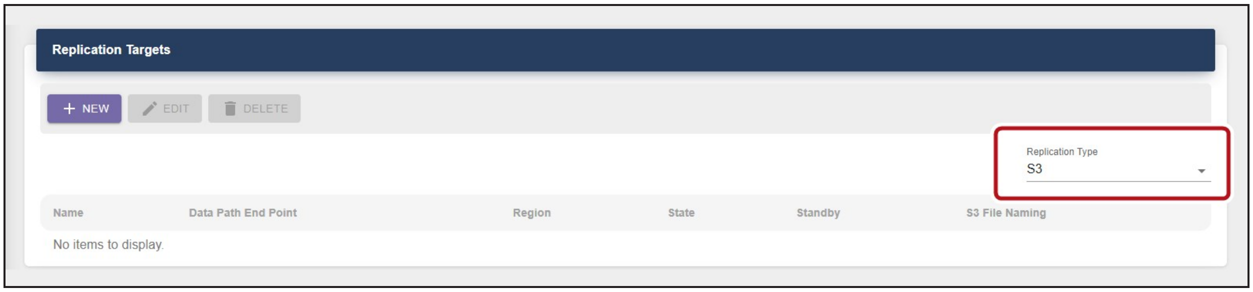
Restrictions

The following restrictions apply to creating an Amazon S3 target:

- You cannot create two Amazon S3 targets using the same Data Path End Point and Access Key.
- You cannot create two Amazon S3 targets using the same Region and Access Key when the Data Path End Point has no value.
- You cannot link multiple Amazon S3 targets to the same Data Policy when both targets have no value for the Data Path End Point, and the prefix and suffix are the same for both targets.

Use the instructions in this section to configure an Amazon S3 target.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.
2. In the Replication Targets pane, use the **Replication Type** drop-down menu to select **S3**.

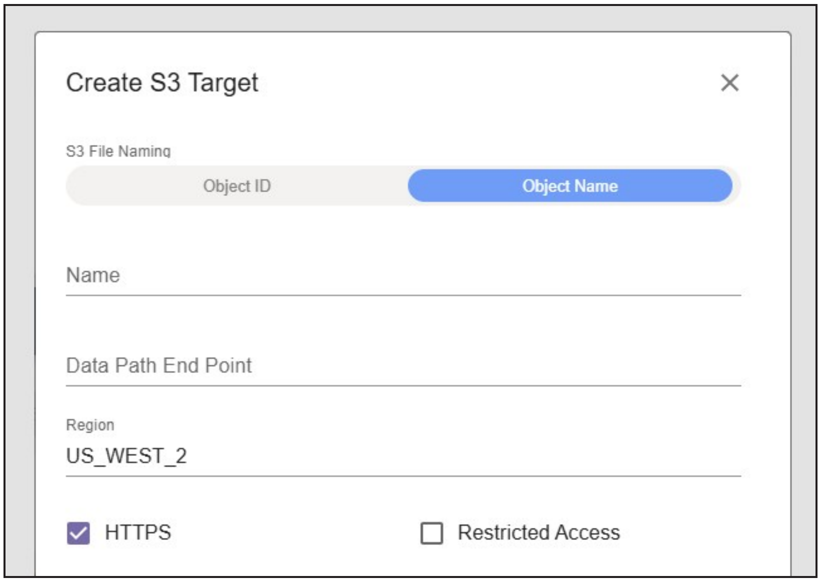


Replication Type: S3

Name	Data Path End Point	Region	State	Standby	S3 File Naming
No items to display.					

Figure 75 The Buckets Screen - Replication Targets pane - Replication Type menu.

3. In the Replication Targets pane, click **New**. The Create S3 Target dialog box displays.



Create S3 Target

S3 File Naming

Object ID | Object Name

Name

Data Path End Point

Region

US_WEST_2

☑ HTTPS

☐ Restricted Access

Figure 76 The Create S3 Target - Options dialog box.

4. Use the **S3 File Naming** slider to select one of the following:
   - **Object ID** - Objects display a UUID when viewed on the Amazon target.
   - **Object Name** - Objects display their name when viewed on the Amazon target.
5. Enter a **Name** for the Amazon S3 target.
6. Enter a **Data Path End Point** (system name or IP address) or a **Region** to identify the remote Amazon S3 target.

Acceptable regions are: **Note: Dashes (-) in the standard AWS S3 region code must be replaced by underscores (_) in the text entered in the Region field.**		
• us_east_1	• ap_south_1	• sa_east_1
• us_east_2	• ap_southeast_1	• cn_north_1
• us_west_1	• ap_southeast_2	• ca_central_1
• us_west_2	• ap_northeast_1	• gov_cloud
• eu_west_1	• ap_northeast_2	
• eu_west_2		
• eu_central_1		

Notes:

- If you enter both a **Data Path End Point** and a **Region**, the Gateway uses the **Data Path End Point** and ignores the **Region**.
- You cannot use the same **Data Path End Point** or **Region** for multiple Amazon S3 targets.

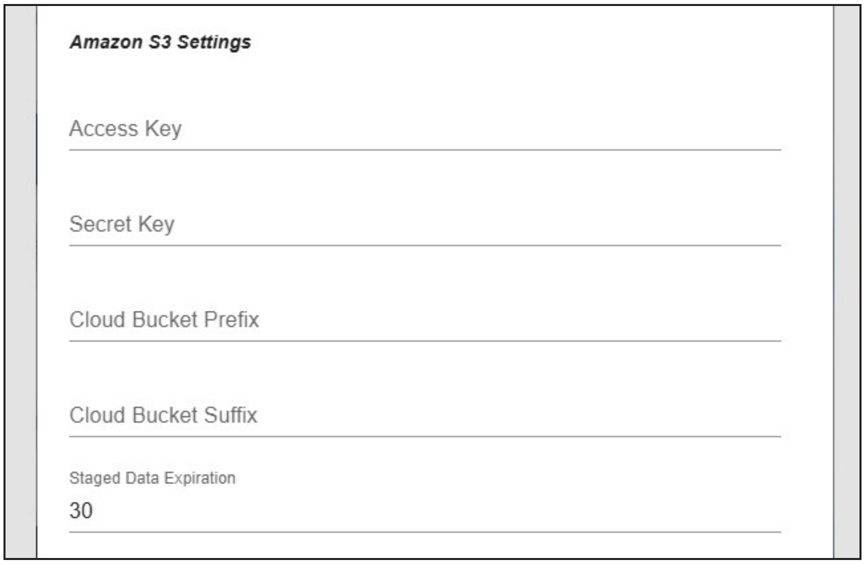
7. By default, **HTTPS** is selected so that the replication uses a secure connection. If desired, clear **HTTPS** to use HTTP.

8. If desired, select **Restricted Access** to limit access to a specific set of credentials and buckets set in your Amazon S3 account. This setting removes the verification the BlackPearl Object Gateway uses to confirm valid credentials when a data path endpoint and region are entered in Step 6.

Note: Spectra Logic recommends against using **Restricted Access**.

9. Enter the **Access Key**, which is the S3 Access Key of a user with administrator privileges for the Amazon S3 account.

Note: Administrator credentials are used to configure and maintain the source/target relationship. They are not used for user driven replication operations.



Amazon S3 Settings

Access Key

Secret Key

Cloud Bucket Prefix

Cloud Bucket Suffix

Staged Data Expiration: 30

Figure 77 The Create S3 Target - Amazon S3 Settings dialog box.

10. In the **Secret Key** field, enter the S3 Secret Key of the user you entered in Step 9.

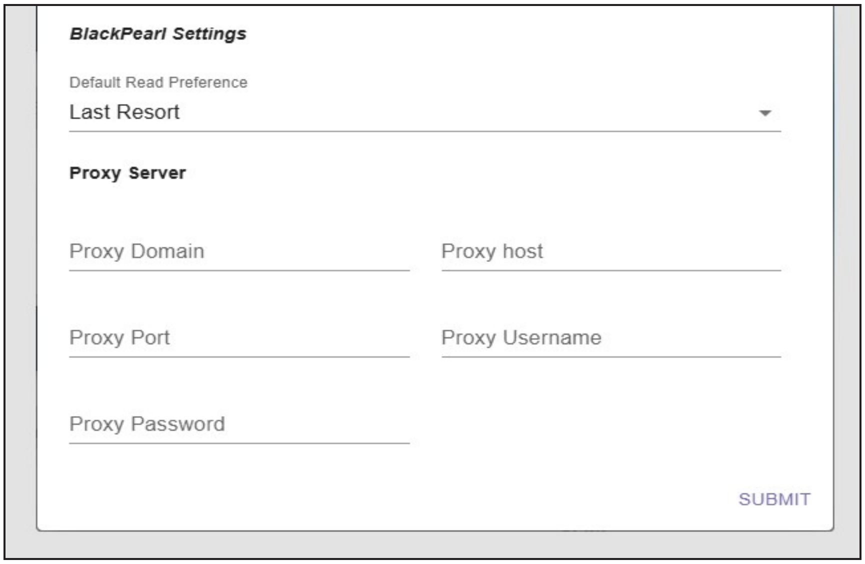
11. Optionally, enter a **Cloud Bucket Prefix** and/or **Cloud Bucket Suffix**. Bucket names on the BlackPearl Object Gateway must be unique within the Gateway, but bucket names in AWS S3 must be unique across the world. To permit friendlier, shorter local bucket names on the BlackPearl Object Gateway while avoiding naming conflicts with AWS S3, the Gateway adds the defined **Cloud Bucket Prefix** and **Cloud Bucket Suffix** to the BlackPearl bucket name when it replicates the bucket. For example, if **Cloud Bucket Prefix**=`prefix`, **Cloud Bucket Suffix**=`suffix`, and the bucket name=`name`, the resulting name of the bucket on the Amazon S3 target is `prefix-name-suffix`.

Note: The prefix and/or suffix must adhere to the replication target naming requirements.

12. Enter a **Staged Data Expiration** time in days using any value between 1 and 365. The default is 30. When data is pre-staged by the S3 service so that the BlackPearl Object Gateway can retrieve the data in an S3-standard manner, you must specify an expiration period in days. This is the minimum number of days before the pre-staged copy expires. If the Gateway does not retrieve all of the data before the copy expires, it has to pre-stage the data again, incurring additional delays and costs.

Note: Spectra Logic strongly discourages configuring a **Staged Data Expiration** of less than 7 days as any potential cost savings are offset by the possibility of multiple stagings.

13. Use the **Default Read Preference** drop-down menu to select a value to configure the behavior when the system cannot read from the target. Data is normally read from the source Gateway whenever possible. This setting determines when data is read back from the Amazon S3 target, if needed.



BlackPearl Settings

Default Read Preference: Last Resort

Figure 78 The Create S3 Target - BlackPearl Settings dialog box.

Note: Spectra Logic recommends that **Default Read Preference** be kept at the default of **Last Resort**.

Name	Description
Last Resort	The source Gateway only reads data from the target if the source Gateway cannot read from any of its own data partitions.
Minimum Latency	The source Gateway reads the data from the data partition with the least latency no matter whether it is connected to the source Gateway or the target.
After Online Pool	The source Gateway only reads data from the target if the source Gateway cannot read from an online pool.

Name	Description
After Nearline Pool	The source Gateway only reads data from the target if the source Gateway cannot read from a nearline pool.
After Non-Ejectable Tape	The source Gateway only reads data from the target Gateway if the source Gateway cannot read from secure media.
Never	Data is never read from the target.

14. Optionally, enter the information for a proxy server:

Field	Description
Proxy Domain	Domain name for the proxy server.
Proxy Host	The host name or IP address for the proxy server through which the Gateway connects.
Proxy Port	The proxy server port through which the Gateway connects.
Proxy Username	The username used when connecting through the proxy server.
Proxy Password	The password used when connecting through the proxy server.

15. Click **Submit**.

Create a Microsoft Azure Target

Configuring a Microsoft Azure target allows a data policy on the BlackPearl Object Gateway to replicate data to the Microsoft Azure cloud. With replication enabled, as soon as data is PUT to the cache of the source Gateway it begins replication to the Microsoft Azure cloud.

Use the instructions in this section to configure a Microsoft Azure target.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.
2. In the Data Policies pane, use the **Replication Type** drop-down menu to select **Azure**.

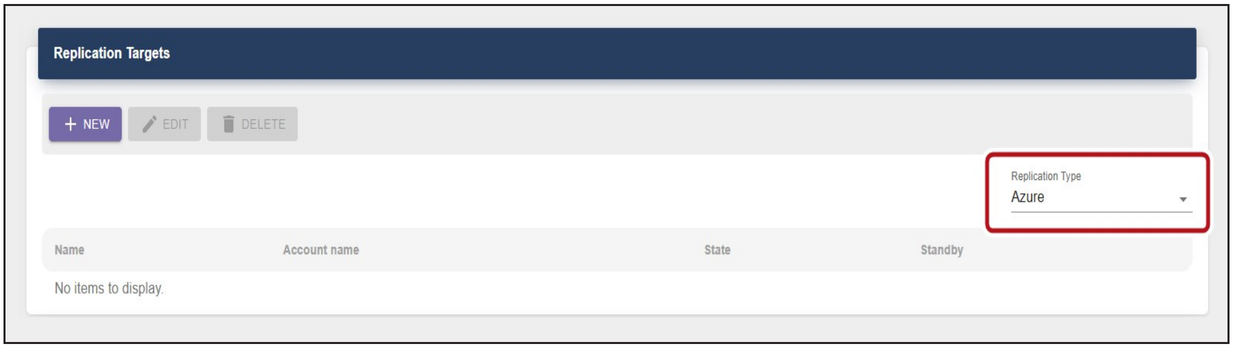
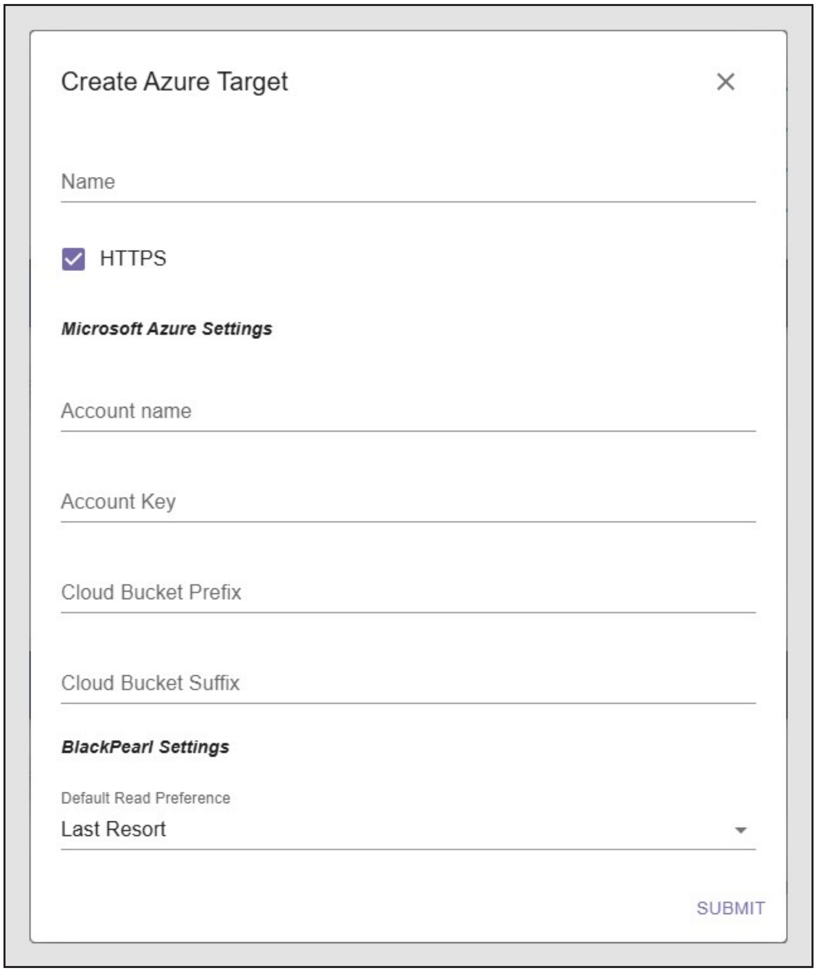


Figure 79 The Buckets Screen - Replication Targets pane - Replication Type menu.

3. In the Replication Target pane, click **New**. The Create Azure Target dialog box displays.



Create Azure Target

Name

☑ HTTPS

Microsoft Azure Settings

Account name

Account Key

Cloud Bucket Prefix

Cloud Bucket Suffix

BlackPearl Settings

Default Read Preference
Last Resort

Figure 80 The Create Azure Target dialog box.

4. Enter a **Name** for the Microsoft Azure target.

Note: Each Azure target name must be unique. You cannot create two Azure targets with the same name.

5. By default, **HTTPS** is selected so that the replication uses a secure connection. If desired, clear the **HTTPS** checkbox to use HTTP.

6. Enter the account name for the Microsoft Azure account in the in the **Account Name** field.

Note: You can not use the same **Account Name** for multiple Microsoft Azure targets.

7. In the **Account Key** field, enter the account key associated with the account entered in Step 6.

8. Optionally, enter a **Cloud Bucket Prefix** and/or **Cloud Bucket Suffix**. Bucket names on the BlackPearl Object Gateway must be unique within the Gateway, but bucket names in Microsoft Azure must be unique across the world. To permit friendlier, shorter local bucket names on the BlackPearl Object Gateway while avoiding naming conflicts with Microsoft Azure, the Gateway adds the defined **Cloud Bucket Prefix** and **Cloud Bucket Suffix** to the BlackPearl bucket name when it replicates the bucket. For example, if **Cloud Bucket Prefix**=`prefix`, **Cloud Bucket Suffix**=`suffix`, and the bucket name=`name`, the resulting name of the bucket on the Azure target is `prefix-name-suffix`.

Note: The prefix and/or suffix must adhere to the replication target naming requirements.

9. Use the **Default Read Preference** drop-down menu to select a value to configure the behavior when the system cannot read from the target. Data is normally read from the source Gateway whenever possible. This setting determines when data is read back from the Microsoft Azure target, if needed.

Note: Spectra Logic recommends using the setting **Last Resort**.

Name	Description
Last Resort	The source Gateway only reads data from the target if the source Gateway cannot read from any of its own data partitions.
Minimum Latency	The source Gateway reads the data from the data partition with the least latency no matter whether it is connected to the source Gateway or the target.
After Online Pool	The source Gateway only reads data from the target if the source Gateway cannot read from an online pool.
After Nearline Pool	The source Gateway only reads data from the target if the source Gateway cannot read from a nearline pool.
After Non-Exportable Tape	The source Gateway only reads data from the target Gateway if the source Gateway cannot read from secure media.
Never	Data is never read from the target.

10. Click **Submit**.

CHAPTER 5 - CONFIGURING NETWORK ATTACHED STORAGE

This chapter describes using the BlackPearl user interface to configure Network Attached Storage pools, volumes, and shares on a BlackPearl Object Gateway. If you have not purchased a NAS activation key, these features do not display in the BlackPearl user interface.

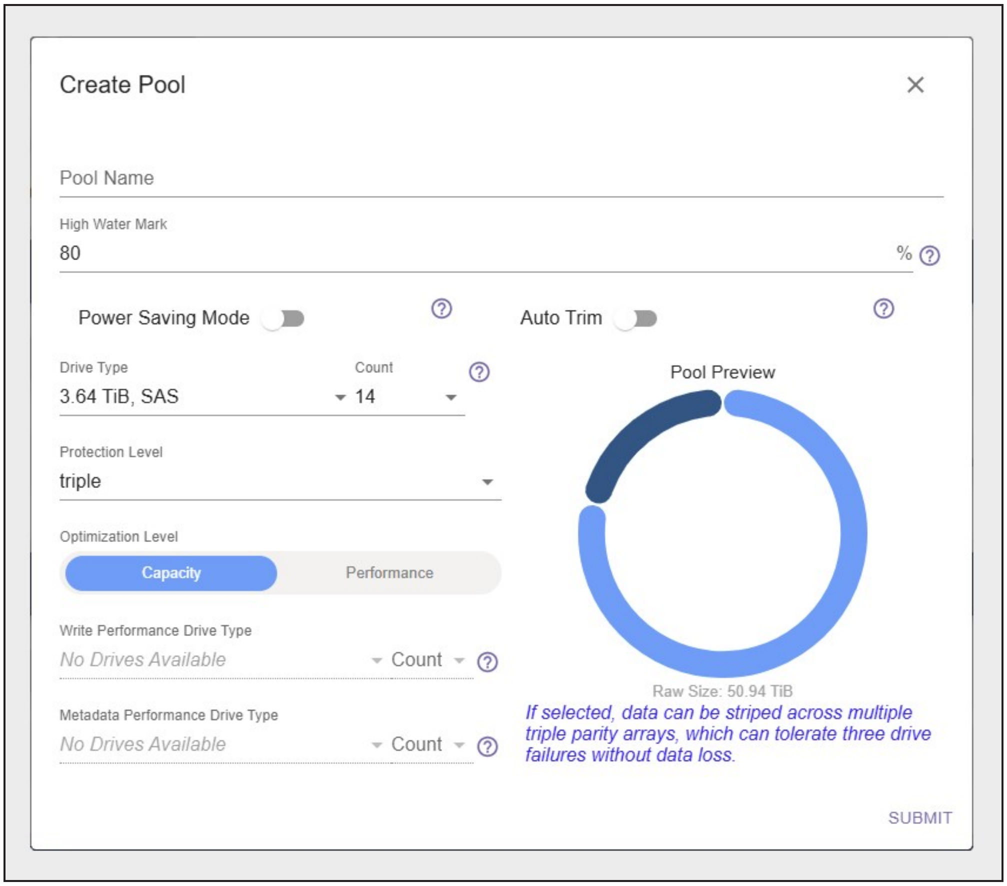
CREATE A NAS STORAGE POOL

When creating a new NAS pool, keep the following in mind:

- Each storage pool requires a minimum of one drive. Spectra Logic recommends using eight drives or more in a storage pool to reduce the impact of the overhead. Overhead is the space on the storage pool used to store parity data, and not used for data storage.
- Drives can only be associated with one storage pool. To create a new storage pool using drives that are already configured in an existing storage pool, you must first delete the existing storage pool. You can then create a new storage pool using newly available drives.
- Any drives not configured in storage pools act as global spare drives. If a drive failure occurs, the Gateway immediately activates a global spare. When the failed drive is replaced it becomes a spare.
- Spectra Logic recommends leaving at least one drive for a global spare.

Use the following steps to create a new NAS storage pool.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. In the Pools pane, click **New**. The Create Pool dialog box displays.



Create Pool

Pool Name

High Water Mark: 80 %

Power Saving Mode

Auto Trim

Drive Type: 3.64 TiB, SAS — Count: 14

Protection Level: triple

Optimization Level: Capacity | Performance

Write Performance Drive Type: No Drives Available — Count

Metadata Performance Drive Type: No Drives Available — Count

Pool Preview

Raw Size: 50.94 TiB

If selected, data can be striped across multiple triple parity arrays, which can tolerate three drive failures without data loss.

Figure 81 The Create Pool dialog box.

3. Configure the storage pool as required for your environment. As you make changes, the screen updates to show the characteristics of the new pool.

4. Enter a **Pool Name**. The pool name is limited to 48 characters.

Notes:
- The combined storage pool and volume name must be 78 characters or fewer. To avoid problems sharing volumes, Spectra Logic recommends a pool name of 32 characters or fewer.
- Each pool name must be unique. This field is case sensitive. Only the following special characters are allowed: hyphen (-), underscore (_), colon (:), and period(.).

5. Enter a percentage for **High Water Mark**. When the used space on the pool reaches this percentage, an alert is generated. Enter 0 if you do not want to set an alert level.

6. If desired, use the slider to enable **Power Saving Mode**. This option allows the disk drives in a disk pool to spin down after 60 minutes of inactivity.

Notes:
- This option is only available if all disk drives in the disk pool are capable of power saving mode.
- Spectra Logic recommends leaving Power Saving Mode **disabled**.

7. If desired, use the slider to enable **Auto Trim**. The option automatically removes unused data blocks from SSD and NVMe drives by marking deleted files as immediately ready for reuse, improving drive performance and longevity.

8. Use the **Drive Type** drop-down menu to select the disk drive type to use for the storage pool. Only one drive type can be used in a nearline pool.

Note: Any drive not in a disk pool acts as a global spare. A global spare drive is activated as soon as a drive configured in a disk pool fails.

9. Use the **Count** drop-down menu to select the number of drives of the previously selected type to use in the storage pool. If you plan to optimize the drive for capacity or performance, select an even number of drives.

10. Use the **Protection Level** drop-down menu to select the level of RAID protection to use on the storage pool:

    - **Mirror**—Data is striped across two mirrors. Any detected data corruption is corrected using checksums. This type of RAID offers the best performance for small random reads and writes.
    - **Single**—Data is striped across multiple single-parity arrays, which can tolerate one drive failure without data loss. This type of RAID has faster performance than double- and triple-parity based RAIDs.
    - **Double**—Data is striped across multiple double-parity arrays, which can tolerate two drive failures without data loss. In most cases, double-parity provides the best balance between data protection, performance, and storage capacity.
    - **Triple**—Data is striped across multiple triple-parity arrays, which can tolerate three drive failures without data loss. This type of RAID provides the most data protection.
    - **None**—The pool is not configured to provide data protection. Any drive failure results in data loss.

Note: Spectra Logic does not recommend setting protection to None.

11. Use the **Optimization Level** slider to select one of the following:

    - **Capacity** - The pool has more storage space, but slower performance.
    - **Performance** - The pool is faster at reading and writing data with less overall capacity.

12. Use the **Write Performance Drive Type** drop-down menu to select the disk drive type to use for the write performance drives, which increase write performance when the pool is shared using NFS.

Note: This feature is only intended for storage pools with NFS shares and typically has little impact on CIFS share performance.

13. Use the **Count** drop-down menu to select the number of write performance drives to add to the storage pool.

14. Use the **Metadata Performance Drive Type** drop-down menu to select the disk drive type to use for metadata performance drives, which improve performance for restoring small files, deduplication operations, and when searching metadata.

Note: These drives are permanently part of the storage pool and cannot be removed.

15. Use the **Count** drop-down menu to select the number of metadata performance drives to add to the storage pool.

Note: Metadata Performance drives can only be selected in multiples of three.

16. Click **Submit**.

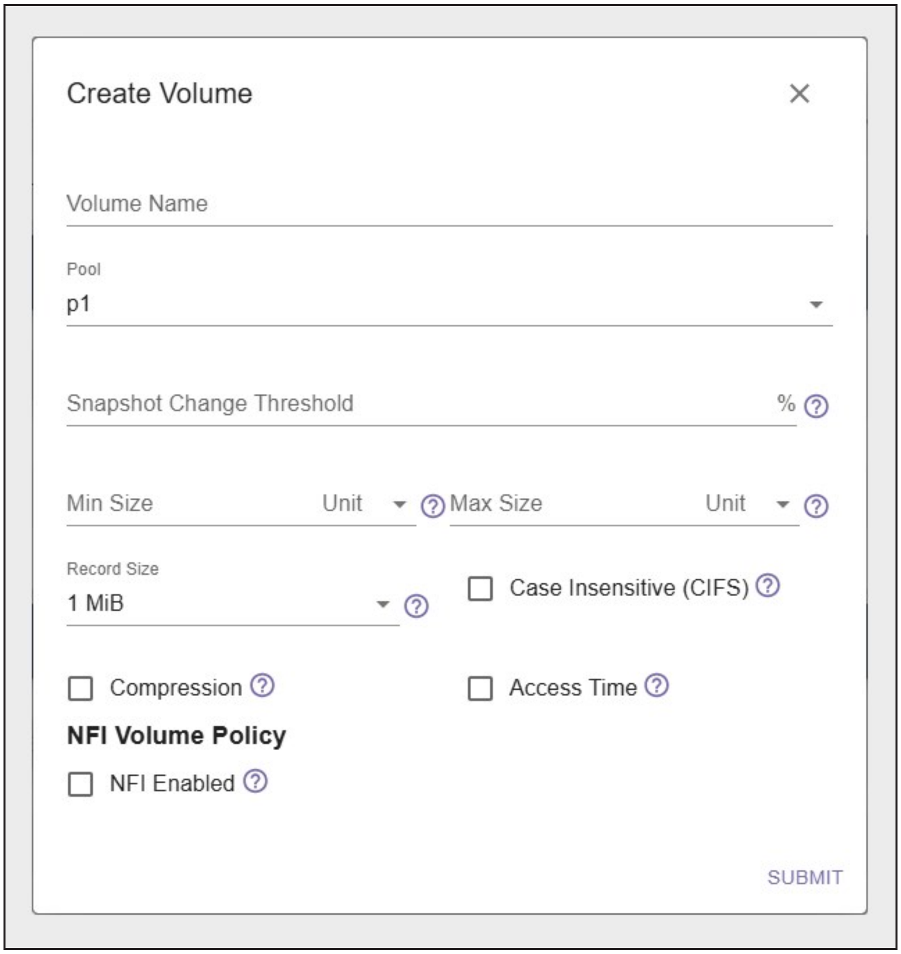
CREATE A VOLUME

Before you begin using a disk pool to store data, you must create one or more volumes to organize how the information is stored on the pool. After you create a volume, you can share the volume using NFS or CIFS, but you cannot share a volume using more than one method.

Volumes are thin provisioned, so it is possible for the combined allocated maximum storage of all volumes to exceed the physical space available.

Use the following steps to create a volume on a disk pool.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. Under Volumes pane, click **New**. The Create Volume dialog box displays.



Create Volume

Pool: p1

Record Size: 1 MiB

Figure 82 The Create Volume dialog box.

3. Enter a **Volume Name**. Volume names are limited to 62 characters or fewer.

Notes:
- The combined disk pool and volume name must be 78 characters or fewer.
- NFS does not allow spaces in share names. As a result, any spaces in the volume name are replaced by underscores in the corresponding NFS share name. The BlackPearl user interface displays the volume name without the underscores. For example, for a volume named **Share One**, the corresponding NFS share is named **Share_One** to external network computers, but it is named **Share One** in the BlackPearl user interface.

4. Use the **Pool** drop-down menu to select a previously configured disk pool on which you want to create a volume.

5. Enter a **Snapshot Change Threshold** percentage. This specifies the percentage of data change between consecutive snapshots that triggers a possible ransomware warning. If the percentage of data changes by more than the threshold, a message displays in the BlackPearl user interface, and an email is sent to the Administrator if the Administrator user is configured to receive warning emails.

Notes:
- Allowed values are between 0 and 99.
- Spectra Logic recommends configuring the Administrator user to receive emails when a warning event occurs.
- The BlackPearl Object Gateway uses unique data to detect the specified percentage change when data is deleted. If you enable compression for this volume, when you change the data on the source, the percentage change on the source and the percentage change in the snapshot may not be the same. The BP uses the percentage change of the snapshot to determine when to trigger a warning.

6. Configure the **Minimum Size**:

Select the desired **Unit** size from the drop-down menu and enter a numerical value for the minimum size in the **Min Size** text box to the left of the unit size drop-down menu. This space is allocated immediately if there is sufficient space available on the disk pool. If there is insufficient space available, volume creation fails.

Note: Leave the **Minimum Size** and **Maximum Size** blank to create the volume with access to all available space on the disk pool.

7. Configure the **Maximum Size**:

Select the desired **Unit** size from the drop-down menu and enter a numerical value for the maximum size in the **Max Size** text box to the left of the unit size drop-down menu.

Notes:
- Volumes are thin provisioned, so it is possible for the combined allocated maximum storage of all volumes to exceed the physical space available.
- Leave the **Minimum Size** and **Maximum Size** blank to create the volume with access to all available space on the disk pool.

8. Use the **Record Size** drop-down menu to select a record size for the volume. This setting determines how data is divided and stored on disk. In general, larger values increase performance at the cost of increased storage space requirements.

IMPORTANT The default value is 1 MiB. Only change this value at the direction of Spectra Logic.

9. If desired, select **Case Insensitive (CIFS)** to configure the volume to treat all names as case insensitive, which can improve performance, especially in situations where directories contain a large number of files.

Notes:
- This option should only be used for volumes shared using CIFS and **cannot** be changed after creating the volume.
- Creating a CIFS share on a case-sensitive volume reduces performance.
- Case-insensitive volumes are useful for Commvault® targets.

CAUTION **DO NOT** enable this setting if you plan to share the volume using NFS.

10. If desired, select **Compression** to enable data compression using ZFS LZ4 algorithm to allow the BlackPearlGateway to store more data. If the data being written is compressible there is typically an increase with store and restore operations, because less data is transferred to and from the disk drives. The size reduction of transferred files depends on how much the system can compress the data, and may fluctuate.

    The data compression process uses CPU cycles to perform the compression. If compression is enabled for non-compressible data, for example JPEG images or movie files that use the H. 264 codec, the compression process may use an excessive number of CPU cycles, slowing the overall performance of the Gateway. This impact is less evident with Gen2 and Gen3 master nodes.

11. If desired, select **Access Time** to configure the Gateway to update the time stamp of a file when it is read from the volume.

Note: Enabling this option may slow performance.

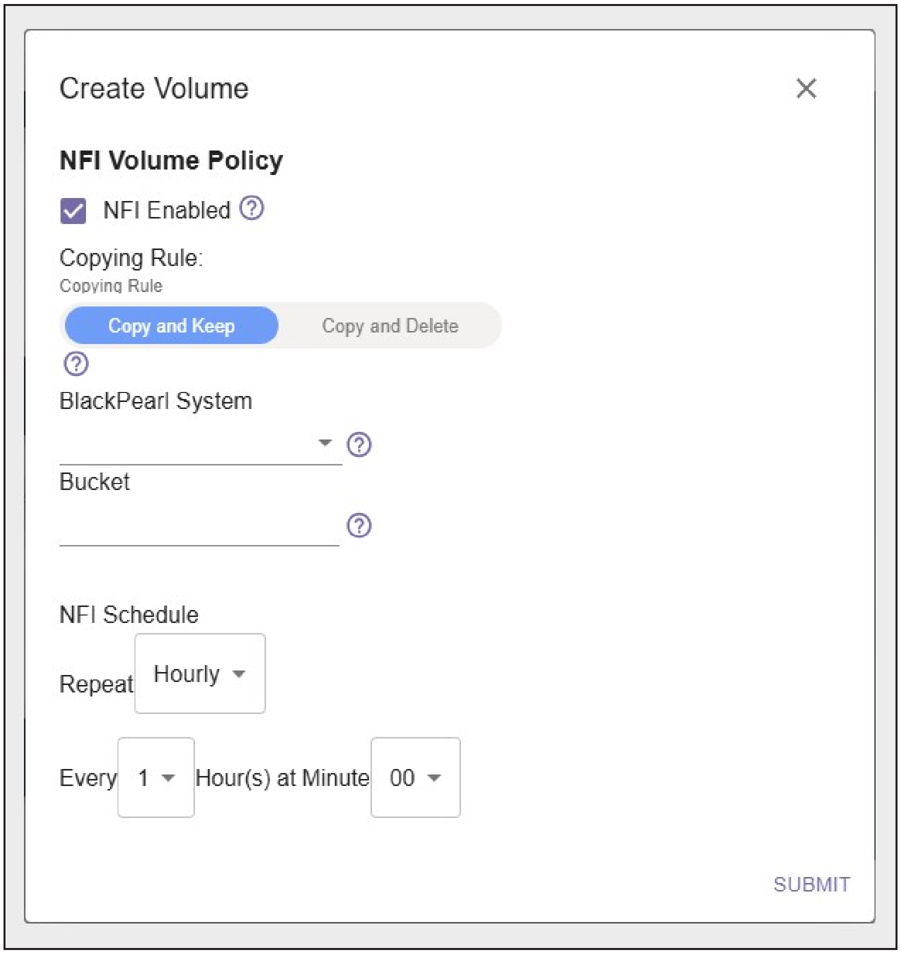
12. Do one of the following:
    - If you are configuring this volume to use NFI replication, continue to Configure NFI Volume Policy on the next page.
    - If you are not configuring NFI, click **Submit**.

Configure NFI Volume Policy

The NFI service is used to automatically transfer files from the NAS volume to the local Gateway's storage domains or to a remote BlackPearl Object Gateway.

Note: Vail shares are not compatible with NFI. Do not enable this feature is you plan to create a Vail share on the volume.

1. After completing the steps in Create a Volume, select **NFI Volume Policy**. The Create Volume screen redisplays to show the NFI Volume Policy options.



Create Volume

NFI Volume Policy

☑ NFI Enabled

Copying Rule: Copy and Keep

BlackPearl System:

Bucket:

NFI Schedule

Repeat: Hourly

Every 1 Hour(s) at Minute 00

Figure 83 The Create Volume dialog box - NFI Options.

2. Use the **Copying Rule** slider to select one of the following:
   - **Copy and Keep** - New or changed data in the volume is copied to the BlackPearl managed object storage and retained in the NAS volume.
   - **Copy and Delete** - Data in the volume is copied to the BlackPearl managed object storage and then deleted from the NAS volume.
3. Use the **BlackPearl System** drop-down menu to select a previously configured BlackPearl NFI Replication Target.

4. Enter the name of the **Bucket** to use to store the data on the BlackPearl Object Gateway. If the bucket does not exist, it is automatically created.

Notes:

- The bucket name cannot contain a colon (:), forward slash (/), or space.
- The bucket name cannot exceed 255 characters.
- If you plan to modify files in the NAS volume you must enter the name of the bucket with a data policy that uses versioning. See Create a Data Policy on page 127.
- If the bucket data policy includes a replication rule for an Amazon S3 or Microsoft Azure target, the bucket name must also conform to the naming conventions of that cloud provider.

IMPORTANT

BlackPearl bucket names are case sensitive, but for some cloud targets, bucket names must be all lower case. The BlackPearl software changes bucket names with upper case letters to all lower case letters when needed. If you are using bucket names that only differ by case, the buckets are combined on the cloud target. For example, the BlackPearl buckets 'Index' and 'index' both map to the cloud bucket 'index', causing possible data collision and bucket ownership/permission problems.

5. Configure the **NFI Volume Policy Schedule**:

   The NFI Volume Policy Schedule transfers data from the NAS volume to a BlackPearl Object Gateway at intervals based on number of hours, days, or days of the week.

6. Use the **Repeat** drop-down menu to select one of the following:

   - Select **Hourly** and use the **Hours** and **Minute** drop-down menus to select values for **Every _ Hours at Minute _**. These values specify the interval in hours between data transfers, and the number of minutes after the top of the hour when the job starts. For example, if the values are set to 4 and 15, data is transferred every four hours, at 15 minutes after the hour.
   - Select **Daily** and enter a value for **Every** to specify the interval, in days, between data transfers. Then use the **Hour** and **Minute** drop-down menus to specify the time of day to start the job.
   - Select **Weekly** and use the **Every** drop-down menu to select one or more day(s) of the week on which to transfer data. Then use the **Hour** and **Minute** drop-down menus to specify the time of day to start the job.

7. Click **Submit**.

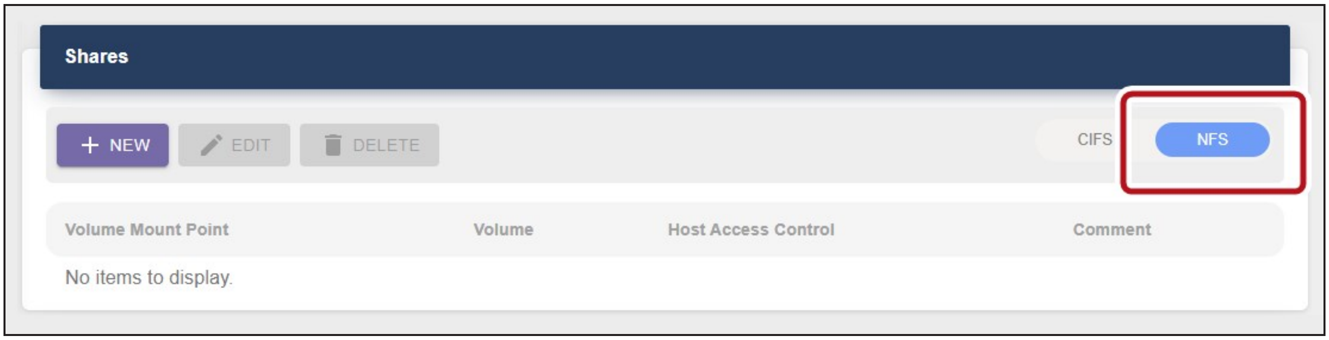
CREATE A NFS SHARE

After you create one or more volumes, you can share a volume using the NFS service.

> **Note:** Shares are not available until network settings are configured. See Configure the Data Connection on page 76.

Use the following steps to create an NFS share.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. In the Shares pane, use the slider on the right side to select **NFS**.

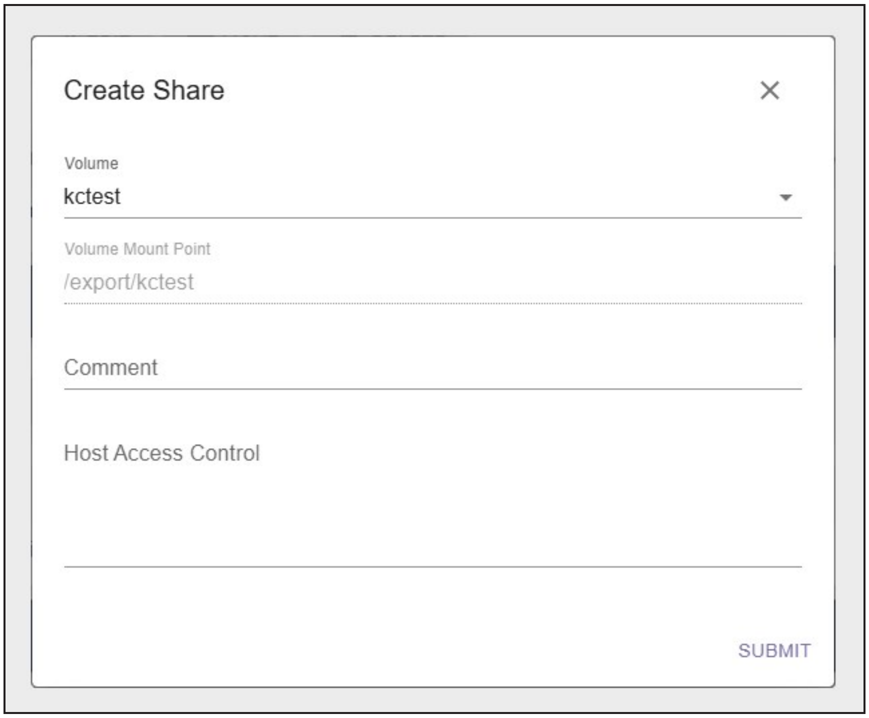


Volume Mount Point	Volume	Host Access Control	Comment

No items to display.

Figure 84 The NAS screen - Shares pane - NFS.

3. In the Shares pane, click **New**. The Create Share dialog box displays.



Volume: kctest

Volume Mount Point: /export/kctest

Comment

Host Access Control

Figure 85 The New NFS Share dialog box.

4. Use the **Volume** drop-down menu to select the previously configured volume you want to share using NFS.
5. The network address displayed for **Volume Mount Point** is the address of the share you are currently configuring.

Note: Before mounting an NFS share, make sure the client supports the NFSv3 protocol and properly handles file locking.

6. If desired, enter a comment in the **Comment** field. This comment only displays on the BlackPearl user interface.
7. In the **Host Access Control** pane, enter the IP address and permission level of all hosts that you want to access the volume. Hosts not listed are not able to access the volume. In addition to the host IP address, you must include one of the following permission parameters for each host you add to the BlackPearl Object Gateway.

Parameter	Description
norootsquash	**Root Access**—The host can access the NFS share with root access to the share. This host is used to set permissions for rootsquash users.
rootsquash	**Standard Access**—The host can access the NFS share, but does not have root access. Standard access allows write permission to the share, but does not allow the user to delete, modify, or rename files for which they do not have write permission.
ro	**Read Only**—The host can access the NFS share, but cannot write data to the shared volume.

For example, entering “`192.168.32.25 rootsquash`” allows the specified host to access the share with standard access.

If you want to allow all hosts to access the share, type `*` and include the permission parameter. For example, entering "`* norootsquash`" allows all hosts to access the share with root access.

8. Click **Submit**.

CREATE A CIFS SHARE

After you create one or more volumes, you can share a volume the CIFS service for use in a Windows environment. Creating a CIFS share consists of 3 major steps:

1. Joining an Active Directory or enabling CIFS access control - this step is usually only required the first time you create a CIFS share. See Access Control for a CIFS Share below.
2. Creating the CIFS share. Create a CIFS Share below
3. Setting Permissions for CIFS Share - This step is required for each CIFS share you create. See Set Permissions for a CIFS Share on page 166

Note: Shares are not available until network settings are configured. See Configure the Data Connection on page 76.

Access Control for a CIFS Share

Spectra Logic recommends using Active Directory to control access to CIFS shares on the BlackPearl Object Gateways.

However, if your Windows operating system environment does not use Active Directory, you can enable CIFS user access, also known as local administrator status on the Gateway to allow a specified user to access the CIFS shares in a Windows workgroup environment. The username and password configured on the BlackPearl Object Gateway are used to access the CIFS shares when using a Windows workgroup environment.

- Configure the Active Directory Service on page 102

-OR-

- Configure Users on page 203

Once you have completed one of the above, continue to Create a CIFS Share below.

Create a CIFS Share

1. If necessary, join an Active Directory domain or configure a user for CIFS user access as described in Access Control for a CIFS Share above. You do not need to do both. This step is usually only required when you create the first CIFS share.
2. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.

3. In the Shares pane, use the slider on the right side to select **CIFS**.

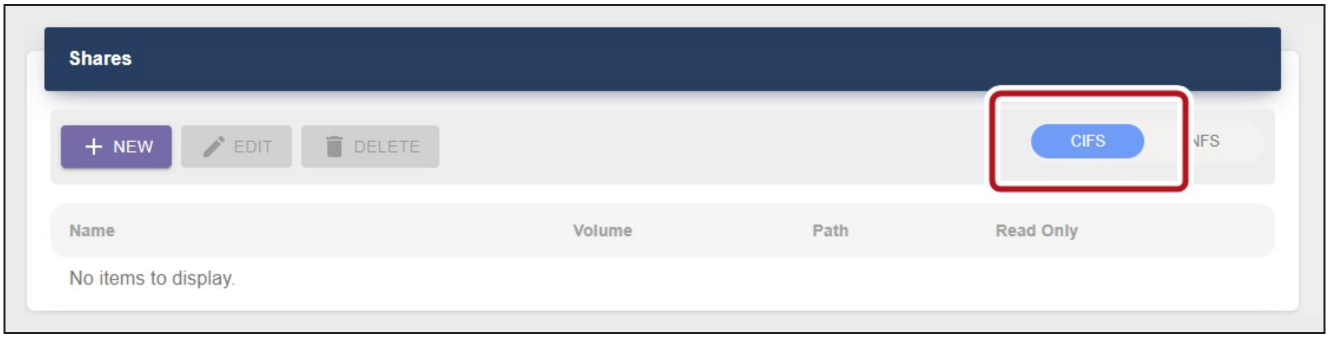
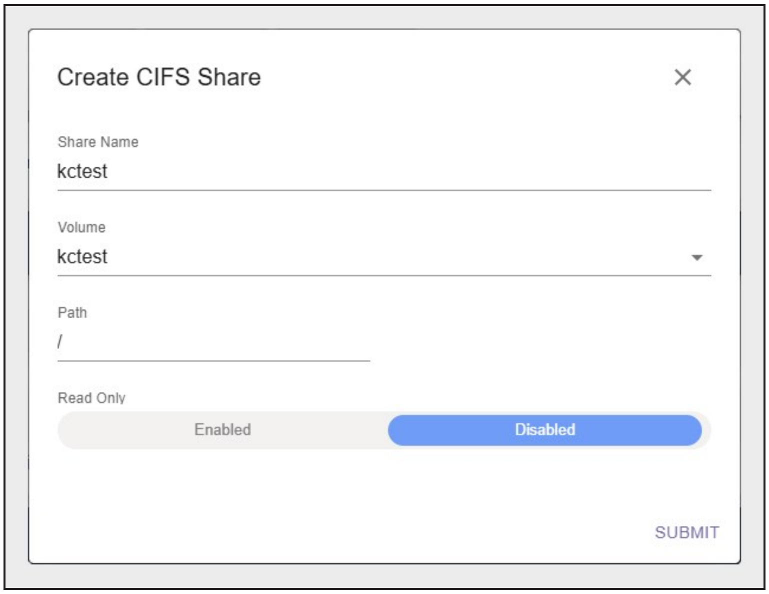


Figure 86 The NAS screen - Shares pane - CIFS.

4. In the Shares pane, click **New**. The Create CIFS Share dialog box displays.


Create CIFS Share

Share Name: kctest

Volume: kctest

Path: /

Read Only: Enabled [✓ Disabled]

Figure 87 The Create CIFS Share dialog box.

5. Enter a **Share Name** for the CIFS share. This is the name that is displayed in Active Directory configurations.
6. Use the **Volume** drop-down menu to select the previously configured volume you want to share using CIFS.

Note: Creating a CIFS share on a case-sensitive volume reduces performance.

7. Enter the desired network access for the **Path** to the share. The default path allows access to the root of the volume.

   After creating the CIFS share, you can connect to it using your Windows-based host and create subdirectories in the share. You can use the **Path** field to allow access to specific directories by specifying the exact subdirectory.

   For example, if you enter `/home/user` in the path field, any user that connects to this CIFS share only has access to the “`user`” directory, even if the “`home`” volume contains other directories.

Note: If you use a path that starts with two slashes (for example \\path) you are unable to edit permissions after the share is created.

8. Use the **Read Only** slider to select one of the following:
   - **Enabled** - The system prevents any data from being written to the share.
   - **Disabled** - Both read and write operations are available.

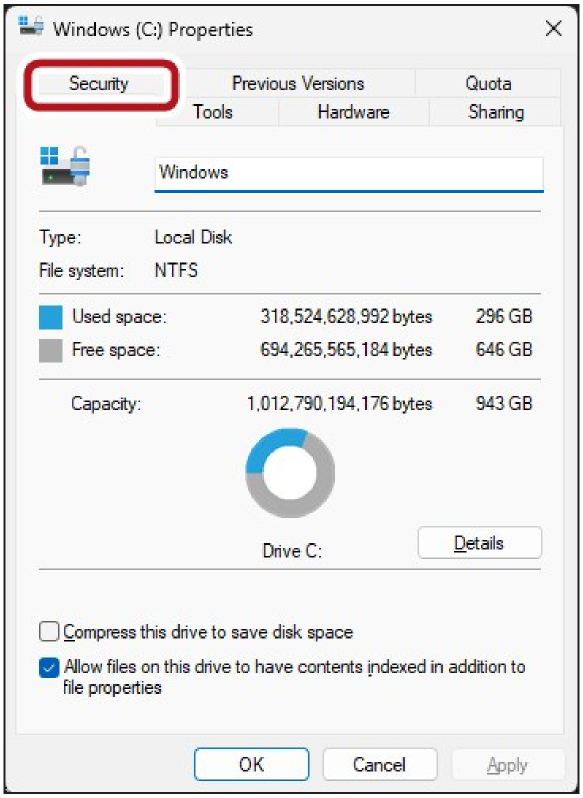
9. Click **Submit**.

Set Permissions for a CIFS Share

When a CIFS share is created, the default permission is “Everyone”. This allows the user creating the initial shares to easily set the proper permissions for additional users without requiring the Active Directory Domain administrator password.

1. Mount the new CIFS share to your Microsoft Windows operating system host.
2. Using Windows Explorer, right-click on the CIFS share, and select **Properties**. The General tab of the Properties window displays.

Note: You cannot use the Computer Management panel to set permissions on CIFS shares.



Windows

Type: Local Disk

File system: NTFS

🟦 Used space: 318,524,628,992 bytes 296 GB

▨ Free space: 694,265,565,184 bytes 646 GB

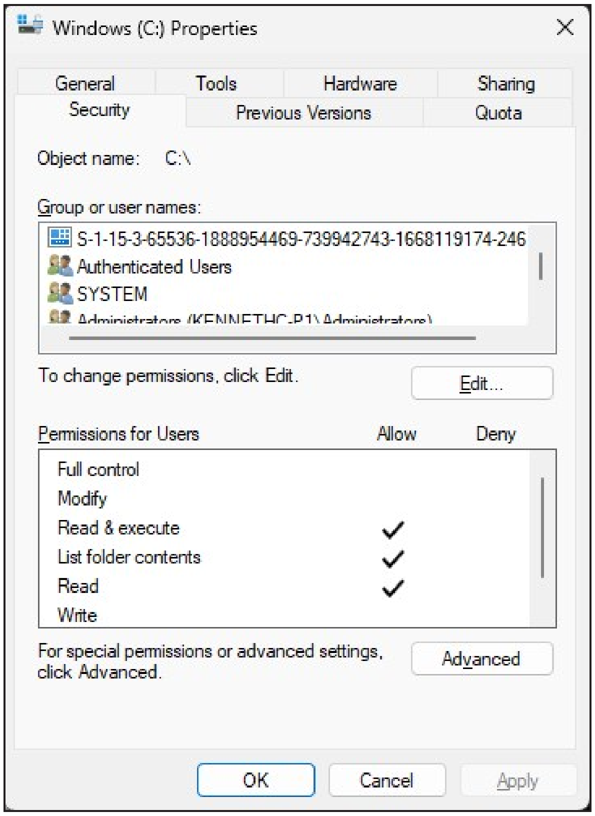
Capacity: 1,012,790,194,176 bytes 943 GB

□ Compress this drive to save disk space

☑ Allow files on this drive to have contents indexed in addition to file properties

Figure 88 The Properties window.

3. Click **Security**. The Security tab displays.



Object name: C:\

Group or user names:

S-1-15-3-65536-1888954469-739942743-1668119174-246
Authenticated Users
SYSTEM
Administrators (KENNETHC-P1\Administrators)

To change permissions, click Edit.

Permissions for Users	Allow	Deny
Full control		
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write		

For special permissions or advanced settings, click Advanced.

Figure 89 The Security tab.

4. Add, or remove users, or modify permissions for users as needed for your storage environment.

5. Click **OK**.

Note: If you remove the "Everyone" group permission in Windows, you must log out of Windows, and then log in again for the change to take effect.

CONFIGURE NFS AND CIFS SERVICES

The NFS and CIFS services are methods of sharing NAS volumes for use by other computers on the network.

Configure the NFS Service

If desired you can configure the transmission protocols and number of threads used by the NFS service. Use the following steps to edit the NFS service.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. In the NFS pane, click **Edit**. The Edit NFS Settings dialog box displays (not shown).
3. Use the sliders to enable or disable the **TCP** and **UDP** transmission protocols.
4. Enter the number of **Threads** for use by the service.

   Note: The default setting is sufficient for most network configurations.
5. Click **Save**.

Configure the CIFS Service

If desired, you can add an advanced parameter for the CIFS service. Advanced parameters are used to adjust/set global or share specific Samba parameters.

Additionally, parameters can be edited and deleted after they are created.

⚠ **CAUTION** Improperly configuring advanced parameters can expose security vulnerabilities and other serious issues. Advanced parameters should not be configured without a full understanding of the consequences.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. In the CIFS pane, click **Add Parameter**. The Add Advanced Parameter dialog box displays (not shown).
3. Enter the desired **Parameter Name** and **Parameter Value**.
4. Click **Create**.

Configure NAS Replication

If the BlackPearl Object Gateway is on a network with Verde arrays, BlackPearl NAS solutions, or other BlackPearl Object Gateways with NAS enabled, you can select to replicate data from the NAS volumes on the Gateway to one or multiple NAS replication targets. Replication uses the same data interface that the Gateway uses for normal file storage operations, so replication to multiple targets may decrease transfer speeds.

This feature also allows you to easily transfer snapshot data stored on NAS volumes to a remote BlackPearl Object Gateway. These snapshots can be retained for archival purposes or restored on the target Gateway to replicate the data contained in the snapshot.

Once you configure the replication service, you need to configure each volume on the Gateway that you want to replicate.

Note: This replication service is only for replicating NAS volumes on the Gateway to other BlackPearl Gateways with NAS enabled or BlackPearl NAS solutions. To replicate NAS volumes to BlackPearl managed object storage, use NFI replication (see Create a Volume on page 156).

Use the instructions in this section to configure the NAS replication service and to configure volumes for replication.

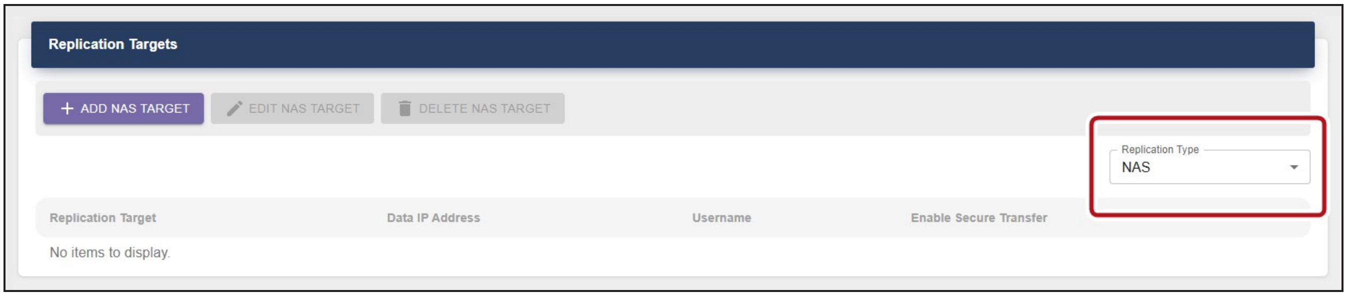
Notes:

- There must be enough space on the target to hold the replicated data, or the replication fails.
- Multiple volumes on the source device cannot replicate to a single volume on the target. Each volume on the source device must replicate to a different volume on the target.
- If multiple devices replicate to the same target, the target must use a different volume for each replication source.
- You must configure the data ports on the source and the target systems before you can configure replication (see Configure Network Connections on page 107).
- Your firewall must allow the source Gateway and all targets configured for replication to access **port 59373** for configuring replication, and **ports 59374-59400** for replication data transfers.
- The user account on the target system used for configuring NAS replication cannot be configured to use multi-factor authentication.
- For both the source Gateway and the targets, make sure you have completed the steps in Configuring Initial Settings on page 67.

Add a NAS Target

Use the instruction in this section to add a NAS target.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. In the Replication Targets pane, use the **Replication Type** drop-down menu to select NAS.



Replication Type: NAS

Replication Target	Data IP Address	Username	Enable Secure Transfer

No items to display.

Figure 90 The NAS screen - Replication Targets pane.

3. In the Replication Targets pane, click **Add NAS Target**. The Add Target dialog box displays.

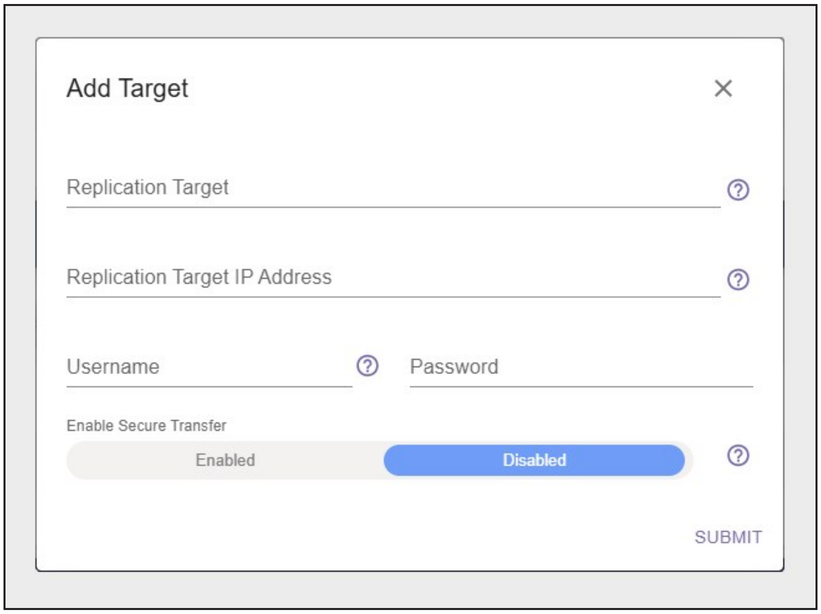


Figure 91 The Add Target dialog box.

4. Enter the IP address or hostname of the target's management port in the **Replication Target** field.

Note: Do not use http:// or https:// to precede the IP address or hostname.

5. Enter the IP address of the target's data port in the **Replication Target Data IP Address** field.

Note: Do not use http:// or https:// to precede the IP address or hostname.

6. Enter the username of a user with administrator privileges configured on the target in the **Username** field.

Note: Replications fail if the user account on the target system is configured to use multi-factor authentication.

7. Enter the user password in the **Password** field, if one is set. Otherwise, leave the field blank.
8. Select the **Enable Secure Transfer** checkbox to configure the Gateway to encrypt the replicated data before transferring it to the target. Data is encrypted using Secure Socket Layer (SSL).
9. Click **Submit**.

Configure the Target System

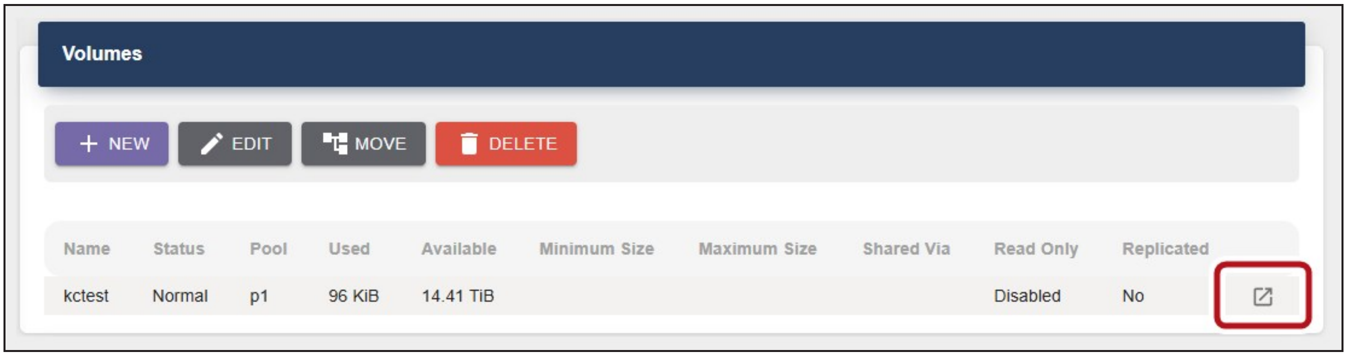
If you have not already done so, use the instructions below to create a disk pool and volume to be the target for the replication.

1. Log into the BlackPearl on the **target system** as described in Log Into the BlackPearl User Interface on page 74.
2. Create one or more storage pools as described in Create a NAS Storage Pool on page 153.
3. Create one or more volumes as described in Create a Volume on page 156. You must create one volume on the **target system** for each volume you want to replicate on the **source system**. Additionally, you can create volumes when performing the steps in Configure NAS Replication, below.

CAUTION You cannot use this volume for normal data storage operations, it can only be used as a replication target. Any data in the specified target volume is deleted each time the source system replicates data to the target system.

Configure Volumes for NAS Replication

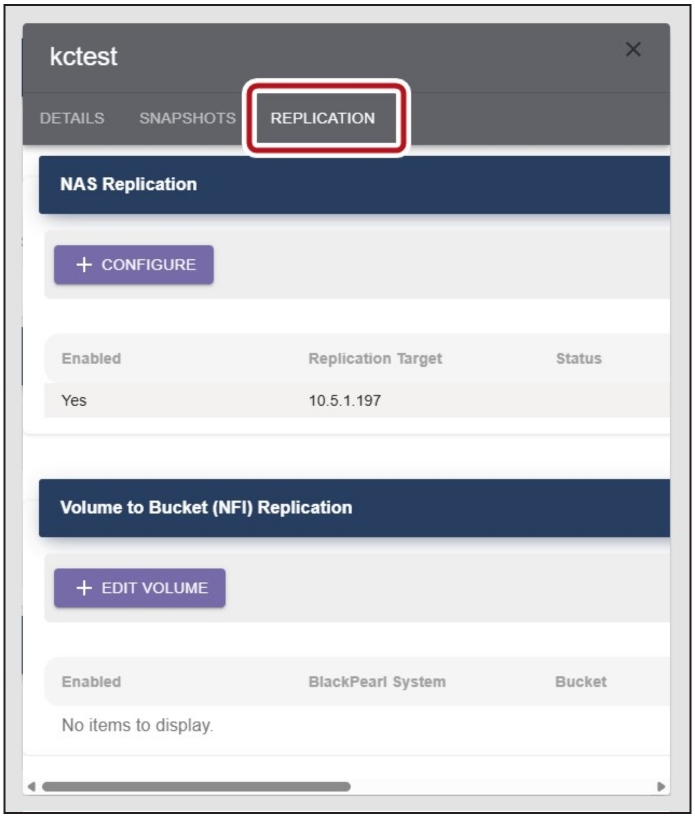
1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.



Name	Status	Pool	Used	Available	Minimum Size	Maximum Size	Shared Via	Read Only	Replicated
kctest	Normal	p1	96 KiB	14.41 TiB				Disabled	No

Figure 92 The NAS screen - Volumes pane - Details button.

2. In the Volumes pane, on the right side, click the **Details** button for the Volume you want to enable NAS replication. The details screen for the volume displays.



Enabled	Replication Target	Status
Yes	10.5.1.197	

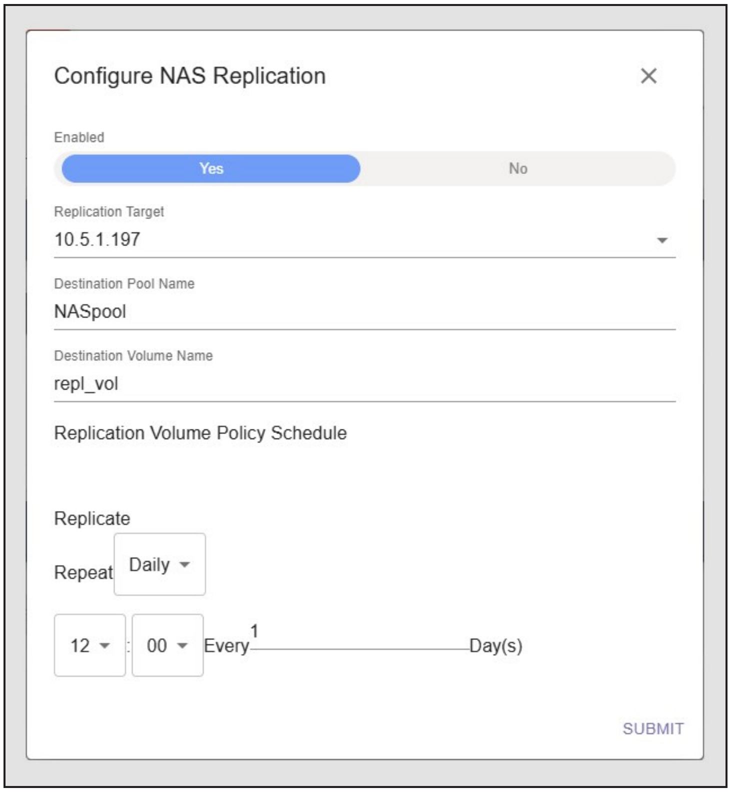
Enabled	BlackPearl System	Bucket

No items to display.

Figure 93 The Volume details screen - Replication.

3. Select the **Replication** tab at the top of the screen.

4. In the NAS Replication pane, click **Configure**. The Configure NAS Replication dialog box displays.



Configure NAS Replication

Enabled: Yes

Replication Target: 10.5.1.197

Destination Pool Name: NASpool

Destination Volume Name: repl_vol

Replication Volume Policy Schedule

Replicate

Repeat: Daily

12 : 00 Every 1 Day(s)

Figure 94 The Configure NAS Replication dialog box.

5. Use the **Enabled** slider to select **Yes** to enable NAS replication for the volume.

6. Use the **Replication Target** drop-down menu to select a previously configured NAS replication target. The targets are listed by the IP address or hostname entered when you configured the target.

7. Enter the **Destination Pool Name** of the storage pool on the target you want to use for replication. This field is case sensitive.

8. Enter the **Destination Volume Name** of a volume that resides on the target storage pool you selected in Step 7, or enter a name for a new volume to be created on the specified storage pool. This field is not case sensitive.

CAUTION You cannot use this volume for normal data storage operations, it can only be used as a replication target. Any data in the specified target volume is deleted each time the Gateway replicates data to the target.

- If the volume does not exist on the target, it is created.
- If the volume exists on the target, a warning message displays informing you that any data currently in the target volume is erased each time data is replicated. Confirm the warning message to continue.

9. Use the **Repeat** drop-down menu to select one of the following:
    - Select **Hourly** and use the **Hours** and **Minute** drop-down menus to select values for **Every _ Hours at Minute _**. These values specify the interval in hours between replicating data, and the number of minutes after the top of the hour when the job starts. For example, if the values are set to 4 and 15, a data is replicated every four hours, at 15 minutes after the hour.
    - Select **Daily** and enter a value for **Every** to specify the interval, in days, between replicating data. Then use the **Hour** and **Minute** drop-down menus to specify the time of day to start the replication.
    - Select **Weekly** and use the **Every** drop-down menu to select one or more day(s) of the week on which to replicate data. Then use the **Hour** and **Minute** drop-down menus to specify the time of day to start the job.
10. Click **Submit**.

Chapter 6 - Configuring Security and Data Protection Features

This chapter describes using the BlackPearl user interface to configure security options for the Gateway, such as Multi-Factor Authentication, volume snapshots, encryption, and database backups, all which help you maintain the security of your system and data.

Volume Snapshots

Volume Snapshots are images of a volume's configuration and data makeup as they were when the snapshot was generated. Restoring to a previously created snapshot allows you to go "back in time" and restore the volume to the state it was in when the snapshot was created.

Notable features of volume snapshots are:

- Snapshots are immutable to the outside word. Snapshots cannot be overwritten or altered, and can only be deleted by a BlackPearl administrator.
- Snapshots can be used to restore access to data in the case of a ransomware attack, and can be useful in restoring a file that was accidentally deleted.
- Snapshots are created manually, on a schedule, or triggered by external applications such as the Spectra StorCycle application.

Volume snapshots are retained on the Gateway until they are manually deleted, or the set Maximum Number of Snapshots limit is reached. When the limit is reached, the oldest snapshot is deleted, freeing up the capacity held by that snapshot.

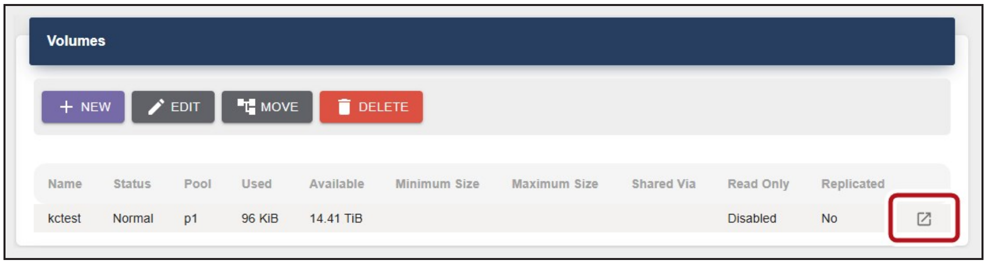
Snapshots are created instantly without any impact to system performance. Snapshots initially occupy very little space on the storage pool, but grow as data is modified or deleted, because this data must be retained by the snapshot.

For example, if you write 100 GB to the volume, and then make a snapshot of that data, the snapshot is 0 bytes in size, as it simply points to the existing data. However, if that 100 GB is deleted, the snapshot grows to 100 GB, because it must retain the data. When the snapshot containing the 100 GB of data is deleted, either manually or based on schedule retention, then 100 GB of capacity is made available for new data.

Create a Snapshot

Here is how you create a snapshot:

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. In the Volumes pane, select the row of the volume for which you want to generate a snapshot, then click the **Details** button on the right-hand side of the row.



Name	Status	Pool	Used	Available	Minimum Size	Maximum Size	Shared Via	Read Only	Replicated
kctest	Normal	p1	96 KiB	14.41 TiB				Disabled	No

Figure 95 The NAS screen - Volumes pane - Details button.

3. On the Volume Details window, click **Snapshots**.
4. In the Snapshots pane, click **New**.

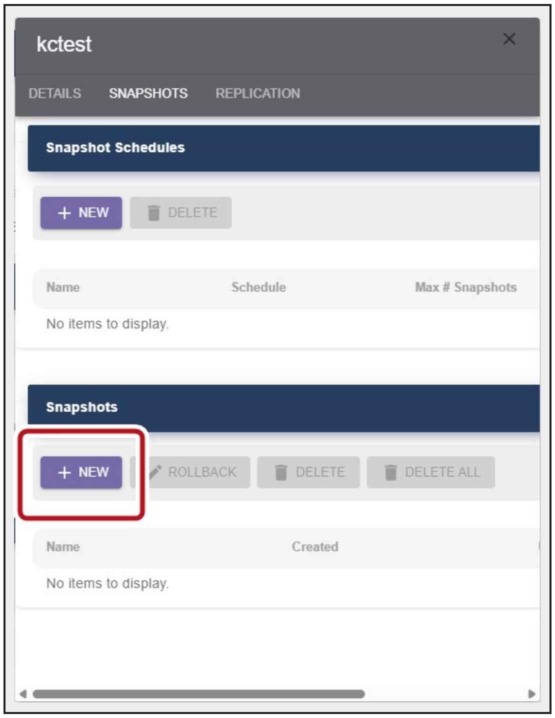


Figure 96 The Volume Details window - Snapshots pane - New Snapshot button.

5. Enter a **Name** for the Snapshot.

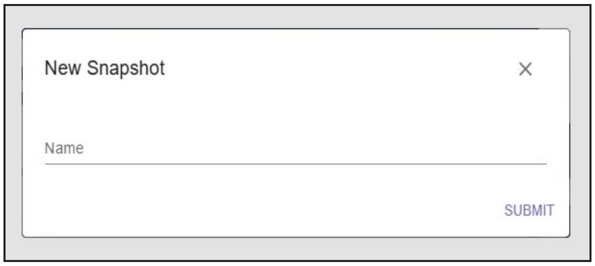


Figure 97 The New Snapshot dialog box.

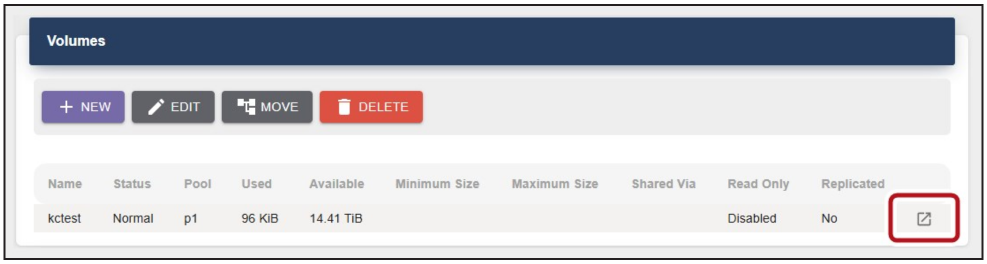
6. Click **Submit**.

Configure a Snapshot Schedule

Snapshot schedules can be configured at intervals based on hours, number of days, or days of the week.

Here is how you configure a snapshot schedule:

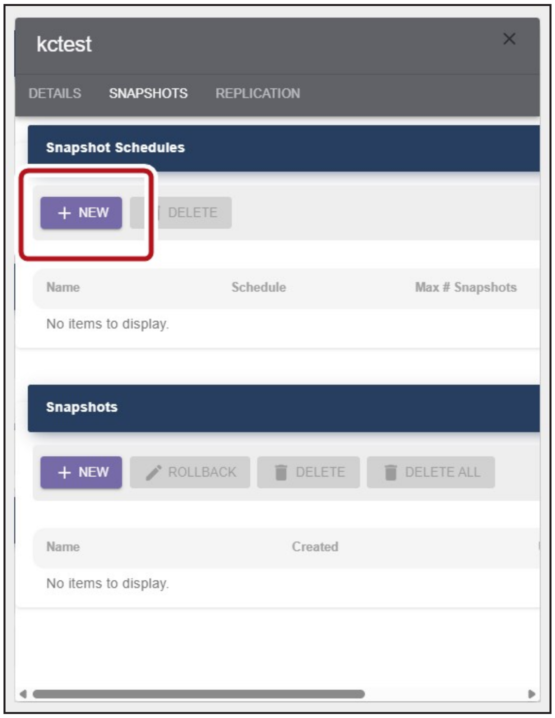
1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. In the Volumes pane, select the row of the volume for which you want to configure a snapshot schedule, then click the **Details** button on the right-hand side of the row.



Name	Status	Pool	Used	Available	Minimum Size	Maximum Size	Shared Via	Read Only	Replicated	
kctest	Normal	p1	96 KiB	14.41 TiB				Disabled	No	⧉

Figure 98 The NAS screen - Volumes pane - Details button.

3. On the Volume Details window, click **Snapshots**.
4. In the Snapshot Schedules pane, click **New**.



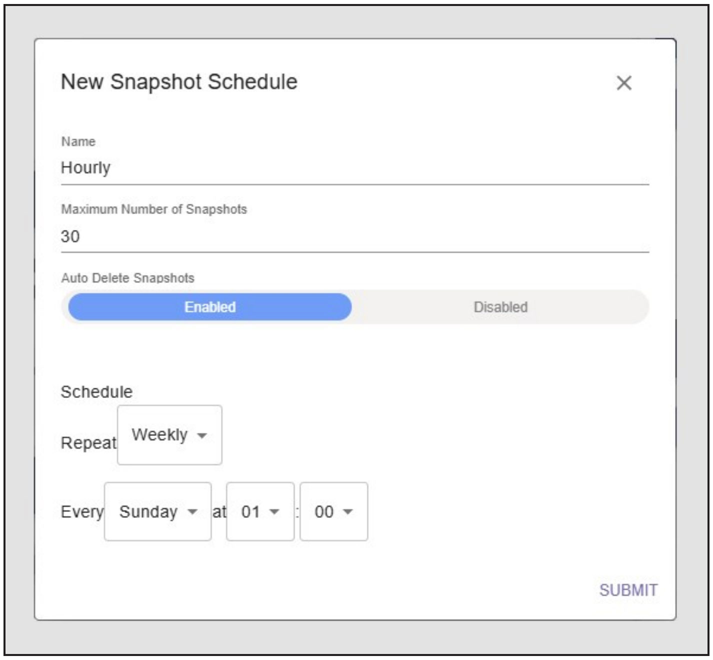
Name	Schedule	Max # Snapshots
No items to display.		

Name	Created
No items to display.	

Figure 99 The Volume Details window - Snapshots pane - New Snapshot Schedule button.

5. On the New Snapshot Schedule dialog box, enter a **Name** for the schedule.

Note: Snapshot schedule names must be unique.



New Snapshot Schedule

Name: Hourly

Maximum Number of Snapshots: 30

Auto Delete Snapshots: Enabled

Schedule

Repeat: Weekly

Every Sunday at 01 : 00

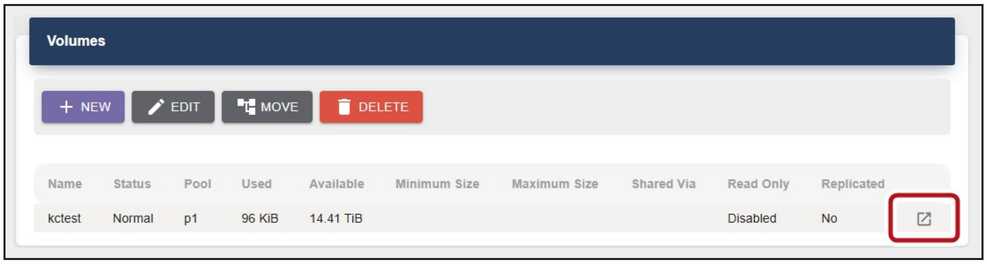
Figure 100 The New Snapshot Schedule dialog box

6. Enter a value for the **Maximum Number of Snapshots** for the volume. When this limit is reached, one of the behaviors described Step 7 occurs.
7. Use the **Auto Delete Snapshots** slider to select one of the following:
   - **Enabled** - When the maximum number of snapshots is reached, the oldest snapshot is deleted to free space for the next snapshot.
   - **Disabled** - When the maximum number of snapshots is reached, the BlackPearl Object Gatewaystops creating new snapshots for the volume.
8. Use the **Repeat** drop-down menu to select one of the following:
   - Select **Hourly** and use the **Hours** and **Minute** drop-down menus to select values for **Every _ Hours at Minute _**. These values specify the interval in hours between generating volume snapshots, and the number of minutes after the top of the hour when the job starts. For example, if the values are set to 4 and 15, a snapshot is created every four hours, at 15 minutes after the hour.
   - Select **Daily** and enter a value for **Every** to specify the interval, in days, between generating volume snapshots. Then use the **Hour** and **Minute** drop-down menus to specify the time of day to create the snapshot.
   - Select **Weekly** and use the **Every** drop-down menu to select one or more day(s) of the week on which to generate volume snapshots. Then use the **Hour** and **Minute** drop-down menus to specify the time of day to create the snapshot.
9. Click **Submit**.

Delete Snapshots

Here is how you delete one or more snapshots:

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. In the Volumes pane, select the row of the volume for which you want to delete a snapshot, then click the **Details** button on the right-hand side of the row.



Name	Status	Pool	Used	Available	Minimum Size	Maximum Size	Shared Via	Read Only	Replicated
kctest	Normal	p1	96 KiB	14.41 TiB				Disabled	No

Figure 101 The NAS screen - Volumes pane - Details button.

3. On the Volume Details window, click **Snapshots**.
4. In the Snapshot pane, do one of the following:
    - To delete a single snapshot - select the snapshot and click **Delete**.
    - To delete all snapshots - click **Delete All**.

   A confirmation screen displays (not shown).
5. Enter the required information in the entry field to confirm the deletion, then click **Submit**.

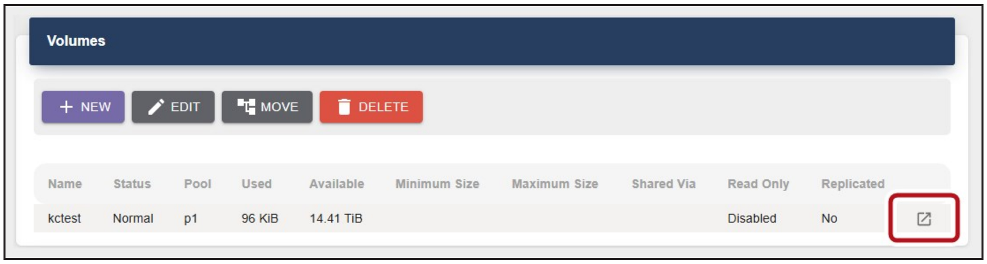
Delete a Snapshot Schedule

If desired, you can delete a previously created snapshot schedule.

Note: Deleting a snapshot schedule does not delete the snapshots previously created by the snapshot schedule. To delete snapshots, see Delete Snapshots on the previous page.

Here is how you delete a snapshot schedule:

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. In the Volumes pane, select the row of the volume for which you want to delete a snapshot schedule, then click the **Details** button on the right-hand side of the row.



Name	Status	Pool	Used	Available	Minimum Size	Maximum Size	Shared Via	Read Only	Replicated
kctest	Normal	p1	96 KiB	14.41 TiB				Disabled	No

Figure 102 The NAS screen - Volumes pane - Details button.

3. On the Volume Details window, click **Snapshots**.
4. In the Snapshot Schedules pane, select the schedule you want to delete, then click **Delete**. A confirmation screen displays (not show).
5. Click **Submit**.

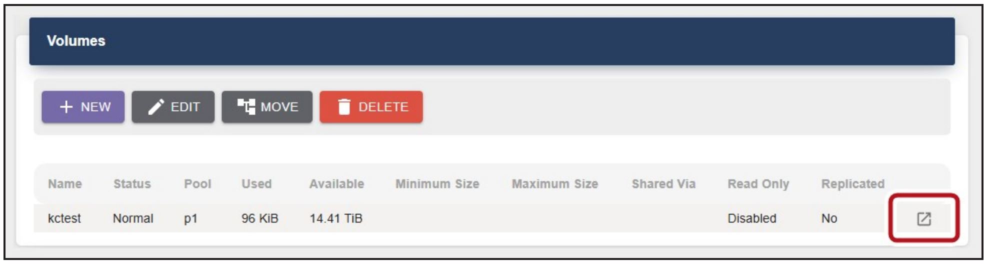
Restore to a Snapshot

Use the following instructions to restore a volume to its previous state using a previously generated snapshot.

Notes:

- If you only want to restore a single file in the snapshot, see Volume Snapshots on page 176.
- You cannot restore to a snapshot if the volume contains a Vail share using the BlackPearl user interface. Use API or CLI commands to restore a snapshot when the volume contains a Vail share.

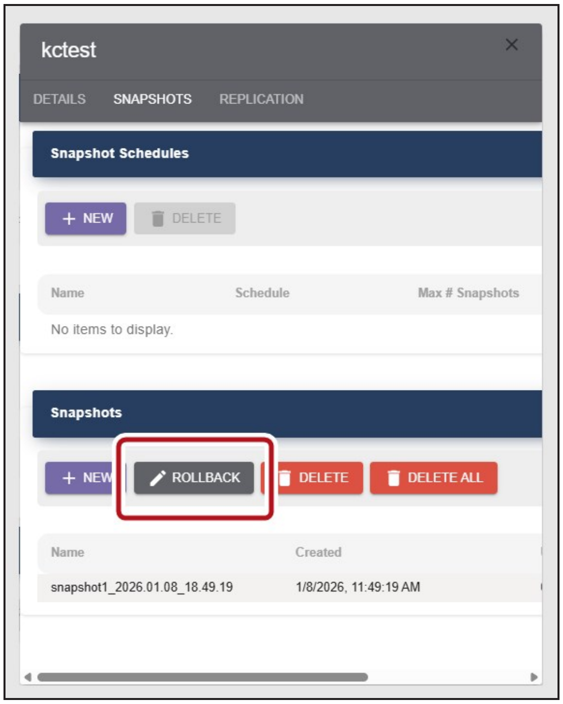
1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. In the Volumes pane, select the row of the volume for which you want to restore a snapshot, then click the **Details** button on the right-hand side of the row.



Name	Status	Pool	Used	Available	Minimum Size	Maximum Size	Shared Via	Read Only	Replicated
kctest	Normal	p1	96 KiB	14.41 TiB				Disabled	No

Figure 103 The NAS screen - Volumes pane - Details button.

3. On the Volume Details window, click **Snapshots**.



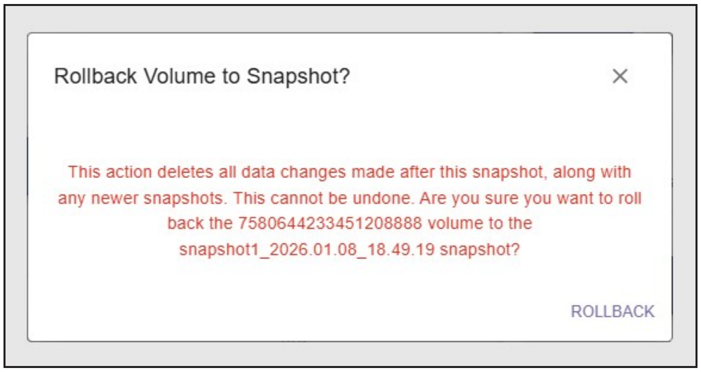
Name	Schedule	Max # Snapshots
No items to display.		

Name	Created
snapshot1_2026.01.08_18.49.19	1/8/2026, 11:49:19 AM

Figure 104 The Volume Details window - Snapshots pane - Rollback button.

4. In the snapshots list, select the snapshot you want to use to restore the volume and click **Rollback**. A confirmation screen displays.

CAUTION Rollback deletes all data changes made after the snapshot was created, and deletes any snapshots that were saved after the one you are using for the restore process. This action cannot be undone.


Rollback Volume to Snapshot?

This action deletes all data changes made after this snapshot, along with any newer snapshots. This cannot be undone. Are you sure you want to roll back the 7580644233451208888 volume to the snapshot1_2026.01.08_18.49.19 snapshot?

Figure 105 Confirm the volume snapshot rollback.

5. Click **Rollback**.

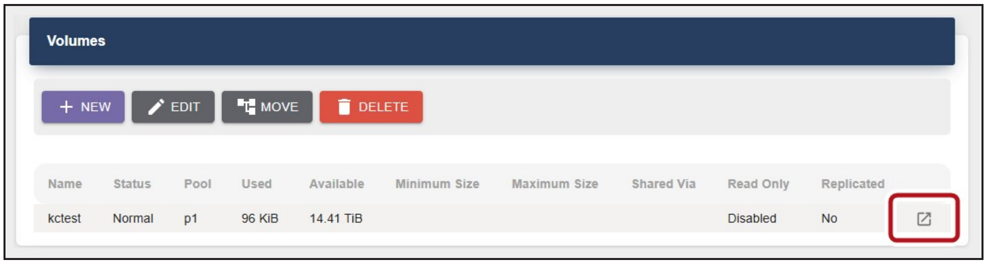
Retrieve a Single File from a Snapshot

If you only need to restore a single file, you do not need to restore an entire snapshot. Use the following instructions to retrieve a single file from a snapshot.

Note: Use Windows Explorer or Linux/Unix command line to complete this procedure.

Use the instructions in this section to retrieve a single file from a snapshot.

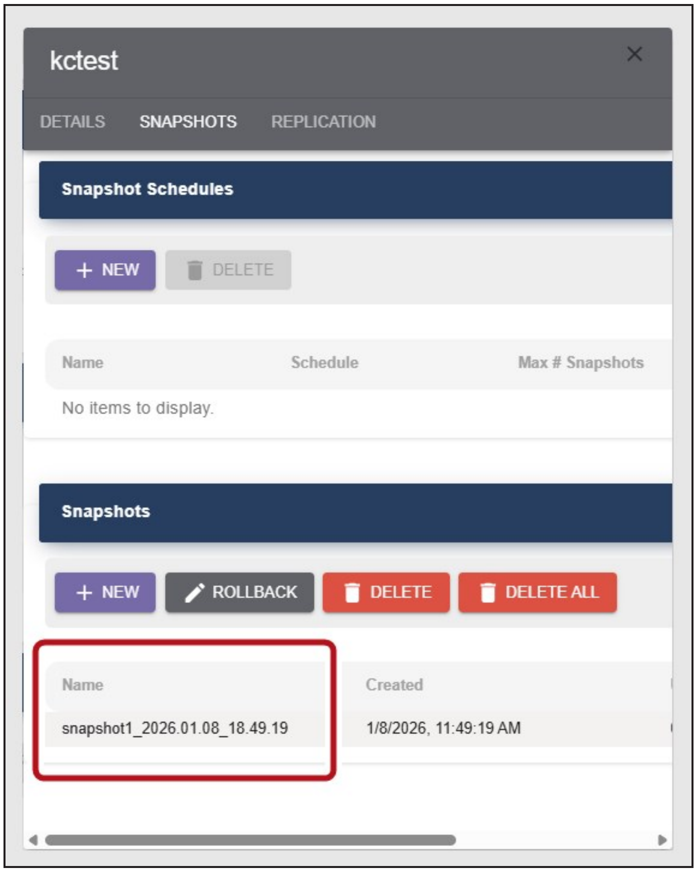
1. If necessary, locate the snapshot from which you want to restore a file.
   a. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
   b. In the Volumes pane, select the row of the volume for which you want to restore a snapshot, then click the **Details** button on the right-hand side of the row.


