Spectra Logic BlackPearl Nearline 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

BlackPearl, BlueScale, CC, RioBroker, Spectra, SpectraGuard, Spectra Logic, StorCycle, TeraPack, TFinity, TranScale, and Vail are registered trademarks of Spectra Logic Corporation. Attack Hardened, Eon Protect, and PreCal are trademarks of Spectra Logic Corporation. MigrationPass is a service mark of Spectra Logic Corporation. All rights reserved worldwide. All other trademarks and registered trademarks are the property of their respective owners.

Part Number

90990093 Revision Z

Revision History

Revision	Date	Description
U	November 2020	Updated for the BlackPearl OS 5.2 release.
V	August 2021	Updated for the BlackPearl OS 5.3 release.
W	January 2022	Updated for the BlackPearl OS 5.4.1 release.
X	May 2022	Updated for the BlackPearl OS 5.4.3 release.
Y	December 2022	Updated for the BlackPearl OS 5.4.8 release.
Z	April 2023	Updated for the BlackPearl OS 5.6 release.

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

To make sure you have the release notes for the most current version of the BlackPearl Release Notes, check the Spectra Logic Technical Support portal at *support.spectralogic.com/documentations/software-release-notes*. You must sign into the portal before viewing Release Notes. The release notes contain updates to the *User Guide* since the last time it was revised.

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:

- 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");
- 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.

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 **Email:**spectralogic@stortrec.de
Mexico, Central and South America, Asia, Australia, and New Zealand **Phone:** 1.303.449.0160	
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	
Spectra Logic Website: *support.spectralogic.com/documentations*	

Table of Contents

About This Guide 24

Intended Audience 24

Discontinued Components 24

BlackPearlUser Interface Screens 24

Related Information 25

Related Publications 25

Tape Library User Guides 27

Online Forum 27

Chapter 1 - Product Overview 28

Overview 28

Features 29

Components 35

Front Bezel 35

Gen2 X Series 36

Gen2 S Series and Gen2 V Series 40

77-Bay and 107-Bay Expansion Nodes 47

Gen1 S Series, Gen1 P Series, and Gen1 V Series 49

44-Bay Expansion Node 55

96-Bay Expansion Node 58

User Interface 60

Menus 60

Status Icons 64

Supported Browsers 65

Chapter 2 - Initial Configuration 66

Before You Begin 67

Rackmount the Chassis 67

Connect Ethernet Cables 67

Automatically Import Activation Keys 68

Power On the Gateway 69

Configure the BlackPearl Management Port 71

Log Into the BlackPearl User Interface 74

Configure the Data Connection 76

Configure an Aggregate Port Data Connection 76
Configure a Single Port Data Connection 79
Configure a Static Route 80
Create a User 82
Description of User Types 82
Create a User 83
View S3 Credentials 86
Next Steps 87
Chapter 3 - Understanding Advanced Bucket Management 88
Goals of Advanced Bucket Management 90
DS3 Overview 90
DS3 Clients 91
BlackPearl Cache 92
Storage Domains 93
Data Policies 93
Data Persistence Rules 93
Data Replication Rules 94
Tape Export Strategy 94
Tape and Disk Partitions 96
Tape Partitions 96
Tape Drive Reservation 96
Tape Media Inspections 97
Object Storage Disk 98
Storage Disk Pools 98
Special Considerations for Exporting Tapes 99
Tape Export Best Practices 99
Special Considerations for Reading Tapes in a Non-BlackPearl Nearline Gateway Environment 100
Example Configurations 102
Single Copy on Tape 103
Dual Copy on Tape 107
Single Copy on Nearline Object Storage Disk 112
Single Copy on Nearline Object Storage Disk and Tape 116
Single Copy on Nearline Object Storage Disk and Dual Copy on Tape 121
Additional Configurations 127

Chapter 4 - Configuring Advanced Bucket Management 128
Create a Disk Pool 130
Create a Nearline Storage Disk Pool 131
Create an Online Disk Pool 134
Create a Disk Partition 137
Create a Tape Partition 138
Create a Replication Target 139
Create a BlackPearl Target 139
Create an Amazon S3 Target 143
Create a Microsoft Azure Target 147
Create a Storage Domain 150
Add a Storage Domain Member to a Storage Domain 156
Create a Data Policy 159
Add Data Persistence Rules and Replication Rules to a Data Policy 163
Create Data Policy ACLs 169
Create a Bucket 171
Create a New Bucket ACL for a Group 173
Create a New Bucket ACL for a User 174
Transfer Data 176
Chapter 5 - Managing Advanced Bucket Management Settings 177
Manage Buckets 179
Show Bucket Physical Placement 179
Edit a Bucket ACL 179
Delete a Bucket ACL 180
Edit a Bucket 180
Delete a Bucket 182
Manage a Storage Domain 183
Edit a Storage Domain Member 183
Exclude a Storage Domain Member 184
Cancel Storage Domain Member Exclusion 185
Delete a Storage Domain Member 185
Edit a Storage Domain 186
Delete a Storage Domain 187
Manage Data Replication Rules 189
Edit a BlackPearl Data Replication Rule 189