Volumes

Name	Status	Pool	Used	Available	Minimum Size	Maximum Size	Shared Via	Read Only	Replicated	
kctest	Normal	p1	96 KiB	14.41 TiB				Disabled	No	⧉

Figure 106 The NAS screen - Volumes pane - Details button.

c. Locate the snapshot from which you want to restore a file and record the name, if desired.



Name	Schedule	Max # Snapshots
No items to display.		

Name	Created
snapshot1_2026.01.08_18.49.19	1/8/2026, 11:49:19 AM

Figure 107 The NAS screen - Volumes pane - Snapshot name.

2. Using a remote host that has access to the shared volume for which you need to restore a single file, map the share containing the snapshot to the remote host (for example "Z:\")

3. You cannot browse to the snapshots directory using Windows explorer, you must enter the full path of the snapshot from which you want to retrieve a file in the Windows explorer address bar. Snapshots are organized as follows:

Z:\.zfs\snapshot\*snapshot name*

4. The specified directory displays. All files contained in the snapshot display.

5. Locate the file you want to restore and copy it to the appropriate location.

Multi-Factor Authentication

The Spectra BlackPearl Object Gateway offers multi-factor authentication as part of Attack Hardened storage, which enhances the security of your Gateway by using Google Authenticator or Microsoft Authenticator to confirm the identity of any user trying to log in to the BlackPearl Object Gateway. This prevents unauthorized access to the Gateway even if the user credentials needed to access the system are compromised.

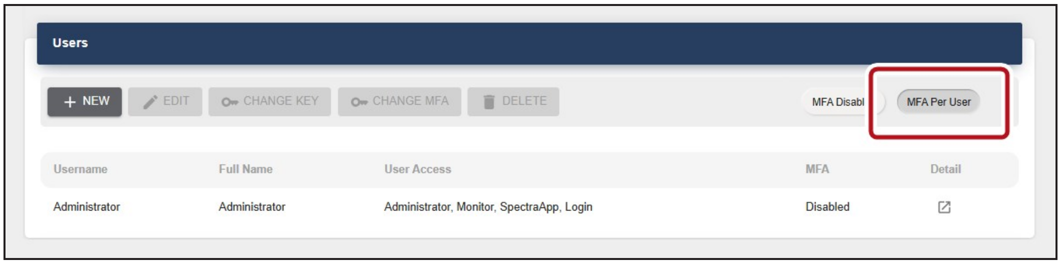
Multi-factor authentication works on a per-user basis by generating a token in the form of a QR code for a selected system user. The user scans the QR code using the Authenticator app to complete the account creation. After the QR code is scanned, the Authenticator app generates a six-digit number every 30 seconds, and does not require cell or internet access to generate these codes.

After multi-factor authentication is enabled, when the user attempts to log in to the BlackPearl user interface, after entering their username and password, they must enter the six-digit number generated by the Authenticator app within 30 seconds to complete the log in.

Enable Multi-Factor Authentication for a User

Notes:
- Only Administrator users can configure the Attack Hardened Service and enable Multi-Factor authentication for a user.
- The user account on the target system configured for NAS replication cannot use multi-factor authentication.

1. If necessary, download and install Google Authenticator or Microsoft Authenticator on your mobile phone.
2. In the BlackPearl user interface, u se the toolbar in the upper-right to select **Settings (gear icon) > Users**.

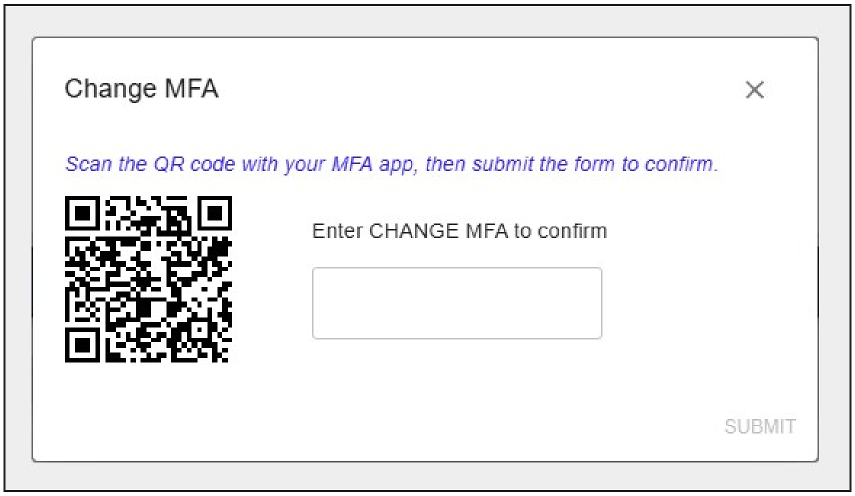


Username	Full Name	User Access	MFA	Detail
Administrator	Administrator	Administrator, Monitor, SpectraApp, Login	Disabled	↗

Figure 108 The Users screen - MFA Per User button.

3. If necessary, enable the MFA feature:
   a. Click **MFA Per User**. A confirmation screen displays (not pictured).
   b. Enter `CHANGE MFA` in the entry field, then click **Submit**.

4. Select the user and then click **Change MFA**. The Change MFA dialog box displays.



Change MFA

Scan the QR code with your MFA app, then submit the form to confirm.

Enter CHANGE MFA to confirm

Figure 109 The Change MFA dialog box.

5. Use the Authenticator app on your phone to **scan** the QR code displayed in the BlackPearl user interface. The username and BlackPearlObjectGateway name display in the Authenticator app, and the authenticator begins generating codes for the user.
6. In the BlackPearl user interface, in the Confirm MFA Code dialog box, enter `CHANGE MFA`, and click **Submit**.

   The next time the user logs into the BlackPearl user interface, they must use the code generated by the Authenticator app to complete the log in process.

Log In to a System Configured to Use Multi-Factor Authentication

1. Using a standard web browser, enter the IP address for the BlackPearl management port configured in Configure the BlackPearl Management Port on page 71.

Note: The BlackPearl user interface uses a secure connection.

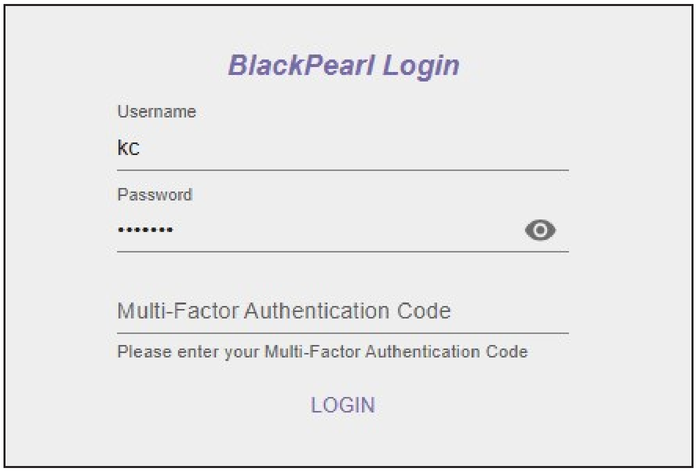
2. If necessary, resolve the security certificate warning for the BlackPearl user interface.

   The BlackPearl Object Gateway ships with non-signed SSL certificates for both the data and management ports. When using the shipped certificates, you must pass a security check every time you attempt to access the management port to view the BlackPearl user interface, or when you attempt to transfer data using the data port.

Notes:

- The absence of the certificate does not affect functionality.
- If desired, you can install signed, trusted SSL certificates for your data and management ports so that you no longer need to pass the security check when accessing these ports. See Configure Certificates on page 92.

3. Enter the **Username** and **Password**.



BlackPearl Login

Username

kc

Password

•••••••

Multi-Factor Authentication Code

Please enter your Multi-Factor Authentication Code

Figure 110 The Login screen with Multi-Factor Authentication enabled on the system.

4. Using Google Authenticator on your phone, enter the six-digit **Multi-Factor Authentication Code** for the user.

Notes:

- The code refreshes every 30 sections. If the code refreshes before you complete the login, you must clear the field and enter the new code.
- If you have more than one user or BlackPearl Object Gateway configured in Google Authenticator, use the *username@systemname* to locate the correct code. The system name is displayed under the product name on the login screen.

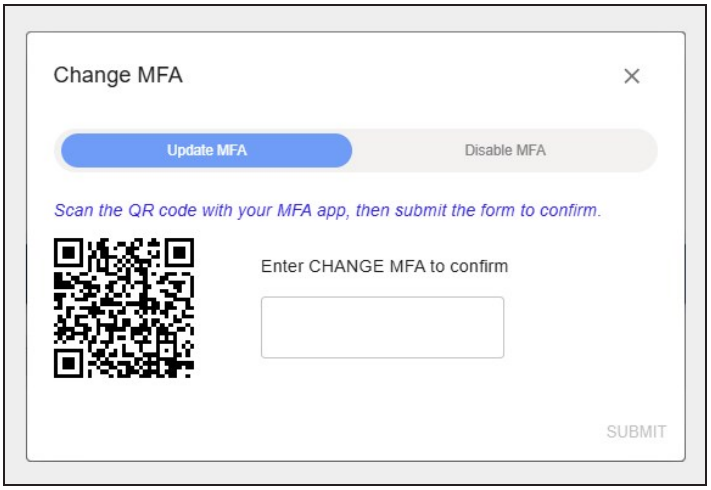
5. Click **Login**.

Update Multi-Factor Authentication for a User

If desired, you can update the token that the Authenticator app uses to generate the MFA code. This is necessary if you disabled the Attack Hardened service, and then later re-enabled the service. This can also be used to provide enhanced security as required by your security environment by updating authentication credentials while still maintaining access for the user.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.

2. Select the user and then click **Change MFA**. The Change MFA dialog box displays.
3. Use the slider to select **Update MFA**.



Scan the QR code with your MFA app, then submit the form to confirm.

Enter CHANGE MFA to confirm

Figure 111 The Change MFA dialog box.

4. Use the Authenticator app on your phone to **scan** the QR code displayed in the BlackPearl user interface. The username and BlackPearl Object Gateway name display in the Authenticator app, and the authenticator begins generating codes for the user.
5. In the BlackPearl user interface, in the Confirm MFA Code dialog box, enter `CHANGE MFA`, and click **Submit**.

   The next time the user logs into the BlackPearl user interface, they must use the code generated by the Authenticator app to complete the log in process.

Disable Multi-Factor Authentication for a User

Use this option to no longer require a user to enter an MFA code when logging in to the BlackPearl user interface.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.
2. Select the user and then click **Change MFA**. The Change MFA dialog box displays (not shown).
3. Use the slider to select **Disable MFA**.
4. In the dialog box, enter `CHANGE MFA`, and click **Submit**.

   The user is no longer required to enter a six-digit authentication code when logging in to the BlackPearl user interface.

Disable the Attack Hardened Service

Disabling the Attack Hardened service disables multi-factor authentication for the BlackPearl Object Gateway.

Note: Disabling the Attack Hardened service deletes the tokens for all users configured to use multi-factor authentication. If you re-enable the Attack Hardened service, each user will need to update their multi-factor authentication token. See Multi-Factor Authentication on page 185.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.
2. In the upper-right corner of the Users pane, click **MFA Disabled**. A confirmation screen displays (not pictured).
3. Enter `CHANGE MFA` in the entry field, then click **Submit**.

CONFIGURE AND USE ENCRYPTION

If your BlackPearl Object Gateway includes disk or solid state Self Encrypting Drives (SEDs), use the encryption service to set the level of encryption, configure passwords, and unlock the drives so that they are usable for data transfer.

Notes:

- An activation key is required to enable this feature.
- This feature only applies to disk-based storage. Tape storage encryption is configured on the tape library. See your Tape Library User Guides on page 22 for information about tape encryption.
- The encryption provided by SEDs is 'encryption at rest'. If a drive is stolen the data on it is unreadable.

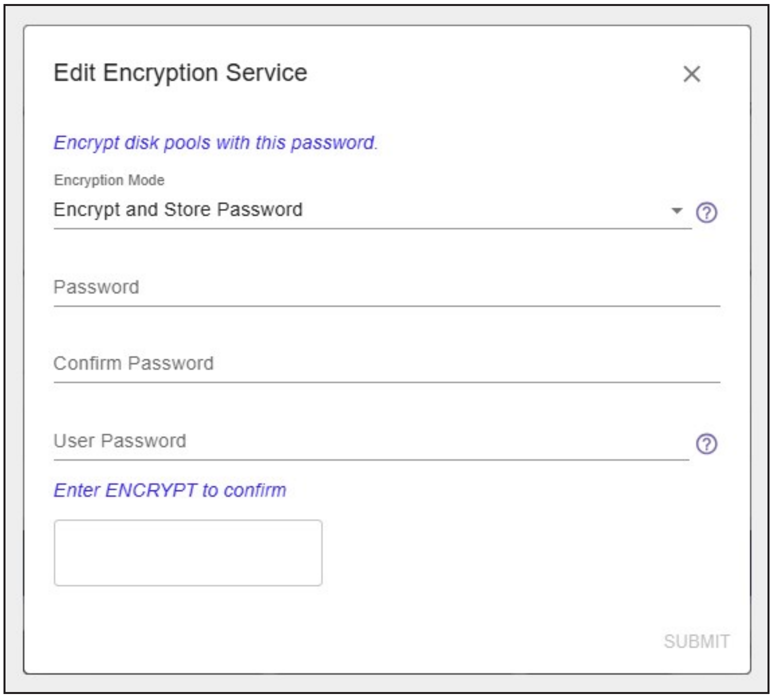
Configure the Encryption Service

Use the encryption service to set the level of encryption and create a password to unlock the drives following a Gateway power cycle. You can select to store the password on the Gateway, so that the drives are unlocked automatically, or to save the password to a USB key that is used when needed to unlock the drives, and is otherwise stored in a safe location.

CAUTION Spectra Logic recommends creating and storing multiple copies of the password used to encrypt data to avoid losing access to encrypted data.

1. If necessary, enter the activation key to enable the encryption service as described in Manually Enter Activation Keys on page 364.
2. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.

3. In the Encryption pane of the Users screen, click **Edit Service**. The Edit Encryption Service dialog box displays.



Edit Encryption Service

Encrypt disk pools with this password.

Encryption Mode: Encrypt and Store Password

Figure 112 The Edit Encryption Service dialog box.

4. Use the **Encryption Mode** drop-down menu to set the encryption mode.

Parameter	Description
No Encryptio n	This setting is included in the drop-down menu as the default so that you do not accidentally select an undesired mode of encryption. If selected, the self-encrypting drives do not use encryption. Data stored on the drives is not encrypted. **Note:** This setting does not disable encryption on the drives once they are encrypted. Drives must be set to unencrypted for each storage pool. See Configure and Use Encryption on the previous page for instructions.
Encrypt and Store Password	The self-encrypting drives encrypt data transferred to them, and the password to unlock the drives is stored on the BlackPearl Object Gateway. The drives are automatically unlocked when the BlackPearl Object Gateway initializes. ⚠ **CAUTION** Even though the password is stored on the system, it is important to record the password and store it in a secure location to avoid losing access to the encrypted data. The password may also be required in the cases of chassis replacement, or the addition of more BlackPearl Object Gateways to the storage architecture that may access the encrypted drives. Spectra Logic recommends storing multiple copies of the password.

5. Enter a **Password** to unlock the self-encrypting drives, and then **Confirm** the password.

6. Enter the **User Password** of the user currently logged in to the BlackPearl user interface.
7. If necessary, enter the **Multi Factor Authentication** code for the user (not shown). See Multi-Factor Authentication on page 185 for information on obtaining the multi-factor authentication code.

Note: This field only displays if multi-factor authentication is enabled for the currently logged in user.

8. Enter `ENCRYPT` into the confirmation dialog box.
9. Click **Submit**.

Note: You may need to navigate away from the encryption details screen and then back for the Gateway to update the information on the details screen.

Export Encryption Key to USB Drive

Use the instructions in this section to export the encryption key to a USB drive for storage in case of disaster recovery. This key can be used to re-import the encryption key if necessary.

CAUTION Spectra Logic recommends creating and storing multiple copies of the password used to encrypt data to avoid losing access to encrypted data. Additionally, Spectra Logic recommends exporting the encryption key to multiple types of storage media. See Configure and Use Encryption on page 190

1. Connect a USB key in to a USB port on the rear of the BlackPearl chassis.
2. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
3. In the Encryption pane on the Users screen, click **USB Key**. The Export Key to USB dialog box displays (not shown).
4. Enter the **User Password** of the user currently logged into the BlackPearl user interface.
5. Click **Submit**.

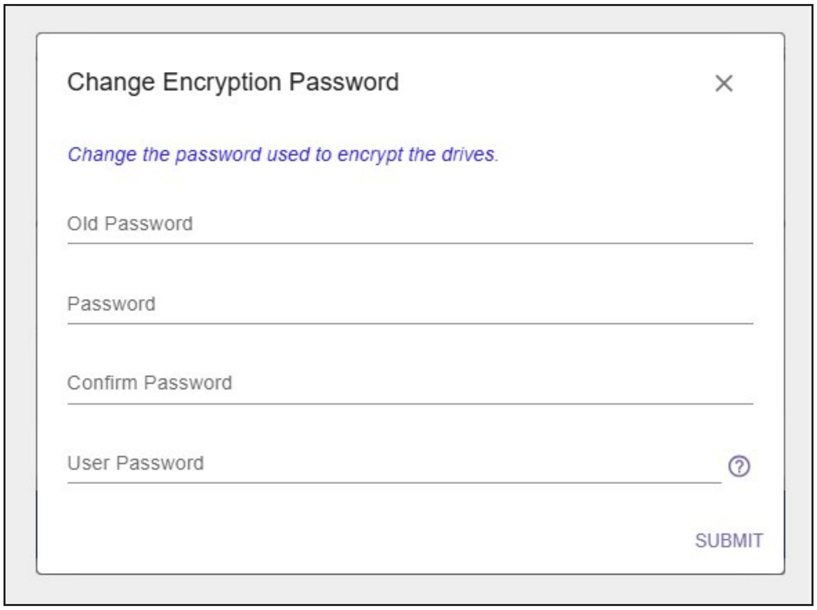
Note: Once created, remove the USB key from the Gateway and store it in a safe location until it is needed.

Change the Encryption Password

If desired, you can change the password used to unlock the self-encrypting drives.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the Encryption pane on the Users screen, click **Change Password**. The Change Encryption Password dialog box displays.

Note: If multi-factor authentication is enabled for the user currently logged in to the BlackPearl user interface, an additional entry field displays in the Change Encryption Password dialog box. (Additional entry field not shown).


Change Encryption Password

Change the password used to encrypt the drives.

Old Password

Password

Confirm Password

User Password

Figure 113 The Change Encryption Password dialog box.

3. Enter the current password in the **Old Password** entry field.
4. Enter the desired new **Password**, and then **Confirm Password**.
5. Enter the **User Password** of the user currently logged in to the BlackPearl user interface.
6. If necessary, enter the **Multi Factor Authentication** code for the user. See Multi-Factor Authentication on page 185 for information on obtaining the multi-factor authentication code.

Note: This field only displays if multi-factor authentication is enabled for the currently logged in user.

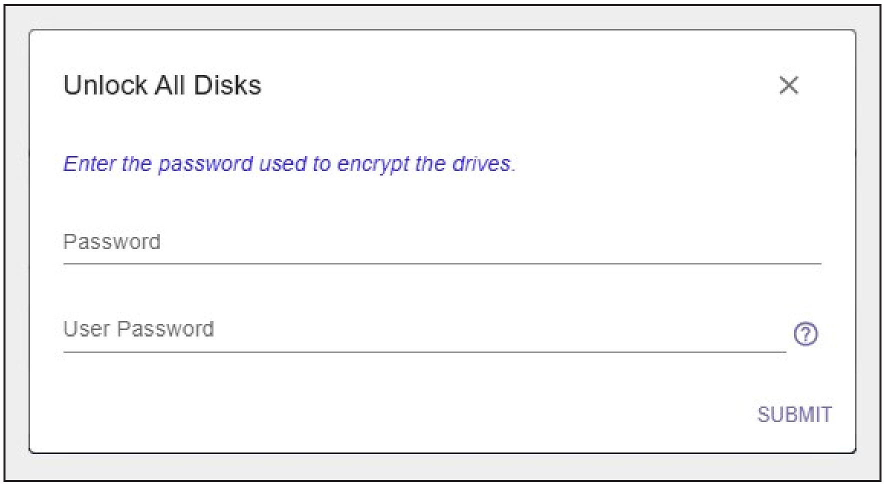
7. Click **Submit**.

IMPORTANT After changing the password, update the USB keys and/or manual records stored in secure locations.

Unlock the Self-Encrypting Drives

If necessary, use the instructions below to manually unlock the self-encrypting drives after the Gateway initializes.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the Encryption pane on the Users screen, click **Unlock All Disks**. The Unlock All Disks dialog box displays.



Unlock All Disks

Enter the password used to encrypt the drives.

Password

User Password

Figure 114 The Unlock All Disks dialog box.

3. Enter the encryption **Password**.
4. Enter the **User Password** of the user currently logged in to the BlackPearl user interface.
5. Click **Submit**.

PSID Erase an Encryption Drive

If you forget the encryption password, you are unable to unlock the drives. If you want to reuse the drives, you need to erase the drive by entering the Physical Secure ID (PSID) in the BlackPearl user interface.

The PSID string is printed on the label physically attached to the drive. It is not available from any other source. Before you can perform a PSID erase, you must remove the drive from the enclosure and record its PSID value.

Note: PSID erasure of a drive is useful if you need to return a failed drive to Spectra Logic. When a drive is PSID erased, Spectra Logic cannot access data on the drive.

CAUTION Performing a PSID Erase on a drive makes all data on the drive permanently inaccessible.

Use the instructions in this section to perform a PSID erase on the drive.

To PSID erase a drive, you must access the legacy user interface used in BlackPearl OS 5.8.x and earlier. Functionality to PSID erase a drive will be added to the new user interface in a later version of the BlackPearl OS.

1. Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with "/legacy". For example:

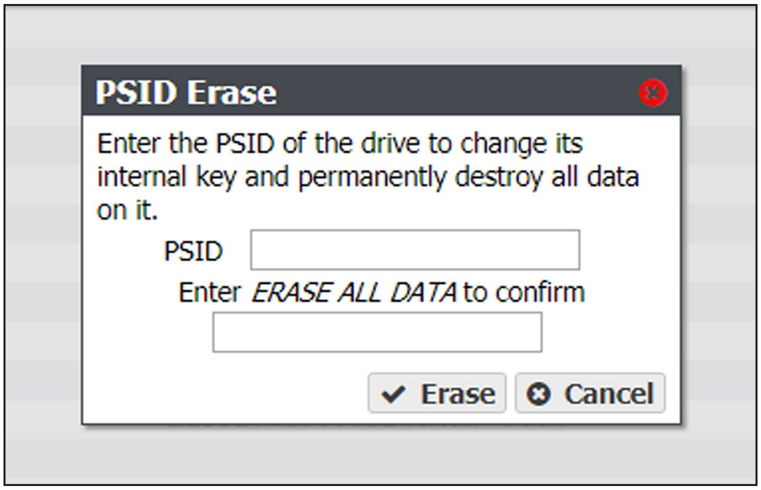
   https://*ipaddress*/legacy

2. Use the toolbar in the upper-right to select **Status > Hardware** or click the Hardware pane on the Dashboard, or click the Hardware link on the status bar. The Hardware screen displays.
3. Click **Data Drives**. The hardware screen refreshes and displays all disk drives present in the Gateway.
4. Record the slot number and serial number for each drive you want to PSID erase.
5. Power down the Gateway as described in Reboot or Shut Down a BlackPearl Object Gateway on page 267.
6. Locate the drive(s) in the chassis using the slot number and verify the serial number(s) you recorded in Step 4.
7. Locate the PSID value on the drive label and record the value.
8. Repeat for any additional drives you want to erase.
9. Power on the Gateway as described in Power On the Gateway on page 69.
10. Log into the BlackPearl legacy user interface as described in Step 1 on page 195.

11. Use the toolbar in the upper-right to select **Status > Hardware** or click the Hardware pane on the Dashboard, or click the Hardware link on the status bar. The Hardware screen displays.

12. Click **Data Drives**. The hardware screen refreshes and displays all disk drives present in the Gateway.

13. On the row of the drive you want to erase, click **PSID Erase**. The PSID Erase dialog box displays.



PSID Erase

Enter the PSID of the drive to change its internal key and permanently destroy all data on it.

PSID

Enter *ERASE ALL DATA* to confirm

Figure 115 The PSID Erase dialog box.

14. Enter the PSID value you recorded in Step 4 on page 195 in the **PSID** entry field.

15. Type `ERASE ALL DATA` in the confirmation entry field.

CAUTION Performing a PSID Erase on a drive permanently erases all data on the drive.

16. Click **Erase**.

17. Repeat for any additional drives you want to erase.

DATABASE BACKUP

The BlackPearl Object Gateway database contains a list of all objects stored on the system cache, tape, and disk media. Backing up the database allows you to restore the database in the event of hardware failure. The database backup does not function as a true backup in that it does not backup or restore objects referenced in the database, only the database itself.

IMPORTANT If the database is lost, no data is lost, but retrieval becomes difficult. Therefore, scheduling regular backups of the database is a best practice to ensure long term reliable operation.

When restoring a database, the Gateway is not aware of any changes to data after creating the database backup.

- Files that exist in the database, but were deleted after the creation of the database backup are not restored.
- New files added or modified after the creation of the database backup are still persisted on a storage medium.

Verify disk pools and tape media so that the database synchronizes with the actual data present on the Gateway.

Database backups are stored on a bucket on the BlackPearl Object Gateway, and kept based on the settings of a preconfigured data policy named “Database Backup”.

If desired, you can modify the settings of the preconfigured data policy, or create a new data policy for database backups (see Create a Data Policy on page 127). If you create a new data policy, you will need to edit the database backup configuration to use the new policy (see Edit Database Backup Data Policy on page 201).

Note: Spectra Logic recommends using the default data policy.

The bucket used for database backups is automatically created when the first backup is generated, either manually, or on a schedule. The database backup bucket is listed on the Buckets screen of the BlackPearl user interface with the name “Spectra-BlackPearl-Backup-*system name-product serial number*“. This bucket cannot be used for data storage.

Note: If you change the system name after the database backup bucket is created, the bucket name does not change.

Backups can be generated manually, or by schedule. When creating a database backup schedule, you specify how many copies of the database to keep at one time. When the Gateway generates a backup that exceeds the value configured, the oldest database backup is automatically deleted.

Note: The default schedule on the BlackPearl Object Gateway generates a backup once per day, and retains a maximum of two backups.

IMPORTANT Creating a backup of the database is a process intensive procedure. Spectra Logic recommends configuring a backup schedule to run during periods of low Gateway activity. Additionally, creating only one backup a day is recommended.

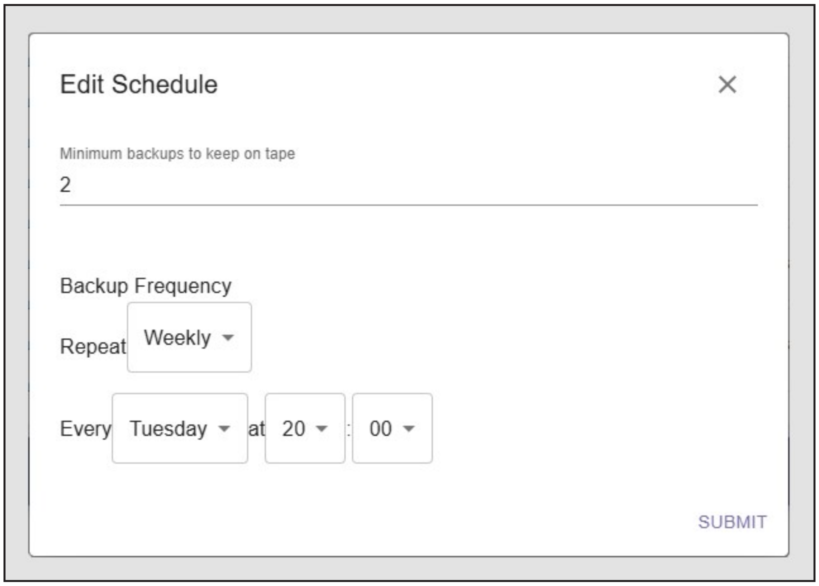
Note: If your BlackPearl Object Gateway does not contain any permanent local storage, the database backup file must be downloaded manually to your host computer.

Configure a Database Backup Schedule

Database backup schedules can be configured at intervals based on the number of hours, number of days, or days of the week.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Database Backup**.
2. In the Backup Schedule pane, click **Edit**. The Edit Schedule dialog box displays.

Note: Spectra Logic recommends offsetting the minutes after the hour for starting database backups so that there are not a large number of jobs starting at exactly the same time.



Edit Schedule

Minimum backups to keep on tape
2

Backup Frequency

Repeat Weekly

Every Tuesday at 20 : 00

Figure 116 The Edit Schedule dialog box.

3. Enter a number for the **Minimum backups to keep on tape**. When the Gateway generates a backup, it determines the number of fully persisted backups and automatically deletes the oldest backups exceeding this number.

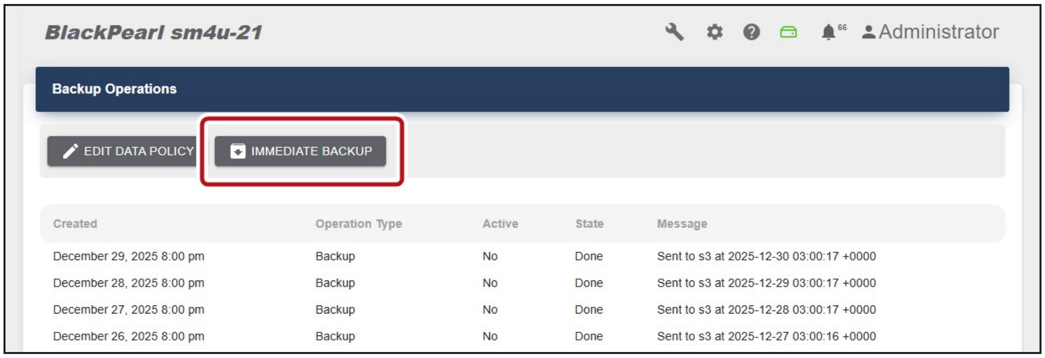
Note: Although the minimum number of backups is always respected, at some times there may be more than the minimum present on the Gateway.

4. Use the **Repeat** drop-down menu to select one of the following:
   - Select **Hourly** and use the **Hours** and **Minute** drop-down menus to select values for **Every _ Hours at Minute _**. These values specify the interval in hours between generating database backups, and the number of minutes after the top of the hour when the job starts. For example, if the values are set to 4 and 15, a backup is created every four hours, at 15 minutes after the hour.
   - Select **Daily** and enter a value for **Every** to specify the interval, in days, between generating database backups. Then use the **Hour** and **Minute** drop-down menus to specify the time of day to create the backup.
   - Select **Weekly** and use the **Every** drop-down menu to select one or more day(s) of the week on which to generate a backup. Then use the **Hour** and **Minute** drop-down menus to specify the time of day to create the backup.
5. Click **Submit**.

Manually Generate a Database Backup

Use the instructions in this section to create a database backup manually.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Database Backup**.



Created	Operation Type	Active	State	Message
December 29, 2025 8:00 pm	Backup	No	Done	Sent to s3 at 2025-12-30 03:00:17 +0000
December 28, 2025 8:00 pm	Backup	No	Done	Sent to s3 at 2025-12-29 03:00:17 +0000
December 27, 2025 8:00 pm	Backup	No	Done	Sent to s3 at 2025-12-28 03:00:17 +0000
December 26, 2025 8:00 pm	Backup	No	Done	Sent to s3 at 2025-12-27 03:00:16 +0000

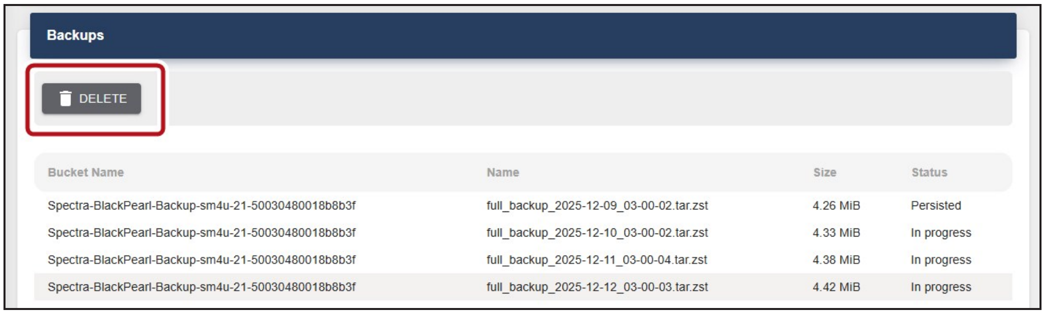
Figure 117 The Database Backup screen - Backup Operations pane - Immediate Backup button

2. In the Backup Operations pane, click **Immediate Backup**. A confirmation window displays (not shown).
3. Click **Submit**.

Delete a Database Backup

Use the following instructions to delete a database backup.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Database Backup**.



Bucket Name	Name	Size	Status
Spectra-BlackPearl-Backup-sm4u-21-50030480018b8b3f	full_backup_2025-12-09_03-00-02.tar.zst	4.26 MiB	Persisted
Spectra-BlackPearl-Backup-sm4u-21-50030480018b8b3f	full_backup_2025-12-10_03-00-02.tar.zst	4.33 MiB	In progress
Spectra-BlackPearl-Backup-sm4u-21-50030480018b8b3f	full_backup_2025-12-11_03-00-04.tar.zst	4.38 MiB	In progress
Spectra-BlackPearl-Backup-sm4u-21-50030480018b8b3f	full_backup_2025-12-12_03-00-03.tar.zst	4.42 MiB	In progress

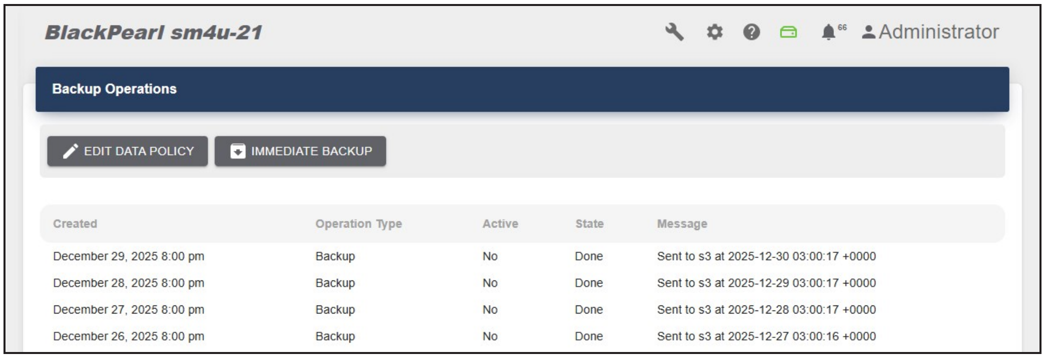
Figure 118 The Database Backup screen - Backup Operations pane - Delete button

2. In the Backups pane, select the backup you want to delete and click **Delete**. A confirmation window displays (not shown).
3. Enter `DELETE BACKUP` in the entry field.
4. Click **Delete**.

Edit Database Backup Data Policy

Use the following instructions to edit the data policy used for the database backup bucket.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Database Backup**.

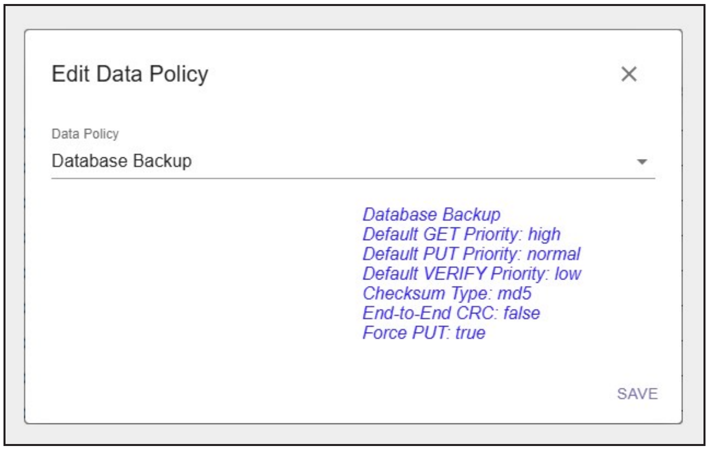


BlackPearl sm4u-21

Created	Operation Type	Active	State	Message
December 29, 2025 8:00 pm	Backup	No	Done	Sent to s3 at 2025-12-30 03:00:17 +0000
December 28, 2025 8:00 pm	Backup	No	Done	Sent to s3 at 2025-12-29 03:00:17 +0000
December 27, 2025 8:00 pm	Backup	No	Done	Sent to s3 at 2025-12-28 03:00:17 +0000
December 26, 2025 8:00 pm	Backup	No	Done	Sent to s3 at 2025-12-27 03:00:16 +0000

Figure 119 The Database Backup screen - Backup Operations pane - Immediate Backup button

2. Click **Edit Data Policy**. The Edit Data Policy screen displays.



Edit Data Policy

Data Policy: Database Backup

Database Backup
Default GET Priority: high
Default PUT Priority: normal
Default VERIFY Priority: low
Checksum Type: md5
End-to-End CRC: false
Force PUT: true

Figure 120 The Edit Data Policy screen.

3. Use the **Data Policy** drop-down menu to select a new data policy for the database backup bucket. The text of the screen changes as you select the new data policy to display the configuration settings for the selected data policy.
4. Click **Save**.

CHAPTER 7 - ADDITIONAL CONFIGURATION OPTIONS

This chapter describes using the BlackPearl user interface to configure additional options for the Spectra BlackPearl Object Gateway.

Configure Users

Use the instructions in this section to edit existing users, change passwords, and configure the session timeout setting.

Description of User Types

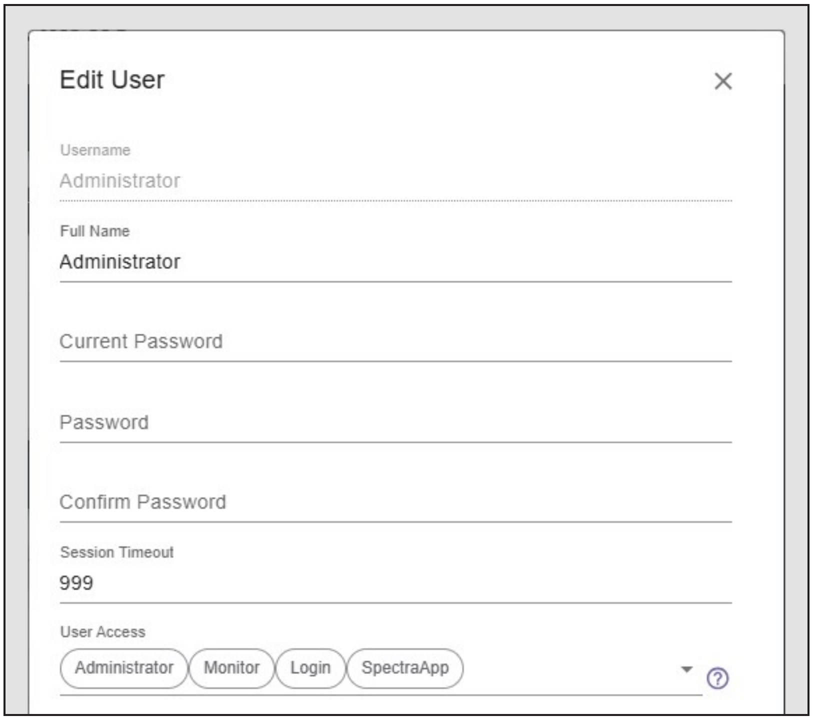
See Description of User Permissions on page 82 for information about each user type.

Create a User

To create a user, see Create a User on page 82.

Edit a User

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.
2. Select the user you want to edit and click **Edit**. The Edit Users screen displays.



Edit User

Username: Administrator

Full Name: Administrator

Current Password

Password

Confirm Password

Session Timeout: 999

User Access: Administrator, Monitor, Login, SpectraApp

Figure 121 The Edit User dialog box - General settings.

3. The **Username** is unavailable and cannot be changed.
4. If desired, edit the user's **Full Name**.

5. If you are changing the password, enter the **Current Password**, the desired **New Password**, and then **Confirm Password**.

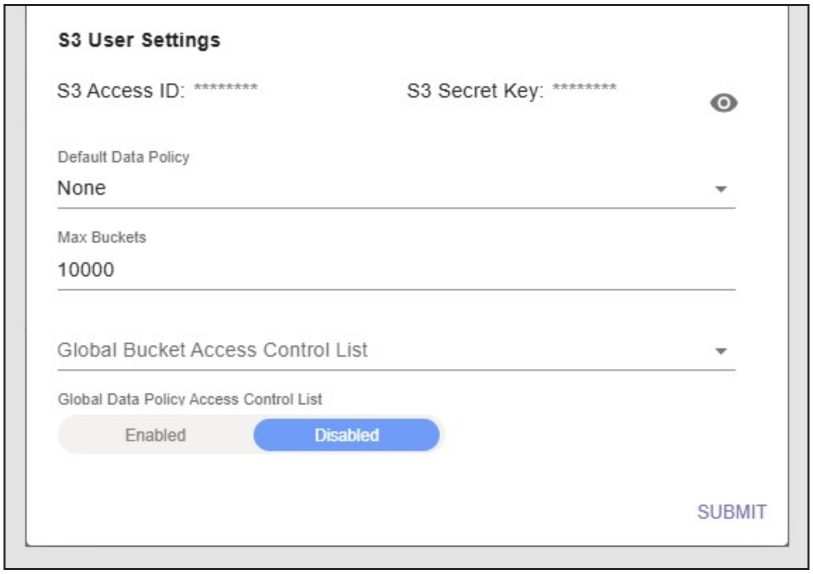
Note: The new password does not take effect until after you log out of the BlackPearl user interface (see Exit the BlackPearl User Interface on page 1).

6. If desired, edit the value for the **Session Timeout** in minutes. This value cannot exceed 999 minutes.

7. Select or clear one or more **User Access** permissions. See Description of User Permissions on page 82 for information on each level of user access permission.

8. Unless directed by Spectra Logic Technical Support, leave the **Remote Support** slider set to **Disabled**.

9. The Amazon compatible **S3 Access ID** and **S3 Secret Key** fields are automatically populated and cannot be changed when editing a user.



S3 User Settings

S3 Access ID: ********

S3 Secret Key: ********

Default Data Policy: None

Max Buckets: 10000

Global Bucket Access Control List

Global Data Policy Access Control List: Enabled [✓ Disabled]

Figure 122 The Edit User dialog box - S3 User Settings.

10. If desired, use the **Default Data Policy** drop-down menu to select a data policy for the user. The Gateway uses the selected data policy for all buckets created by the user, unless a different policy is specified during bucket creation.

11. If desired, edit the value for the **Max Buckets** the user is allowed to create.

12. Select or clear options for the **Global Bucket Access Control List**. These options give or deny permission for the user being created to perform the action described in the table below, for all buckets present on the Gateway, as well as any buckets created at a future date.

Name	Description
List	The user can see the bucket and can list the objects in a bucket.
Read	The user can get objects and create GET jobs.
Write	The user can put objects and create PUT jobs.
Delete	The user can delete objects, but cannot delete the bucket.
Job	The user can modify or cancel jobs created by other users. The user can also see the details of jobs created by other users. **Note:** All users can view all jobs, but by default, only the initiator of the job can see the full details of a job.
Owner	The user receives full access to all buckets, including all permissions listed above.

13. Use the **Global Data Policy Access Control List** slider to select one of the following:

- **Enabled** - Allows the user to use to any data policy created on the Gateway.
- **Disabled** - The user can only use the data policy configured in Step 10 on page 204.

14. Click **Save**.

Change Amazon Compatible S3 Secret Key

If an Amazon compatible S3 secret key is compromised, or you otherwise want to change it, use the instructions in this section to change an Amazon compatible S3 secret key for a user.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.
2. Select the user you want to change the S3 keys and click **Change Key**. The Change S3 Secret Key dialog box displays.

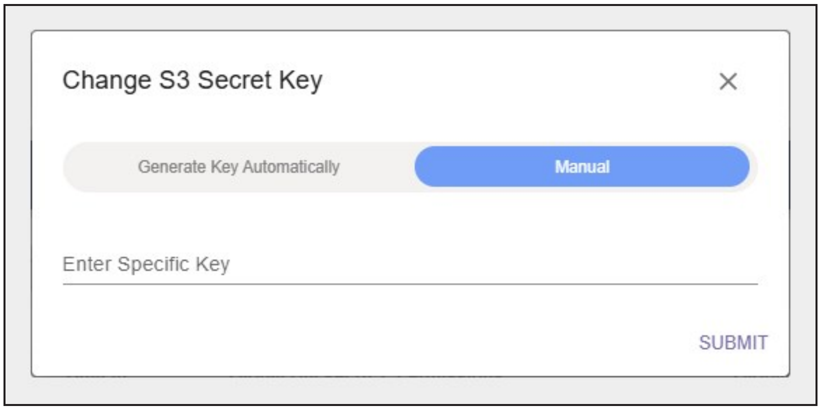


Figure 123 The Change S3 Secret Key dialog box.

3. Use the slider to select one of the following:
   - **Generate Key Automatically** - The key is generated automatically by the system when you complete the wizard.
   - **Manual** - The key must be entered manually in the **Enter Specific Key** entry field.
4. Click **Submit**.

Delete a User

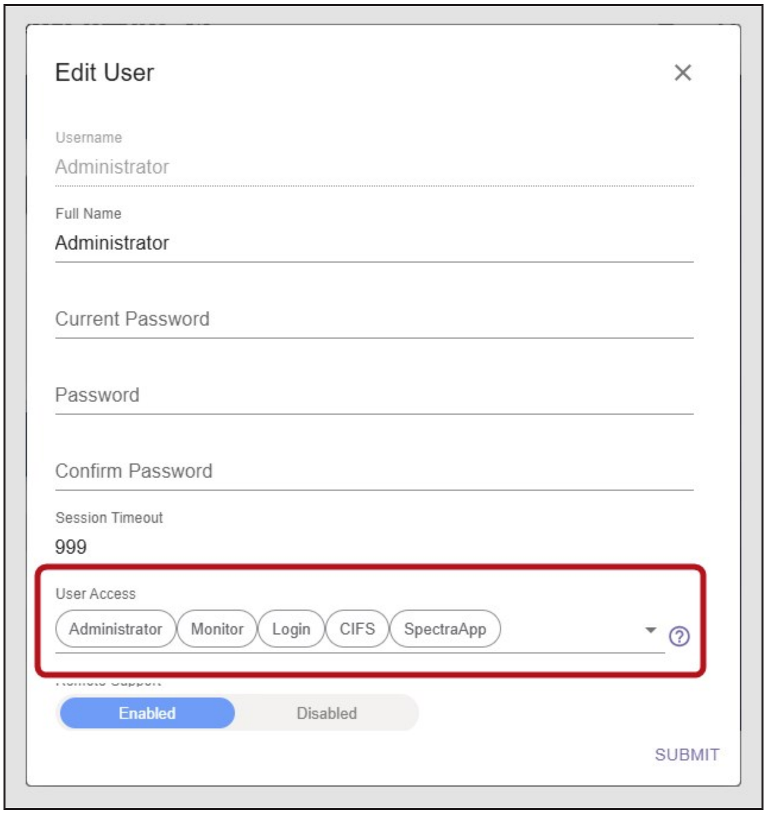
1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.
2. Select the user you want to delete and click **Delete**. The Delete User confirmation screen displays.
3. Click **Delete** to delete the user.

Enable CIFS User Access

If you are creating CIFS shares and if your Windows environment does not use Active Directory, you must edit a user to enable CIFS user access, also known as local administrator status.

Note: Alternatively, you can create a new user with CIFS user access. See Create a User on page 82.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.
2. Select the user and click **Edit**. The Edit User dialog box displays.



Edit User

Username: Administrator

Full Name: Administrator

Current Password

Password

Confirm Password

Session Timeout: 999

User Access: Administrator, Monitor, Login, CIFS, SpectraApp

Figure 124 The Edit User dialog box.

3. Use the **User Access** drop-down menu to select **CIFS**.
4. If desired, change other settings as described in Edit a User on page 203.
5. Click **Submit**.
6. Continue to Configure Users on page 203.

Configure Amazon Compatible S3 Groups

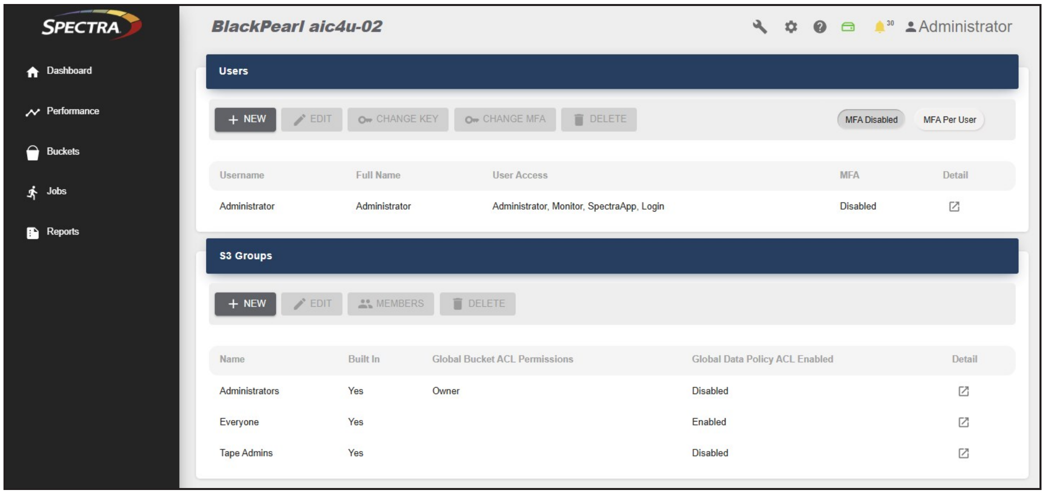
Use the instructions in this section to create, edit, or delete an Amazon compatible S3 user group.

Create an Amazon Compatible S3 Group

An Amazon compatible S3 group on the BlackPearl Object Gateway is a group of previously created Amazon compatible S3 users. Members of an S3 group can be individual users, or groups of users. When creating an S3 group, you specify the global bucket and data policy access control lists.

Use the instructions in this section to create a new Amazon compatible S3 group.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.

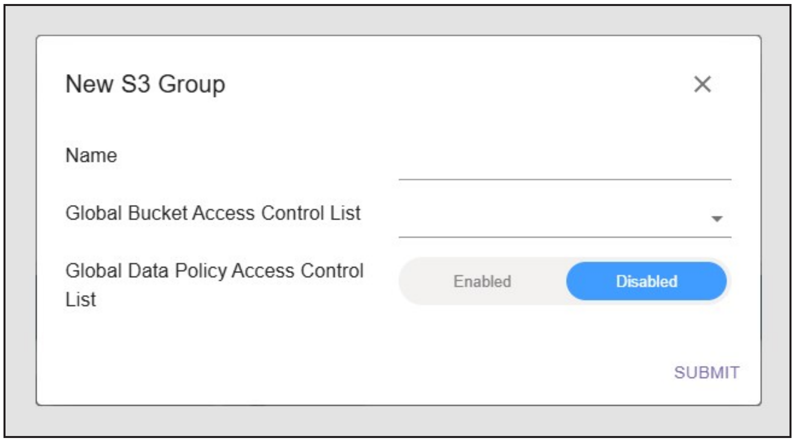


Username	Full Name	User Access	MFA	Detail
Administrator	Administrator	Administrator, Monitor, SpectraApp, Login	Disabled	☐

Name	Built In	Global Bucket ACL Permissions	Global Data Policy ACL Enabled	Detail
Administrators	Yes	Owner	Disabled	☐
Everyone	Yes		Enabled	☐
Tape Admins	Yes		Disabled	☐

Figure 125 The Users screen.

2. In the S3 Groups pane, click **New**. The New S3 Group dialog box displays.



New S3 Group

Name

Global Bucket Access Control List

Global Data Policy Access Control List: Enabled [✓ Disabled]

Figure 126 The New S3 Group dialog box.

3. Enter a **Name** for the group.
4. Use the **Global Bucket Access Control List** drop-down menu to select one or more options for the group. These options give or deny permission for the group being created to perform the action described in the table below, for all buckets present on the Gateway, as well as any buckets created at a future date.

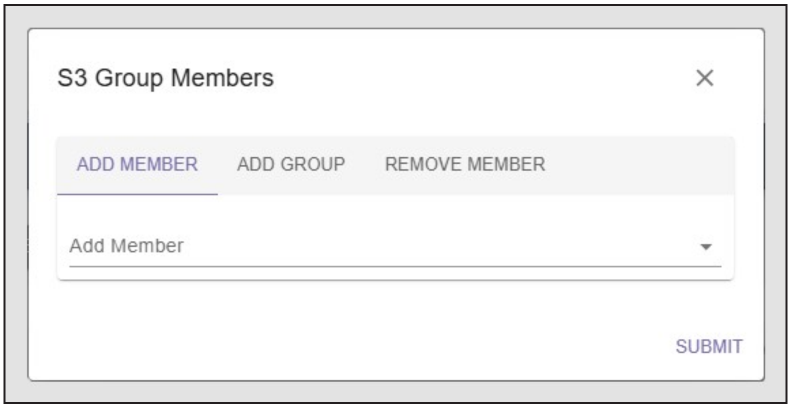
Note: The access control list options selected for an Amazon compatible S3 group complement the options previously selected for each member of the group. For example, if a user has Read permission and is added to an Amazon compatible S3 group that has Write permission, the user now has both Read and Write permissions.

Name	Description
List	The Amazon compatible S3 group can see the bucket and can list the objects in a bucket.
Read	The Amazon compatible S3 group can get objects and create GET jobs.
Write	The Amazon compatible S3 group can put objects and create PUT jobs.
Delete	The Amazon compatible S3 group can delete objects, but cannot delete the bucket.
Job	The Amazon compatible S3 group can modify or cancel jobs created by other users. The Amazon compatible S3 group can also see the details of jobs created by other users. **Note:** All users can view all jobs, but by default, only the initiator of the job can see the full details of a job.
Owner	The Amazon compatible S3 group receives full access to all buckets, including all permissions listed above.

5. Use the **Global Data Policy Access Control List** slider to select one of the following:
   - **Enabled** - Select this option to allow the user access to any data policy created on the Gateway.
   - **Disabled** - Select this option to configure the user group to only be able to access data policies created by the users in the user group.
6. Click **Submit**.

Add a Member or Group to an S3 Group

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.
2. In the S3 Groups pane, select the S3 group to which you want to add members, then click **Members**. The S3 Group Members dialog box displays.



S3 Group Members

Figure 127 The S3 Group Member dialog box.

- To add a member:
  a. Click **Add Member** at the top of the dialog box.
  b. Use the **Add Member** drop-down menu to select one or more members to add to the S3 group.
- To add a group:
  a. Click **Add Group** at the top of the dialog box.
  b. Use the **Add Group** drop-down menu (not shown) to select one or more groups to add to the S3 group.

3. Click **Submit**.

Remove an S3 Group Member

Use the following instructions to remove a user from an Amazon compatible S3 group.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.
2. In the S3 Groups pane, select the S3 group to which you want to remove members, then click **Members**. The S3 Group Members dialog box displays.

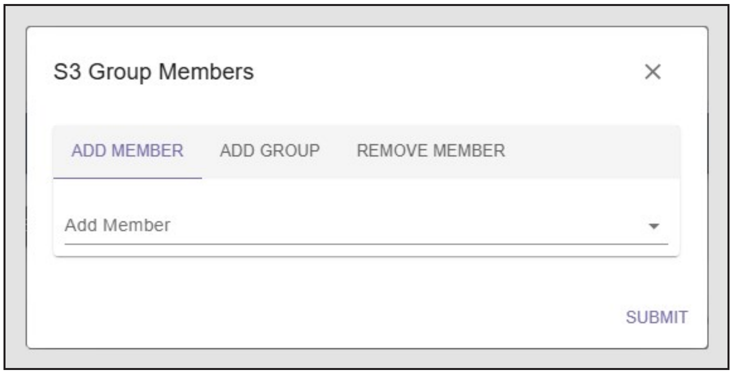


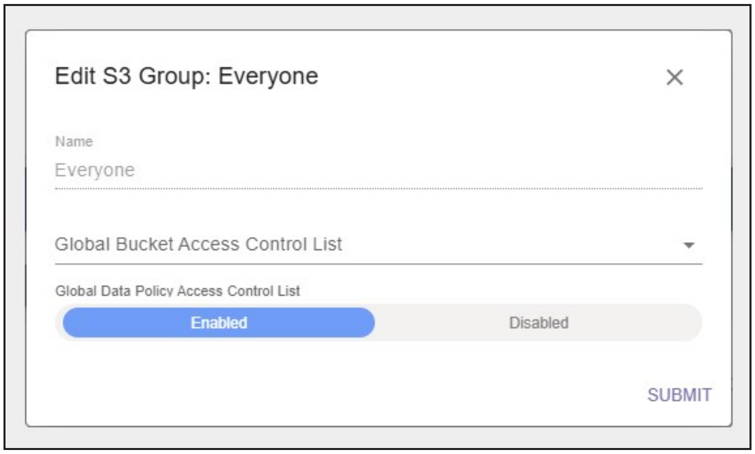
Figure 128 The S3 Group Member dialog box.

3. Click the **Remove Member** tab.
4. Use the **Remove Members** drop-down menu to select one or more group member(s) that you want to remove.
5. Click **Submit**.

Edit an S3 Group

Use the following instructions to edit an Amazon compatible S3 group.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.
2. In the S3 Groups pane, select the S3 group to which you want to remove members, then click **Edit**. The Edit S3 Group: *Group Name* dialog box displays.


Edit S3 Group: Everyone

Name: Everyone

Global Data Policy Access Control List: Enabled

Figure 129 The Edit S3 Group: *Group Name* dialog box.

3. Use the **Global Bucket Access Control List** drop-down menu to select permissions for the S3 Group. These options give or deny permission for the group to perform the action described in the table below, for all buckets present on the Gateway, as well as any buckets created at a future date.

Name	Description
List	The Amazon compatible S3 group can see the bucket and can list the objects in a bucket.
Read	The Amazon compatible S3 group can get objects and create GET jobs.
Write	The Amazon compatible S3 group can put objects and create PUT jobs.
Delete	The Amazon compatible S3 group can delete objects, but cannot delete the bucket.
Job	The Amazon compatible S3 group can modify or cancel jobs created by other users. The Amazon compatible S3 group can also see the details of jobs created by other users. **Note:** All users can view all jobs, but by default, only the initiator of the job can see the full details of a job.
Owner	The Amazon compatible S3 group receives full access to all buckets, including all permissions listed above.

4. Use the **Global Data Policy Access Control List** slider to select one of the following:
   - **Enabled** - Select this option to allow the user access to any data policy created on the Gateway.
   - **Disabled** - Select this option to configure the user group to only be able to access data policies created by the users in the user group.
5. Click **Submit**.

Delete an S3 Group

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.
2. In the S3 Groups pane, select the S3 group to which you want to delete, then click **Delete**. A confirmation screen displays (not shown).
3. Click **Delete** to delete the Amazon compatible S3 group.

Chapter 8 - Managing Object Storage Settings

This chapter describes using the BlackPearl user interface to manage storage domains, data policies, disk partitions, and buckets on the Gateway after configuring object storage. For initial object storage configuration steps, see Configuring Object Storage on page 110.

Amazon Compatible S3 Operations

Use the instructions in this section to manually download an object, view, edit, or cancel an Amazon compatible S3 job, to manually start the datapath backend, and to allow or disallow new jobs.

Download an Object

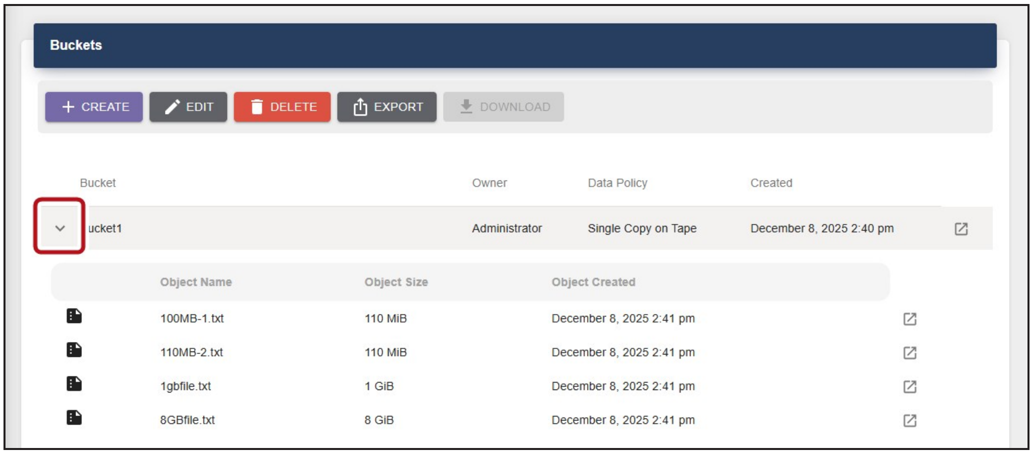
Objects present on the BlackPearl Object Gateway can be downloaded using the BlackPearl user interface, a DS3 client, or the Spectra Eon Browser. For information on using the Spectra Eon Browser, see the *BlackPearl Eon Browser User Guide.*

Use the instructions in this section to download an object through the BlackPearl user interface.

IMPORTANT The object must be a single blob. If blobbing is enabled for the data policy and the object is greater than the maximum blob size, the object must be downloaded through a DS3 client or the Spectra Eon Browser.

Note: Only one object can be selected for download at a time.

1. On the left-hand menu bar, click **Buckets**. The Buckets screen displays.
2. Click the **Expand arrow** on the left side of the Buckets pane to display the contents of the bucket.



Bucket	Owner	Data Policy	Created
ucket1	Administrator	Single Copy on Tape	December 8, 2025 2:40 pm

Object Name	Object Size	Object Created
100MB-1.txt	110 MiB	December 8, 2025 2:41 pm
110MB-2.txt	110 MiB	December 8, 2025 2:41 pm
1gbfile.txt	1 GiB	December 8, 2025 2:41 pm
8GBfile.txt	8 GiB	December 8, 2025 2:41 pm

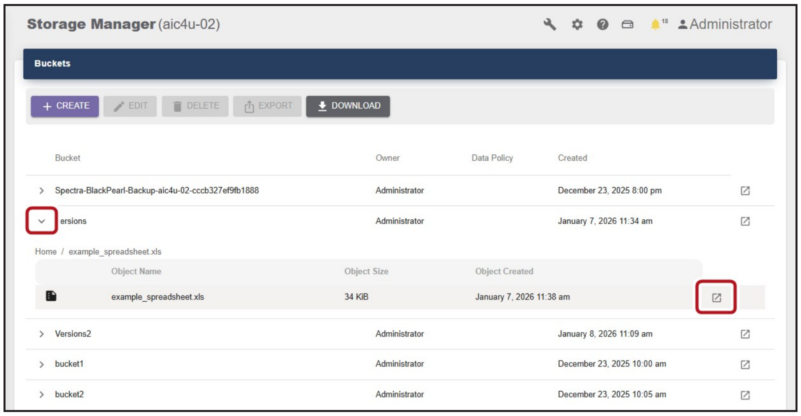
Figure 130 The Buckets screen - Buckets pane - Expand arrow.

3. Select the object you want to download, and click **Download**. The object begins downloading through your web server.

View Object Versioning

If a bucket is configured with versioning, you can view the versions of an object on a per-object basis.

1. From the left-side menu, click **Buckets**.
2. Click the **Expand arrow** on the left side of the Buckets pane to display the contents of the bucket.



Bucket	Owner	Data Policy	Created
Spectra-BlackPearl-Backup-aic4u-02-cccb327ef9fb1888	Administrator		December 23, 2025 8:00 pm
ersions	Administrator		January 7, 2026 11:34 am

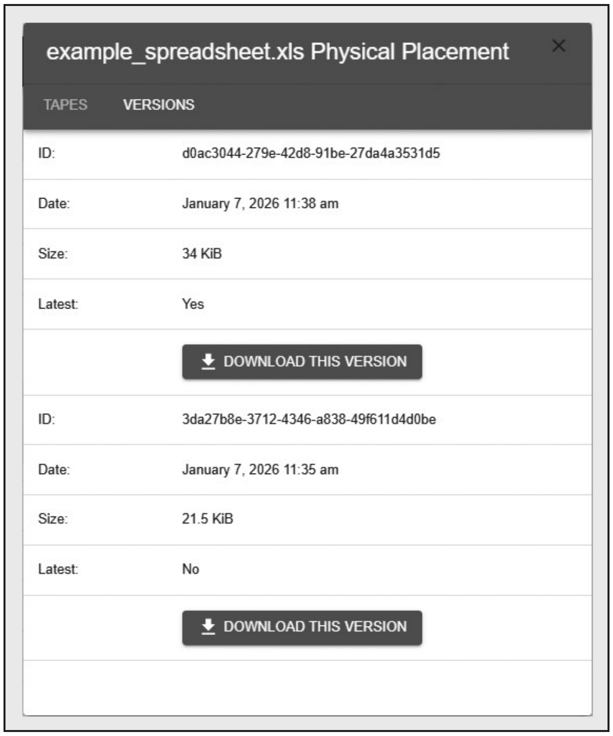
Home / example_spreadsheet.xls

Object Name	Object Size	Object Created
example_spreadsheet.xls	34 KiB	January 7, 2026 11:38 am

Bucket	Owner	Data Policy	Created
Versions2	Administrator		January 8, 2026 11:09 am
bucket1	Administrator		December 23, 2025 10:00 am
bucket2	Administrator		December 23, 2025 10:05 am

Figure 131 The Buckets screen - Buckets pane - Expand Arrow and Details button.

3. Click the **Details** button at the right-side end of the row of the objects for which you want to view versions. The *Object Name* Physical Placement screen displays.



ID: d0ac3044-279e-42d8-91be-27da4a3531d5

Date: January 7, 2026 11:38 am

Size: 34 KiB

Latest: Yes

ID: 3da27b8e-3712-4346-a838-49f611d4d0be

Date: January 7, 2026 11:35 am

Size: 21.5 KiB

Latest: No

Figure 132 The Object Physical Placement window - Versions tab.

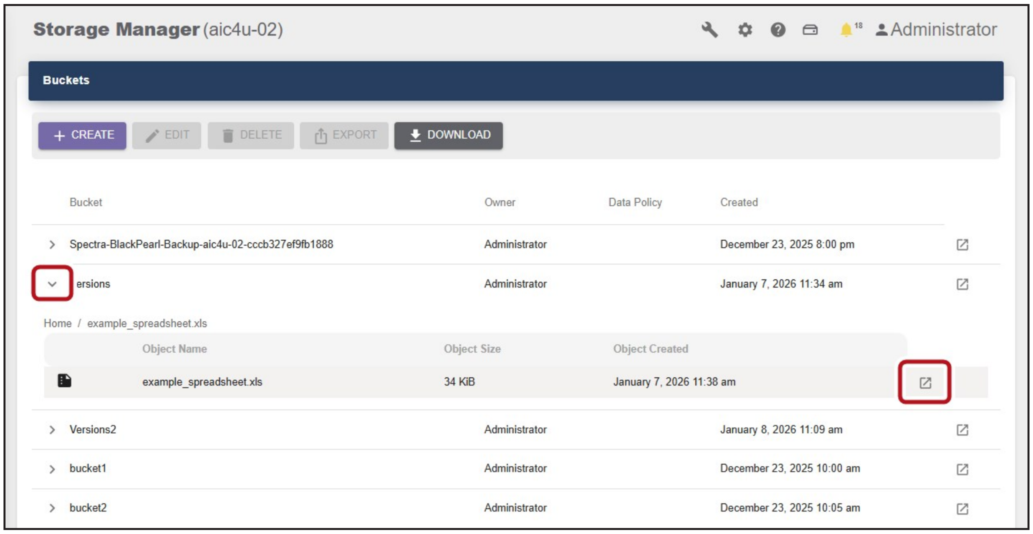
4. Click the **Versions** tab. The versions details screen displays the following information for each version of the object:

This row...	Shows...
ID	The UUID of the object version.
Date	The timestamp of when the object was written to the bucket.
Size	The size of the object.
Latest	Indicates if the object is the latest version. Values: **Yes, No**

Download a Object Version

Use the instructions in this section to download an object version through the BlackPearl user interface.

1. On the left-hand menu bar, click **Buckets**. The Buckets screen displays.
2. Click the **Expand arrow** on the left side of the Buckets pane to display the contents of the bucket.



	Bucket	Owner	Data Policy	Created
>	Spectra-BlackPearl-Backup-aic4u-02-cccb327ef9fb1888	Administrator		December 23, 2025 8:00 pm
⌄	ersions	Administrator		January 7, 2026 11:34 am

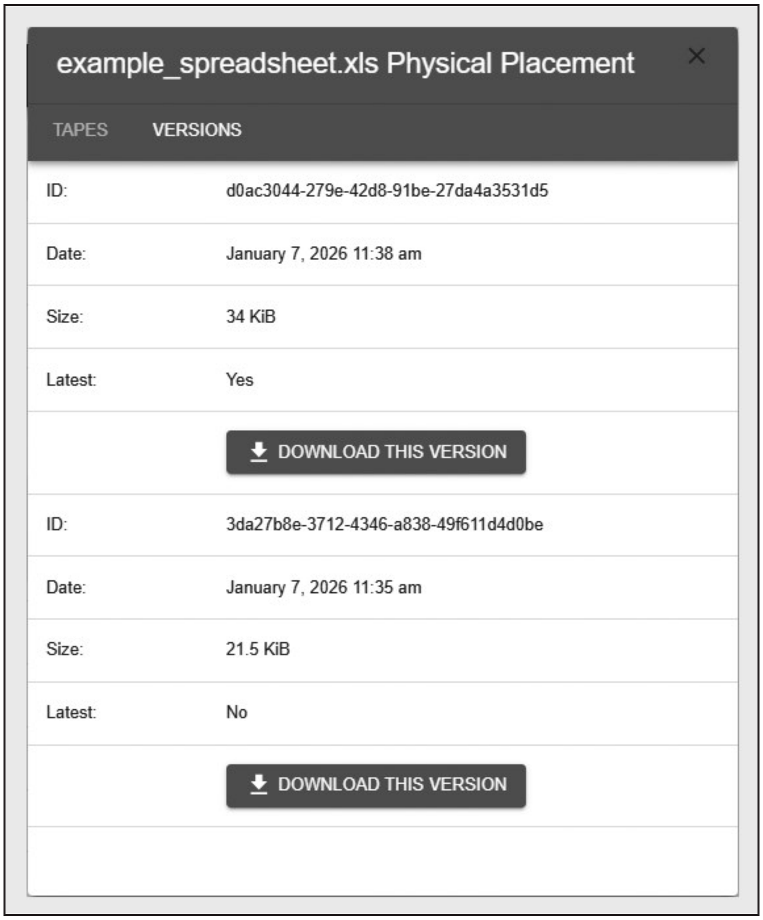
Home / example_spreadsheet.xls

Object Name	Object Size	Object Created
example_spreadsheet.xls	34 KiB	January 7, 2026 11:38 am

	Bucket	Owner	Data Policy	Created
>	Versions2	Administrator		January 8, 2026 11:09 am
>	bucket1	Administrator		December 23, 2025 10:00 am
>	bucket2	Administrator		December 23, 2025 10:05 am

Figure 133 The Buckets screen - Buckets pane - Expand Arrow and Details button.

3. Click the **Details** button at the right-side of the row of the objects for which you want to view versions. The *Object Name* Physical Placement screen displays.



ID:	d0ac3044-279e-42d8-91be-27da4a3531d5
Date:	January 7, 2026 11:38 am
Size:	34 KiB
Latest:	Yes
ID:	3da27b8e-3712-4346-a838-49f611d4d0be
Date:	January 7, 2026 11:35 am
Size:	21.5 KiB
Latest:	No

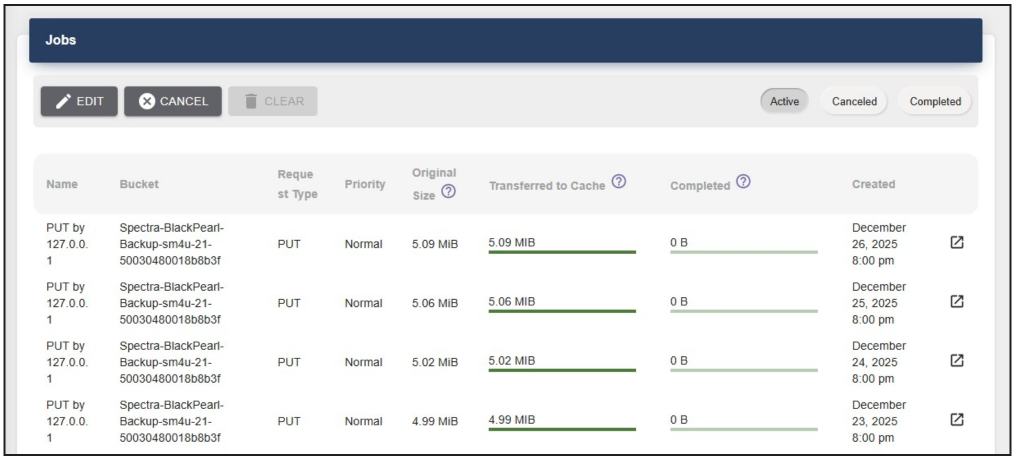
Figure 134 The Object Physical Placement window - Versions tab.

4. Click the **Versions** tab. The versions details screen displays the following information for each version of the object :
5. Locate the object version you want to download and click **Download This Version**.

View DS3 Jobs

The Jobs screen displays the status of all DS3 jobs the Gateway is currently processing, all canceled jobs, and all completed jobs.

1. On the side navigation pane, click **Jobs**.



Name	Bucket	Request Type	Priority	Original Size	Transferred to Cache	Completed	Created
PUT by 127.0.0.1	Spectra-BlackPearl-Backup-sm4u-21-50030480018b8b3f	PUT	Normal	5.09 MiB	5.09 MiB	0 B	December 26, 2025 8:00 pm
PUT by 127.0.0.1	Spectra-BlackPearl-Backup-sm4u-21-50030480018b8b3f	PUT	Normal	5.06 MiB	5.06 MiB	0 B	December 25, 2025 8:00 pm
PUT by 127.0.0.1	Spectra-BlackPearl-Backup-sm4u-21-50030480018b8b3f	PUT	Normal	5.02 MiB	5.02 MiB	0 B	December 24, 2025 8:00 pm
PUT by 127.0.0.1	Spectra-BlackPearl-Backup-sm4u-21-50030480018b8b3f	PUT	Normal	4.99 MiB	4.99 MiB	0 B	December 23, 2025 8:00 pm

Figure 135 The Jobs screen.

2. Use the job status buttons to select **Active**, **Canceled** or **Completed** as desired.

The Jobs screen displays the following information:

This column…	Shows…
Name	The name of the job request, which is generated automatically using the job request type and IP address of the source or destination host. **Note:** Multiple jobs of the same request type from the same host IP address all have the same name.
Bucket	The name of the bucket that is acted on by the job request. **Note:** Jobs created from standard Amazon compatible S3 PUT and GET requests do not display a bucket name on the Jobs screen.
Request Type	If the job is a **PUT** (write), **GET** (read), or **VERIFY** (verify) operation.
Priority	The priority for processing the job. The job priority determines the resources assigned and the processing order. Values: **Critical, Urgent, High, Normal, Low, Background**.
Original Size	The amount of data to be transferred by the job.

This column...	Shows...
Transferred to Cache	The amount of data that was transferred to the cache for this job. For PUTs, this is the amount of data successfully transferred to the Gateway from the client. For GETs, this is the amount of data either in cache originally, or loaded into cache from tape. For VERIFY jobs, this is the amount of data loaded into cache from the permanent data store.
Completed	The amount of data that is completely processed for this job. For PUTs, this indicates the amount of data written to tape media. For GETs, this indicates the amount of data that was read successfully by the client. For VERIFY jobs, this is the amount of data loaded into cache from the permanent data store.
Created	The timestamp of when the job was created.

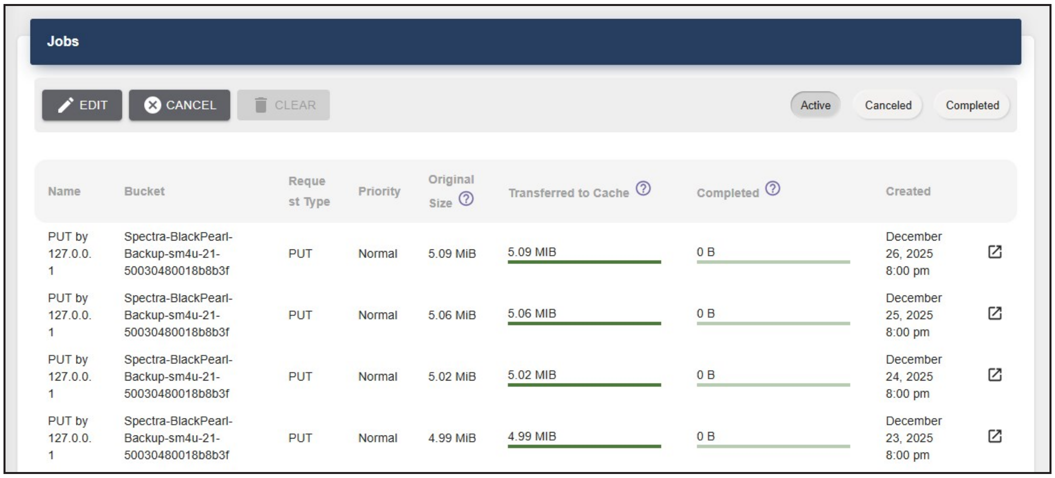
Cancel DS3 Jobs

You can use the BlackPearl user interface to cancel an in-progress DS3 job instead of using your DS3 client.

> **Note:** You cannot cancel a PUT or GET job initiated by the Vail application associated with the BlackPearl Object Gateway.

Use the instructions in this section to cancel a DS3 job(s).

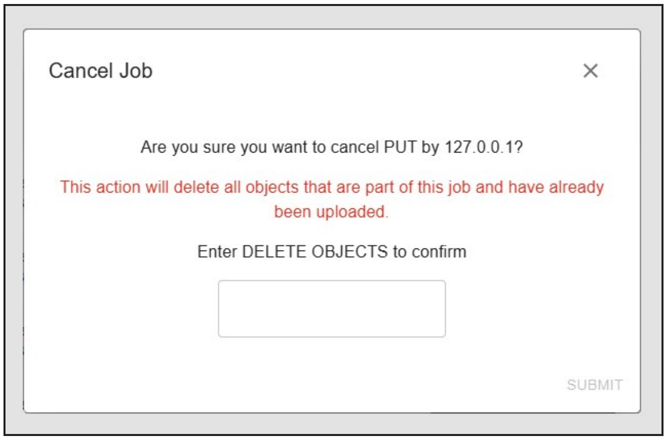
1. On the left-hand menu bar, click **Jobs**. The Jobs screen displays.



Name	Bucket	Request Type	Priority	Original Size	Transferred to Cache	Completed	Created
PUT by 127.0.0.1	Spectra-BlackPearl-Backup-sm4u-21-50030480018b8b3f	PUT	Normal	5.09 MiB	5.09 MiB	0 B	December 26, 2025 8:00 pm
PUT by 127.0.0.1	Spectra-BlackPearl-Backup-sm4u-21-50030480018b8b3f	PUT	Normal	5.06 MiB	5.06 MiB	0 B	December 25, 2025 8:00 pm
PUT by 127.0.0.1	Spectra-BlackPearl-Backup-sm4u-21-50030480018b8b3f	PUT	Normal	5.02 MiB	5.02 MiB	0 B	December 24, 2025 8:00 pm
PUT by 127.0.0.1	Spectra-BlackPearl-Backup-sm4u-21-50030480018b8b3f	PUT	Normal	4.99 MiB	4.99 MiB	0 B	December 23, 2025 8:00 pm

Figure 136 The Jobs screen.

2. Select the job you want to cancel, then click **Cancel**. The Cancel Job confirmation screen displays.



Cancel Job

Are you sure you want to cancel PUT by 127.0.0.1?

This action will delete all objects that are part of this job and have already been uploaded.

Enter DELETE OBJECTS to confirm

Figure 137 The Cancel Job screen.

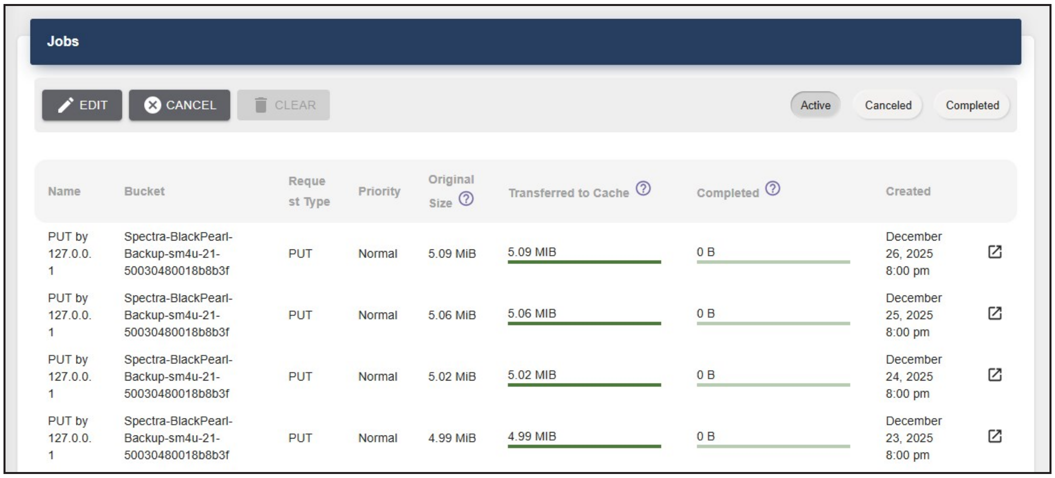
3. Enter `DELETE OBJECTS` in the entry field, then click **Submit**.

Edit an S3 Job

If desired, you can edit the name and priority level of an active S3 job. Use the instructions in this section to edit the name or priority of a DS3 job(s).

Note: You cannot edit completed jobs.

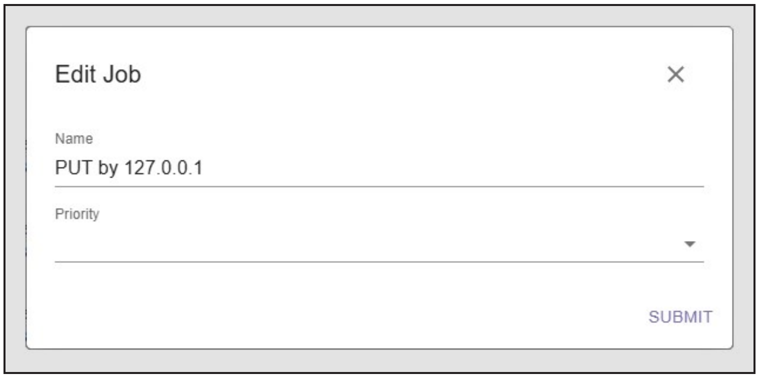
1. On the left-hand menu bar, click **Jobs**. The Jobs screen displays.



Name	Bucket	Request Type	Priority	Original Size	Transferred to Cache	Completed	Created
PUT by 127.0.0.1	Spectra-BlackPearl-Backup-sm4u-21-50030480018b8b3f	PUT	Normal	5.09 MiB	5.09 MIB	0 B	December 26, 2025 8:00 pm
PUT by 127.0.0.1	Spectra-BlackPearl-Backup-sm4u-21-50030480018b8b3f	PUT	Normal	5.06 MiB	5.06 MIB	0 B	December 25, 2025 8:00 pm
PUT by 127.0.0.1	Spectra-BlackPearl-Backup-sm4u-21-50030480018b8b3f	PUT	Normal	5.02 MiB	5.02 MIB	0 B	December 24, 2025 8:00 pm
PUT by 127.0.0.1	Spectra-BlackPearl-Backup-sm4u-21-50030480018b8b3f	PUT	Normal	4.99 MiB	4.99 MIB	0 B	December 23, 2025 8:00 pm

Figure 138 The Jobs screen.

2. Select the row of the S3 job for which you want to edit, then click **Edit**. The Edit Job dialog box displays.



Edit Job

Name
PUT by 127.0.0.1

Priority

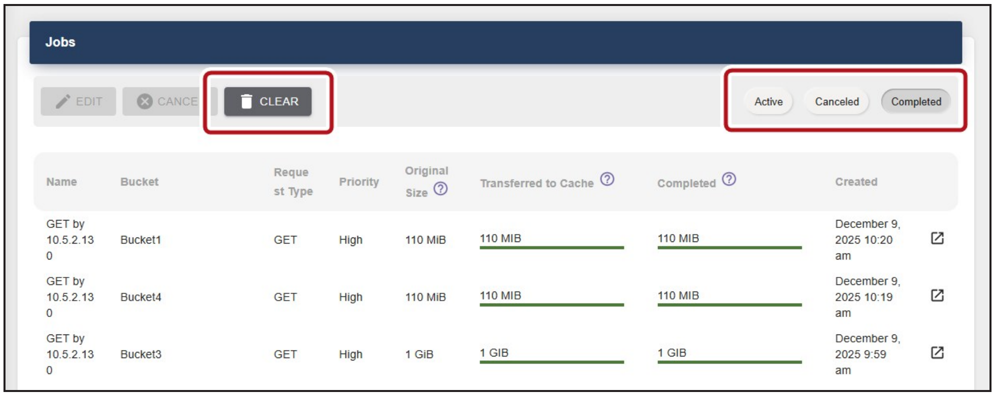
Figure 139 The Edit Job dialog box.

3. If desired, enter the desired **Name**.
4. Use the **Priority** drop-down menu to select a new priority for the job.
5. Click **Submit**.

Clear All Canceled or Completed Jobs

If desired, you can clear completed or canceled jobs from the BlackPearl user interface.

1. On the left-hand menu bar, click **Jobs**. The Jobs screen displays.
2. In the upper-right corner of the Jobs pane, click **Canceled** or **Completed**. The screen refreshes to display the selected job category.



Name	Bucket	Request Type	Priority	Original Size	Transferred to Cache	Completed	Created
GET by 10.5.2.130	Bucket1	GET	High	110 MiB	110 MiB	110 MiB	December 9, 2025 10:20 am
GET by 10.5.2.130	Bucket4	GET	High	110 MiB	110 MiB	110 MiB	December 9, 2025 10:19 am
GET by 10.5.2.130	Bucket3	GET	High	1 GiB	1 GiB	1 GiB	December 9, 2025 9:59 am

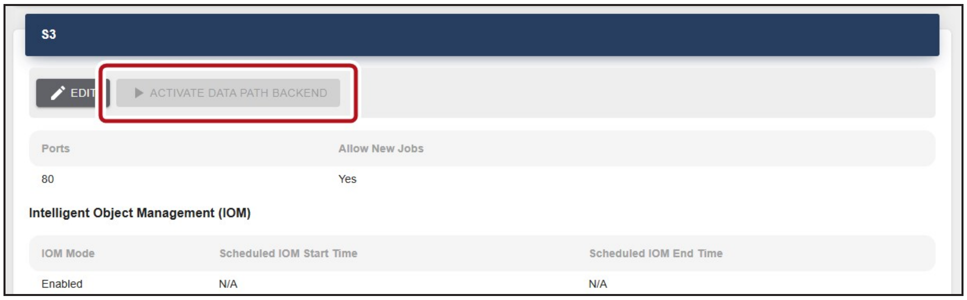
Figure 140 The Jobs screen.

3. Click **Clear**. A confirmation window displays (not shown).
4. Enter `CLEAR` in the dialog box, then click **Submit**.

Manually Starting the S3 Data Path Backend

If the BlackPearl Object Gateway is powered off for longer than the timeout value specified in the Amazon compatible S3 service options, the data path backend must be manually started. Use the instructions in this section to manually start the data path backend.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.



Ports	Allow New Jobs
80	Yes

Intelligent Object Management (IOM)

IOM Mode	Scheduled IOM Start Time	Scheduled IOM End Time
Enabled	N/A	N/A

Figure 141 The Services screen - S3 Pane

2. In the S3 pane, click **Activate Data Path Backend**. A confirmation window displays (not shown).
3. Click **Submit**.

Disallow New Jobs

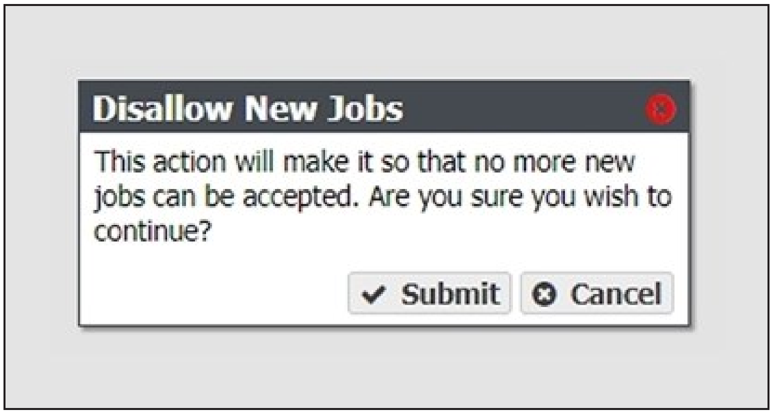
If desired, you can stop the BlackPearl Object Gateway from accepting new Amazon compatible S3 jobs.

To disallow new jobs, you must access the legacy user interface used in BlackPearl OS 5.8.x and earlier. Functionality to disallow new jobs will be added to the new user interface in a later version of the BlackPearl OS.

1. Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with "/legacy". For example:

   https://*ipaddress*/legacy

2. Use the toolbar in the upper-right to select **Configuration > Services** to display the Services screen.
3. Double-click the Amazon compatible S3 service, or select the Amazon compatible S3 service and select **Action > Show Details**. The Amazon compatible S3 details screen displays.
4. On the Amazon compatible S3 service details screen, select **Action > Disallow New Jobs**. The Disallow New Jobs confirmation window displays.



Disallow New Jobs

This action will make it so that no more new jobs can be accepted. Are you sure you wish to continue?

Figure 142 The Disallow New Jobs confirmation window.

5. Click **Submit**.

Allow New Jobs

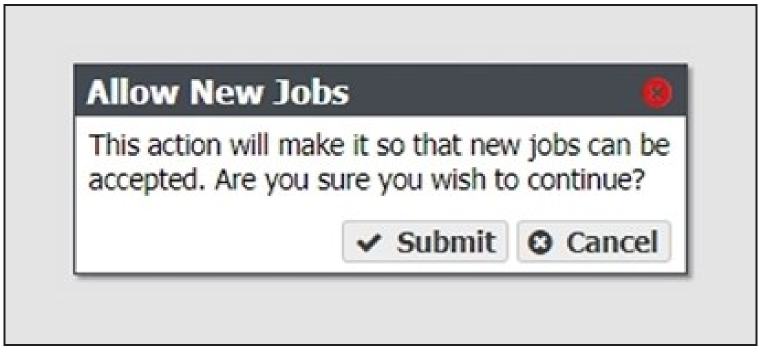
If you have configured the BlackPearl Object Gateway to no longer accept new Amazon compatible S3 jobs, use the instructions in this section to configure the Gateway to allow new jobs.

To allow new jobs, you must access the legacy user interface used in BlackPearl OS 5.8.x and earlier. Functionality to allow new jobs will be added to the new user interface in a later version of the BlackPearl OS.

1. Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with "/legacy". For example:

   https://*ipaddress*/legacy

2. Use the toolbar in the upper-right to select **Configuration > Services** to display the Services screen.
3. Double-click the Amazon compatible S3 service, or select the Amazon compatible S3 service and select **Action > Show Details**. The S3 details screen displays.
4. On the Amazon compatible S3 service details screen, select **Action > Allow New Jobs**. The Allow New Jobs confirmation window displays.



Allow New Jobs

This action will make it so that new jobs can be accepted. Are you sure you wish to continue?

Figure 143 The Allow New Jobs confirmation window.

5. Click **Submit**.

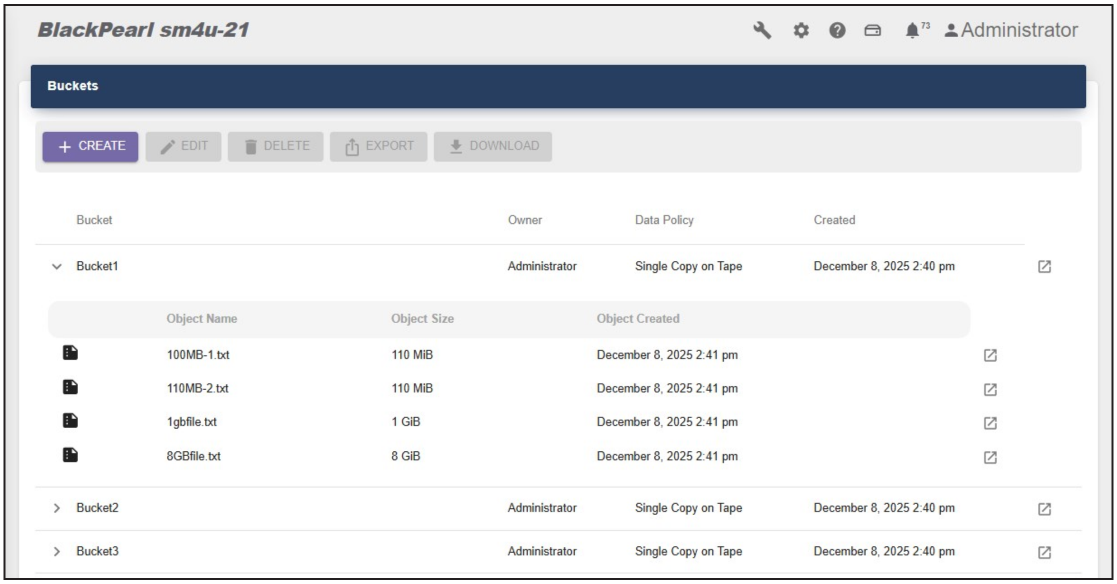
MANAGE BUCKETS

Use the instructions in this section to view the physical placement of a bucket, and to delete a bucket. For instructions on creating a new bucket, see Create a Bucket on page 139.

View Bucket Contents

Use the instructions in this section to view the contents of a bucket configured on the BlackPearlObjectGateway.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**. The Buckets screen displays.



Bucket	Owner	Data Policy	Created
Bucket1	Administrator	Single Copy on Tape	December 8, 2025 2:40 pm

Object Name	Object Size	Object Created
100MB-1.txt	110 MiB	December 8, 2025 2:41 pm
110MB-2.txt	110 MiB	December 8, 2025 2:41 pm
1gbfile.txt	1 GiB	December 8, 2025 2:41 pm
8GBfile.txt	8 GiB	December 8, 2025 2:41 pm

Bucket	Owner	Data Policy	Created
Bucket2	Administrator	Single Copy on Tape	December 8, 2025 2:40 pm
Bucket3	Administrator	Single Copy on Tape	December 8, 2025 2:40 pm

Figure 144 The Buckets screen with the contents of a bucket displayed.

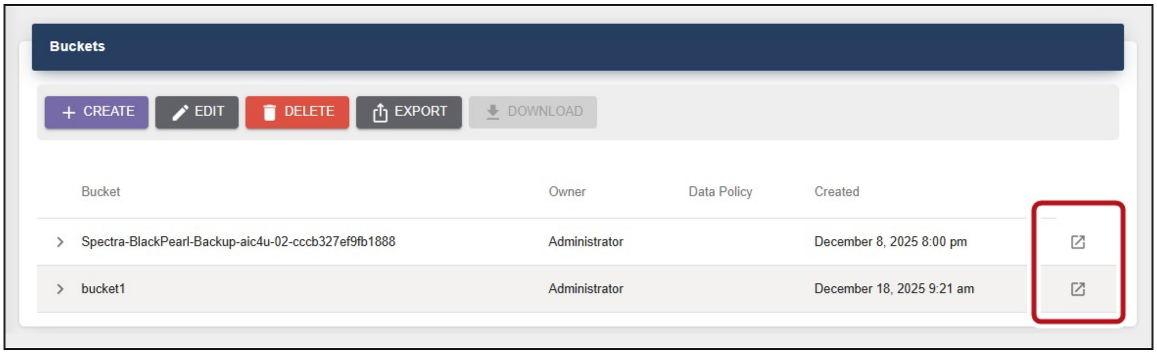
2. Click the **expand arrow** to display the contents of a bucket. The following information displays:

This row...	Shows...
Object Name	The name of an object in the specified bucket.
Object Size	The size of the object.
Object Created	The timestamp of when the object was written to the bucket.

Show Bucket Physical Placement

Once data is transferred to the BlackPearl Object Gateway, you can view the physical placement of the data. The BlackPearl user interface displays data placement on disk pools, tapes, and replication targets. Use the instructions in this section to view physical placement of a specified bucket.

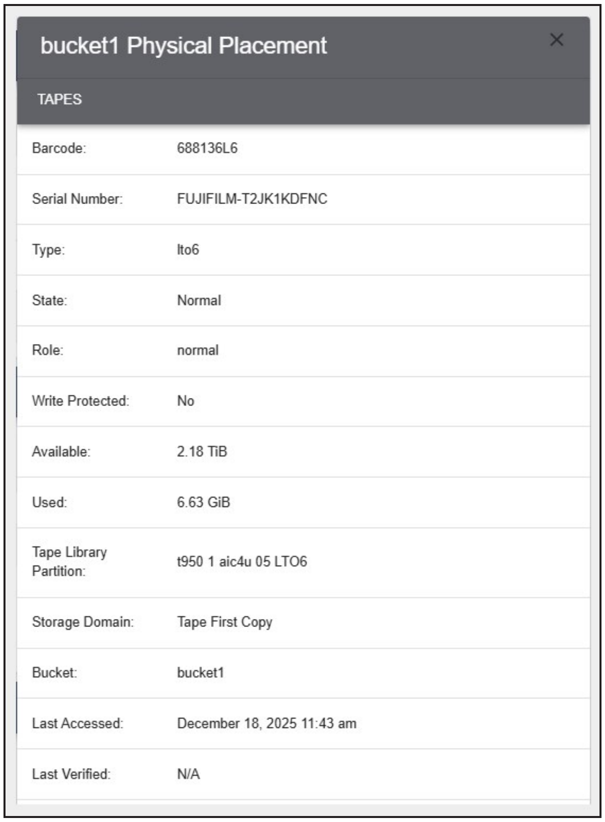
1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.



Bucket	Owner	Data Policy	Created
Spectra-BlackPearl-Backup-aic4u-02-cccb327ef9fb1888	Administrator		December 8, 2025 8:00 pm
bucket1	Administrator		December 18, 2025 9:21 am

Figure 145 The Buckets screen - Buckets pane - Details button.

2. Click the **Details** button on the row of the bucket for which you want to view physical placement. The *Bucket Name* Physical Placement screen displays.



Barcode:	688136L6
Serial Number:	FUJIFILM-T2JK1KDFNC
Type:	lto6
State:	Normal
Role:	normal
Write Protected:	No
Available:	2.18 TiB
Used:	6.63 GiB
Tape Library Partition:	t950 1 aic4u 05 LTO6
Storage Domain:	Tape First Copy
Bucket:	bucket1
Last Accessed:	December 18, 2025 11:43 am
Last Verified:	N/A

Figure 146 The *Bucket* Physical Placement screen.

This row...	Shows...
Barcode	The barcode label on the tape cartridge.
Serial Number	The manufacturer assigned serial number for the tape cartridge.
Type	The media type. Values: **LTO-5, LTO-6, LTO-7, LTO-7 Type M, LTO-8, LTO-9, LTO-10, TS1140, TS1150, TS1155, TS1160, TS1170**
State	The status of the tape. See Manage Buckets on page 225 for a list of tape cartridge states.
Role	The role of the tape. Values: **Normal, Test**.
Write Protected	The status of the write-protect switch on the cartridge.
Available	The amount of unused space that is available on the tape cartridge.
Used	The amount of space on the tape containing data.
Tape Library Partition	The serial number of the partition on the Spectra Logic or other supported tape library containing the tape cartridge.
Storage Domain	The storage domain to which the tape is assigned.
Bucket	The bucket to which the tape is assigned.
Last Accessed	The timestamp of the last time the tape was loaded into a tape drive.
Last Verified	The timestamp of the last time data was verified on the tape cartridge, by either a manual verification, or when the number of days specified in the storage domain that owns the tape passed.

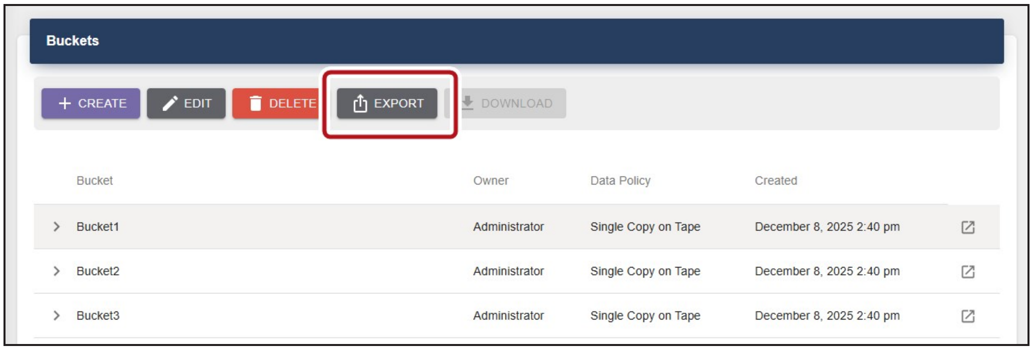
Export a Bucket

A bucket is exported from the BlackPearl Object Gateway by exporting all tapes containing bucket data from the tape library storage pool to the Entry/Exit pool. The tapes can then be exported physically from the tape library.

When a bucket is exported the data contained on exported tape cartridges is not available until the tapes are imported back into the BlackPearl Object Gateway. If the data policy used by the bucket is configured to copy the bucket data to multiple storage domains, the data remains accessible to the BlackPearl Object Gateway and available for download.

Use the instructions in this section to export a bucket.

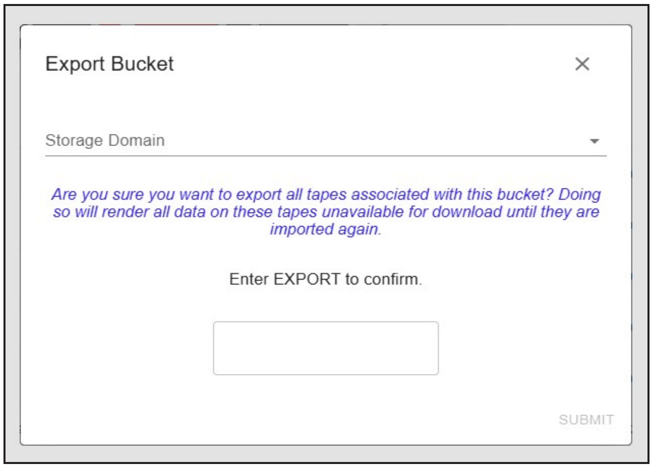
1. On the left-hand menu bar, click **Buckets**. The Buckets screen displays.



Bucket	Owner	Data Policy	Created
Bucket1	Administrator	Single Copy on Tape	December 8, 2025 2:40 pm
Bucket2	Administrator	Single Copy on Tape	December 8, 2025 2:40 pm
Bucket3	Administrator	Single Copy on Tape	December 8, 2025 2:40 pm

Figure 147 The Buckets screen - Buckets pane - Export button.

2. Select the bucket you want to export and then click **Export**. The Export Bucket dialog box displays.



Are you sure you want to export all tapes associated with this bucket? Doing so will render all data on these tapes unavailable for download until they are imported again.

Enter EXPORT to confirm.

Figure 148 The Export Bucket dialog box.

3. Enter `EXPORT` to confirm the action.

4. Click **Submit**.

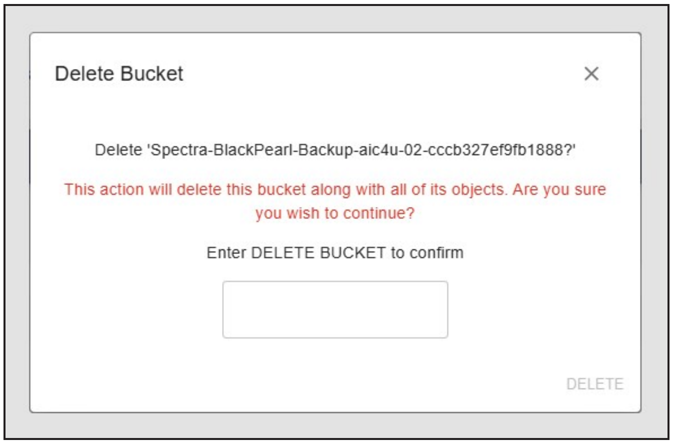
Delete a Bucket

Use the instructions in this section to delete a bucket.

CAUTION When you delete a bucket, all data contained in the bucket is lost. Any tapes associated with the bucket are marked as Free, and are available to the Gateway for other storage operations immediately. Any bucket data that was written to tape media is retained until the tape is loaded into a drive and new data is written.

Note: You cannot delete a bucket created by the Spectra Vail, StorCycle, or RioBroker applications if the bucket contains data. To delete the bucket, use application that created the bucket to delete all data, then delete the bucket using the BlackPearl user interface.

1. Use the toolbar in the upper-right to select **Configuration (gear icon) > Buckets**.
2. Select the bucket you want to delete and click **Delete**. A confirmation dialog box displays.



Delete 'Spectra-BlackPearl-Backup-aic4u-02-cccb327ef9fb1888?'

This action will delete this bucket along with all of its objects. Are you sure you wish to continue?

Enter DELETE BUCKET to confirm

Figure 149 The Delete Bucket confirmation dialog box.

3. Type `DELETE BUCKET` into the entry field, and then click **Delete**.

IMPORTANT If you delete all buckets on a storage, the storage is disabled automatically. After you finish configuring the system to use that storage again, the storage can be enabled using the BlackPearl user interface.

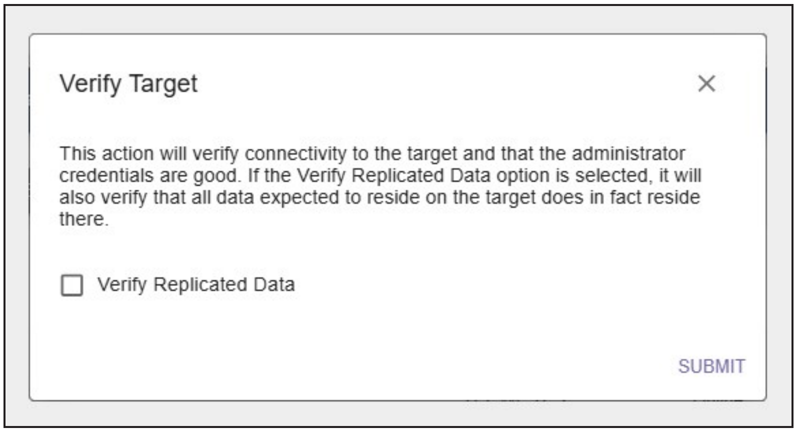
MANAGE REPLICATION TARGETS

Use the instruction in this section to manage existing replication targets.

Verify a Replication Target

Use the instructions in this section to verify connectivity to the target and optionally verify replicated data on the replication target.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.
2. In the Replication Targets pane, use the **Replication Type** drop-down menu on the right-hand side to select the type of replication targets to display.
3. Select replication target for which you want to verify and click **Verify**. The Verify Target dialog box displays.



Verify Target

This action will verify connectivity to the target and that the administrator credentials are good. If the Verify Replicated Data option is selected, it will also verify that all data expected to reside on the target does in fact reside there.

□ Verify Replicated Data

Figure 150 The Verify Target dialog box.

4. If desired, select **Verify Replicated Data** to confirm that the expected data resides on the replication target.

Note: Depending on the amount of data on the replication target, this process may take a long time to complete.

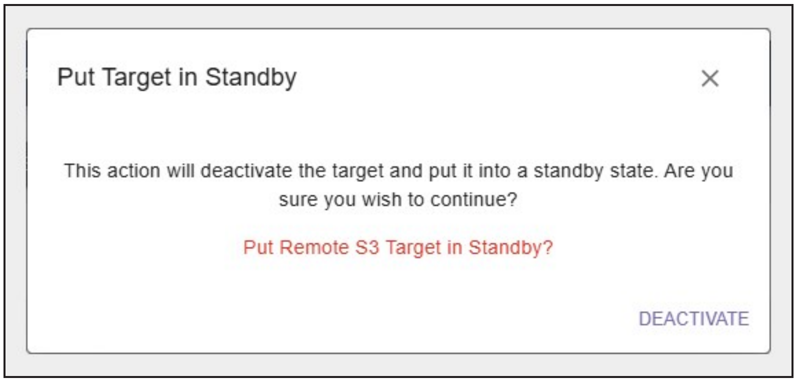
5. Click **Submit**. The Gateway confirms connectivity to the target and optionally verifies the replicated data.

Put a Replication Target in Standby State

If you need to perform service on a replication target, it is recommended that you first put the replication target into a standby state. Otherwise, the BlackPearl Object Gateway may attempt to use the target while it is in service.

No data is transferred to the replication target while in standby.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.
2. In the Replication Targets pane, use the **Replication Type** drop-down menu on the right-hand side to select the type of replication targets to display.
3. Select the replication target that you want to put into standby and click **Standby**. The Put Target in Standby dialog box displays.



Put Target in Standby

This action will deactivate the target and put it into a standby state. Are you sure you wish to continue?

Put Remote S3 Target in Standby?

Figure 151 The Put Target in Standby dialog box.

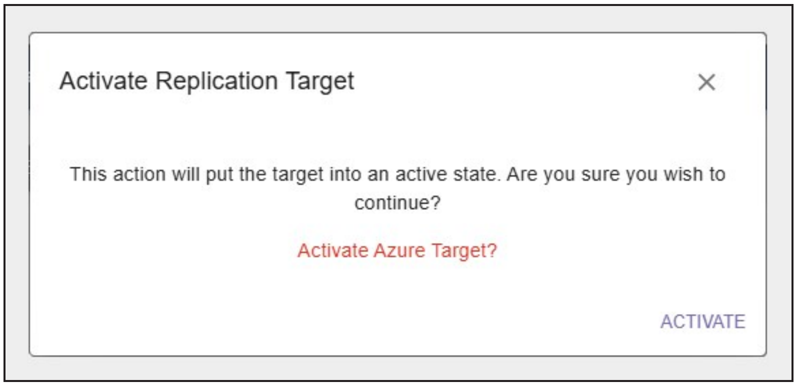
4. Click **Deactivate**. The target is now in standby.

Activate a Replication Target

Use the instructions in this section to activate a replication target currently in standby. Once activated, data transfers are allowed to the replication target.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.
2. In the Replication Targets pane, use the **Replication Type** drop-down menu on the right-hand side to select the type of replication targets to display.

3. Select the replication target that you want to activate and click **Activate**. The Activate Replication Target dialog box displays.



Activate Replication Target

This action will put the target into an active state. Are you sure you wish to continue?

Activate Azure Target?

Figure 152 The Activate Replication Target dialog box.

4. Click **Activate**. The target is now in an active state.

Edit Replication Targets

All options available when creating a BlackPearl, Amazon S3, or Azure replication target are available when editing a replication target.

Use the instructions in the Create Replication Targets sections to help you edit a replication target:

- Create a BlackPearl Target on page 141
- Create an Amazon S3 Target on page 145
- Create a Microsoft Azure Target on page 149

Delete a Replication Target

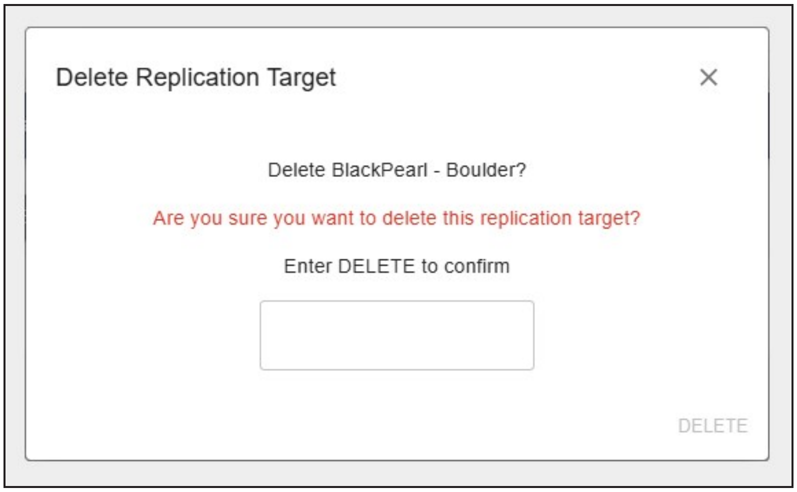
Use the instructions to delete an existing replication target.

CAUTION If you delete a replication target, all data on the target is deleted.

Note: You cannot delete a replication target if it is used by a data policy. See Manage Data Replication Rules on page 1 for instructions on removing a replication target from a data policy.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**.
2. In the Replication Targets pane, use the **Replication Type** drop-down menu on the right-hand side to select the type of replication targets to display.

3. Select the replication target that you want to delete and click **Delete**. The Delete Replication Target dialog box displays.



Delete Replication Target

Delete BlackPearl - Boulder?

Are you sure you want to delete this replication target?

Enter DELETE to confirm

Figure 153 The Delete Replication Target dialog box.

4. Enter `DELETE` in the entry field to confirm you want to delete the replication target.
5. Click **Delete**.

MANAGE DISK POOLS

Use the instructions in this section to manage nearline and online disk pools. For information on managing network attached storage (NAS) storage pools, see Manage Storage Pools on page 1.

Import a Nearline or Online Disk Pool

If you move a set of disk drives containing a previously configured pool from one BlackPearl Object Gateway to a different BlackPearl Object Gateway, you must import the pool on the new system before it can be used.

Contact Spectra Logic Technical Support for assistance in importing a disk pool.

Chapter 9 - Managing Network Attached Storage

This chapter describes using the BlackPearl user interface to manage the creation and use of volume snapshots, and managing NAS replication.

For initial NAS configuration steps, see Configuring Network Attached Storage on page 152.

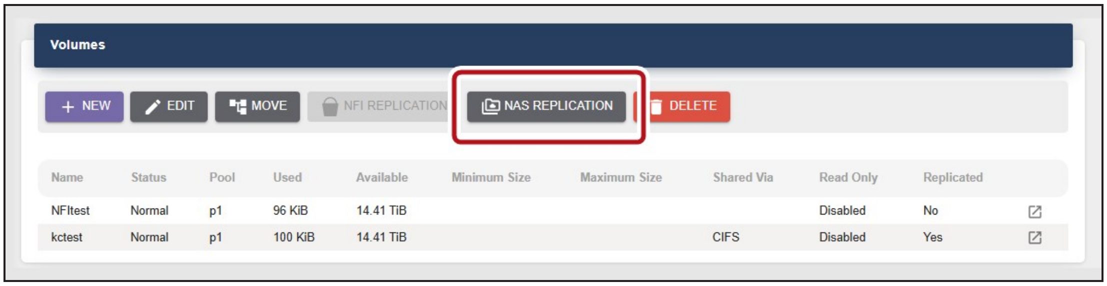
Manage NAS Replication

After configuring replication (see Configure NAS Replication on page 169), use the instructions in this section to manually start or cancel a volume replication, edit or delete the NAS replication configuration, and to restore replicated files.

Manually Start NAS Replication

If desired, you can initiate volume replication manually, regardless of the automatic replication schedule configured for the volume. Starting a manual NAS replication begins the replication immediately. Once complete, replication for the volume continues on its previously defined schedule.

1. On the source system's BlackPearl user interface, use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.



Name	Status	Pool	Used	Available	Minimum Size	Maximum Size	Shared Via	Read Only	Replicated
NFItest	Normal	p1	96 KiB	14.41 TiB				Disabled	No
kctest	Normal	p1	100 KiB	14.41 TiB			CIFS	Disabled	Yes

Figure 154 The NAS screen - Volumes pane - NAS Replication button.

2. Select the volume name you want to replicate and click **NAS Replication**. A confirmation window displays (not shown).
3. Click **Submit** to begin a manual NAS replication.

Restoring Files from a NAS Replication Target

If the source Gateway in a NAS replication configuration fails, you can restore files from the replication target. Use the instructions in this section to restore files from a NAS replication target.

1. On the source system's BlackPearl user interface, clear the write-protected status of the replicated volume.

Note: You cannot add a share while the volume has write-protection enabled.

   a. Use the toolbar in the upper-right to select **Configuration > NAS > Volumes**. The Volumes screen displays.

   b. Select the replicated volume and select **Action > Edit**. The Edit *volume name* dialog box displays.

   c. Clear the **Read Only** checkbox.

   d. Click **Save**.

2. Depending on your operating system environment, create either a CIFS or NFS share, selecting the replicated volume during the creation process. See Create a CIFS Share on page 163 or Create a NFS Share on page 161 for instructions.

3. If desired, write protect the replicated volume before you copy files from the volume:

Note: Spectra Logic highly recommends that you write-protect the volume after sharing it.

   a. Use the toolbar in the upper-right to select **Configuration > NAS > Volumes**. The Volumes screen displays.

   b. Select the replicated volume and select **Action > Edit**. The Edit *volume name* dialog box displays.

   c. Select the **Read Only** checkbox.

   d. Click **Save**.

4. Using your host machine, connect to the new share on the replication target.

5. Copy the needed files from the replication target share to the source Gateway.

6. If desired, stop sharing the NAS replication target volume.

CHAPTER 10 - MONITOR THE BLACKPEARL GATEWAY

This chapter describes using the BlackPearl user interface to monitor the system messages, performance, and reports.

VIEW SYSTEM MESSAGES

Check the system messages regularly. These messages provide important information about the BlackPearl Object Gateway and its operation. Reviewing the messages is the first step in troubleshooting.

Types of Message Severity

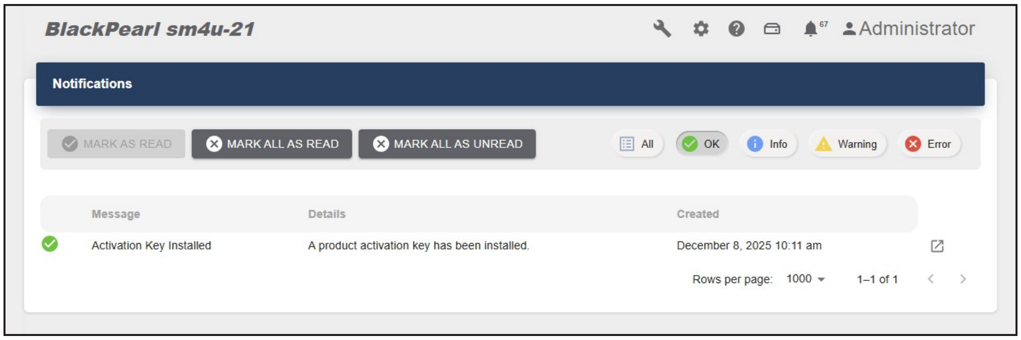
Messages displayed in the BlackPearl user interface use one of the below severities:

Type	Description
Information	Notifies the user about an event that requires no action and does not fit the other categories.
Success	Notifies the user of successful completion of an event.
Alert	Notifies the user that a failure as part of normal operation occurred which requires some sort of user interaction, and until this occurs, adverse impact to the BlackPearl Object Gateway may occur.
Warning	Notifies the user of a failure that may adversely impact the BlackPearl Object Gateway.
Critical	Notifies the user of a failure that caused significant adverse impact to the BlackPearl Object Gateway.

View System Messages

Use the instructions in this section to check system messages.

1. Click **Messages (bell icon)**.



	Message	Details	Created
✓	Activation Key Installed	A product activation key has been installed.	December 8, 2025 10:11 am

Figure 155 The Messages screen.

Pay extra attention to any messages flagged with the Warning or Critical icon and follow any recommended steps. Contact Spectra Logic Technical Support if you need assistance (see Contacting Spectra Logic on page 7).

2. If desired, use the **Rows Per Page** drop-down menu to limit the Messages screen to the specified number of messages.

3. To mark a single message as read, select the message and then click **Mark As Read**. To mark all messages as read, click **Mark All As Read**.

Notes:

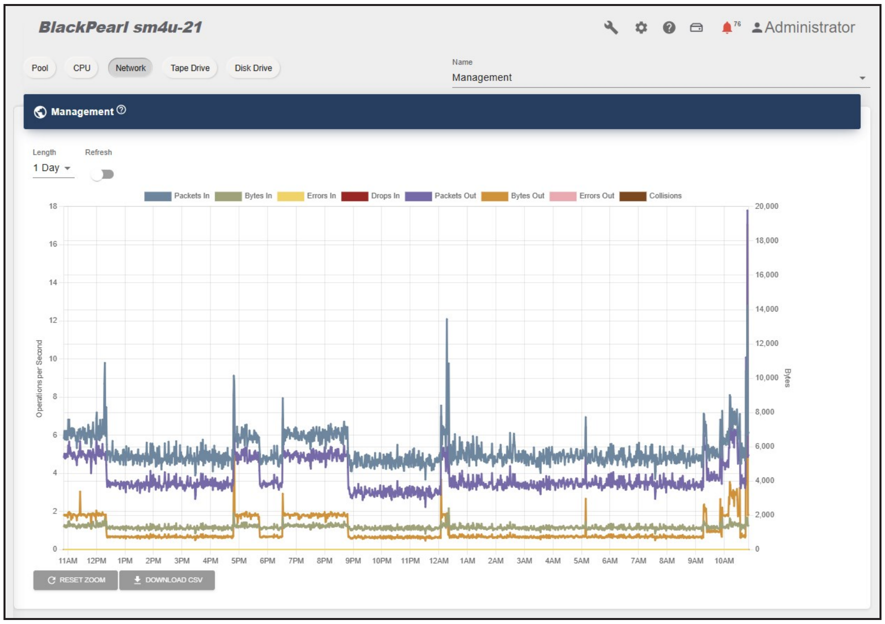
- You cannot delete messages. The Gateway automatically deletes the oldest messages on a first-in, first-out basis as space is required, retaining the most recent messages. The Gateway holds 10,000 messages.
- Messages can also be marked as **Unread**.

VIEW PERFORMANCE METRICS

The Performance screen displays performance metrics for the BlackPearl storage pools, CPUs, network traffic, and individual tape or disk drives. Performance graphs can be configured to display either the last 5 minutes of activity, or the last 24 hours.

Here is how you view performance metrics:

1. From the left-hand menu, click **Performance**.

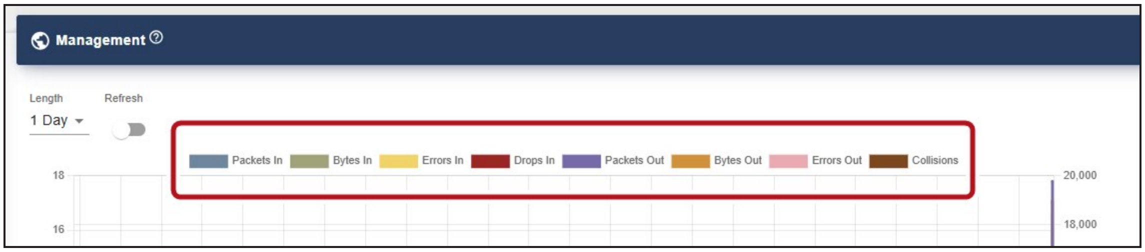


Name: Management

Length: 1 Day

Figure 156 The Performance screen.

2. Select **Pools, CPU, Network, Tape Drive, or Disk Drive** to display performance information about the selected component.
3. Use the **Name** drop-down menu in the upper-right corner to select an individual component of the selected category.
4. Use the **Length** drop-down menu to select the time interval to display. The data can be displayed in 6 second increments (5 minutes total) or 1 hour increments (1 day total).
5. Use the **Element buttons** at the top of the graph to select to display or hide graph elements.



Length: 1 Day

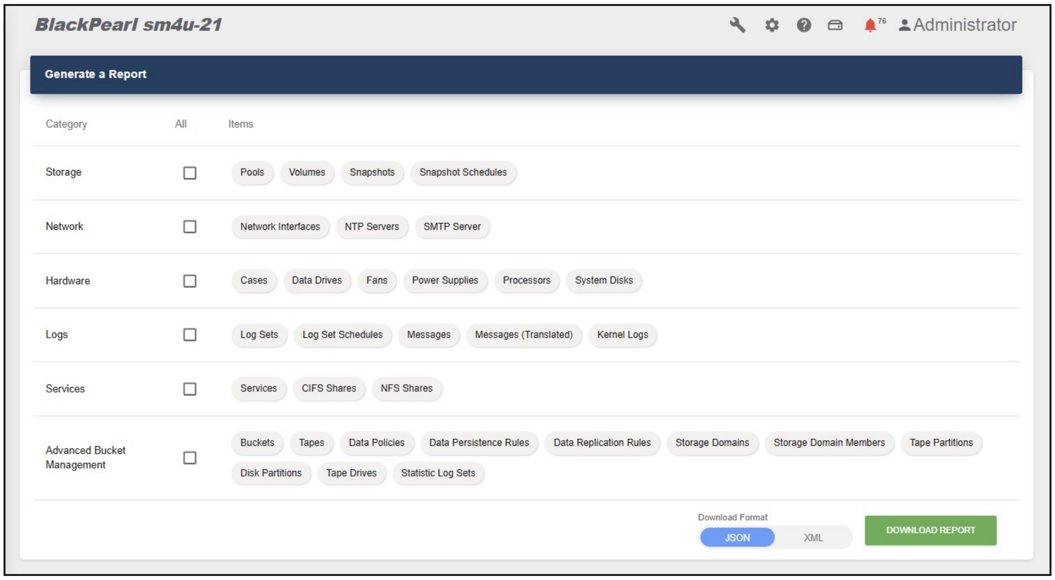
Figure 157 The Performance screen - Element buttons.

6. To see the performance data in greater detail, use the mouse to **click and drag** the cursor horizontally over the section of the detail graph that you want to magnify. The highlighted section of data is shown on the graph.
7. Click **Reset Zoom** to reset the graph to the default view.
8. If desired, click **Download CSV** to download a comma separated value file containing the data for the graph you are currently viewing. The file can then be imported into Microsoft Excel® or other software applications that support this file type.

VIEW REPORTS

The Reports screen allows you to generate reports on all aspects of the BlackPearl Object Gateway, including component status, and configuration. Reports can be downloaded in either JSON or XML format.

1. From the left-hand menu, click **Reports**.



BlackPearl sm4u-21

Generate a Report

Category	All	Items
Storage	□	Pools, Volumes, Snapshots, Snapshot Schedules
Network	□	Network Interfaces, NTP Servers, SMTP Server
Hardware	□	Cases, Data Drives, Fans, Power Supplies, Processors, System Disks
Logs	□	Log Sets, Log Set Schedules, Messages, Messages (Translated), Kernel Logs
Services	□	Services, CIFS Shares, NFS Shares
Advanced Bucket Management	□	Buckets, Tapes, Data Policies, Data Persistence Rules, Data Replication Rules, Storage Domains, Storage Domain Members, Tape Partitions, Disk Partitions, Tape Drives, Statistic Log Sets

Download Format: JSON / XML

Figure 158 The Reports screen.

Note: Depending on the configuration of your BlackPearl Object Gateway, the information displayed may look different than the image above.

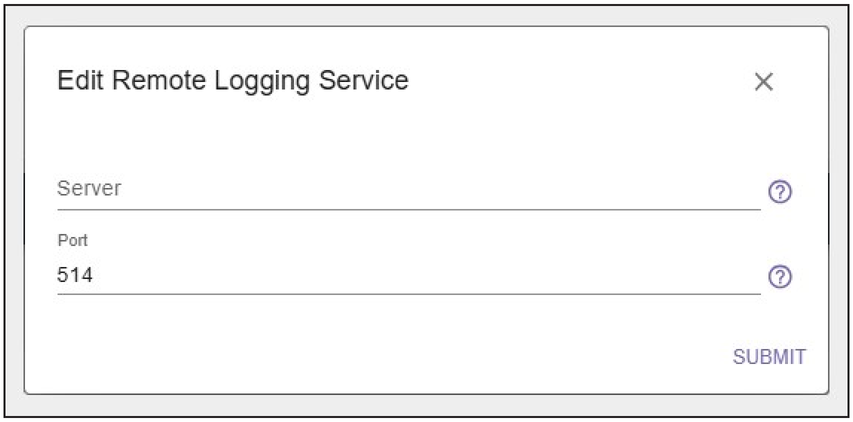
2. Select the **All** checkbox next to the report(s) you want to generate, or **select individual components**.
3. Use the **Download Format** slider to select either JSON or XML formatting for the downloaded report(s).
4. Click **Download Report**. The selected reports are saved to your local host.

ENABLE REMOTE LOGGING

Remote Logging is a feature that allows the BlackPearl Object Gateway to send any messages generated by the system to a syslog server.

Use the instructions in this section to enable remote logging.

1. Enter the Remote Logging activation key as described in Manually Enter Activation Keys on page 364.
2. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
3. In the Remote Logging pane, click **Edit**. The Edit Remote Logging Service dialog box displays.



Edit Remote Logging Service

Server

Port

514

Figure 159 The Edit Remote Logging Service dialog box.

4. Enter a hostname or IP address for the remote logging **Server**.
5. Enter the **Port** used to communicate with the remote logging server.

Note: The default port is 514.

6. Click **Submit**.

CHAPTER 11 - BLACKPEARL OBJECT GATEWAY HARDWARE OPERATIONS

This chapter describes hardware operations for the Spectra BlackPearl Object Gateway, including hardware monitoring, activating the chassis beacon, installing drives, and diagnosing failed components.

MONITOR THE GATEWAY HARDWARE

The BlackPearl Object Gateway features multiple tools to help you monitor the health and performance system hardware components including:

- The Visual Status Beacon light bar in the front bezel changes color to indicate the current status of the Gateway (see Front Bezel Visual Status Beacon below).

  Note: The front bezels in BlackPearl Gen1 2U master nodes, and some Gen1 4U chassis, do not include a Visual Status Beacon light bar.

- LEDs on the front of the BlackPearl chassis indicate system status and error conditions (see System Status LEDs on page 250
- Icons on the Hardware screen provide overall status of the hardware components in each group (see View the Status of Hardware Components on page 254).

- You can also use the BlackPearl user interface to do the following:
  - View the status of NAS pools and volumes (see View the Status of NAS Pools on page 256 and View the Status of NAS Volumes on page 259).
  - View the status of the database and cache (see View the Status of the System Pools on page 260).
  - View the status of media in the associated tape library (see View Tape Media Information on page 262).

Front Bezel Visual Status Beacon

The Visual Status Beacon light bar in the front bezel provides an at-a-glance status of the Gateway to which it is mounted. The light bar changes color to indicate the status of the Gateway. See the chart below for each color displayed and its associated condition.

Color Display	Condition
Purple Scroll	The Gateway is operating normally. **Note:** The color displayed when the Gateway is operating normally can be changed on the Hardware screen. See Configuring the Visual Status Beacon Color on page 248 for more information.
Yellow Scroll	The Gateway is experiencing a Warning condition. Log in to the BlackPearl user interface to determine the cause of the warning.
Red Scroll	The Gateway is experiencing an Error condition. Log in to the BlackPearl user interface to determine the cause of the error.

Color Display	Condition
Orange Scroll	The Gateway is experiencing a move failure in the attached tape library. Log in to the BlackPearl user interface to determine the cause of the error.
Rainbow	The Gateway is currently powering on and performing self-tests.
Flashing Blue	The beacon feature was activated for this Gateway. This can help you identify a specific Gateway when you have more than one Gateway in your environment. See Flash the Visual Status Beacon on page 249 for instructions on activating the beacon.
Pulsing Red	The Visual Status Beacon lost communication with the Gateway. This can occur if the Gateway experiences a software hang.
No Light	The BlackPearl Object Gateway is powered off.

Note: Other patterns may display if the front bezel is not properly seated on the chassis.

Configuring the Visual Status Beacon Color

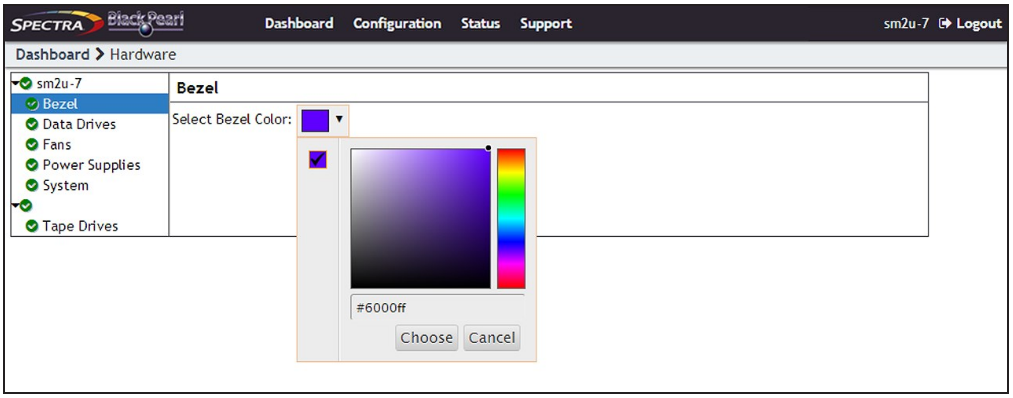
The BlackPearl Object Gateway is configured to display a purple scrolling light on the Visual Status Beacon when the Gateway is operating normally. If desired, you can change the color displayed for normal operation.

To configure the bezel color, you must access the legacy user interface used in BlackPearl OS 5.8.x and earlier. Functionality to configure the bezel color will be added to the new user interface in a later version of the BlackPearl OS.

1. Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with "/legacy". For example:

   https://*ipaddress*/legacy

2. Use the toolbar in the upper-right to select **Status > Hardware**, or click the Hardware pane on the Dashboard, or click the Hardware link on the status bar. The Hardware screen displays.
3. Click **Bezel**. The Bezel pane of the Hardware screen displays.
4. Click the colored box next to **Select Bezel Color**. The color picker window displays.



Select Bezel Color:

#6000ff

Figure 160 Use the color picker to set the color of the Visual Status Beacon when the Gateway is operating normally.

5. Use the color picker to select the color to display when the Gateway is operating normally. Optionally, you can enter an HTML color code in the entry field.

Note: Spectra Logic recommends against using yellow, orange, or red, so that you can more easily determine if the Gateway is in a warning or error state.

6. Click **Choose** to set the color of the Visual Status Beacon.

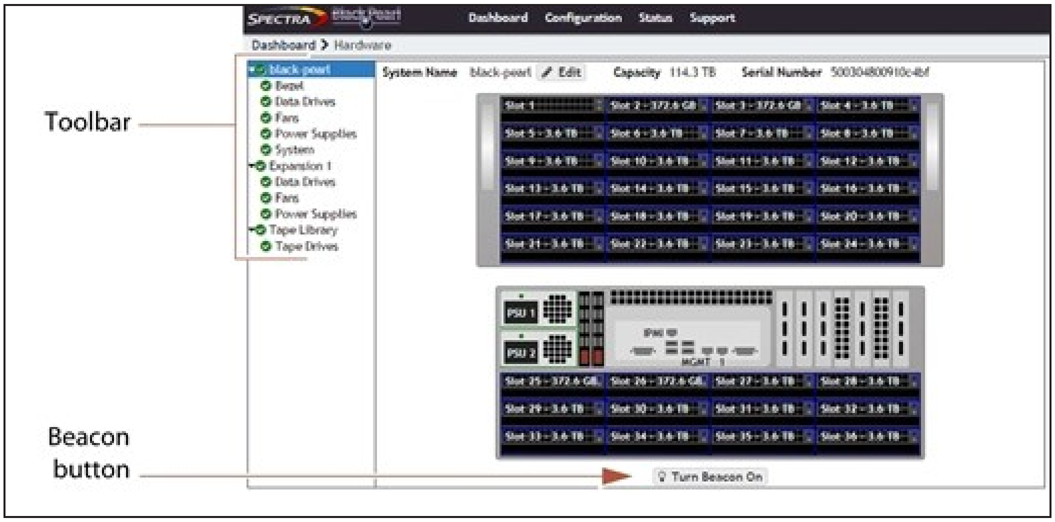
Flash the Visual Status Beacon

To activate the visual status beacon to flash blue, you must access the legacy user interface used in BlackPearl OS 5.8.x and earlier. Functionality to enable this feature will be added to a later version of the BlackPearl OS.

1. Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with "/legacy". For example:

   https://*ipaddress*/legacy

2. Use the toolbar in the upper-right to select **Status > Hardware**, or click the Hardware pane on the Dashboard, or click the Hardware link on the status bar. The Hardware screen displays.



System Name black-pearl Capacity 114.3 TB Serial Number 500304800910c4bf

Figure 161 The Turn Beacon On button.

3. In the chassis graphic, click **Turn Beacon On**. Click the button again to stop the beacon from flashing.

System Status LEDs

The system status LEDs provide information about the status of the Gateway, its fans, network connections, and power supplies.

Gen3 H Series Chassis

The table below lists each system status LED, from top to bottom, and its function.

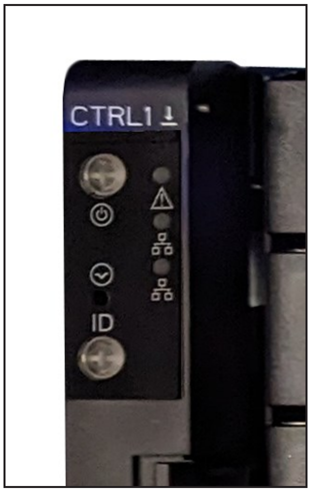


Figure 162 The Gen3 H Series chassis system status LEDs.

Location	LED	Color	Meaning When Lit
Upper-left	**Chassis Power**	**Blue**	The enclosure is powered on and operating correctly. OFF: The enclosure is not powered on.
Upper-right	**Chassis Fault**	**Amber**	One or more components within the enclosure have experienced a fault requiring a service action.
Middle-right	**Network Activity**	**Green**	The system is sending/receiving network traffic on an Ethernet port on the motherboard.
Lower-left	**Chassis Identify**	**Blue**	The enclosure is receiving an identify command. The chassis can also be located using the Visual Status Beacon. See Flash the Visual Status Beacon on the previous page for instructions.

Gen2 X Series Chassis

The table below lists each system status LED, in order from left to right, and its function.

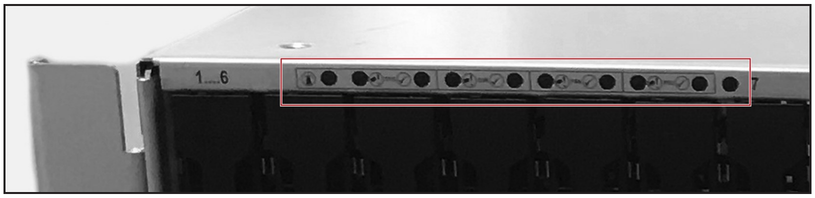


Figure 163 The top left section of the front of the Gen2 X chassis (front bezel removed) showing system status LEDs.

Location	LED	Color	Meaning When Lit
1	**Chassis Identify**	**Blue**	The enclosure is receiving an identify command. The chassis can also be located using the Visual Status Beacon. See Flash the Visual Status Beacon on page 249 for instructions.
2	**Chassis Fault**	**Amber**	One or more components within the enclosure have experienced a fault requiring a service action.
3	**Chassis Power**	**Green**	The enclosure is powered on and operating correctly. OFF: The enclosure is not powered on.
4	**Server Fault**	**Amber**	One or more server modules have experienced a fault requiring a service action.
5	**Server OK**	**Green**	Both server modules are powered on and operating correctly.
6	**Fan Fault**	**Amber**	One or more fan modules have experienced a fault requiring a service action.
7	**Fans OK**	**Green**	All fan modules are powered on and operating correctly.
8	**PM Fault**	**Amber**	One or more power modules have experienced a fault requiring a service action.
9	**PMs OK**	**Green**	Both power modules are powered on and operating correctly.
10	**Not in use**	**N/A**	N/A

Gen2 S Series and Gen2 V Series Chassis

The table below lists each system status LED, in order from left to right, and its function.

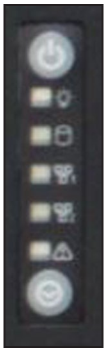


Figure 164 The top right section of the front of the Gen2 S Series chassis, with the front bezel removed, showing system status LEDs.

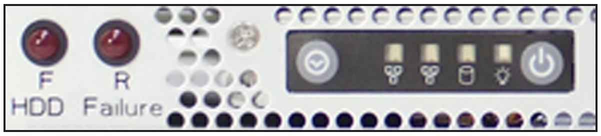


Figure 165 The top left section of the front of the Gen2 V Series chassis, with the front bezel removed, showing system status LEDs.

Icon	LED	Meaning When Lit
💡	**Chassis Power**	The enclosure is powered on and operating correctly. OFF: The enclosure is not powered on.
⛁	**System HDD Activity**	Indicates activity on the system disks.
🖧	**LAN Activity**	The upper or left most LED indicates LAN activity on the BlackPearl management port. The lower or right most LED indicates LAN activity on the data port.
⚠	**Service ID**	This LED is only present on the Gen2 S Series chassis.
HDD Tray LEDs - V Series only		
F	**HDD Failure**	One or more drives in the front row of the drive tray have failed.
R	**HDD Failure**	One or more drives in the rear row of the drive tray have failed.

Gen1 S Series and Gen1 V Series Chassis

The table below lists each system status LED and its function.

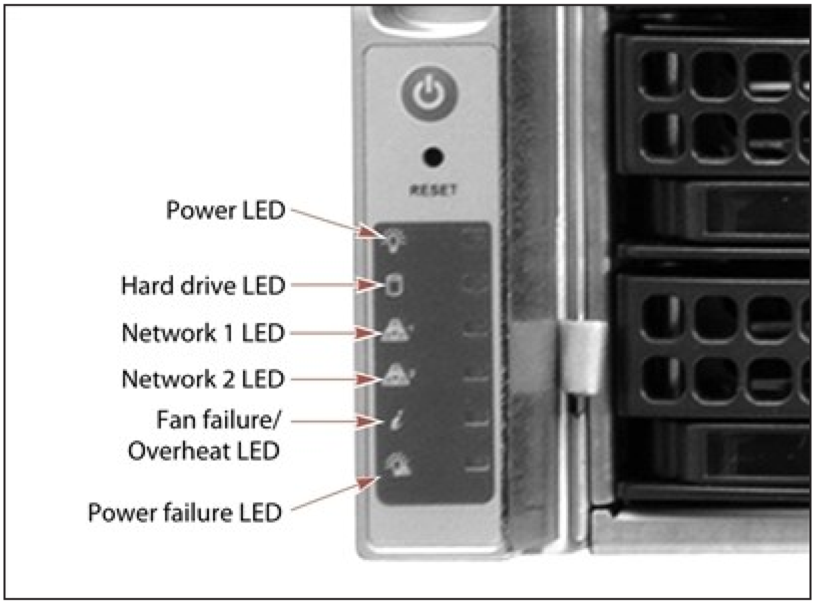


Figure 166 The left side of the front of the Gen1 S Series chassis showing system status LEDs.

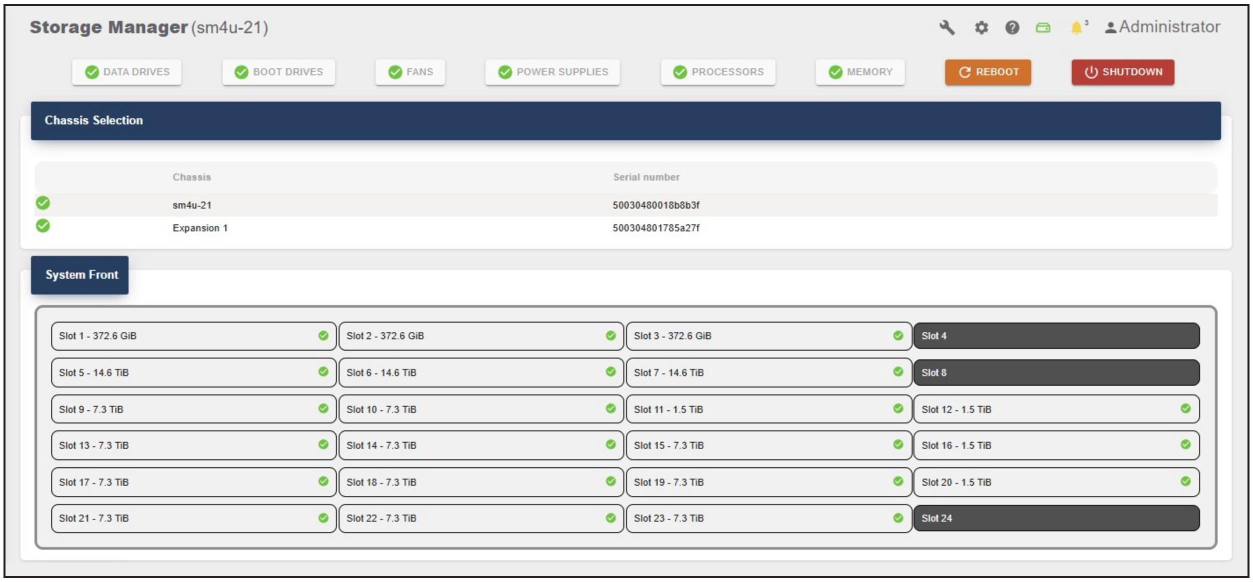
LED	Function
Power	Indicates if the unit is powered on or off.
Hard Drive	Indicates boot drive activity.
Network 1	Indicates network activity on the BlackPearl management port.
Network 2	Indicates network activity on data interface 1. This LED also shows network activity if data interface 1 is configured in link aggregation mode.
Fan Failure / Overheat	• If the LED is blinking red, it indicates a fan failure. Check the BlackPearl user interface to determine which fan failed. • If the LED is solid red, it indicates an overheat condition. Check the BlackPearl user interface to view the status of the Gateway. If the problem persists, contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 7.
Power Failure	Indicates a power supply failure. Check the BlackPearl user interface to determine which power supply failed.

View the Status of Hardware Components

The BlackPearl user interface lets you monitor the status of hardware components in the Gateway without having direct physical access. This is especially useful when your BlackPearl Object Gateway is operating in a “lights out” data center. Check the BlackPearl user interface regularly to ensure that you always know the status of the hardware components.

Use the following instructions to check the status of hardware components.

1. Click **Hardware (hard drive icon)**. The Hardware screen displays.



	Chassis	Serial number
✓	sm4u-21	50030480018b8b3f
✓	Expansion 1	500304801785a27f

Slot 1 - 372.6 GiB ✓	Slot 2 - 372.6 GiB ✓	Slot 3 - 372.6 GiB ✓	Slot 4
Slot 5 - 14.6 TiB ✓	Slot 6 - 14.6 TiB ✓	Slot 7 - 14.6 TiB ✓	Slot 8
Slot 9 - 7.3 TiB ✓	Slot 10 - 7.3 TiB ✓	Slot 11 - 1.5 TiB ✓	Slot 12 - 1.5 TiB ✓
Slot 13 - 7.3 TiB ✓	Slot 14 - 7.3 TiB ✓	Slot 15 - 7.3 TiB ✓	Slot 16 - 1.5 TiB ✓
Slot 17 - 7.3 TiB ✓	Slot 18 - 7.3 TiB ✓	Slot 19 - 7.3 TiB ✓	Slot 20 - 1.5 TiB ✓
Slot 21 - 7.3 TiB ✓	Slot 22 - 7.3 TiB ✓	Slot 23 - 7.3 TiB ✓	Slot 24

Figure 167 The Hardware screen.

2. If your system contains multiple chassis, under the Chassis Selection pane, select the row of the chassis for which you want to view information.
3. Use the buttons on the top of the Hardware screen to jump to that category to view detailed information about the selected component groups.

Clicking...	Shows the...
Data Drives	• Status of each drive (see Data Drive Status Definitions on the next page) • The status of the pool to which the drive is assigned. • Slot number of each drive • Drive size, type, serial number, and firmware level • The name of the pool to which the drive is assigned • If the drive is a SED (Self-Encrypting Drive) • If the drive is currently encrypted • The wear level of the drive (SSD and NVMe drives only)

Clicking...	Shows the...
Boot Drives	• The status of each drive • The serial number, manufacturer, model, size, and firmware of the drive
Fans	• Status and speed of fans
Power Supplies	• Power supply status and wattage **Note:** Power supply information is not available for the 77-bay or 107-bay expansion node.
Processors	• CPU status and temperature • Hyperthreading status • CPU Fan status
Memory	• System memory size

IMPORTANT

To view the status of the SAS ports on a 78-drive expansion node, you must access the legacy user interface used in BlackPearl OS 5.8.x and earlier. Functionality to configure a single port data connection will be added to a later version of the BlackPearl OS.

Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with "/legacy". For example:

https://*ipaddress*/legacy

Data Drive Status Definitions

The table below describes each status for a data drive when viewed on the Hardware screen of the BlackPearl user interface.

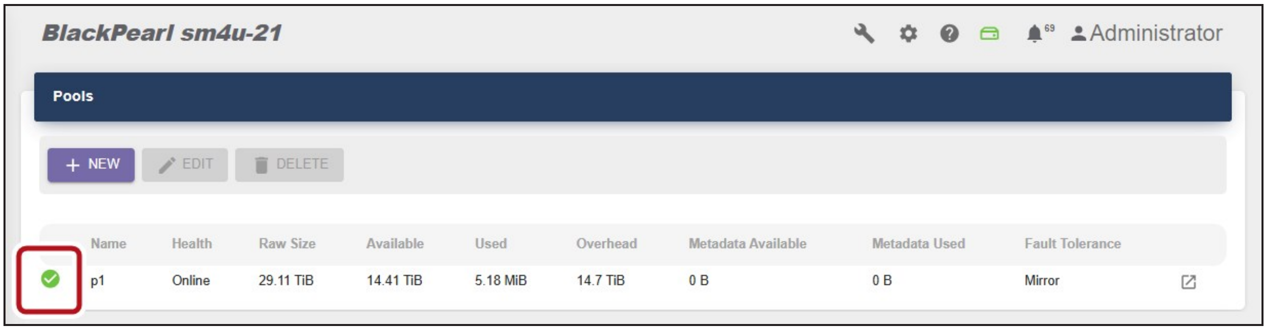
Status	Description
Normal	The drive is in use in a storage pool and is functioning normally.
Spare	The drive not currently in use in the assigned storage pool.
Spare-Available	Unused drive.
Critical	The drive is in a critical state. Contact Spectra Logic Technical Support.
Exported	The drive belongs to a storage pool that was previously exported.
Foreign	The drive is from a different BlackPearl Object Gateway and must be imported.

Status	Description
Rebuilding	The drive is rebuilding. This typically occurs when a spare drive is promoted in the storage pool to Normal.
Unbranded	A drive not sold by Spectra Logic. This drive cannot be used by the system.
Empty	No drive is present in the slot.
SED Initialization Failed	The drive failed to initialize encryption.
SED Unlock Failed	The drive failed to unlock encryption.

View the Status of NAS Pools

The Pools screen provides status information about all NAS storage pools that are configured on the Gateway.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**. The NAS screen displays.



	Name	Health	Raw Size	Available	Used	Overhead	Metadata Available	Metadata Used	Fault Tolerance
✓	p1	Online	29.11 TiB	14.41 TiB	5.18 MiB	14.7 TiB	0 B	0 B	Mirror

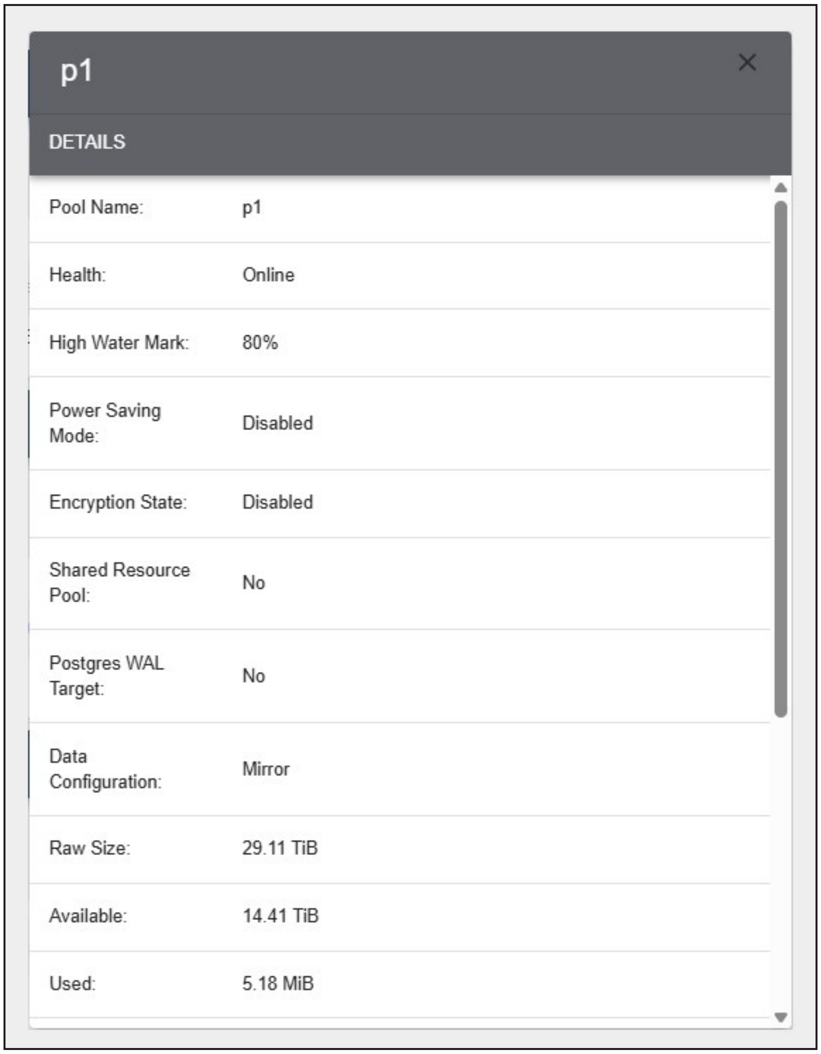
Figure 168 The NAS screen - Pools pane - Status icon.

- The status of each pool is indicated by the status icons on the left side of the screen.
- The Pools pane displays the following information.

This column...	Shows...
Name	The name of each NAS pool.
Health	The current health of each pool. • **Online**—The cache is operating normally. • **Degraded**—One or more drives in the cache is missing, or failed.

This column...	Shows...
Raw Size	The total amount of storage space assigned to each pool.
Available	The amount of unused storage space in each pool.
Used	The amount of used storage space in each pool.
Overhead	The amount of disk space used for overhead, such as parity data.
Metadta Available	The amount of disk space available for metadata information.
Metadata Used	The amount of disk space used by metadata information.
Fault Tolerance	The fault tolerance setting for each pool.

2. To view additional information about a NAS pool, click the **Details** button on the right side of the screen. The *pool name* details screen displays.



Pool Name:	p1
Health:	Online
High Water Mark:	80%
Power Saving Mode:	Disabled
Encryption State:	Disabled
Shared Resource Pool:	No
Postgres WAL Target:	No
Data Configuration:	Mirror
Raw Size:	29.11 TiB
Available:	14.41 TiB
Used:	5.18 MiB

Figure 169 A NAS Pool details screen (partial shown).

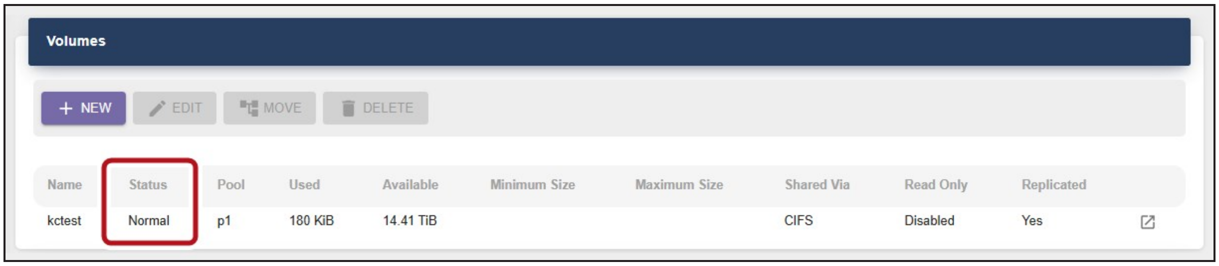
The *pool name* details screen displays the following information:

This row...	Shows...
Name	The name of the pool.
Health	The current health of the pool.
High Water Mark	When the used space on the pool reaches this percentage, an alert is generated. No alert is generated when the percentage is set to zero.
Power Saving Mode	Indicates if power saving mode is enabled or disabled.
Encryption State	Indicates if the pool is encrypted.
Shared Resource Pool	
Postgres WAL Target	
Data Configuration	The protection level for the pool.
Raw Size	The total amount of storage space assigned to the pool.
Available	The amount of available (unused) storage space in the pool.
Used	The amount of used storage space in the pool.
Overhead	The amount of disk space used for overhead, such as parity data.
Drives	The size, RPM, type, and number of drives assigned to the pool.
Write Performance	The number of write performance drives assigned to the pool.
Created	The timestamp of when the pool was created.

View the Status of NAS Volumes

The Volumes screen provides status information about all NAS volumes that are configured on the Gateway.

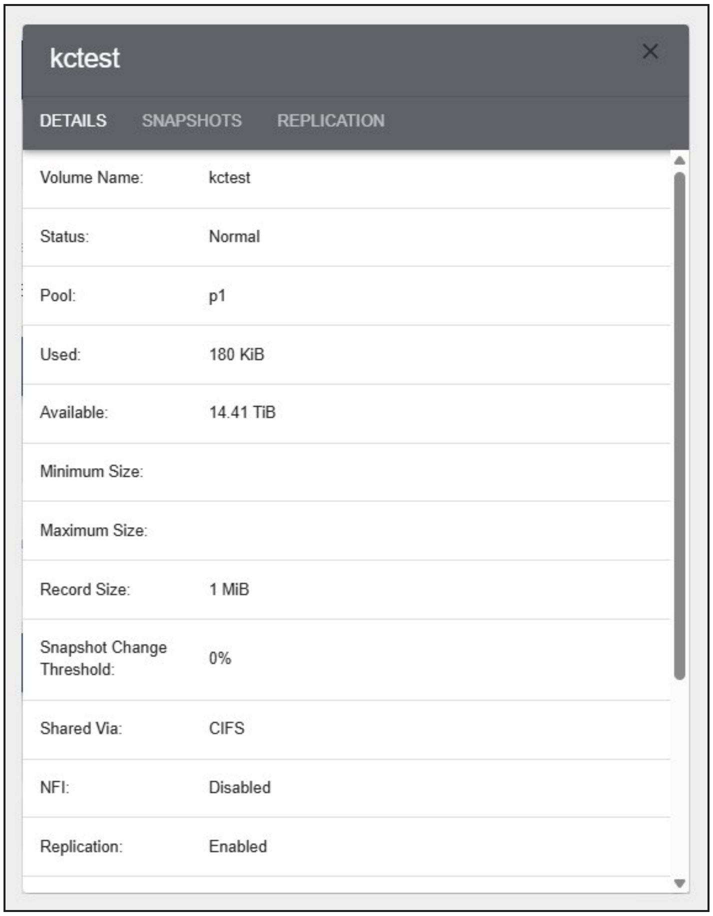
1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**. The NAS screen displays.
2. The status of each volume is indicated by the status column on the left side of the screen.



Name	Status	Pool	Used	Available	Minimum Size	Maximum Size	Shared Via	Read Only	Replicated
kctest	Normal	p1	180 KiB	14.41 TiB			CIFS	Disabled	Yes

Figure 170 The NAS screen - Volumes pane - Status column.

3. To view additional information about a volume, click the **Details** button on the right side of the screen. The *volume name* details screen displays.



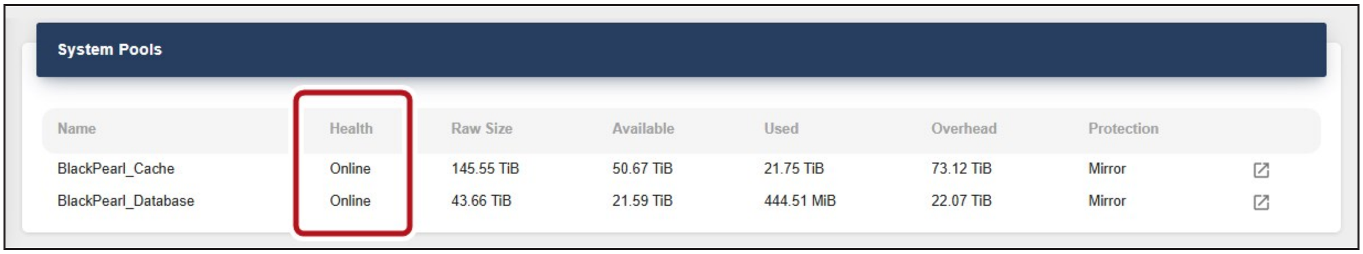
Volume Name:	kctest
Status:	Normal
Pool:	p1
Used:	180 KiB
Available:	14.41 TiB
Minimum Size:	
Maximum Size:	
Record Size:	1 MiB
Snapshot Change Threshold:	0%
Shared Via:	CIFS
NFI:	Disabled
Replication:	Enabled

Figure 171 A NAS Volume details screen (partial).

View the Status of the System Pools

The System Pools pane of the Buckets screen provides status information about the database and cache pools configured on the BlackPearl Object Gateway, as well as status information for each system pool.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Buckets**. The Buckets screen displays.
2. The status of each system pool is indicated in the **Health** column.


System Pools

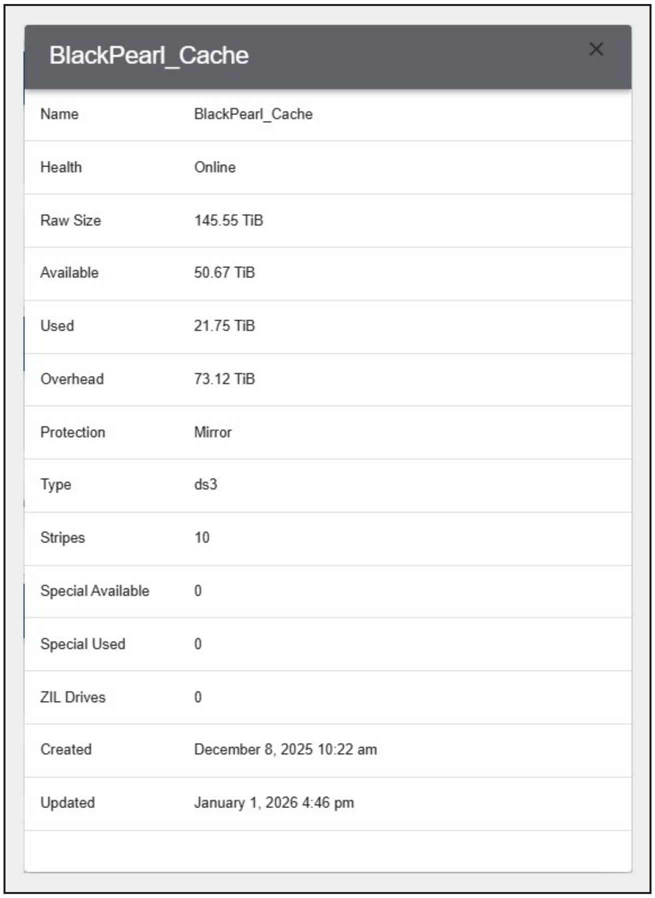
Name	Health	Raw Size	Available	Used	Overhead	Protection
BlackPearl_Cache	Online	145.55 TiB	50.67 TiB	21.75 TiB	73.12 TiB	Mirror
BlackPearl_Database	Online	43.66 TiB	21.59 TiB	444.51 MiB	22.07 TiB	Mirror

Figure 172 The Buckets screen - System Pools pane - Health column.

The System Pools pane displays the following information.

This column...	Shows...
Name	The name of each system pool.
Health	The current health of each system pool. • **Online**—The cache is operating normally. • **Degraded**—One or more drives in the cache is missing, or failed.
Raw Size	The total amount of storage space assigned to each system pool.
Available	The amount of unused storage space in each system pool.
Used	The amount of used storage space in each system pool.
Overhead	The amount of disk space used for overhead, such as parity data.
Protection	The RAID protection setting for each system pool.

3. To view additional information about a system pool, click the **Details** button on the right side of the screen. The *system pool name* details screen displays.



BlackPearl_Cache

Name	BlackPearl_Cache
Health	Online
Raw Size	145.55 TiB
Available	50.67 TiB
Used	21.75 TiB
Overhead	73.12 TiB
Protection	Mirror
Type	ds3
Stripes	10
Special Available	0
Special Used	0
ZIL Drives	0
Created	December 8, 2025 10:22 am
Updated	January 1, 2026 4:46 pm

Figure 173 The BlackPearl_Cache details screen.

The *system pool name* details screen displays the following information:

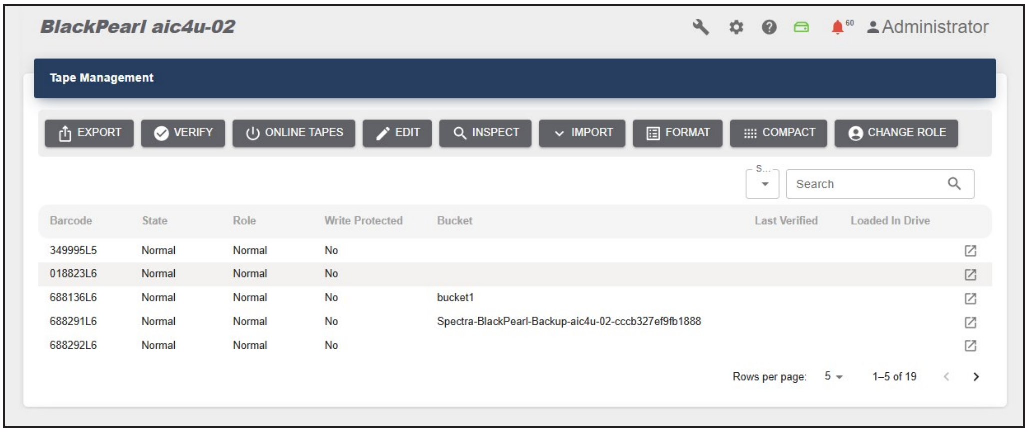
This row...	Shows...
Name	The name of the pool.
Health	The current health of the pool.
Raw Size	The total amount of storage space assigned to the pool.
Available	The amount of available (unused) storage space in the pool.
Used	The amount of used storage space in the pool.
Overhead	The amount of disk space used for overhead, such as parity data.
Protection	The RAID protection setting for the system pool.
Type	The type of pool.

This row...	Shows...
Stripes	The number of stripes used for the system pool.
Special Available	
Special Used	
ZIL Drives	The number of ZIL drives assigned to the pool.
Created	The timestamp of when the pool was created.
Updated	The timestamp of the last time the system pool was accessed.

View Tape Media Information

The Tape Management screen allows you to view the status of all tapes in the associated Spectra Logic or supported tape library.

- Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**.



Barcode	State	Role	Write Protected	Bucket	Last Verified	Loaded In Drive
349995L5	Normal	Normal	No			
018823L6	Normal	Normal	No			
688136L6	Normal	Normal	No	bucket1		
688291L6	Normal	Normal	No	Spectra-BlackPearl-Backup-aic4u-02-cccb327ef9fb1888		
688292L6	Normal	Normal	No			

Rows per page: 5 1–5 of 19

Figure 174 The Tape Management screen.

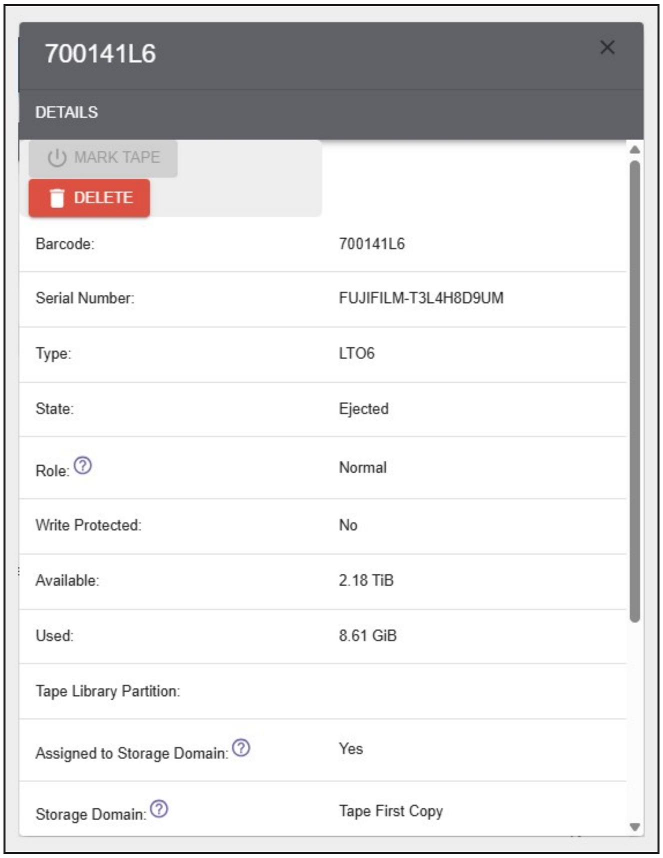
The Tape Management screen displays the following information:

This column...	Shows...
Barcode	The barcode label on the tape cartridge.
State	The status of the tape: During normal operation, the tape state is **MANAGED**. Other possible states are: • **NORMAL** — The tape is ready for use.

This column...	Shows...
	• **AUTO COMPACTION IN PROGRESS** — The tape is in the process of having unused tape space, due to deleted objects that still reside on a tape, reclaimed. • **BAD** — The tape has been identified as bad due to I/O errors or too many write cycles. • **BAR CODE MISSING** — The barcode for the tape is unknown or missing. • **BLACKPEARL FOREIGN** — A tape from another BlackPearl Object Gateway. This data must be copied into a bucket on this Gateway before it is accessible. • **CANNOT FORMAT DUE TO WRITE PROTECTION** — The tape is write-protected and cannot be formatted. • **DATA CHECKPOINT FAILURE** — The tape should have data on it that is recognizable to the BlackPearl Object Gateway, but the Gateway could not verify that the data on the tape is at the correct checkpoint or there was an error rolling back to a checkpoint. • **DATA CHECKPOINT FAILURE DUE TO READ ONLY** — The tape should have data on it that is recognizable to the BlackPearl Object Gateway, but the Gateway could not verify that the data on the tape is at the correct checkpoint or there was an error rolling back to a checkpoint because the tape is read only. • **DATA CHECKPOINT MISSING** — The tape should have data on it that is recognizable to the BlackPearl Object Gateway, but the checkpoint containing the data could not be found on the tape. • **EXPIRED** — The cleaning tape is expired. • **EXPORT FROM EE PENDING** — The tape is in the Entry/Exit (E/E) pool waiting to be physically exported. • **EXPORT TO EE IN PROGRESS** — The tape is currently being moved to the E/E pool. • **EXPORTED** — The tape was exported from the library and is not physically present. • **FORMAT IN PROGRESS** — The tape is currently being formatted. • **FORMAT PENDING** — A format was requested for the tape but has not yet started. • **IMPORT IN PROGRESS** — A **FOREIGN** tape is in the process of being imported into a bucket. • **IMPORT PENDING** — A **FOREIGN** tape is queued to be imported into a bucket. • **INCOMPATIBLE** — The tape type is not supported by the BlackPearlObjectGateway. • **LOST** — The tape was removed from the tape library without first exporting it from a bucket.

This column...	Shows...
State *(continued)*	• **LTFS WITH FOREIGN DATA** — An LTFS formatted tape not associated with a BlackPearl Object Gateway. This data must be copied into a bucket on this Gateway using a raw import before it is accessible. • **OFFLINE** — The tape is in the E/E pool and requires user confirmation to move it to the storage pool and make it online. • **ONLINE IN PROGRESS** — The tape is in the process of being moved from the E/E pool to the storage pool. When complete, its state will change to **PENDING INSPECTION**. • **ONLINE PENDING** — The tape was **OFFLINE** and received user confirmation to bring it online, but this action has not yet begun. • **PENDING INSPECTION** — The tape has not yet been inspected. • **RAW IMPORT IN PROGRESS** — The data on an LTFS formatted tape not associated with a BlackPearl Object Gateway is being imported into the BlackPearl Object Gateway. • **RAW IMPORT PENDING** — An LTFS formatted tape not associated with a BlackPearl Object Gateway is queued to have the data it contains imported into the BlackPearl Object Gateway. • **SERIAL NUMBER MISMATCH** — The tape serial number does not match the one stored in the BlackPearl Object Gateway. • **UNKNOWN** — The tape contains unknown data or is otherwise unavailable to the BlackPearl Object Gateway.
Role	The role of the tape. Values: **Normal, Test**.
Write Protected	The status of the write-protect switch on the cartridge.
Bucket	The bucket to which the tape is assigned.
Last Verified	The timestamp of the last time data was verified on the tape cartridge, by either a manual verification, or when the number of days specified in the storage domain that owns the tape passed.
Loaded In Drive	The BlueScale serial number of the tape drive in which the tape cartridge is loaded.

4. To display detailed information about a tape cartridge, select the tape cartridge row and click the **Details** button on the right-hand side of the row.



Barcode: 700141L6
Serial Number: FUJIFILM-T3L4H8D9UM
Type: LTO6
State: Ejected
Role: Normal
Write Protected: No
Available: 2.18 TiB
Used: 8.61 GiB
Tape Library Partition:
Assigned to Storage Domain: Yes
Storage Domain: Tape First Copy

Figure 175 The Details screen for a selected tape.

The details screen for a selected tape cartridge displays the following:

This row...	Shows...
Barcode	The barcode label on the tape cartridge.
Serial Number	The manufacturer assigned serial number for the tape cartridge.
Type	The media type. Values: **LTO-5, LTO-6, LTO-7, LTO-7 Type M, LTO-8, LTO-9, LTO-10, TS1140, TS1150, TS1155, TS1160, TS1170**
State	The status of the tape. See State on page 262 for a list of tape cartridge states.
Role	The role of the tape. Values: **Normal, Test**.
Write Protected	The status of the write-protect switch on the cartridge.
Available	The amount of unused space that is available on the tape cartridge.

This row...	Shows...
Used	The amount of space on the tape containing data.
Tape Library Partition	The serial number of the partition on the Spectra Logic or other supported tape library containing the tape cartridge.
Assigned to Storage Domain	Whether the tape is allocated to a storage domain. Values: **Yes**, **No**
Storage Domain	The storage domain to which the tape is assigned.
Bucket	The bucket to which the tape is assigned.
Last Modified	The timestamp of the last time data was written to, or read from, the tape cartridge.
Last Verified	The timestamp of the last time data was verified on the tape cartridge, by either a manual verification, or when the number of days specified in the storage domain that owns the tape passed.
Loaded in Drive	
Physical Location	

REBOOT OR SHUT DOWN A BLACKPEARL OBJECT GATEWAY

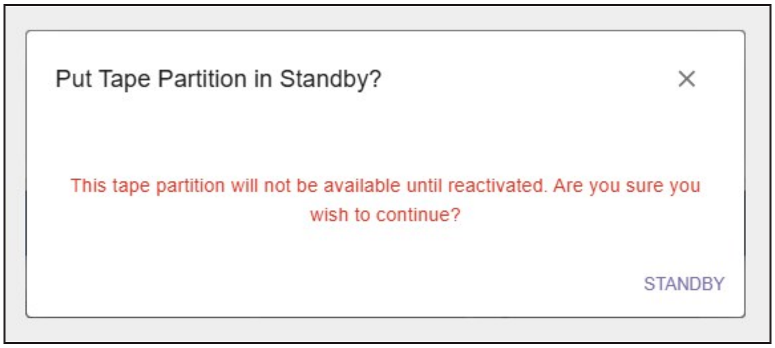
This section discusses rebooting or shutting down a Gateway.

IMPORTANT If the BlackPearl Object Gateway is connected to a tape library, you must put the tape library into standby before you shut down or reboot the BlackPearl Object Gateway.

Using the BlackPearl User Interface

Use the following instructions to reboot or shutdown a Gateway using the BlackPearl user interface.

1. If your BlackPearl Object Gateway is connected to a tape library, you must put each tape partition into standby before you reboot or power-off the BlackPearl Object Gateway. If your configuration does not include a tape library, skip to Step 2 on page 268.
   a. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**.
   b. In the Tape Partitions pane, select the tape partition and click **Standby Tape Partition**. A confirmation window displays.



Put Tape Partition in Standby?

This tape partition will not be available until reactivated. Are you sure you wish to continue?

Figure 176 The Put Tape Partition in Standby confirmation window.

   c. Click **Standby**. The tape partition enters the standby state.
   d. If necessary, repeat for **all** additional tape partitions.

2. Click **Hardware (hard drive icon)** in the upper-right corner of the user interface.

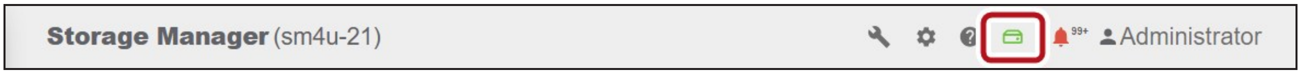


Figure 177 The Hardware button in the upper-right corner of the user interface.

3. Click either **Reboot** or **Shutdown**. A confirmation screen displays (not shown).

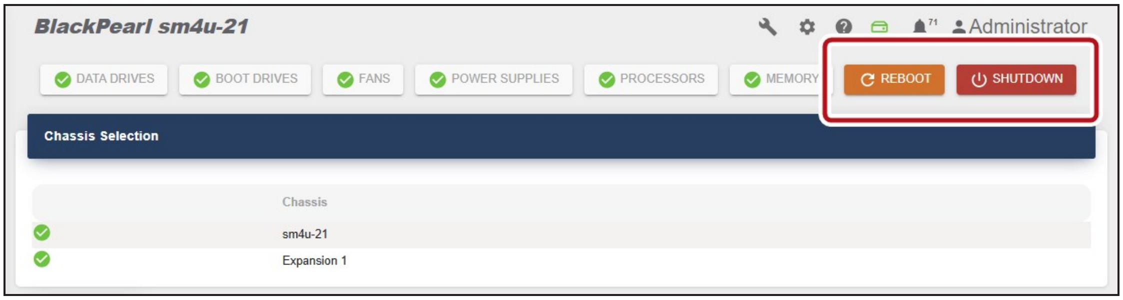


Figure 178 The Hardware screen - Reboot and Shutdown buttons.

4. Click **Submit**.

Note: If you put one or more tape partitions into standby, you must manually activate them after the BlackPearl Object Gateway initializes. See Tape Library Options on page 291.

Power-Cycle Reset

Under some circumstances, Spectra Logic Technical Support may direct you to perform a power-cycle reset of a BlackPearl Object Gateway to recover from an error. To power-cycle reset a BlackPearl Object Gateway, remove the front bezel, and then press and hold the front panel power button until the button’s LED turns off. After a few moments, press the button again to turn the Gateway back on.

CAUTION	Do not use the power button to turn off a BlackPearl Object Gateway unless you are specifically instructed to do so by Spectra Logic Technical Support.

Replace a Failed Component

If a component in a BlackPearl Object Gateway is not functioning properly, the Gateway generates a message and the hardware icon on the status bar of the BlackPearl user interface changes to an error icon (see Status Icons).