Edit an Amazon S3 Data Replication Rule 190
Edit a Microsoft Azure Data Replication Rule 191
Delete a Data Replication Rule 192
Manage a Data Policy 193
Edit a Data Policy 193
Delete a Data Policy 194
Delete a Data Policy ACL 195
Edit a Data Persistence Rule 195
Delete a Data Persistence Rule 197
Manage Replication Targets 198
Edit a BlackPearl Replication Target 198
Edit an Amazon Replication Target 199
Edit an Azure Replication Target 200
Verify a Replication Target 200
Put a Replication Target in Standby State 201
Activate a Replication Target 202
Delete a Replication Target 203
Manage a Disk Partition 204
Edit a Disk Partition 204
Delete a Disk Partition 205
Manage Online and Nearline Disk Pools 206
Import a Nearline or Online Disk Pool 206
Delete a Nearline or Online Disk Pool 207
Change the BlackPearl Gateway Cache Configuration 209
Chapter 6 - Configuring Network Attached Storage 211
Overview of NAS Storage Pools, Volumes, and Shares 212
Storage Pools 212
Volumes and Shares 212
Naming Considerations 212
Create a NAS Storage Pool 213
Create a Volume 217
Create a Share 226
Create a CIFS Share 226
Create an NFS Share 231
Create a Vail S3 Share 232

Configure NAS Services 234
Configure the CIFS Service 234
Configure the NFI Service 235
Configure the NFS Service 237
Configure NAS Replication 239
Configure the NAS Replication Service 239
Configure the Target System 241
Configure Volumes for NAS Replication 241
Chapter 7 - Managing Network Attached Storage 246
Manage Storage Pools 248
Edit a Storage Pool 248
Expand a Storage Pool 249
Delete a Storage Pool 251
Manage Volumes 252
Move a Volume 252
Cancel a Volume Move 252
Edit a Volume 253
Delete a Volume 256
Volume Snapshots 257
Create a Snapshot 257
Create a Snapshot Schedule 259
Delete a Snapshot Schedule 262
Delete Snapshots 262
Restore to a Snapshot 264
Retrieve a Single File from a Snapshot 265
Manage Shares 267
Edit a CIFS Share 267
Edit an NFS Share 267
Delete a Share 268
Manage NAS Replication 270
Manually Start NAS Replication 270
Cancel a NAS Replication In Progress 271
Restoring Files from a NAS Replication Target 271
Disable NAS Replication for a Volume 272
Edit the NAS Replication Service 273
Delete the NAS Replication Service Configuration 274

Manage NFI Replication 276
Edit the NFI Service 276
Delete the NFI Service Configuration 276
Manually Starting an NFI Replication 277
Reinitialize NFI Replication 277
Edit the NFI Volume Policy 278
Restoring Files From an NFI Target BlackPearl Gateway 278
Chapter 8 - Additional Configuration Options 279
Configure Network Connections and Settings 280
Configure Ethernet Ports 281
Configure DNS Settings 287
Configure SMTP Settings 288
Configure Date and Time 290
Edit the System Name 291
Configure Networking Services 292
Configure the DS3 Service 292
Configure the Active Directory Service 296
Configure the SNMP Service 300
Multi-Factor Authentication 303
Enable the Attack Hardened Service 303
Enable Multi-Factor Authentication for a User 304
Log In to a System Configured to Use Multi-Factor Authentication 306
Update Multi-Factor Authentication for a User 307
Disable Multi-Factor Authentication for a User 309
Disable the Attack Hardened Service 309
Configure a Vail Sphere 310
Register with a Vail Sphere 310
Edit the Vail Service 310
Configure and Use Encryption 311
Configure the Encryption Service 312
Export Encryption Key to USB Drive 316
Change the Encryption Password 318
Unlock the Self-Encrypting Drives 319
Encrypt or Decrypt a Storage Pool 320
PSID Erase an Encryption Drive 321
Configure Users 323

Description of User Types 323
Create a User 323
Edit a User 323
Change S3 Secret Key 326
Delete a User 327
Configure S3 Groups 329
Create an S3 Group 329
Remove an S3 Group Member 331
Edit an S3 Group 332
Delete an S3 Group 332
Configure Certificates 334
Enable Remote Logging 336
Manually Enter Activation Keys 338
Chapter 9 - Working with Tape Libraries and Media 341
Tape Library Best Practices 343
Tape Library Barcode Reporting 343
WORM Media 343
Available TeraPack Magazines 343
BlackPearl System Memory 343
Moving a BlackPearl Nearline to a New Tape Library 344
Tape Terminology 344
Tape Library Support 345
Tape Library Options 346
Activate a Tape Library Partition 346
Put a Tape Library Partition into Standby 347
Delete a Tape Partition 348
Tape Drive Options 349
Tape Drive Reservation 349
Offline a Tape Drive 353
Online a Tape Drive 354
Remove a Tape Drive from a Tape Partition 356
Test Tape Drive 357
Collect Drive Diagnostic Logs 359
Compact a Tape Cartridge 360
Format Managed BlackPearl Tapes 362