Identify the Failed Component

1. Click **Hardware (hard drive icon)** in the upper-right corner of the user interface.

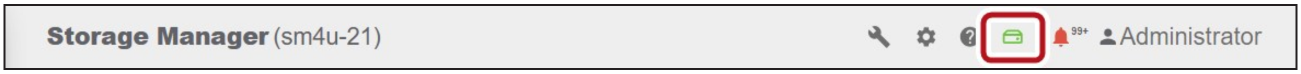
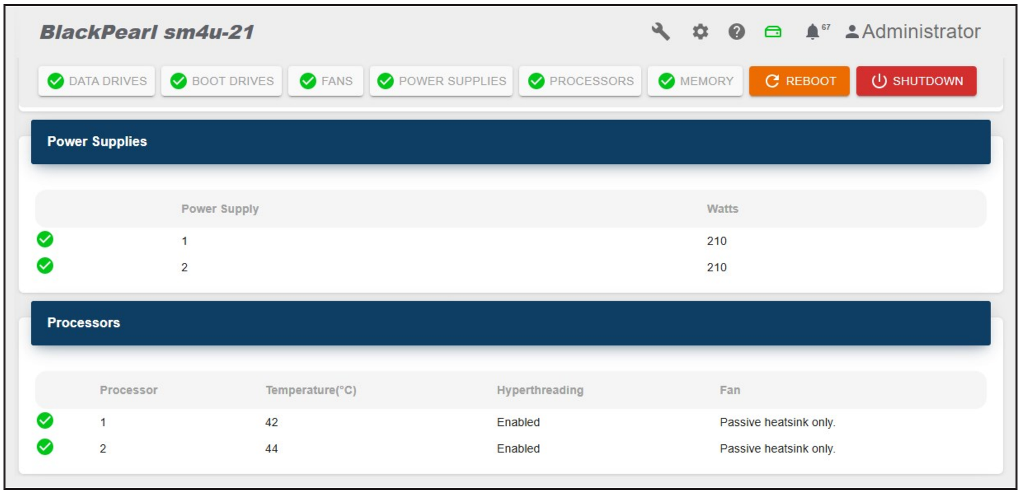


Figure 179 The Hardware button in the upper-right corner of the user interface.

2. Locate the failed component. An **X** in a red circle indicates a failure (icon not shown below).



Power Supplies

	Power Supply	Watts
✓	1	210
✓	2	210

Processors

	Processor	Temperature(°C)	Hyperthreading	Fan
✓	1	42	Enabled	Passive heatsink only.
✓	2	44	Enabled	Passive heatsink only.

Figure 180 The top section of the Hardware screen.

Activate Chassis Beacon

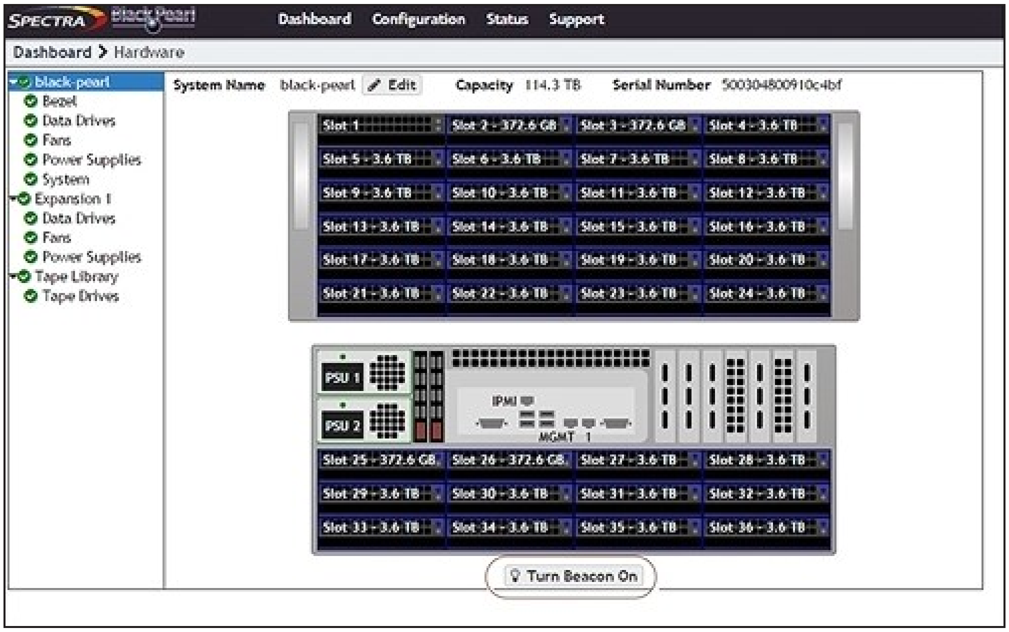
If you have multiple BlackPearl Object Gateways, you can use the beacon feature to help locate the Gateway with the failed component.

To activate the chassis beacon, you must access the legacy user interface used in BlackPearl OS 5.8.x and earlier. Functionality to activate the chassis beacon will be added to the new user interface in a later version of the BlackPearl OS.

1. Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with "/legacy". For example:

   https://*ipaddress*/legacy

2. On the Hardware screen, click the server name. The screen refreshes to show the main Hardware screen.



System Name black-pearl Capacity 114.3 TB Serial Number 500304800910c4bf

Figure 181 The Hardware screen. Gen1 S Series 4U chassis shown.

3. Click **Turn Beacon On**. The BlackPearl Object Gateway Visual Status Beacon light bar flashes blue, making it easy to find.

4. After you locate the unit in your data center, click **Turn Beacon Off** to stop the lights from flashing.

Replace the Failed Component

For specific part replacement procedures, refer to one of the following guides, which can be found after logging into the Spectra Logic support portal at support.spectralogic.com.

- The *Spectra 96-Bay Chassis Drive Replacement Guide* provides instructions for replacing a failed data drive in the 96-bay expansion node.
- The *Spectra 96-Bay Chassis Fan Replacement Guide* provides instructions for replacing a failed fan in the 96-bay expansion node.
- The *Spectra 96-Bay Chassis Power Supply Replacement Guide* provides instructions for replacing a failed power supply in the 96-bay expansion node.
- The *Spectra 96-Bay Chassis I/O Module Replacement Guide* provides instructions for replacing a failed I/O module in the 96-bay expansion node.
- The *Spectra 107-Bay Expansion Node FRU Guide* provides instructions for replacing fans, power supplies, drives, and SAS expanders in the 77-bay and 107-bay expansion node.
- The *Spectra BlackPearl H-Series Chassis Part Replacement Guide* provides instructions for replacing parts in the Spectra BlackPearl H-series chassis.

INSTALLING DATA DRIVES

Use the following instructions to add new drives to a BlackPearl chassis.

Ensure ESD Protection

The working environment for the chassis must be free of conditions that could cause electrostatic discharge (ESD). To protect the chassis from ESD, follow these procedures when installing, repairing, or testing the chassis:

- Place a static protection mat on the work surface used while removing and installing system components. Use a 1-megohm resistor to ground the static protection mat.
- Wear a static protection wrist band or grounding foot strap whenever you handle system components that are removed from their anti-static bags. Connect the wrist band to the static protection mat or to other suitable ESD grounding.
- Keep all electronic components in anti-static bags when not in use.

CAUTION

Any damage to a BlackPearl chassis caused by failure to protect it from electrostatic discharge (ESD) voids the BlackPearl chassis' warranty. To protect the drives from damage:

- Wear an anti-static wristband, properly grounded, throughout the procedure. If a wristband is not available, touch a known grounded surface, such as the unpainted metal chassis.
- Leave the drive in its anti-static bag until you are ready to install it.
- Do not place the un-bagged drive on any metal surfaces.

Select the instructions for your chassis:

- Install a Drive in a Gen3 H Series Chassis
- Install a Drive in a Gen2 S Series Chassis
- Install a Drive in a Gen2 V Series Chassis on page 281
- Install a Drive in a Gen2 X Series Chassis on page 282
- Install a Drive in a Gen1 Chassis on page 284

Install a Drive in a Gen3 H Series Chassis

Install Data Drives

Use the instructions in this section to replace a SAS drive in the BlackPearl H Series chassis.

1. Remove the front bezel.
   a. Using one hand, press and hold the tab on the left-hand side of the chassis.

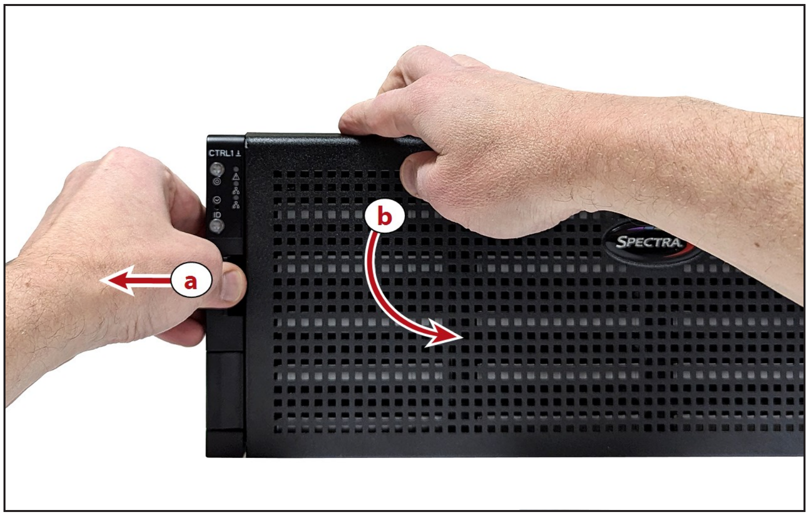


Figure 182 Remove the front bezel.

   b. Use your other hand to pull the faceplate away from the chassis.
2. Press the locking tab on the left side of the sled you want to remove to extend the handle.

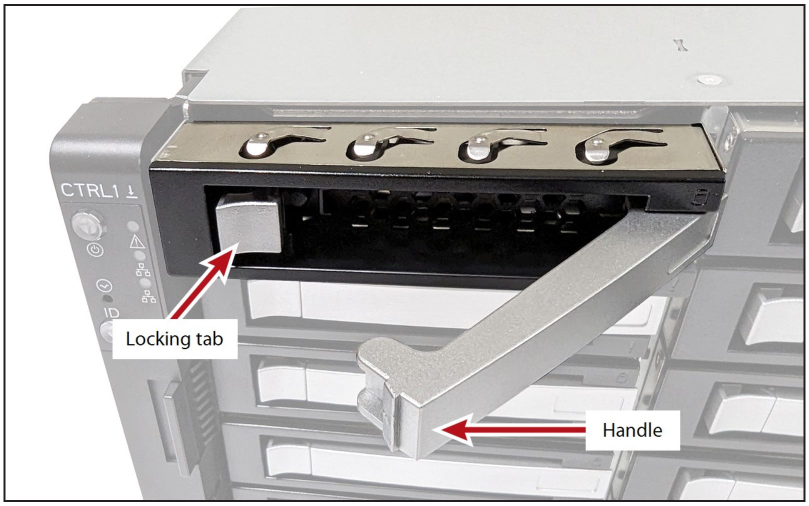


Figure 183 Unlock the drive sled.

3. Pull the handle to remove the drive sled from the chassis.
4. Remove the drive from the anti-static bag.
5. With the front of the drive sled facing you, insert the right side of the drive into the sled. PEMs on the right side of the sled insert into the screw holes in the side of the drive.

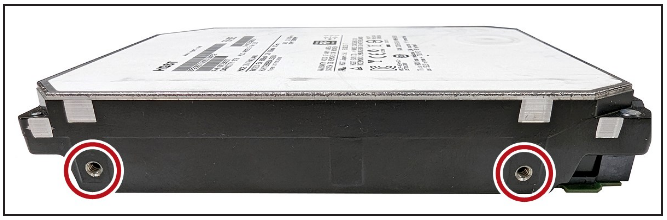


Figure 184 Screw holes in drive.

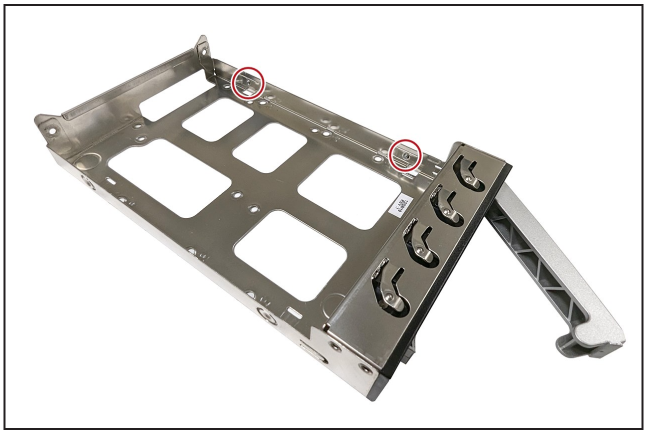


Figure 185 PEMs on right side of sled.

6. Rotate the left side of the drive down into the sled until it snaps into place.

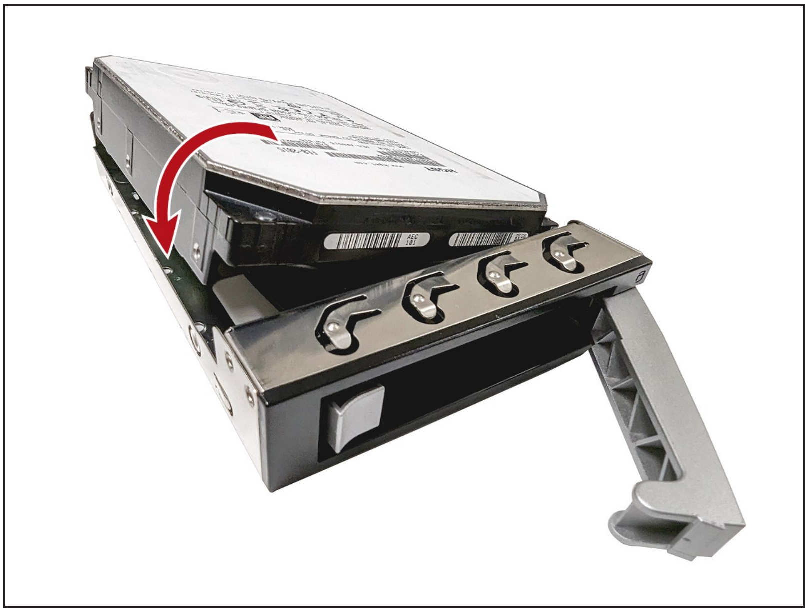


Figure 186 Unlock the drive sled.

7. Slide the drive sled all the way into the chassis, then rotate the sled handle towards the chassis until it locks into place.

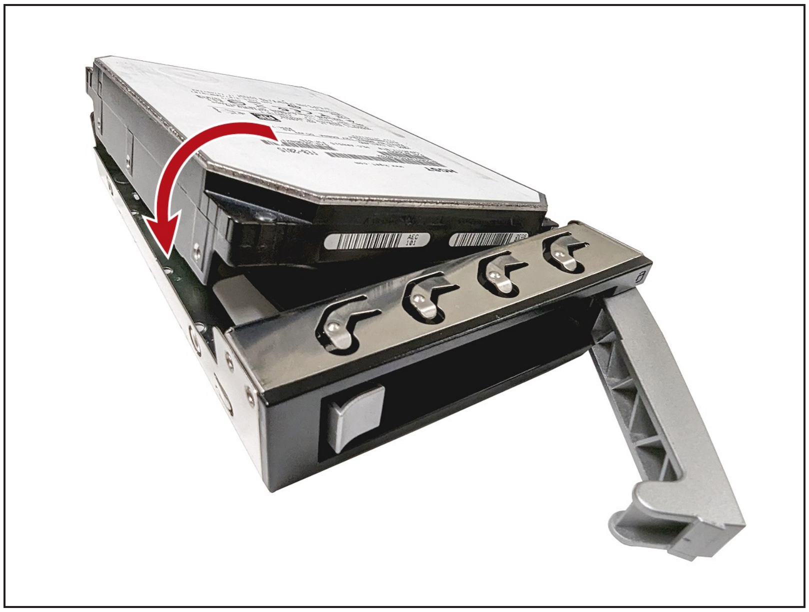


Figure 187 Insert drive into chassis.

8. Attach the front bezel.
   a. Orient the front bezel with the Spectra logo upright and facing you.
   b. Insert the tabs on the right side of the chassis power control faceplate into the slots on the right side of the front bezel.

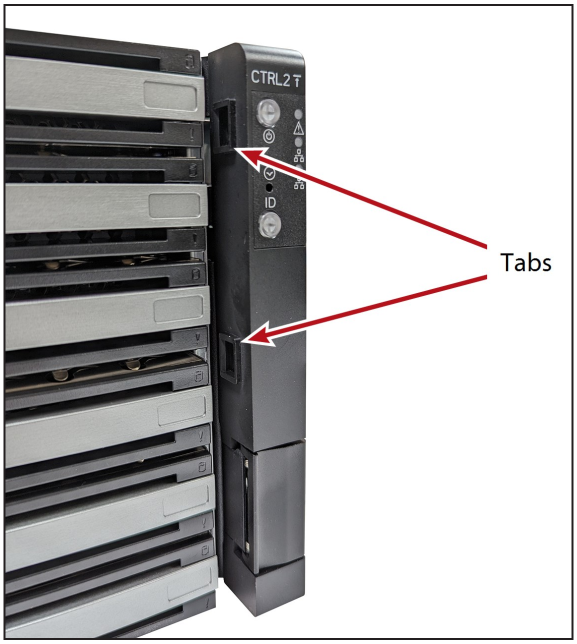


Figure 188 Tabs on the side of power control.

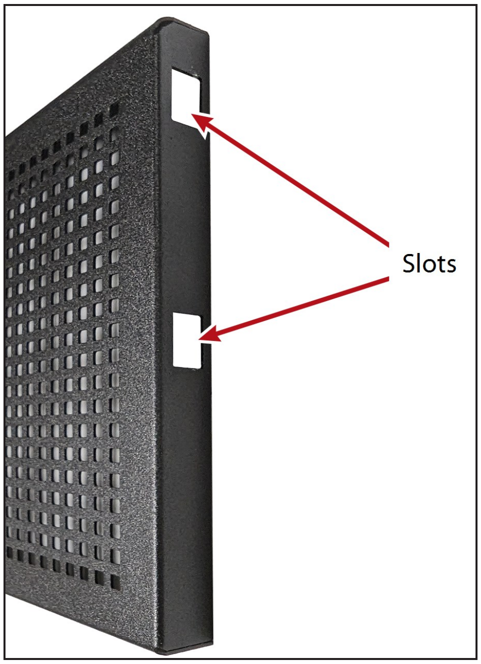


Figure 189 Slots in side of front bezel.

c. Rotate the left side of the front bezel towards the chassis until the tab on the left side of the chassis snaps into place.

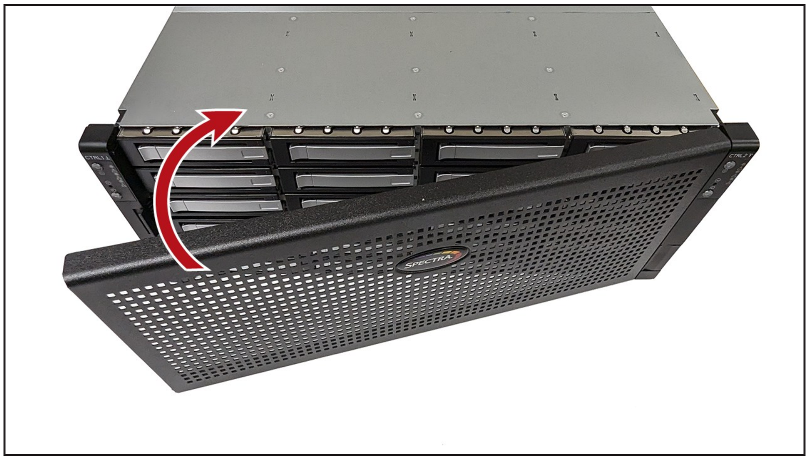


Figure 190 Insert drive into chassis.

Install NVMe Drives

Use the instructions in this section to replace an NVMe drive in the BlackPearl H Series chassis.

Note: If you install a NVMe drive into a powered-on H Series chassis, the system does not recognize the drive until you reboot the system. If you install an NVMe drive into a powered-on HotPair solution, you need to reboot both nodes of the solution.

1. Rotate the handle of the NVMe drive fan module down.

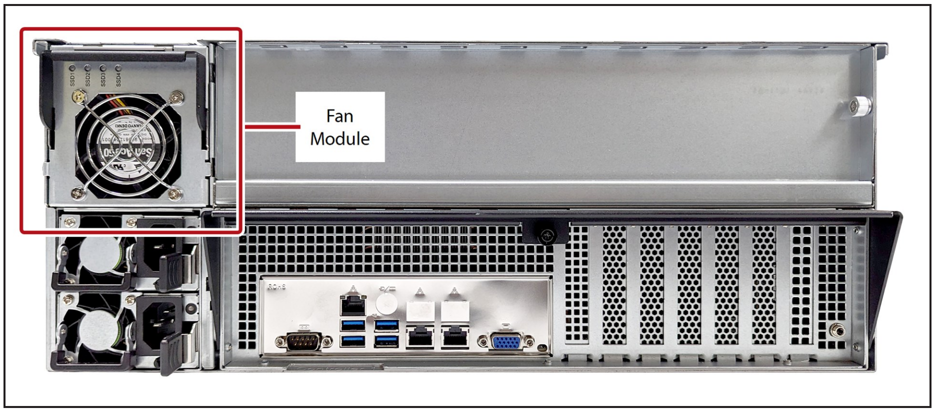


Figure 191 The NVMe drive fan module.

2. While holding the handle of the fan module, use your thumb to press and hold down the locking latch at the top of the fan module, then pull the module away from the chassis.

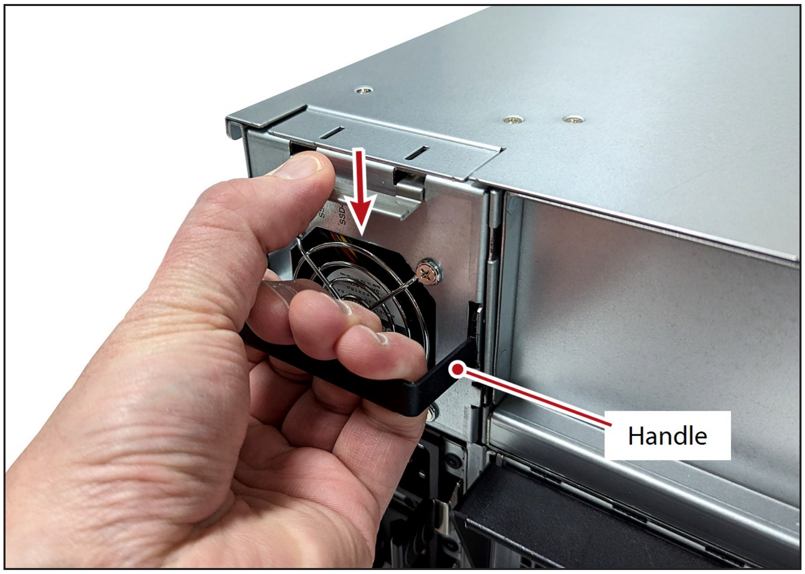


Figure 192 Remove the NVMe drive fan module.

3. Press the tab on the right side of the sled you want to remove to extend the handle.

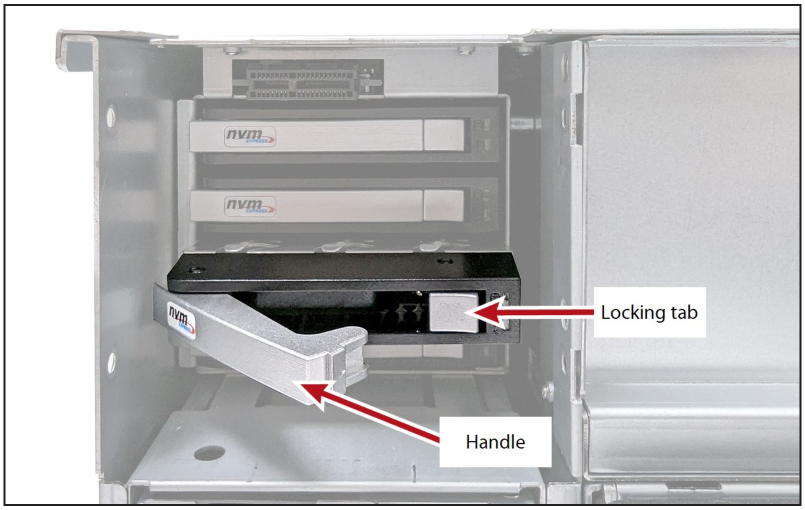


Figure 193 Unlock the drive sled.

4. Pull the handle to remove the drive sled from the chassis.
5. Remove the drive from the anti-static bag.
6. With the front of the drive sled facing you, insert the right side of the NVMe drive into the sled. PEMs on the right side of the sled insert into the screw holes on the side of the drive.

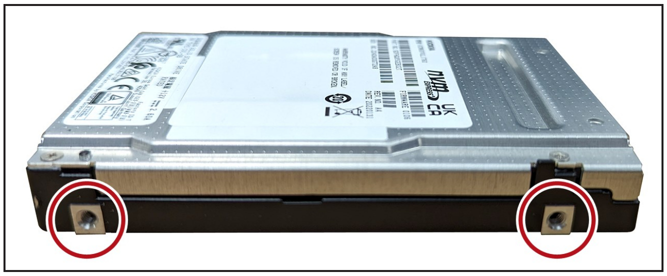


Figure 194 Screw holes in drive.

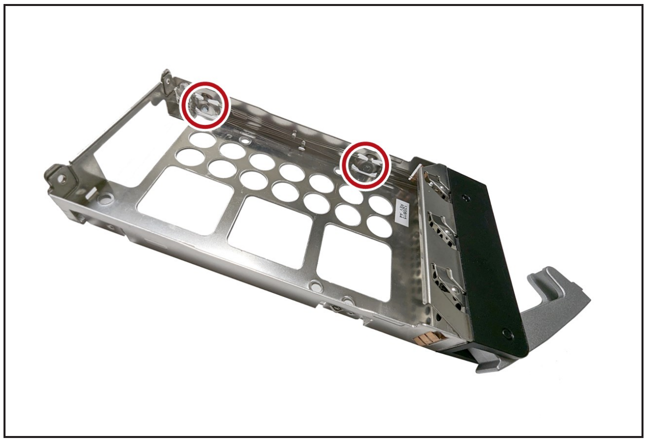


Figure 195 PEMs on right side of sled.

7. Rotate the left side of the drive down into the sled until it snaps into place.

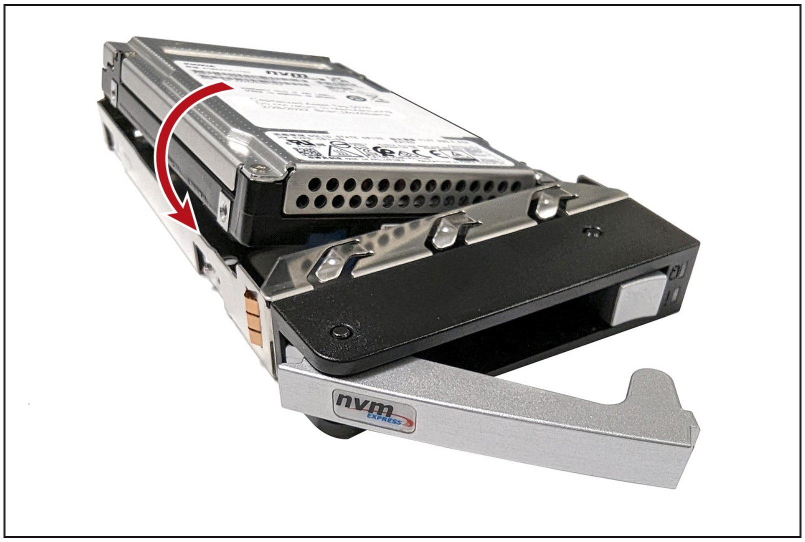


Figure 196 Install the drive into the sled.

8. Slide the drive sled all the way into the chassis, then rotate the sled handle towards the chassis until it locks into place.

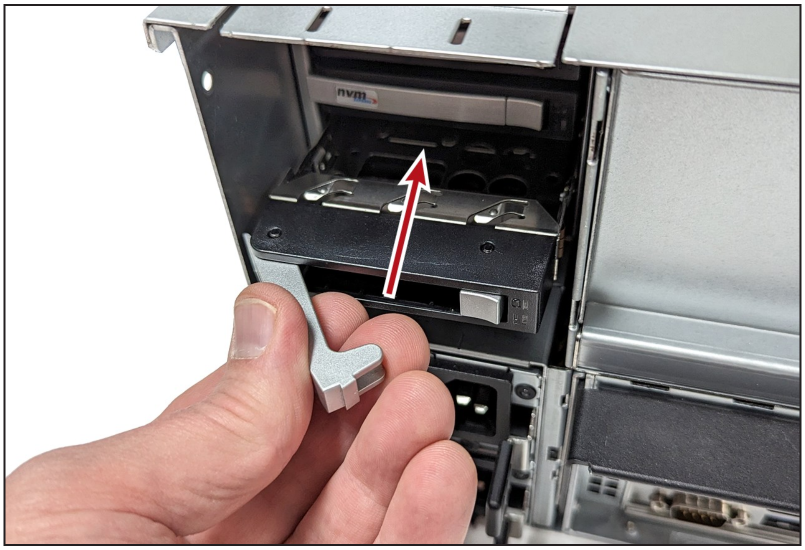


Figure 197 Insert drive into chassis.

9. Repeat Step 3 through Step 8 as need until all drives are installed.
10. Orient the fan module with the drive status lights at the top of the module.
11. Push the module into the chassis until it locks into place.

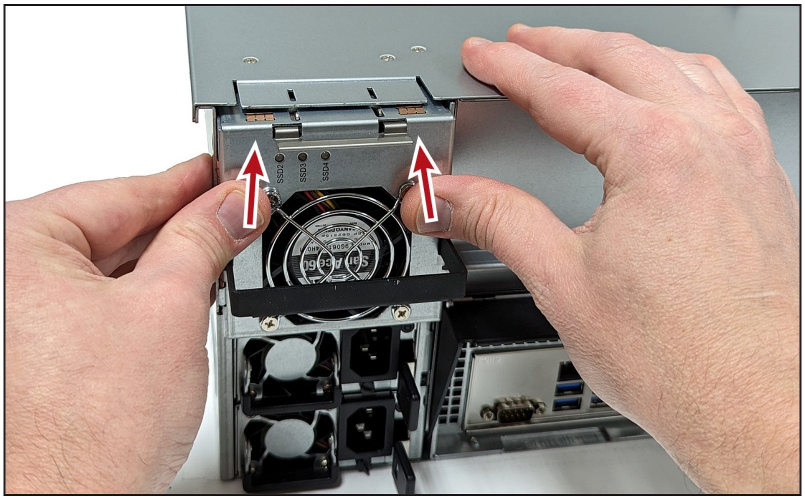


Figure 198 Insert drive into chassis.

12. Rotate the fan module handle upwards until it locks in place.

Install a Drive in a Gen2 S Series Chassis

1. Disconnect the bezel USB connection and remove the bezel from the chassis. The bezel is held on with magnets.
2. Extend the chassis from the rack far enough to remove the front top cover.
3. Simultaneously press the top cover release buttons (**1**) on both sides of the chassis.

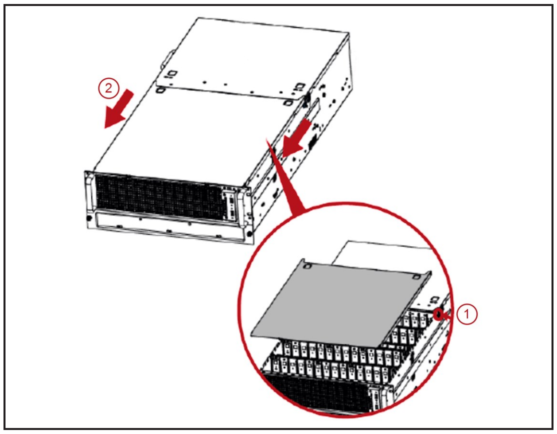


Figure 199 Remove the front top cover.

4. Slide the front top cover toward the front of the chassis (**2**) and lift the cover upward to remove it.

5. Rotate the drive sled locking tab upward (**3**).

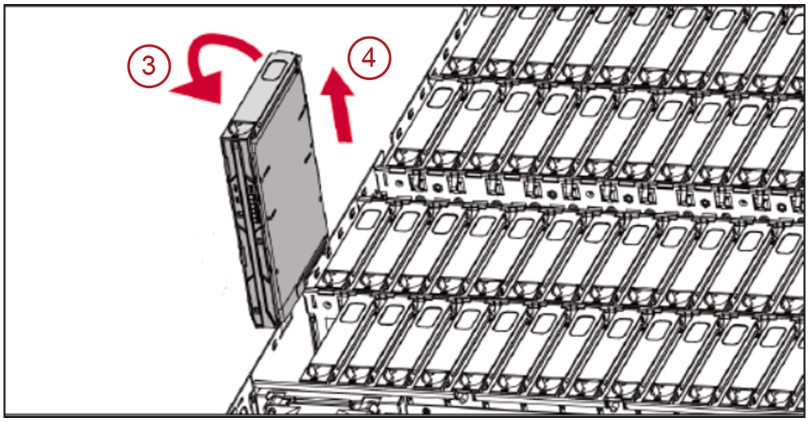


Figure 200 Remove the drive from the BlackPearl chassis.

6. Lift the drive sled out of the chassis (**4**).
7. Match the dimples on the drive sled with the dimples on the drive and insert the drive into the drive sled.

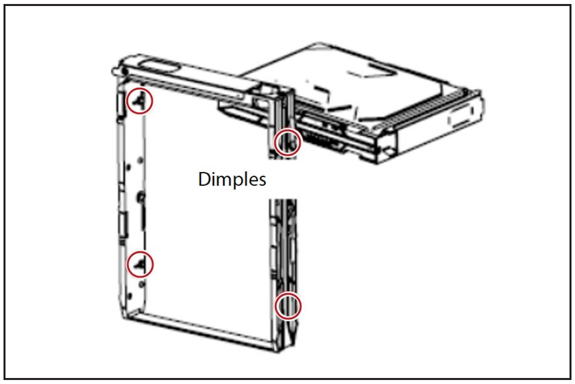


Figure 201 Match the dimples on the drive sled to the dimples on the drive.

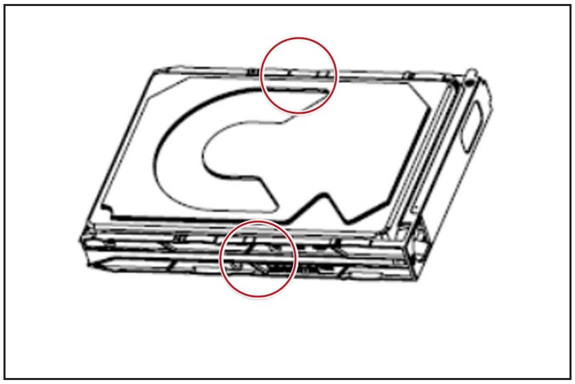


Figure 202 The drive installed in the drive sled.

8. With the locking tab in the open position, slide the drive sled back into the chassis and move the locking tab to the locked position. The drive sled slides in easily; do not force it.
9. Repeat these instructions, starting with Step 5 on page 281 for each additional drive.
10. After installing all of the new drives, slide the cover back on the chassis.
11. Reattach the front bezel and the bezel USB connection.

Install a Drive in a Gen2 V Series Chassis

1. Disconnect the bezel USB connection and remove the front bezel from the chassis. The front bezel is held on by magnets.
2. Press the release buttons (**1**) on the ends of a tray inward to unlock it.

3. Pull the tray out of the chassis(**2**).

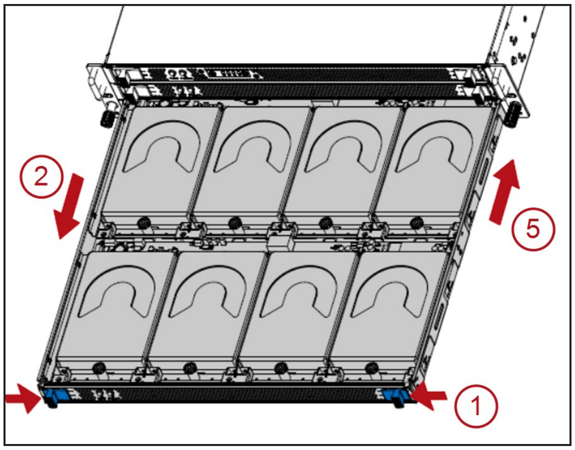


Figure 203 Remove the drive tray.

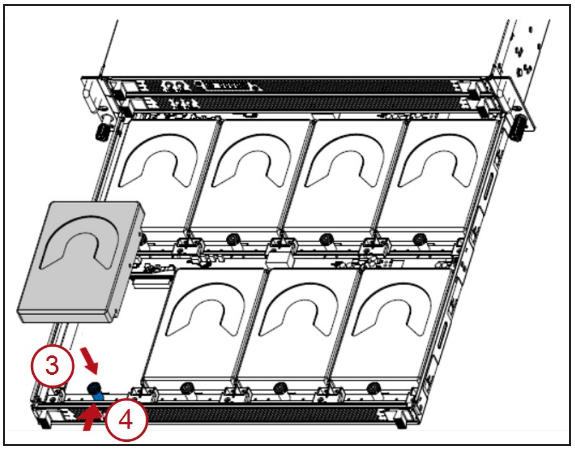


Figure 204 Install the drive.

4. Insert a drive into the chassis (**3**). If necessary, push the plunger (**4**) inward to seat the drive. Make sure that the drive is aligned and locked into the tray.
5. Repeat Step until all drives are installed or the tray is full.
6. Push the tray into the chassis (**5**).
7. If necessary, repeat these instructions starting with Step 2 on page 281 for additional drive trays.
8. Reattach the front bezel and the bezel USB connection.

Install a Drive in a Gen2 X Series Chassis

The drives used in the Gen2 X Series chassis are mounted on drive sleds that ensure proper data and electrical connection with the backplane inside the chassis.

1. Disconnect the bezel USB connection and remove the front bezel from the chassis. The front bezel is held on by magnets.
2. Identify the location where you want to install the drive.

3. Press the release catch (**1**) on the drive carrier in the direction of the arrow to open the handle (**2**). Rotate the drive sled handle upward (**3**) and extend the drive sled slightly out of the chassis by pulling the middle of the handle.

CAUTION Use care to avoid damaging the release latch and drive sled handle.

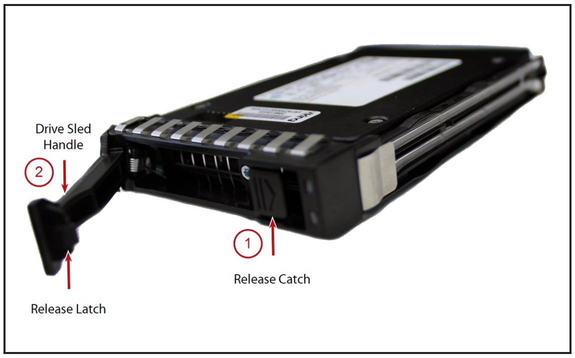


Figure 205 Drive sled parts.

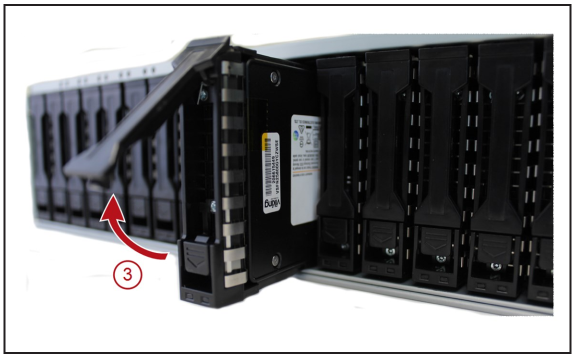


Figure 206 Remove the drive sled with drive blank and insert the drive sled with drive.

4. Grab the carrier frame below the release handle and pull the drive sled completely out of the drive bay.

CAUTION When hot-swapping a drive or drive sled, the replacement must be completed within five (5) minutes to maintain proper system airflow and cooling. If a replacement will take longer than five minutes, install a drive carrier containing a drive blank to prevent thermal damage to the system.

5. Dispose of the empty sled in accordance with your company's guidelines.
6. New drives are shipped installed in a drive sled. Press the release catch (**1** in Figure 205 on page 283) on the drive sled in the direction of the arrow to release the handle.
7. With the drive handle (**2**) in the open position, grab the drive sled just below the handle and gently push the drive sled into the drive bay until the handle engages. The drive sled slides in easily; do not force it.
8. Press the drive handle (**2**) downward until the release latch connects with the release catch (**1**) and the drive locks in place.
9. Repeat these instructions, starting with Step 2 on page 282 for each additional drive.
10. Reattach the front bezel and the bezel USB connection.

Install a Drive in a Gen1 Chassis

The drives used in the Gen1 BlackPearl Object Gateway are mounted on drive sleds that ensure proper data and electrical connection with the backplane inside the BlackPearl Object Gateway.

Remove the Front Bezel

If you are installing a new drive in the front of the Gateway, you need to remove the front bezel prior to installing the drive. The bezel is held in place with magnets. Grasp the sides of the bezel and pull it straight off the Gateway.

Remove the Empty Drive Sled

Use the following steps to remove an empty drive sled.

1. Locate the empty drive bays where you want to install a new drive.

Note: If your Gateway includes an active bezel, do not install a drive in slot 1, which is the top left drive in the front of the Gateway. This slot is reserved for the Visual Status Beacon control sled. The images below show a normal drive sled in slot 1 for clarity.

2. Slide the drive sled locking tab to the right to release the drive sled handle.

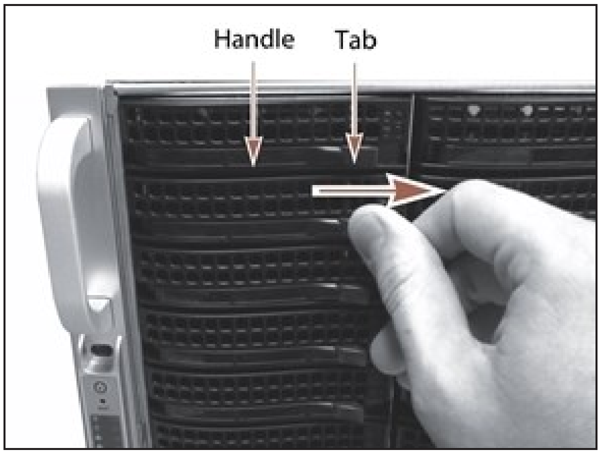


Figure 207 Slide the tab to the right to release the drive sled handle.

3. Grasp the handle and slide the sled completely out of the chassis. If the sled does not slide easily by pulling on the handle, grasp the sides of the sled and pull the sled out of the enclosure.

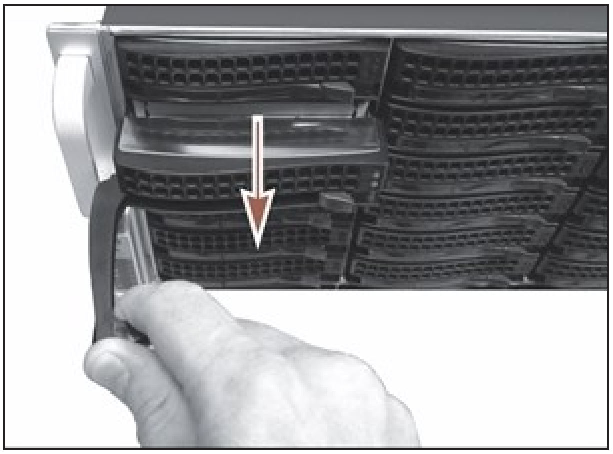


Figure 208 Pull the sled out of the Gateway.

4. Dispose of the empty sled in accordance with your company's guidelines.

Install the New Drive

1. New drives are shipped installed in a drive sled. Slide the locking tab on the front of the drive sled to the right to release the handle.
2. With the drive handle in the open position, slide the drive sled into the chassis until the front of the drive sled is flush against the chassis. The drive sled slides in easily; do not force it.

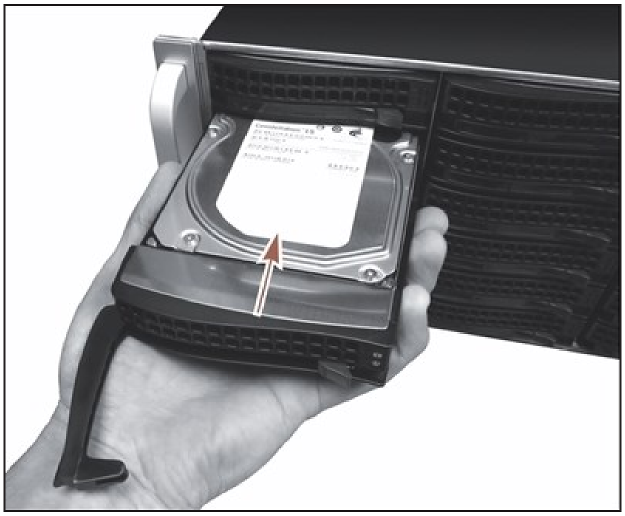


Figure 209 Install the drive into the BlackPearl Object Gateway.

3. When the drive sled is in position, push the handle inward and to the right until the locking tab secures it in place. An audible click indicates that the drive sled is locked into position.
4. If necessary, reinstall the front bezel.

Chapter 12 - Working with Tape Libraries and Media

This chapter describes using the BlackPearl user interface to perform tasks relating to tape libraries and tape media.

TAPE LIBRARY BEST PRACTICES

Tape Library Barcode Reporting

Once a tape library partition(s) and associated tape media are under the control of the BlackPearl Object Gateway, it is important that you do not change the barcode reporting option on the Spectra Logic tape library.

IMPORTANT If you must change the barcode reporting on the tape library for any reason, contact Spectra Logic Technical Support before proceeding.

WORM Media

If the BlackPearl Object Gateway is configured to transfer data to tape, make sure the partitions configured for use by the BlackPearl Object Gateway do not contain WORM (Write Once-Read Many) media. The BlackPearl Object Gateway is not compatible with WORM media.

Available TeraPack Magazines

Spectra Logic recommends having enough empty TeraPack magazines available in each tape library partition to allow for the number of tape cartridge exports in your workflow. If there are not sufficient empty slots in TeraPack magazines, the library marks the tape as a pending export. When empty magazines are imported into the library partition, tapes are physically exported in the order they were logically exported.

BlackPearl System Memory

Spectra Logic recommends having a minimum of 128 GB of system memory for up to four tape drives, and another 16 GB for each additional tape drive. For example, a BlackPearl Object Gateway with 256 GB of system memory can support up to 12 tape drives.

Contact Spectra Logic for information on memory expansion kits for your BlackPearl Object Gateway.

Moving a BlackPearl Object Gateway to a New Tape Library

If you need to move your BlackPearl Object Gateway and the associated tape partition to a new tape library, you must contact Spectra Logic Technical Support for assistance. This type of migration can be easily accomplished, but involves several complex steps which are outside of the scope of this User Guide.

Tape Terminology

In the BlackPearl ecosphere, the following terms are used when discussing tape media.

- **Import** - Adding tape media into the library. New tapes are inspected by the BlackPearl Object Gateway and made available for use.
- **Export** - Removing tape media from the BlackPearl Object Gateway and then from the tape library.
- **Eject** - Removing a tape cartridge from a drive.
- **Entry/Exit Port** - Chambers used as temporary storage while tapes are being imported or exported from a tape library. During import tapes in the entry/exit port are inspected by the BlackPearl Object Gateway and moved to storage chambers. During export, tapes are moved from storage chambers to the entry/exit port before they are physically removed from the library.
- **Storage Chamber** - Chambers used to store tape media while in use by the BlackPearl Object Gateway.

TAPE LIBRARY SUPPORT

The BlackPearl Object Gateway supports Spectra Logic tape libraries, and supports LTO and TS11*xx* technology drives with compatible media.

A tape library may be shared by multiple backup applications, but each application must use one or more tape partition(s) isolated from partition(s) used by other applications. Tape drives assigned to a partition cannot be shared with other partitions.

For detailed information on Spectra Logic tape libraries and drive technology, see your library's *User Guide*.

TAPE LIBRARY OPTIONS

The following sections describe activating a tape library partition, putting a tape library or tape drive into standby, and deleting an existing tape partition.

Activate a Tape Library Partition

If you add a new tape library to your BlackPearl Object Gateway, or your existing tape library has completed service, you must activate the tape partition in the BlackPearl user interface before the Gateway is able to transfer data to the tape library.

Note: If you are activating a new tape library, you must create a partition on the library so that Gateway can automatically detect the new tape library. See your *Library User Guide* for information on creating a partition in a tape library.

Use the instructions in this section to activate a tape library.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**.
2. In the Tape Partitions pane, select the tape partition you want to activate and click **Online Tape Partition**. A confirmation screen displays (not shown).
3. Click **Submit**. The tape partition is activated and is usable by the BlackPearl Object Gateway.

Put a Tape Library Partition into Standby

If you need to perform service on the tape library associated with your BlackPearl Object Gateway, or with the BlackPearl Object Gateway itself, you must first put the tape library into a standby state. Otherwise, the BlackPearl Object Gateway may attempt to use the tape library while it is in service. Putting the tape library into standby allows you to service the tape library without disconnecting the interface cables between the tape library and the BlackPearl Object Gateway.

Note: After the tape partition is placed in standby, any currently running tape operations continue until they are complete, which may take 30 minutes or longer.

Use the instructions in this section to put a tape library partition into standby.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**.
2. In the Tape Partitions pane, select the tape partition you want to put into standby and click **Standby Tape Partition**. A confirmation screen displays (not shown).

3. Click **Submit**. The tape partition is placed in a standby state.

Notes:

- If you have multiple partitions in the same tape library configured for use by the BlackPearl Object Gateway, you must repeat steps Step 2 and Step 3 for each partition in the tape library that requires service.
- After the tape partition is placed in standby, any currently running tape operations continue until they are complete, which may take 30 minutes or longer.

Once you complete service on the tape library and/or the BlackPearl Object Gateway, return the tape library to service using the steps in Activate a Tape Library Partition on page 291.

Tape Drive Options

The following sections describe reserving tape drives, setting a drive to an online or offline state, and removing a tape drive from a partition.

Tape Drive Reservation

Tape drive reservation allows you to control how the tape drives are used to transfer data, by dedicating drives to accept only read commands or write commands, and to accept only jobs of a specified priority level or higher. With a large number of tape drives, using drive reservation can increase efficiency and reduce latency when either reading or writing data. Reserving tape drives for either reading or writing, or for a specified job priority level, is not required and is typically only used when read or write throughput and drive availability are important enough to dedicate tape drives to that function.

Note: Tape drive reservation is not recommended for a BlackPearl Object Gateway connected to two or fewer tape drives.

Tape drive reservation is configured on both the drive, and library partition level.

- When reserving an individual tape drive, you can exclude the drive from performing reads, writes, or jobs lower than a specified level.
- You can also configure the library partition to reserve a specified number of drives for either reads or writes. This can prevent unavailable drives, or drives experiencing a tape drive failure, from impacting the desired number of drives available for either read or write commands.

IMPORTANT Spectra Logic does not recommend setting both a minimum reservation priority and reserved task type for the same drive.

Note: Tape drives always allow inspection and verify tasks.

Tape Drive Reservation Best Practices

If a BlackPearl Object Gateway tape partition only has a small number of tape drives, reservations may not improve the overall performance, but may cause greatly reduced performance if a tape drive fails or goes offline. On a larger tape system, using drive reservations can increase efficiency and reduce latency when either reading or writing data.

It is a best practice to always have two tape drives available for writes to allow the Gateway additional tape failure handling retry logic.

When reserving an individual tape drive, setting the Minimum Task Priority to normal excludes low priority jobs, such as default IOM jobs, from using that tape drive. It also excludes all low priority jobs which may include write or read jobs, which may not be desired if IOM management is the primary use case.

Some BlackPearl workflows and use cases place more importance on ensuring data is written onto tape storage as quickly as possible in a very predictable manner. In these use cases, reserving a majority of the tape drives for writes ensures those tape drives are not interrupted or used by reads from a GET job.

- For example, if there are seven tape drives in a BlackPearl Object Gateway with a 20 (or more) disk drive cache pool, reserving four of the tape drives for writes provides maximum throughput for writes. Those four tape drives cannot be used for GET or restore jobs that need to read data from tape.

For use cases where restoring data is more critical, using tape partition drive reservation is best.

- For example, if there are seven tape drives in a BlackPearl Object Gateway with a 20 (or more) disk drive cache pool, the tape partition can reserve a minimum number of drives for read operations to five. Setting the policy to capacity mode, and enabling minimize spanning also helps increase overall read performance. These settings will generally restrict the write throughput on the BlackPearl Object Gateway to a single tape drive (or two drives for dual copy), making the effective sustained write performance on the BlackPearl Object Gateway approximately 300 MBps. This leaves approximately 500 MBps worth of available throughput in the cache to be used for reads across the five reserved tape drives. This available bandwidth is spread across the five tape drives, which the BlackPearl Object Gateway can utilize to restore subsets of data spread across a large number of tapes.

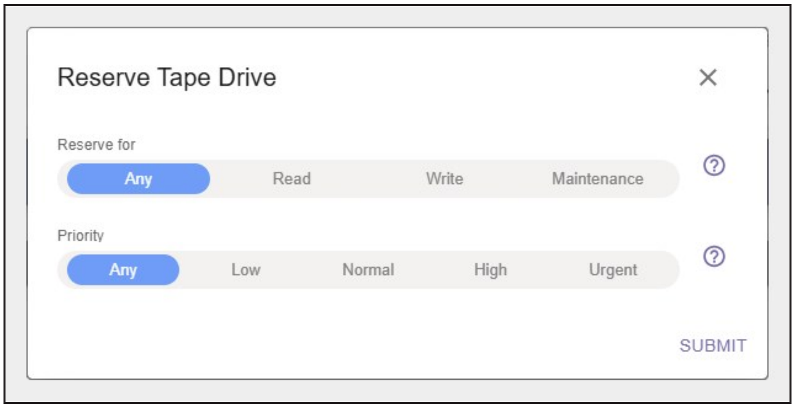
Individual Tape Drive Reservation

If desired, you can reserve a specified tape drive in an existing library partition to dedicate the drive to either read or write operations, or to make the drive available for both types of operations. You can also choose to reserve a drive for operations at or above a configured priority.

⚠ **IMPORTANT** Do not change the Minimum Task Priority when there are active jobs in progress. If you set the priority higher than the priority of active jobs to tape, those jobs do not complete.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**.

2. In the Tape Drives pane, select the drive you want to reserve and click **Reserve Tape Drive**. The Reserve Tape Drive dialog box displays.



Reserve Tape Drive

Reserve for: **Any** | Read | Write | Maintenance

Priority: **Any** | Low | Normal | High | Urgent

Figure 210 The Reserve Tape Drive dialog box.

IMPORTANT Spectra Logic does not recommend setting both a reserved task type and priority level for the same drive.

3. Use the **Reserve For** slider to select one of the following:
   - Select **Any** to make the drive available for both read and write operations.
   - Select **Read** to reserve the drive for read operations and exclude allowing PUT job write tasks from using that drive.
   - Select **Write** to reserve the drive for write operations and exclude allowing GET job read tasks from using that drive.

   Note: Tape drives always allow inspection and verify tasks.

   - Select **Maintenance** to reserve the drive for testing.
4. Use the **Priority** slider to select the priority at which the drive is reserved for tasks at or above the selected priority.

Notes:
- When reserving a tape drive, setting the Priority to **Normal** excludes low priority jobs such as default IOM jobs from using that tape drive, which may not be desired if IOM management is the primary use case. It also excludes all low priority jobs which may include write or read jobs.
- At least one drive in the tape partition must be configured with a Priority of **Any** or **Low**. If only one drive is configured for Any or Low, you cannot change the tape drive reservation.

5. Click **Save**.

Offline a Tape Drive

If you need to perform service on a tape drive in the tape library associated with your BlackPearl Object Gateway, you must first offline the tape drive. Otherwise, the BlackPearl Object Gateway may attempt to use the tape drive while it is in service.

> **Note:** You do not need to put the tape library in a standby state to offline a tape drive.

Use the instructions in this section to offline a tape drive.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**.
2. In the Tape Drives pane, select the drive you want to offline and click **Take Offline**. The Offline Tape Drive dialog box displays (not shown).
3. Click **Submit**. The tape drive is now offline.

Once you complete service on the tape drive, make the tape drive available to the BlackPearl Object Gateway using the steps in Online a Tape Drive below.

Online a Tape Drive

If you add a new tape drive to a partition in your tape library, or finish service on an existing tape drive, you must online the tape drive in the BlackPearl user interface before the Gateway is able to transfer data to the tape drive.

> **Note:** If you are activating a new tape drive, you must configure the drive in a partition on the library so that the BlackPearl Gateway can automatically detect the new tape drive. See your *Library User Guide* for instructions on adding a tape drive to an existing library partition.

Use the instructions in this section to online a tape drive.

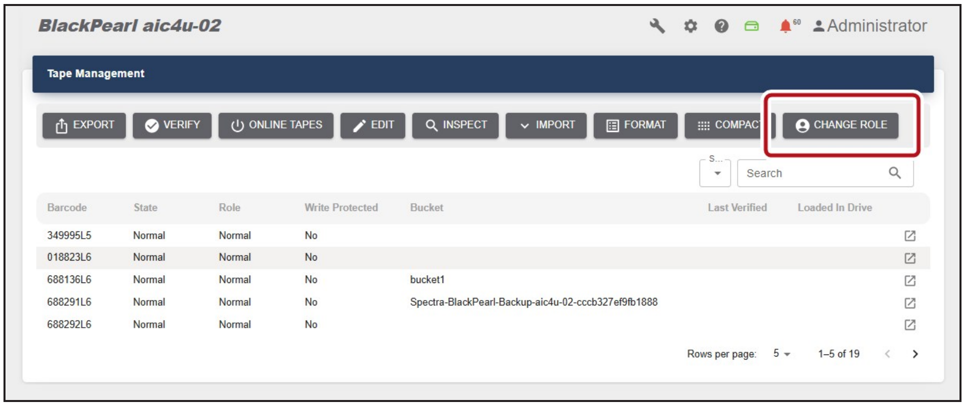
1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**.
2. In the Tape Drives pane, select the drive you want to offline and click **Put Online**. The Online Tape Drive dialog box displays (not shown).
3. Click **Submit**. The tape drive is now online.

Test Tape Drive

A tape drive can be tested using the BlackPearl management interface. The process of testing a drive takes approximately five to ten minutes.

Note: If a cleaning tape is present in the associated tape library, the drive is cleaned prior to testing.

1. If necessary, import a tape cartridge to use for the drive test as described in:
   - Importing Tape Media into a BlueScale Library on page 329.
   - Importing Tape Media into a LumOS Library on page 323.
   - For other tape libraries, see Tape Library User Guides on page 22.
2. If necessary, configure a tape cartridge to use for the drive test.
   a. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**.



BlackPearl aic4u-02

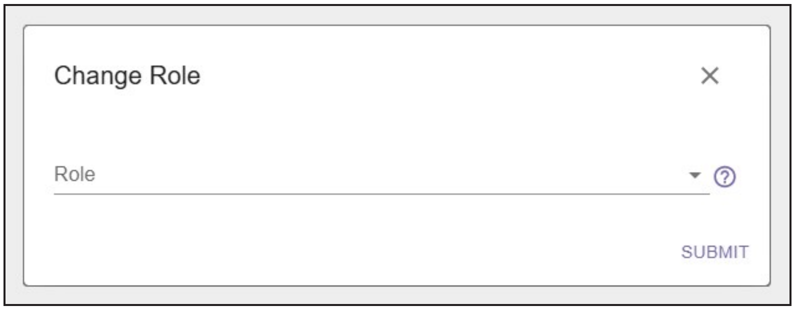
Tape Management

Barcode	State	Role	Write Protected	Bucket	Last Verified	Loaded In Drive
349995L5	Normal	Normal	No			
018823L6	Normal	Normal	No			
688136L6	Normal	Normal	No	bucket1		
688291L6	Normal	Normal	No	Spectra-BlackPearl-Backup-aic4u-02-cccb327ef9fb1888		
688292L6	Normal	Normal	No			

Rows per page: 5 1–5 of 19

Figure 211 The Tape Management screen.

   b. In the Tape Management pane, select the tape to convert to a test tape and click **Change Role**. The Change Role dialog box displays.



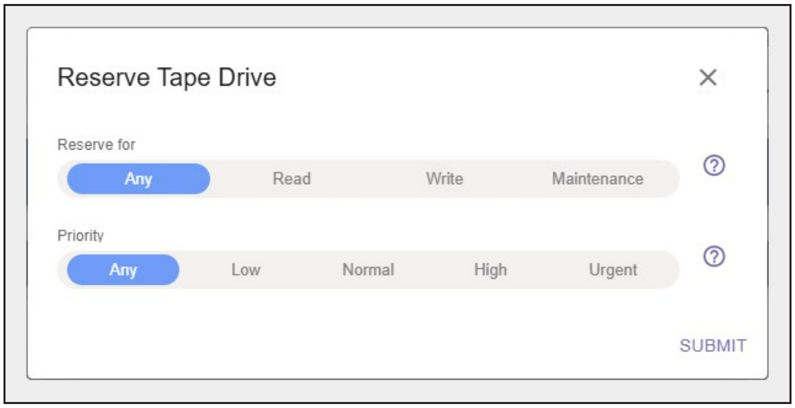
Change Role

Figure 212 The Change Role dialog box.

   c. Use the **Role** drop-down menu to select **Test**.
   d. Click **Submit**.

3. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**.

4. In the Tape Drives pane, select the drive you want to reserve and click **Reserve Tape Drive**. The Reserve Tape Drive dialog box displays.



Reserve Tape Drive

Reserve for: [✓ Any] Read Write Maintenance

Priority: [✓ Any] Low Normal High Urgent

Figure 213 The Reserve Tape Drive dialog box.

5. Use the **Reserve For** slider to select **Maintenance**.

6. Click **Submit**.

7. In the Tape Drives pane, select the drive you want to test and click **Test Tape Drive**. The Test Tape Drive dialog box displays (not shown).

8. Use the **Test Tape** drop-down menu to select a tape with a reservation state of maintenance. Only tapes in this state display in the drop-down menu.

9. Click **Submit**.

- If the drive test **passes**, return the drive to service.

   a. In the Tape Drives pane, select the drive you want to reserve and click **Reserve Tape Drive**. The Reserve Tape Drive dialog box displays.

   b. Use the **Reserved For** slider to select the desired role for the drive, and click **Submit**.

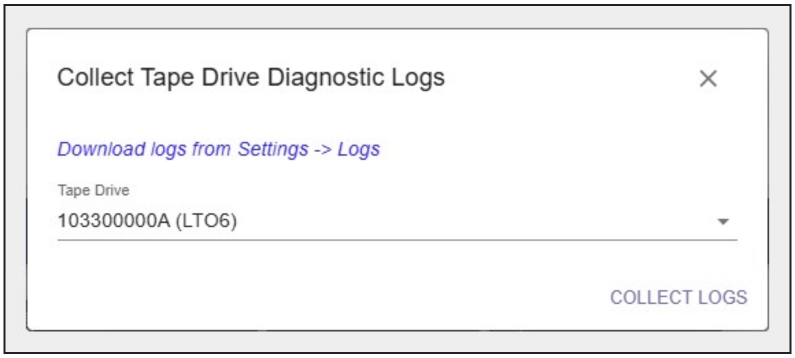
- If the drive test **fails**, collect drive diagnostic logs as described in Collect and Download Drive Diagnostic Logs on the next page and contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

Collect and Download Drive Diagnostic Logs

If desired, or at the direction of Spectra Logic Technical Support, use the instructions in this section to generate drive diagnostic logs (also referred to as drive dumps). The process takes approximately 30 seconds.

Collect the Drive Log

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**.
2. In the Tape Drives pane, click **Collect Logs**. The Collect Tape Drive Diagnostic Logs dialog box displays.



Collect Tape Drive Diagnostic Logs

Download logs from Settings -> Logs

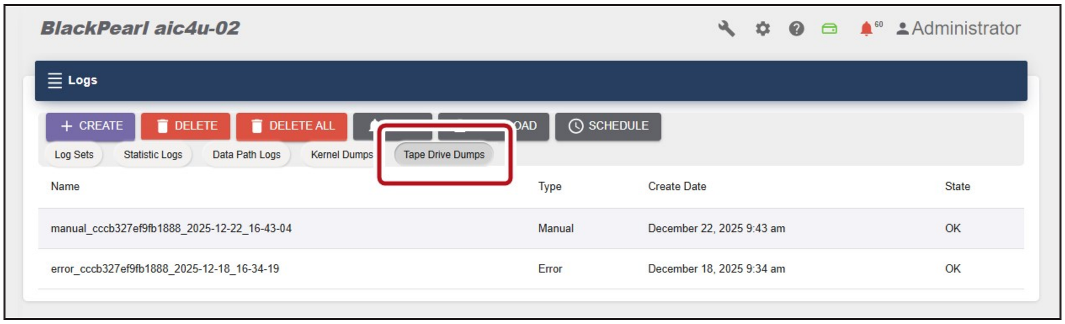
Tape Drive: 103300000A (LTO6)

Figure 214 The Collect Tape Drive Diagnostic Logs window.

3. Use the **Tape Drive** drop-down menu to select the drive for which you want to collect logs.
4. Click **Collect Logs**. The process takes approximately 30 seconds.

Download the Drive Diagnostic Log

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Logs**.
2. Filter the list by clicking **Tape Drive Dumps**.



BlackPearl aic4u-02

Logs

Name	Type	Create Date	State
manual_cccb327ef9fb1888_2025-12-22_16-43-04	Manual	December 22, 2025 9:43 am	OK
error_cccb327ef9fb1888_2025-12-18_16-34-19	Error	December 18, 2025 9:34 am	OK

Figure 215 The Logs screen - Tape Drive Dumps button.

3. Select the tape drive diagnostic log (drive dump) you want to download, and click **Download**. The Download Logset window displays (not shown).
4. Click **Submit**. The log begins downloading through your web browser.

Compact a Tape Cartridge

The BlackPearl Object Gateway uses tape compaction to reclaim space used by deleted objects that still reside on tape media, and to clone data from a specified tape cartridge to available space on one or more different tape cartridge(s).

When a tape is compacted, any space used by deleted files is reclaimed by marking the sections of tape used by deleted files as available for use. This is helpful to reclaim space on tape cartridges, or to recycle entire tapes if they only contain deleted files.

Additionally, any active data on the tape cartridge being compacted is cloned to available space on other tape cartridge(s) assigned to the same bucket. This allows you to easily create an additional copy the data on a specified tape cartridge.

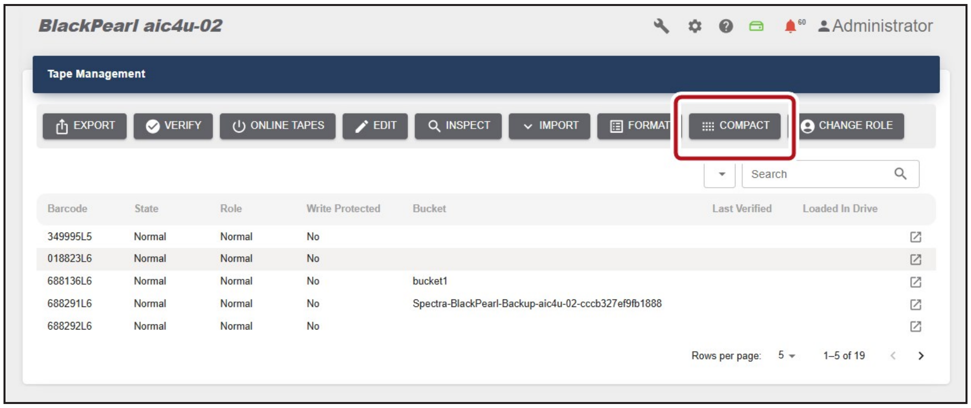
This is helpful if you want to retire or repurpose specific pieces of media while still maintaining a copy of the data on the tape in your BlackPearl ecosystem.

Note: Tape compaction does not create a direct 1:1 copy of a tape cartridge. The BlackPearl Object Gateway clones data on the tape cartridge to available space on other tape media, and may use more than one tape cartridge.

If a tape partition is configured to automatically compact tapes, but you want a specified tape cartridge to be compacted before it is normally selected for tape compaction, you can force the BlackPearl Object Gateway to include a tape cartridge in the next tape compaction cycle.

Use the instructions in this section to add a tape cartridge to the next auto compaction cycle.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**.

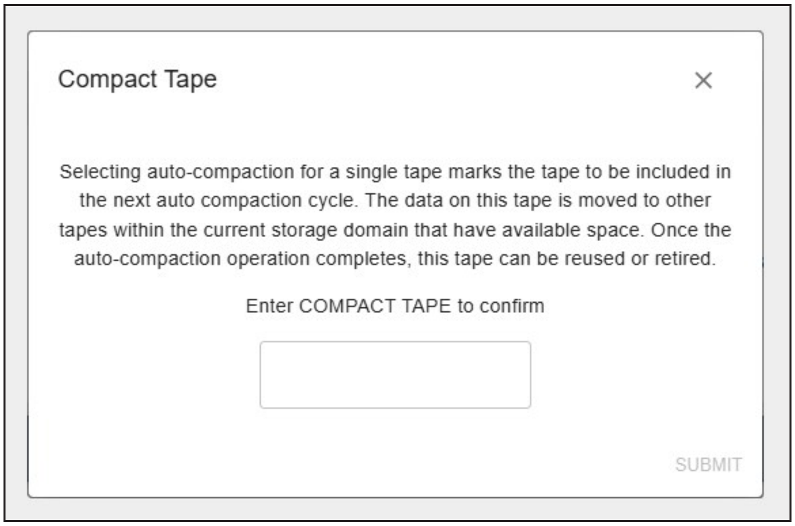


Barcode	State	Role	Write Protected	Bucket	Last Verified	Loaded In Drive
349995L5	Normal	Normal	No			
018823L6	Normal	Normal	No			
688136L6	Normal	Normal	No	bucket1		
688291L6	Normal	Normal	No	Spectra-BlackPearl-Backup-aic4u-02-cccb327ef9fb1888		
688292L6	Normal	Normal	No			

Rows per page: 5 1–5 of 19

Figure 216 The Tape Management screen - Tape Management pane - Compact button.

2. In the Tape Management pane, select the tape cartridge you want to compact and click **Compact**. The Compact Tape dialog box displays.



Compact Tape

Selecting auto-compaction for a single tape marks the tape to be included in the next auto compaction cycle. The data on this tape is moved to other tapes within the current storage domain that have available space. Once the auto-compaction operation completes, this tape can be reused or retired.

Enter COMPACT TAPE to confirm

Figure 217 The Compact Tape dialog box.

3. Enter `COMPACT TAPE` in the entry box, and click **Submit**. The tape cartridge is added to the next auto compaction cycle.

FORMAT MANAGED BLACKPEARL TAPES

If you want to reclaim tapes currently managed by the BlackPearl Object Gateway for use as new data storage, use the instructions in this section to format tapes. During formatting, the BlackPearl Object Gateway creates two partitions on the tape media, and writes the corresponding index information to the tape cartridge MAM. Once the format is complete, the tape cartridges are available for use.

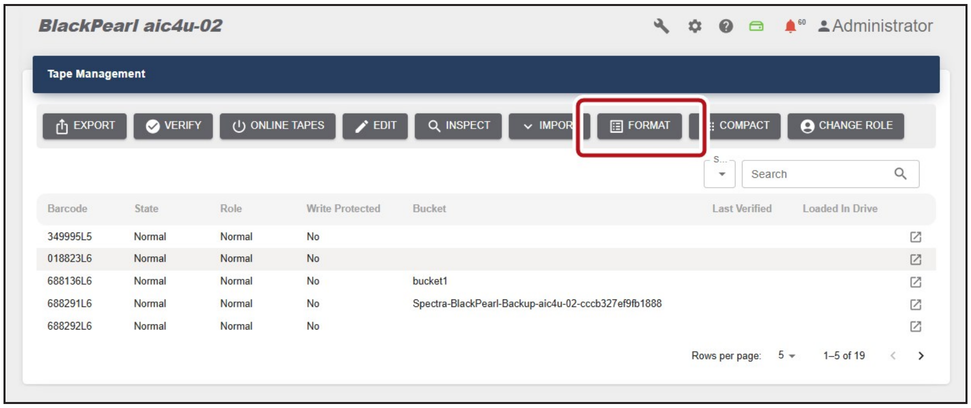
⚠ **CAUTION** Any data currently on the tape media is lost during the format operation.

The **Force** parameter must be used to format a tape if any of the below conditions are met:

- To format a tape before it is inspected.
- To format a tape that has already been formatted by a BlackPearl Object Gateway,
- To format a tape that contains data written by a BlackPearl Object Gateway.
- To format a tape that currently has reads or writes scheduled.

Note: Tapes are not eligible for formatting if they have a state of EXPORTED, LOST, EXPORT_ PENDING, or OFFLINE.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**.



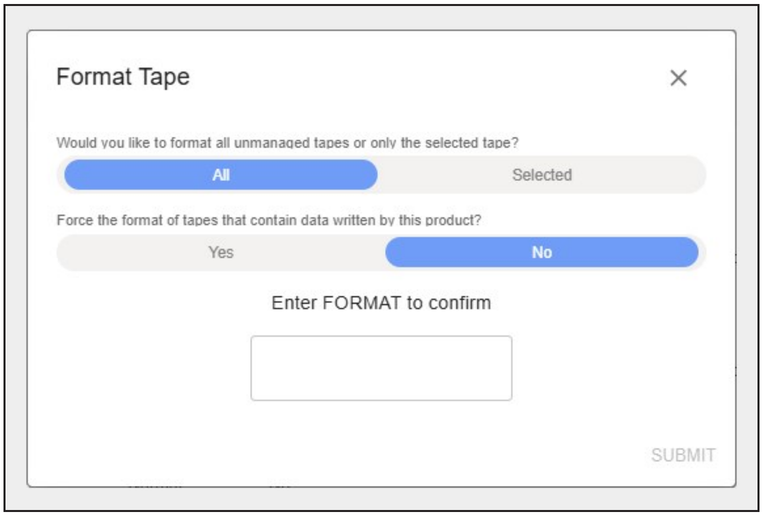
Barcode	State	Role	Write Protected	Bucket	Last Verified	Loaded In Drive
349995L5	Normal	Normal	No			
018823L6	Normal	Normal	No			
688136L6	Normal	Normal	No	bucket1		
688291L6	Normal	Normal	No	Spectra-BlackPearl-Backup-aic4u-02-cccb327ef9fb1888		
688292L6	Normal	Normal	No			

Rows per page: 5 1–5 of 19

Figure 218 The Tape Management screen - Tape Management pane - Format button.

2. Select one of the tapes you want to format, and click **Format**. The Format Tape dialog box displays.

Note: If you want to format all tapes, you must select at least one tape to proceed to the next step.



Format Tape

Would you like to format all unmanaged tapes or only the selected tape?

Force the format of tapes that contain data written by this product?

Enter FORMAT to confirm

Figure 219 The Format Tape dialog box.

3. Use the **All Tapes/Selected Tape** slider to select one of the following:
    - **All** - All unmanaged tapes are formatted.
    - **Selected** - Only the tape you selected in the previous step is formatted.
4. Use the **Force Format** slider to select one of the following:
    - **Yes** - The tape is formatted even if it contains data from a BlackPearl Object Gateway.
    - **No** - The tape is not formatted if it contains data from a BlackPearl Object Gateway

Note: If the selected tape contains data from a BlackPearl Object Gateway, you cannot format the tape unless you select the **Force** option.

IMPORTANT Do not use the **Force** option to force a format on a cleaning tape. If you do so the cleaning tape is set to "expired" and no longer usable for cleaning drives.

5. Enter `FORMAT` in the entry field and click **Submit**.

    The Gateway instructs the library to load the selected tapes into tape drives configured in the library, to format the tape(s) for LTFS. This is the format used by the BlackPearl Object Gateway. This process can take up to five minutes per tape.

INSPECT TAPES

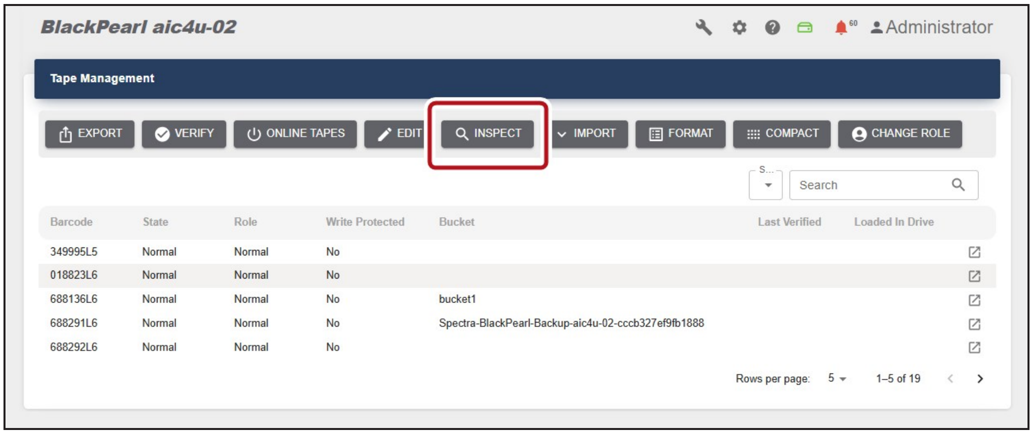
Tapes are normally inspected automatically by the Gateway. If you use the tape library's user interface to move a tape cartridge in a partition associated with a BlackPearl Object Gateway, the tape may transition to the Pending Inspection state (see Monitor the Gateway Hardware on page 246) and become unusable by the Gateway until it is inspected either automatically when the system is able based on current workload, or by manually requesting an inspection. To return the cartridge to a usable state, manually request an inspection of the cartridge.

Inspecting a tape manually is useful if the tape cartridge transitions to a state of "Unknown" or "Bad". Inspecting the tape cartridge while in these states may recover the cartridge for use.

IMPORTANT Tape inspection may take several hours or days depending on the number of tapes to be inspected.

Use the instructions in this section to inspect a tape.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**.

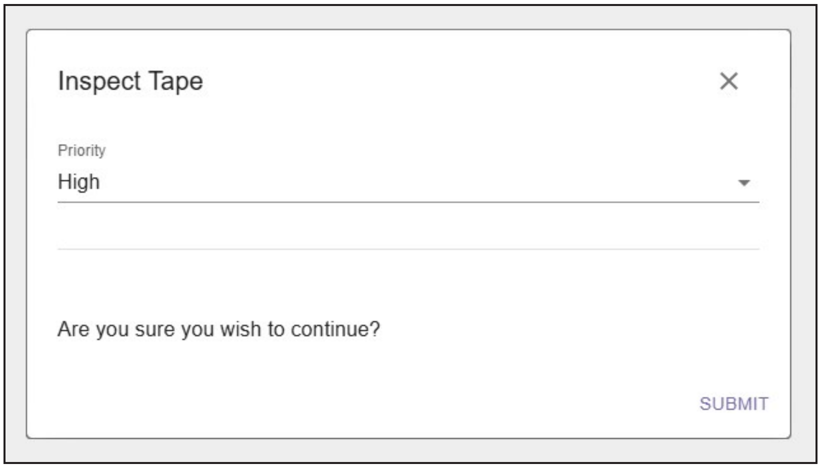


Barcode	State	Role	Write Protected	Bucket	Last Verified	Loaded In Drive
349995L5	Normal	Normal	No			
018823L6	Normal	Normal	No			
688136L6	Normal	Normal	No	bucket1		
688291L6	Normal	Normal	No	Spectra-BlackPearl-Backup-aic4u-02-cccb327ef9fb1888		
688292L6	Normal	Normal	No			

Rows per page: 5 1–5 of 19

Figure 220 The Tape Management screen - Inspect button.

2. Select the tape you want to inspect, and then select **Action > Inspect**. The Inspect Tape dialog box displays.



Inspect Tape

Priority: High

Are you sure you wish to continue?

Figure 221 The Inspect Tape window.

3. Use the **Priority** drop-down menu to select the inspection priority for the tape cartridge.
4. Click **Submit**.

MANAGE TAPES NOT IN INVENTORY

Additional functions of the Tape Management screen allow you to mark a tape missing from the tape library inventory as exported, and to delete lost or exported tapes.

Mark Tape as Exported

If you export a tape cartridge from the tape library inventory before exporting the tape from the BlackPearl Object Gateway, the tape displays as “Not in Inventory” on the Tape Management screen. If you cannot, or do not want to re-import the tape into the tape library, or you exported tapes from a multi-partition T50e or T120 library, use the instructions in this section to mark the tape as “Exported”.

To perform this operation, you must access the legacy user interface used in BlackPearl OS 5.8.x and earlier. Functionality this operation will be added to the new user interface in a later version of the BlackPearl OS.

1. Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with "/legacy". For example:

   https://*ipaddress*/legacy

2. Select **Status > Tape Management** from the menu bar. The Tape Management screen displays.
3. Select the tape with a status of “Not in Inventory” and select **Action > Mark Tape Not In Inventory As Exported**. A confirmation window displays.
4. In the confirmation window, click **Confirm**. The Tape Management screen updates the tape status to “Exported”.

Delete Lost or Exported Tape

If desired, you can delete tape cartridges that are lost or were exported from the library so that they no longer display on the Tape Management screen. This is useful if you exported tapes and do not plan to ever use them again with the BlackPearl Object Gateway.

Note: If you re-import a tape that you previously marked as deleted, the tape has a status of “Foreign”. See Import Tapes on page 313 for more information.

Use the instruction in this section to delete a lost or exported tape from the BlackPearl database.

To perform this operation, you must access the legacy user interface used in BlackPearl OS 5.8.x and earlier. Functionality this operation will be added to the new user interface in a later version of the BlackPearl OS.

1. Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with "/legacy". For example:

   https://*ipaddress*/legacy

2. Select **Status > Tape Management** from the menu bar. The Tape Management screen displays.
3. Select the tape with a status of “Not in Inventory” and select **Action > Delete Lost or Exported Tape**. A confirmation window displays.
4. In the confirmation window, click **Delete**. The Gateway deletes the tape from the database and it no longer displays on the Tape Management screen.

DATA MIGRATION

If desired, you can migrate data from one storage technology to another within a storage domain. This migration method is only available for permanent copies of data. The BlackPearl Object Gateway supports the following data migration:

- Tape to tape
- Disk to disk
- Disk to tape
- Tape to disk

The instructions below describe migrating data from a storage domain member using one tape technology to a storage domain member using a different tape technology. However, the process is similar for any of the above listed migration types. Use the instructions in this section to migrate data.

IMPORTANT This process assumes that all required data policies, data persistence rules, storage domains, and storage partitions are already configured on the BlackPearl Object Gateway.

To perform a data migration, you must access the legacy user interface used in BlackPearl OS 5.8.x and earlier.

1. Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with "/legacy". For example:

   https://*ipaddress*/legacy

2. If necessary, create a tape partition that contains the new media technology. This is the **target tape** partition.
3. If exporting the older generation of tapes is desired, in the BlackPearl user interface, select **Status > Tape Management** to navigate to the tape management screen and make a note of all tape barcodes associated with the storage domain.
4. Add the **target tape** partition to the storage domain as a storage domain member.
5. In the same storage domain, select the **source tape** storage domain member from which you want to migrate data and select **Action > Exclude**. The **source tape** storage domain member now displays “exclusion in progress”.
6. Select **Status > S3 Jobs** to examine the S3 Jobs screen and verify the IOM read and write operations are initiated. Wait until all operations complete.
7. Manually create a database backup. The data migration is now complete.
8. If desired, using the list of tapes you recorded in Step 2, export tapes from the **source tape** partition.

Chapter 13 - Importing and Exporting Tape Media

This chapter describes importing and exporting tape media in the BlackPearl ecosystem using a combination of the tape library front panel and BlackPearl user interface.

IMPORT TAPES

Use the instructions in this section to import tape media physically into a tape library partition and logically into the BlackPearl Object Gateway database. This may be done to add additional tape storage to your BlackPearl ecosystem, to access data on previously exported media, or to reclaim previously exported tape media.

Note: To import media that is being requested by a GET job, see Import Requested Tape Media on page 321.

Importing tape media into a BlackPearl Object Gateway is a multi-step processes and depends on the characteristics of the tape library. First, media is physically imported into the entry/exit pool in the tape library, if necessary. Second, the media in the entry/exit pool is moved by the BlackPearl Object Gateway to the storage pool. Lastly the media is moved to tape drives for inspection.

During the inspection, the BlackPearl Object Gateway determines if the media is new to the Gateway, previously exported by the Gateway, or is foreign to the Gateway.

- New media is added to the BlackPearl database, and is then automatically formatted by the BlackPearl Object Gateway before it is available for use.
- Media previously exported by the BlackPearl Object Gateway is automatically assigned to the bucket to which it was previously associated. The objects stored on the tape media are immediately available for retrieval.

CAUTION If the bucket associated with the imported tape media no longer exists, the tape cartridges are marked for formatting and reclaimed by the Gateway.

- Media marked as foreign then uses a second process to integrate it into the BlackPearl Object Gateway. The process is different for BlackPearl foreign, and LTFS foreign media.

  Note: Some applications that have written LTFS (such as SGL Flashnet) have not fully and accurately followed the LTFS format specifications.

  Note: The BlackPearl Object Gateway and Spectra Logic make a best effort to import foreign LTFS tapes. The BlackPearl support contract does not guarantee import of, nor cover any issues while importing foreign LTFS tapes. For the subset of LTFS tapes that cannot be imported, the Spectra Logic Professional Services team can help with the migration process.

IMPORTANT LTFS foreign tapes must have the physical write-protect tab set in the “write-protected” position before you import them into the BlackPearl Object Gateway. Tapes not set to write-protected are not imported.

Imported Tape Object Name Restrictions for Amazon S3 Replication

If you plan to migrate data from foreign tapes to an Amazon S3 target, Spectra BlackPearl, or the Spectra Vail application, the object names on the foreign tape media must conform to the naming convention restrictions of an Amazon S3 target.

The following characters are not compatible with Amazon S3 targets. Any object using one of these characters prevents the object from migrating to the Amazon S3 target.

- Backslash (\)
- Left curly bracket ({)
- Right curly bracket (})
- Caret (^)
- Percent character (%)
- Grave accent / back tick (`)
- Right square bracket (])
- Left square bracket ([)
- Quotation marks ("")
- Greater Than symbol (>)
- Less Than symbol (<)
- Tilde (~)
- Pound / hash tag character (#)
- Vertical bar / pipe (|)
- Non-printable ASCII characters (128–255 decimal characters)
- File names with multiple consecutive slash characters (//)

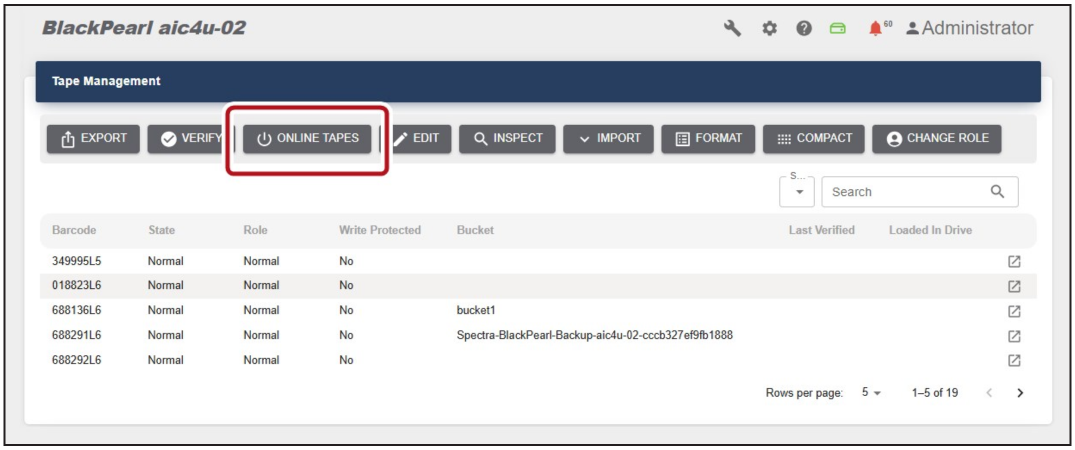
Import Tape Media

Use the instructions in this section to import tape media into the BlackPearl Object Gateway database.

1. Use the instructions in Importing Tape Media into a LumOS Library on page 323 or Importing Tape Media into a BlueScale Library on page 329 to import the requested tape media into the Entry/Exit pool of a Spectra Logic tape library associated with the BlackPearl Object Gateway.

Note: For instructions on importing tape media in to the I/O slots of an IBM tape library, see Related Information on page 21.

2. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**.



Barcode	State	Role	Write Protected	Bucket	Last Verified	Loaded In Drive
349995L5	Normal	Normal	No			
018823L6	Normal	Normal	No			
688136L6	Normal	Normal	No	bucket1		
688291L6	Normal	Normal	No	Spectra-BlackPearl-Backup-aic4u-02-cccb327ef9fb1888		
688292L6	Normal	Normal	No			

Rows per page: 5 1–5 of 19

Figure 222 The Tape Management screen - Tape Management pane - Online Tapes button.

3. Click **Online Tapes**. A confirmation window displays (not shown).

4. Click **Submit**. The tapes present in the Entry/Exit pool of a Spectra Logic tape library, or the I/O slots of an IBM tape library, are physically moved into the library storage pool and display on the Tape Management screen.

- If you imported new media, the tape cartridges are automatically formatted. During formatting, the BlackPearl Object Gateway creates two partitions on the tape media, and writes the corresponding index information to the tape cartridge MAM. Once the format is complete, the tape cartridges are available for use.

Note: For LTO-9 media, the first time a tape cartridge is loaded in a drive it goes through media optimization to create a referenced calibration which allows optimized data placement. This process can take up to two hours after which the tape is formatted. If you are using Spectra Logic Certified LTO-9 media, the tape cartridges have already gone through media optimization.

- If you imported media previously exported from the BlackPearl Object Gateway, it is automatically assigned to the bucket to which it was previously associated. The objects stored on the tape media are immediately available for retrieval.

CAUTION If the bucket associated with the imported tape media no longer exists, the tape cartridges are marked for formatting and reclaimed by the Gateway.

- To reclaim previously-used media for new data storage, see Format Managed BlackPearl Tapes on page 304.

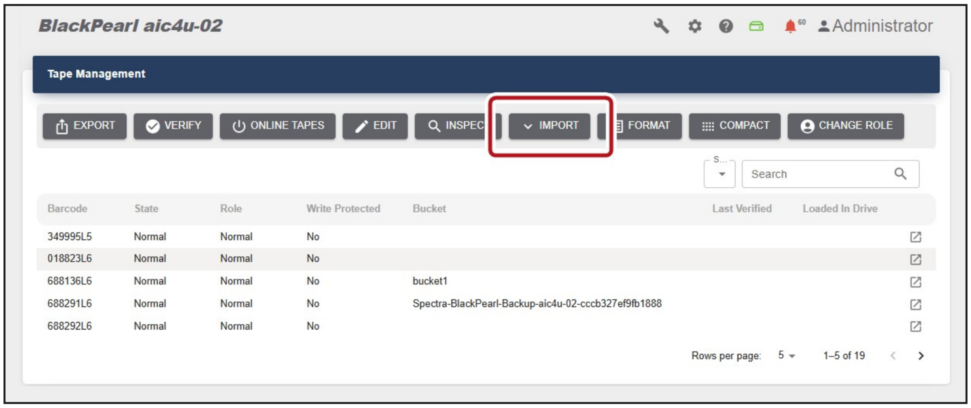
- If you imported foreign media, use the appropriate instructions below to complete the import process:
  - Import BlackPearl Foreign Tapes below
  - Import LTFS Foreign Tapes on page 318

Import BlackPearl Foreign Tapes

After importing tapes into a tape library and allowing the BlackPearl Object Gateway to online and inspect the tape, use the instructions in this section to complete the import of BlackPearl foreign tapes.

Note: If one or more buckets being imported does not already exist, the owner, data policy, and storage domain to use for any new buckets created during the import must be specified.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**.

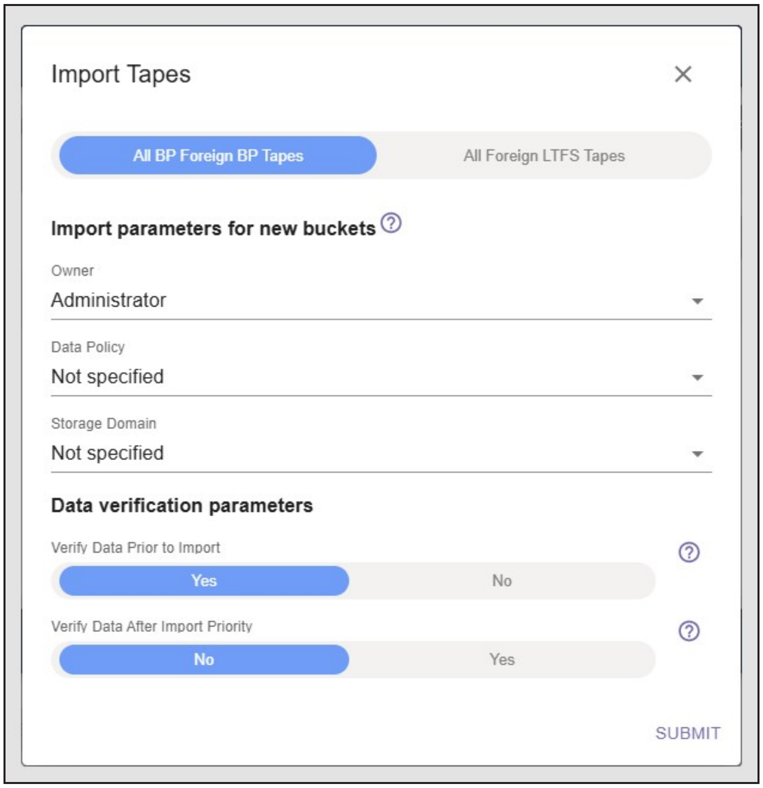


Barcode	State	Role	Write Protected	Bucket	Last Verified	Loaded In Drive
349995L5	Normal	Normal	No			
018823L6	Normal	Normal	No			
688136L6	Normal	Normal	No	bucket1		
688291L6	Normal	Normal	No	Spectra-BlackPearl-Backup-aic4u-02-cccb327ef9fb1888		
688292L6	Normal	Normal	No			

Rows per page: 5 1–5 of 19

Figure 223 The Tape Management screen - Tape Management pane - Import button.

2. Click **Import**. The Import Tapes dialog box displays.
3. Click **All Foreign BP Tapes**. The screen redisplays to show the options for importing foreign BlackPearl tapes.



Import Tapes

Import parameters for new buckets

Owner: Administrator

Data Policy: Not specified

Storage Domain: Not specified

Data verification parameters

Verify Data Prior to Import: Yes

Verify Data After Import Priority: No

Figure 224 The Import Tapes dialog box - Foreign BP.

4. Use the **Owner** drop-down menu to select a user from the list of previously created users to be the owner of all buckets on the foreign tape(s). The bucket owner has full permission to access the bucket, as well list, read, write, and delete permissions.
5. Use the **Data Policy** drop-down menu to select a data policy from the list of previously created data policies to use for all buckets on the foreign tape(s).
6. Use the **Storage Domain** drop-down menu to select a storage domain from the list of previously created storage domains to use for all buckets on the foreign tape(s).

Note: If you plan to import data to a storage domain, the storage media type must be added as a member to the selected storage domain

7. Use the **Verify Data Prior to Import** slider to select one of the following:
   - **Yes** - The system performs a data verification the data on the foreign tape(s) before importing. Data verification ensures the data on the tape is still viable.
   - **No** - The system does not verify the data before importing the tape media.

Notes: • Spectra Logic recommends selecting **Yes** to verify data prior to import when possible.

- Depending on the amount of data on a tape cartridge, verifying data prior to import may take a long time.

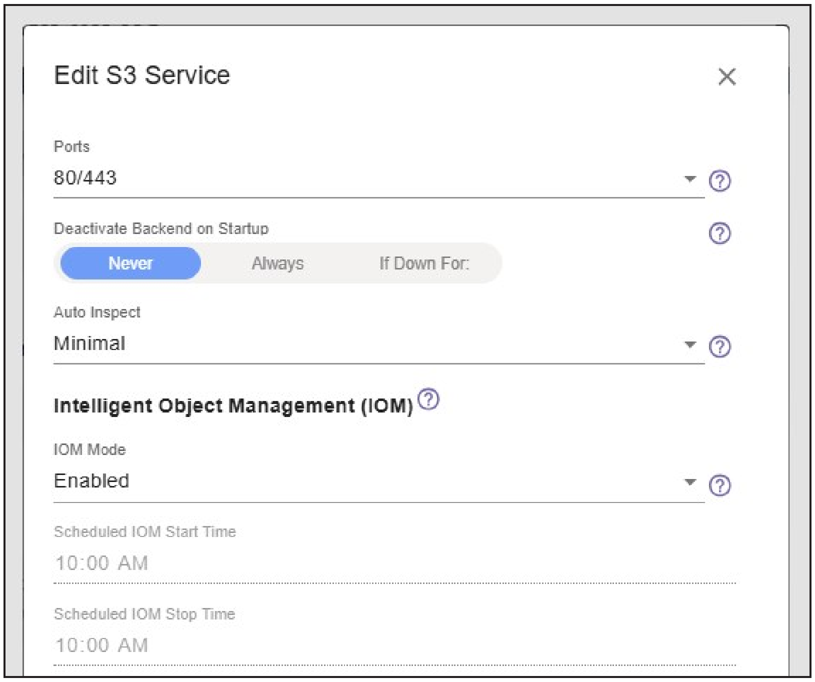
8. Use the **Verify Data After Import Priority** slider to select one of the following:
   - **Yes** - This setting makes imported foreign options available, and schedules a verify job with the selected priority at a later time. Data verification ensures the data on the tape is still viable.
   - **No** - Data is not verified after importing tape media.
9. Click **Submit**. The foreign tape(s) are imported into the BlackPearl Object Gateway.

Import LTFS Foreign Tapes

After importing tapes into a tape library and allowing the BlackPearl Object Gateway to online and inspect the tape, use the instructions in this section to complete the import of LTFS foreign tapes.

Note: Importing LTFS tape media must be done while the Intelligent Object Management (IOM) service is disabled. After you finish importing foreign LTFS tape media, you can re-enable IOM, which may trigger the creation of missing copies of files as required by the associated data policy. After the LTFS import completes, you can manually start an IOM migration.

1. **Disable** the IOM service.
   a. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
   b. In the S3 pane, click **Edit**. The Edit S3 Service screen displays.



Edit S3 Service

Ports: 80/443

Deactivate Backend on Startup: Never (selected) | Always | If Down For:

Auto Inspect: Minimal

Intelligent Object Management (IOM)

IOM Mode: Enabled

Scheduled IOM Start Time: 10:00 AM

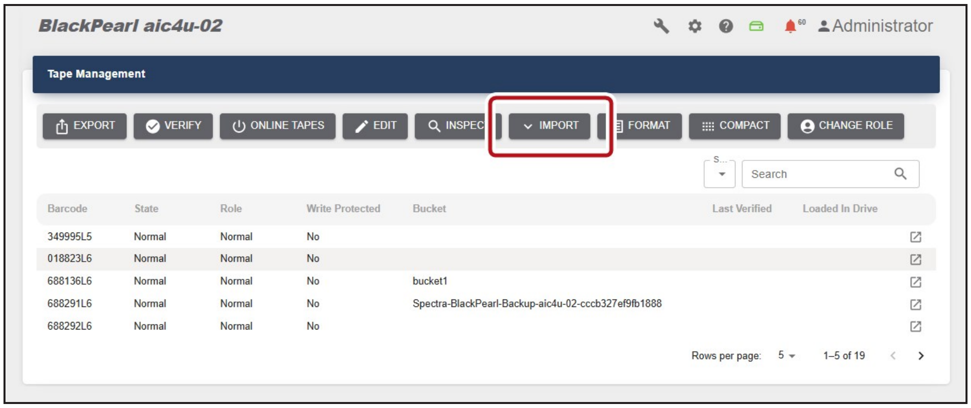
Scheduled IOM Stop Time: 10:00 AM

Figure 225 The Edit S3 Service dialog box - top half.

c. Use the **IOM Mode** drop-down menu to select **Disabled**.

d. Leave all other settings unchanged, and click **Save** (not shown).

2. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**. The Tape Management screen displays.



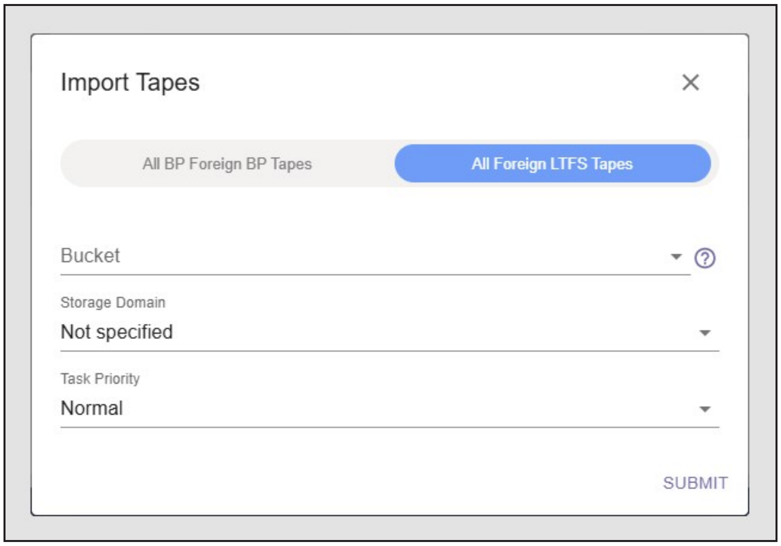
Barcode	State	Role	Write Protected	Bucket	Last Verified	Loaded In Drive
349995L5	Normal	Normal	No			
018823L6	Normal	Normal	No			
688136L6	Normal	Normal	No	bucket1		
688291L6	Normal	Normal	No	Spectra-BlackPearl-Backup-aic4u-02-cccb327ef9fb1888		
688292L6	Normal	Normal	No			

Rows per page: 5 1–5 of 19

Figure 226 The Tape Management screen - Tape Management pane - Import button.

3. Click **Import**. The Import Tapes dialog box displays.

4. Click **All Foreign LTFS Tapes**. The screen redisplays to show the options for importing foreign LTFS tapes.



Bucket

Storage Domain: Not specified

Task Priority: Normal

Figure 227 The Import Tapes dialog box - Foreign LTFS.

5. Use the **Bucket** drop-down list to select the bucket into which to import the LTFS foreign tape(s).

Note: The bucket must have a data policy including a persistence rule for a tape storage domain, or the import fails.

6. Use the **Storage Domain** drop-down list to specify into which storage domain to import the foreign LTFS tapes.

7. Use the **Task Priority** drop-down list to select the priority for the import process. The priority determines the job order and resources used.

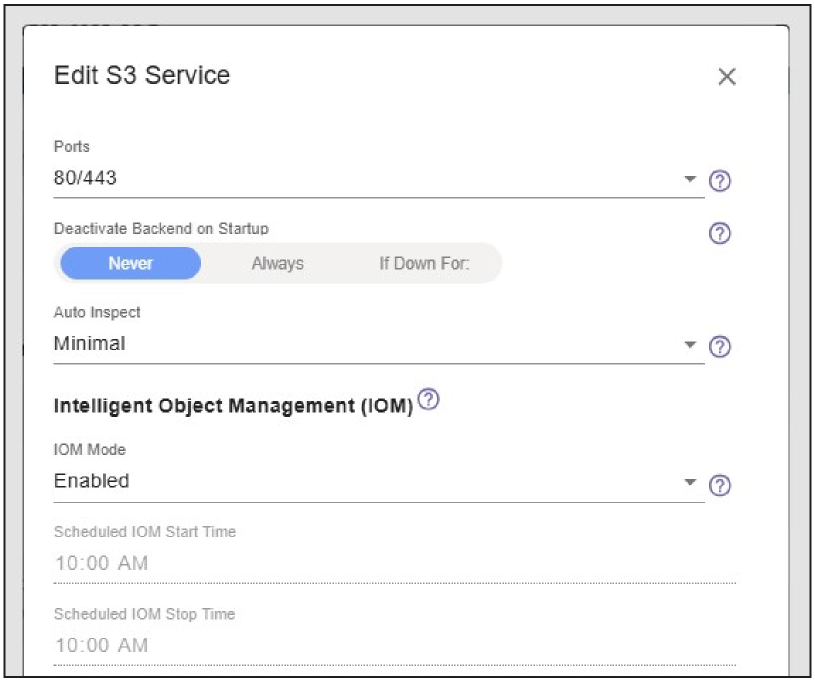
Note: Jobs with priority **Urgent** can use up all of the resources and prevent other jobs from making progress. Use this priority sparingly.

8. Click **Submit**. The foreign LTFS tape(s) are imported into the BlackPearl Object Gateway.

9. After the import completes, enable the IOM service.

   a. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.

   b. In the S3 pane, click **Edit**. The Edit S3 Service screen displays.



Edit S3 Service

Ports: 80/443

Deactivate Backend on Startup: Never | Always | If Down For:

Auto Inspect: Minimal

Intelligent Object Management (IOM)

IOM Mode: Enabled

Scheduled IOM Start Time: 10:00 AM

Scheduled IOM Stop Time: 10:00 AM

Figure 228 The Edit S3 Service dialog box - top half.

   c. Use the **IOM Mode** drop-down menu to select **Enabled**.

   d. Leave all other settings unchanged, and click **Save**.

IMPORTANT If you import additional LTFS foreign tapes at a later date, you must disable IOM again before the import operation, and enable it after the import is complete.

Import Requested Tape Media

Use the instructions in this section to import tape media into the BlackPearl Object Gateway in response to a GET job requesting data from a previously exported tape.

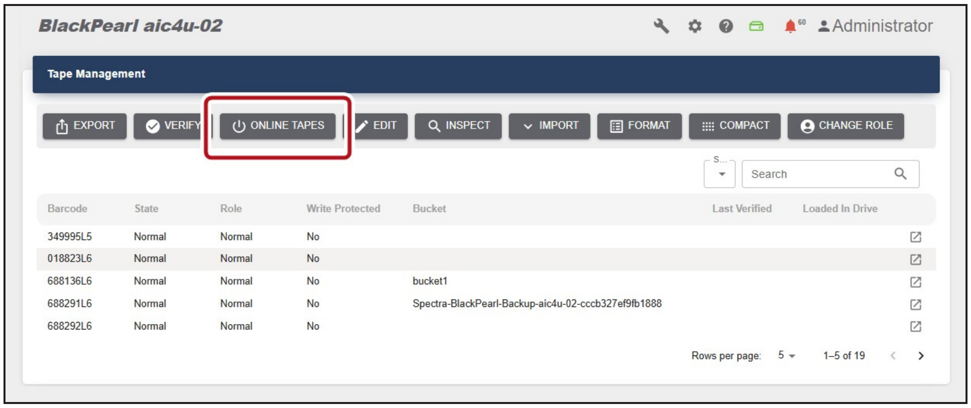
Note: This workflow is optimized for importing requested tape media. To import new or foreign tape media, see Import Tapes on page 313 .

1. Refer to system messages or emails sent to the administrator account for a list of tape barcode(s) to import. See Tape Media Import on page 405 for more information.
2. Use the instructions in Importing Tape Media into a BlueScale Library on page 329 or Importing Tape Media into a LumOS Library on page 323 to import the requested tape media into the Entry/Exit pool of a Spectra Logic tape library associated with the BlackPearl Object Gateway.

Notes:

- The tape media requested for import may need to be transported from an offsite location to the tape library.
- For instructions on importing tape media in to the I/O slots of an IBM tape library, see Related Information on page 21.

3. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**.



Barcode	State	Role	Write Protected	Bucket	Last Verified	Loaded In Drive
349995L5	Normal	Normal	No			
018823L6	Normal	Normal	No			
688136L6	Normal	Normal	No	bucket1		
688291L6	Normal	Normal	No	Spectra-BlackPearl-Backup-aic4u-02-cccb327ef9fb1888		
688292L6	Normal	Normal	No			

Rows per page: 5 1–5 of 19

Figure 229 The Tape Management screen - Tape Management pane - Online Tapes button.

4. Click **Online Tapes**. A confirmation window displays.

CAUTION If the bucket associated with the imported tape media no longer exists, the tape cartridges are marked for formatting and reclaimed by the BlackPearlObjectGateway.

5. Click **Submit**. The tapes present in the Entry/Exit pool of a Spectra Logic tape library, or the I/O slots of an IBM tape library, are physically moved into the library storage pool and display on the Tape Management screen.

   Once the media is online, it is automatically assigned to the bucket to which it was previously associated. The objects stored on the tape media are immediately available for retrieval by the pending GET job.

IMPORTING TAPE MEDIA INTO A LUMOS LIBRARY

Use the instructions in this section to import tape media into a TeraPack-based library running the LumOS operating system, including the Spectra Cube and TFinity Plus tape libraries. You must be physically at the tape library to import tape media.

Notes:

- These instructions describe importing tape media for data storage use. For instructions on importing cleaning media, see your *Library User Guide* for instructions.
- The instructions below assume your tape library was previously configured and is under the control of a BlackPearl Object Gateway.
- These instructions describe a simplified workflow for importing tape media for use by a BlackPearl Object Gateway. For advanced import options, see your *Library User Guide* for instructions.
- If you are importing new media, make sure you have prepared the tape cartridges for use in the tape library. See **Preparing Cartridges for Use** in your *Library User Guide* for more information.
- For instructions on importing tapes into a BlueScale operating system library, see Importing Tape Media into a BlueScale Library on page 329.
- For instructions on importing tapes into a Spectra Stack, Spectra SL3, T120, and T50e tape libraries, see your *Library User Guide*.

Log Into the User Interface

Use the following steps to log into the library using the front panel touch screen.

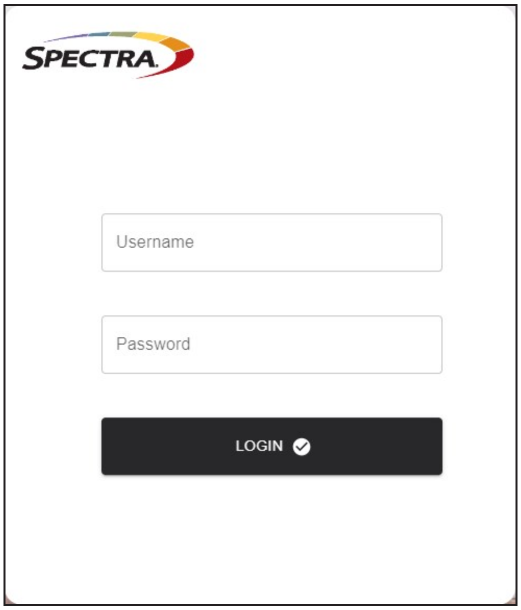
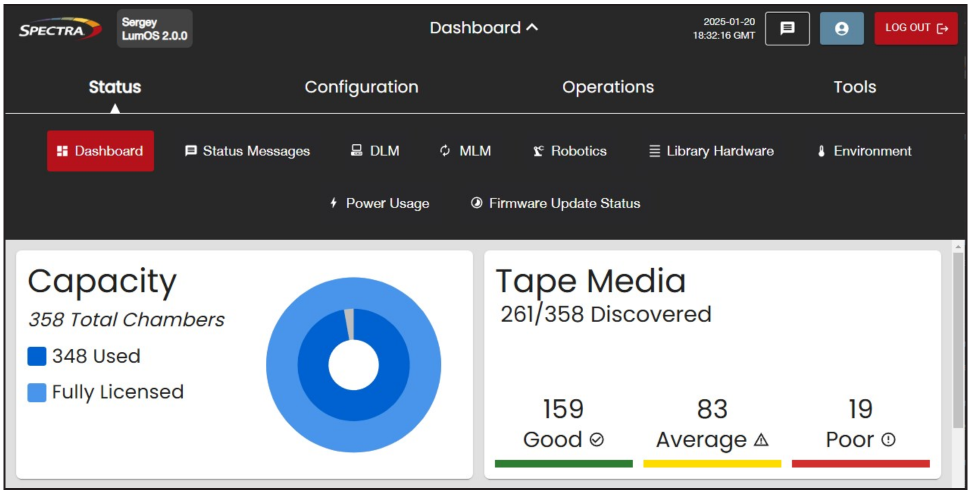


Figure 230 The LumOS Login screen.

1. Enter in the **Username** and **Password**.
2. Click **Login**. The user interface Dashboard screen displays.



Capacity

358 Total Chambers

🟦 348 Used

🟦 Fully Licensed

Tape Media

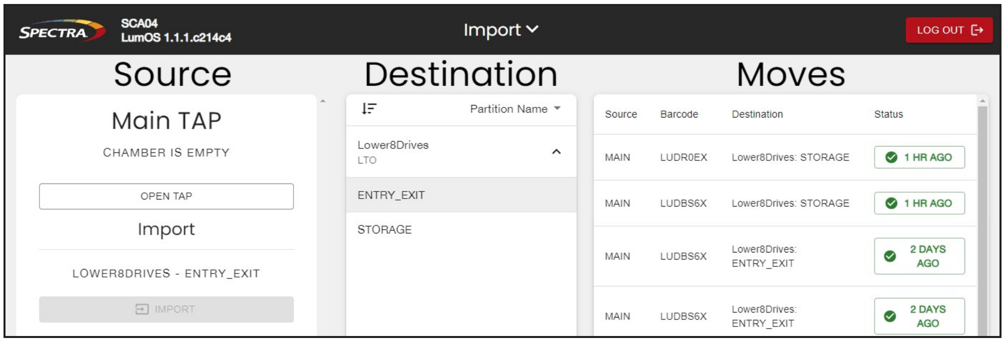
261/358 Discovered

159	83	19
Good	Average	Poor

Figure 231 The LumOS user interface Dashboard screen.

Import Magazines - Spectra Cube TAP

1. Select **Operations > Import Media** in the LumOS user interface.



Source	Barcode	Destination	Status
MAIN	LUDR0EX	Lower8Drives: STORAGE	1 HR AGO
MAIN	LUDBS6X	Lower8Drives: STORAGE	1 HR AGO
MAIN	LUDBS6X	Lower8Drives: ENTRY_EXIT	2 DAYS AGO
MAIN	LUDBS6X	Lower8Drives: ENTRY_EXIT	2 DAYS AGO

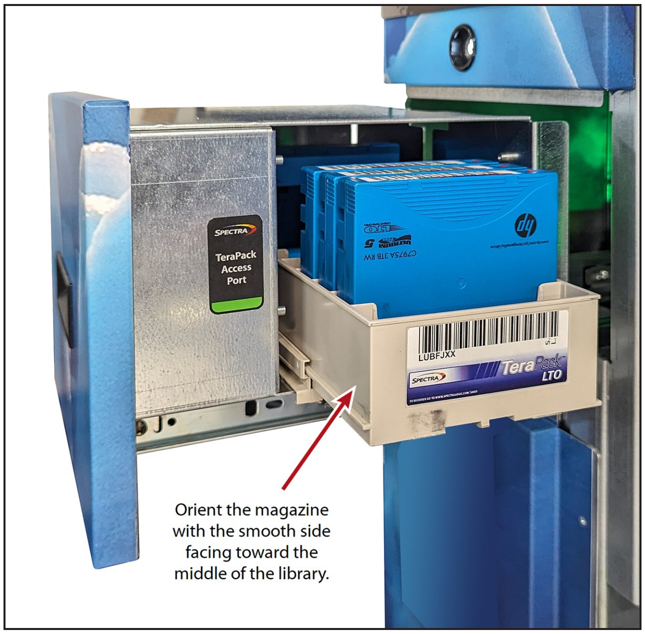
Figure 232 The LumOS Import screen.

1. Select the desired **Destination** partition and the **Entry/Exit** port of the partition.

IMPORTANT Only import tape cartridges into the Entry/Exit port. The BlackPearl Object Gateway controls the movement of tape media inside the library.

2. Click **Open TAP**.

3. Insert the magazine into the tray on the open TAP with the smooth side of the magazine facing towards the middle of the library as shown in Figure 233 on page 325.



Orient the magazine with the smooth side facing toward the middle of the library.

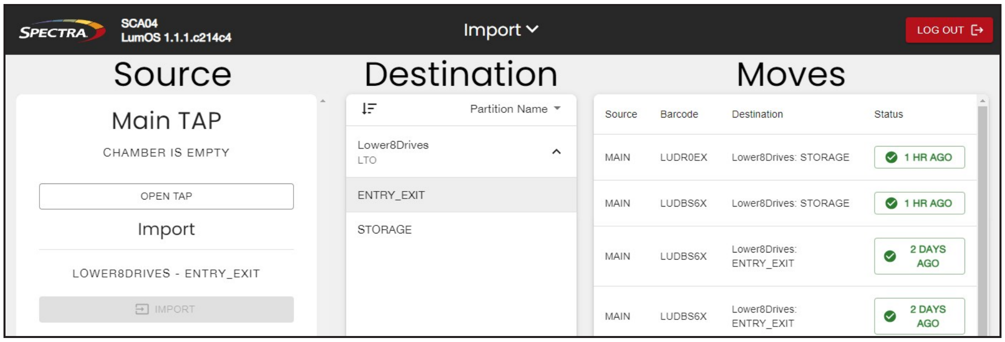
Figure 233 Insert a magazine into the TAP, making sure that it is correctly oriented.

4. After inserting the TeraPack magazine, physically push the TAP closed.

5. Click **Close TAP**, then click **Import** to start the import.

Import Magazines - TFinity Plus Center TAP

1. Select **Operations > Import Media** in the LumOS user interface.



Source	Barcode	Destination	Status
MAIN	LUDR0EX	Lower8Drives: STORAGE	✓ 1 HR AGO
MAIN	LUDBS6X	Lower8Drives: STORAGE	✓ 1 HR AGO
MAIN	LUDBS6X	Lower8Drives: ENTRY_EXIT	✓ 2 DAYS AGO
MAIN	LUDBS6X	Lower8Drives: ENTRY_EXIT	✓ 2 DAYS AGO

Figure 234 The LumOS Import screen.

1. Select the desired **Destination** partition and the **Entry/Exit** port of the partition.

IMPORTANT Only import tape cartridges into the Entry/Exit port. The BlackPearl Object Gateway controls the movement of tape media inside the library.

2. Click **Open TAP**.
3. Insert a magazine into the tray on the open TAP, making sure that it is oriented with the textured surface on each side toward the outside of the library, as shown in Figure 235 on page 326.

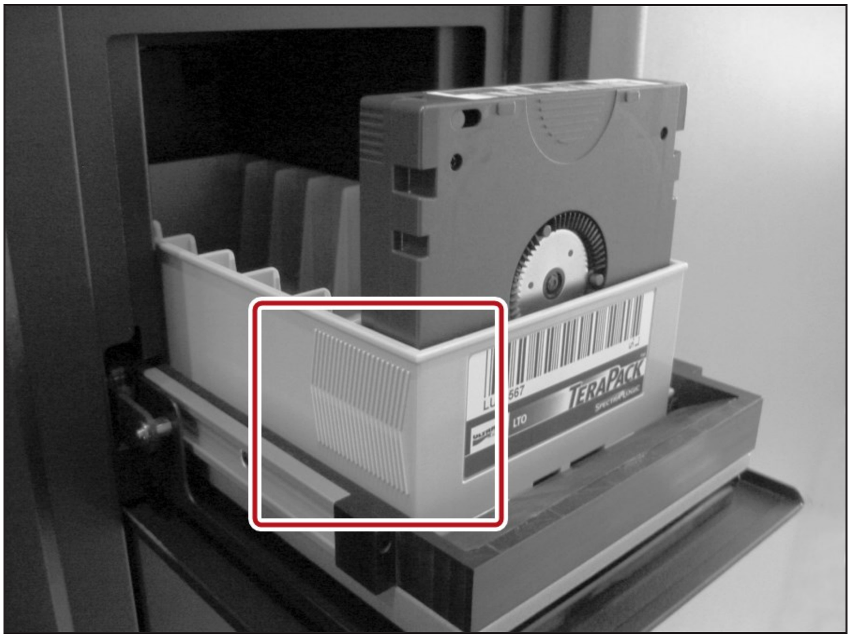
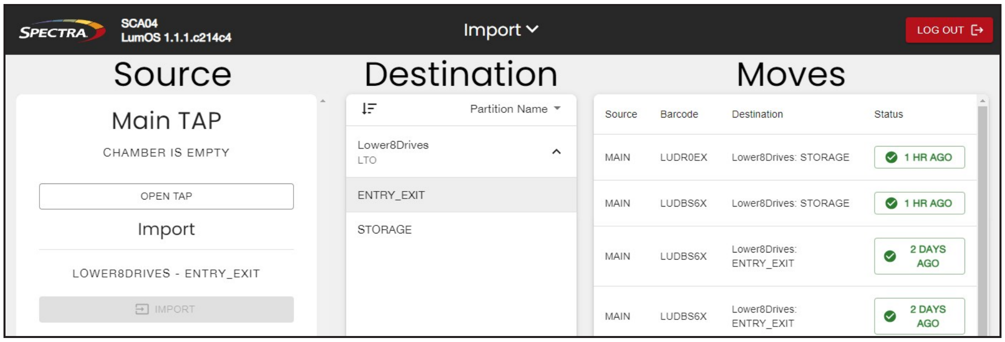


Figure 235 Insert a magazine into the TAP, making sure that it is correctly oriented.

4. Click **Close TAP**, then click **Import** to start the import.

Import Magazines - TFinity Plus Bulk TAP

1. Select **Operations > Import Media** in the LumOS user interface.



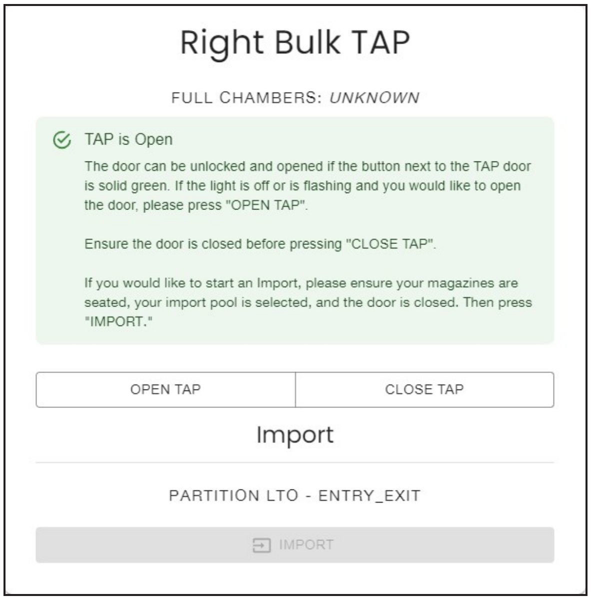
Source	Barcode	Destination	Status
MAIN	LUDR0EX	Lower8Drives: STORAGE	1 HR AGO
MAIN	LUDBS6X	Lower8Drives: STORAGE	1 HR AGO
MAIN	LUDBS6X	Lower8Drives: ENTRY_EXIT	2 DAYS AGO
MAIN	LUDBS6X	Lower8Drives: ENTRY_EXIT	2 DAYS AGO

Figure 236 The LumOS Import screen.

1. Select the desired **Destination** partition and the **Entry/Exit** port of the partition.

IMPORTANT Only import tape cartridges into the Entry/Exit port. The BlackPearl Object Gateway controls the movement of tape media inside the library.

2. Open a bulk TAP door by clicking **Open TAP** to unlock the door.



TAP is Open

The door can be unlocked and opened if the button next to the TAP door is solid green. If the light is off or is flashing and you would like to open the door, please press "OPEN TAP".

Ensure the door is closed before pressing "CLOSE TAP".

If you would like to start an Import, please ensure your magazines are seated, your import pool is selected, and the door is closed. Then press "IMPORT."

Figure 237 The Bulk TAP window.

3. When the door release button LED is solid green, press the button to open the bulk TAP door.

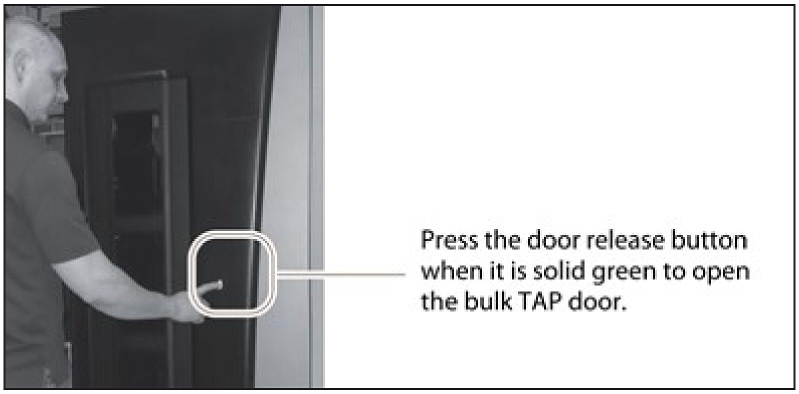

Press the door release button when it is solid green to open the bulk TAP door.

Figure 238 Press the door release button to open the door.

4. Insert up to 14 TeraPack magazines onto the shelves in the bulk TAP carousel.

CAUTION When you place a magazine in the bulk TAP, make sure that the textured surface (**1**) on each side of the magazine is toward the inside of the library and that the guides on the sides of the magazine fit into the media guides on the media shelf (**2**), as shown in Figure 238 on page 328. Loading the magazines incorrectly or at an angle can result in damage to the carousel or the robotics.

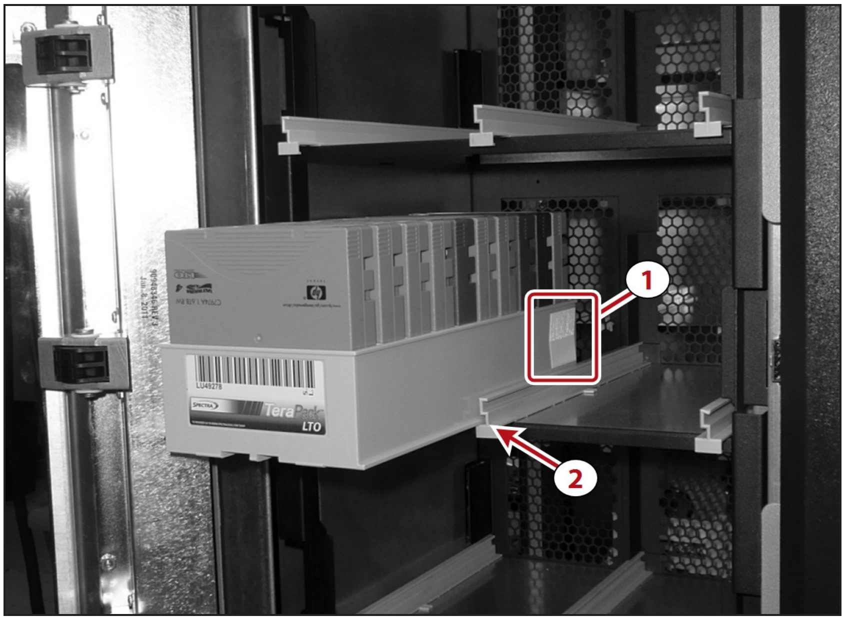


Figure 239 Insert the magazine into the bulk TAP carousel, making sure that it is correctly positioned.

5. Close the bulk TAP door firmly by pressing at the top and bottom. An audible click indicates that the door is latched closed.

6. In the user interface, click **Close TAP**, then click **Import**.

Importing Tape Media into a BlueScale Library

Use the instructions in this section to import tape media into a TeraPack-based library running the BlueScale operating system, including the Spectra TFinity, T950, T680, T380, and T200 tape libraries. You must be physically at the tape library to import tape media.

Notes:

- These instructions describe importing tape media for data storage use. For instructions on importing cleaning media, see your *Library User Guide* for instructions.
- The instructions below assume your tape library was previously configured and is under the control of a BlackPearl Object Gateway.
- These instructions describe a simplified workflow for importing tape media for use by a BlackPearl Object Gateway. For advanced import options, see your *Library User Guide* for instructions.
- If you are importing new media, make sure you have prepared the tape cartridges for use in the tape library. See **Preparing Cartridges for Use** in your *Library User Guide* for more information.
- For instructions on importing tapes into a LumOS library, see Importing Tape Media into a LumOS Library on page 323
- For instructions on importing tapes into a Spectra Stack, Spectra SL3, T120, and T50e tape libraries, see your *Library User Guide*.

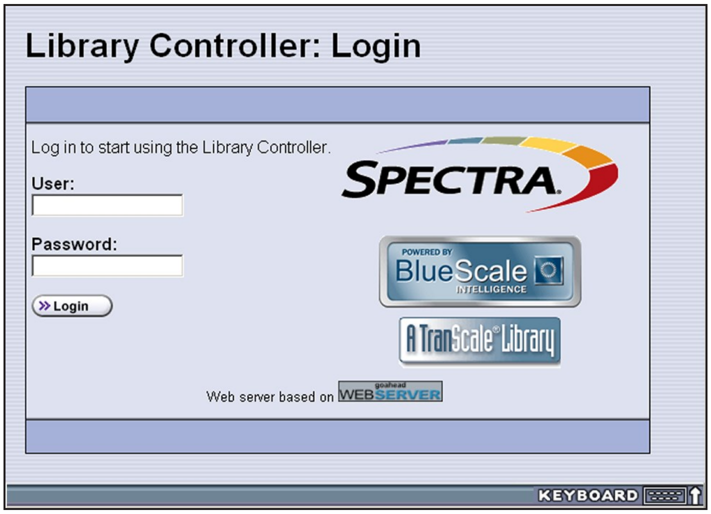
Log Into the User Interface

Use the following steps to log into the library using the front panel touch screen.

1. Select the **User** text box. A cursor appears in the box.

Note: When using the touch screen on the library operator panel, touch the keyboard icon on the Login screen to activate the soft keyboard on the library's touch screen. Use the stylus or your finger to select fields and to type information using the soft keyboard.

Touching the keyboard icon again closes the soft keyboard.



Library Controller: Login

Log in to start using the Library Controller.

User:

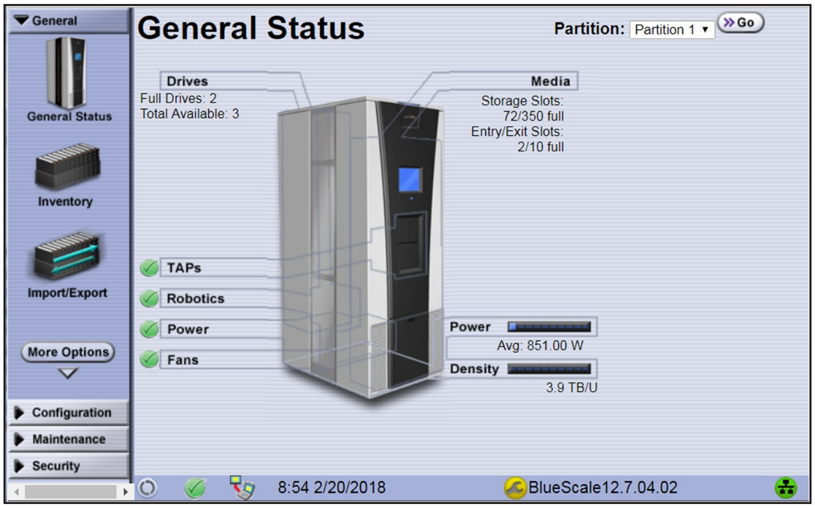
Password:

» Login
SPECTRA
POWERED BY BlueScale INTELLIGENCE
A TranScale Library
Web server based on goahead WEBSERVER
KEYBOARD

Figure 240 Log into the library using the Library Controller: Login screen.

2. Type your user name (**su** is the default user name for a superuser).
3. Type your password in the **Password** text box. By default, passwords are not configured for the three default users.

4. Click **Login**. The library’s General Status screen displays.



General Status

Partition: Partition 1

Drives
Full Drives: 2
Total Available: 3

Media
Storage Slots: 72/350 full
Entry/Exit Slots: 2/10 full

Power
Avg: 851.00 W

Density
3.9 TB/U

8:54 2/20/2018

BlueScale12.7.04.02

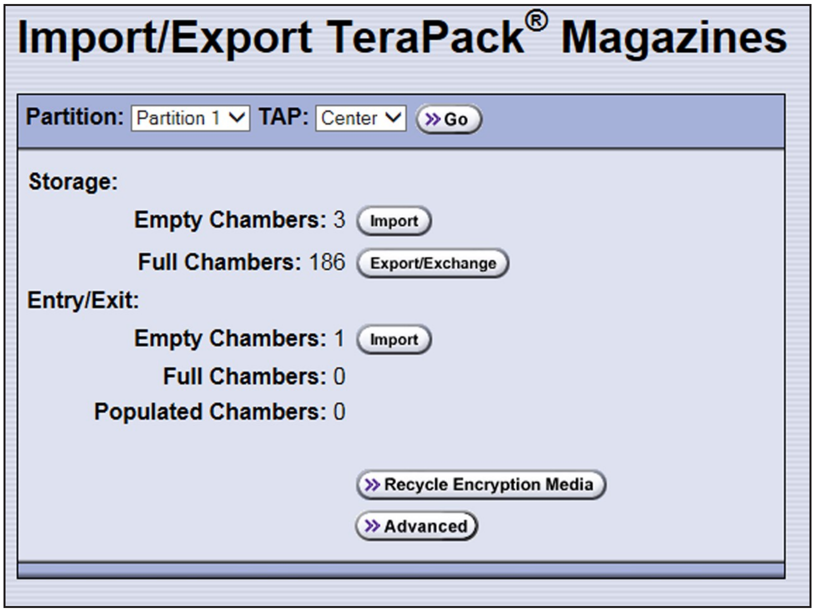
Figure 241 The BlueScale user interface General Status screen for a Spectra TeraPack-based tape library.

Import the Magazines

1. From the toolbar menu, select **General > Import/Export**. The Import/Export TeraPack Magazines screen displays.
2. Use the **Partition** drop-down menu to select the partition into which you want to import tapes, and the **TAP** drop-down menu to select the TAP (TeraPack Access Port) you want to use to import tapes.

Select this TAP...	If you want to use...
Center	The TAP located in the main frame. • TFinity, T950, and T680 libraries feature a dual chamber TAP. • T380 and T200 libraries feature a single chamber TAP.
Left	The bulk TAP located on the left end of the library, if present.
Right	The bulk TAP located in the bulk TAP service frame on the right end of the library, if present.
LeftAndRight	Both the bulk TAP located in the bulk TAP service frame on the left end of the library, and the bulk TAP located in the bulk TAP service frame on the right end of the library.

3. Click **Go**. The Import/Export TeraPack Magazines screen refreshes to show the current status of the chambers assigned to the selected partition.



Import/Export TeraPack® Magazines

Partition: Partition 1 TAP: Center

Storage:

Empty Chambers: 3

Full Chambers: 186

Entry/Exit:

Empty Chambers: 1

Full Chambers: 0

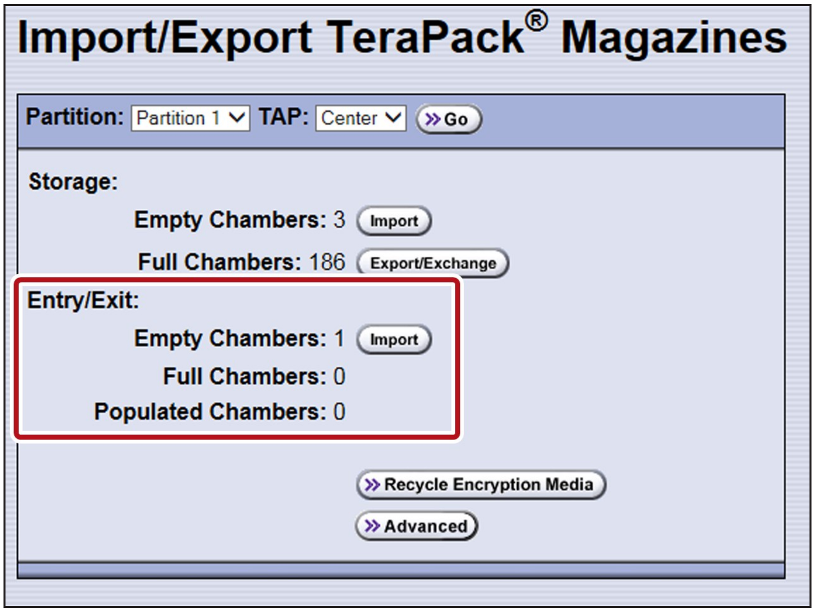
Populated Chambers: 0

Figure 242 Select the partition and the TAP.

4. Under Entry/Exit, click the **Import** button.

IMPORTANT Only import tape cartridges into the Entry/Exit port. The BlackPearl Object Gateway controls the movement of tape media inside the library.

Note: If there are no empty chambers in the selected pool, the **Import** button is not present. Export one or more magazines to make space for the new magazines.



Import/Export TeraPack® Magazines

Partition: Partition 1 TAP: Center

Storage:

Empty Chambers: 3

Full Chambers: 186

Entry/Exit:

Empty Chambers: 1

Full Chambers: 0

Populated Chambers: 0

Figure 243 Click **Import** for the Entry/Exit pool.

5. The next steps in the import process depend on which TAP you selected:
   - Center TAP in a TFinity or T950 Library below
   - Center TAP in a T680, T380, or T200 Library on the next page
   - Bulk TAP on page 337

Center TAP in a TFinity or T950 Library

The top TAP door opens and a Feedback Required screen displays instructing you to place a TeraPack in the TAP.

a. Insert a magazine into the tray on the open TAP, making sure that it is oriented with the textured surface on each side toward the outside of the library, as shown in Step Figure 244 on page 333.

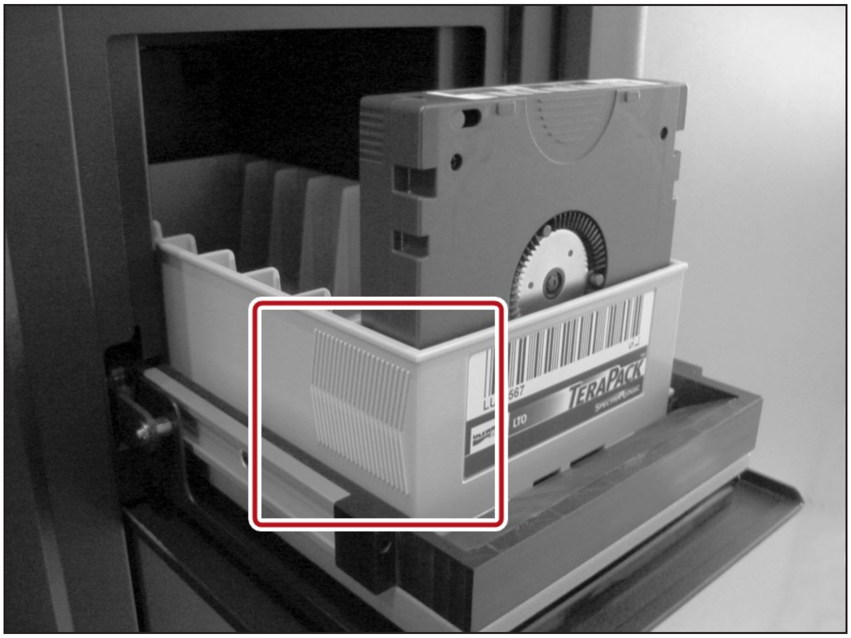


Figure 244 Insert a magazine into the TAP, making sure that it is correctly oriented.

b. Return to the operator panel and select the appropriate option on the Feedback Required screen.

Select...	If...
Continue	You plan to import another magazine after the one currently in the TAP. The import process continues as follows: **1.** The TAP door closes automatically. The TeraPorter (robot) retrieves the magazine from the TAP and moves it to a chamber in the entry/exit pool. **2.** If there are still empty chambers available in the entry/exit pool, the second TAP door opens, ready to accept the next magazine. The TAP doors alternate as you continue to import magazines. **3.** The import process continues as long as there are empty chambers available or until you click **Stop Importing** on the Feedback Required screen. Continue to insert magazines into the TAP, clicking **Continue** after each one. When there are no empty chambers remaining in the entry/exit pool, the process stops automatically and the Import/Export TeraPack Magazines screen displays.
Stop Importing	The magazine you placed in the TAP is the last one you want to import.

Note: If you wait more than 10 minutes to respond, the library times out and displays a message on the operator panel. The TAP door is left open.

Center TAP in a T680, T380, or T200 Library

The top TAP door (T680) or single TAP door (T380 and T200) opens and a Feedback Required screen displays instructing you to place a TeraPack magazine in the TAP.

a. Insert a magazine into the tray on the open TAP, making sure that it is oriented with the textured surface on each side toward the outside of the library, as shown in .

The alignment guides on each side of the media pack slide easily into the grooves on either side of the TAP opening. If the media pack does not slide into place easily, remove and reinsert it.

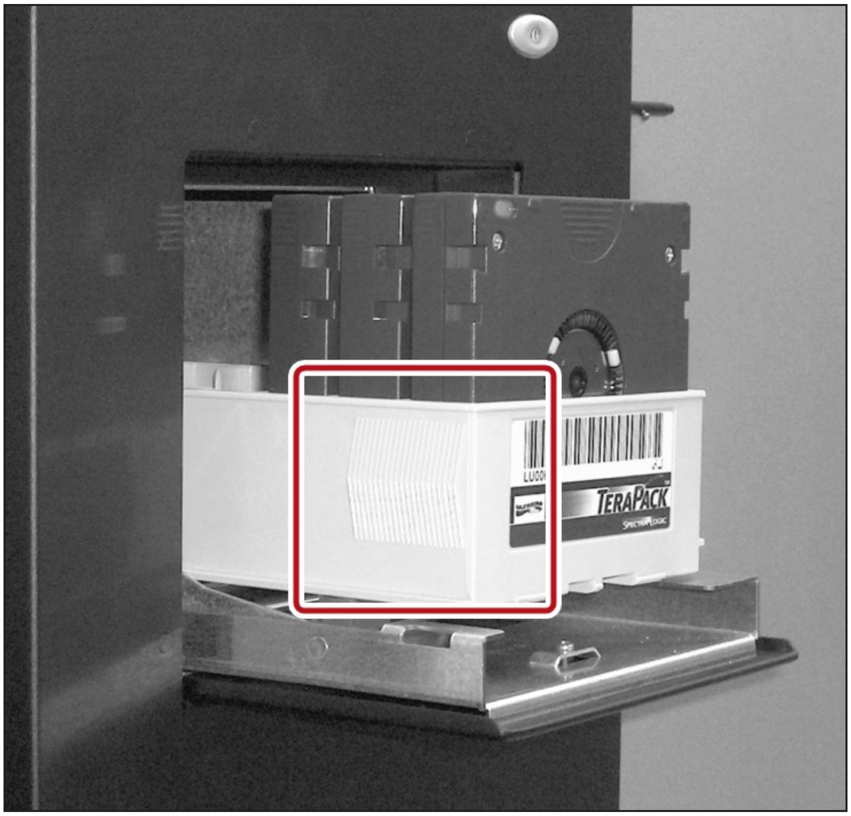


Figure 245 Insert a magazine into the TAP, making sure that it is correctly oriented.

b. Gently raise the TAP door and press it firmly into the latch for approximately one second.

Note: Close the TAP door firmly, but do not use excessive force.

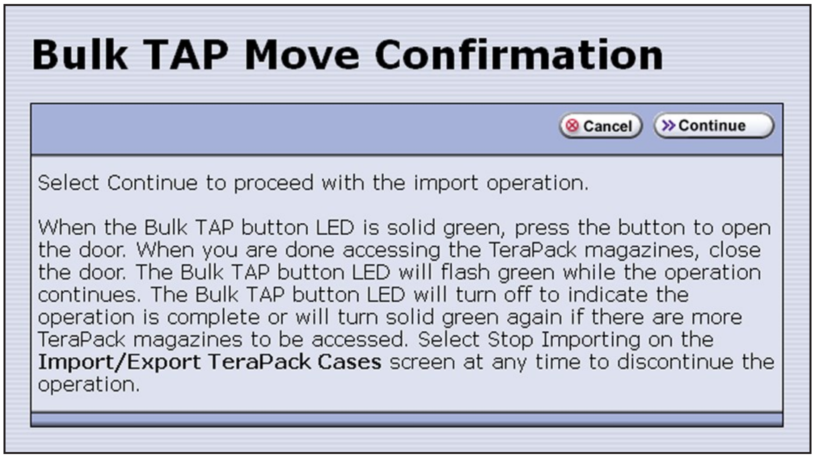
c. Return to the operator panel and select the appropriate option on the Feedback Required screen.

Select...	If...
Continue	You plan to import another magazine after the one currently in the TAP. The import process continues as follows: **1.** After the door is closed, the TeraPorter (robot) retrieves the magazine from the TAP and moves it to a chamber in the entry/exit pool. **2.** If there are still empty chambers available in the entry/exit pool, the TAP door opens, ready to accept the next magazine. **Note:** In a T680 library, the TAP doors alternate as you continue to import magazines. **3.** The import process continues as long as there are empty chambers available or until you click **Stop Importing** on the Feedback Required screen. Continue to insert magazines into the TAP, clicking **Continue** after each one. When there are no empty chambers remaining in the entry/exit pool, the process stops automatically and the Import/Export TeraPack Magazines screen displays.
Stop Importing	The magazine you placed in the TAP is the last one you want to import.

Note: If you wait more than 10 minutes to respond, the library times out and displays a message on the operator panel. The TAP door is left open.

Bulk TAP

If you selected the Left, Right, or LeftAndRight TAP - The Bulk TAP Move Confirmation screen displays a confirmation message with instructions for performing the import operation.



Bulk TAP Move Confirmation

Select Continue to proceed with the import operation.

When the Bulk TAP button LED is solid green, press the button to open the door. When you are done accessing the TeraPack magazines, close the door. The Bulk TAP button LED will flash green while the operation continues. The Bulk TAP button LED will turn off to indicate the operation is complete or will turn solid green again if there are more TeraPack magazines to be accessed. Select Stop Importing on the **Import/Export TeraPack Cases** screen at any time to discontinue the operation.

Figure 246 Read the instructions on the Bulk TAP Move Confirmation screen, then click **Continue**.

a. Click **Continue**. The bulk TAP carousel rotates to face the outside of the library.

Note: If you selected **LeftAndRight** TAP and there are fewer than 14 empty chambers available in the destination, only the left bulk TAP rotates to face outward. If you select **LeftAndRight** TAP and more than 14 chambers are available, both bulk TAPs rotate outward.

IMPORTANT If the carousel contains magazines from a previous export or import operation, the library will alert you to remove those magazines. When the door release button LED is solid green, press it to open the bulk TAP door. Remove the magazines, close the door firmly by pressing at the top and bottom, and click **Continue** to restart the import process.

b. When the door release button LED is solid green, press the button to open the bulk TAP door.

Note: If you wait more than 10 minutes to open the door, the LED turns off and the carousel rotates to face the interior of the library. The library considers the import operation complete.

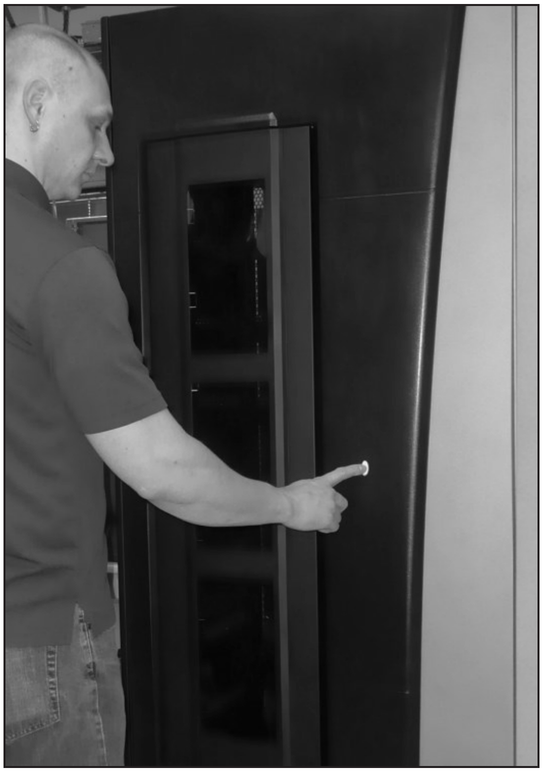


Figure 247 Press the door release button to open the door.

c. Slide one or more TeraPack magazines onto the shelves in the bulk TAP carousel.

CAUTION When you place a magazine in the bulk TAP, make sure that the textured surface (**1**) on each side of the magazine is toward the inside of the library and that the guides on the sides of the magazine fit into the media guides on the media shelf (**2**), as shown in Figure 247 on page 338. Loading the magazines incorrectly or at an angle can result in damage to the carousel or the robotics.

Notes:

- The correct orientation of the magazines when inserted into the left or right TAP is opposite that for the center TAP.
- You can insert up to 14 magazines at a time.

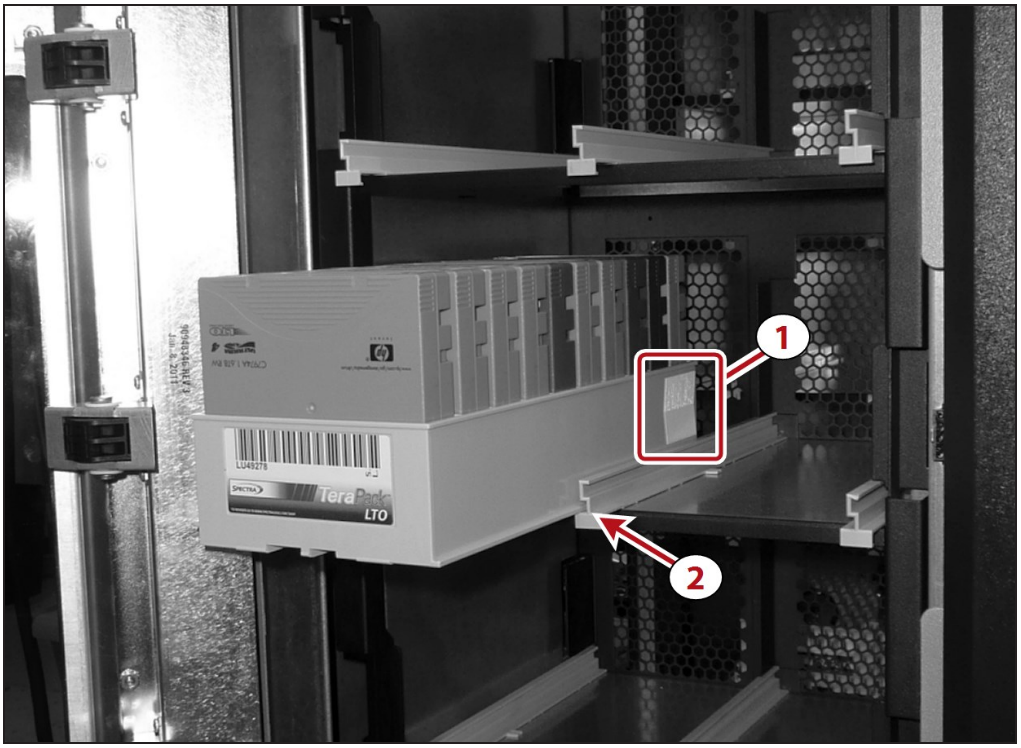
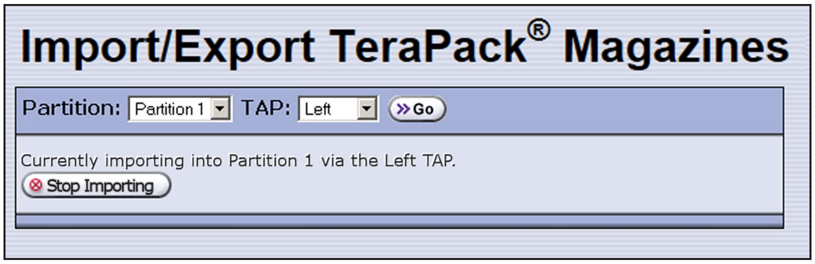


Figure 248 Insert the magazine into the bulk TAP carousel, making sure that it is correctly positioned.

d. Close the bulk TAP door firmly by pressing at the top and bottom. An audible click indicates that the door is latched closed. The carousel rotates the magazines to the interior of the library and the TeraPorter begins moving the magazines to open chambers in the entry/exit pool. The Import/Export TeraPack Magazines screen refreshes to show that the moves are in progress.

Notes:

- If you fail to close the door within 10 minutes, the import operation times out.
- If you selected **LeftAndRight** TAP, the library starts processing moves as soon as you close one bulk TAP door. The library completes processing moves from the first bulk TAP before starting to process moves for the second bulk TAP.
- If you want to terminate the import operation before it completes, click **Stop Importing** . If there are still magazines in the bulk TAP, you will be instructed to remove them before the next import or export operation.



Currently importing into Partition 1 via the Left TAP.

Figure 249 The Import/Export TeraPack Magazines screen shows that the import process is underway.

e. When a TeraPorter finishes moving all of the magazines out of a bulk TAP, the carousel rotates to face the outside of the library and the door release button LED turns solid green again, indicating that it is ready to for you to load additional magazines. The process described in this section continues until one of the following occurs:

- **You insert fewer than 14 magazines in a bulk TAP —** When the library detects that the bulk TAP door was closed with fewer than 14 magazines inserted, the magazines are imported, if applicable the other bulk TAP is checked and magazines imported, and the operation ends.
- **There are no more empty chambers in the entry/exit pool** — The operation ends when the destination is full. If the entry/exit pool did not contain enough empty chambers to accommodate all of the magazines that you loaded into the carousel, the extra magazines are left in the bulk TAP.
- **You click Stop Importing** — When you click **Stop Importing** the import operation terminates. If there are still magazines in the bulk TAP, you will be instructed to remove them before the next import or export operation.

EXPORT TAPES

Tape media and the data they contain can be removed from the BlackPearl Object Gateway by exporting them. Once tapes are exported from the Gateway, they are exported physically from the tape library, and can be imported into another tape library associated with a BlackPearl Object Gateway, or stored off site.

If you use a data policy configured to persist multiple copies of data on tape media, it is helpful to keep one copy of data in your tape library while exporting the second copy. This allows the data to be stored offsite for data protection, while still allowing access to the other copy of the data in the tape library.

IMPORTANT

Do not use the Spectra Logic or supported tape library front panel or RLC connection to move tape cartridges while the tape library is under the control of the BlackPearl Object Gateway.

If you suspect that a tape was exported from the library without being exported from the BlackPearl Object Gatewayusing the BlackPearl user interface, see Tape Media Export on page 406

Notes:

- The BlackPearl Object Gateway Administrator **must** be configured to receive emails with both Informational and Warning message severity to be notified when tape media is exported. This allows the user to retrieve the tape media when it is exported. Do not leave the media in the library Entry/Exit port for long periods of time. Tape media left in the Entry/Exit port may interfere with other automatic tape export operations, or import of new or requested tape media.
- If you plan to export tapes to be used in a non-BlackPearl environment, see Special Considerations for Ejecting Tapes for important information on how to configure your BlackPearl Object Gateway so that tapes written by the Gateway are readable in a non-BlackPearl environment.
- Always store tapes exported from the Spectra tape library in TeraPack magazines. When tapes are outside the library, Spectra Logic recommends storing them in magazines with dust covers. See “Storing Cartridges” in your Spectra Logic *Related Information* for more information.
- Spectra T50e and T120 libraries must be configured in Standard Entry/Exit Port mode in order for the BlackPearl Object Gateway to automatically export tapes. If your library has only one partition, it is already in Standard Entry/Exit Port mode.

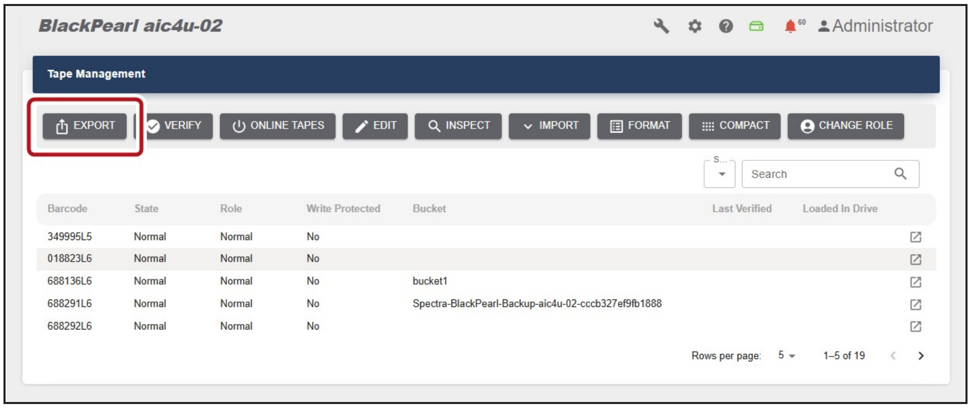
If there is more than one partition, including a cleaning partition, in order for the BlackPearl Object Gateway to automatically export tapes you must delete partitions until only one remains, and then edit the remaining partition to use Standard mode. See your Spectra Logic *Related Information* for more information on partition management. To manually export tapes from a T50e or T120 library with multiple partitions, see Export Tapes from a T50e or T120 Library with Multiple Partitions on page 344.

Export One or More Tapes

Exporting a tape moves that tape to the Entry/Exit pool of a Spectra Logic tape library, or the I/O slots of an IBM tape library. Any objects on the exported tape are inaccessible until the tape is re-imported into a storage pool.

Tapes are exported one at a time using the BlackPearl user interface. Use the following instructions to export a tape from the BlackPearl Object Gateway.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**.

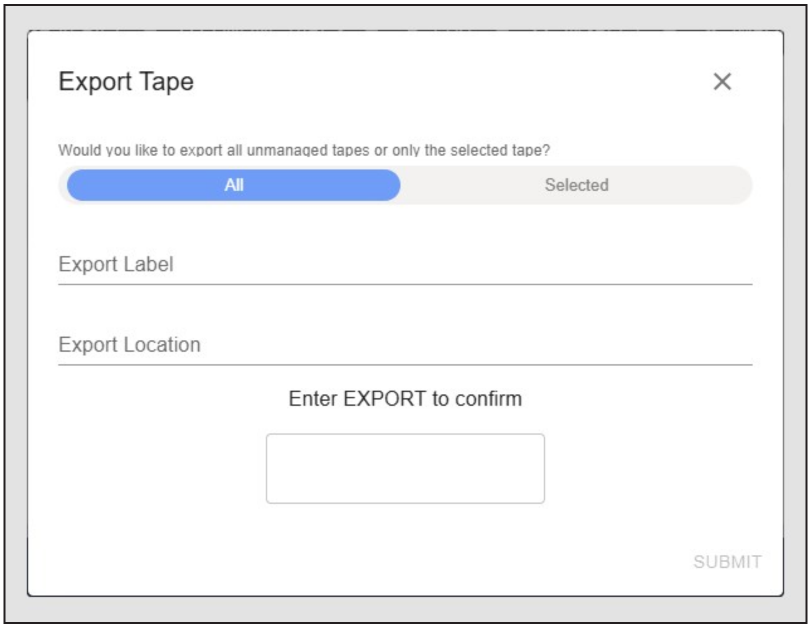


Barcode	State	Role	Write Protected	Bucket	Last Verified	Loaded In Drive
349995L5	Normal	Normal	No			
018823L6	Normal	Normal	No			
688136L6	Normal	Normal	No	bucket1		
688291L6	Normal	Normal	No	Spectra-BlackPearl-Backup-aic4u-02-cccb327ef9fb1888		
688292L6	Normal	Normal	No			

Rows per page: 5 1–5 of 19

Figure 250 The Tape Management screen - Tape Management pane - Export button.

2. Select one of the tapes you want to export and click **Export**. The Export Tape dialog box displays.



Export Tape

Would you like to export all unmanaged tapes or only the selected tape?

Enter EXPORT to confirm

Figure 251 The Export Tape dialog box.

3. Use the slider to select one of the following:
   - **All**- The system exports all unmanaged tapes.
   - **Selected** - The system exports the selected tape.
4. If desired, enter information in the **Export Label** and **Export Location** fields. This information is stored in the BlackPearl database and is visible when re-importing the tape into a BlackPearl Object Gateway. You are not required to enter this information.

Note: If you previously entered information in these fields when editing the tape, the previously entered information displays.

5. In the entry field, enter `EXPORT` to confirm the operation.
6. Click **Submit**. The tape is marked as exported in the BlackPearl Object Gateway database, and moved to the Entry/Exit pool of a Spectra Logic tape library, or the I/O slots of an IBM tape library.
7. Repeat Step 2 through Step 6 as necessary to export additional tapes.
8. Once you have exported the desired tape(s) in the BlackPearl user interface, use the instructions in Export Tapes on page 341 to export the requested tape media into the Entry/Exit pool of a Spectra Logic tape library associated with the BlackPearl Object Gateway.

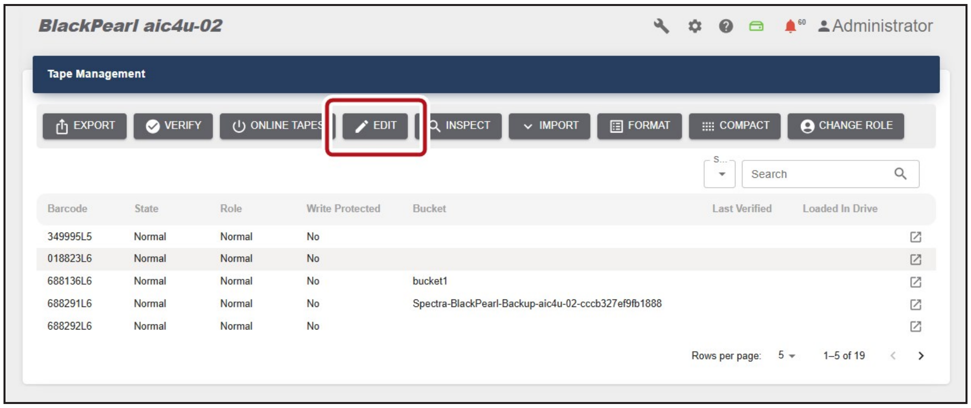
Note: For instructions on importing tape media in to the I/O slots of an IBM tape library, see Related Information on page 21.

Edit Tape Export Information Without Exporting Tape Media

If desired, you can enter information about the export location of a tape cartridge and assign it a label without exporting the tape from the Gateway.

Note: You are also asked to enter this information when you export a tape.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**.



Barcode	State	Role	Write Protected	Bucket	Last Verified	Loaded In Drive
349995L5	Normal	Normal	No			
018823L6	Normal	Normal	No			
688136L6	Normal	Normal	No	bucket1		
688291L6	Normal	Normal	No	Spectra-BlackPearl-Backup-aic4u-02-cccb327ef9fb1888		
688292L6	Normal	Normal	No			

Figure 252 The Tape Management screen - Tape Management pane - Edit button.

2. Select one of the tapes you want to edit and click **Edit**. The Edit Tape dialog box displays.
3. Enter information in the **Eject Label** and **Eject Location** fields. This information is stored on the BlackPearl database and is visible when re-importing the tape into a BlackPearl Object Gateway.
4. Click **Save**.

Export Tapes from a T50e or T120 Library with Multiple Partitions

If a T50e or T120 library with multiple partitions is associated with a BlackPearl Object Gateway, you cannot use the BlackPearl Object Gateway to export the tapes because of the library's shared Entry/Exit port. In this situation, use the following steps to export tapes.

1. Use the library's front panel to export the tapes. See "Export Specific Cartridges from the Library" in the *Spectra T120 User Guide* or "Create a Move Queue" in the *Spectra T50e User Guide* for instructions.
2. Mark the tapes as exported in the BlackPearl user interface. See Manage Tapes Not in Inventory on page 309.

EXPORTING TAPE MEDIA FROM A LUMOS LIBRARY

Use the instructions in this section to export tape media into a TeraPack-based library running the LumOS operating system, including the Spectra Cube and TFinity Plus tape libraries. You must be physically at the tape library to export tape media.

Notes:

- These instructions describe exporting tape media for data storage use. For instructions on exporting/exchanging cleaning media, see your *Library User Guide* for instructions.
- The instructions below assume your tape library was previously configured and is under the control of a BlackPearl Object Gateway.
- These instructions describe a simplified workflow for exporting tape media for use by a BlackPearl Object Gateway. For advanced export options, see your *Library User Guide* for instructions.
- For instructions on importing tapes into a BlueScale operating system library, see Exporting Tape Media from a BlueScale Library on page 350.
- For instructions on exporting tapes from a Spectra Stack, Spectra SL3, T120, and T50e tape libraries, see your *Library User Guide.*

Log Into the User Interface

Use the following steps to log into the library using the front panel touch screen.

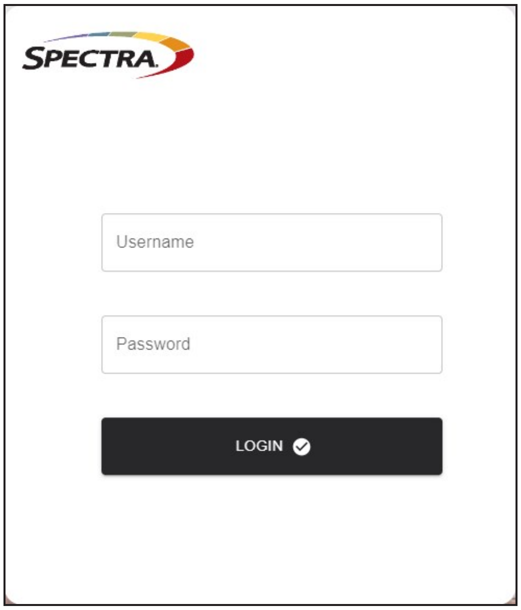
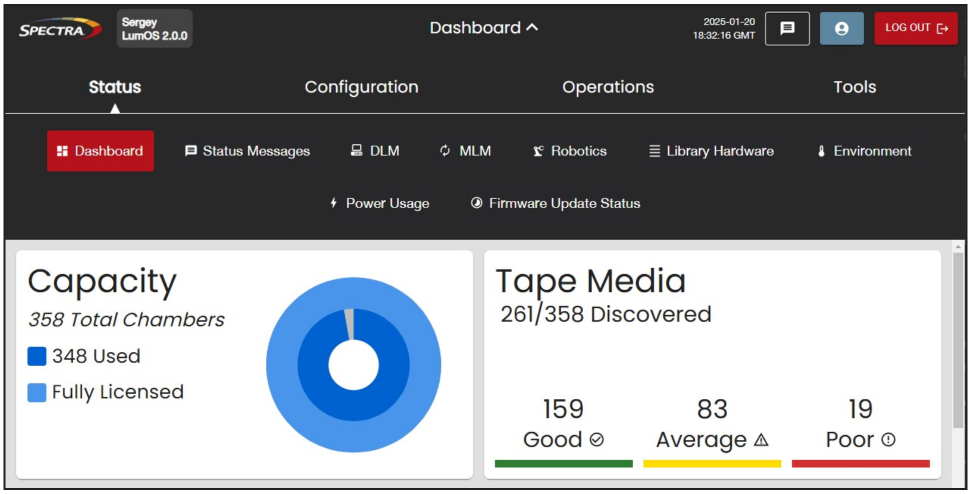


Figure 253 The LumOS Login screen.

1. Enter in the **Username** and **Password**.

2. Click **Login**. The user interface Dashboard screen displays.



Capacity

358 Total Chambers

🟦 348 Used

🟦 Fully Licensed

Tape Media

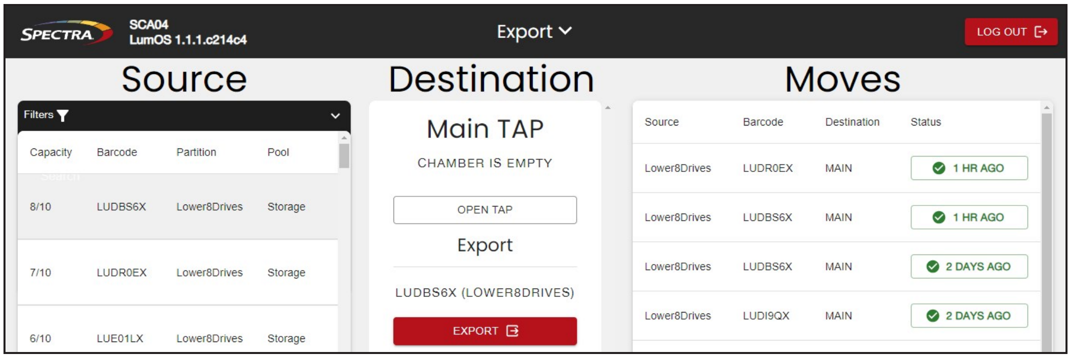
261/358 Discovered

159	83	19
Good ✓	Average ⚠	Poor ⓘ

Figure 254 The LumOS user interface Dashboard screen.

Export Magazines - Spectra Cube TAP

1. Select **Operations > Export Media** in the LumOS user interface.



Capacity	Barcode	Partition	Pool
8/10	LUDBS6X	Lower8Drives	Storage
7/10	LUDR0EX	Lower8Drives	Storage
6/10	LUE01LX	Lower8Drives	Storage

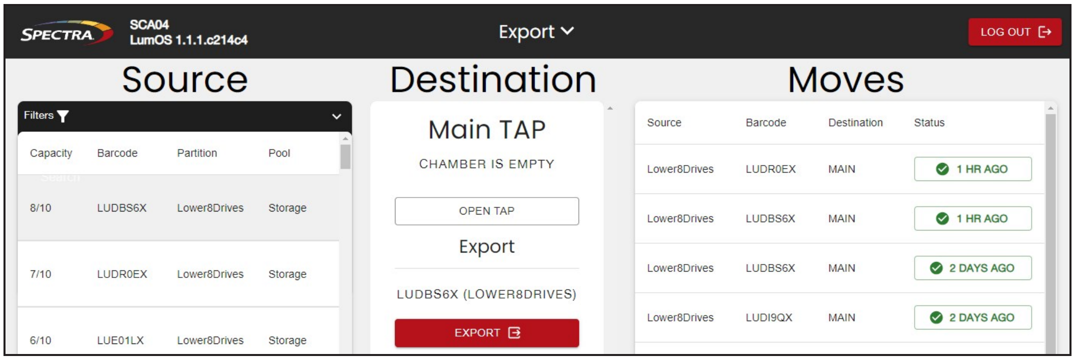
Source	Barcode	Destination	Status
Lower8Drives	LUDR0EX	MAIN	✓ 1 HR AGO
Lower8Drives	LUDBS6X	MAIN	✓ 1 HR AGO
Lower8Drives	LUDBS6X	MAIN	✓ 2 DAYS AGO
Lower8Drives	LUDI9QX	MAIN	✓ 2 DAYS AGO

Figure 255 The LumOS Export screen.

2. Select the desired **Magazine** in the **Source** column.
3. Click **Export**.
4. Click **Open TAP** to access the exported magazine. Remove the magazine or desired cartridges from the magazine.
5. Gently push the TAP closed.
6. Click **Close TAP** to complete the export.

Export Magazines - TFinity Plus Center TAP

1. Select **Operations > Export Media** in the LumOS user interface.



Capacity	Barcode	Partition	Pool
8/10	LUDBS6X	Lower8Drives	Storage
7/10	LUDR0EX	Lower8Drives	Storage
6/10	LUE01LX	Lower8Drives	Storage

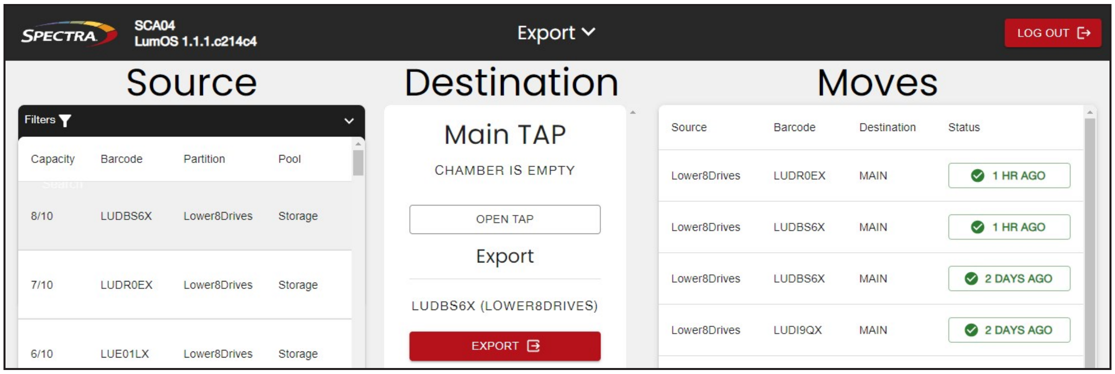
Source	Barcode	Destination	Status
Lower8Drives	LUDR0EX	MAIN	✓ 1 HR AGO
Lower8Drives	LUDBS6X	MAIN	✓ 1 HR AGO
Lower8Drives	LUDBS6X	MAIN	✓ 2 DAYS AGO
Lower8Drives	LUDI9QX	MAIN	✓ 2 DAYS AGO

Figure 256 The LumOS Export screen.

2. Select the desired **Magazine** in the **Source** column.
3. Click **Export**.
4. Click **Open TAP** to access the exported magazine. Remove the magazine or desired cartridges from the magazine.
5. Click **Close TAP** to close the TAP.

Export Magazines - TFinity Bulk TAP

1. Select **Operations > Export Media** in the LumOS user interface.



Capacity	Barcode	Partition	Pool
8/10	LUDBS6X	Lower8Drives	Storage
7/10	LUDR0EX	Lower8Drives	Storage
6/10	LUE01LX	Lower8Drives	Storage

LUDBS6X (LOWER8DRIVES)

Source	Barcode	Destination	Status
Lower8Drives	LUDR0EX	MAIN	✓ 1 HR AGO
Lower8Drives	LUDBS6X	MAIN	✓ 1 HR AGO
Lower8Drives	LUDBS6X	MAIN	✓ 2 DAYS AGO
Lower8Drives	LUDI9QX	MAIN	✓ 2 DAYS AGO

Figure 257 The LumOS Export screen.

2. Select the desired **Magazine**(s) in the **Source** column.
3. Click **Export**.
4. Open the bulk TAP door by clicking **Open TAP** to unlock the door then manually open the door by pressing the button next to the door. The button is solid green when the door is unlocked.

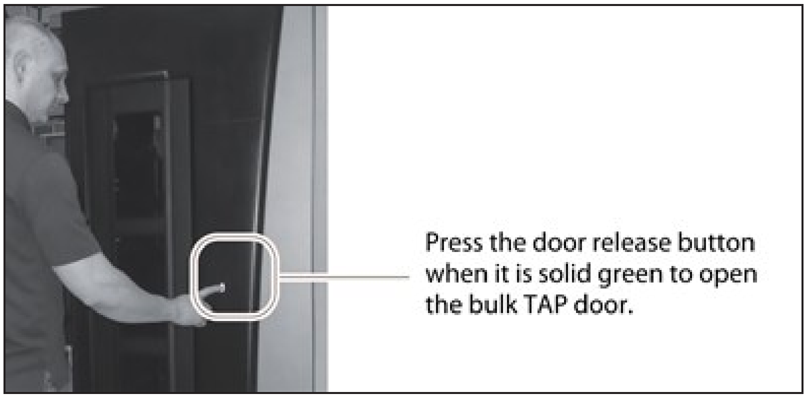
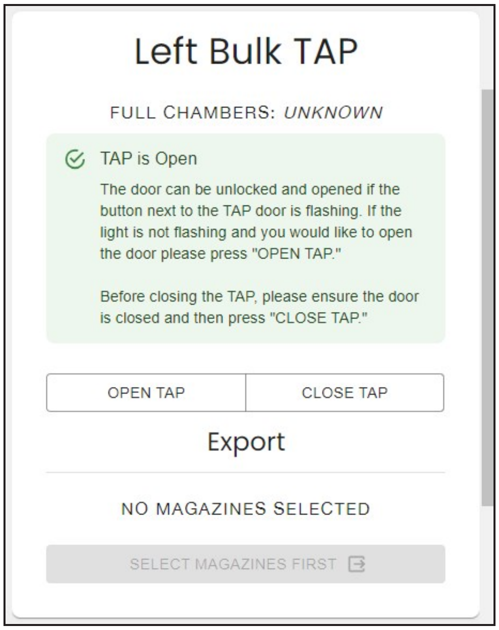

Press the door release button when it is solid green to open the bulk TAP door.

Figure 258 Press the door release button to open the door.

5. Remove the magazine(s) or desired cartridges from the magazine(s).
6. Close the bulk TAP door firmly by pressing at the top and bottom. An audible click indicates that the door is latched closed.



Left Bulk TAP

FULL CHAMBERS: *UNKNOWN*

TAP is Open

The door can be unlocked and opened if the button next to the TAP door is flashing. If the light is not flashing and you would like to open the door please press "OPEN TAP."

Before closing the TAP, please ensure the door is closed and then press "CLOSE TAP."

Figure 259 Bulk TAP Dialogue.

7. In the user interface, click **Close TAP**.

EXPORTING TAPE MEDIA FROM A BLUESCALE LIBRARY

Use the instructions in this section to export tape media into a TeraPack-based library running the BlueScale operating system, including the Spectra TFinity, T950, T680, T380, and T200 tape libraries. You must be physically at the tape library to export tape media.

Notes:

- These instructions describe exporting tape media for data storage use. For instructions on exporting/exchanging cleaning media, see your *Library User Guide* for instructions.
- The instructions below assume your tape library was previously configured and is under the control of a BlackPearl Object Gateway.
- These instructions describe a simplified workflow for exporting tape media for use by a BlackPearl Object Gateway. For advanced export options, see your *Library User Guide* for instructions.
- For instructions on exporting tapes from a Spectra Stack, Spectra SL3, T120, and T50e tape libraries, see your *Library User Guide*.

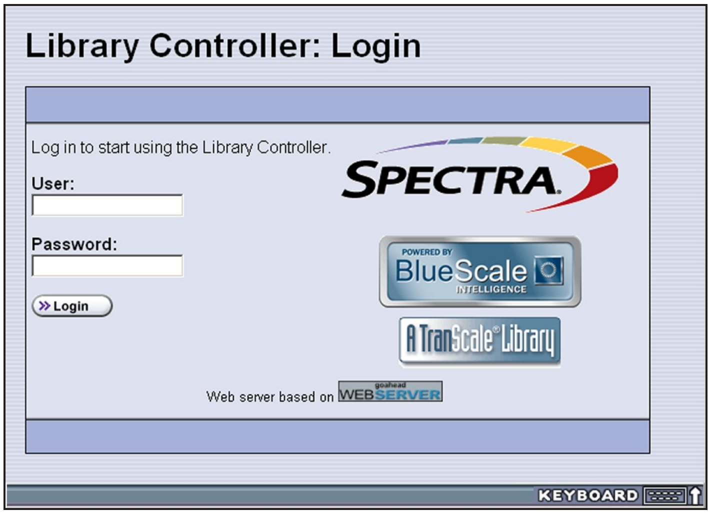
Log Into the User Interface

Use the following steps to log into the library using the front panel touch screen.

1. Select the **User** text box. A cursor appears in the box.

Note: When using the touch screen on the library operator panel, touch the keyboard icon on the Login screen to activate the soft keyboard on the library's touch screen. Use the stylus or your finger to select fields and to type information using the soft keyboard.

Touching the keyboard icon again closes the soft keyboard.



Library Controller: Login

Log in to start using the Library Controller.

User:

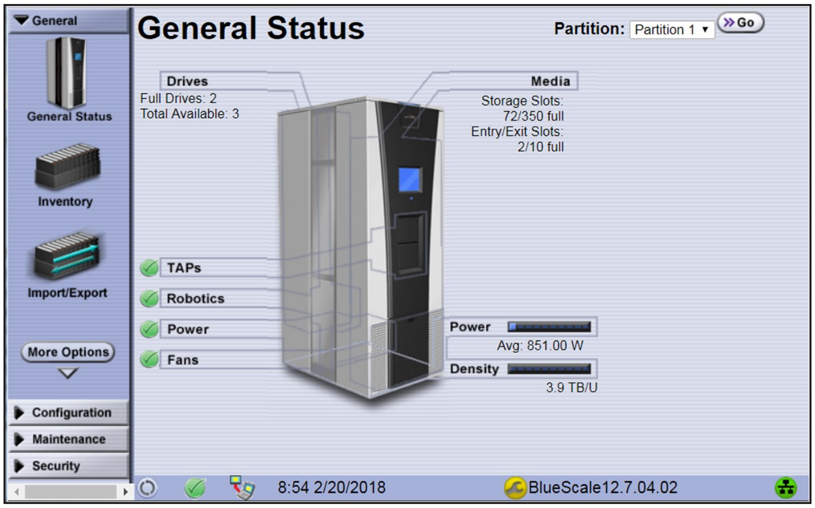
Password:

» Login
SPECTRA
POWERED BY BlueScale INTELLIGENCE
A TranScale Library
Web server based on goahead WEBSERVER
KEYBOARD

Figure 260 Log into the library using the Library Controller: Login screen.

2. Type your user name (**su** is the default user name for a superuser).
3. Type your password in the **Password** text box. By default, passwords are not configured for the three default users.