Cancel Tape Format 364

Inspect Tapes 365

Manage Tapes Not in Inventory 366

Mark Tape as Exported 366

Delete Lost or Exported Tape 366

Data Migration 367

Chapter 9 - Importing and Exporting Tape Media 369

Import Tapes 370

Imported Tape Object Name Restrictions for Amazon S3 Replication 371

Import Tape Media 371

Import BlackPearl Foreign Tape(s) 373

Import LTFS Foreign Tape(s) 375

Import Requested Tape Media 378

Importing Tape Media in to a TeraPack-Based Library 379

Log Into the User Interface 380

Import the Magazines 381

Import Requested Tape Media 392

Export Tapes 393

Export a Single Tape 394

Cancel Tape Export 395

Edit Tape Export Information Without Exporting Tape Media 395

Export Tapes from a T50e or T120 Library with Multiple Partitions 396

Exporting Tape Media from a TeraPack-Based Library 397

Log Into the User Interface 398

Export the Magazines 399

Chapter 10 - Operating the BlackPearl Nearline Gateway 407

S3 Operations 409

Download an Object 409

Cancel DS3 Jobs 410

Edit an S3 Job 410

Clear All Canceled or Completed Jobs 411

Manually Starting the S3 Data Path Backend 412

Disallow New Jobs 412

Allow New Jobs 413

Monitor the BlackPearl Gateway 414

Front Bezel Visual Status Beacon 415
Configuring the Visual Status Beacon Color 416
System Status LEDs 416
Check System Messages 420
View the Status of Hardware Components 421
View the Status of Services 423
View the Status of NAS Pools 423
View the Status of NAS Volumes 426
View the Status of NAS Shares 426
View the Status of the System Pools 428
View Bucket Contents 430
View DS3 Jobs Information 431
View Tape Media Information 433
View Performance Metrics 438
View Reports 440
Database Backup & Restore 441
Create a Database Backup Schedule 442
Manually Generate a Database Backup 446
Restore from a Database Backup 446
Delete Backup 448
Edit Backup Data Policy 449
Show Backup Physical Placement 449
Exit the BlackPearl User Interface 450
Reboot or Shut Down a BlackPearl Gateway 451
Using the BlackPearl User Interface 451
Power-Cycle Reset 452
Chapter 11 - Using AutoSupport 453
About AutoSupport 454
Enter Contact Information 454
Configure Mail Recipients 455
Create a New Mail Recipient 455
Edit a Mail Recipient 456
Send a Test Email 457
Delete a Mail Recipient 458
Log Sets 459
Configure a Log Set Schedule 459

Manually Generate Log Sets 460
Email a Log Set 461
Download a Log Set 462
Delete Log Sets 462
Chapter 12 - Maintaining the BlackPearl Nearline Gateway 464
Data Integrity Verification - Disk Media 465
Cancel Data Integrity Verification 466
Data Integrity Verification - Tape Media 467
Cancel Tape Media Verification 468
Initiate RSC Backup 469
Access the Technical Support Portal 470
Create an Account 470
Log Into the Portal 471
Configure Automated Software Upload 472
Update the Software 474
Considerations for Updating to BlackPearl OS 5.4 475
Check the Current Software Version 475
Check the Currently Released Software Version 477
Download and Stage the Updated Software 478
Install the Update 479
Installing Data Drives 481
Ensure ESD Protection 481
Install a Drive in a Gen2 S Series Chassis 482
Install a Drive in a Gen2 V Series Chassis 483
Install a Drive in a Gen2 X Series Chassis 484
Install a Drive in a Gen1 Chassis 486
Replace a Failed Component 489
Identify the Failed Component 489
Chapter 13 - FAQ, Troubleshooting, and Support 492
BlackPearl Cache 495
How is Cache Used and Allocated? 495
Why Does the BlackPearl User Interface Display 80% Cache Usage? 495
Tape Partitions 497
How Does a User Upgrade to Later Generations of Media in the Same Tape Library? 497

What Happens When a Tape Partition is Placed in Standby/Quiesced? 497
What Happens When a Tape Partition is Re-Activated? 498
How do I Change the Tape Library Used by the BlackPearl gateway While Minimizing the Impact, Management Time, and System Downtime? 498
Tape Media 499
How Does a User Know if Tape Media is Running Out of Space? 499
Can Data be Overwritten on Existing Tapes? 499
Can WORM Media be Used With the BlackPearl Gateway? 499
Tape Media Import 500
How Does a User Know What Tape Cartridge(s) to Import in Response to a GET Request for Objects on Exported Media? 500
Tape Media Export 501
What Happens if a User Exports a Tape From the Library Before Exporting the Tape in the BlackPearl User Interface? 502
How Does a User Configure Their T50e or T120 Library to Support Exporting Tapes From the BlackPearl Gateway? 502
Tape Drive Cleaning 503
How Does a User Know Their Cleaning Media is Expired? 503
How Does a User Use Cleaning Media in a T50e or T120 Library That Does Not Have a Cleaning Partition? 504
Tape Drive Test 505
How Does a User Test a Tape Drive in a Spectra Logic Library? 505
Collect Drive Diagnostic Logs 506
Write to Tape Drive Test 507
How Does a User Test That Data is Being Written to Tape Media? 507
BlackPearl Database Backup 508
How Does a User Verify the Database Backup Schedule? 508
How Does a User Create a Bucket Isolated Data Policy for the Database Backup Tapes? 508
BlackPearl Disk Storage Data Retention 509
BlackPearl Component Hardware 511
How Does a User Know if a Component of the BlackPearl Gateway Has an Error? 511
Why Do Drives Added to an Expansion Node Fail to Display in the BlackPearl Management Interface? 511
Intelligent Object Management (IOM) 512

Best Practices 512
Using a BlackPearl Gateway with the Vail Application 514
Why Do Vail Jobs Show as Canceled in the BlackPearl User Interface? 514
What Ports Does the BlackPearl Gateway Use to Connect to a Vail Sphere? 514
Special Firewall Feature for Connecting to the BlueScale User Interface 515
Introduction 515
Warning 515
Basic Steps 515
Capacity Mode versus Performance Mode 516
Chunks 516
Performance Mode 516
Capacity Mode 516
Tape Handling Refactor Starting with BlackPearl OS 5.3 518
General BlackPearl Notes 518
Tape Drive Failure Modes 518
Move Failures/Tape Stuck in Drive 519
Library, Drive, and Tape Failure Behavior in BlackPearl version 5.3 519
Enabling iSCSI For Use With the Spectra Swarm 522
Tape Library Errors 525
What is a Data Checkpoint Failure? 525
Troubleshooting 526
Resolve a BlackPearl Management Port IP Address Conflict 536
Using the Console 536
Using a Separate Computer 536
Network Setup Tips 539
Configuration 539
Connectivity to the Network 539
Troubleshooting 541
Tools 542
Spectra Logic Technical Support 544
Before Contacting Support 544
Determine the Gateway Serial Number 544
Opening a Support Ticket 545
Remote Support 550
Enabling Remote Support 550