4. Click **Login**. The library's General Status screen displays.



General Status

Partition: Partition 1 ▾

Drives
Full Drives: 2
Total Available: 3

Media
Storage Slots:
72/350 full
Entry/Exit Slots:
2/10 full

Power
Avg: 851.00 W

Density
3.9 TB/U

8:54 2/20/2018

BlueScale12.7.04.02

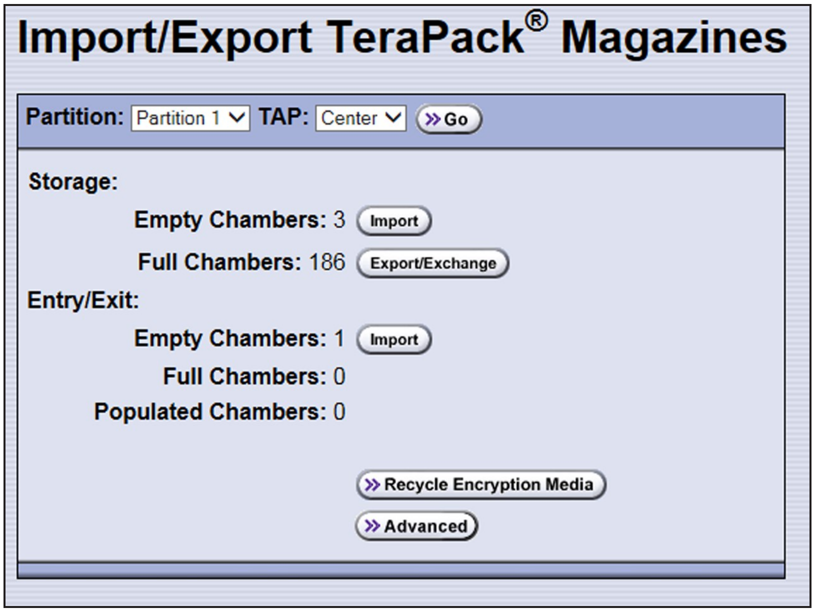
Figure 261 The BlueScale user interface General Status screen for a Spectra TeraPack-based tape library.

Export the Magazines

1. From the toolbar menu, select **General > Import/Export**. The Import/Export TeraPack Magazines screen displays.
2. Use the **Partition** drop-down menu to select the partition from which you want to export tapes, and the **TAP** drop-down menu to select the TAP (TeraPack Access Port) you want to use to export tapes.

Select this TAP...	If you want to use...
Center	The TAP located in the main frame. • TFinity, T950, and T680 libraries feature a double TAP. • T380 and T200 libraries feature a single TAP.
Left	The bulk TAP located in the bulk TAP service frame on the left end of the library, if present.
Right	The bulk TAP located in the bulk TAP service frame on the right end of the library, if present.
LeftAndRight	Both the bulk TAP located in the bulk TAP service frame on the left end of the library, and the bulk TAP located in the bulk TAP service frame on the right end of the library.

3. Click **Go**. The Import/Export TeraPack Magazines screen refreshes to show the current status of the chambers assigned to the selected partition.



Import/Export TeraPack® Magazines

Partition: Partition 1 TAP: Center

Storage:

Empty Chambers: 3

Full Chambers: 186

Entry/Exit:

Empty Chambers: 1

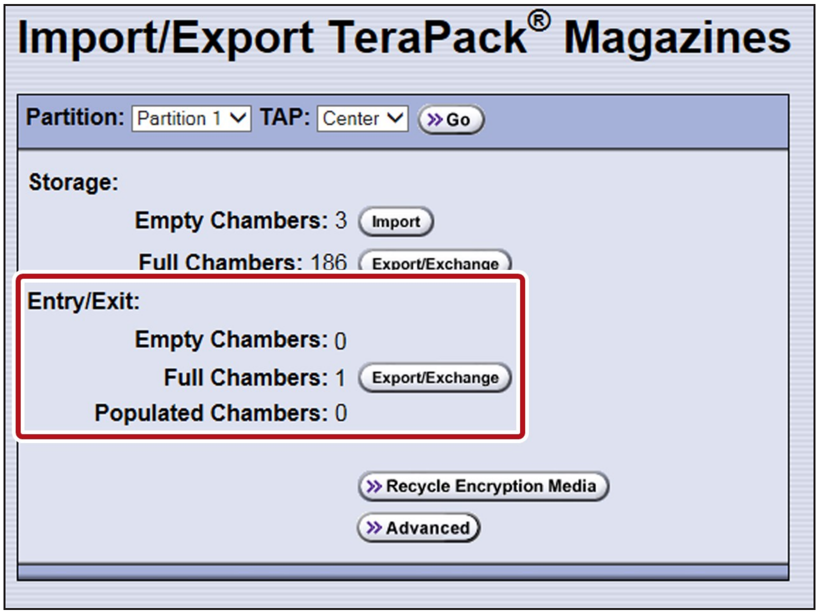
Full Chambers: 0

Populated Chambers: 0

Figure 262 Select the partition and the TAP.

4. Under Entry/Exit, click the **Export/Exchange** button.

IMPORTANT Only export tape cartridges from the Entry/Exit port. The BlackPearl Object Gateway controls the movement of tape media inside the library.



Import/Export TeraPack® Magazines

Partition: Partition 1 TAP: Center

Storage:

Empty Chambers: 3

Full Chambers: 186

Entry/Exit:

Empty Chambers: 0

Full Chambers: 1

Populated Chambers: 0

Figure 263 Click **Export/Exchange** for the Entry/Exit pool.

5. The next steps depend on which TAP you selected.

If you selected the Center TAP

a. A TeraPorter retrieves a magazine from the specified pool and places it in the center TAP. The TAP door opens and a Feedback Required screen displays.

b. Remove the magazine from the open TAP and set it aside.

c. If you are exporting media from a TFinity or T950 library, continue to Step . If you are exporting tape media from a T680, T380, or T200 tape library, gently raise the TAP door and press it firmly into the latch for approximately one second.

Note: Close the TAP door firmly, but do not use excessive force.

d. Return to the operator panel and select the appropriate option on the Feedback Required screen.

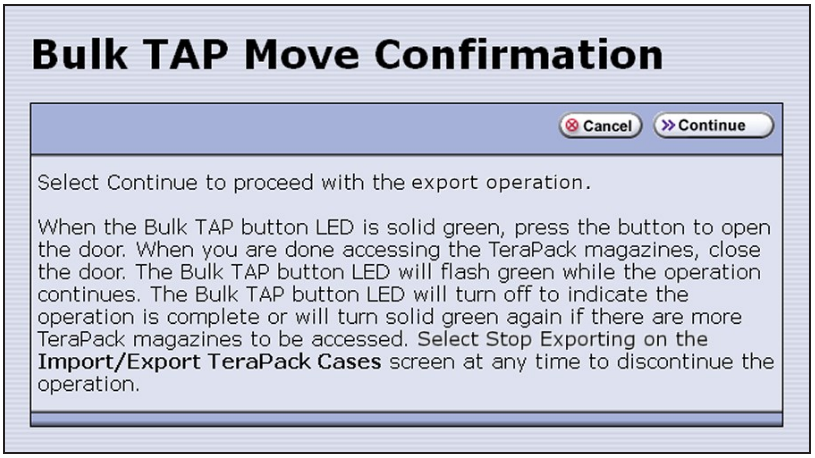
Note: If you wait more than 10 minutes to respond, the library times out and displays a message on the operator panel. For TFinity and T950 libraries, the TAP door is left open.

Select...	If...
Continue	You want to export another magazine. The process continues as follows: 1. After the TAP door closed either manually or automatically, the TeraPorter retrieves the next magazine and delivers it to the center TAP. **Note:** On TFinity, T950, and T680 libraries, the TAP doors alternate as you continue to export magazines. 2. The export process continues as long as there are magazines in the entry/exit pool, or until you click **Stop Exporting** on the Feedback Required screen. Continue to remove the magazines from the TAP and click **Continue** after each one. When all of the magazines in the Entry/Exit pool have been exported, the process stops automatically and the Import/Export TeraPack Magazines screen displays.
Stop Exporting	The magazine you removed from the TAP is the last one you want to export.

If you selected the Bulk Left, Right, or LeftAndRight TAP

a. The Bulk TAP Move Confirmation screen displays a message with instructions for performing the export operation.

IMPORTANT If the carousel contains magazines from a previous export or import operation, the library will alert you to remove those magazines. When the door release button LED is solid green, press it to open the bulk TAP door. Remove the magazines, close the door firmly by pressing at the top and bottom, and select **Continue** to restart the export process.



Select Continue to proceed with the export operation.

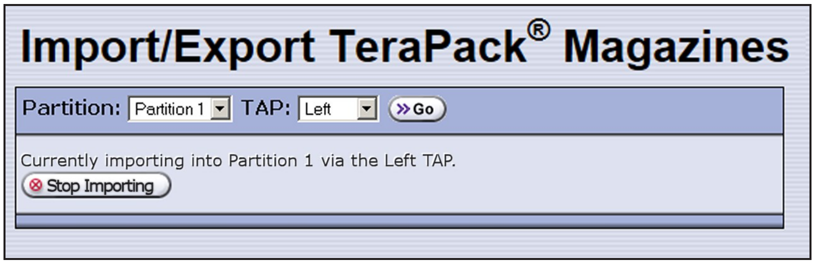
When the Bulk TAP button LED is solid green, press the button to open the door. When you are done accessing the TeraPack magazines, close the door. The Bulk TAP button LED will flash green while the operation continues. The Bulk TAP button LED will turn off to indicate the operation is complete or will turn solid green again if there are more TeraPack magazines to be accessed. Select Stop Exporting on the **Import/Export TeraPack Cases** screen at any time to discontinue the operation.

Figure 264 Read the instructions on the Bulk TAP Move Confirmation screen, then click **Continue**.

b. Click **Continue**. The TeraPorter retrieves magazines from the entry/exit pool and places them in the bulk TAP.

Note: If you selected **LeftAndRight** TAP, and there are fewer than 14 magazines to export, all of the magazines are moved to the left bulk TAP. If you selected **LeftAndRight** TAP and there are more then a 14 magazines to export, the magazines are distributed as evenly as possible between the two bulk TAPs.

c. The Import/Export TeraPack Magazines screen refreshes to show that the moves are in progress.



Import/Export TeraPack® Magazines

Partition: Partition 1 TAP: Left

Currently importing into Partition 1 via the Left TAP.

Figure 265 The Import/Export TeraPack Magazines screen shows that the export process is underway.

Note: Click **Stop Exporting** on the Import/Export TeraPack Magazines screen to end the current export operation. If there are magazines in the bulk TAP, you will be instructed to remove them before the next import or export operation.

d. When all of the magazines have been retrieved or when a bulk TAP is full, the carousel rotates to face the outside of the library and the door release button LED turns solid green. Press the button to open the bulk TAP door.

Note: If you wait more than 10 minutes to open the door, the library considers the export operation complete. The LED turns off and the carousel rotates to face the interior of the library. When you attempt the next import or export operation using the bulk TAP, the library will require you to remove any magazines in the carousel before you can proceed.

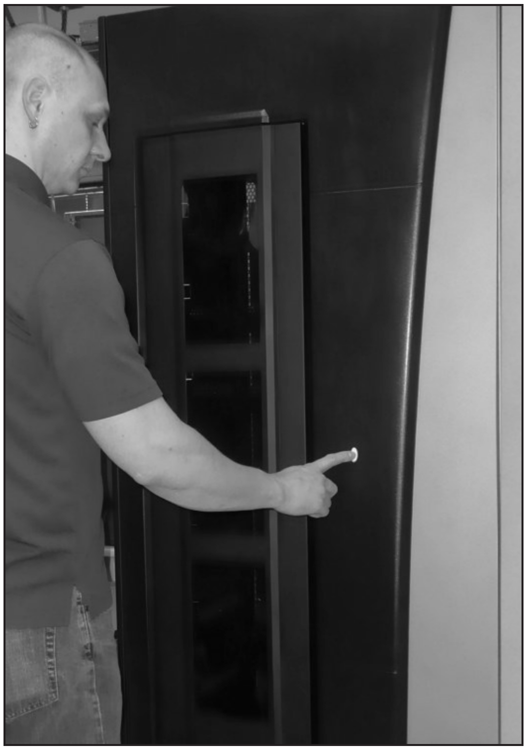


Figure 266 Press the door release button to open the door.

e. Remove the TeraPack magazines from the carousel(s) and set them aside.

f. Close the bulk TAP door firmly by pressing at the top and bottom. An audible click indicates that the door is latched closed.

Note: If you fail to close the door within 10 minutes, the export operation times out.

g. If the bulk TAP could not accommodate all of the magazines in the entry/exit pool, the TeraPorter moves the next set of magazines from the entry/exit pool to the carousel. The process continues as long as there are magazines in the entry/exit pool. When the process stops, the door release button LED turns off, the carousel rotates to face the interior of the library, and the Import/Export TeraPack Magazines screen displays.

CHAPTER 14 - MAINTAINING THE BLACKPEARL OBJECT GATEWAY

This chapter describes software maintenance procedures for the Spectra BlackPearl Object Gateway.

Data Integrity Verification - Disk Media

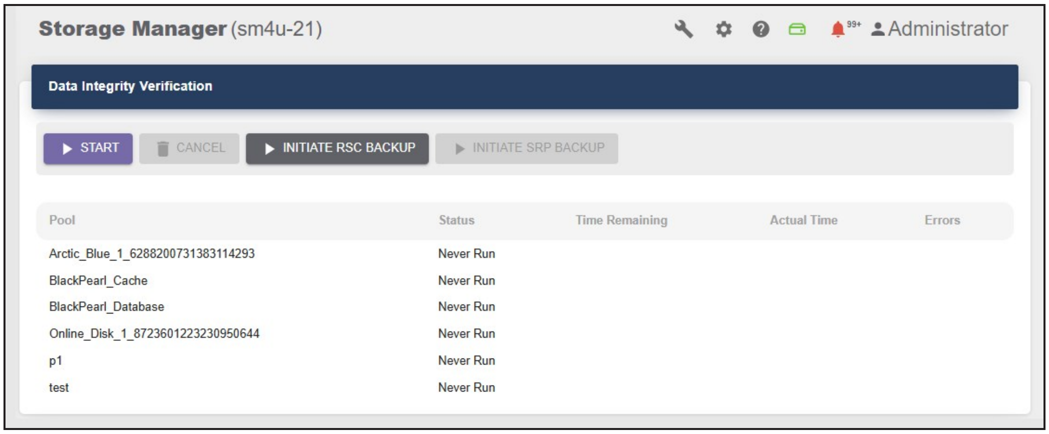
The BlackPearl Object Gateway allows you to perform on-demand data integrity verifications on any disk pools connected to the Gateway, including the internal disk pools containing the BlackPearl cache and database. Performing a data integrity verification on a disk pool is useful when you want to ensure the data on the disk pool is stored correctly.

Data integrity verification is a sector by sector check of the entire storage pool, not just the data contained on the pool. The duration of a data integrity verification varies based on the size of the disk pool, and in some cases can take a very long time to complete.

Start Disk Media Data Integrity Verification

Use the instructions in this section to perform a data integrity verification on a disk pool.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Data Integrity Verification**.



Pool	Status	Time Remaining	Actual Time	Errors
Arctic_Blue_1_6288200731383114293	Never Run			
BlackPearl_Cache	Never Run			
BlackPearl_Database	Never Run			
Online_Disk_1_8723601223230950644	Never Run			
p1	Never Run			
test	Never Run			

Figure 267 The Data Integrity Verification screen.

2. Select the disk pool for which you want to start the data integrity verification and click **Start.** A confirmation screen displays.

Note: While the verification is in progress, the disk pool may experience degraded performance. However, client access and rebuilds have priority over data integrity verification.

3. Click **Start Data Verification**.

CAUTION

In the event that the data integrity verification detects suspect objects, they are listed in the Suspect Objects pane. If possible, retrieve the object from another storage domain, delete the object from the Gateway and then PUT the object again.

The affected files cannot be retrieved from the storage pool, and may need to be transferred to the BlackPearl Object Gateway again, if the data policy did not specify multiple copies of the data. If you do not have copies of the affected files on your host or another location, they are lost.

Cancel Disk Media Data Integrity Verification

If desired, you can stop a data integrity verification while it is in progress.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Data Integrity Verification**.
2. Select the pool for which you want to stop verification and click **Cancel**. A confirmation screen displays.
3. Click **Submit** to stop the verification.

DATA INTEGRITY VERIFICATION - TAPE MEDIA

The BlackPearl Object Gateway automatically performs data integrity verification for any tape cartridge that is unchanged for the number of days specified in a given storage domain.

The BlackPearl user interface also allows you to perform an on-demand data integrity verification on any data tape cartridge present in the tape library connected to the Gateway. Performing a data integrity verification on a tape cartridge is useful when you want to ensure the data on the tape is stored correctly. Spectra Logic recommends verifying any tape you plan to export from your BlackPearl Object Gateway and store off-site.

You can configure the Gateway to verify the entire tape, or a specified percentage of the total reported capacity of the tape cartridge. If you specify a percentage, the Gateway starts the scan the specified percentage of the tape capacity before the EOD (End of Data) marker and ends the scan at the EOD marker. This is useful when you only want to validate the most recent data written to the tape.

You can select to verify a single specified tape cartridge, or to verify all tape cartridges using a single operation.

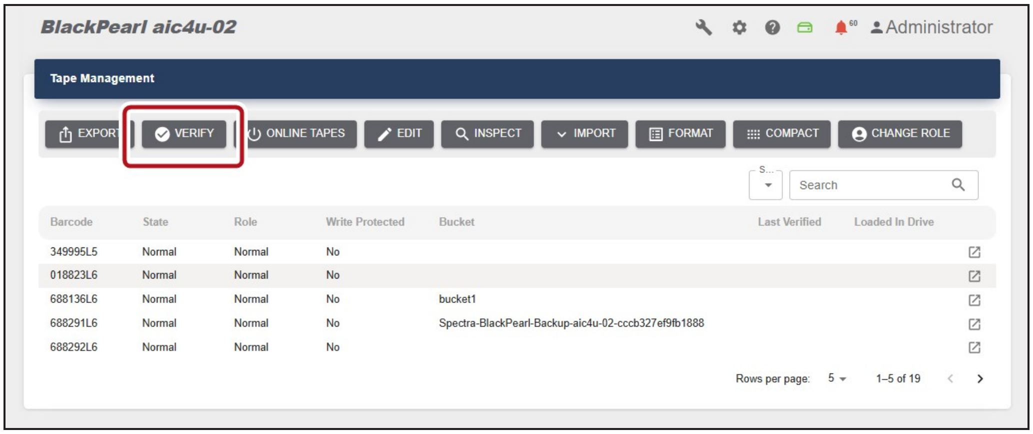
Notes:

- If there are cleaning tapes present in a data partition, they display on the Tape Management screen. However, it is not possible to individually verify a cleaning tape, and cleaning tapes do not undergo data integrity verification if you opt to verify all tapes in a single operation.
- Cleaning tapes in cleaning partitions are not processed by data integrity verification.

Start Tape Media Data Integrity Verification

Use the instruction in this section to verify data on tape media.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Tape Management**.



Barcode	State	Role	Write Protected	Bucket	Last Verified	Loaded In Drive
349995L5	Normal	Normal	No			
018823L6	Normal	Normal	No			
688136L6	Normal	Normal	No	bucket1		
688291L6	Normal	Normal	No	Spectra-BlackPearl-Backup-aic4u-02-cccb327ef9fb1888		
688292L6	Normal	Normal	No			

Rows per page: 5 1–5 of 19

Figure 268 The Tape Management screen - Verify button.

2. Select the tape you want to verify and click **Verify**. A confirmation window displays.

3. Click **Verify** to begin the data integrity verification.

CAUTION	In the event that the data integrity verification fails, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7) for assistance in determining the affected files on the tape cartridge. The affected files cannot be retrieved from the tape cartridge, and may need to be transferred to the BlackPearl Object Gateway again, if the data policy did not specify multiple copies of the data. If you do not have copies of the affected files on your host or another location, they are lost.

Cancel Tape Media Data Integrity Verification

If desired, you can cancel queued data integrity verification. Only tapes currently queued for data integrity verification are canceled. Any tapes undergoing verification when the cancel command is issued will complete the verification process.

To cancel a tape verification, you must access the legacy user interface used in BlackPearl OS 5.8.x and earlier. Functionality to cancel a tape verification will be added to the new user interface in a later version of the BlackPearl OS.

1. Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with "/legacy". For example:

   https://*ipaddress*/legacy

2. Use the toolbar in the upper-right to select **Support > Tools > Data Integrity Verification.** The Data Integrity Verification screen displays.

3. Select the tape for which you want to cancel verification in the Tape Management screen, and then select **Action > Cancel Tape Verification**.

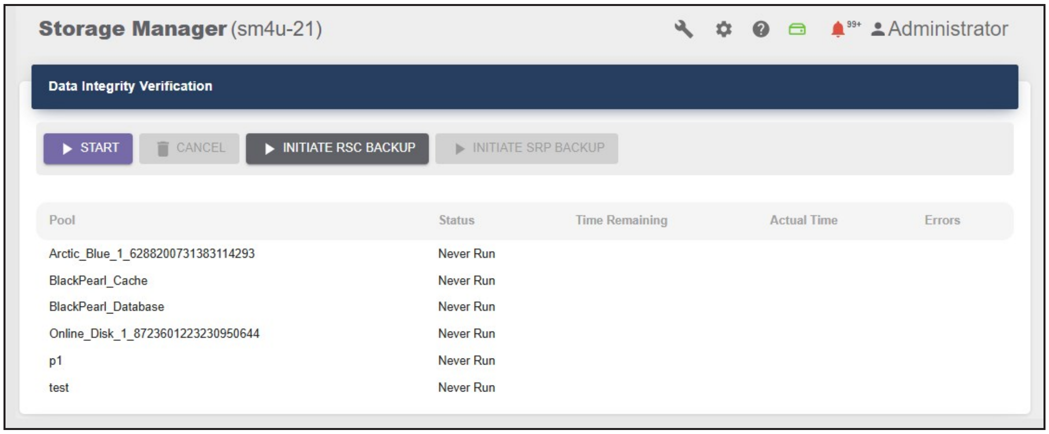
Note: To stop verification on all tapes in the tape library, select **Action > Cancel All Tapes Verifications.**

4. A confirmation screen displays. Click **OK** to stop the tape verification(s).

INITIATE RSC BACKUP

The replicated system configuration backup stores the current configuration of all settings for the BlackPearl Object Gateway on a storage pool present in the Gateway. This backup occurs automatically each time you create a storage pool, or once every seven days. If you make major changes to your BlackPearl Object Gateway, Spectra Logic recommends that you backup the configuration manually.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Data Integrity Verification**.



Pool	Status	Time Remaining	Actual Time	Errors
Arctic_Blue_1_6288200731383114293	Never Run			
BlackPearl_Cache	Never Run			
BlackPearl_Database	Never Run			
Online_Disk_1_8723601223230950644	Never Run			
p1	Never Run			
test	Never Run			

Figure 269 The Data Integrity Verification screen.

2. Click **Initiate RSC Backup.** A confirmation screen displays (not shown).
3. Click **Submit** to manually backup the current Gateway configuration.

Manually Enter Activation Keys

Use the following instructions to manually enter activation keys.

IMPORTANT For an initial installation, the activation keys must be entered in the order described in these instructions. Failure to enter the keys in the proper order causes an error.

1. When manually entering the activation keys for an initial installation, they **must** be entered in the following order:

   - Capacity keys
   - Product keys
   - All other keys

   If this is not an initial installation, you can enter activation keys in any order. Proceed with Step 2 on page 365.

Capacity keys:

Key Type	Description
<product type> SAS Count	Enables the specified number of SAS drives present in the system for NAS storage and Amazon compatible S3 pools.
<product type> SATA Count	Enables the specified number of SATA drives present in the system for NAS storage and Amazon compatible S3 pools.
<product type> SSD Count	Enables the specified number of SSDs present in the system for NAS storage and Amazon compatible S3 pools.
DS3 & on premise Glacier SAS Count	Enables the specified number of SAS drives present in the system for cache, database, OSD.
DS3 & on premise Glacier SATA Count	Enables the specified number of SATA drives present in the system for cache, database, OSD.
DS3 & on premise Glacier SSD Count	Enables the specified number of SSDs present in the system for cache, database, OSD.
DS3 & on-premise Glacier Tape Count	Enables the specified number of tape slots present in the attached Spectra Logic or supported tape library.

Product keys:

Key Type	Description
DS3 Object Gateway	Enables the system to use the BlackPearl interface and functionality. **Note:** The system reboots after entering this product key. When the system completes initialization, you are automatically logged into the BlackPearl management interface.
Amazon compatible S3 Support Enabled	Enables Amazon compatible S3 support on the BlackPearl Object Gateway. **Note:** The system reboots after entering this product key. When the system completes initialization, you are automatically logged into the BlackPearl management interface.
On-premise Glacier	Enables tape support for a BlackPearl Object Gateway.
Third party tape library enabled	Enables object storage on a non-Spectra library.

All Other Keys:

Any additional keys included on the Software Activation Key Certificate, for example the Software Update key, can be entered in any order, as long as they are entered after the product keys.

2. Use the toolbar in the upper-right to select **Settings (gear icon)> Activation Keys**.
3. In the Activation Keys pane, click **Add**. The Add Activation Key dialog box displays (not shown).
4. Enter the **Activation Key**.
5. Click **Submit**.
6. If necessary, repeat Step 3 through Step 5 to add additional keys.

CHAPTER 15 - TROUBLESHOOTING

This section helps you troubleshoot problems with the Spectra BlackPearl Object Gateway and the attached Spectra tape library.

Note: Troubleshooting steps below that describe actions that involve a tape library apply only to Spectra Logic tape libraries.

If your problem is not addressed by any of the below entries, contact Spectra Logic Technical Support for assistance (see Contacting Spectra Logic on page 7).

LEGACY USER INTERFACE ACCESS

The troubleshooting sections below require you to use the legacy operating system. Here is how to access the legacy interface:

Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with "/legacy". For example:

https://*ipaddress*/legacy

The troubleshooting instructions will be updated to use the new user interface in a subsequent release of this User Guide.

Troubleshooting Events

Issue	Resolution
An email is sent from the tape library indicating that drives need cleaning	If the BlackPearl Object Gateway is connected to a **Spectra T200, T380, T680, T950, TFinity, or Cube library**, the library should be configured with a cleaning partition, which automatically cleans drives when cleaning is requested by the drive. If the BlackPearl Object Gateway is connected to a **Spectra T50e or T120 library**, there can only be one partition on the library if you want to use the BlackPearl Object Gateways' export function. If there is cleaning media in the data partition, the BlackPearl Object Gateway automatically initiates cleaning tape drives using this media. • If your cleaning tapes are LTO or TS11*xx* technology and MLM-enabled, you can use the MLM feature to monitor the status of cleaning media. Check that valid cleaning media is present in the cleaning partition as described below. **Note:** For LumOS instructions, see your LumOS Library User Guide. **1.** Log in to the BlueScale interface as described in your *Tape Library User Guide*. **2.** **T50e -** Select **MENU > General > Media Lifecycle Management**. **All other libraries -** Select **General > Media Lifecycle Management**. The MLM Report screen displays. **3.** Use the **Partition** drop-down menu to select **Total Library**. **4.** Use the **Report** drop-down menu to select **Cleans Remaining**. **5.** Click **Go**. The screen re-displays to show the number of cleans remaining for all cleaning cartridges present in the library. Confirm at least one tape still has cleans remaining. • If your cleaning tapes are not MLM-enabled, you cannot use MLM to monitor cleaning media. You must use the messages posted to the tape library's System Messages screen to determine when a piece of cleaning media expires. If there are no cleaning tapes with cleans remaining, use the *Tape Library User Guide* appropriate for your library type for instructions on exchanging expired cleaning media. If you continue to receive emails that drives are not being cleaned, contact Spectra Logic Technical Support for assistance (see Contacting Spectra Logic on page 7).

Issue	Resolution
An email is sent from the tape library regarding a problem with a tape drive	Check the tape library's BlueScale interface to ensure that the tape drives are functioning normally. **1.** Log in to the BlueScale interface as described in your *Tape Library User Guide*. **2.** Review any System Messages that were posted by the library and take any action described in the message(s). If the system messages do not provide enough information to resolve the issue, look for additional information on the DLM (Drive Lifecycle Management) Details screen. **1.** In your library user interface, display the MLM screen. **2.** Examine the status of each tape drive. If a drive shows any status besides a good status (green check mark in a circle), click **Details** for that drive, and take any action described in the details screen. **3.** Once the tape drives are returned to good status, retry the job. **Note:** If you cannot return your tape drives to good status, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).
An email is sent from the tape library that a tape drive cannot export a tape cartridge	Contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).
An email is sent from the tape library that indicates a robotics failure in the library	Gather an ASL as described in the "Configuring and Using AutoSupport" chapter in your *Tape Library User Guide*, and contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

Issue	Resolution
An email is sent from the tape library indicating a tape cartridge experienced a read or write error	If the BlackPearl Object Gateway detects a media error with a tape cartridge, the Gateway attempts to roll-back to a previously saved, known good checkpoint. Use the instructions in this section to resolve a media error. **1.** Make note of the tape barcode that experienced the media error, and what drive it was in when the error occurred. **2.** Log in to the tape library as described in your *Tape Library User Guide*. **3.** Use the instructions in "Cleaning a Drive" in your *Tape Library User Guide* to clean the affected drive twice. **4.** See "Use DLM to Test an LTO Drive" in your *Tape Library User Guide* to test the drive. If the drive test fails, contact Spectra Logic Technical Support for assistance (see Contacting Spectra Logic on page 7). **5.** Use the toolbar in the upper-right to select **Status > Tape Management**. The Tape Management screen displays. **6.** Select the tape that experienced the error, and then select **Action > Export Tape**. The Export Tape dialog box displays. **7.** If desired, enter information in the Export Label and Export Location fields. This information is stored on the BlackPearl database and is visible when reimporting the tape into a BlackPearl Object Gateway. **8.** Click **Export**. The tape is marked as exported in the BlackPearl Object Gateway database, and moved to the Entry/Exit pool in the attached tape library. **9.** Export the cartridge from the tape library as described in Export Tapes on page 341. **10.** Inspect the cartridge for damage. If the tape does not show any signs of damage, re-import the cartridge into the tape library. If the cartridge is damaged, discard the cartridge. If you continue to experience media errors, contact Spectra Logic Technical Support for assistance (see Contacting Spectra Logic on page 7).
The BlackPearl Object Gateway reports tapes as "Write Protected" on the Tape Management screen	If the tape has write protection set intentionally to protect valuable data from being overwritten, then select another tape. If the tape no longer needs to remain write protected, use your *Tape Library User Guide* to export the tape and disable write protection. Then re-import the tape cartridge into the tape library. **Note:** If the tape is still reported as Write Protected, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

Issue	Resolution
A system message on the BlackPearl Object Gateway reports "No tapes available" for a storage domain	When the BlackPearl Object Gateway runs out of usable tape media, it posts a message that indicates there are "No tapes available." Import additional cartridges into the tape library as described in your *Tape Library User Guide.* **Note:** If your tape library is at full capacity, you may need to exchange full tapes for new ones, or increase the capacity license on your library. If exchanging tapes, you must export the tapes from the BlackPearl Object Gateway before exporting the tapes from the tape library. See Export Tapes on page 341.
The BlackPearl Object Gateway displays an error message when attempting to export a tape	In order to use the BlackPearl export function on a T50e or T120 library, you must configure a single partition and select **Standard** as the partition's Entry/Exit Port Mode. If you configure the partition to use either the Shared or Queued Eject mode, or you configure more than one partition on your library, exports from the BlackPearl Object Gateway fail. See "Configuring and Managing Partitions" in the *T50e Library User Guide*, or "Partition Management" in the *T120 Library User Guide* for instructions on configuring a partition to use the Standard mode for the Entry/Exit port.
An email is sent from the BlackPearl Object Gateway indicating that the tape backend is deactivated	This issue can occur if the attached tape library either reboots or powers down. • If the tape library reboots, wait while the library completes initialization. The BlackPearl Object Gateway automatically establishes communication with the tape library once it completes its initialization. • If the tape library powers down, power on the library by pressing the power button on the front panel (see your *Tape Library User Guide* for more information). Then wait while the library completes initialization. The BlackPearl Object Gateway automatically establishes communication with the tape library once it completes it's initialization. • You may need to activate the data path backend on the BlackPearl Object Gateway. **1.** Use the toolbar in the upper-right to select **Configuration > Services**. The Services screen displays. **2.** Select the Amazon compatible S3 Service and select **Action > Show Details**. The Amazon compatible S3 Service details screen displays. **3.** On the Amazon compatible S3 Service detail screen, make sure the **Data Path Backend Activated** is set to **Yes**. If not, select **Action > Activate Data Path Backend**. If you continue to experience problems with the tape library, gather an AutoSupport log as described in your *Tape Library User Guide*, and contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

Issue	Resolution
An email is sent from the BlackPearl Object Gateway indicating that a tape it needs to complete a GET operation is not present in the tape library	The tape may have been exported from the tape library either on purpose or by mistake. Locate and re-import the tape into the tape library as described in your *Tape Library User Guide*. Once the tape is re-imported into the tape library, use the BlackPearl user interface to Online the tape as described in Import Tapes on page 313. Once the tape has a status of Online, the Gateway inspects the tape and uses it as needed.
An email is sent from the BlackPearl Object Gateway indicating a hardware failure	Over time, replaceable components in the BlackPearl Object Gateway may wear down and fail. Use the instructions in this section to determine the failed component. **1.** Use the toolbar in the upper-right to select **Hardware (hard drive icon)**. The Hardware screen displays. **2.** Examine the Hardware screen for any failed components, which are designated by a red X in a circle. **3.** Contact Spectra Logic Technical Support to request a part replacement (see Contacting Spectra Logic on page 7). Spectra Logic provides you with the replacement part. The documentation for all replacement parts can be found on the Spectra Logic support portal, at *support.spectralogic.com*, after you log in to the portal. The list of customer replaceable parts is as follows. Any other part failures are resolved by on-site Spectra representatives. • Data Drives • Boot Drives • Fans • Power Supplies • HBAs • RAM • Tape Drives (installed in the tape library)

Issue	Resolution
An email is sent from the BlackPearl Object Gateway indicating that the cache is full	The BlackPearl cache can become full for several reasons: • For PUT jobs, one or more data repositories (tape library, disk partition) is offline, or does not have sufficient space to write all the data currently in the cache. Data will sit in the cache until the problem is corrected. Check to make sure the data path backend is activated. 1. Use the toolbar in the upper-right to select **Configuration > Services and Protocols**. 2. Examine the S3 pane to view the status of the datapath backed. Check to make sure that no tape libraries are in standby state. 1. Use the toolbar in the upper-right to select **Configuration > Tape Management**. 2. Examine the Tape Partitions pane to view the status of tape libraries Check for system messages that indicate the partition is out of space. See Troubleshooting on page 366. • For GET jobs, data retrieved into the cache will remain in the cache until the client either gets the data or the job is canceled. Either use your client to complete the GET job, or cancel the job as described below. 1. In the left hand menu click **Jobs**. 2. Select the job you want to cancel and select **Cancel**.
An email is sent from the BlackPearl Object Gateway indicating that the database is full	If the database reaches full capacity, the BlackPearl Object Gateway is no longer usable. Additional drives must be installed to accommodate the database size. Contact Spectra Logic Technical Support for assistance (see Contacting Spectra Logic on page 7).
A system message on the BlackPearl Object Gateway indicates that the database is not being backed up	The BlackPearl Object Gateway reports a failure to backup the database in the system messages. Check the system messages to determine the cause. 1. Use the toolbar in the upper-right to select **Messages (bell icon)**. 2. Examine the list of messages for additional information about the failure. If the database backup schedule is not configured, the BlackPearl Object Gateway displays the following message once per day: “The database is not being backed up. Select a data policy from the Database backup screen to enable backups”. See Database Backup on page 197 for more information.

Issue	Resolution
The BlackPearl Object Gateway does not display tapes with duplicate barcodes on the Tape Management screen	Although a Spectra tape library allows duplicate barcodes within the same partition, the BlackPearl Object Gateway does not allow duplicate barcodes. Any tapes with duplicate barcodes are not displayed on the Tape Management screen and are not used by the Gateway. **1.** Use your *Tape Library User Guide* to export tapes with duplicate barcodes. **2.** Apply new, non-duplicate barcodes to the tapes and re-import them into the tape library. **3.** The BlackPearl Object Gateway automatically inspects and uses the tapes as needed.
The BlackPearl Tape Management screen shows media in the attached tape library as "Inspect Failed"	The BlackPearl Object Gateway uses tapes formatted with LTFS to store data. Only LTO-5 and higher Ultrium or TS 11*xx* technology tape media supports LTFS. If your tape library contains LTO-4 or older media, or you import LTO-4 or older media into a partition being utilized by a BlackPearl Object Gateway, the unsupported pieces of media display a Type of "Inspect Failed" on the Tape Management screen. Use the following steps to export LTO-4 and older media from your tape library. **Note:** The instructions in this section use the legacy user interface. Similar functionality is present in the new user interface starting with BlackPearl OS 5.9, but the steps are not documented here. **1.** Use the toolbar in the upper-right to select **Status > Tape Management**. The Tape Management screen displays. **2.** Examine the Tape Management screen for any tapes that display a Type of "Inspect Failed". Make note of all barcodes of "Inspect Failed" tapes. **3.** Select the affected tape, and then select **Action > Export Tape**. The Export Tape dialog box displays. **4.** If desired, enter information in the Export Label and Export Location fields. This information is stored on the BlackPearl database and is visible when reimporting the tape into a BlackPearl Object Gateway. **5.** Click **Export**. The tape is marked as exported in the BlackPearl Object Gateway database, and moved to the Entry/Exit pool in the attached tape library. **6.** Export the media from the tape library as described in your *Tape Library User Guide*.

Issue	Resolution
The BlackPearl Object Gateway displays a system message that a "Job did not complete in a 24 hour period"	If the BlackPearl Object Gateway experiences a network error when transferring data, the data transfer fails. Network errors occur due to a variety of circumstances. Use the information in this section to help you troubleshoot a network error. Network errors may occur if the client is saturating the network with information. Consider reducing the number of threads the client uses to transfer data. For example, a 1 GB connection should be set to a maximum of 3 threads. Network errors may also occur due to problems with cabling, network switch issues, or SAN issues. See the Networking Best Practices on page 89 for troubleshooting information. If you cannot resolve the network issue, use the steps below to collect logs and open a ticket with Spectra Logic Technical Support. **Note:** The instructions in this section use the legacy user interface. Similar functionality is present in the new user interface starting with BlackPearl OS 5.9, but the steps are not documented here. **1.** In the client software, collect a set of logs, if available. **2.** Download the Archive Provider logs on to your local host computer. **3.** Use the toolbar in the upper-right to select **Support > Logs**. The Logs screen displays. **4.** Select **Action > New Log Set** to generate a log set for use in general troubleshooting. **5.** Select the log set you just generated, and then select **Action > Download**. The log set begins downloading to your host computer. **6.** Submit a support incident using the Spectra Logic Technical Support portal as described in Spectra Logic Technical Support on page 388.
The BlackPearl user interface does not appear to update correctly	The BlackPearl Object Gateway may have rebooted. If the system reboots, all in-progress jobs are resumed or restarted, but the BlackPearl user interface is not being updated. Log out and then log back in to re-establish a connection with the system.
The BlackPearl Object Gateway displays a system message that a there is a problem with a Shared Resource Pool (SRP)	Shared Resource Pools are created when the BlackPearl Object Gateway is used with the Spectra Vail application, or in a HotPair configuration to maintain a shared database used by the BlackPearl OS. The pools are not accessible and cannot be modified or used for data storage. Contact Spectra Logic Technical Support if you receive error messages regarding Shared Resource Pools.

CHAPTER 16 - TECHNICAL SUPPORT

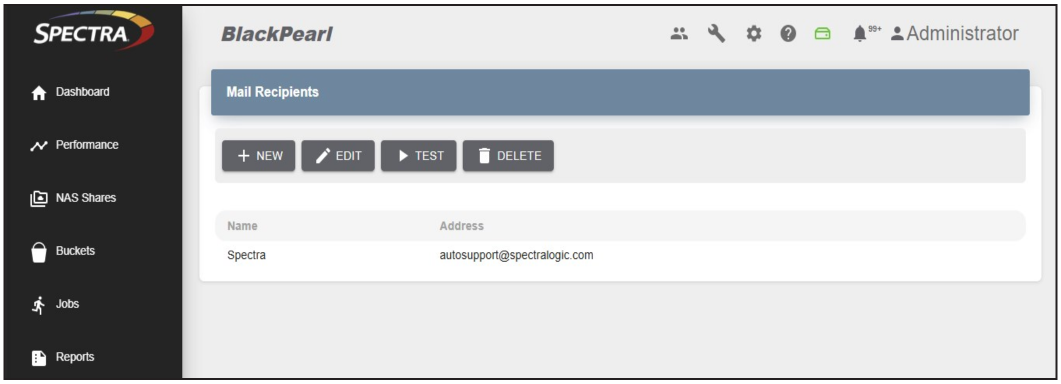
This chapter describes using the BlackPearl user interface to configure the support features of the Spectra BlackPearl Object Gateway, and how to submit a support ticket to Spectra Logic.

About AutoSupport

AutoSupport lets the BlackPearl Object Gateway automatically contact mail recipients when certain kinds of messages are generated. It is also used to generate AutoSupport Log (ASL) sets for use by Spectra Logic Technical Support. You can configure the Gateway to email ASL sets when critical events occur, or on a monthly basis. You can also choose to have mail recipients receive ASL sets.

Configure AutoSupport Mail Recipients

You can configure AutoSupport to email system messages and log sets, as they are generated, to selected recipients. All log sets and messages are sent to a previously configured mail recipient. You cannot send log sets or messages directly to an email address. Use the Mail Recipient screen to add, edit, or delete mail recipient accounts.

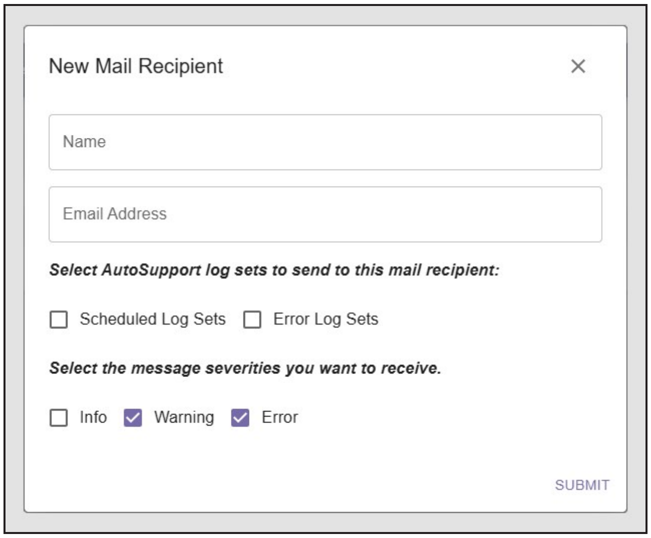


Name	Address
Spectra	autosupport@spectralogic.com

Figure 270 The Mail Recipients screen.

Create a New Mail Recipient

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Mail Recipients**. The Mail Recipients screen displays.
2. Click **New**. The New Mail Recipient dialog box displays.



New Mail Recipient

Name

Email Address

Select AutoSupport log sets to send to this mail recipient:

□ Scheduled Log Sets □ Error Log Sets

Select the message severities you want to receive.

□ Info ☑ Warning ☑ Error

SUBMIT

Figure 271 The New Mail Recipient dialog box.

3. Enter the following information for the mail recipient:

Field	Description
Name	The name of the recipient.
Email Address	The email address of the recipient. Be sure to use the full address using the standard email format, including the @ symbol. **Note:** The address cannot contain spaces or other non-alphanumeric characters (for example, an ampersand, &).
Select AutoSupport log sets to send to this mail recipient	Select **Scheduled Log Sets**, **Error Log Sets**, both options, or neither option for the mail recipient. Scheduled log sets are sent from the BlackPearl Object Gateway on the first of each month. Error log sets are sent anytime an error occurs that causes the Gateway to generate a log set.
Choose the message severities you want to receive	Select from the listed message types which severities of message this mail recipient should receive. The BlackPearl Object Gateway automatically sends email messages of the selected severity to the recipient when they are generated. **Note:** For the mail recipient to receive all messages generated by the Gateway, select all boxes.

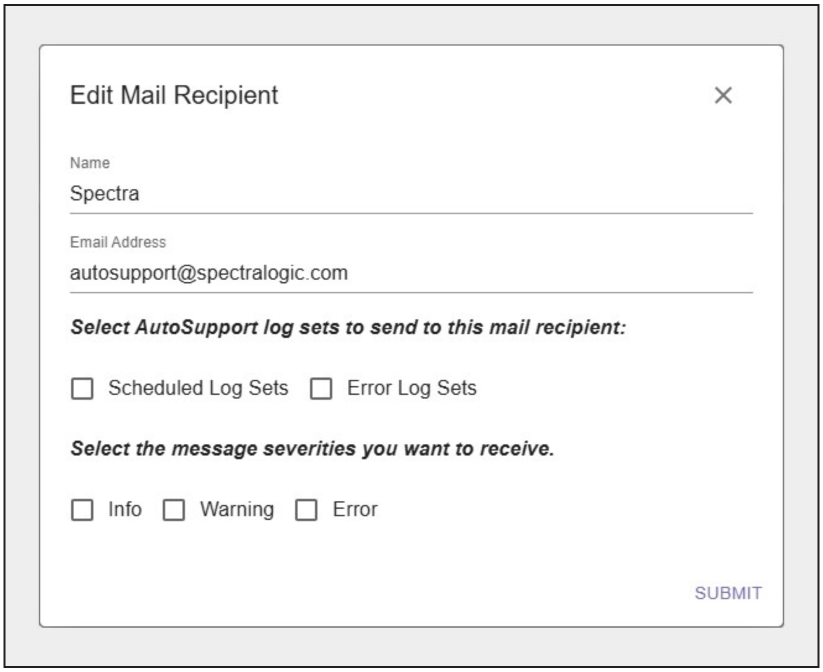
4. Click **Submit** to save the information. The Mail Recipients screen re-displays with the new mail recipient added to the list of mail recipients.

Edit a Mail Recipient

Use the following steps to edit a mail recipient account.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Mail Recipients**. The Mail Recipients screen displays.

2. From the list of mail recipients, select the name and then click **Edit**. The Edit Mail Recipient dialog box displays.



Edit Mail Recipient ×

Name
Spectra

Email Address
autosupport@spectralogic.com

Select AutoSupport log sets to send to this mail recipient:

□ Scheduled Log Sets □ Error Log Sets

Select the message severities you want to receive.

□ Info □ Warning □ Error

SUBMIT

Figure 272 The Edit Mail Recipient dialog box.

3. Change the information for the recipient as required and then click **Submit**.

Send a Test Email

Use the following steps to send a test email to a mail recipient.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Mail Recipients**. The Mail Recipients screen displays.
2. From the list of mail recipients, select the name of the recipient you want to receive a test email, and then click **Test**. The Send Test Email dialog box displays.
3. Click **Send**. The BlackPearl Object Gateway immediately sends a test email to the selected account.
4. Verify the user received the email from the BlackPearl Object Gateway. If the email is not received, verify that you entered the SMTP server settings correctly (see Configure the SNMP Service on page 105).

Delete a Mail Recipient

Use the following steps to delete a mail recipient account.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Mail Recipients**. The Mail Recipients screen displays.

2. From the list of mail recipients, select the name of the recipient you want to delete, and then click **Delete**. The Delete Mail Recipient dialog box displays (not shown).

Note: The default **Spectra** mail recipient cannot be deleted.

3. Click **Delete** to confirm the deletion.

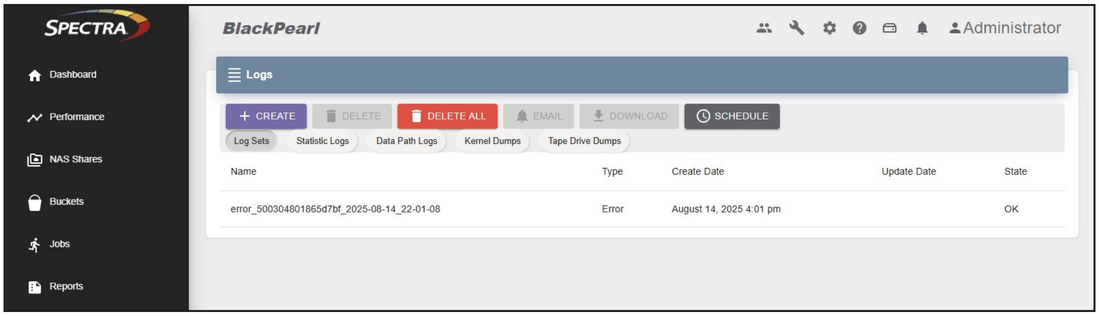
LOG SETS

The BlackPearl Object Gateway automatically generates log sets when errors occur. Log sets can also be generated manually, or generated on a schedule. The Gateway generates these types of log sets:

- **Log Sets** contain information about the configuration and status of the BlackPearl Object Gateway and are used for general troubleshooting. Log sets can be mailed to configured mail recipients or to Spectra Logic Technical Support.
- **Statistic Log Sets** contain performance data about the Gateway and are used by Spectra Logic Technical Support for in-depth troubleshooting. Statistic log sets are too large to be mailed directly from the Gateway and must be downloaded.
- **Kernel Log Sets** are generated whenever a process on the Gateway fails. This report cannot be generated manually.
- **Data Path Log Sets** are used to determine if there is a problem in the data planner code. This logset contains no customer data and is used by Spectra Logic Technical Support.
- **Tape Drive Dumps** are generated manually and are used by Spectra Logic Technical Support for drive troubleshooting.

Use the Logs screen to generate, email, or download log sets, as well as to configure a log set schedule.

Note: To generate drive dumps, see Collect and Download Drive Diagnostic Logs on page 300.



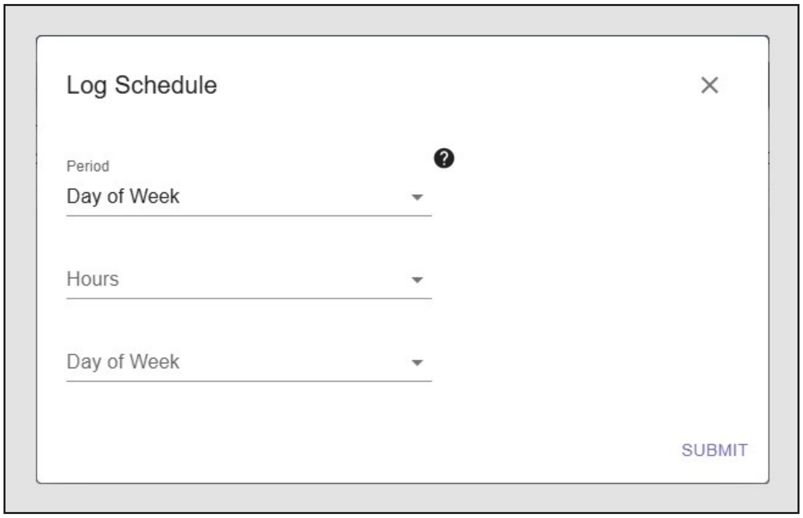
Name	Type	Create Date	Update Date	State
error_500304801865d7bf_2025-08-14_22-01-08	Error	August 14, 2025 4:01 pm		OK

Figure 273 The Logs screen.

Configure a Log Set Schedule

Use the instructions in this section to configure a log set schedule.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Logs**. The Logs screen displays.
2. Click **Schedule**. The Log Schedule dialog box displays.



Log Schedule

Period: Day of Week

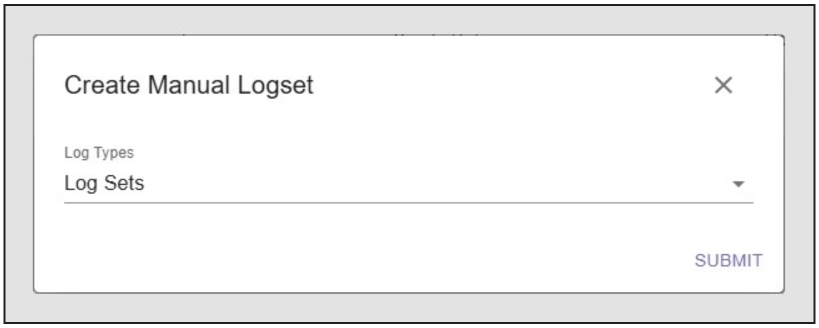
Figure 274 The Log Schedule dialog box.

3. Use the **Period** drop-down menu to select the frequency of the log schedule.
4. Use the **Hours** drop-down menu to select the hour when you want the system to generate the log set.
5. If you selected **Day of Week** or **Day of Month**, use the corresponding drop-down menu to select the day(s) on which to run the schedule.
6. Click **Submit**.

Manually Generate Log Sets

Although the BlackPearl Object Gateway auto generates log sets whenever errors occur, you may want to create log sets manually for troubleshooting purposes, or at the request of Spectra Logic Technical Support. Use the following instructions to manually generate a log set.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Logs**. The Logs screen displays.
2. Click **Create**. The Create Manual Logset dialog box displays.


Create Manual Logset

Log Types: Log Sets

Figure 275 The Create Manual Logset dialog box.

3. Use the **Log Types** drop-down menu to select the type of log to generate:
   - **Log Set** - generates a log set for use in general troubleshooting.
   - **Statistic Logs** - generates a log set used for in-depth troubleshooting. This log is not human readable.
   - **Data Path Logs** - generates a log set used for troubleshooting the data communication path to the Gateway and its associated tape library.
4. If you are generating a data path log, select the **Application** for which you want to generate a log set.

Application	Description
S3 Server	The Amazon compatible S3 Server log shows all DS3 API commands sent to the Gateway.
Data Planner	The Data Planner log shows how data sent to the Gateway is organized and stored to tape.

5. Click **Submit**.

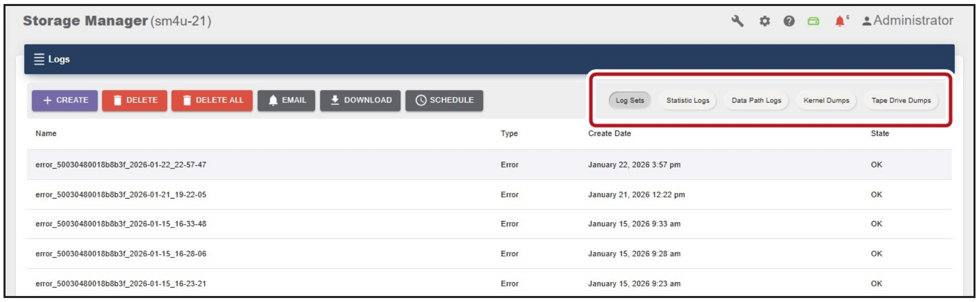
Email a Log Set

Use the instructions in this section to email a log set.

Notes:

- You must configure the SMTP settings on the Gateway before you can send emails. See Configure the SNMP Service on page 105 to configure the SMTP settings.
- Statistic Log Sets are too large to be emailed from the Gateway, and must be downloaded. See Download a Log Set on the next page.

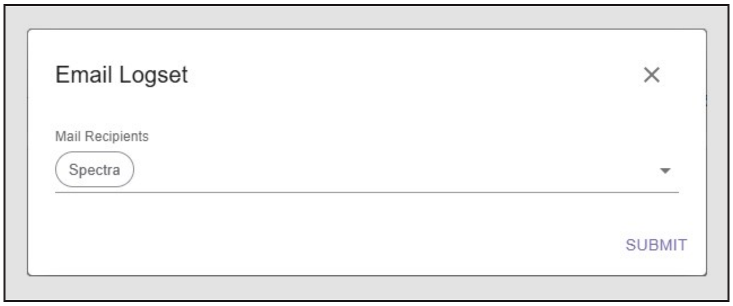
1. Use the toolbar in the upper-right to select **Settings (gear icon) > Logs**. The Logs screen displays.
2. Use the **logset type** buttons in the upper-right to select the type of logs to display.



Name	Type	Create Date	State
error_50030480018b8b3f_2026-01-22_22-57-47	Error	January 22, 2026 3:57 pm	OK
error_50030480018b8b3f_2026-01-21_19-22-05	Error	January 21, 2026 12:22 pm	OK
error_50030480018b8b3f_2026-01-15_16-33-48	Error	January 15, 2026 9:33 am	OK
error_50030480018b8b3f_2026-01-15_16-28-06	Error	January 15, 2026 9:28 am	OK
error_50030480018b8b3f_2026-01-15_16-23-21	Error	January 15, 2026 9:23 am	OK

Figure 276 The Logs screen - Logset Type buttons

3. Select the logset you want to email and click **Email**. The Email Logset dialog box displays.



Mail Recipients: Spectra

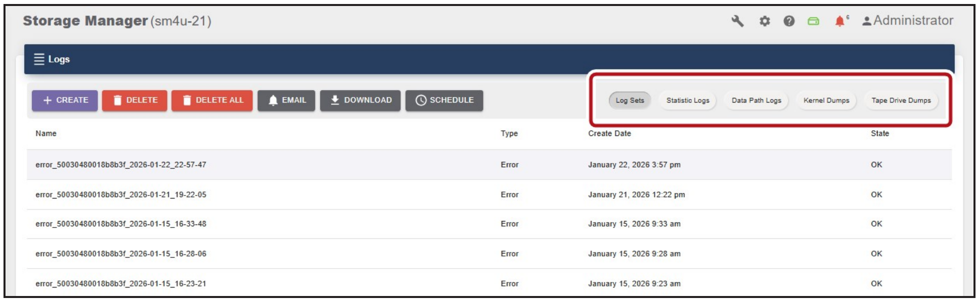
Figure 277 The Email Logset dialog box.

4. Use the **Mail Recipients** drop-down menu to select one or more configured mail recipients.
5. Click **Submit**.

Download a Log Set

Use the instructions in this section to download a log set.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Logs**. The Logs screen displays.
2. Use the **logset type** buttons in the upper-right to select the type of logs to display.



Name	Type	Create Date	State
error_50030480018b8b3f_2026-01-22_22-57-47	Error	January 22, 2026 3:57 pm	OK
error_50030480018b8b3f_2026-01-21_19-22-05	Error	January 21, 2026 12:22 pm	OK
error_50030480018b8b3f_2026-01-15_16-33-48	Error	January 15, 2026 9:33 am	OK
error_50030480018b8b3f_2026-01-15_16-28-06	Error	January 15, 2026 9:28 am	OK
error_50030480018b8b3f_2026-01-15_16-23-21	Error	January 15, 2026 9:23 am	OK

Figure 278 The Logs screen - Logset Type buttons

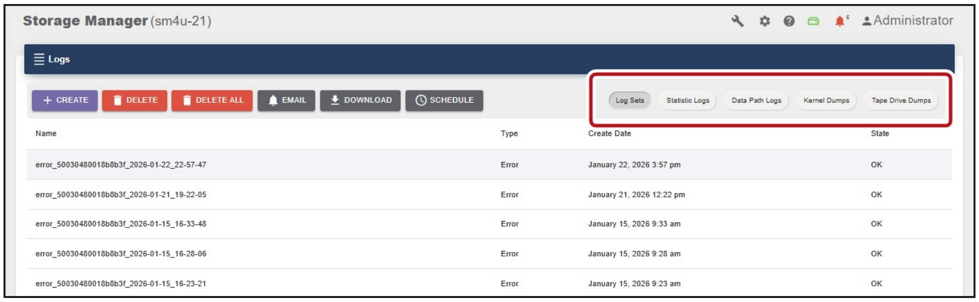
3. Select the logset you want to download and click **Download**. The Download Logset screen displays (not shown).
4. On the Download Logset screen, click **Submit**.

Delete Log Sets

Delete a Single Log Set

Use the instructions in this section to delete a single log set.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Logs**. The Logs screen displays.
2. Use the **logset type** buttons in the upper-right to select the type of logs to display.



Name	Type	Create Date	State
error_50030480018b8b3f_2026-01-22_22-57-47	Error	January 22, 2026 3:57 pm	OK
error_50030480018b8b3f_2026-01-21_19-22-05	Error	January 21, 2026 12:22 pm	OK
error_50030480018b8b3f_2026-01-15_16-33-48	Error	January 15, 2026 9:33 am	OK
error_50030480018b8b3f_2026-01-15_16-28-06	Error	January 15, 2026 9:28 am	OK
error_50030480018b8b3f_2026-01-15_16-23-21	Error	January 15, 2026 9:23 am	OK

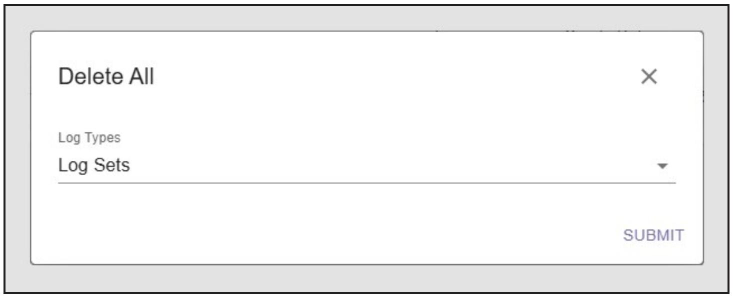
Figure 279 The Logs screen - Logset Type buttons

3. Select the logset you want to delete and click **Delete**. The Delete Log screen displays (not shown)
4. On the Delete Log screen, click **Submit**.

Delete All Log Set of a Specified Type

Use the instructions in this section to delete all log sets of a specified type of log.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Logs**. The Logs screen displays.
2. Click **Delete All**. The Delete All dialog box displays.



Delete All

Log Types: Log Sets

Figure 280 The Delete All dialog box.

3. Use the **Log Types** drop-down menu to select which type of logs to delete.
4. Click **Submit**.

Spectra Logic Technical Support

Spectra Logic Technical Support provides a worldwide service and maintenance structure.

Before Contacting Support

If you have a problem with your BlackPearl Object Gateway, use the information in this section to attempt to resolve the problem.

System Messages

If you are encountering problems, review any System Messages that were posted (see Monitor the Gateway Hardware on page 246) and take any action described in the message(s).

Product Support

The Spectra Logic Technical Support portal at *support.spectralogic.com* provides information about the most current version of the BlackPearl software, and additional service and support tools. After logging into the support portal, check the options under the **Support by Product** and **Knowledge Base** tabs for additional troubleshooting information.

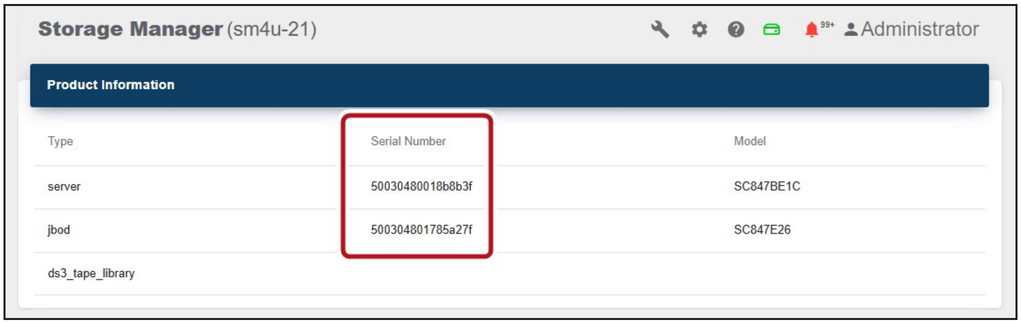
Contact Support

If the problem persists, open a support ticket (see Spectra Logic Technical Support above).

Determine the Gateway Serial Number

If you have more than one BlackPearl Object Gateway, it is necessary to determine the serial number of the Gateway before contacting Spectra Logic Technical Support. Use the following steps to determine the Gateway serial number.

1. Use the toolbar in the upper-right to select **Help & Support (question mark icon) > About**.
2. The Gateway serial number is listed in the Product Information pane.



Product Information

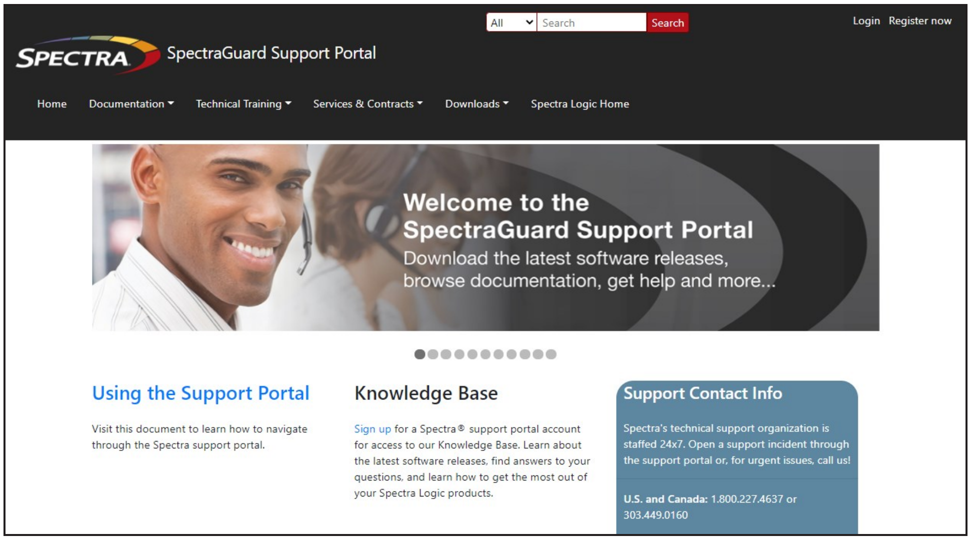
Type	Serial Number	Model
server	50030480018b8b3f	SC847BE1C
jbod	500304801785a27f	SC847E26
ds3_tape_library		

Figure 281 The Product Information screen - Serial Number column.

Opening a Support Ticket

You can open a support incident using the Spectra Logic Technical Support portal or telephone.

Search for Help Online



Welcome to the SpectraGuard Support Portal

Download the latest software releases, browse documentation, get help and more...

Using the Support Portal

Visit this document to learn how to navigate through the Spectra support portal.

Knowledge Base

Sign up for a Spectra® support portal account for access to our Knowledge Base. Learn about the latest software releases, find answers to your questions, and learn how to get the most out of your Spectra Logic products.

Support Contact Info

Spectra's technical support organization is staffed 24x7. Open a support incident through the support portal or, for urgent issues, call us!

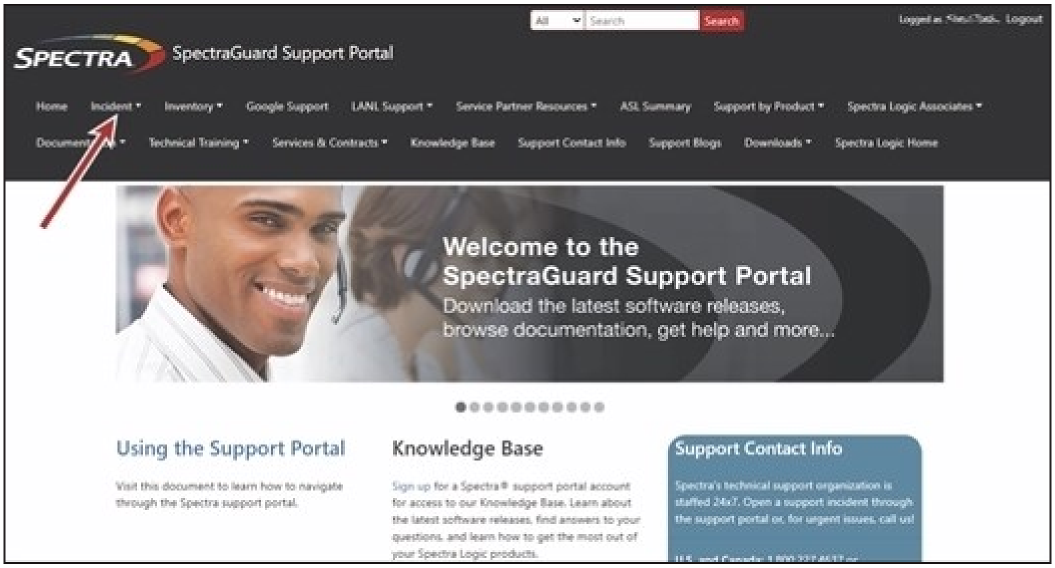
U.S. and Canada: 1.800.227.4637 or 303.449.0160

Figure 282 The Spectra Logic Technical Support portal home page.

1. Make notes about the problem, including what happened just before the problem occurred.
2. Gather the following information:
   - Your Spectra Logic customer number
   - Company name, contact name, phone number, and email address
   - The library serial number (see Determine the Gateway Serial Number on the previous page)
   - Type of host system being used
   - Type and version of host operating system being used
   - Type and version of host storage management software being used
3. If necessary, log in to the Support Portal by clicking **Login**, enter your **email address** and **password**, and click **Log in**.

Note: See Access the Technical Support Portal on page 395 if you have not previously created an account on the Technical Support portal.

4. From any page, select **Incident>Incidents & Inventory**.



Welcome to the SpectraGuard Support Portal

Download the latest software releases, browse documentation, get help and more...

Using the Support Portal

Visit this document to learn how to navigate through the Spectra support portal.

Knowledge Base

Sign up for a Spectra® support portal account for access to our Knowledge Base. Learn about the latest software releases, find answers to your questions, and learn how to get the most out of your Spectra Logic products.

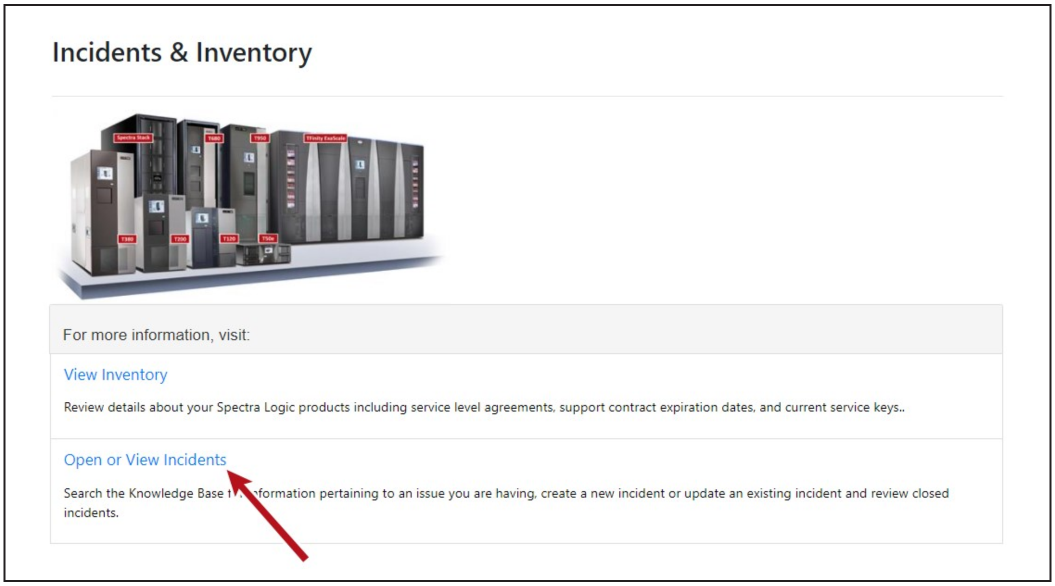
Support Contact Info

Spectra's technical support organization is staffed 24x7. Open a support incident through the support portal or, for urgent issues, call us!

U.S. and Canada: 1.800.227.4637 or

Figure 283 Select **Incidents > Incidents & Inventory**.

5. Select **Open or View Incidents**.



Incidents & Inventory

For more information, visit:

View Inventory

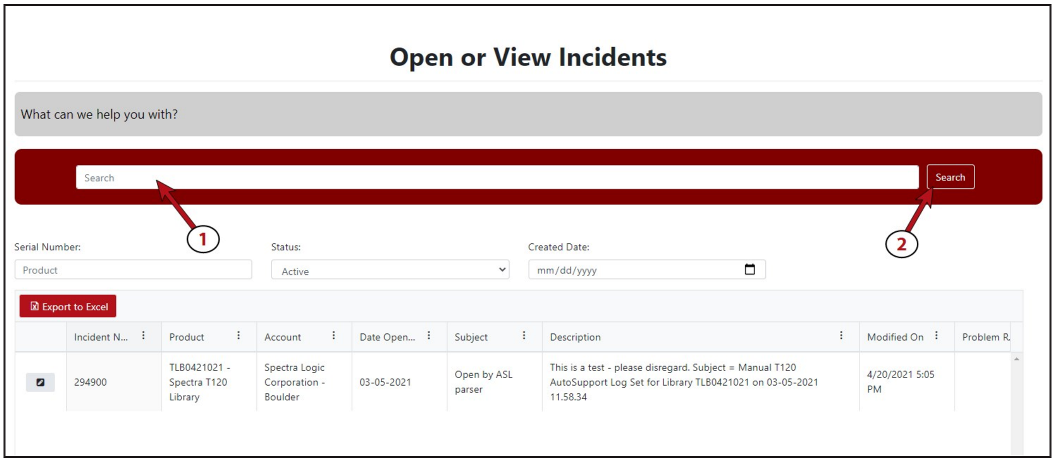
Review details about your Spectra Logic products including service level agreements, support contract expiration dates, and current service keys..

Open or View Incidents

Search the Knowledge Base for information pertaining to an issue you are having, create a new incident or update an existing incident and review closed incidents.

Figure 284 Select **Open or View Incidents**.

6. In the Search dialog box, enter a term or phrase about your problem (**1**) and click **Search** (**2**).



Open or View Incidents

What can we help you with?

Search: Search

Serial Number: Product

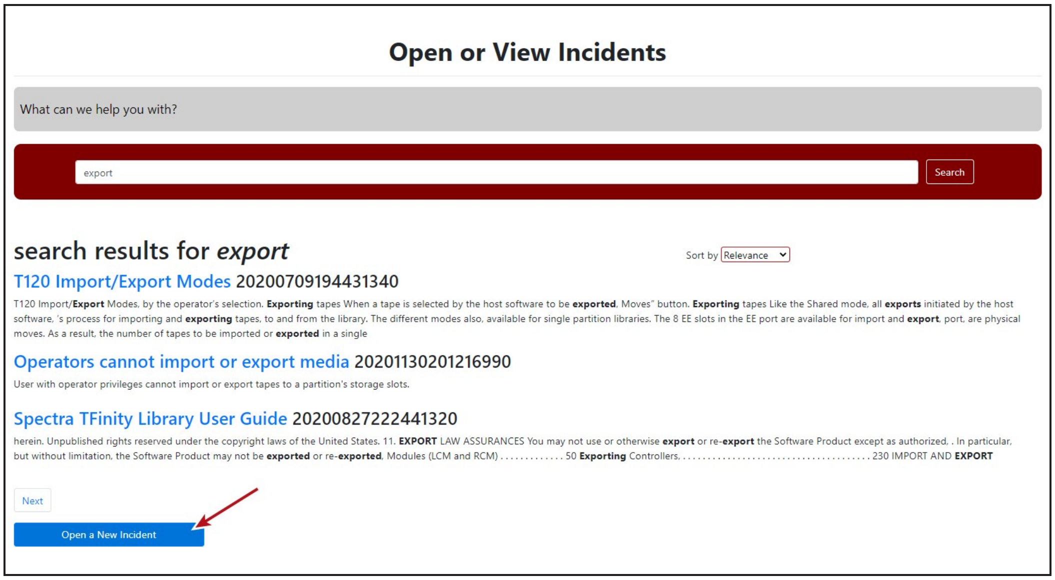
Status: Active

Created Date: mm/dd/yyyy

	Incident N...	Product	Account	Date Open...	Subject	Description	Modified On	Problem R.
	294900	TLB0421021 - Spectra T120 Library	Spectra Logic Corporation - Boulder	03-05-2021	Open by ASL parser	This is a test - please disregard. Subject = Manual T120 AutoSupport Log Set for Library TLB0421021 on 03-05-2021 11.58.34	4/20/2021 5:05 PM	

Figure 285 Enter a search phrase and click **Search**.

7. If the search does not provide an answer, click **Open a New Incident**.



Open or View Incidents

What can we help you with?

export

search results for *export*

Sort by Relevance

T120 Import/Export Modes 20200709194431340

T120 Import/**Export** Modes, by the operator's selection. **Exporting** tapes When a tape is selected by the host software to be **exported**, Moves" button. **Exporting** tapes Like the Shared mode, all **exports** initiated by the host software, 's process for importing and **exporting** tapes, to and from the library. The different modes also, available for single partition libraries. The 8 EE slots in the EE port are available for import and **export**, port, are physical moves. As a result, the number of tapes to be imported or **exported** in a single

Operators cannot import or export media 20201130201216990

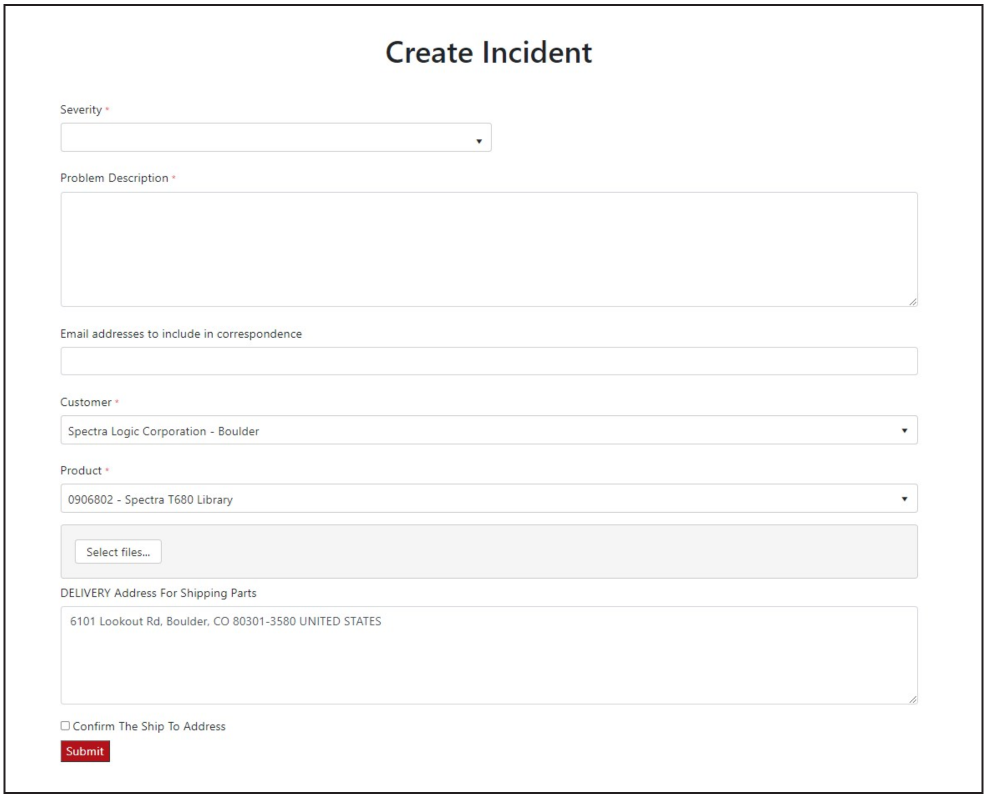
User with operator privileges cannot import or export tapes to a partition's storage slots.

Spectra TFinity Library User Guide 20200827222441320

herein. Unpublished rights reserved under the copyright laws of the United States. 11. **EXPORT** LAW ASSURANCES You may not use or otherwise **export** or re-**export** the Software Product except as authorized, . In particular, but without limitation, the Software Product may not be **exported** or re-**exported**, Modules (LCM and RCM) . . . . 50 **Exporting** Controllers, ... 230 IMPORT AND **EXPORT**

Figure 286 Click **Open a New Incident**.

8. On the Create Incident page, enter the requested information providing as much detail as possible. When you are finished, click **Submit**.



Create Incident

Severity *

Problem Description *

Email addresses to include in correspondence

Customer *

Spectra Logic Corporation - Boulder

Product *

0906802 - Spectra T680 Library

Select files...

DELIVERY Address For Shipping Parts

6101 Lookout Rd, Boulder, CO 80301-3580 UNITED STATES

□ Confirm The Ship To Address

Submit

Figure 287 Enter information about your incident and click **Submit**.

Submit an Incident Online

1. Make notes about the problem, including what happened just before the problem occurred.
2. Gather the following information:

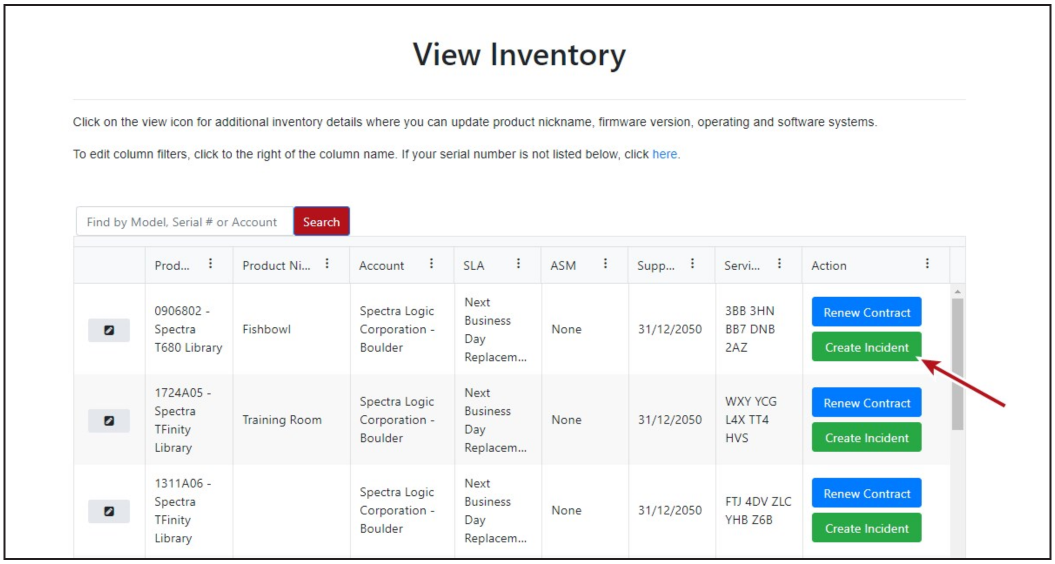
- Your Spectra Logic customer number
- Company name, contact name, phone number, and email address
- The library serial number (see Determine the Gateway Serial Number on page 388)
- Type of host system being used
- Type and version of host operating system being used
- Type and version of host storage management software being used

3. If necessary, log in to the Support Portal by clicking **Login**, enter your **email address** and **password**, and click **Log in**.

Note: See Access the Technical Support Portal on page 395 if you have not previously created an account on the Technical Support portal.

4. From any page, select **Inventory>My Inventory**.

5. Locate the row of the product for which you want to submit an incident and click **Create Incident**.



View Inventory

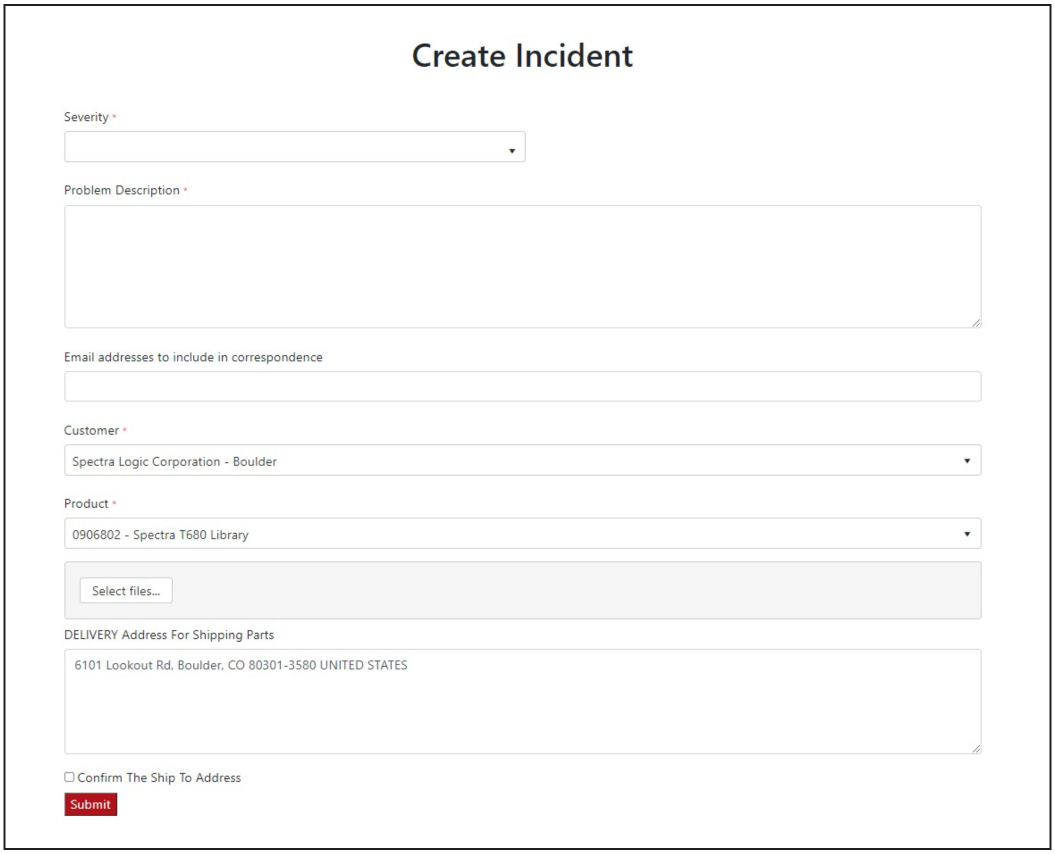
Click on the view icon for additional inventory details where you can update product nickname, firmware version, operating and software systems.

To edit column filters, click to the right of the column name. If your serial number is not listed below, click here.

	Prod...	Product Ni...	Account	SLA	ASM	Supp...	Servi...	Action
	0906802 - Spectra T680 Library	Fishbowl	Spectra Logic Corporation - Boulder	Next Business Day Replacem...	None	31/12/2050	3BB 3HN BB7 DNB 2AZ	Renew Contract Create Incident
	1724A05 - Spectra TFinity Library	Training Room	Spectra Logic Corporation - Boulder	Next Business Day Replacem...	None	31/12/2050	WXY YCG L4X TT4 HVS	Renew Contract Create Incident
	1311A06 - Spectra TFinity Library		Spectra Logic Corporation - Boulder	Next Business Day Replacem...	None	31/12/2050	FTJ 4DV ZLC YHB Z6B	Renew Contract Create Incident

Figure 288 Click **Create Incident**.

6. On the reate Incident page, enter the requested information providing as much detail as possible. When you are finished, click **Submit**.



Create Incident

Severity *

Problem Description *

Email addresses to include in correspondence

Customer *

Spectra Logic Corporation - Boulder

Product *

0906802 - Spectra T680 Library

DELIVERY Address For Shipping Parts

6101 Lookout Rd, Boulder, CO 80301-3580 UNITED STATES

□ Confirm The Ship To Address

Figure 289 Enter information about your incident and click **Submit**.

Submit an Incident by Phone

Contact Spectra Logic Technical Support by phone using the information below.

<table>
<tr><th colspan="2">Spectra Logic Technical Support</th></tr>
<tr><td colspan="2"><b>Technical Support Portal:</b> <i>support.spectralogic.com</i></td></tr>
<tr><td><b>United States and Canada</b>
<b>Phone:</b>
<b>Toll free US and Canada:</b> 1.800.227.4637
<b>International:</b> 1.303.449.0160</td><td><b>Europe, Middle East, Africa</b>
<b>Phone:</b> 44 (0) 870.112.2185
<b>Deutsch Sprechende Kunden</b>
<b>Phone:</b> 49 (0) 6028.9796.507</td></tr>
<tr><td colspan="2"><b>Additional international numbers available at</b> <i>support.spectralogic.com/home</i>
<b>If you have a Spectra Logic Portal account, please log in for country-specific numbers at</b> <i>support.spectralogic.com/support-contact-info</i></td></tr>
</table>

ACCESS THE TECHNICAL SUPPORT PORTAL

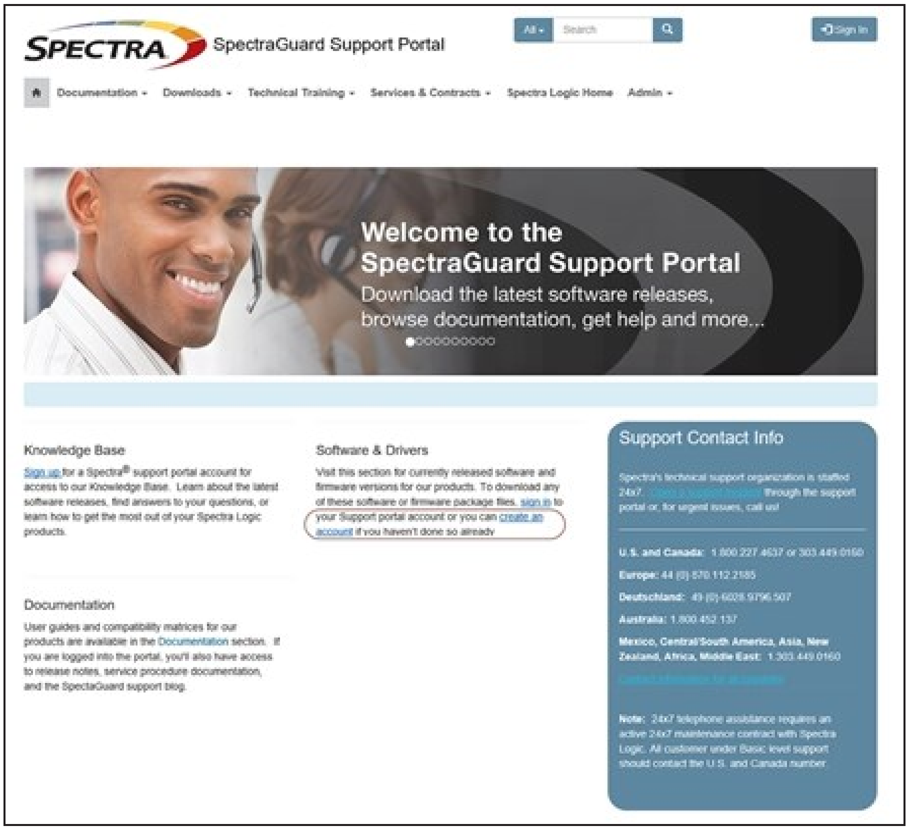
The Spectra Logic Technical Support portal provides access to the Knowledge Base, the current version of BlackPearl software for the Gateway, and additional service and support tools. You can also open or update a support incident and upload log files.

Create an Account

Access to User Guides and compatibility matrices does not require you to create an account. You must create a user account and log in to access Release Notes or repair documents, to download the latest version of BlackPearl software, or to open a support ticket.

> **Note:** If you own multiple Spectra Logic products, the serial numbers for all products are associated with your account. If you do not see the serial numbers for all of your products when you log in, contact Technical Support (see Contacting Spectra Logic on page 7).

1. Access the Technical Support portal login page at *support.spectralogic.com*.
2. On the home page, click **create an account**.