Disabling Remote Support ... 551

Appendix A - IPMI Configuration ... 553

Appendix B - Specifications ... 556

Data Storage Specifications ... 556

System Specification ... 560

Size and Weight ... 563

Environmental Specifications ... 568

Heat Generation ... 571

Power Requirements ... 571

Input Power Requirements ... 571

Power Cord Specifications ... 573

Interface Specifications ... 577

System Interface Connectors ... 578

Expansion Node and Tape Drive Interface Connectors ... 580

Network Interface Cables ... 581

Networking Naming Conventions ... 582

Universal Serial Bus (USB) Support ... 583

Appendix C - Regulatory & Safety Standards ... 584

EU Declaration of Conformity ... 585

Certifications ... 589

CE Marking ... 590

FCC Notice ... 591

Class A Emissions Warning ... 592

Safety Standards and Compliance ... 593

Waste of Electronic and Electrical Equipment (WEEE) Directive ... 593

Restriction of Hazardous Substances in Electrical and Electronic Equipment (RoHS) ... 593

Recycling Your System ... 594

Conflict Minerals Policy ... 595

Appendix D - Open Source Code Acknowledgments & Package List ... 596

Apache ... 597

FreeBSD ... 598

Java ... 599

Samba ... 606

Nginx 607
Ruby 608
Ruby on Rails 609
ZFS 610
Included Packages 611
Index 633

About This Guide

This guide describes how to configure, monitor, and maintain the Spectra® BlackPearl® Nearline 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 Nearline 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 system 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 Nearline gateway, log into the Support portal (see Access the Technical Support Portal on page 470), and navigate to **Documentation > Product Life Cycle Information**.

BlackPearlUser 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 Nearline 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 Nearline gateway and the DS3 interface, refer to the publications listed in this section.

Spectra BlackPearl Nearline Gateway

The following documents related to the Spectra BlackPearl Nearline 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 gateway in your storage environment.
- The *Spectra BlackPearl Rack Mounting Instructions Guide* provides detailed instructions for installing a Gen1 BlackPearl 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 *Spectra BlackPearl HotPair Installation & Configuration Guide* document provides detailed information on installing and using the BlackPearl gateway in a HotPair configuration.

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 gateway, including information about the latest software releases and documentation updates.
- The *BlackPearl Eon Browser User Guide* provides installation and usage information for the Spectra Eon browser.
- The *Spectra 12- & 36-Drive Chassis HBA Installation Guide* provides instructions for installing an HBA in a Gen1 master node.
- The *Spectra 12- & 36-Drive Chassis Boot Drive Replacement Guide* provides instructions for replacing a failed boot drive in a Gen1 master node.
- The *Spectra 12-, 36- & 45-Drive Chassis Drive Replacement Guide* provides instructions for replacing a failed data drive in a Gen1 master node or 44-bay expansion node.
- The *Spectra 12-, 36- & 45-Drive Chassis Fan Replacement Guide* provides instructions for replacing a failed fan in a Gen1 master node or 44-bay expansion node.
- The *Spectra 12-, 36- & 45-Drive Chassis Power Supply Replacement Guide* provides instructions for replacing a failed power supply in a Gen1 master node or 44-bay expansion node.
- The *Spectra 12-Drive Chassis HBA Replacement Guide* and *Spectra 36-Drive Chassis HBA Replacement Guide* provide instructions for replacing a failed HBA in a Gen1 master node.
- 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.

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*.

IBM Tape Libraries

User Guides for compatible IBM® tape libraries are posted on the IBM Knowledge Center website at: *ibm.com/support/knowledgecenter/products/*.

Online Forum

Need help with Spectra Logic's S3 software development kits or the DS3 API? Post your question at the Spectra Logic S3-SDK discussion forum located at: *https://developer.spectralogic.com/forums*

CHAPTER 1 - PRODUCT OVERVIEW

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

Overview 28

Features 29

Components 35

Front Bezel 35

Gen2 X Series 36

Gen2 S Series and Gen2 V Series 40

77-Bay and 107-Bay Expansion Nodes 47

Gen1 S Series, Gen1 P Series, and Gen1 V Series 49

44-Bay Expansion Node 55

96-Bay Expansion Node 58

User Interface 60

Menus 60

Status Icons 64

Supported Browsers 65

OVERVIEW

The BlackPearl Nearline 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 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 Nearline 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 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 Clients

Users can leverage a library of existing DS3 clients available through the *Spectra Logic Developer Program,* or develop their own client. The user moves data through the client to the BlackPearl gateway and then the gateway handles all interaction with the 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. The first implementation supports bulk object storage operations with tape for accessibility to the lowest cost media option.

Easy Network-Based Administration

The BlackPearl Nearline 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.

Integration with the IBM® TS4500 Tape Library

Fibre Channel HBAs can be installed to provide connectivity to the IBM TS4500 tape library using LTO or TS11*xx* technology drives.

Intelligent Object Management

With IOM, the BlackPearl 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 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 system now offers multi-factor authentication, which enhances the security of your BlackPearl system by using Google Authenticator 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 gateway.

RAID-Protected Data Drives

The base BlackPearl 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 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

Data Replication

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

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.

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.

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 Nearline gateway.

Snapshot Change Threshold

The BlackPearl system now 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

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.

Write Performance Drives

The BlackPearl 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 or a Gen2 X Series 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

For Gen1 master nodes, 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

For Gen1 and Gen2 master 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 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 nine 77-bay and 107-bays expansion nodes can be connected to a Gen2 S or V 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

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 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 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 gateway.

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 gatewaywith 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 Nearline.

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 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.

COMPONENTS

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

Note: For a description of the components on the BlackPearl 1.0 chassis, see BlackPearl 1.0 Chassis Overview & Specifications.

Front Bezel

All BlackPearl chassis include a front bezel. For the 96-bay expansion node (see 96-Bay Expansion Node on page 58), the 77-bay and the 107-bay expansion node (see 77-Bay and 107-Bay Expansion Nodes on page 47), the bezel is permanently attached. For all other chassis, the bezel is attached with magnets.

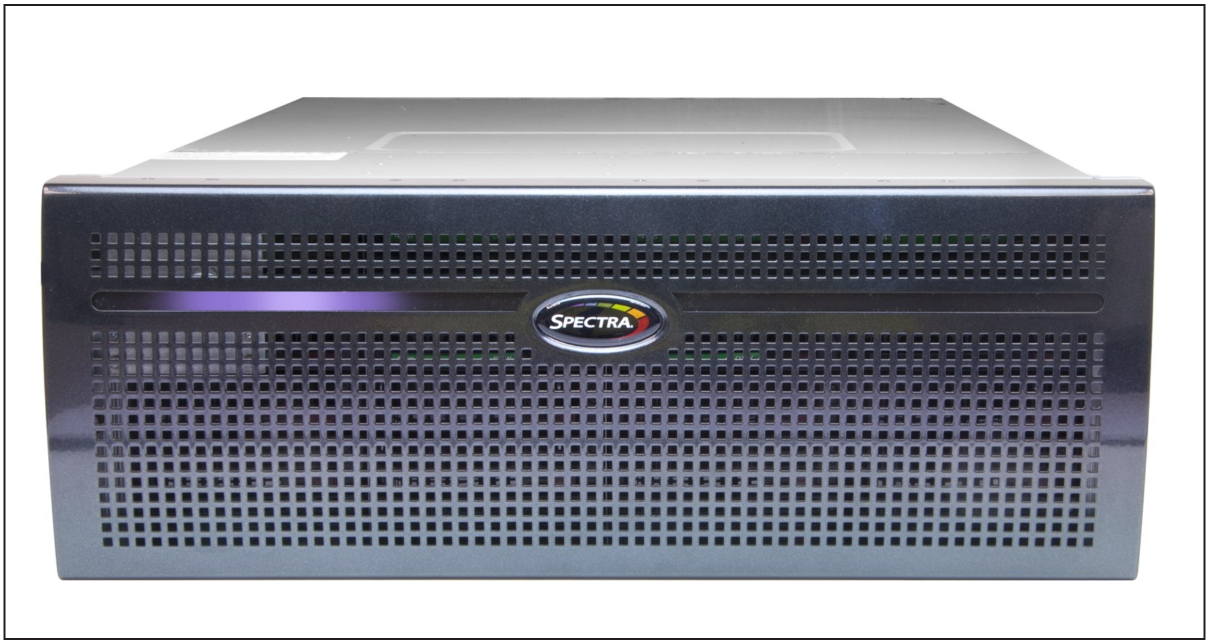


Figure 1 A 4U BlackPearl chassis with front bezel and visual status beacon.

In most cases, the front bezel includes a visual status beacon light bar which provides status information for the gateway. See Front Bezel Visual Status Beacon on page 415 for information about the status indicated by each visual status beacon color/pattern.

Gen2 X Series

Front View

Figure 2 shows the components on the front of the Gen2 X Series BlackPearl gateways with the front bezel removed.

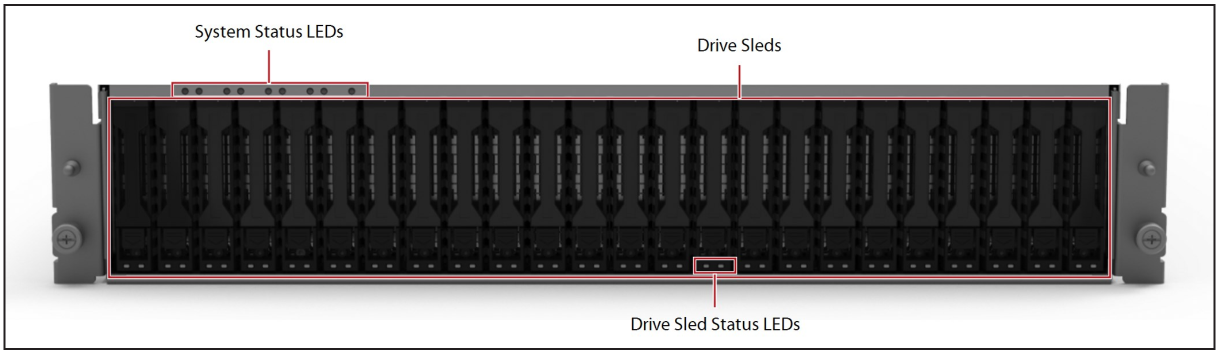


Figure 2 The front view of the Gen2 X Series BlackPearl gateway (front bezel removed).

Component	Description
System status LEDs	The status LEDs indicate power status, fan status, server status, and chassis status. See System Status LEDs on page 416 for more information. **Note:** The LEDs are not visible with the bezel installed.
Data drives	The base Gen2 X Series BlackPearl Nearline 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. 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.
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 show the major components on the rear of the Gen2 X Series BlackPearl chassis.