Welcome to the SpectraGuard Support Portal

Download the latest software releases, browse documentation, get help and more...

Knowledge Base

Sign up for a Spectra® support portal account for access to our Knowledge Base. Learn about the latest software releases, find answers to your questions, or learn how to get the most out of your Spectra Logic products.

Software & Drivers

Visit this section for currently released software and firmware versions for our products. To download any of these software or firmware package files, sign in to your Support portal account or you can create an account if you haven't done so already

Documentation

User guides and compatibility matrices for our products are available in the Documentation section. If you are logged into the portal, you'll also have access to release notes, service procedure documentation, and the SpectaGuard support blog.

Support Contact Info

Spectra's technical support organization is staffed 24x7. [illegible] through the support portal or, for urgent issues, call us!

U.S. and Canada: 1.800.227.4637 or 303.449.0160

Europe: 44 (0) 870.112.2185

Deutschland: 49 (0) 6028.9796.507

Australia: 1.800.452.137

Mexico, Central/South America, Asia, New Zealand, Africa, Middle East: 1.303.449.0160

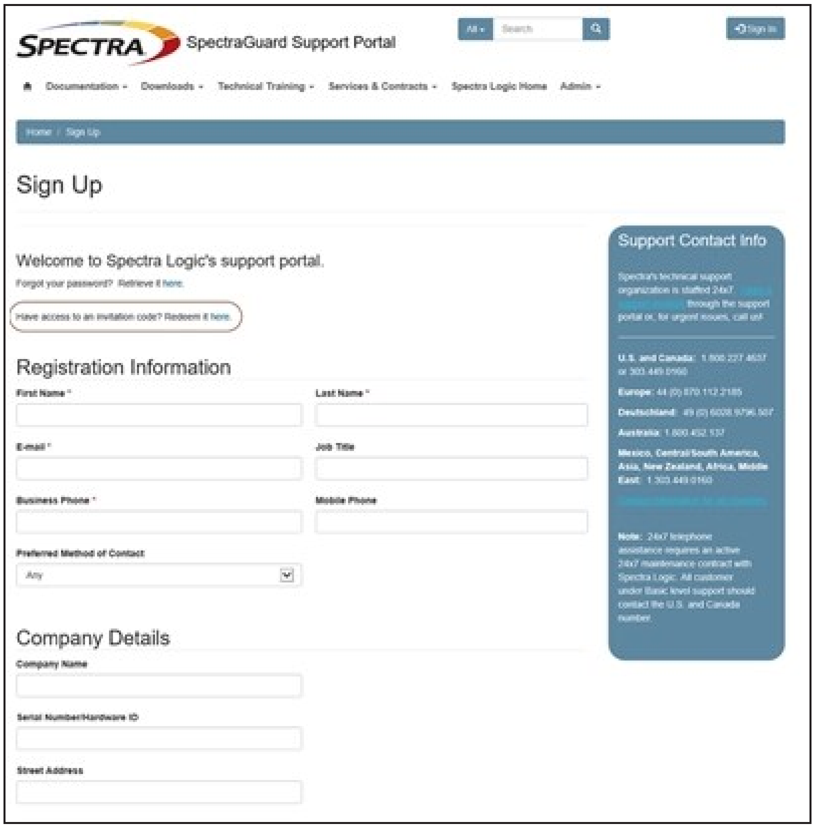
[illegible]

Note: 24x7 telephone assistance requires an active 24x7 maintenance contract with Spectra Logic. All customer under Basic level support should contact the U.S. and Canada number

Figure 290 The Spectra Logic Technical Support portal home page.

3. Enter your registration information. Your account is automatically associated with the serial numbers of all Spectra Logic products owned by your site.

- If you have an invitation, follow the link and enter the invitation code.



Sign Up

Welcome to Spectra Logic's support portal.

Forgot your password? Retrieve it here.

Have access to an invitation code? Redeem it here.

Registration Information

First Name *

Last Name *

E-mail *

Job Title

Business Phone *

Mobile Phone

Preferred Method of Contact

Any

Company Details

Company Name

Serial Number/Hardware ID

Street Address

Support Contact Info

Spectra's technical support organization is staffed 24x7. [illegible] through the support portal or, for urgent issues, call us!

U.S. and Canada: 1.800.227.4637 or 303.449.0160

Europe: 44 (0) 870.112.2185

Deutschland: 49 (0) 6028.9796.507

Australia: 1.800.452.137

Mexico, Central/South America, Asia, New Zealand, Africa, Middle East: 1.303.449.0160

[illegible]

Note: 24x7 telephone assistance requires an active 24x7 maintenance contract with Spectra Logic. All customer under Basic level support should contact the U.S. and Canada number.

Figure 291 Follow the link to enter your invitation code or enter your registration information.

- If you do not have an invitation, enter the requested information to create your account. When you are finished, click **Sign Up**.

When the account is approved, you receive an email with a link to setup your initial password. Use your email address and the password provided in the email to log in to your account. After you log in, you can change your password if desired.

Log Into the Portal

Access the Technical Support portal login page at *support.spectralogic.com*. Use your email address and password to log into the Technical Support Portal.

Remote Support

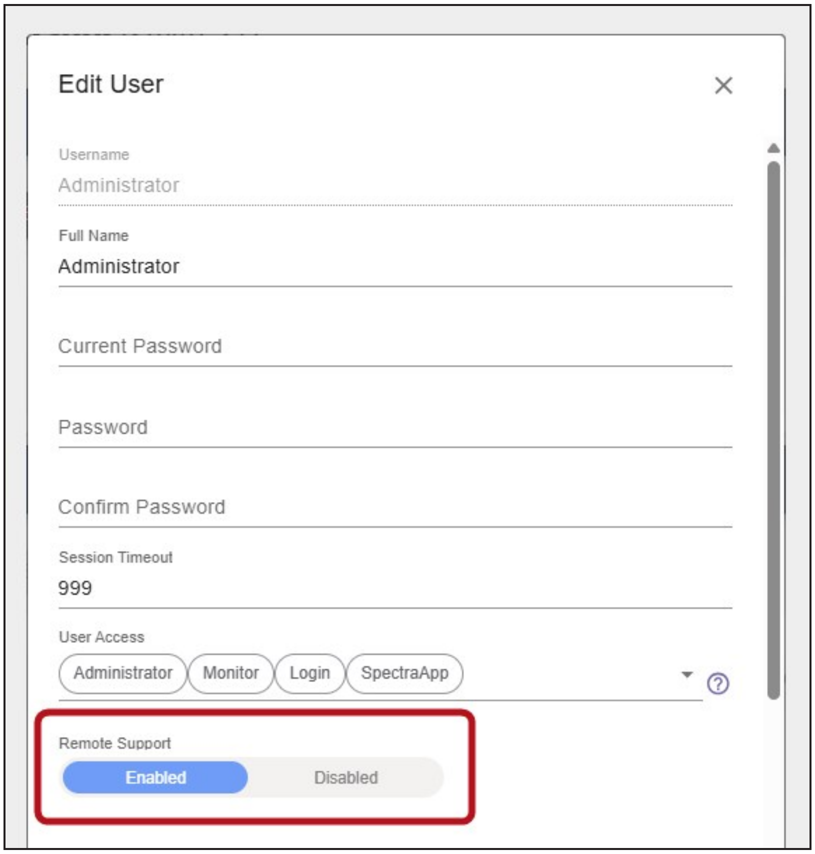
Remote Support is an option that allows Spectra Logic Technical Support personnel to access the root console of the Gateway. This option is for troubleshooting purposes only.

Enabling Remote Support

1. Enter the Remote Support activation key as described in Manually Enter Activation Keys on page 364.

Note: The Remote Support activation key is only valid for 24 hours. When the key expires, remote access is automatically disabled.

2. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.
3. Select the **Administrator** account and then click **Edit**. The Edit User dialog box displays.



Edit User

Username
Administrator

Full Name
Administrator

Current Password

Password

Confirm Password

Session Timeout
999

User Access
Administrator Monitor Login SpectraApp

Remote Support
Enabled Disabled

Figure 292 The Edit User dialog box - Remote Support slider.

4. Use the **Remote Support** slider to select **Enabled**.

Note: The Enable Remote Support checkbox does not display until you enter a Remote Support activation key.

5. Click **Submit** (not pictured).

IMPORTANT After Spectra Logic Technical Support informs you that they no longer require root access to the Gateway, you should disable Remote Support to prevent any potential unauthorized access.

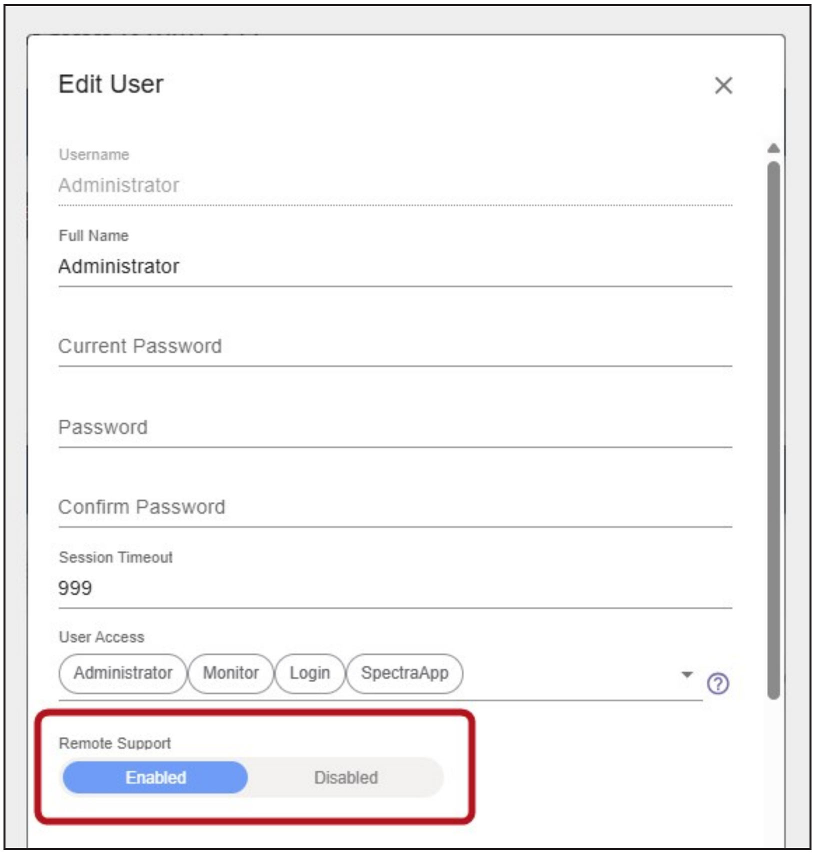
The Remote Support activation key is only valid for 24 hours. When the key expires, remote access is automatically disabled.

Disabling Remote Support

Use the instruction in this section to disable Remote Support.

Note: The Remote Support activation key is only valid for 24 hours. When the key expires, remote access is automatically disabled.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.
2. Select the **Administrator** account and then click **Edit**. The Edit User dialog box displays.



Edit User

Username
Administrator

Full Name
Administrator

Current Password

Password

Confirm Password

Session Timeout
999

User Access
Administrator Monitor Login SpectraApp

Remote Support
Enabled Disabled

Figure 293 The Edit User dialog box - Remote Support slider.

3. Use the **Remote Support** slider to select **Disabled**.
4. Click **Submit** (not pictured).

CHAPTER 17 - FREQUENTLY ASKED QUESTIONS (FAQ)

BlackPearl Cache

How is Cache Used and Allocated?

The BlackPearl cache is allocated physical storage on either HDDs or SSDs installed in the Gateway. The cache functions as a transient location for all data transferred to the BlackPearl Object Gateway from a client, or transferred from tape storage to the BlackPearl Object Gateway.

The capacity available for cache is managed by the BlackPearl data planner, where active jobs reserve various amounts of cache capacity known as 'chunks'. Up to 85% of the cache can be reserved for jobs with a job priority level of 'high', or less. The remaining 15% of cache capacity is only available for jobs with a priority level of 'urgent'.

The cache is managed by chunk allocations. The chunk size can vary. When writing data to cache destined for tape storage, or restoring data from tape storage to the BlackPearl Object Gateway, the chunk size is typically 2% of the capacity of a single tape cartridge. If the total job size is less than that amount, the chunk size reduces in size to match the job size. An internal job, such as IOM migration, can also reserve cache capacity. If needed, internal jobs can reserve all of the available cache capacity based on job priority, which may impact other jobs, occasionally preventing or delaying them from accessing cache chunks. If IOM is impacting normal production use, the Schedule IOM feature in the Amazon compatible S3 service allows you to set a schedule to minimize downtime.

Why Does the BlackPearl User Interface Display 80% Cache Usage?

The Cache Used capacity graph on the user interface dashboard now displays only the actual capacity used by active jobs. It no longer displays the capacity of objects that are available in cache for a GET job. This information is available by examining the used capacity cache pool details screen, which is accessed from the Jobs screen by viewing the details of the pool labeled "BlackPearl_Cache".

TAPE PARTITIONS

How Does a User Upgrade to Later Generations of Media in the Same Tape Library?

The method used to add a newer generation of tape media depends on if the new and existing media are compatible, and if the existing tape drives are to be used for migration. If a media migration is required, keeping the older tape drives may increase performance during the migration.

A newer generation of media and drives can be added to an existing tape partition, if it is a one generation advancement. For example, adding LTO-7 media and drives into a library originally purchased with LTO-6 drives and media.

If the existing media is compatible with the new drives, the tape partition is upgraded to the new drive generation, and the old drives are removed.

However, if the old media **cannot** be used (either read from or written to) with the newer drives (for example, LTO-6 media cannot be read by LTO-8 tape drives) then a second tape partition in the library is required to support the new tape drives and media. The new tape partition can be in the same tape library, or a separate tape library.

After completing changes to the tape library, add the new tape media into existing storage domain(s), and ensure the newer media generation has a higher write preference than the older generation. For example, set the write preference on LTO-7 media to "normal", then set LTO-6 media to a lower setting such as "never". If a data migration to the newer higher-density media is desired, then exclude the older storage domain member media, which then forces IOM migration for all data within that individual storage domain. See Migration for more details.

What Happens When a Tape Partition is Placed in Standby/Quiesced?

After an administrator issues a tape partition quiesce command, the BlackPearl Object Gateway stops any new tape drive tasks for that partition. Any existing tasks are allowed to complete, which may take 30 minutes or more. After the tape task is complete for a tape drive, the drive is automatically unloaded and the tape is returned to its previous slot. While the tape partition is in standby, the BlackPearl Object Gateway does not issue any internal tape task commands. The Amazon compatible S3 service stays enabled and active while the tape partition is in standby, which allows any DS3 applications, such as the Eon Browser or Spectra StorCycle application, to write data into, or to request data from the BlackPearl Object Gateway. The write jobs go into the BlackPearl cache and wait until the tape partition is ready. For a restore or GET job, if the requested data is only available on tape, the job request returns a status that the tape partition is offline, and includes the tape barcodes required for the job.

What Happens When a Tape Partition is Re-Activated?

While the partition is in standby, the BlackPearl Object Gateway monitors the tape partition robotic exporter for any updates or changes, such as a change in the library inventory. When the tape partition comes out of standby and is activated, the BlackPearl Object Gateway automatically begins to use the partition as normal. With BlackPearl OS 5.2 or earlier, if there was an inventory change in the tape library while in standby, the BlackPearl Object Gateway could react by re-inspecting all tapes in the library. Starting with BlackPearl OS 5.3, the Gateway no longer re-inspects tapes when there is an inventory change while the partition is in standby if the Amazon compatible S3 service is set to "Never Inspect".

How do I Change the Tape Library Used by the BlackPearl Object Gateway While Minimizing the Impact, Management Time, and System Downtime?

If you plan to upgrade the library used by the BlackPearl Object Gateway, for example change from a Spectra T120 to a Spectra Stack, it is advised to work with Spectra Logic Technical Support before changing the tape partition used by the BlackPearl Object Gateway, and before moving any tapes to the new tape library or partition.

IMPORTANT Create a manual database backup before changing to a new tape library or partition.

Tape Media

How Does a User Know if Tape Media is Running Out of Space?

The available tape media capacity should be monitored per the daily operation and maintenance procedures by using the BlackPearl dashboard to ensure that adequate media is available for BlackPearl Object Gateway to use for planned archive jobs, or to maintain a minimum available capacity per company policy.

Can Data be Overwritten on Existing Tapes?

With a full administrator login and multiple confirmation screens, any tape can be manually reformatted and put back into the blank media pool for use by the BlackPearl Object Gateway. For example, older tapes with expired data.

Users with adequate permissions for a bucket could also use the BlackPearl user interface, a BlackPearl client, or an Amazon compatible S3 browser tool like the Spectra Eon Browser to delete objects from a bucket. When all objects on a tape have been deleted, the tape is automatically reformatted and put back into the blank media pool.

CAUTION Deleting objects or buckets is a manual process and extreme caution should be exercised to ensure that only data that is no longer needed is deleted.

Can WORM Media be Used With the BlackPearl Object Gateway?

The BlackPearl Object Gateway is not compatible with WORM (Write Once-Read Many) media. If the BlackPearl Object Gateway is configured to transfer data to tape, make sure the partitions configured for use by the BlackPearl Object Gateway do not contain WORM media.

TAPE MEDIA IMPORT

How Does a User Know What Tape Cartridge(s) to Import in Response to a GET Request for Objects on Exported Media?

If a GET job requests an object on a tape cartridge that was previously exported, both system messages in the BlackPearl user interface, and emails sent to a system administrator, list the required tapes by barcode.

The system Administrator **must** be configured to receive emails with both Informational and Warning message severity to receive notifications when tape is media requested.

Below are examples of both an email and a system messages requesting tape cartridges to be imported.

Example Email:

> Automated notification from *BlackPearl system name* (*management port IP address, management port MAC address*), your Spectra Logic BlackPearl.
>
> The following message has been generated. This could indicate a problem with your system.
>
> **Severity:** Warning
>
> **Description:** Tape Partition Notification
>
> **Details:** The following tapes need to be imported/onlined: LTO8020L8 (Export Label: "Auto-exported since storage domain is autoExportUponJobCompletion"). The following user requested these tapes: Administrator.

Example System Message:

> Failed to create job
>
> The following tapes need to be imported/onlined: LTO8020L8 (Export Label: "Auto-exported since storage domain is autoExportUponJobCompletion"). The following user requested these tapes: Administrator.

Once you have retrieved the tapes referenced in the email and system message, see Import Tapes on page 313.

TAPE MEDIA EXPORT

A tape export strategy must be considered as part of a data policy. For information about the default data policies and options available to customize data policies, see see the *Advanced Bucket Management Guide*. For additional information about exporting and importing tapes, see Working with Tape Libraries and Media on page 287.

Spectra recommends keeping at least one copy of all archived data in the library at all times. Spectra Logic tape libraries can be easily upgraded by purchasing more slot licenses, or, if the slots become completely full, upgrading the library itself to one with more slots using the exclusive Spectra TranScale technology.

A tape library user or administrator may decide to export media cartridges from a tape library for any of the reasons described below:

- **Exporting a copy for off-site disaster recovery:** The BlackPearl Object Gateway allows a user to make multiple copies of data automatically. A typical use case is to create a "tape first copy" that is intended to be left in the library for easy retrieval as well as an "export copy" intended to be removed from the library once full for archival at an alternate site for safety. See the *Advanced Bucket Management Guide* for information on setting up multiple copies and exporting a copy, and the *Tape Library User Guide* for details on the physical process of exporting and importing tapes into the library.
- **Exporting a copy of data for transfer to another location:** In some work flows, a user exports a tape or an entire bucket to transfer the data to another facility. Individual tapes or entire buckets can be exported manually using the BlackPearl user interface (see Export Tapes on page 341).
- **Exporting tapes to free up space in the library:** Some work flows and budgets, require older or unused media to be exported, making it not readily available. Individual tapes or entire buckets can be exported manually using the BlackPearl user interface (see Export Tapes on page 341).

"Export" has multiple definitions within the Gateway:

- From the BlackPearl Object Gateway's perspective, export means that a tape has been marked as exported in the BlackPearl database and an instruction has been given to the tape library to move the tape for export from the library.

Note: You cannot export a tape that is currently in use.

- From a tape library perspective, export indicates the physical process of exporting tapes from the library.

What Happens if a User Exports a Tape From the Library Before Exporting the Tape in the BlackPearl User Interface?

Tape media should not be exported from the tape library without first exporting the tapes in the BlackPearl user interface.

If you suspect that a tape was exported from the library without being exported from the BlackPearl Object Gateway, in the BlackPearl user interface, select **Status > Tape Management**. The Tape Management screen displays. Re-import the tape with the status “Managed Not In Inventory”.

See the *Tape Library User Guide* for instructions for importing the tape into a Spectra Logic tape library.

Once the tape is re-imported into the tape library, use the BlackPearl user interface to Online the tape as described in Import Tapes on page 313. Once the tape has a status of Online, the Gateway inspects the tape and uses it as needed.

If a tape is exported from the tape library and is queued for a job, the client displays an error. If the client error message does not display the barcode of the tape, in the BlackPearl user interface, select **Status > Messages**, or click the **Messages** link on the status bar, to display the Messages screen. Inspect the messages to determine the barcode of the missing tape. See the *Tape Library User Guide* for instructions for importing the tape into a Spectra Logic tape library. Once the tape is re-imported, the Gateway inspects the tape and uses it as needed.

How Does a User Configure Their T50e or T120 Library to Support Exporting Tapes From the BlackPearl Object Gateway?

The BlackPearl export function allows you to export tapes from the BlackPearl user interface, which are then moved to the Entry/Exit port on the tape library.

In order to use the BlackPearl export function on a T50e or T120 library, you must configure a single partition and select **Standard** as the partition’s Entry/Exit Port Mode. If you configure the partition to use either the Shared or Queued Eject mode, or you configure more than one partition on your library, exports from the BlackPearl Object Gateway fail.

See “Configuring and Managing Partitions” in the *T50e Library User Guide*, or “Partition Management” in the *T120 Library User Guide* for instructions on configuring a partition to use the Standard mode for the Entry/Exit port.

Note: The Spectra Stack, T200, T380, T680, T950 and TFinity libraries do not have limitations on the partition count or Entry/Exit mode for BlackPearl tape export.

TAPE DRIVE CLEANING

How Does a User Know Their Cleaning Media is Expired?

Cleaning media expires after a specified number of uses to ensure that drives are thoroughly cleaned. The BlackPearl Object Gateway does not track cleaning media health. Only the tape library tracks cleaning media health. When a piece of cleaning media expires, a message is posted to the System Messages screen in the tape library's BlueScale interface.

If your cleaning media are LTO or TS11*xx* tapes with MLM enabled, you can proactively monitor the status of cleaning media through the tape library's BlueScale interface.

Notes:

- If your cleaning tapes are not MLM-enabled, you cannot use MLM to proactively monitor cleaning media. You must use the messages posted to the System Messages screen to determine when a piece of cleaning media expires.
- If there are no cleaning tapes with cleans remaining, see your *Related Information*for instructions on exchanging expired cleaning media.

Use the instructions in this section to determine if your cleaning media is expired or about to expire.

Spectra Logic T120 and larger libraries

1. Log in to the BlueScale interface as described in your *Tape Library User Guide*.
2. Select **General > Media Lifecycle Management**. The MLM Report screen displays.
3. Select the partition from the **Partition** drop-down list and **Cleans Remaining** from the **Report** drop-down list.
4. Click **Go**. The screen re-displays to show the number of cleans remaining for all cleaning cartridges present in the partition. Confirm at least one tape still has cleans remaining.

Spectra Logic T50e library

1. Log in to the BlueScale interface as described in the *Spectra T50e Library User Guide.*
2. Click **MENU**, then select **General > MLM**. The MLM Reports screen displays.
3. Select **Total Library** from the **Partition** drop-down list and **Cleans Remaining** from the **Report** drop-down list.
4. Click **Go**. The MLM Reports screen refreshes to display the Cleanings Remaining report with a list of the barcode labels for all cleaning tapes in the selected location and the number of cleanings remaining for each tape.

How Does a User Use Cleaning Media in a T50e or T120 Library That Does Not Have a Cleaning Partition?

In order to use the BlackPearl export function on a T50e or T120 library, the library can only have a single data partition. In order for drives to be automatically cleaned, you must store cleaning media in the single data partition on your T50e or T120 library.

When the BlackPearl Object Gateway detects cleaning media in the data partition, the Gateway automatically cleans drives when cleaning is requested by a tape drive.

TAPE DRIVE TEST

How Does a User Test a Tape Drive in a Spectra Logic Library?

If you suspect a tape drive is bad, you can test the tape drive using one of the methods below:

Using the BlackPearl User Interface

The preferred method to test the tape drive is to use the steps described in Test Tape Drive on page 298.

Using a Tape Library User Interface

The process below describes using the legacy BlackPearl user interface and a BlueScale tape library to test a tape drive.

IMPORTANT Only use the process below if you cannot use the BlackPearl user interface to test a tape drive.

1. Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with "/legacy". For example:

   https://*ipaddress*/legacy

2. In the BlackPearl management interface, select **Configuration > Advanced Bucket Management > Storage & Policy Management**.
3. In the Tape Partitions heading, **double-click** the partition containing the drive you want to test.
4. Select the row of the drive, select **Action > Offline Tape Drive**, then click **Deactivate**.
5. Select **Action > Reserve Tape Drive**.
6. Use the **Reserved Task Type** drop-down menu to select **Maintenance** and then click **Save**. Once all jobs using the tape cartridge in the drive complete, the library ejects from the drive, and moves it to storage.
7. Use the tape library BlueScale user interface to edit the tape partition to remove the drive you want to test. See your tape library *User Guide* for instructions.

Note: Continue to see your tape library User Guide for the remainder of the test process.

8. Create a new partition with the drive to test as the only drive in the partition.
9. Import a scratch tape and a cleaning cartridge into the Entry/Exit port of the new partition.

10. Test the drive using the tape library MLM Drive Test feature.

11. After the drive test completes, delete the partition you created in Step .

- If the drive passed the drive test, edit the tape partition used by the BlackPearl Object Gateway to include the drive. In the BlackPearl management interface tape partition details screen, select the drive you tested and select **Online Tape Drive**.
- If the drive test failed, collect drive diagnostic logs as described in Collect and Download Drive Diagnostic Logs on page 300 and contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

Write to Tape Drive Test

How Does a User Test That Data is Being Written to Tape Media?

Use the steps below to confirm your BlackPearl Object Gateway is correctly configured to write data to tape media.

1. In the BlackPearl management interface, select **Configuration > Database Backup**.
2. On the Database Backup screen, select **Action > Start Immediate Backup**.
3. Click **Backup** to start the database backup process. Once the database backup is generated, the file is pushed to the BlackPearl cache.
4. On the Dashboard screen, in the Jobs pane, wait until a new job displays using the BlackPearl database backup bucket.
5. Once the job begins writing to cache, select **Status > S3 Jobs** to display the Amazon compatible Jobs screen.
6. On the Jobs screen, select **Action > Active Jobs**.
7. Monitor the database backup job and wait until the job no longer displays on the active job screen.
8. Select **Action > Canceled Jobs** and confirm the database backup job is in the list of canceled jobs.
9. Select **Configuration > Buckets**, then double-click the database backup bucket.
10. Select the database file created for the test and select **Action > Show Physical Placement**. The tape(s) used to store the backup file display.

BLACKPEARL DATABASE BACKUP

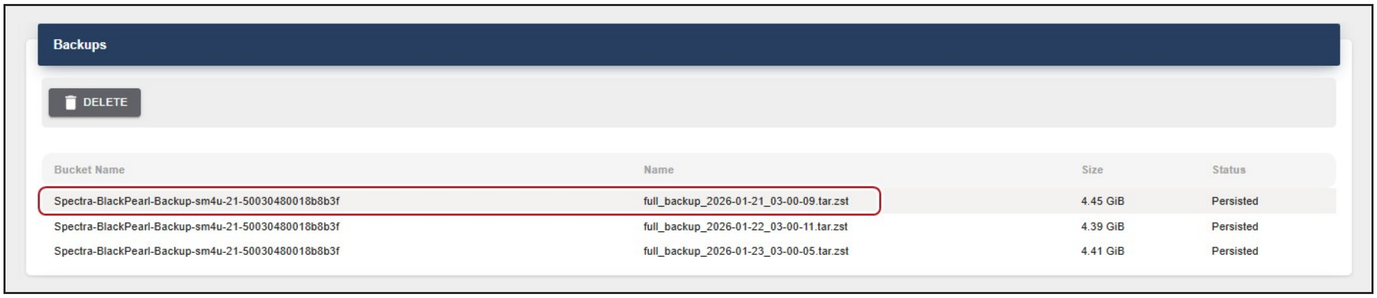
The BlackPearl database is contained on a set of flash (SSD) drives within BlackPearl Object Gateway. Information on every object stored by the Gateway is saved, including object name, policy, physical location (including which tape or disk location), and other information critical for search and retrieval of objects. While all of this information could be retrieved by allowing the Gateway to physically load and read every tape, this is a time consuming process and some bucket location information may be lost. If the database is lost, no data is lost, but retrieval becomes difficult.

Therefore, scheduling regular backups of the database is a best practice to ensure long term reliable operation. The BlackPearl user interface allows the administrator to set up regular and automatic database backups to both tape and disk, and also allows creation of an off site export copy. The default database backup schedule generates a backup once per day, and retains a maximum of two backups.

How Does a User Verify the Database Backup Schedule?

From the BlackPearl menu bar, select **Configuration (wrench icon) > Database Backup**. The Database Backup screen displays.

- In the Backup Schedule pane, view the configured **Schedule**.
- In the Backups pane, view the date code in the **Name** of the complete backups available to verify the most recent backups.



Bucket Name	Name	Size	Status
Spectra-BlackPearl-Backup-sm4u-21-50030480018b8b3f	full_backup_2026-01-21_03-00-09.tar.zst	4.45 GiB	Persisted
Spectra-BlackPearl-Backup-sm4u-21-50030480018b8b3f	full_backup_2026-01-22_03-00-11.tar.zst	4.39 GiB	Persisted
Spectra-BlackPearl-Backup-sm4u-21-50030480018b8b3f	full_backup_2026-01-23_03-00-05.tar.zst	4.41 GiB	Persisted

Figure 294 The Database Backup screen - Backups pane.

Note: See Database Backup on page 197 for more information.

How Does a User Create a Bucket Isolated Data Policy for the Database Backup Tapes?

Creating a bucket isolated data policy for your database backup tapes ensures that only the database backup bucket is present on a tape cartridge. This makes off-site archival of your database backup tapes easier. Use the instruction in this section to create a data policy with bucket isolation.

1. Follow the instructions in Create a Storage Domain on page 119 to create a new storage domain for the database backups.
2. Follow the instructions in Create a Data Policy on page 127 to create a new data policy for the database backups. It is helpful to use a name similar to “DataBaseBackup”. Make sure you select **Bucket Isolation** when assigning the storage domain created in Step 1 to the data policy.
3. Select **Configuration > Database Backup**. The Database Backup screen displays.
4. Select **Action > Edit Data Policy**. The Modify Data Policy window displays.
5. Use the **Data Policy to Use** drop-down menu to select the data policy you created in Step 2.

BlackPearl Disk Storage Data Retention

When a BlackPearl ABM data policy writes a copy of data to a storage domain that contains a disk partition, pool members from that disk partition get assigned to the storage domain as needed, similar to the way tapes get assigned from a tape partition to a storage domain. The BlackPearl Object Gateway then writes in parallel to all the disk pools assigned to the storage domain (even in capacity mode) in a round-robin fashion writing out different chunks to different pools.

Note: To allow for more pools allocated or assigned to a storage domain, either use performance mode, or if in capacity mode, wait until after the first pool is filled with data, causing the BlackPearl Object Gateway to assign another pool.

When a disk-based storage domain is configured in a temporary persistence rule, the configured Minimum Days to Retain sets the retention period. The BlackPearl Object Gateway only deletes data off that storage domain if the create date of an object is older than the retention policy. When an individual pool in the disk partition meets the configured watermark (by default 80%) the BlackPearl Object Gateway starts to delete objects with a create date older then the retention policy, starting with objects with the oldest last access date.

If the BlackPearl Object Gateway cannot delete data based on retention policy, it tries to assign another pool after the first pool is full (approximately 95% or 96%). If the Gateway cannot assign another disk pool, any jobs targeting the storage domain do not complete and the BlackPearl Object Gateway displays an error message indicating it cannot assign additional storage for that bucket/job.

A general best practice is to use standard isolation on the disk-based storage domain, and force the BlackPearl Object Gateway to allocate multiple disk pools into the storage domain. This both increases performance, and allows for more data to stay on disk after the retention period

For example, if there are 10 disk pools, one storage domain for disk, and no foreseen business requirements to isolate data on disk (using either bucket isolation or storage domain isolation) then force the BlackPearl Object Gateway to assign all 10 pools into the storage domain before production operations start. To do this, setup the storage domain in performance mode, and write data into the data policy containing the disk-based storage domain until all 10 pools are assigned to the storage domain. If there are no future plans to isolate disk storage, leaving the storage domain in performance mode is acceptable. Otherwise, as a safety precaution, change the storage domain to capacity mode write optimization, which in this use case retains the performance of performance mode. Even in capacity mode, the BlackPearl Object Gateway still writes to all 10 pools in parallel when there are lots of chunks flowing through the cache. Capacity mode just prevents BlackPearl from adding additional disk pools to the storage domain (until all 10 disk pools are full).

BlackPearl Component Hardware

How Does a User Know if a Component of the BlackPearl Object Gateway Has an Error?

During installation of the BlackPearl Object Gateway, users are configured to receive emails if the BlackPearl Object Gateway or the tape library issues a warning or error message. See “Configure Mail Users” in your *Tape Library User Guide* and Configure AutoSupport Mail Recipients on page 378 to verify or set up email recipients.

Use the information in the message emails, and the Messages screen in the BlackPearl user interface, and the Spectra Logic tape library’s BlueScale user interface, along with the Troubleshooting on page 366 section to correct any issues.

Why Do Drives Added to an Expansion Node Fail to Display in the BlackPearl Management Interface?

If you add new drives to a BlackPearl expansion node, the system must be power-cycled before the new drives are detected and available for use. Use the following power sequence if you added drives to a powered-on expansion nodes.

1. Power-down the BlackPearl Object Gateway and all expansion nodes.
2. Power-on all expansion nodes
3. Wait approximately four minutes
4. Power-on the BlackPearl Object Gateway.

Intelligent Object Management (IOM)

With IOM, the BlackPearl Object Gateway is capable of self-healing files present on the Gateway, as well as automatically compacting data stored on tape, and providing an easy migration path from one type of storage to another. IOM also allows multiple object versioning and data pre-staging from tape to disk, and improves tape library performance by reducing the number of cartridge mounts.

Intelligent Object Management (IOM) has several key roles, including:

- Self-healing to rebuild a missing copy of data. Self-healing includes rebuilding a new storage domain member after it is added as an additional copy of data on the data policy.
- Migrating a copy of data to new or different media within a given storage domain by excluding the other storage domain member.
- Tape compaction, which moves all valid data off of a tape to other tapes in that storage domain, which allows the compacted tape to be reused or decommissioned.

IOM works by creating both a PUT job and GET job for the data it needs to move. IOM may create additional jobs depending on workload. When running an IOM migration, the Gateway creates a pair of jobs for each storage domain, and additional job(s) for any tape cartridge(s) that are exported from the tape library.

IOM only acts on data in BlackPearl buckets, it does not replicate the buckets themselves. If two BlackPearl Object Gateways are configured for replication, and a bucket is deleted on the target BlackPearl Object Gateway, IOM does not self-heal the bucket.

Best Practices

Spectra Logic recommends running IOM on a subset of data when possible.

- **Migration Example** - If there are five storage domains where each domain is isolated from the other storage domains, use IOM to migrate one storage domain at a time. Within that storage domain, add a new storage domain member, and exclude the other member to start the IOM migration. See Create a Storage Domain on page 119 and Exclude a Storage Domain Member for instructions.
- **Self-healing Example** - Start with a data policy that only has a single, smaller capacity bucket. This data policy is duplicated with the same configuration settings. It is then possible to change the bucket(s) to use the new data policy. Then modify the new data policy to add an additional storage domain, which triggers the IOM self-healing job to rebuild the missing copy of data. See Create a Data Policy on page 127 and Edit a Data Policy.

Spectra Logic recommends configuring your storage environment so that IOM uses more drives to write data than drives to read data.

IOM jobs are created with a task priority of low. Configuring all tape drives with a minimum task priority of normal, or higher, prevents IOM operations and is not recommended.

If you have configured a storage domain to use automatic tape compaction, allow the system to complete all tape compactions before starting an IOM job. Configuring a low percentage, aggressive tape drive compaction threshold may cause ongoing tape compaction, which can interfere with IOM operations. Before starting an IOM migration, allow the system to complete all current tape compaction operations, then configure tape drive compaction to a higher, more conservative setting, and ensure no tapes are being actively compacted.

Considerations for IOM Resource Impact

The BlackPearl Object Gateway can be configured to limit or prevent the impact of IOM operations on the normal production workload. The main considerations are the cache pool size and throughput, and the number of tape drives available for IOM. The BlackPearl tape drive task priority can be set to limit which, and how many, tape drives are available for IOM operations. This also limits the impact on cache bandwidth.

If throughput and bandwidth need to be prioritized for the normal production workflow, or if there is not enough throughput available, then a hardware configuration change may be necessary to meet the project goals. Throughput can be increased by adding additional disk drives to the cache pool, while adding additional tape drives increases the Gateway available bandwidth. If further improvements are necessary, the chassis can be upgraded to new hardware.

Note: Contact the Spectra Logic Professional Services team for help sizing and managing both migration and self-healing IOM projects, as well as assistance with hardware upgrades to improve the throughput bandwidth of your Gateway.

IOM jobs that are the result of a new data persistence rule being created in a data policy are sized at the total amount of data under management by the data policy. This can take a long time to complete and can use multiple tape drives for an extended period of time. Consider using IOM scheduling to balance IOM operations with ongoing production requirements that use the same tape or disk partitions.

USING A BLACKPEARL OBJECT GATEWAY WITH THE VAIL APPLICATION

Why Do Vail Jobs Show as Canceled in the BlackPearl User Interface?

When the Vail application requests an object(s) from a BlackPearl Object Gateway, it initiates a Start Bulk Get job on the BlackPearl Object Gateway. However, the Vail application has a back-door path to read objects from the BlackPearl cache. The BlackPearl Object Gateway is only aware of when objects are read through the front door path. When the Vail application completes reading the requested object(s) from the BlackPearl cache, it cancels the job on the BlackPearl Object Gateway.

What Ports Does the BlackPearl Object Gateway Use to Connect to a Vail Sphere?

In order to use a BlackPearl Object Gateway with a Vail sphere, make sure the following ports are open.

Port	Description
Inbound 80 and/or 443	Inbound access is needed for these ports to access the BlackPearl user interface, and for Amazon compatible S3 clients to transfer data to the Gateway, using either the open (80) or secure port (443)
Outbound 443	Outbound access is needed for port 443 to allow data transfer to the Vail sphere, or other Amazon compatible S3 endpoint nodes.

SPECIAL FIREWALL FEATURE FOR CONNECTING TO THE BLUESCALE USER INTERFACE

Introduction

The BlackPearl Object Gateway can act as a Gateway for a Spectra Logic tape library network management interface. This feature enables a private network behind the BlackPearl Object Gateway, where Proxy/NAT information is entered into the BlackPearl Object Gateway to allow a connection to either a BlueScale library or BlueVision library with the BlackPearl Object Gateway.

Warning

- This will greatly reduce performance of the overall system.
- Only use at the direction of Spectra Logic Technical Support.
- Consult your Professional Services team for proper configurations when a tape library management Gateway is required.

Basic Steps

1. Obtain the key from Technical Support.
2. Enter the "EM BlueScale" key in the BlackPearl user interface.
3. Connect the tape library management port directly to the RJ45 data port on the BlackPearl chassis.
4. Enter tape library Proxy/NAT information for the tape library in the BlackPearl user interface.
5. Verify the connection for the tape library remote management interface using a client browser.

CAPACITY MODE VERSUS PERFORMANCE MODE

Chunks

The BlackPearl Object Gateway writes to tape drives based on chunks, with default chunk size of approximately 128 GB, or 2% of the tape media capacity. When there is a queue of jobs, the BlackPearl Object Gateway aggregates smaller jobs or smaller chunks into a size of approximately 128 GB for each tape drive read or write task.

Performance Mode

When running in performance mode, the BlackPearl Object Gateway spreads the chunks or aggregations across all available tape drives, or disk pools. The number of tape drives used can be limited by using tape drive reservations. It is recommended to use performance mode only at the direction of Spectra Logic. There may be other methods to increase performance while using capacity mode based on workloads and use cases.

The consequence of using performance mode with tape media is that during a restore or GET job, more tape drives and tapes cartridges are required to restore a data set that was initially spread across many tapes. This can drastically reduce overall performance during restores, as the Gateway takes longer to get access to the full data set.

IMPORTANT Spectra Logic highly recommends working with Spectra Logic Technical Support, or Spectra Professional Services before using Performance mode.

Capacity Mode

When running in capacity mode, the BlackPearl Object Gateway uses as few tape cartridges or disk pools as possible. The Gateway only allocates a new tape cartridge or disk pool when capacity is needed.

This means that for smaller jobs, the BlackPearl Object Gateway only writes to one tape drive regardless of how fast the cache is. However, the Gateway monitors the total job queue capacity, and if there is more data in the queue than there is capacity on the tape(s) available, it will allocate an additional tape and start writing data to the newly allocated tape in parallel.

Note: When the data policy setting "Minimize Spanning" is enabled, it overrides the capacity mode and performance mode logic for a given job, up to 1 TB in size. Minimize spanning increases the chunk size to 1 TB, and always keeps one chunk on a single tape regardless of write mode. If the job is larger than 1 TB, then multiple chunks are used and the Gateway uses the logic for capacity mode vs performance mode, where different chunks may transfer to different tapes.

TAPE HANDLING REFACTOR

Use the information in this section to understand the changes to tape handling in the BlackPearl OS.

General BlackPearl Notes

- Tape drives can be taken offline and new drives brought online without restarting the BlackPearl Object Gateway.
- For clearing a 'stuck' tape drive reservation, the sa(4) driver reserves a drive on open and releases it on close using SCSI-2 reservations that are not persistent. A power cycle or drive reset clears the reservation. The reason for the reservation is to ensure no other initiator attempts to use the tape drive while the BlackPearl Object Gateway is using it.
- Most drive sense is handled by the sa(4) driver and LTFS. The tape drivers used by the BlackPearl Object Gateway almost exclusively interacts with a tape drive via libltfs. The LTFS library handles all sense codes itself or through its tape device drivers, and returns a generic error when a failure of the LTFS library management occurs.
- The BlackPearl Object Gateway does not issue reset tape drive commands.

Tape Drive Failure Modes

The BlackPearl Object Gateway does not react to many sense codes from tape drives, as the BlackPearl management code only receives them from the tape library management subsystem when the BlackPearl Object Gateway attempts to read tape MAM attributes, such as determining the density of a piece of tape media or issuing a Test Unit Ready (TUR).

Most of the hard failures the BlackPearl Object Gateway encounter include:

- Read and write errors.
- Command timeout issues due to the drive firmware being stuck on a process.
- A tape cartridge physically stuck in a tape drive.
- Tape drive seek errors.

When the BlackPearl Object Gateway experiences any of these issues inside a libltfs call, a generic sense code is returned to the system management code.

Move Failures/Tape Stuck in Drive

Information about move failures comes from the changer device, and not a tape drive. The BlackPearl Object Gateway detects these events through the tape library management subsystem. Currently, the BlackPearl Object Gateway responds to sense codes from the media changer device as recommended in the Spectra TSeries Developer Guide. When a move failure occurs, the BlackPearl Object Gateway is limited to just retrying the move.

Note: Spectra Logic is currently investigating other tape and media changer errors to add new functionality for restoring drive operation based on sense codes received from the tape library.

- **Encryption failure** – The 5.3.0 data planner now handles this failure. This is not handled by BlackPearl software 5.2 or earlier, and the BlackPearl Object Gateway instead tries all tapes in the library.
- **Hardware failure** – The 5.3.0 data planner now handles this failure. This is not handled by BlackPearl software 5.2 or earlier, and the BlackPearl Object Gateway continues to retry using the drive or tape.
- **Read failure** – The 5.3.0 data planner handles this failure using new tape handler logic. BlackPearl OS prior to version 5.3 have error handling to move a tape to at least two tape drives before marking the tape as bad. Starting with BlackPearl OS 5.3, the Gateway retries the read using up to three tape drives.
- **Write failure** - The 5.3.0 data planner handles this failure using new tape handler logic. BlackPearl OS prior to version 5.3 have error handling to move a tape to at least two tape drives before marking the tape as bad. Starting with BlackPearl OS 5.3, the Gateway retries the write using up to three tape drives.
- **MAM failure** – This error is handled by driver retry logic.
- **LTFS failure** – This is a failure other than Encryption, Hardware, or read/write failures. This failure is not handled in OS 5.3 and the BlackPearl Object Gateway will try all tapes in the library.
- **Replace tape drive** – This operation does not require a BlackPearl reboot. (See point 1 below in Library, Drive, and Tape Failure Behavior in BlackPearl version 5.3 below).
- **Add a new tape drive** - This operation does not require a BlackPearl reboot. (See point 1 below in Library, Drive, and Tape Failure Behavior in BlackPearl version 5.3 below).

Library, Drive, and Tape Failure Behavior in BlackPearl version 5.3

Use the information in this section to understand the behavior of the BlackPearl Object Gateway when encountering failures in tape library operation.

1. Lower level kernel and tape backend behavior:

   a. The tape backend communicates with the media changer via SCSI pass-through. Generally, any retries are handled in the tape library management subsystem and not the kernel. If the kernel handles the retries, the BlackPearl Object Gateway receives Unit Attention conditionals from the library that tell the BlackPearl Object Gateway that the inventory has changed.

   b. The tape library management subsystem communicates with a tape drive via SCSI pass-through, tape driver IOCTLs, and LTFS. Depending on which of the approximately 50 tape drive calls LTFS is issuing, LTFS communicates with the tape drive via read/write communications to the tape driver, tape driver IOCTLs, or via SCSI pass-through. LTFS specifies whether or not it retries SCSI pass-through commands. For read/write, the sa(4) driver does not retry.

2. For move failures of any kind, the tape library management subsystem tries the move command again through the pass device (with no CAM retries) up to five times. The driver does no error handling for the BlackPearl Object Gateway. For each attempt that fails, the BlackPearl Object Gateway examines the sense code and tries to take remedial action on it. If the sense code does not indicate a terminal failure, the BlackPearl Object Gateway tries again, otherwise the Gateway returns a failure. If the Gateway exhausts all retries and is attempting a drive-to-drive move, the source drive is put into an error state. Otherwise the CCBFailure error is returned.

3. Tape error handling (the “3-strikes to quiesce” rule)

   a. Three consecutive failures on a tape drive on the same operation should not occur, because the BlackPearl Object Gateway stops retrying the operation on the drive and currently loaded tape after two failures before trying with a different drive or a different tape.

   b. The BlackPearl Object Gateway will quiesce a drive if it has outstanding (not cleared) failures for three tapes regardless of how many failures per tape there are, of what tasks originated the failures, and of what type of failures they are. Failure type does matter when clearing failures. The BlackPearl Object Gateway ages failures out of memory after 24 hours, no longer counting against the drive for this quiesce rule. However, the failures are retained in the database.

   c. Here's an example scenario for events on a single tape drive:

      i. Tape A fails twice with two write failures. That is considered one strike and not two, because the failures occurred on only one tape.

      ii. Tape B fails with an import failure, which is considered the second strike on the tape drive.

      iii. Tape C successfully writes some data, clearing all write failures for the drive. This reduces the number of strikes counted against the drive back to one strike.

      iv. Tape B fails with a write failure. The drive is still considered to have just one strike because there was already a failure with tape B.

- **v.** Tape C fails with a write failure, which is considered a second strike on the tape drive.
- **vi.** Tape D is successfully inspected by the tape drive. No changes to the strike count occur, because the BlackPearl Object Gateway does not have any inspect failures to clear.
- **vii.** Tape D fails with a write failure. Since all of these events occurred in a span of 24 hours, none of the errors has aged out, and this failure is considered a third strike on the drive (using strikes from failures with tapes B, C, D), and the BlackPearl Object Gateway quiesces the tape drive.

- **d.** The default number of strikes (three) can be changed by Spectra Logic Technical Support. If set to zero, the BlackPearl Object Gateway will not automatically quiesce the tape drive.

4. An LTFS Encryption error, or 500 Hardware error from tape drive causes the BlackPearl Object Gateway to quiesce the tape drive.
5. Manual quiescing of individual tape drive is still permitted.
6. If the BlackPearl "Auto-Inspect" data path is set to "Never Inspect", quiescing a tape partition causes the BlackPearl Object Gateway to stop monitoring or reconciling a tape library change (tape inspections are not eliminated). Instead, the BlackPearl Object Gateway no longer "loses" the tapes, because the Gateway is not monitoring the tape library, and therefore the Gateway does not have reason to inspect the same tapes after the tape partition is brought online. If the BlackPearl "Auto-Inspect" data path is set to "Full", then the Gateway inspects the tapes when the partition is brought online. If the tape library inventory changes, new tapes require inspection regardless of setting.

   If a tape library disappears unexpectedly (for example a RIM or robot connection is accidentally disconnected), the BlackPearl Object Gateway automatically quiesces the tape partition, and does not mark the tapes as lost. Then item 6 applies, and tapes are not inspected if the data path is set to "Never Inspect".

Note: The BlackPearl GUI does not notify users when the library comes back online.

The auto-quiesce feature is set to "ON" by default for BlackPearl OS 5.3.0. The Gateway follows normal quiesce behavior, and waits for chunks writing/reading from tapes to finish before taking tape drives offline.

If the auto-quiesce feature is set to "OFF", the tape cartridges are marked as "lost".

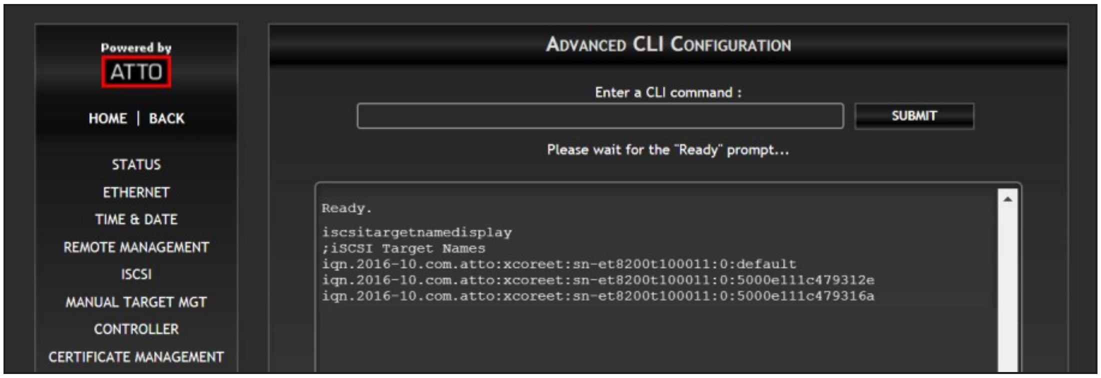
Enabling iSCSI For Use With the Spectra Swarm

The BlackPearl Object Gateway can communicate with the Spectra Swarm using the iSCSI protocol. This allows the BlackPearl to use SAS tape drives connected to the Spectra Swarm bridge.

The instructions below assume an understanding of creating and editing files in the FreeBSD environment. You must also have the BlackPearl Object Gateway and Spectra Swarm installed and configured.

This procedure is to be used only at the direction of Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

1. Log in to the Spectra Swarm user interface. See the *Spectra Swarm Install and Configuration Guide* for instructions.
2. Determine the target partition iSCSI name.
   a. In the left-hand pane, click **Advanced**. The Advanced screen displays.
   b. In the Enter a CLI Command dialog box, enter `iscsitargetnamedisplay` and click **Submit**. The list of iSCSI targets displays.



```
Ready.
iscsitargetnamedisplay
;iSCSI Target Names
iqn.2016-10.com.atto:xcoreet:sn-et8200t100011:0:default
iqn.2016-10.com.atto:xcoreet:sn-et8200t100011:0:5000e111c479312e
iqn.2016-10.com.atto:xcoreet:sn-et8200t100011:0:5000e111c479316a
```

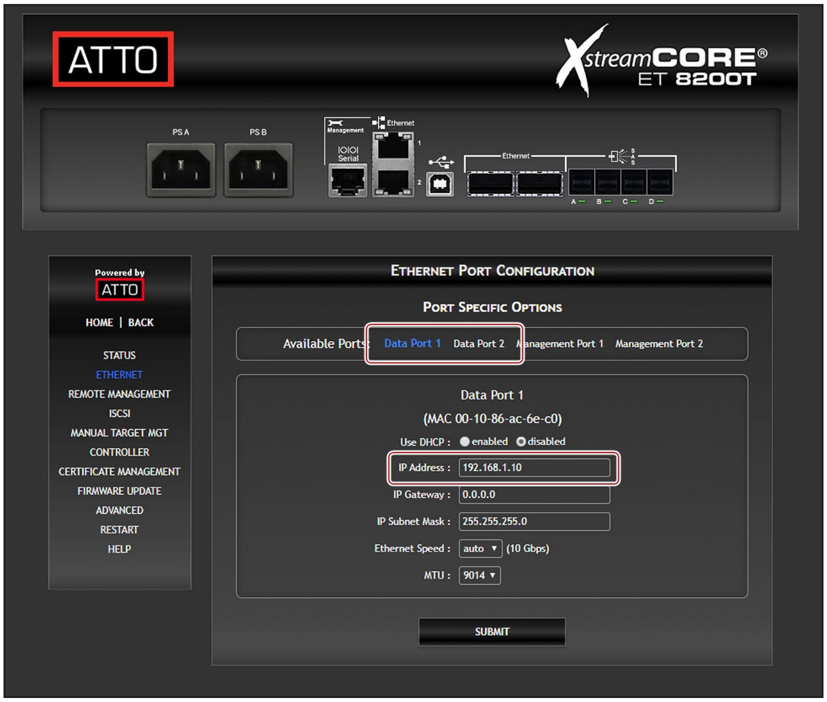
The name of each target is based on the WWN of each partition connected to the Spectra Swarm bridge. See *Spectra Swarm Install and Configuration Guide* the if you need to determine which WWN is associated with each partition.

IMPORTANT Using the default target may cause drive reservation errors with other appliances connected to the Spectra Swarm.

Note: The default target is a collection of all iSCSI targets attached to the bridge, and is not recommended for use with the BlackPearl Object Gateway.

3. Determine the Spectra Swarm bridge data port IP address.
   a. In the left-hand pane of the Swarm user interface, click **Ethernet**. The Ethernet Port Configuration screen displays.

b. Select the desired data port to display the IP Address for the port.



ETHERNET PORT CONFIGURATION

PORT SPECIFIC OPTIONS

Available Ports: Data Port 1 Data Port 2 Management Port 1 Management Port 2

Data Port 1

(MAC 00-10-86-ac-6e-c0)

Use DHCP : ○ enabled ● disabled

IP Address : 192.168.1.10

IP Gateway : 0.0.0.0

IP Subnet Mask : 255.255.255.0

Ethernet Speed : auto ▾ (10 Gbps)

MTU : 9014 ▾

4. Access the BlackPearl Object Gateway FreeBSD command line interface.
5. Create the file **/etc/iscsi.conf**.
6. Once created, enter the following in the **iscsi.conf** file for each partition you want the BlackPearl Object Gateway to access.

```
tlx <where x is the number of the partition>

{

    TargetAddress = <Spectra Swarm Data Port IP>

    TargetName = <iSCSI Target Name>

}
```

For example:

```
tl0
{
<192.168.1.10>
<iqn.2016-10.com.atto:xcoreet:sn-
et8200t100011:0:5000e111c479312e>
}
```

7. Save the **/etc/iscsi.conf** file.

8. Open the **/etc/rc.conf** file and add the following startup flags.

   ```
   iscsictl_enable=”YES”
   ```

   ```
   iscsictl_flags=”-Aa
   ```

9. Enable the iSCSI modules by adding the following line under the "builtin services" section of the **/etc/rc.conf** file.

   ```
   iscsid_enable=”YES”
   ```

10. Save the **/etc/rc.conf** file.

11. The BlackPearl Object Gateway must be restarted for this change to take effect. During system initialization, the BlackPearl Object Gateway automatically connects to all iSCSI targets defined in the /etc/iscsi.conf file.

If the tape partition does not display in the BlackPearl user interface, contact Spectra Logic Technical Support for assistance (see Contacting Spectra Logic on page 7).

TAPE LIBRARY ERRORS

What is a Data Checkpoint Failure?

A data checkpoint failure results from the BlackPearl Object Gateway not being able to verify a checkpoint on a tape cartridge. A checkpoint failure can occur during any tape operation, including reads, writes, tape compaction, and data verification. These errors occur due to problems with a tape drive, or with the tape cartridge itself.

There are three types of data checkpoint failures:

Data Checkpoint Failure – The BlackPearl Object Gateway was unable to verify data on a tape was at the correct checkpoint, or there was an error rolling back to a checkpoint.

Data Checkpoint Failure Due To Read Only - The BlackPearl Object Gateway was unable to verify data on a tape was at the correct checkpoint, or there was an error rolling back to a checkpoint because the physical read-only switch on a tape cartridge is engaged.

Data Checkpoint Missing – The tape checkpoint containing the data the BlackPearl Object Gateway is trying to locate is missing.

If a data checkpoint failure occurs, both system messages in the BlackPearl Object Gateway user interface, and emails sent to a system administrator, list the affected tape cartridge by barcode.

The system Administrator **must** be configured to receive emails with Error message severity to receive notifications when a data checkpoint failure occurs.

Below is an example of an email indicating a data checkpoint failure.

Example Email:

Automated notification from *BlackPearl system name* (*management port IP address, management port MAC address*), your Spectra Logic BlackPearl.

The following message has been generated. This could indicate a problem with your system.

Severity: Warning

Description: Tape Notification

Details: Data checkpoint failure for tape with barcode: 846544L7. LTFS_ERROR[500]: RPC TapeDrive$1012004E34.verifyQuiescedToCheckpoint<61891> FAILED: Rollback failed Created: 2021-10-12 03:46:08 UTC.

Resolve a BlackPearl Management Port IP Address Conflict

The default address of the BlackPearl management port is set to **10.0.0.2** with a netmask of **255.255.255.0**. If your network is already using this IP address, you are not able to access the BlackPearl user interface.

One resolution to the issue is to change the IP address of the machine already on your network to a different address. Then connect to the BlackPearl Object Gateway as described in Log Into the BlackPearl User Interface on page 74. If you cannot, or do not want to change the IP address of the existing machine, follow the instructions in this section to connect your BlackPearl Object Gateway to your network.

Using the Console

Using the BlackPearl Object console is the recommended way to change the BlackPearl management port IP address. For instructions on using the console to configure the management port IP address, see Configure the BlackPearl Management Port on page 71.

Using a Separate Computer

If you cannot use the console, use a computer or laptop disconnected from any existing network to change the BlackPearl management port IP address.

1. Gather a laptop or desktop computer not currently on any network. Disable any wireless networking, if necessary.
2. Using a standard Ethernet cable, connect the Ethernet port on the computer to the BlackPearl management port on the BlackPearl Object Gateway. See Components on page 32 to locate the management port.
3. Open a web browser on the computer. For a list of compatible browsers, see Supported Browsers.
4. Enter the IP address below in the browser address bar:

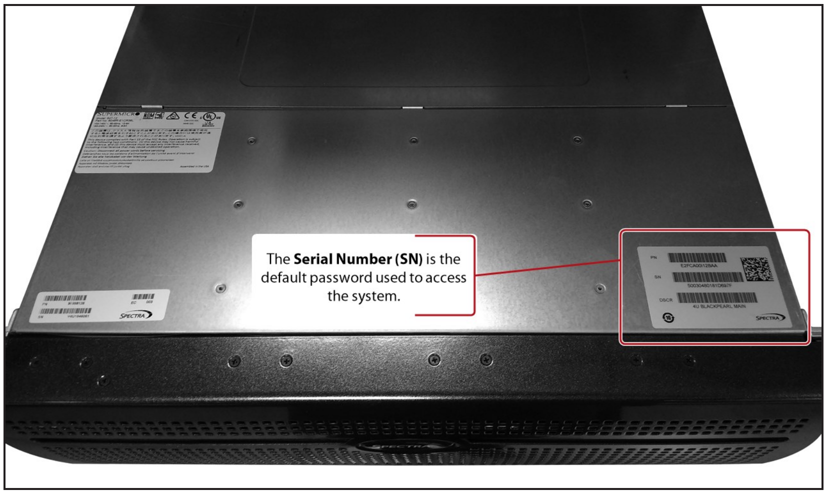
   ```
   https://10.0.0.2
   ```

Notes:
- The netmask for the default IP address is 255.255.255.0.
- The BlackPearl user interface uses a secure connection.

5. Resolve the security certificate warning for the BlackPearl user interface. The warning displays because the Gateway does not have a security certificate.

Notes:
- Consult your browser documentation for instructions on how to resolve the security certificate warning.
- The absence of the certificate does not affect functionality.

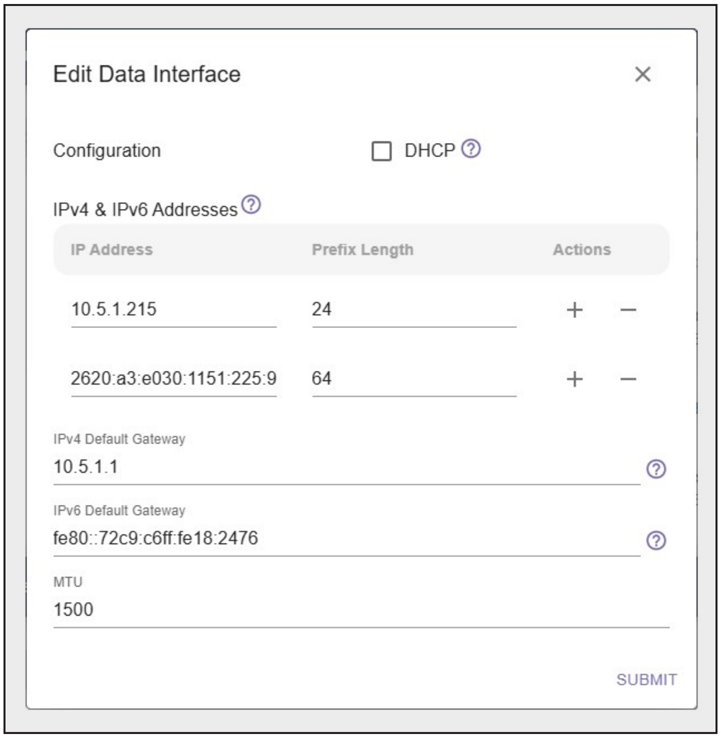
6. Enter the primary administrator username and password. The fields are case sensitive.
   - The default username is **Administrator**.
   - The default password is the serial number of the master node. Find the serial number on the sticker positioned on the top of the chassis, on the right-hand side, toward the front. The serial number is indicated by the letters "SN" on the sticker.



The **Serial Number (SN)** is the default password used to access the system.

Figure 295 The BlackPearl serial number sticker.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Network**.
2. In the Network Interfaces pane, select the **Management** row and then click **Edit**. The Edit Data Interface dialog box displays.



Edit Data Interface

Configuration □ DHCP

IPv4 & IPv6 Addresses

IP Address	Prefix Length	Actions
10.5.1.215	24	+ −
2620:a3:e030:1151:225:9	64	+ −

IPv4 Default Gateway: 10.5.1.1

IPv6 Default Gateway: fe80::72c9:c6ff:fe18:2476

MTU: 1500

Figure 296 The Edit Management dialog box.

3. Select the **DHCP** checkbox to configure the Gateway to automatically acquire an IPv4 address using DHCP. This setting does not apply to IPv6.

IMPORTANT If you select DHCP, you are not able to see the IP address assigned by DHCP before you are logged out of the BlackPearl user interface. Contact your system administrator to determine the DHCP address for the management port.

4. To configure a static IP address, click the **+** button and enter the following information:

- **IP Address**—Enter a valid IPv4 or IPv6 address.

Note: You cannot enter an IPv4 address if you selected DHCP.

- **Prefix Length**—Enter the subnet mask.

Note: If desired, you can enter **Aliases**, multiple IP and prefix lengths assigned to the data port. Use the **+** button to configure additional IP and Netmask addresses. You can configure a maximum of 16 aliases.

5. Enter the **IPv4 Default Gateway**.

Note: If you selected DHCP in Step on page 430, this option is unavailable.

6. Enter the **IPv6 Default Gateway**.

7. Change the **MTU** value, if desired. If you set the MTU value to something other than 1500, make sure that your switch configuration supports larger MTU settings, as well as all the hosts on the network. Acceptable values are 576 to 65535.

Note: Most networking designs are configured to use a value of 1500 or 9000.

8. Click **Submit**.

Note: When you change the IP address of the BlackPearl management port, you lose your connection to the user interface when you save your changes. To re-establish the connection, enter the new IP address in your browser and log in again.

9. Disconnect the Ethernet cable from the BlackPearl management port.

10. Connect a cable from your network to the management port on the BlackPearl Object Gateway. You are now able to connect to the Gateway with the IP address configured.

APPENDIX A - IPMI CONFIGURATION

This appendix provides instructions for configuring IPMI for the BlackPearl Object Gateway using the Gateway BIOS.

CAUTION **DO NOT** make any changes in the BIOS other than changing the IPMI settings as described below. Changing any other setting is not supported by Spectra Logic and may cause adverse Gateway performance.

1. If the BlackPearl Object Gateway is currently powered on, shut down the Gateway as described in Reboot or Shut Down a BlackPearl Object Gateway on page 267.
2. Connect a monitor and USB keyboard to the rear of the BlackPearl Object Gateway. See Components on page 32 to locate the monitor and USB connectors.
3. Power on the monitor.
4. Power on the Gateway as described in Power On the Gateway on page 69.
5. When prompted by the Gateway, press **DEL** to enter the Gateway BIOS.

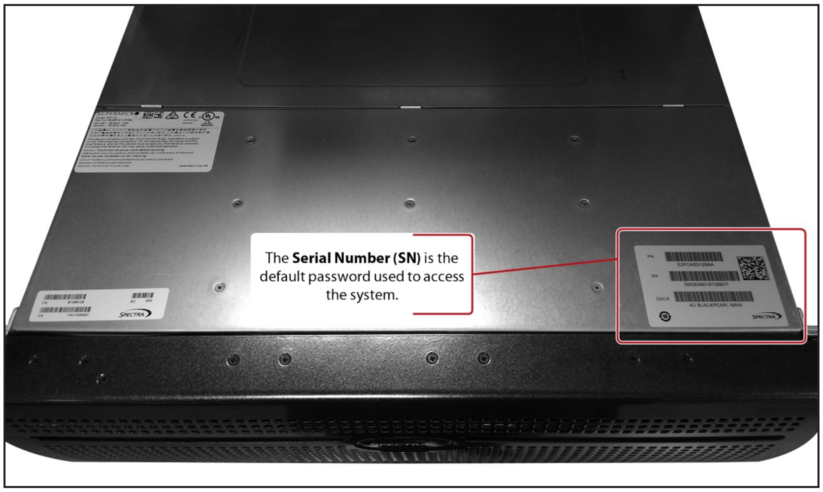
Note: The Gateway only displays this prompt for a few seconds. If you do not press **DEL** in time to enter the BIOS, let the Gateway complete it's boot process, then reboot the Gateway and repeat Step 4.

6. If necessary, log into the IPMI interface.
   - The username is **admin**.
   - The default password depends on when the product was sold by Spectra Logic.
     - For BlackPearl Object Gateways sold **after** February 2024, the password is the serial number of the master node with the characters '@a' appended to the end of the serial number. For example:

       `productserialnumber@a`

     - For BlackPearl Object Gateways sold **before** February 2024, the password is the serial number of the master node.

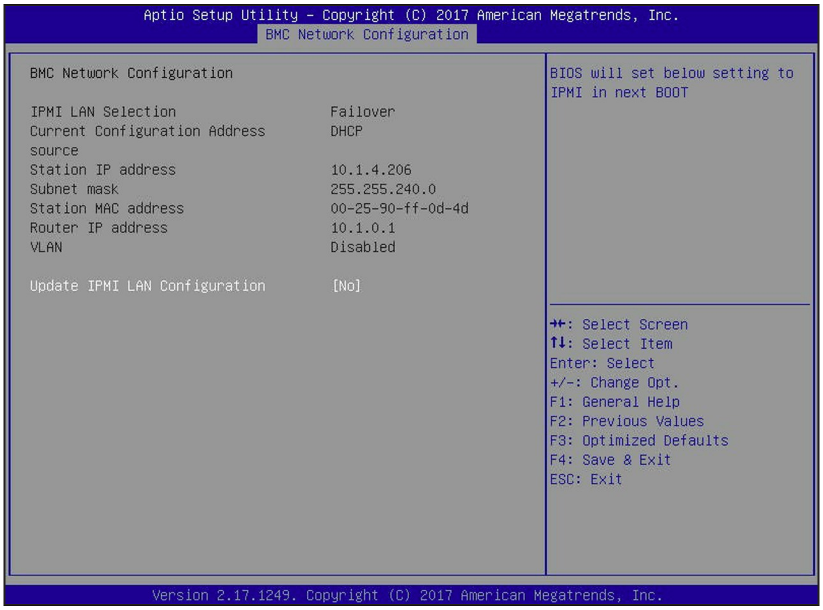
   Find the serial number on the sticker positioned on the top of the chassis, on the right-hand side, toward the front.



The **Serial Number (SN)** is the default password used to access the system.

Figure 297 The BlackPearl serial number sticker.

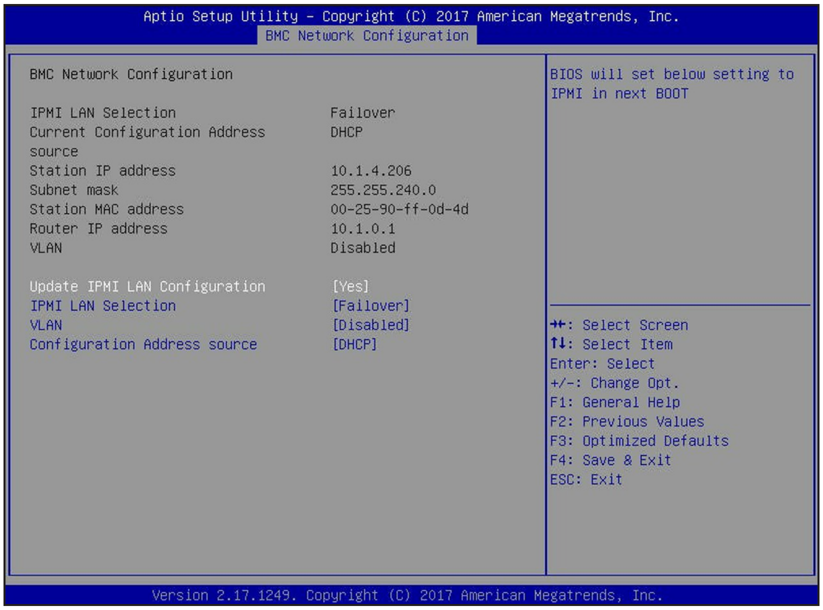
7. Use the keyboard to navigate to the **IPMI** tab and then select **BMC Network Configuration**. The current settings of the BMC configuration display.



```
Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
BMC Network Configuration

BMC Network Configuration                                   BIOS will set below setting to
                                                            IPMI in next BOOT
IPMI LAN Selection                    Failover
Current Configuration Address         DHCP
source
Station IP address                    10.1.4.206
Subnet mask                           255.255.240.0
Station MAC address                   00-25-90-ff-0d-4d
Router IP address                     10.1.0.1
VLAN                                  Disabled

Update IPMI LAN Configuration         [No]

                                                            →←: Select Screen
                                                            ↑↓: Select Item
                                                            Enter: Select
                                                            +/-: Change Opt.
                                                            F1: General Help
                                                            F2: Previous Values
                                                            F3: Optimized Defaults
                                                            F4: Save & Exit
                                                            ESC: Exit

Version 2.17.1249. Copyright (C) 2017 American Megatrends, Inc.
```

Figure 298 The BMC Configuration screen.

8. Use the keyboard to select **Update IPMI LAN Configuration**. A confirmation window displays. Select **YES** to continue. The current IPMI settings display.



```
Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
BMC Network Configuration

BMC Network Configuration                                   BIOS will set below setting to
                                                            IPMI in next BOOT
IPMI LAN Selection                    Failover
Current Configuration Address         DHCP
source
Station IP address                    10.1.4.206
Subnet mask                           255.255.240.0
Station MAC address                   00-25-90-ff-0d-4d
Router IP address                     10.1.0.1
VLAN                                  Disabled

Update IPMI LAN Configuration         [Yes]
IPMI LAN Selection                    [Failover]
VLAN                                  [Disabled]            →←: Select Screen
Configuration Address source          [DHCP]                ↑↓: Select Item
                                                            Enter: Select
                                                            +/-: Change Opt.
                                                            F1: General Help
                                                            F2: Previous Values
                                                            F3: Optimized Defaults
                                                            F4: Save & Exit
                                                            ESC: Exit

Version 2.17.1249. Copyright (C) 2017 American Megatrends, Inc.
```

Figure 299 Current IPMI settings.

9. If desired, select **IPMI LAN Selection**. Change the configured setting as needed.

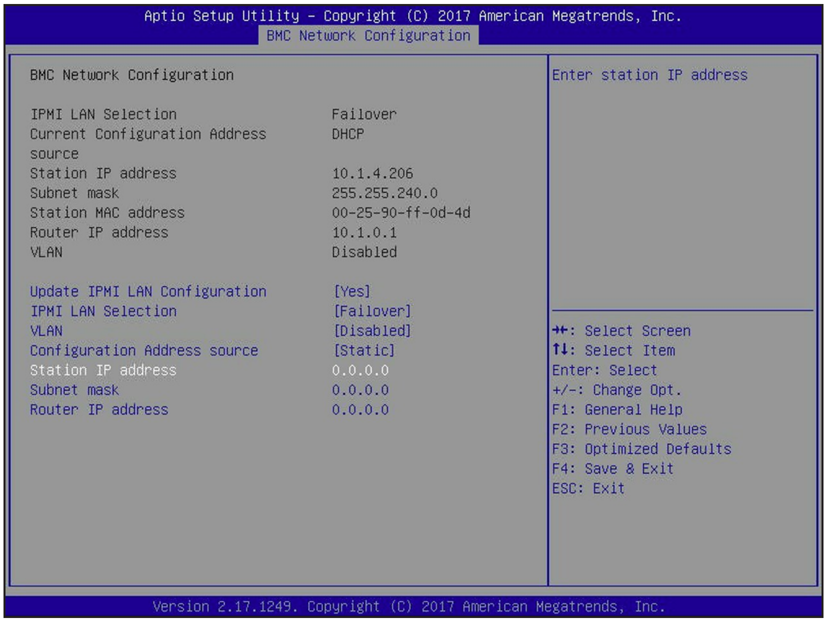
- **Dedicated** - Always uses the dedicated IPMI port for IPMI traffic.
- **Shared** - Always uses the LAN1 port for IPMI traffic.
- **Failover** - On Gateway startup, detect if the dedicated IPMI port is connected. If not, the Gateway uses the LAN1 port for IPMI traffic.

10. If desired, select **VLAN** to enable or disable VLAN as needed.

11. To change the IPMI address settings, select **Configuration Address source**. The current address source information displays.

12. Select **Static** or **DHCP** addressing.

- If you select **DHCP**, skip to Step 14.
- If you select **Static**, IP addressing fields display.



```
Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
BMC Network Configuration

BMC Network Configuration                                  Enter station IP address

IPMI LAN Selection                    Failover
Current Configuration Address         DHCP
source
Station IP address                    10.1.4.206
Subnet mask                           255.255.240.0
Station MAC address                   00-25-90-ff-0d-4d
Router IP address                     10.1.0.1
VLAN                                  Disabled

Update IPMI LAN Configuration         [Yes]
IPMI LAN Selection                    [Failover]
VLAN                                  [Disabled]           →←: Select Screen
Configuration Address source          [Static]             ↑↓: Select Item
Station IP address                    0.0.0.0              Enter: Select
Subnet mask                           0.0.0.0              +/-: Change Opt.
Router IP address                     0.0.0.0              F1: General Help
                                                           F2: Previous Values
                                                           F3: Optimized Defaults
                                                           F4: Save & Exit
                                                           ESC: Exit

Version 2.17.1249. Copyright (C) 2017 American Megatrends, Inc.
```

Figure 300 Enter Static IP information.

13. Configure the **Station IP address**, **Subnet mask**, and **Router IP address** with the desired address values.

Note: Only IPv4 addresses are valid.

14. Press **F4** to exit the BIOS and save the entered settings. The BlackPearl Object Gateway reboots.

APPENDIX B - SPECIFICATIONS

This appendix provides detailed specifications for the BlackPearl Object Gateway master nodes, the 44-bay expansion node, 77-bay expansion node, 96-bay expansion node, and 107-bay expansion node. The specifications listed here pertain to the currently shipping BlackPearl chassis.

DATA STORAGE SPECIFICATIONS

The following tables show the data storage specifications for the BlackPearl Object Gateways.

Notes:
- 1 TB is defined as 1,000,000,000,000 bytes.
- 1 GB is defined as 1,000,000,000 bytes.

BlackPearl Gen3 F Series

Drive Purpose	Drive Type
Database Storage, Object Cache, Storage pools, Vail pools, NAS	24 NVMe SSD Gen5 Drive storage capacities: 1.6 TB, 6.4 TB, 12.8 TB, or 25.6 TB.

BlackPearl Gen3 H Series

Drive Purpose	Drive Type
Database Storage	1.6 TB NVMe SSD Gen4 6.4 TB NVMe SSD Gen4
Object Cache	4, 8, 16, 20, or 22 TB Spinning-Disk SAS
Storage pools, Vail pools, Write Performance, Metadata Performance, or NAS	4, 8, 16, 20, or 22 TB Spinning-Disk SAS

BlackPearl Gen2 X Series

Drive Purpose	Drive Type
Database Storage	1.6 TB NVMe SSD Gen4
Object Cache	6.4 TB NVMe SSD Gen4
Storage pools, Vail pools, Write Performance, Metadata Performance, or NAS	• 1.6 TB SSD Gen4 • 6.4 TB SSD Gen4

BlackPearl Gen2 S Series and Gen2 V Series

Drive Purpose	Drive Type
Database Storage	• 1.6 TB NVMe SSD • 6.4 TB NVMe SSD
Object Cache	• 4 TB SAS HDD • 16 TB SAS Self-Encrypting Drive • 1.6 TB NVMe SSD • 6.4 TB NVMe SSD
Write Performance, Metadata Performance	• 1.6 TB SSD Gen4 • 6.4 TB SSD Gen4 (S Series only)
Storage pools, Vail pools, or NAS	• 4 TB SAS HDD • 8, 12, and 20 TB SAS Self-Encrypting Drive

BlackPearl Gen1 S Series 4U Gateway

Drive Purpose	Drive Type
Database Storage	400 or 800 GB Solid-State SAS
Object Cache	• 4, 8, 12, or 16 TB Spinning-Disk SAS • 8, 12, and 20 TB SAS Self-Encrypting Drive
Storage Pools or NAS	• 4, 8, or 12 TB Spinning-Disk SAS • 12 or 16 TB Spinning-Disk SATA • 8, 12, and 20 TB SAS Self-Encrypting Drive

BlackPearl Gen1 P Series 4U Gateway

Drive Purpose	Drive Type
Database Storage	400 or 800 GB Solid-State SAS
Object Cache	960, 1600, or 1920 GB Solid-State SAS
Storage Pools or NAS	960, 1600, or 1920 GB Solid-State SAS

BlackPearl Gen1 V Series 2U Gateway

Drive Purpose	Drive Type
Database Storage	400 or 800 GB Solid-State SAS
Object Cache	• 4, 8, 12, or 16 TB Spinning-Disk SAS • 8, 12, and 20 TB SAS Self-Encrypting Drive
Storage Pools or NAS	• 4, 8, 12, or 16 TB Spinning-Disk SAS • 12 or 16 TB Spinning-Disk SATA • 8, 12, and 20 TB SAS Self-Encrypting Drive

44-Bay Expansion Node

Drive Purpose	Specification
Storage Pools or NAS	• 4, 8, 12, or 16 TB Spinning-Disk SAS • 12 or 16 TB Spinning-Disk SATA • 8, 12, and 20 TB SAS Self-Encrypting Drive

77-Bay Expansion Node

Drive Purpose	Specification
Storage Pools or NAS	• 800 GB Solid-State SAS • 4, 8, 12, or 16 TB Spinning-Disk SAS [1] • 12 or 16 TB Spinning-Disk SATA • 8, 12, and 20 TB SAS Self-Encrypting Drive

96-Bay Expansion Node

Drive Purpose	Specification
Storage Pools or NAS	8, 12, or 16 TB Spinning-Disk SATA

107-Bay Expansion Node

Drive Purpose	Specification
Storage Pools or NAS	• 800 GB Solid-State SAS • 4, 8, 12, or 16 TB Spinning-Disk SAS • 12 or 16 TB Spinning-Disk SATA • 8, 12, and 20 TB SAS Self-Encrypting Drive

[1]) 16 TB SAS drives only supported in a HotPair configuration.

System Specification

The following tables provide an overview of the devices in the BlackPearl Object Gateways.

Gen3 F Series BlackPearl Object

Parameter	Specifications
CPU	One 64-bit 24 core CPU
System disk drives	Two 512 GB M.2 NVMe
Memory	512 GB (8 x 64 GB DIMMs)
Interface connections	• One integrated 10 GigE Ethernet port [a] • One integrated 1 GigE IPMI port • One standard dual-port 100 GigE Ethernet card • (Optional) Four-port SAS card [b] • (Optional) Four-port Fibre Channel card [c]

[a] Dedicated to the BlackPearl user interface for Gateway management.

[b] Each SAS card is used to connect the BlackPearl master node to disk expansion nodes or SAS tape drives.

[c] Each Fibre Channel card is used to connect the BlackPearl master node to Fibre Channel tape drives.

Gen3 H Series 3300 & 3310 BlackPearl Object

Parameter	Specifications
CPU	One 64-bit 8 core CPU (base) One 64-bit 24 core CPU (upgrade)
System disk drives	Two 512 GB M.2 NVMe
Memory	256 GB (4 x 64 GB DIMMs) 512 GB (8 x 64 GB DIMMs)
Interface connections	• One integrated 1 GigE Ethernet port [a] • One integrated 1 GigE IPMI port • One standard dual-port 25 GigE or 100 GigE Ethernet card • (Optional) Four-port SAS card [b] • (Optional) Four-port Fibre Channel card [c]

Gen2 X Series BlackPearl Object

Parameter	Specifications
CPU	One 64-core CPU
System disk drives	Two 480 GB NVMe
Memory	512 GB (8 x 64 GB DIMMs)
Interface connections	• One integrated 1 GigE Ethernet ports [d] • One standard two-port 100 GigE Ethernet card • (Optional) Four-port SAS card [e] • (Optional) Four-port Fibre Channel card [f]

[a] Dedicated to the BlackPearl user interface for Gateway management.

[b] Each SAS card is used to connect the BlackPearl master node to disk expansion nodes or SAS tape drives.

[c] Each Fibre Channel card is used to connect the BlackPearl master node to Fibre Channel tape drives.

[d] Dedicated to the BlackPearl user interface for Gateway management.

[e] Each SAS card is used to connect the BlackPearl master node to disk expansion nodes or SAS tape drives.

[f] Each Fibre Channel card is used to connect the BlackPearl master node to Fibre Channel tape drives.

Gen2 V Series BlackPearl Object

Parameter	Specifications
CPU	One 16-core CPU
System disk drives	Two 480 GB M.2 SSD
Memory	256 GB (4 x 64 GB DIMMs)
Interface connections	• Two integrated 10GBase-T Ethernet ports [a] • (Optional) Dual-port 100 Gigabit Ethernet NIC • (Optional) Four-port SAS card [b] • (Optional) Four-port Fibre Channel card [c]

Gen2 S Series BlackPearl Object

Parameter	Specifications
CPU	One 32-core CPU
System disk drives	Two 480 GB M.2 SSD
Memory	128 GB (8 x 16 GB DIMMs)
Interface connections	• Two integrated 10GBase-T Ethernet ports [b] • (Optional) Dual-port 100 Gigabit Ethernet NIC • (Optional) four-port SAS card [c] • (Optional) four-port Fibre Channel card [d]

[a] One port is available for data transfers, one port is dedicated to the BlackPearl user interface for Gateway management.

[b] One port is available for data transfers, one port is dedicated to the BlackPearl user interface for Gateway management.

[c] Each SAS card is used to connect the BlackPearl master node to disk expansion nodes or SAS tape drives.

[d] Each Fibre Channel card is used to connect the BlackPearl master node to Fibre Channel tape drives.

Gen1 V Series BlackPearl 2U Gateway

Parameter	Specifications
CPU	One multi-core processor
System disk drives	Two 500 GB SATA disk drives
Memory	32 GB (4 x 8 GB DIMMs) 64 GB (8 x 8 GB DIMMs or 4 x 16 GB DIMMs)
Interface connections	• Two integrated 10GBase-T Ethernet ports [a] • (Optional) One dual-port 10 Gigabit Ethernet NIC • (Optional) four-port SAS card [b] • (Optional) two-port SAS card [b] • (Optional) two-port Fibre Channel card [c]

Gen1 S Series BlackPearl 4U Gateway

Parameter	Specifications
CPU	Two multi-core processors
System disk drives	Two 500 GB SATA disk drives
Memory	64 GB (8 x 8 GB DIMMs) 128 GB (16 x 8 GB DIMMs or 8 x 16 GB DIMMs)
Interface connections	• Two integrated 10GBase-T Ethernet ports [a] • One dual-port 10 Gigabit Ethernet NIC • (Optional) One dual-port 40 Gigabit Ethernet NIC • (Optional) One dual-port 10GBase-T Ethernet NIC • (Optional) four-port SAS card [b] • (Optional) two-port SAS card [b] • (Optional) two-port Fibre Channel card [c]

[a] One port is available for data transfers, one port is dedicated to the BlackPearl user interface for Gateway management.

[b] Each SAS card is used to connect the BlackPearl master node to disk expansion nodes or SAS tape drives.

[c] Each Fibre Channel card is used to connect the BlackPearl master node to Fibre Channel tape drives.

Size and Weight

The following tables provide the size and weight of each chassis. Specifications are provided for each unit in both an operational environment, and in the shipping container.

Gen3 F Series BlackPearl Object Gateway

Parameter	Gen3 F Series BlackPearl Object Gateway	Shipping Container [a]
Dimensions		
• Height (4U)	3.5 in. (8.9 cm)	12 in. (30.5 cm)
• Width	19 in. (48.3 cm)	25 in. (73.6 cm)
• Depth	30 in. (76.2 cm)	37 in. (94 cm)
Weight		77 lb (35 kg)
• Chassis without drives	55 lb (25 kg)	
• Each NVMe drive	0.5 lb (0.23 kg)	

Gen3 H 3310 Series BlackPearlGateway

Parameter	Gen3 H 3310 Series BlackPearlGateway	Shipping Container [b]
Dimensions		
• Height (4U)	7 in. (17.8 cm)	18 in. (45.7 cm)
• Width	19 in. (48.3 cm)	25 in. (73.6 cm)
• Depth	29 in. (73.7 cm) [c]	39 in. (99 cm)
Weight		
• Chassis without drives	72 lb (33 kg) - single node 89 lb (40 kg) - dual node	
• Each NVMe drive	0.5 lb (0.23 kg)	

[a] Includes chassis, drives, box, and packaging.

[b] Includes chassis, drives, box, and packaging.

[c] Includes the front bezel.

Gen3 H 3300 Series BlackPearl Object Gateway

Parameter	Gen3 H 3300 Series BlackPearl Object Gateway	Shipping Container [a]
Dimensions • Height (4U) • Width • Depth	 7 in. (17.8 cm) 19 in. (48.3 cm) 29 in. (73.7 cm) [b]	 18 in. (45.7 cm) 25 in. (73.6 cm) 39 in. (99 cm)
Weight • Chassis without drives • Each SAS drive	 75 lb (34 kg) 1.5 lb (0.67 kg)	114 lb (51.8 kg)

Gen2 X Series BlackPearl Object Gateway

Parameter	Gen2 X Series BlackPearl Object Gateway	Shipping Container [c]
Dimensions • Height (2U) • Width • Depth	 3.5 in. (8.9 cm) 19 in. (48.3 cm) 29 in. (73.7 cm) [d]	
Maximum Weight Including rail kit [e]	60 lb (27.2 kg)	

Gen2 V Series BlackPearl Object Gateway

Parameter	Gen2 V Series BlackPearl Object Gateway	Shipping Container [a]
Dimensions		

[a] Includes chassis, drives, box, and packaging.

[b] Includes the front bezel.

[c] Includes chassis, drives, box, and packaging.

[d] Includes the front bezel.

[e] Weights are approximate.

Parameter	Gen2 V Series BlackPearl Object Gateway	Shipping Container [a]
- Height (2U) - Width - Depth	3.5 in. (8.9 cm) 19 in. (48.3 cm) 33 in. (83.8 cm) [b]	11.5 in. (29.2 cm) 23.7 in. (60.2 cm) 45 in. (114.3 cm)
Weight [c] - Empty chassis - Additional for each HDD - Additional for each SSD	72 lb (32.7 kg) 1.8 lb (0.8 kg) 0.8 lb (0.4 kg)	

Gen2 S Series BlackPearl Object Gateway

Parameter	Gen2 S Series BlackPearl Object Gateway	Shipping Container [a]
Dimensions - Height (2U) - Width - Depth	7 in. (17.8 cm) 19 in. (48.3 cm) 37.5 in. (95.3 cm) [b]	15.9 in. (40.4 cm) 23.7 in. (60.2 cm) 46.9 in. (119.1 cm)
Weight [c] - Empty chassis - Additional for each HDD - Additional for each SSD	99 lb (44.9 kg) 1.8 lb (0.8 kg) 0.8 lb (0.4 kg)	

Gen1 V Series 2U BlackPearl Object Gateway

Parameter	Gen1 V Series 2U BlackPearl Object Gateway	Shipping Container [a]
Dimensions - Height (2U)	3.5 in. (8.9 cm)	13.25 in. (33.7 cm)

[a] Includes chassis, drives, box, and packaging.

[b] Includes the front bezel.

[c] Weights are approximate.