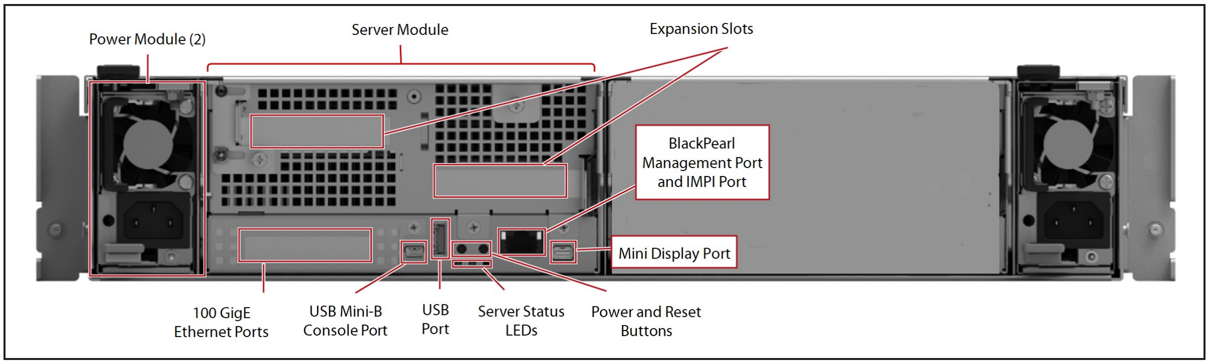


Figure 3 The rear view of the Gen2 X Series BlackPearl gateway.

Component	Description
Power modules	The Gen2 X Series BlackPearl 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.
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.

Component	Description
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 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 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 four 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 4 shows the components on the front of the Gen2 S Series BlackPearl gateway with the front bezel removed. Figure 5 shows the components on the front of the Gen2 V Series BlackPearl gateway with the front bezel removed.

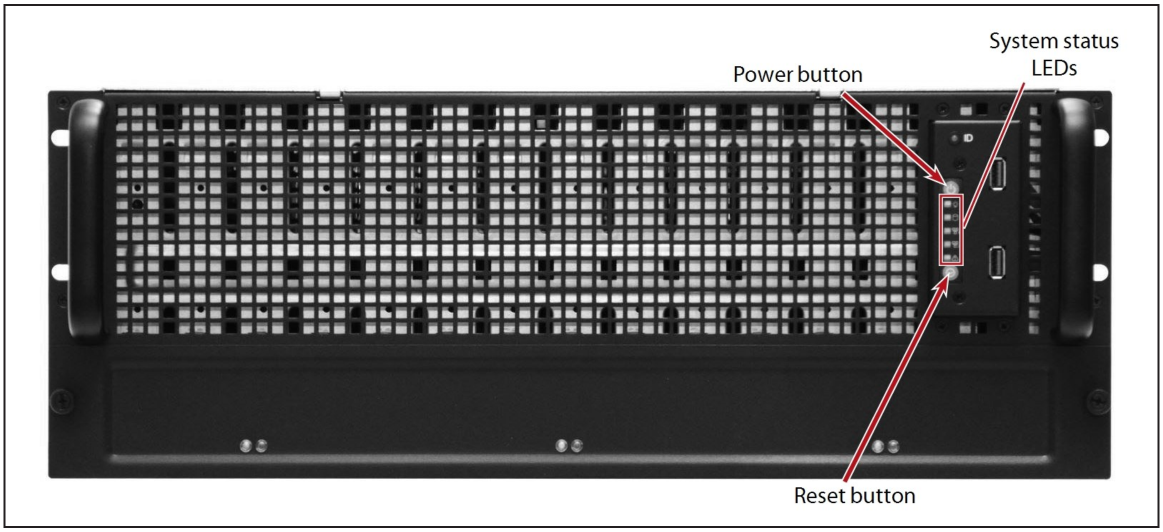


Figure 4 The front view of the Gen2 S Series BlackPearl 4U gateway (front bezel removed).

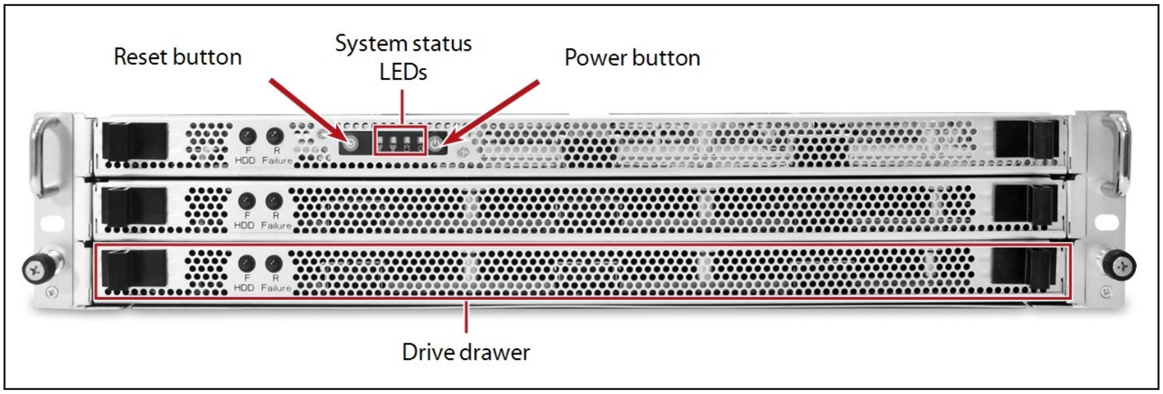


Figure 5 The front view of the Gen2 V Series BlackPearl 2U gateway (front bezel removed).

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 System Status LEDs on page 416 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 Nearline gateway may optionally contain solid state drives to improve NAS write performance. See Write Performance Drives on page 32 for more information.

Rear View

Figure 6 shows the major components on the rear of the Gen2 S BlackPearl gateway. Figure 7 shows the major components on the rear of the Gen2 V Series BlackPearl gateway.

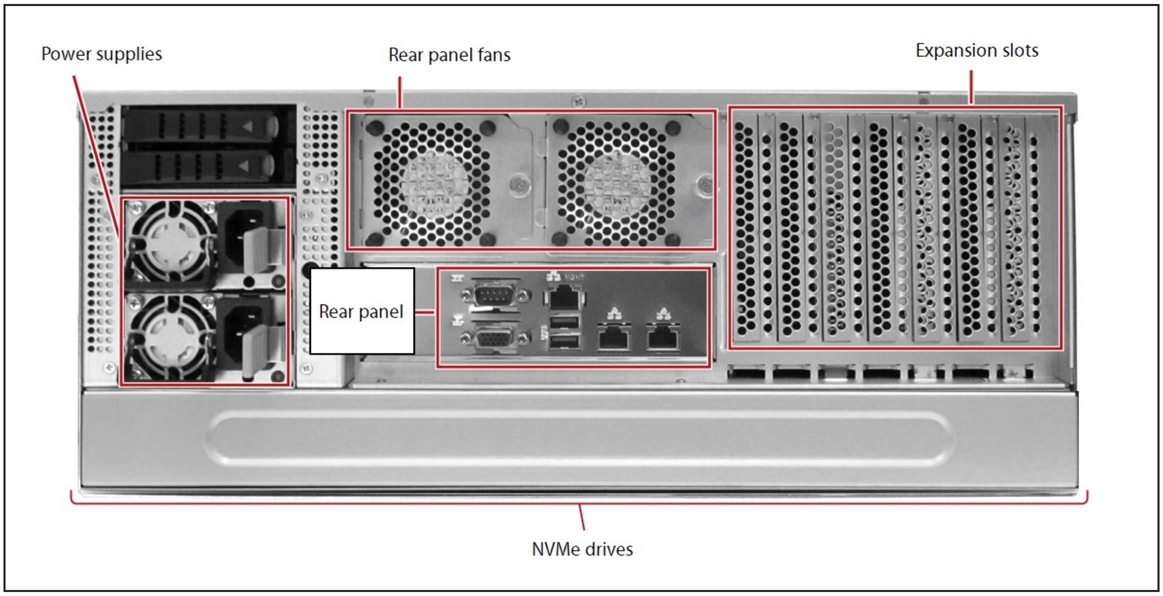


Figure 6 The rear view of the Gen2 S Series BlackPearl 4U gateway.

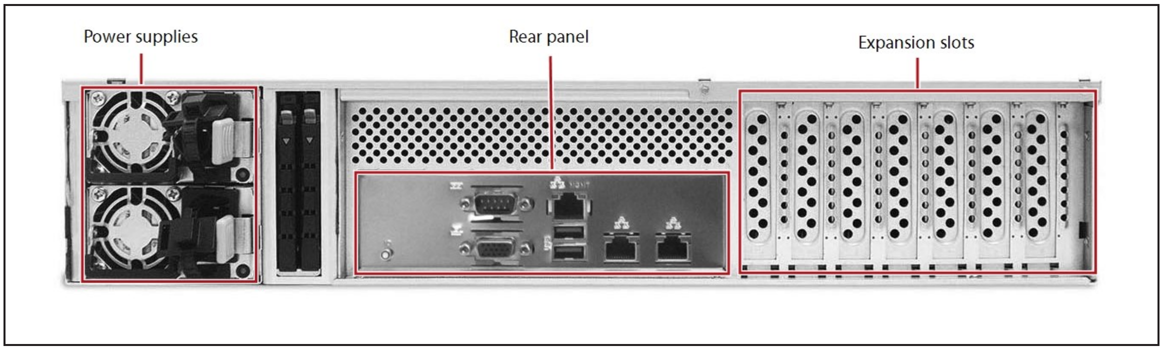


Figure 7 The rear view of the Gen2 V Series BlackPearl 2U gateway.

Component	Description
Power supplies	The standard BlackPearl 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 page for 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 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 8 shows the components on the rear panel of the Gen2 S Series and Gen 2 V Series BlackPearl 4U and 2U master nodes.

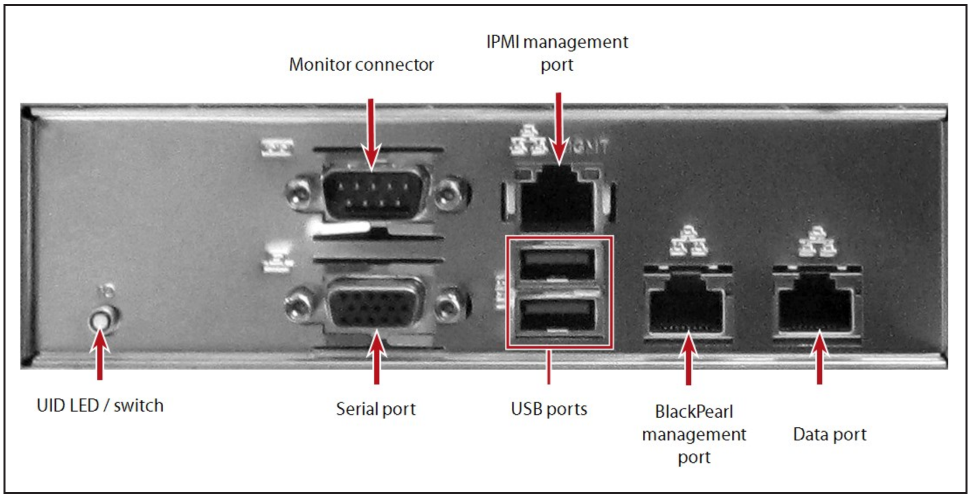


Figure 8 The Gen2 S Series and Gen 2 V Series BlackPearl rear panel components.