Parameter	Gen1 V Series 2U BlackPearl Object Gateway	Shipping Container [a]
• Width	19 in. (48.3 cm)	26 in. (66.0 cm)
• Depth	27.5 in. (69.9 cm) [b]	34.25 in. (87.0 cm)
Weight [c]		
• Empty chassis	37.2 lb (16.9 kg)	N/A
• Empty chassis with:		
• 4 HDDs & 2 SSDs	46.7 lb (21.2 kg)	67.7 lb (30.7 kg)
• 9 HDDs & 2 SSDs	55.7 lb (25.3 kg)	76.7 lb (34.8 kg)

Gen1 S Series 4U BlackPearl Object Gateway and 44-Bay Expansion Node

Parameter	Gen1 S Series 4U BlackPearl Object Gateway and 44-Bay Expansion Node	Shipping Container [a]
Dimensions		
• Height (4U)	7 in. (17.8 cm)	17.5 in. (44.5 cm)
• Width	19 in. (48.3 cm)	27 in. (68.6 cm)
• Depth	29.5 in. (74.9 cm) [b]	39 in. (99.0 cm)
Weight [c]		
• Empty chassis	57 lb (25.8 kg)	91.3 lb (41.4 kg)
• Additional for each HDD	1.8 lb (0.8 kg)	1.8 lb (0.8 kg)
• Additional for each SSD	0.8 lb (0.4 kg)	0.8 lb (0.4 kg)

77-Bay Expansion Node

Parameter	77-bay Expansion Node	Shipping Container
Dimensions		

[a] Includes chassis, drives, box, and packaging.

[b] Includes the front bezel.

[c] Weights are approximate.

Parameter	77-bay Expansion Node	Shipping Container
• Height (4U)	7 in. (17.8 cm)	21.1 in. (53.6 cm)
• Width	19 in. (48.3 cm)	26.6 in. (67.6 cm)
• Depth	32 in. (81 cm) [b] 38.5 in. (97.8 cm) [a]	44.1 in. (112 cm)
Weight [b]		
• Empty chassis		127 lb (57.8 kg)
• Additional for each HDD	1.5 lb (0.67 kg)	
• Additional for each SSD	0.8 lb (0.36 kg)	
• Additional for rack mounting kit	21 lb (9.5 kg)	
• Fully loaded chassis with rack mounting kit		242 lb (110 kg) [c]

96-Bay Expansion Node

Parameter	96-bay Expansion Node	Shipping Container
Dimensions		
• Height (4U)	7 in. (17.8 cm)	14 in. (35.6 cm)
• Width	19 in. (48.3 cm)	24.5 in. (62.2 cm)
• Depth	40 in. (101.6 cm) [b]	43.5 in. (110.5 cm)
Weight [c]		
• Empty chassis	76 lb (34.5 kg)	108 lb (49 kg) [d]
• Additional for each HDD	1.8 lb (0.8 kg)	1.8 lb (0.8 kg)
• Additional for rack mounting kit	21 lb (9.5 kg)	21 lb (9.5 kg)
• Fully loaded chassis	270 lb (122.5 kg)	302 lb (137 kg)

[a] Includes optional cable management arm.

[b] Weights are approximate.

[c] Includes chassis and packaging.

[d] Includes chassis and packaging.

107-Bay Expansion Node

Parameter	107-bay Expansion Node	Shipping Container
Dimensions		
• Height (4U)	7 in. (17.8 cm)	18.4 in. (46.7 cm)
• Width	19 in. (48.3 cm)	24.3 in. (61.7 cm)
• Depth	41 in. (104.1 cm) [a] 47.5 in. (120.6 cm) [b]	52.3 in. (132.8 cm)
Weight [c]		
• Empty chassis	88.5 lb (40.1 kg)	180 lb (81.6 kg)
• Additional for each disk drive	1.5 lb (0.67 kg)	
• Additional for rack mounting kit	21 lb (9.5 kg)	
• Fully loaded chassis with rack mounting kit	270 lb (122.5 kg)	336 lb (152.4 kg) [d]

[a] Includes the front bezel.

[b] Includes optional cable management arm.

[c] Weights are approximate.

[d] Includes chassis and packaging.

Environmental Specifications

Temperature & Humidity

The tables below show the temperature, humidity, and altitude requirements for each chassis.

Gen3 F Series BlackPearl Object Gateway

Parameter	Operating Environment [a]	Storing and Shipping (Non-Operating) Environment [b]	Transit Conditions Storage Environment
Humidity		5% to 95% (non-condensing)	10% to 90% (non-condensing)
Temperature	32° F to 86° F [c] (0° C to 30° C)	–4° F to 158° F (–20° C to 70° C)	–40° F to 140° F (–40° C to 60° C)
Altitude	-200 ft to 10,000 ft (-61 m to 3,048 m)	-200 ft to 10,000 ft (-61 m to 3,048 m)	-200 ft to 40,000 ft (-61 m to 12,192 m)
Maximum wet bulb temperature			

[a] When moving the BlackPearl Object Gateway or expansion node from a cold storage environment to a warm operating environment, it must acclimate in its packaging for at least 12 hours before opening to prevent serious condensation damage.

[b] Specifications are for the BlackPearl Object Gateway or expansion node in its original packaging. The packaging protects the BlackPearl Object Gateway from condensation caused by extreme temperature variations (27° F per hour or 15° C per hour, or more).

[c] Maximum operating temperature is specified at sea level and is 2 percent lower per 1,000 ft (305 m) of increased altitude.

Gen3 H Series 3300 & 3310 BlackPearl Object Gateway

Parameter	Operating Environment [a]	Storing and Shipping (Non-Operating) Environment [b]	Transit Conditions Storage Environment
Humidity		5% to 95% (non-condensing)	10% to 90% (non-condensing)
Temperature	32° F to 95° F [c] (0° C to 35° C)	–4° F to 158° F (–20° C to 70° C)	–40° F to 140° F (–40° C to 60° C)
Altitude	-200 ft to 10,000 ft (-61 m to 3,048 m)	-200 ft to 10,000 ft (-61 m to 3,048 m)	-200 ft to 40,000 ft (-61 m to 12,192 m)
Maximum wet bulb temperature			

Gen2 X Series BlackPearl Object Gateway

Parameter	Operating Environment [a]	Storing and Shipping (Non-Operating) Environment [b]	Transit Conditions Storage Environment
Humidity	20% to 80% (non-condensing)	10% to 90% (non-condensing)	10% to 90% (non-condensing)
Temperature	41° F to 95° F [c] (5° C to 35° C)	–40° F to 113° F (–40° C to 45° C)	–40° F to 140° F (–40° C to 60° C)
Altitude	-200 ft to 10,000 ft (-61 m to 3,048 m)	-200 ft to 10,000 ft (-61 m to 3,048 m)	-200 ft to 40,000 ft (-61 m to 12,192 m)
Maximum wet bulb temperature	84° F (29° C)	95° F (35° C)	

[a]) When moving the BlackPearl Object Gateway or expansion node from a cold storage environment to a warm operating environment, it must acclimate in its packaging for at least 12 hours before opening to prevent serious condensation damage.

[b]) Specifications are for theBlackPearl Object Gateway or expansion node in its original packaging. The packaging protects the BlackPearl Object Gateway from condensation caused by extreme temperature variations (27° F per hour or 15° C per hour, or more).

[c]) Maximum operating temperature is specified at sea level and is 2 percent lower per 1,000 ft (305 m) of increased altitude.

Gen2 S Series and Gen2 V Series BlackPearl Object Gateway

Parameter	Operating Environment [a]	Storing and Shipping (Non-Operating) Environment [b]
Humidity	5% to 95% (non-condensing)	5% to 95% (non-condensing)
Temperature	50° F to 95° F (10° C to 35° C)	32° F to 122° F (0° C to 50° C)
Altitude	-200 ft to 10,000 ft (-61 m to 3,048 m)	-200 ft to 10,000 ft (-61 m to 3,048 m)
Maximum wet bulb temperature	84° F (29° C)	95° F (35° C)

Gen1 S Series and Gen1 V Series BlackPearl Object Gateway

Parameter	Operating Environment [a]	Storing and Shipping (Non-Operating) Environment [b]
Humidity	8% to 90% (non-condensing)	5% to 95% (non-condensing)
Temperature	50° F to 95° F (10° C to 35° C)	–40° F to 158° F (–40° C to 70° C)
Altitude	Sea level to 10,000 ft (3,048 m)	Sea level to 39,370 ft (12,000 m)
Maximum wet bulb temperature	84° F (29° C)	95° F (35° C)

[a] When moving the BlackPearl Object Gateway or expansion node from a cold storage environment to a warm operating environment, it must acclimate in its packaging for at least 12 hours before opening to prevent serious condensation damage.

[b] Specifications are for the BlackPearl Object Gateway or expansion node in its original packaging. The packaging protects the BlackPearl Object Gateway from condensation caused by extreme temperature variations (27° F per hour or 15° C per hour, or more).

44-Bay Expansion Node

Parameter	Operating Environment [a]	Storing and Shipping (Non-Operating) Environment [b]
Humidity	8% to 90% (non-condensing)	5% to 95% (non-condensing)
Temperature	50° F to 95° F (10° C to 35° C)	–40° F to 158° F (–40° C to 70° C)
Altitude	Sea level to 10,000 ft (3,048 m)	Sea level to 39,370 ft (12,000 m)
Maximum wet bulb temperature	84° F (29° C)	95° F (35° C)

77-Bay Expansion Node

Parameter	Operating Environment [a]	Storing and Shipping (Non-Operating) Environment [b]
Humidity	20% to 80% (non-condensing)	10% to 90% (non-condensing)
Temperature	32° F to 95° F (0° C to 35° C)	–4° F to 140° F (–20° C to 60° C)
Altitude	-200 ft to 10,000 ft (-61 m to 3,048 m)	-200 ft to 40,000 ft (-61 m to 12,192 m)

[a] When moving the BlackPearl Object Gateway or expansion node from a cold storage environment to a warm operating environment, it must acclimate in its packaging for at least 12 hours before opening to prevent serious condensation damage.

[b] Specifications are for the BlackPearl Object Gateway or expansion node in its original packaging. The packaging protects the BlackPearl Object Gateway from condensation caused by extreme temperature variations (27° F per hour or 15° C per hour, or more).

96-Bay Expansion Node

Parameter	Operating Environment [a]	Storing and Shipping (Non-Operating) Environment [b]
Humidity	20% to 80% (non-condensing)	10% to 90% (non-condensing)
Temperature	41° F to 95° F (5° C to 35° C)	–40° F to 140° F (–40° C to 60° C)
Altitude	-200 ft to 10,000 ft (-61 m to 3,048 m)	-200 ft to 40,000 ft (-61 m to 12,192 m)

107-Bay Expansion Node

Parameter	Operating Environment [a]	Storing and Shipping (Non-Operating) Environment [b]
Humidity	20% to 80% (non-condensing)	10% to 90% (non-condensing)
Temperature	32° F to 95° F (0° C to 35° C)	–4° F to 140° F (–20° C to 60° C)
Altitude	-200 ft to 10,000 ft (-61 m to 3,048 m)	-200 ft to 40,000 ft (-61 m to 12,192 m)

[a]) When moving the expansion node from a cold storage environment to a warm operating environment, it must acclimate in its packaging for at least 12 hours before opening to prevent serious condensation damage.

[b]) Specifications are for the expansion node is in its original packaging. The packaging is designed to protect the expansion node from condensation caused by extreme temperature variations (27° F per hour or 15° C per hour, or more).

Heat Generation

The following table shows the approximate heat generation of each BlackPearl chassis.

Chassis	Heat Generation at Maximum Wattage
Gen3 F Series 2U master node	3412-5459 BTUs/hour
Gen3 H Series 4U master node	2729 - 4092 BTUs/hour
Gen2 X Series 2U master node	5460 BTUs/hour
Gen2 V Series 2U master node	2729 BTUs/hour
Gen2 S Series 4U master node	5460 BTUs/hour
Gen1 V Series 2U master node	3138 BTUs/hour
Gen1 S or P Series 4U master node	3410 - 4365 BTUs/hour
44-bay expansion node	3751 - 4775 BTUs/hour
77-bay expansion node	3950 BTUs/hour
96-bay expansion node	3751 BTUs/hour
107-bay expansion node	6820 BTUs/hour

POWER REQUIREMENTS

The BlackPearl Object Gateways, 44-bay, 77-bay, 96-bay, and 107-bay expansion nodes, have the following power requirements.

CAUTION

Failure to meet the cabling and power specifications could damage your BlackPearl Object Gateway, result in data loss, or both.

Input Power Requirements

The following tables provide the input power requirements for each Gateway or expansion node.

Gen3 F Series BlackPearl Object Gateway

Parameter	Requirements
Input Voltage	100-120 VAC, 13 A, 1000 watts maximum

Parameter	Requirements
	200–240 VAC, 10 A, 1600 watts maximum
Input Frequency	50–60 Hz

Gen3 H Series 3300 and 3310 BlackPearl Object Gateway

Parameter	Requirements
Input Voltage	100-127 VAC, 10 A, 800 watts maximum 200–240 VAC, 8 A, 1200 watts maximum
Input Frequency	50–60 Hz

Gen2 X Series BlackPearl Object Gateway

Parameter	Requirements
Input Voltage	200–240 VAC, 7 A, 1600 watts maximum
Input Frequency	50–60 Hz

Gen2 V Series BlackPearl Object Gateway

Parameter	Requirements
Input Voltage	100-240 VAC, 8-4 A, 800 watts maximum
Input Frequency	50–60 Hz

Gen2 S Series BlackPearl Object Gateway

Parameter	Requirements
Input Voltage	200–240 VAC, 10 A, 1600 watts maximum
Input Frequency	50–60 Hz

Gen1 V Series 2U BlackPearl Object Gateway

Parameter	Requirements
Input Voltage	100–240 VAC, 11–4.5 A, 920 watts maximum

Parameter	Requirements
Input Frequency	50–60 Hz

Gen1 S Series 4U BlackPearl Object Gateway

Parameter	Requirements
Input Voltage	100–140 VAC, 12–8 A, 1000 watts maximum 180–240 VAC, 8–6 A, 1280 watts maximum
Input Frequency	50–60 Hz

44-Bay Expansion Node

Parameter	Requirements
Input Voltage	100–140 VAC, 13.5–9.5 A, 1100 watts maximum 180–240 VAC, 9.5–7 A, 1400 watts maximum
Input Frequency	50–60 Hz

77-Bay Expansion Node

Parameter	Requirements
Input Voltage	200–240 VAC, 12 A, 1600 watts maximum
Input Frequency	50-60 Hz

96-Bay Expansion Node

Parameter	Requirements
Input Voltage	90-264 VAC, 1100 watts maximum
Input Frequency	47–63 Hz

107-Bay Expansion Node

Parameter	Requirements
Input Voltage	200–240 VAC, 15 A, 2000 watts maximum
Input Frequency	50–60 Hz

Power Cord Specifications

The power cords included with the BlackPearl Object Gateways are part of the unit and are not intended for use with any other equipment.

IMPORTANT Confirm the PDU used with the BlackPearl Object Gateway has enough amperage for the power supply in each chassis included in your installation.

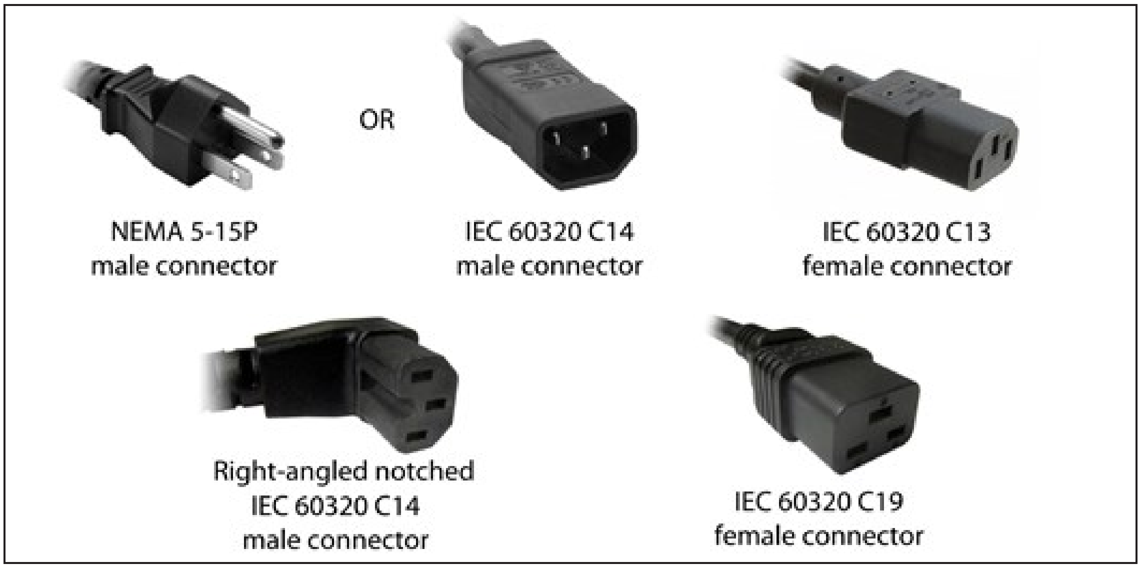
Cables provided by Spectra Logic are between 6 ft (1.8m) to 6.5 ft (2m) in length. If you need to use a longer cord, make sure it conforms to the specifications listed below.

Power cords must comply with local electrical codes.

WARNING Using extension cords in conjunction with the cords provided with a 77-bay expansion node, a 96-bay expansion node, or 107-bay expansion node, may cause serious damage.

WARNUNG Die Verwendung von Verlängerungskabeln in Verbindung mit den Kabeln, die mit einem 77-Schacht-Erweiterungsknoten, 96-Schacht-Erweiterungsknoten, oder 107-Schacht-Erweiterungsknoten geliefert werden, kann schwere Schäden verursachen.

Note: 96-bay expansion nodes ship with cables for use with the chassis. These power cables have a right-angled notched C14 connector, which is required for the 96-bay expansion node. Only use the cords provided by Spectra Logic with the 96-bay expansion node.



North American 120 Volt-AC Power Cord

The criteria for a 120-volt power cord for use in the United States and Canada are as follows:

Parameter	Specification
Power cordage	Three-conductor, 14 AWG
Power input connectors	**Gen1 S, P and V Series, Gen2 X and V Series, Gen 3 H Series, and 44-Bay Expansion Node:** • **Male:** NEMA 5-15P or IEC-60320 C14 • **Female:** IEC 60320 C13

North American 220 Volt-AC Power Cord

The criteria for a 220-volt power cord for use in the United States and Canada are as follows:

Parameter	Specification
Power cordage	SJT type, three-conductor, 14 AWG minimum
Power input connectors	**Gen1 S, P, and V Series, Gen2 X, S, and V Series, Gen 3 H Series, Gen 3 F Series, and 44-Bay Expansion Node:** • **Male:** NEMA 5-15P or IEC-60320 C14 • **Female:** IEC 60320 C13 **77-Bay Chassis Expansion Node:** • **Male:** Connector must be of the proper type, rating, and safety approval. • **Female:** IEC 60320 C19 **96-Bay Expansion Node:** • **Male:** Connector must be of the proper type, rating, and safety approval. • **Female:** Right-angled notched IEC 60320 C14 **107-Bay Chassis Expansion Node:** • **Male:** Connector must be of the proper type, rating, and safety approval. • **Female:** IEC 60320 C19

International 220 Volt-AC Power Cord

The criteria for an international 220-volt AC power cord are as follows:

Parameter	Specification
Power cordage	Flexible, HAR (harmonized) type H05VV-F, three conductor, cord with minimum conductor size of 1.7 square millimeters (0.0026350 square inches).
Power input connectors	**Gen1 S, P, and V Series, Gen2 X, S, and V Series, Gen 3 H Series, Gen 3 F Series, and 44-Bay Expansion Node:** • **Male:** Connector must be of the proper type, rating, and safety approval. • **Female:** IEC 60320 C13 **77-Bay Chassis Expansion Node:** • **Male:** Connector must be of the proper type, rating, and safety approval. • **Female:** IEC 60320 C19 **96-Bay Expansion Node:** • **Male:** Connector must be of the proper type, rating, and safety approval. • **Female:** Right-angled notched IEC 60320 C14 **107-Bay Chassis Expansion Node:** • **Male:** Connector must be of the proper type, rating, and safety approval. • **Female:** IEC 60320 C19

Power Connection Best Practice

For greater power redundancy, connect each of the two power cords to separate circuits.

INTERFACE SPECIFICATIONS

This section provides information about the interfaces used to connect a BlackPearl Object Gateway to expansion nodes, tape drives, and host systems.

System Interface Connectors

Gen3 F Series BlackPearl Object Gateway

Interface Type	Number of Ports and Connector Type
Ethernet • 25 and 100 GigE	Two QSFP28 sockets.
IPMI Management Port	One RJ-45 socket.
SAS (12 Gbps) (Optional)	• Four SFF-8644 sockets per 12 Gbps SAS card provide connections to four 77-bay, or 107-bay disk expansion nodes, using one port per expansion node. • Four SFF-8644 sockets per 12 Gbps SAS card provide connection to sixteen SAS tape drives in the tape library, using one port for four tape drives. **IMPORTANT** If the BlackPearl Object Gateway configuration includes both SAS tape drives and disk expansion nodes, separate HBAs must be used for each device type. If an OSW-2400 SAS Switch is used to connect to both tape drives and disk expansion nodes, a single SAS HBA is allowed.
Fibre Channel (16 Gb or 32 Gb) (Optional)	Four SFP+ optical modules with LC connectors per Fibre Channel card provide connections to four Fibre Channel tape drives in the tape library, using one port for each tape drive.

Gen3 H Series 3300 & 3310 BlackPearl Object Gateway

Interface Type	Number of Ports and Connector Type
Ethernet • 1 GigE • 25 and 100 GigE	Two RJ-45 sockets. Two QSFP28 sockets.
IPMI Management Port	One RJ-45 socket.
SAS (12 Gbps) (Optional)	• Four SFF-8644 sockets per 12 Gbps SAS card provide connections to four 77-bay, or 107-bay disk expansion nodes, using one port per expansion node. • Four SFF-8644 sockets per 12 Gbps SAS card provide connection to sixteen SAS tape drives in the tape library, using one port for four tape drives. **IMPORTANT** If the BlackPearl Object Gateway configuration includes both SAS tape drives and disk expansion nodes, separate HBAs must be used for each device type. If an OSW-2400 SAS Switch is used to connect to both tape drives and disk expansion nodes, a single SAS HBA is allowed.
Fibre Channel (16 Gb or 32 Gb) (Optional)	Four SFP+ optical modules with LC connectors per Fibre Channel card provide connections to four Fibre Channel tape drives in the tape library, using one port for each tape drive.

Gen2 X Series BlackPearl Object Gateway

Interface Type	Number of Ports and Connector Type
Ethernet • 1 Gig E • 100 GigE	One RJ-45 socket Two QSFP28 sockets.
SAS (12 Gbps) (Optional)	• Four SFF-8644 sockets per 12 Gbps SAS card provide connections to four 77-bay, or 107-bay disk expansion nodes, using one port per expansion node. • Four SFF-8644 sockets per 12 Gbps SAS card provide connection to sixteen SAS tape drives, using one port for four tape drives. **IMPORTANT** If the BlackPearl Object Gateway configuration includes both SAS tape drives and disk expansion nodes, separate HBAs must be used for each device type. If an OSW-2400 SAS Switch is used to connect to both tape drives and disk expansion nodes, a single SAS HBA is allowed.
Fibre Channel (16 Gb or 32 Gb) (Optional)	Four SFP+ optical modules with LC connectors per Fibre Channel card provide connections to four Fibre Channel tape drives in the tape library, using one port for each tape drive.

Gen2 S Series and V Series BlackPearl Object Gateway

Interface Type	Number of Ports and Connector Type
Ethernet 1 Gigabit (Gen2 V series only)	Two RJ-45 sockets.
Ethernet 10GBase-T (Gen2 S series only)	Two RJ-45 sockets.
IPMI Management Port	One RJ-45 socket.
Ethernet 10GBase-T (Optional)	Two RJ-45 sockets.
Ethernet (100 GigE) (Optional)	Two SFP28 optical modules with a duplex LC connector per optional 100 GigE NIC.
SAS (12 Gbps) (Optional)	• Four SFF-8644 sockets per 12 Gbps SAS card provide connections to four 77-bay, 96-bay, or 107-bay disk expansion nodes, using one port per expansion node. • Four SFF-8644 sockets per 12 Gbps SAS card provide connection to sixteen SAS tape drives, using one port for four tape drives. **IMPORTANT** If the BlackPearl Object Gateway configuration includes both SAS tape drives and disk expansion nodes, separate HBAs must be used for each device type. If an OSW-2400 SAS Switch is used to connect to both tape drives and disk expansion nodes, a single SAS HBA is allowed.
Fibre Channel (8 Gb or 16 Gb) (Optional)	Four SFP+ optical modules with LC connectors per Fibre Channel card provide connections to four Fibre Channel tape drives in the tape library, using one port for each tape drive.

Gen1 S Series and Gen1 V Series BlackPearl Object Gateway

Interface Type	Number of Ports and Connector Type
Ethernet (1000BaseT, 10GBase-T)	Two RJ-45 sockets.
IPMI Management Port	One RJ-45 socket
Ethernet (10 GigE)	Two SFP+ optical modules with a duplex LC connector per optional 10 GigE NIC.
Ethernet (40 GigE)	Two QSFP+ optical modules with a duplex LC connector per optional 40 GigE NIC.
SAS (6 Gbps) (Optional)	• Four SFF-8644 sockets per optional 6 Gbps SAS card provide connections to two 44-bay expansion nodes, using two ports for each expansion node. • Four SFF-8644 sockets per optional 6 Gbps SAS card provide connections to 16 SAS tape drives, using one port for four tape drives. **IMPORTANT** If the BlackPearl Object Gateway configuration includes both SAS tape drives and disk expansion nodes, separate HBAs must be used for each device type. If an OSW-2400 SAS Switch is used to connect to both tape drives and disk expansion nodes, a single SAS HBA is allowed.
SAS (12 Gbps) (Optional)	• Two or four SFF-8644 sockets per optional 12 Gbps SAS card provide connections to two or four 77-bay, 96-bay, or 107-bay disk expansion nodes, using one port per expansion node. • Two or four SFF-8644 sockets per optional 12 Gbps SAS card provide connection to eight or sixteen SAS tape drives, using one port for four tape drives. **IMPORTANT** If the BlackPearl Object Gateway configuration includes both SAS tape drives and disk expansion nodes, separate HBAs must be used for each device type. If an OSW-2400 SAS Switch is used to connect to both tape drives and disk expansion nodes, a single SAS HBA is allowed.
Fibre Channel (8 Gb) (Optional)	Two or four SFP+ optical modules with LC connectors per optional 8 Gb Fibre Channel card provide connections to two Fibre Channel tape drives in the tape library, using one port for each tape drive.

Expansion Node and Tape Drive Interface Connectors

Interface Type	Number of Ports and Connector Type
44-Bay Expansion Node	Two SFF-8088 ports per 44-bay expansion node. Both ports are required to connect the expansion node to a BlackPearl Object Gateway.
77-Bay Expansion Node	• Four SFF-8644 ports per expander in the 77-bay expansion node. Maximum of two expanders. • One 1 GigE Ethernet port per expander in the 77-bay expansion node. Maximum of two expanders.
96-Bay Expansion Node	Two SFF-8644 ports per 96-bay expansion node. Only a single port is required to connect the expansion node to a BlackPearl Object Gateway.
107-Bay Expansion Node	• Four SFF-8644 ports per expander in the 107-bay expansion node. Maximum of two expanders. • One 1 GigE Ethernet port per expander in the 107-bay expansion node. Maximum of two expanders.
SAS Tape Drive	• **T50e library:** Two SFF-8088 ports per tape drive. Only a single port is required to connect the tape drive to a BlackPearl Object Gateway. Either port can be used for the connection. • **All other libraries:** One SFF-8088 port per tape drive. The single port is required to connect the tape drive to a BlackPearl Object Gateway.
Fibre Channel Tape Drive	• **T50e and T120 libraries:** One multimode optical LC port per tape drive. The single port is required to connect the tape drive to a BlackPearl Object Gateway • **All other libraries:** Two multimode optical LC ports per tape drive. Only a single port is required to connect the tape drive to a BlackPearl Object Gateway. Either port can be used for the connection.

Network Interface Cables

The type of cables required to connect the BlackPearl Object Gateway to an Ethernet network, a 44-bay, 77-bay, 96-bay, or 107-bay expansion node, a SAS tape drive, or a Fibre Channel tape drive depend on the type of interface.

Interface Type	Cable Requirements
Ethernet (10GBase-T or 10/100/1000Base-T)	**10GBase-T** - Shielded Category 6A data-grade cable with an RJ-45 connector. **10/100/1000Base-T** - Shielded Category 5 data-grade cable with an RJ-45 connector. **Note:** Cables to be provided by the customer.

Interface Type	Cable Requirements
Ethernet (10 GigE)	SFP+ transceiver multimode optical cable with duplex LC connectors. **Note:** Cables to be provided by the customer.
Ethernet (25 GigE)	SFP28 transceiver multimode optical cable with duplex LC connectors. **Note:** Cables to be provided by the customer.
Ethernet (40 GigE)	QSFP+ transceiver MPT optical cables with duplex LC connectors, or copper cables with QSFP+ connector. **Note:** Cables to be provided by the customer.
Ethernet (100 GigE)	100 GbE QSFP28 cable. **Note:** Cables to be provided by the customer.
SAS	**44-bay expansion node:** 6 Gbps 4 lane cable with SFF-8644 and SFF-8088 connectors. Two SAS cables are required for each 44-bay expansion node. **Note:** Two SAS cables are included with each 44-bay expansion node. **77-bay expansion node:** 12 Gbps cable with SFF-8644 connectors. One SAS cable is required for each 77-bay expansion node. **96-bay expansion node:** 12 Gbps cable with SFF-8644 connectors. One SAS cable is required for each 96-bay expansion node. **107-bay expansion node:** 12 Gbps cable with SFF-8644 connectors. One SAS cable is required for each 107-bay expansion node. **Note:** One SAS cable is included with each 96-bay expansion node or 107-bay expansion node. **SAS tape drive:** 6 Gbps 4 lane fan-out cable with SFF-8644 and four SFF-8088 connectors. One SAS cable is required for every four SAS tape drives. **Note:** Cables to be provided by the customer.
Fibre Channel	50 micron—400-M5-SN-I classification optical cable with LC connectors. One fiber cable is required for each Fibre Channel tape drive. **Note:** Cables to be provided by the customer.

Networking Naming Conventions

SFP naming (LC fiber)

- 1G is SFP
- 10G is SFP+
- 25G is SFP28

QSFP naming (MPO/MTP fiber)

- 40G is QSFP+ (4 lanes)
- 50G is QSFP28 (2 lanes)
- 100G is QSFP28 (4 lanes)

Universal Serial Bus (USB) Support

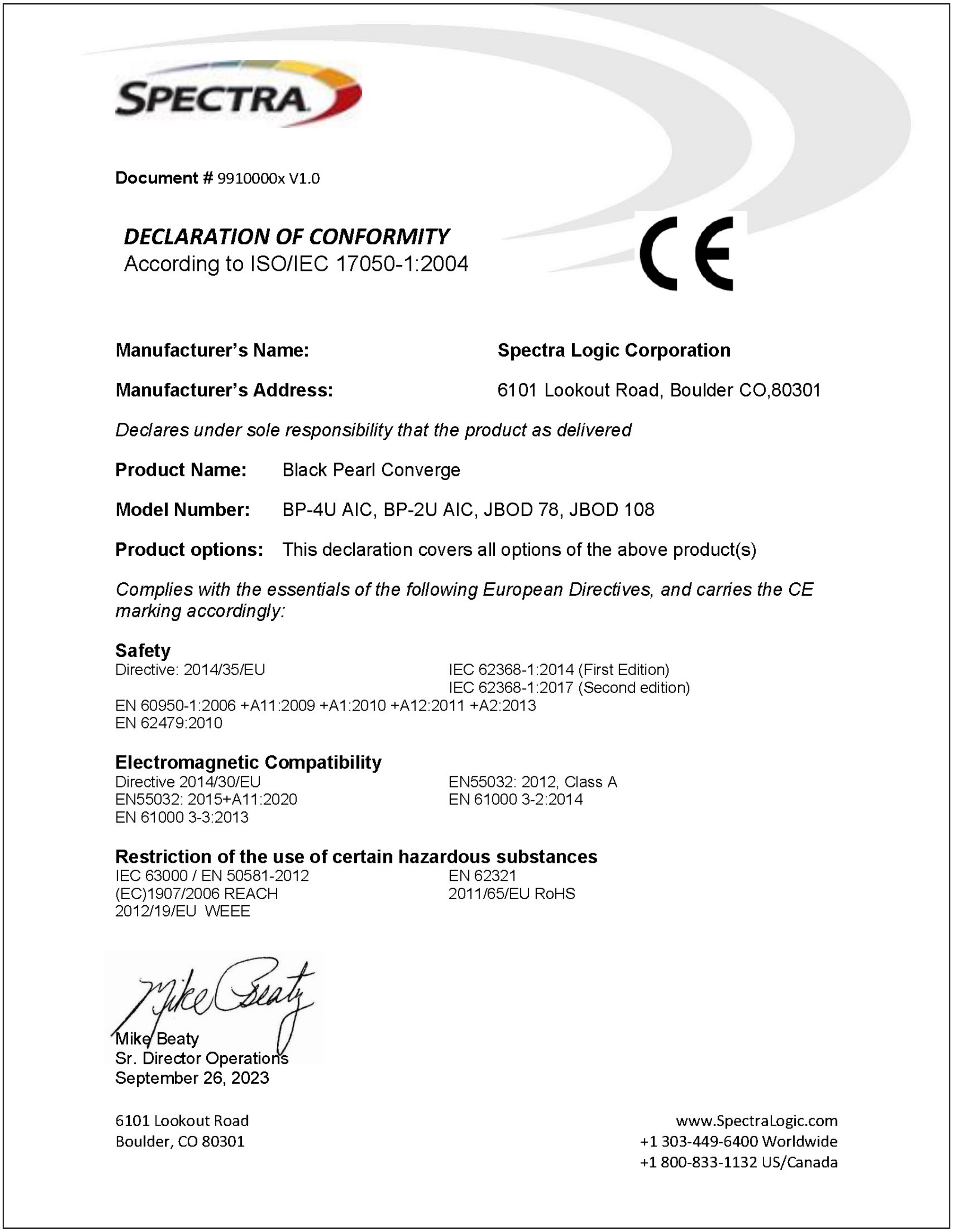
Spectra Logic supports using the USB ports on the Gateway for the following:

- USB mass storage devices (for example, flash drives)
- Keyboards & pointer devices (for example, a computer mouse)
- CD or DVD drives with USB interface

Appendix C - Regulatory & Safety Standards

The Spectra BlackPearl Object Gateway complies with the safety and regulatory agency standards listed below when installed by a Spectra Logic certified engineer or third-party provider.

EU Declaration of Conformity



SPECTRA

Document # 9910000x V1.0

DECLARATION OF CONFORMITY
According to ISO/IEC 17050-1:2004

CE

Manufacturer's Name: **Spectra Logic Corporation**

Manufacturer's Address: 6101 Lookout Road, Boulder CO,80301

Declares under sole responsibility that the product as delivered

Product Name: Black Pearl Converge

Model Number: BP-4U AIC, BP-2U AIC, JBOD 78, JBOD 108

Product options: This declaration covers all options of the above product(s)

Complies with the essentials of the following European Directives, and carries the CE marking accordingly:

Safety
Directive: 2014/35/EU
IEC 62368-1:2014 (First Edition)
IEC 62368-1:2017 (Second edition)
EN 60950-1:2006 +A11:2009 +A1:2010 +A12:2011 +A2:2013
EN 62479:2010

Electromagnetic Compatibility
Directive 2014/30/EU
EN55032: 2012, Class A
EN55032: 2015+A11:2020
EN 61000 3-2:2014
EN 61000 3-3:2013

Restriction of the use of certain hazardous substances
IEC 63000 / EN 50581-2012
EN 62321
(EC)1907/2006 REACH
2011/65/EU RoHS
2012/19/EU WEEE

Mike Beaty

Mike Beaty
Sr. Director Operations
September 26, 2023

6101 Lookout Road
Boulder, CO 80301

www.SpectraLogic.com
+1 303-449-6400 Worldwide
+1 800-833-1132 US/Canada

Directive	Compliance
EU EMC Directive 89/336/EEC	Essential health and safety requirements relating to electromagnetic compatibility.
EN 55022 (CISPER 22) Class A	Limits and methods of measurements of radio interference characteristics of information technology equipment.
EN 55024	1998, Information Technology Equipment - Immunity Characteristics Limits and Methods of Measurement.
EN 61000-4-2	1995 + A1:1998+A2: 2001, Electrostatic Discharge
EN 61000-4-3	1995 + A1:1998 + A2:2001, ENV 50204: 1995, Radiated RF Immunity
EN 61000-4-4	1995 + A1:2001, Electrical Fast Transient/Burst
EN 61000-4-5	1995 + A1:2001 + A2:2001, Surge Immunity
EN 61000-4-6	1996 + A1:2001 + A2:2001, Conducted RF Immunity
EN 61000-4-8	1994 + A1:2001, Power Frequency H-field Immunity
EN 61000-4-11	1994 + A1:2001, Voltage Dips and Interrupts
EN 61000-3-2	2000, Power Line Harmonics
EN 61000-3-3	1995, Power Line Flicker
EC Low Voltage Directive 72/336/EEC	Essential health and safety requirements relating to electrical equipment designed for use with certain violate limits.
EN 60950-1 (EN 60950-1)	Safety requirements of information technology equipment including electrical machines.

Certifications

Country	Certification	Covers [a]
Australia	RCM	826-9, 847-12, 847JBOD-14, SP-5, JBOD 108
Canada	UL	826-9, 847-12, 847JBOD-14, SP-5, JBOD 108
EU	CE	826-9, 847-12, 847JBOD-14, SP-5, JBOD 108
Mexico	NOM	826-9, 847-12, 847JBOD-14, SP-5, JBOD 108
USA	UL, FCC	826-9, 847-12, 847JBOD-14, SP-5, JBOD 108
Japan	VCCI	826-9, 847-12, 847JBOD-14, SP-5, JBOD 108

The BlackPearl Object Gateway complies with all safety-relevant provisions referring to:

- Protection against electrical hazards
- Protection against hazards such as:
  - Mechanical hazards
  - Fire hazards
  - Noise
  - Vibration

The safety issues of this information technology equipment type have been evaluated by a government-accredited European third-party organization, such as Nemko.

[a] The BlackPearl 4U System is regulatory model number "826-9", The BlackPearl 2U System is regulatory model number "847-12". The 44-Bay Expansion Node is regulatory model number "847JBOD-14", The 96-Bay Expansion Node is regulatory model number "BSP-5". The 107-Bay Expansion Node is regulatory model number "JBOD 108"

CE Marking

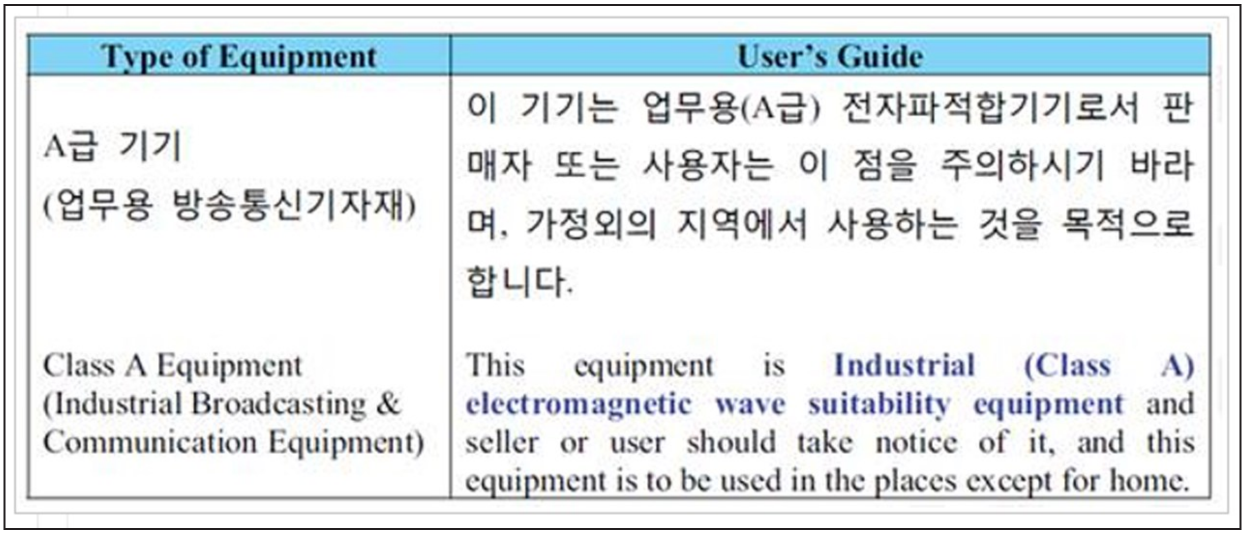
The CE marking is affixed on this device according to Article 10 of the EU Directive 90/336/EEC.

Note: To meet CE certification requirements, you must be running the BlackPearl Object Gateway on uninterpretable power supplies.

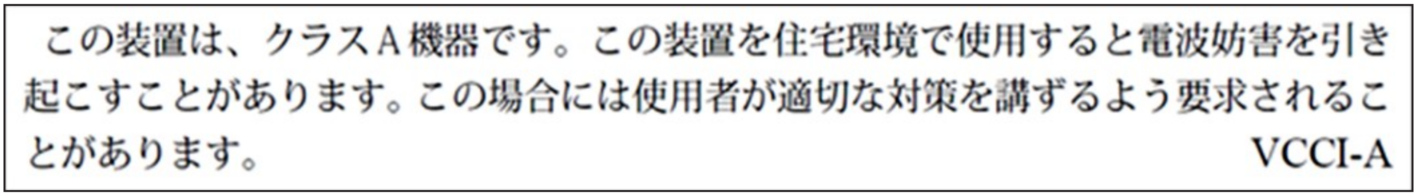
FCC Notice

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to CFR 47 Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user is required to correct the interference at the user's own expense.

Class A Emissions Warning



Type of Equipment	User's Guide
A급 기기 (업무용 방송통신기자재)	이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.
Class A Equipment (Industrial Broadcasting & Communication Equipment)	This equipment is **Industrial (Class A) electromagnetic wave suitability equipment** and seller or user should take notice of it, and this equipment is to be used in the places except for home.



この装置は、クラスＡ機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

LASER WARNING

Optical Transceivers

A Class 1 laser assembly, in the optical transceiver, is mounted on each Fibre Channel or Ethernet electronics card. This laser assembly is registered with the DHHS and is in compliance with IEC825. These products contain components that comply with performance standards that are set by the U.S. Food and Drug administration. This means that these products belong to a class of laser products that do not emit hazardous laser radiation. This classification was accomplished by providing the necessary protective housings and scanning safeguards to ensure that laser radiation is inaccessible during operation or is within Class 1 limits. External safety agencies have reviewed these products and have obtained approvals to the latest standards as they apply to this product type.

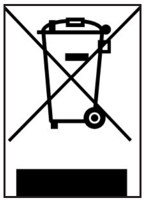
Safety Standards and Compliance

The Spectra BlackPearl Object Gateway complies with the following domestic and international product safety standards.

- EN 60950-1 Second Edition
- UL 60950-1 Second Edition
- CSA-C22.2 No. 60950-1-03
- Low Voltage Directive (EU: CE Mark)

Waste of Electronic and Electrical Equipment (WEEE) Directive

The following symbol on the back of this product indicates that this product meets the European Directive 2000/96/EC on Waste Electrical and Electronic Equipment known as the WEEE directive. This directive, only applicable in European Union countries, indicates that this product should not be disposed of with normal unsorted municipal waste.



Within participating European Union countries, special collection, recycling, and disposal arrangement have been established for this product. At the end of life, the product user should dispose of this product using special WEEE collection systems. These special systems mitigate the potential affects on the environment and human health that can result from hazardous substances that may be contained in this product.

European Union users should contact their local waste administration for WEEE collection instructions for this product.

Restriction of Hazardous Substances in Electrical and Electronic Equipment (RoHS)

The RoHS marking indicates that this product is in compliance with European Council Directive 2011/65/2008, on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

Conflict Minerals Policy

Spectra Logic is committed to complying with the OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas, as well as the applicable requirements of Section 1502 of the Dodd-Frank Act, which aims to prevent the use of minerals that directly or indirectly finance or benefit armed groups in the Democratic Republic of the Congo (DRC) or in adjoining countries (“conflict minerals”).

Affected suppliers to Spectra Logic will be required to commit to being or becoming “conflict-free” (which means that such supplier does not source conflict minerals) and sourcing, where possible, only from conflict-free smelters. Each affected supplier to Spectra Logic will be required to provide completed EICC-GeSI declarations evidencing such supplier's commitment to becoming conflict-free and documenting countries of origin for the tin, tantalum, tungsten, and gold that it purchases.

For more information on Spectra Logic's conflict minerals program contact Spectra Logic for more information.

Recycling Your System

For information on recycling your Spectra Gateway, check the Spectra Logic website at: *spectralogic.com/environment*.

APPENDIX D - OPEN SOURCE CODE ACKNOWLEDGMENTS & PACKAGE LIST

This appendix contains the licenses and notices for open source software used in the BlackPearl Object Gateway. If you have any questions or want to receive a copy of the free/open source software to which you are entitled under the applicable free/open source license(s) (such as the Common Development and Distribution License (CCDL)), contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

APACHE

Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License.

You may obtain a copy of the License at:

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

FreeBSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE FREEBSD PROJECT ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FREEBSD PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the FreeBSD Project.

Java

ORACLE AMERICA, INC. ("ORACLE"), FOR AND ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES UNDER COMMON CONTROL, IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. BY SELECTING THE "ACCEPT LICENSE AGREEMENT" (OR THE EQUIVALENT) BUTTON AND/OR BY USING THE SOFTWARE YOU ACKNOWLEDGE THAT YOU HAVE READ THE TERMS AND AGREE TO THEM. IF YOU ARE AGREEING TO THESE TERMS ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE LEGAL AUTHORITY TO BIND THE LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO BE BOUND BY THE TERMS, THEN SELECT THE "DECLINE LICENSE AGREEMENT" (OR THE EQUIVALENT) BUTTON AND YOU MUST NOT USE THE SOFTWARE ON THIS SITE OR ANY OTHER MEDIA ON WHICH THE SOFTWARE IS CONTAINED.

1. DEFINITIONS. "Software" means the software identified above in binary form that you selected for download, install or use (in the version You selected for download, install or use) from Oracle or its authorized licensees, any other machine readable materials (including, but not limited to, libraries, source files, header files, and data files), any updates or error corrections provided by Oracle, and any user manuals, programming guides and other documentation provided to you by Oracle under this Agreement. "General Purpose Desktop Computers and Servers" means computers, including desktop and laptop computers, or servers, used for general computing functions under end user control (such as but not specifically limited to email, general purpose Internet browsing, and office suite productivity tools). The use of Software in systems and solutions that provide dedicated functionality (other than as mentioned above) or designed for use in embedded or function-specific software applications, for example but not limited to: Software embedded in or bundled with industrial control systems, wireless mobile telephones, wireless handheld devices, kiosks, TV/STB, Blu-ray Disc devices, telematics and network control switching equipment, printers and storage management systems, and other related systems are excluded from this definition and not licensed under this Agreement. "Programs" means (a) Java technology applets and applications intended to run on the Java Platform, Standard Edition platform on Java-enabled General Purpose Desktop Computers and Servers; and (b) JavaFX technology applications intended to run on the JavaFX Runtime on JavaFX-enabled General Purpose Desktop Computers and Servers. “Commercial Features” means those features identified in Table 1-1 (Commercial Features In Java SE Product Editions) of the Java SE documentation accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html. “README File” means the README file for the Software accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html.

2. LICENSE TO USE. Subject to the terms and conditions of this Agreement including, but not limited to, the Java Technology Restrictions of the Supplemental License Terms, Oracle grants you a non-exclusive, non-transferable, limited license without license fees to reproduce and use internally the Software complete and unmodified for the sole purpose of running Programs. THE LICENSE SET FORTH IN THIS SECTION 2 DOES NOT EXTEND TO THE COMMERCIAL FEATURES. YOUR RIGHTS AND OBLIGATIONS RELATED TO THE COMMERCIAL FEATURES ARE AS SET FORTH IN THE SUPPLEMENTAL TERMS ALONG WITH ADDITIONAL LICENSES FOR DEVELOPERS AND PUBLISHERS.

3. RESTRICTIONS. Software is copyrighted. Title to Software and all associated intellectual property rights is retained by Oracle and/or its licensors. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that the Software is developed for general use in a variety of information management applications; it is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use the Software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Oracle or its licensors is granted under this Agreement. Additional restrictions for developers and/or publishers licenses are set forth in the Supplemental License Terms.

4. DISCLAIMER OF WARRANTY. THE SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ORACLE FURTHER DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.

5. LIMITATION OF LIABILITY. IN NO EVENT SHALL ORACLE BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF ORACLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ORACLE'S ENTIRE LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. $1,000).

6. TERMINATION. This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Oracle if you fail to comply with any provision of this Agreement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon termination, you must destroy all copies of Software.

7. EXPORT REGULATIONS. You agree that U.S. export control laws and other applicable export and import laws govern your use of the Software, including technical data; additional information can be found on Oracle's Global Trade Compliance web site (http://www.oracle.com/products/export). You agree that neither the Software nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

8. TRADEMARKS AND LOGOS. You acknowledge and agree as between you and Oracle that Oracle owns the ORACLE and JAVA trademarks and all ORACLE- and JAVA-related trademarks, service marks, logos and other brand designations ("Oracle Marks"), and you agree to comply with the Third Party Usage Guidelines for Oracle Trademarks currently located at

http://www.oracle.com/us/legal/third-party-trademarks/index.html. Any use you make of the Oracle Marks inures to Oracle's benefit.

9. U.S. GOVERNMENT LICENSE RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation shall be only those set forth in this Agreement.

10. GOVERNING LAW. This agreement is governed by the substantive and procedural laws of California. You and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco, or Santa Clara counties in California in any dispute arising out of or relating to this agreement.

11. SEVERABILITY. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

12. INTEGRATION. This Agreement is the entire agreement between you and Oracle relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

SUPPLEMENTAL LICENSE TERMS

These Supplemental License Terms add to or modify the terms of the Binary Code License Agreement. Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement. These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

A. COMMERCIAL FEATURES. You may not use the Commercial Features for running Programs, Java applets or applications in your internal business operations or for any commercial or production purpose, or for any purpose other than as set forth in Sections B, C, D and E of these Supplemental Terms. If You want to use the Commercial Features for any purpose other than as permitted in this Agreement, You must obtain a separate license from Oracle.

B. SOFTWARE INTERNAL USE FOR DEVELOPMENT LICENSE GRANT. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the README File incorporated herein by reference, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Oracle grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the Software complete and unmodified for the purpose of designing, developing, and testing your Programs.

C. LICENSE TO DISTRIBUTE SOFTWARE. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the README File, including, but not limited to the Java Technology Restrictions and Limitations on Redistribution of these Supplemental Terms, Oracle grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software, (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that: (a) is a complete, unmodified reproduction of this Agreement; or (b) protects Oracle's interests consistent with the terms contained in this Agreement and that includes the notice set forth in Section H, and (vi) you agree to defend and indemnify Oracle and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software. The license set forth in this Section C does not extend to the Software identified in Section G.

D. LICENSE TO DISTRIBUTE REDISTRIBUTABLES. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the README File, including but not limited to the Java Technology Restrictions and Limitations on Redistribution of these Supplemental Terms, Oracle grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute those files specifically identified as redistributable in the README File ("Redistributables") provided that: (i) you distribute the Redistributables complete and unmodified, and only bundled as part of Programs, (ii) the Programs add significant and primary functionality to the Redistributables, (iii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README File), (iv) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (v) you only distribute the Redistributables pursuant to a license agreement that: (a) is a complete, unmodified reproduction of this Agreement; or (b) protects Oracle's interests consistent with the terms contained in the Agreement and includes the notice set forth in Section H, (vi) you agree to defend and indemnify Oracle and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software. The license set forth in this Section D does not extend to the Software identified in Section G.

E. DISTRIBUTION BY PUBLISHERS. This section pertains to your distribution of the JavaTM SE Development Kit Software (“JDK”) with your printed book or magazine (as those terms are commonly used in the industry) relating to Java technology ("Publication"). Subject to and conditioned upon your compliance with the restrictions and obligations contained in the Agreement, Oracle hereby grants to you a non-exclusive, nontransferable limited right to reproduce complete and unmodified copies of the JDK on electronic media (the "Media") for the sole purpose of inclusion and distribution with your Publication(s), subject to the following terms: (i) You may not distribute the JDK on a stand-alone basis; it must be distributed with your Publication(s); (ii) You are responsible for downloading the JDK from the applicable Oracle web site; (iii) You must refer to the JDK as JavaTM SE Development Kit; (iv) The JDK must be reproduced in its entirety and without any modification whatsoever (including with respect to all proprietary notices) and distributed with your Publication subject to a license agreement that is a complete, unmodified reproduction of this Agreement; (v) The Media label shall include the following information: “Copyright [YEAR], Oracle America, Inc. All rights reserved. Use is subject to license terms. ORACLE and JAVA trademarks and all ORACLE- and JAVA-related trademarks, service marks, logos and other brand designations are trademarks or registered trademarks of Oracle in the U.S. and other countries.” [YEAR] is the year of Oracle's release of the Software; the year information can typically be found in the Software’s “About” box or screen. This information must be placed on the Media label in such a manner as to only apply to the JDK; (vi) You must clearly identify the JDK as Oracle's product on the Media holder or Media label, and you may not state or imply that Oracle is responsible for any third-party software contained on the Media; (vii) You may not include any third party software on the Media which is intended to be a replacement or substitute for the JDK; (viii) You agree to defend and indemnify Oracle and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of the JDK and/or the Publication; ; and (ix) You shall provide Oracle with a written notice for each Publication; such notice shall include the following information: (1) title of Publication, (2) author(s), (3) date of Publication, and (4) ISBN or ISSN numbers. Such notice shall be sent to Oracle America, Inc., 500 Oracle Parkway, Redwood Shores, California 94065 U.S.A, Attention: General Counsel.

F. JAVA TECHNOLOGY RESTRICTIONS. You may not create, modify, or change the behavior of, or authorize your licensees to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun", “oracle” or similar convention as specified by Oracle in any naming convention designation.

G. LIMITATIONS ON REDISTRIBUTION. You may not redistribute or otherwise transfer patches, bug fixes or updates made available by Oracle through Oracle Premier Support, including those made available under Oracle's Java SE Support program.

H. COMMERCIAL FEATURES NOTICE. For purpose of complying with Supplemental Term Section C.(v)(b) and D.(v)(b), your license agreement shall include the following notice, where the notice is displayed in a manner that anyone using the Software will see the notice:

Use of the Commercial Features for any commercial or production purpose requires a separate license from Oracle. “Commercial Features” means those features identified Table 1-1 (Commercial Features In Java SE Product Editions) of the Java SE documentation accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html

I. SOURCE CODE. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

J. THIRD PARTY CODE. Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME file accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html. In addition to any terms and conditions of any third party opensource/freeware license identified in the THIRDPARTYLICENSEREADME file, the disclaimer of warranty and limitation of liability provisions in paragraphs 4 and 5 of the Binary Code License Agreement shall apply to all Software in this distribution.

K. TERMINATION FOR INFRINGEMENT. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right.

L. INSTALLATION AND AUTO-UPDATE. The Software's installation and auto-update processes transmit a limited amount of data to Oracle (or its service provider) about those specific processes to help Oracle understand and optimize them. Oracle does not associate the data with personally identifiable information. You can find more information about the data Oracle collects as a result of your Software download at http://www.oracle.com/technetwork/java/javase/documentation/index.html.

SAMBA

Samba is provided under the terms of the GNU General Public License (GPL version 3)

For more details and for the full text for each of these licenses, read the LICENSES and COPYING files included with the source packaging of this software.

On Debian GNU/Linux systems, the complete text of the GNU General Public License can be found in `/usr/share/common-licenses/GPL'.

NGINX

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

RUBY

Ruby is copyrighted free software by Yukihiro Matsumoto <matz@netlab.jp>.

You can redistribute it and/or modify it under either the terms of the
2-clause BSDL (see the file BSDL), or the conditions below:

1. You may make and give away verbatim copies of the source form of the software without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.
2. You may modify your copy of the software in any way, provided that you do at least ONE of the following:
    a. place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or by allowing the author to include your modifications in the software.
    b. use the modified software only within your corporation or organization.
    c. give non-standard binaries non-standard names, with instructions on where to get the original software distribution.
    d. make other distribution arrangements with the author.
3. You may distribute the software in object code or binary form, provided that you do at least ONE of the following:
    a. distribute the binaries and library files of the software, together with instructions (in the manual page or equivalent) on where to get the original distribution.
    b. accompany the distribution with the machine-readable source of the software.
    a. give non-standard binaries non-standard names, with instructions on where to get the original software distribution.
    b. make other distribution arrangements with the author.
4. You may modify and include the part of the software into any other software (possibly commercial). But some files in the distribution are not written by the author, so that they are not under these terms.

    For the list of those files and their copying conditions, see the file LEGAL.
5. The scripts and library files supplied as input to or produced as output from the software do not automatically fall under the copyright of the software, but belong to whomever generated them, and may be sold commercially, and may be aggregated with this software.
6. THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Ruby on Rails

ZFS

COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) Version 2.1

INCLUDED PACKAGES

Judy-1.0.5_3

alsa-lib-1.2.2_1

apache-commons-daemon-1.2.4

apr-1.7.0.1.6.1_2

atf-0.21

avahi-app-0.8

awscli-1.20.61

bash-5.1.16

black_pearl-3.0_4

bluestorm_backend-2.0.3206514_7

bluestorm_frontend-2.1.3207762

bluestorm_gui-2.0.3207767_6

bluestorm_mgmt-2.0.3207724

bluestorm_tests-2.0.2886232_1

bluestorm_workers-2.0.3199353_7

boost-libs-1.72.0_7

brotli-1.0.9,1

c-ares-1.18.1

ca_root_nss-3.77

cdbcmd-0.0.3150262,1

compat10x-amd64-10.4.1004000.20181014

compat11x-amd64-11.2.1102000.20181014

ctags-5.8

curl-8.1.2

cyrus-sasl-2.1.28

dbus-1.12.20_5

dbus-glib-0.112

dejavu-2.37_1

dfu-util-0.11_1

dmidecode-3.3

ds3-3.2.0.1701306

e2fsprogs-libuuid-1.46.5

encodings-1.0.5,1

expat-2.5.0

expect-5.45.4_3,1

fieldmod-2.0.0.2867631

fio-3.30

font-bh-ttf-1.0.3_4

font-misc-ethiopic-1.0.4

font-misc-meltho-1.0.3_4

fontconfig-2.13.94_2,1

freetype2-2.12.0

fsx-1.0.2959490_1

fusefs-libs-2.9.9_2

gamin-0.1.10_10

gdb-11.2

gdbm-1.23

gettext-runtime-0.21

giflib-5.2.1

glib-2.70.4_5,2

gmp-6.2.1

gnome_subr-1.0

gnupg-2.3.3_3

gnutls-3.7.9

goserver-0.0.1.3208413_4

graphite2-1.3.14

harfbuzz-4.2.0

icu-71.1,1

indexinfo-0.3.1

intel-ipsec-mb-1.1

iozone-3.491

iperf-2.1.7

iperf3-3.11

ipmitool-1.8.18_3

jansson-2.14

javavmwrapper-2.7.9

jbigkit-2.1_1

jpeg-turbo-2.1.3

jq-1.6

ksh93-93.u_1,2

kyua-0.13_6,3

lcms2-2.12

libICE-1.0.10,1

libSM-1.2.3,1

libX11-1.8.6,1

libXau-1.0.9

libXdmcp-1.1.3

libXext-1.3.4,1

libXfixes-6.0.0

libXi-1.8,1

libXrandr-1.5.2

libXrender-0.9.10_2

libXt-1.2.1,1

libXtst-1.2.3_2

libarchive-3.6.0,1

libassuan-2.5.5

libcyaml-1.3.1

libdaemon-0.14_1

libedit-3.1.20210910,1

libevent-2.1.12

libffi-3.4.2

libfontenc-1.1.4

libgcrypt-1.9.4

libgpg-error-1.45

libiconv-1.16

libidn2-2.3.2

libinotify-20211018

libksba-1.6.0

liblz4-1.9.3,1

libnghttp2-1.46.0

libpsl-0.21.1_4

libpthread-stubs-0.4

libqrencode-4.1.1

libsmi-0.4.8_1

libssh2-1.10.0,3

libsunacl-1.0.1

libtasn1-4.18.0

libunistring-1.0

libunwind-20211201

libuv-1.42.0

libxcb-1.14_1

libxml2-2.9.13_2

libxslt-1.1.35_3

libyaml-0.2.5

llvm14-14.0.1

lnav-0.10.1

logrotate-3.13.0_1

lua52-5.2.4

lua53-5.3.6

lutok-0.4_7

mbuffer-20211018

mhash-0.9.9.9_5

mkfontscale-1.2.1

monit-5.32.0

mpdecimal-2.5.1

mpfr-4.1.0_1

mtx-1.3.12_1

ncurses-6.3

net-snmp-5.9_3,1

netperf-2.7.1.p20170921_1

nettle-3.7.3

nginx-1.24.0_10,3

node16-16.20.1

npth-1.6

oniguruma-6.9.7.1

openjdk17-17.0.2+8.1

openldap24-client-2.4.59_4

p4-2016.1.1492381_3

pam_google_authenticator-1.09,1

pcre-8.45_1

pcre2-10.39_1

pdksh-5.2.14p2_6

perl5-5.32.1_1

pg_cron-1.6.4

pgbadger-11.8

pinentry-1.2.0

pinentry-curses-1.2.0

pkg-1.17.5_1

png-1.6.37_1

popt-1.18_1

postgresql14-client-14.8

postgresql14-contrib-14.8

postgresql14-server-14.8_1

py38-boost-libs-1.72.0_1

py38-boto3-1.18.61

py38-botocore-1.21.61

py38-certifi-2021.10.8

py38-cffi-1.15.0

py38-charset-normalizer-2.0.12

py38-colorama-0.4.4

py38-cryptography-3.3.2

py38-dateutil-2.8.2

py38-docutils-0.17.1,1

py38-idna-3.3

py38-jmespath-0.10.0

py38-openssl-20.0.1,1

py38-passlib-1.7.4

py38-pyasn1-0.4.8

py38-pycparser-2.21

py38-pysocks-1.7.1

py38-requests-2.27.1

py38-rsa-4.8

py38-s3transfer-0.5.0

py38-setuptools-57.0.0

py38-six-1.16.0

py38-urllib3-1.26.9,1

py38-yaml-5.4.1

python-3.8_3,2

python3-3_3

python38-3.8.17

readline-8.1.2

redis-7.0.12

rrdtool-1.7.2_6

ruby-3.0.5,1

ruby30-gems-3.3.11

rubygem-actioncable61-6.1.6

rubygem-actionmailbox61-6.1.6

rubygem-actionmailer61-6.1.6

rubygem-actionpack61-6.1.6

rubygem-actiontext61-6.1.6

rubygem-actionview61-6.1.6

rubygem-activejob61-6.1.6

rubygem-activemodel-serializers-xml-1.0.2_2

rubygem-activemodel61-6.1.6

rubygem-activerecord-import-1.4.0_2

rubygem-activerecord61-6.1.6

rubygem-activeresource-6.0.0_1

rubygem-activestorage61-6.1.6

rubygem-activesupport61-6.1.6

rubygem-addressable-2.8.0

rubygem-aws-eventstream-1.2.0

rubygem-aws-partitions-1.577.0

rubygem-aws-sdk-3.1.0

rubygem-aws-sdk-accessanalyzer-1.29.0

rubygem-aws-sdk-account-1.6.0

rubygem-aws-sdk-acm-1.51.0

rubygem-aws-sdk-acmpca-1.48.0

rubygem-aws-sdk-alexaforbusiness-1.56.0

rubygem-aws-sdk-amplify-1.40.0

rubygem-aws-sdk-amplifybackend-1.17.0

rubygem-aws-sdk-amplifyuibuilder-1.5.0

rubygem-aws-sdk-apigateway-1.76.0

rubygem-aws-sdk-apigatewaymanagementapi-1.30.0

rubygem-aws-sdk-apigatewayv2-1.42.0

rubygem-aws-sdk-appconfig-1.25.0

rubygem-aws-sdk-appconfigdata-1.5.0

rubygem-aws-sdk-appflow-1.26.0

rubygem-aws-sdk-appintegrationsservice-1.13.0

rubygem-aws-sdk-applicationautoscaling-1.62.0

rubygem-aws-sdk-applicationcostprofiler-1.9.0

rubygem-aws-sdk-applicationdiscoveryservice-1.44.0

rubygem-aws-sdk-applicationinsights-1.30.0

rubygem-aws-sdk-appmesh-1.45.0

rubygem-aws-sdk-appregistry-1.15.0

rubygem-aws-sdk-apprunner-1.13.0

rubygem-aws-sdk-appstream-1.65.0

rubygem-aws-sdk-appsync-1.52.0

rubygem-aws-sdk-athena-1.53.0

rubygem-aws-sdk-auditmanager-1.23.0

rubygem-aws-sdk-augmentedairuntime-1.22.0

rubygem-aws-sdk-autoscaling-1.78.0

rubygem-aws-sdk-autoscalingplans-1.40.0

rubygem-aws-sdk-backup-1.43.0

rubygem-aws-sdk-backupgateway-1.3.0

rubygem-aws-sdk-batch-1.61.0

rubygem-aws-sdk-billingconductor-1.0.0

rubygem-aws-sdk-braket-1.18.0

rubygem-aws-sdk-budgets-1.49.0

rubygem-aws-sdk-chime-1.67.0

rubygem-aws-sdk-chimesdkidentity-1.9.0

rubygem-aws-sdk-chimesdkmeetings-1.9.0

rubygem-aws-sdk-chimesdkmessaging-1.10.0

rubygem-aws-sdk-cloud9-1.45.0

rubygem-aws-sdk-cloudcontrolapi-1.7.0

rubygem-aws-sdk-clouddirectory-1.41.0

rubygem-aws-sdk-cloudformation-1.68.0

rubygem-aws-sdk-cloudfront-1.63.0

rubygem-aws-sdk-cloudhsm-1.39.0

rubygem-aws-sdk-cloudhsmv2-1.42.0

rubygem-aws-sdk-cloudsearch-1.40.0

rubygem-aws-sdk-cloudsearchdomain-1.33.0

rubygem-aws-sdk-cloudtrail-1.48.0

rubygem-aws-sdk-cloudwatch-1.64.0

rubygem-aws-sdk-cloudwatchevents-1.57.0

rubygem-aws-sdk-cloudwatchevidently-1.5.0

rubygem-aws-sdk-cloudwatchlogs-1.52.0

rubygem-aws-sdk-cloudwatchrum-1.4.0

rubygem-aws-sdk-codeartifact-1.19.0

rubygem-aws-sdk-codebuild-1.88.0

rubygem-aws-sdk-codecommit-1.51.0

rubygem-aws-sdk-codedeploy-1.49.0

rubygem-aws-sdk-codeguruprofiler-1.24.0

rubygem-aws-sdk-codegurureviewer-1.30.0

rubygem-aws-sdk-codepipeline-1.53.0

rubygem-aws-sdk-codestar-1.38.0

rubygem-aws-sdk-codestarconnections-1.24.0

rubygem-aws-sdk-codestarnotifications-1.19.0

rubygem-aws-sdk-cognitoidentity-1.40.0

rubygem-aws-sdk-cognitoidentityprovider-1.65.0

rubygem-aws-sdk-cognitosync-1.36.0

rubygem-aws-sdk-comprehend-1.60.0

rubygem-aws-sdk-comprehendmedical-1.36.0

rubygem-aws-sdk-computeoptimizer-1.32.0

rubygem-aws-sdk-configservice-1.77.0

rubygem-aws-sdk-connect-1.68.0

rubygem-aws-sdk-connectcontactlens-1.11.0

rubygem-aws-sdk-connectparticipant-1.22.0

rubygem-aws-sdk-connectwisdomservice-1.6.0

rubygem-aws-sdk-core-3.130.1

rubygem-aws-sdk-costandusagereportservice-1.40.0

rubygem-aws-sdk-costexplorer-1.76.0

rubygem-aws-sdk-customerprofiles-1.20.0

rubygem-aws-sdk-databasemigrationservice-1.67.0

rubygem-aws-sdk-dataexchange-1.26.0

rubygem-aws-sdk-datapipeline-1.36.0

rubygem-aws-sdk-datasync-1.45.0

rubygem-aws-sdk-dax-1.39.0

rubygem-aws-sdk-detective-1.28.0

rubygem-aws-sdk-devicefarm-1.51.0

rubygem-aws-sdk-devopsguru-1.23.0

rubygem-aws-sdk-directconnect-1.54.0

rubygem-aws-sdk-directoryservice-1.49.0

rubygem-aws-sdk-dlm-1.50.0

rubygem-aws-sdk-docdb-1.42.0

rubygem-aws-sdk-drs-1.4.0

rubygem-aws-sdk-dynamodb-1.74.0

rubygem-aws-sdk-dynamodbstreams-1.38.0

rubygem-aws-sdk-ebs-1.26.0

rubygem-aws-sdk-ec2-1.307.0

rubygem-aws-sdk-ec2instanceconnect-1.24.0

rubygem-aws-sdk-ecr-1.56.0

rubygem-aws-sdk-ecrpublic-1.12.0

rubygem-aws-sdk-ecs-1.99.0

rubygem-aws-sdk-efs-1.54.0

rubygem-aws-sdk-eks-1.74.0

rubygem-aws-sdk-elasticache-1.76.0

rubygem-aws-sdk-elasticbeanstalk-1.51.0

rubygem-aws-sdk-elasticinference-1.21.0

rubygem-aws-sdk-elasticloadbalancing-1.40.0

rubygem-aws-sdk-elasticloadbalancingv2-1.77.0

rubygem-aws-sdk-elasticsearchservice-1.65.0

rubygem-aws-sdk-elastictranscoder-1.38.0

rubygem-aws-sdk-emr-1.59.0

rubygem-aws-sdk-emrcontainers-1.14.0

rubygem-aws-sdk-eventbridge-1.38.0

rubygem-aws-sdk-finspace-1.11.0

rubygem-aws-sdk-finspacedata-1.14.0

rubygem-aws-sdk-firehose-1.48.0

rubygem-aws-sdk-fis-1.13.0

rubygem-aws-sdk-fms-1.49.0

rubygem-aws-sdk-forecastqueryservice-1.21.0

rubygem-aws-sdk-forecastservice-1.33.0

rubygem-aws-sdk-frauddetector-1.32.0

rubygem-aws-sdk-fsx-1.55.0

rubygem-aws-sdk-gamelift-1.56.0

rubygem-aws-sdk-gamesparks-1.0.0

rubygem-aws-sdk-glacier-1.46.0

rubygem-aws-sdk-globalaccelerator-1.39.0

rubygem-aws-sdk-glue-1.109.0

rubygem-aws-sdk-gluedatabrew-1.22.0

rubygem-aws-sdk-greengrass-1.49.0

rubygem-aws-sdk-greengrassv2-1.17.0

rubygem-aws-sdk-groundstation-1.27.0

rubygem-aws-sdk-guardduty-1.56.0

rubygem-aws-sdk-health-1.47.0

rubygem-aws-sdk-healthlake-1.13.0

rubygem-aws-sdk-honeycode-1.17.0

rubygem-aws-sdk-iam-1.68.0

rubygem-aws-sdk-identitystore-1.15.0

rubygem-aws-sdk-imagebuilder-1.40.0

rubygem-aws-sdk-importexport-1.35.0

rubygem-aws-sdk-inspector-1.43.0

rubygem-aws-sdk-inspector2-1.4.0

rubygem-aws-sdk-iot-1.88.0

rubygem-aws-sdk-iot1clickdevicesservice-1.37.0

rubygem-aws-sdk-iot1clickprojects-1.37.0

rubygem-aws-sdk-iotanalytics-1.49.0

rubygem-aws-sdk-iotdataplane-1.39.0

rubygem-aws-sdk-iotdeviceadvisor-1.14.0

rubygem-aws-sdk-iotevents-1.33.0

rubygem-aws-sdk-ioteventsdata-1.26.0

rubygem-aws-sdk-iotfleethub-1.11.0

rubygem-aws-sdk-iotjobsdataplane-1.36.0

rubygem-aws-sdk-iotsecuretunneling-1.20.0

rubygem-aws-sdk-iotsitewise-1.40.0

rubygem-aws-sdk-iotthingsgraph-1.23.0

rubygem-aws-sdk-iottwinmaker-1.4.0

rubygem-aws-sdk-iotwireless-1.22.0

rubygem-aws-sdk-ivs-1.20.0

rubygem-aws-sdk-kafka-1.49.0

rubygem-aws-sdk-kafkaconnect-1.7.0

rubygem-aws-sdk-kendra-1.48.0

rubygem-aws-sdk-keyspaces-1.2.0

rubygem-aws-sdk-kinesis-1.41.0

rubygem-aws-sdk-kinesisanalytics-1.40.0

rubygem-aws-sdk-kinesisanalyticsv2-1.40.0

rubygem-aws-sdk-kinesisvideo-1.41.0

rubygem-aws-sdk-kinesisvideoarchivedmedia-1.43.0

rubygem-aws-sdk-kinesisvideomedia-1.37.0

rubygem-aws-sdk-kinesisvideosignalingchannels-1.19.0

rubygem-aws-sdk-kms-1.55.0

rubygem-aws-sdk-lakeformation-1.26.0

rubygem-aws-sdk-lambda-1.83.0

rubygem-aws-sdk-lambdapreview-1.35.0

rubygem-aws-sdk-lex-1.45.0

rubygem-aws-sdk-lexmodelbuildingservice-1.57.0

rubygem-aws-sdk-lexmodelsv2-1.23.0

rubygem-aws-sdk-lexruntimev2-1.15.0

rubygem-aws-sdk-licensemanager-1.40.0

rubygem-aws-sdk-lightsail-1.64.0

rubygem-aws-sdk-locationservice-1.21.0

rubygem-aws-sdk-lookoutequipment-1.10.0

rubygem-aws-sdk-lookoutforvision-1.14.0

rubygem-aws-sdk-lookoutmetrics-1.15.0

rubygem-aws-sdk-machinelearning-1.37.0

rubygem-aws-sdk-macie-1.38.0

rubygem-aws-sdk-macie2-1.44.0

rubygem-aws-sdk-managedblockchain-1.32.0

rubygem-aws-sdk-managedgrafana-1.7.0

rubygem-aws-sdk-marketplacecatalog-1.21.0

rubygem-aws-sdk-marketplacecommerceanalytics-1.41.0

rubygem-aws-sdk-marketplaceentitlementservice-1.35.0

rubygem-aws-sdk-marketplacemetering-1.41.0

rubygem-aws-sdk-mediaconnect-1.44.0

rubygem-aws-sdk-mediaconvert-1.88.0

rubygem-aws-sdk-medialive-1.86.0

rubygem-aws-sdk-mediapackage-1.52.0

rubygem-aws-sdk-mediapackagevod-1.36.0

rubygem-aws-sdk-mediastore-1.41.0

rubygem-aws-sdk-mediastoredata-1.38.0

rubygem-aws-sdk-mediatailor-1.54.0

rubygem-aws-sdk-memorydb-1.8.0

rubygem-aws-sdk-mgn-1.12.0

rubygem-aws-sdk-migrationhub-1.40.0

rubygem-aws-sdk-migrationhubconfig-1.20.0

rubygem-aws-sdk-migrationhubrefactorspaces-1.5.0

rubygem-aws-sdk-migrationhubstrategyrecommendations-1.4.0

rubygem-aws-sdk-mobile-1.35.0

rubygem-aws-sdk-mq-1.46.0

rubygem-aws-sdk-mturk-1.40.0

rubygem-aws-sdk-mwaa-1.15.0

rubygem-aws-sdk-neptune-1.45.0

rubygem-aws-sdk-networkfirewall-1.15.0

rubygem-aws-sdk-networkmanager-1.22.0

rubygem-aws-sdk-nimblestudio-1.13.0

rubygem-aws-sdk-opensearchservice-1.10.0

rubygem-aws-sdk-opsworks-1.41.0

rubygem-aws-sdk-opsworkscm-1.52.0

rubygem-aws-sdk-organizations-1.69.0

rubygem-aws-sdk-outposts-1.30.0

rubygem-aws-sdk-panorama-1.7.0

rubygem-aws-sdk-personalize-1.40.0

rubygem-aws-sdk-personalizeevents-1.27.0

rubygem-aws-sdk-personalizeruntime-1.32.0

rubygem-aws-sdk-pi-1.39.0

rubygem-aws-sdk-pinpoint-1.67.0

rubygem-aws-sdk-pinpointemail-1.35.0

rubygem-aws-sdk-pinpointsmsvoice-1.32.0

rubygem-aws-sdk-pinpointsmsvoicev2-1.0.0

rubygem-aws-sdk-polly-1.54.0

rubygem-aws-sdk-pricing-1.37.0

rubygem-aws-sdk-prometheusservice-1.14.0

rubygem-aws-sdk-proton-1.15.0

rubygem-aws-sdk-qldb-1.25.0

rubygem-aws-sdk-qldbsession-1.22.0

rubygem-aws-sdk-quicksight-1.64.0

rubygem-aws-sdk-ram-1.39.0

rubygem-aws-sdk-rds-1.143.0

rubygem-aws-sdk-rdsdataservice-1.34.0

rubygem-aws-sdk-recyclebin-1.2.0

rubygem-aws-sdk-redshift-1.80.0

rubygem-aws-sdk-redshiftdataapiservice-1.19.0

rubygem-aws-sdk-rekognition-1.66.0

rubygem-aws-sdk-resiliencehub-1.4.0

rubygem-aws-sdk-resourcegroups-1.45.0

rubygem-aws-sdk-resourcegroupstaggingapi-1.47.0

rubygem-aws-sdk-resources-3.128.0

rubygem-aws-sdk-robomaker-1.47.0

rubygem-aws-sdk-route53-1.62.0

rubygem-aws-sdk-route53domains-1.40.0

rubygem-aws-sdk-route53recoverycluster-1.11.0

rubygem-aws-sdk-route53recoverycontrolconfig-1.10.0

rubygem-aws-sdk-route53recoveryreadiness-1.10.0

rubygem-aws-sdk-route53resolver-1.37.0

rubygem-aws-sdk-s3-1.113.0

rubygem-aws-sdk-s3control-1.50.0

rubygem-aws-sdk-s3outposts-1.13.0

rubygem-aws-sdk-sagemaker-1.121.0

rubygem-aws-sdk-sagemakeredgemanager-1.11.0

rubygem-aws-sdk-sagemakerfeaturestoreruntime-1.12.0

rubygem-aws-sdk-sagemakerruntime-1.42.0

rubygem-aws-sdk-savingsplans-1.26.0

rubygem-aws-sdk-schemas-1.23.0

rubygem-aws-sdk-secretsmanager-1.59.0

rubygem-aws-sdk-securityhub-1.63.0

rubygem-aws-sdk-serverlessapplicationrepository-1.43.0

rubygem-aws-sdk-servicecatalog-1.70.0

rubygem-aws-sdk-servicediscovery-1.46.0

rubygem-aws-sdk-servicequotas-1.23.0

rubygem-aws-sdk-ses-1.47.0

rubygem-aws-sdk-sesv2-1.27.0

rubygem-aws-sdk-shield-1.48.0

rubygem-aws-sdk-signer-1.38.0

rubygem-aws-sdk-simpledb-1.35.0

rubygem-aws-sdk-sms-1.40.0

rubygem-aws-sdk-snowball-1.49.0

rubygem-aws-sdk-snowdevicemanagement-1.7.0

rubygem-aws-sdk-sns-1.53.0

rubygem-aws-sdk-sqs-1.51.0

rubygem-aws-sdk-ssm-1.134.0

rubygem-aws-sdk-ssmcontacts-1.13.0

rubygem-aws-sdk-ssmincidents-1.13.0

rubygem-aws-sdk-ssoadmin-1.16.0

rubygem-aws-sdk-ssooidc-1.19.0

rubygem-aws-sdk-states-1.48.0

rubygem-aws-sdk-storagegateway-1.67.0

rubygem-aws-sdk-support-1.41.0

rubygem-aws-sdk-swf-1.36.0

rubygem-aws-sdk-synthetics-1.26.0

rubygem-aws-sdk-textract-1.37.0

rubygem-aws-sdk-timestreamquery-1.16.0

rubygem-aws-sdk-timestreamwrite-1.14.0

rubygem-aws-sdk-transcribeservice-1.74.0

rubygem-aws-sdk-transcribestreamingservice-1.42.0

rubygem-aws-sdk-transfer-1.52.0

rubygem-aws-sdk-translate-1.44.0

rubygem-aws-sdk-voiceid-1.6.0

rubygem-aws-sdk-waf-1.47.0

rubygem-aws-sdk-wafregional-1.48.0

rubygem-aws-sdk-wafv2-1.38.0

rubygem-aws-sdk-wellarchitected-1.15.0

rubygem-aws-sdk-workdocs-1.39.0

rubygem-aws-sdk-worklink-1.32.0

rubygem-aws-sdk-workmail-1.49.0

rubygem-aws-sdk-workmailmessageflow-1.21.0

rubygem-aws-sdk-workspaces-1.67.0

rubygem-aws-sdk-workspacesweb-1.3.0

rubygem-aws-sdk-xray-1.47.0

rubygem-aws-sigv2-1.1.0

rubygem-aws-sigv4-1.4.0

rubygem-bindata-2.4.10

rubygem-bindex-0.8.1

rubygem-bluestorm_cli-3.0.0.3155059

rubygem-bootsnap-1.11.1

rubygem-builder-3.2.4

rubygem-bundler-2.3.11,1

rubygem-byebug-11.1.3

rubygem-capybara-3.36.0

rubygem-childprocess-4.1.0

rubygem-colorize-0.8.1

rubygem-concurrent-ruby-1.1.10

rubygem-cookiejar-0.3.3

rubygem-crack-0.4.5

rubygem-crass-1.0.6

rubygem-cucumber-7.1.0_3

rubygem-cucumber-core-10.1.1_1

rubygem-cucumber-create-meta-6.0.4_1

rubygem-cucumber-cucumber-expressions14-14.0.0

rubygem-cucumber-gherkin22-22.0.0

rubygem-cucumber-html-formatter17-17.0.0_1

rubygem-cucumber-messages17-17.1.1

rubygem-cucumber-tag-expressions-4.1.0

rubygem-cucumber-wire-6.2.1_1

rubygem-daemons-1.4.1

rubygem-dalli-3.2.1

rubygem-devdctl-0.1.0.3141754

rubygem-devstat_stat-0.0.1.3141769

rubygem-diff-lcs-1.5.0

rubygem-digest-crc-0.6.4

rubygem-docile-1.4.0

rubygem-ds3-0.0.1.1358398

rubygem-ds3apitest-0.1.0.1759726_8

rubygem-e2mmap-0.1.0

rubygem-ejs-1.1.1

rubygem-em-http-request-1.1.7

rubygem-em-socksify-0.3.2

rubygem-erubi-1.10.0

rubygem-etc-1.3.0

rubygem-eventmachine-1.2.7

rubygem-execjs-2.8.1_2

rubygem-faraday-1.9.3

rubygem-faraday-em_http-1.0.0

rubygem-faraday-em_synchrony-1.0.0

rubygem-faraday-excon-1.1.0

rubygem-faraday-httpclient-1.0.1

rubygem-faraday-multipart-1.0.3

rubygem-faraday-net_http-1.0.1

rubygem-faraday-net_http_persistent-1.2.0

rubygem-faraday-patron-1.0.0

rubygem-faraday-rack-1.0.0

rubygem-faraday-retry-1.0.3

rubygem-faraday_middleware-1.2.0

rubygem-faye-1.4.0

rubygem-faye-websocket-0.11.1

rubygem-ffi-1.15.5

rubygem-ffi-locale-1.0.1_2

rubygem-ffi-ncurses-0.4.0_3

rubygem-fio_rb-1.1.0.2908800

rubygem-freebsd_cam-1.0.7.3188006

rubygem-freebsd_mps-1.1.1.3141765

rubygem-freebsd_ses-1.3.2.3183772

rubygem-globalid-rails61-1.0.0

rubygem-hashdiff-1.0.1

rubygem-http_parser.rb-0.8.0

rubygem-i18n-1.10.0,2

rubygem-i18n-js-3.0.11

rubygem-inifile-3.0.0

rubygem-io-console-0.5.11

rubygem-ipaddress-0.8.3

rubygem-irb-1.4.1

rubygem-jbuilder-rails61-2.11.5

rubygem-jmespath-1.6.1

rubygem-jquery-rails-rails61-4.4.0

rubygem-json-2.5.1

rubygem-json_pure-2.6.1

rubygem-jwt-2.3.0

rubygem-key_verify-1.0.1.3141771

rubygem-libifconfig-0.1.0.2959489_1

rubygem-libxml-ruby-3.2.2_1

rubygem-live_record-0.2.1.3141773

rubygem-liveresource-2.1.2.3180522

rubygem-loofah-2.16.0

rubygem-lsiexp-1.2.4.3175307

rubygem-mail-2.7.1_2,2

rubygem-marcel-1.0.2

rubygem-matrix-0.4.2

rubygem-method_source-1.0.0

rubygem-mime-types-3.4.1

rubygem-mime-types-data-3.2022.0105

rubygem-mini_mime-1.1.2

rubygem-minitest-5.15.0

rubygem-mocha-1.13.0

rubygem-msgpack-1.5.1

rubygem-multi_json-1.15.0

rubygem-multi_test-0.1.2_1

rubygem-multipart-post-2.1.1

rubygem-net-ping-2.0.8

rubygem-net-scp-3.0.0

rubygem-net-ssh-6.1.0,2

rubygem-nio4r-2.5.8

rubygem-nokogiri-1.13.4

rubygem-open4-1.3.4

rubygem-os-1.1.4

rubygem-pam-1.5.2.3141780

rubygem-passenger-nginx-6.0.12_2

rubygem-pg-1.3.5

rubygem-pkg-config-1.4.7

rubygem-pmbus-1.1.2.3141787

rubygem-power_assert-2.0.1

rubygem-pqueue-2.1.0

rubygem-pretty-xml-0.2.2

rubygem-psych-4.0.3

rubygem-public_suffix-4.0.7

rubygem-puma-5.6.4

rubygem-racc-1.6.0

rubygem-rack-2.2.6.2,3

rubygem-rack-proxy-0.7.2

rubygem-rack-test-1.1.0_2

rubygem-rails-dom-testing-rails61-2.0.3

rubygem-rails-html-sanitizer-1.4.2

rubygem-rails61-6.1.6

rubygem-railties61-6.1.6

rubygem-rake-13.0.6

rubygem-rb-kqueue-0.2.8

rubygem-rbcurse-1.5.3

rubygem-rbcurse-core-0.0.14_2

rubygem-rbcurse-extras-0.0.0

rubygem-rdoc-6.4.0

rubygem-redis-4.6.0

rubygem-regexp_parser-2.1.1

rubygem-reline-0.3.1

rubygem-rexml-3.2.5

rubygem-rice-2.2.0

rubygem-rrd-ffi-0.2.14_4

rubygem-rspec-expectations-3.11.0

rubygem-rspec-support-3.11.0

rubygem-ruby-termios-1.1.0

rubygem-ruby2_keywords-0.0.5

rubygem-rubyzip-2.3.2

rubygem-sass-rails-rails61-6.0.0

rubygem-sassc-rails-rails61-2.1.2

rubygem-sassc22-2.2.1

rubygem-selenium-webdriver-4.1.0

rubygem-semantic_range-3.0.0

rubygem-serialport-1.3.2

rubygem-simplecov-0.21.2

rubygem-simplecov-html-0.12.3

rubygem-simplecov_json_formatter-0.1.4

rubygem-smart_data-0.0.2.3141789

rubygem-snmp-1.2.0

rubygem-spectra_acl-1.2.1.2959489_2

rubygem-spectra_cli-1.0.2.3197626

rubygem-spectra_platform-1.3.1.3187661

rubygem-spectra_support-5.0.0.3150998

rubygem-spectra_view-2.3.0.3207748_10

rubygem-spectra_workers-5.0.0.3207786

rubygem-spring-4.0.0

rubygem-sprockets-rails-rails61-3.4.2

rubygem-sprockets3-3.7.2_2

rubygem-sqlite3-1.4.2

rubygem-staf4ruby-0.1.3.3141819,1

rubygem-stringio-3.0.1

rubygem-sys-uname-1.2.2

rubygem-tape_backend-0.1.3163739

rubygem-test-unit-3.5.3

rubygem-thin-1.8.1_2

rubygem-thor-1.2.1

rubygem-thwait-0.2.0

rubygem-tilt-2.0.10

rubygem-turbolinks-5.2.1

rubygem-turbolinks-source-5.2.0

rubygem-tzinfo-2.0.4

rubygem-uglifier-4.2.0

rubygem-uuidtools-2.2.0

rubygem-web-console-rails61-4.2.0

rubygem-webdrivers-5.0.0

rubygem-webmock-3.14.0

rubygem-webpacker-rails61-5.4.3_2

rubygem-webrick-1.7.0

rubygem-websocket-driver-0.7.5

rubygem-websocket-extensions-0.1.5

rubygem-xpath-3.2.0

rubygem-yard-0.9.27

rubygem-zeitwerk-2.5.4

rubygem-zfs-0.0.12.3154388

samba413-4.13.17_5

sedutil-1.12.3198939

sg3_utils-1.45

smartmontools-7.3

smp_utils-0.99

source-highlight-3.1.9_1

spectra_ltfs-2.5.0.0.3136603

sqlite3-3.38.5,1

staf-3.4.26_1

stress-1.0.4_1

stress-ng-0.13.12

t5seeprom-0.0.1366684_1

talloc-2.3.1

tcgstorageapi-1.0_2

tcl86-8.6.12

tdb-1.4.3,1

tevent-0.10.2_1

tidy-html5-5.8.0_2

tiff-4.3.0

tmux-3.2a

tomcat-native-1.2.35

tomcat85-8.5.91

vail-3.1.0_4

verde_hotpair-3.0.3206585

vim-8.2.4669

xorg-fonts-truetype-7.7_1

xorgproto-2021.5

yarn-1.22.18

zfs-stats-1.3.1

zip-3.0_1

zsh-5.8.1

zstd-1.5.2

INDEX