Component	Description
UID LED / switch	Pressing the unit ID LED / switch displays a flashing blue pattern on the visual status beacon (see Front Bezel Visual Status Beacon on page 415) 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 553 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 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 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 Nearline gateway. The BlackPearl management port cannot be used for data transfer.

77-Bay and 107-Bay Expansion Nodes

Front View

Figure 9 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.

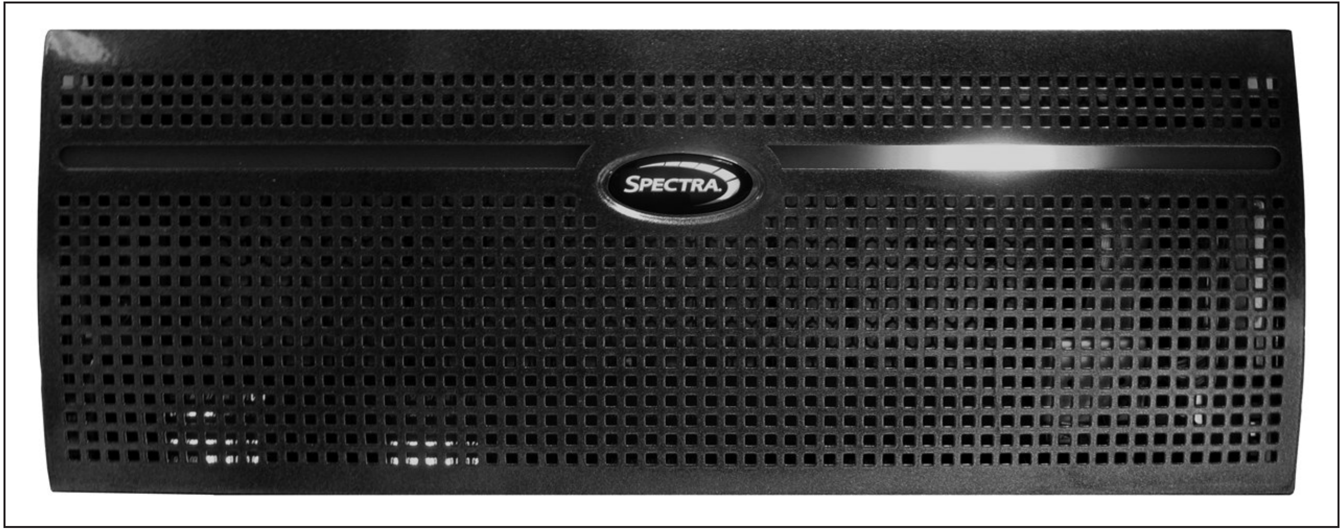


Figure 9 The front view of the 77-bay and 107-bay expansion nodes.

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

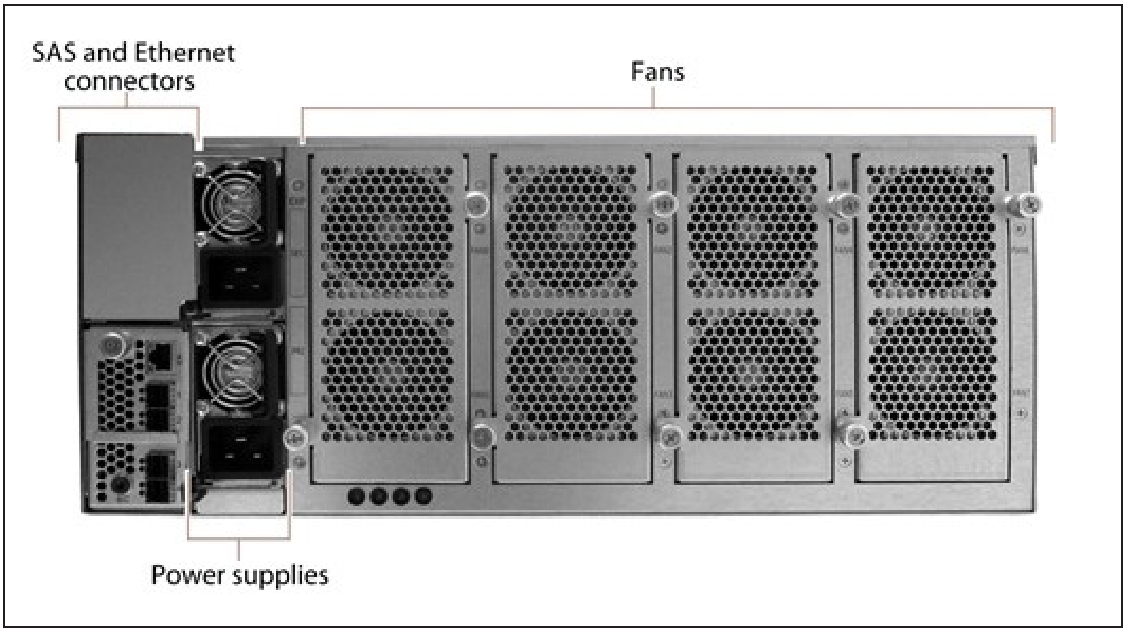


Figure 10 The rear view of the 77-bay and 107-bay expansion nodes.

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 11 shows the components on the front of the Gen1 S Series or Gen1 P Series BlackPearl gateway. All information is the same for the Gen1 S Series and Gen1 P Series unless specified. Figure 12 shows the components on the front of the Gen1 V Series BlackPearl gateway with the front bezels removed.

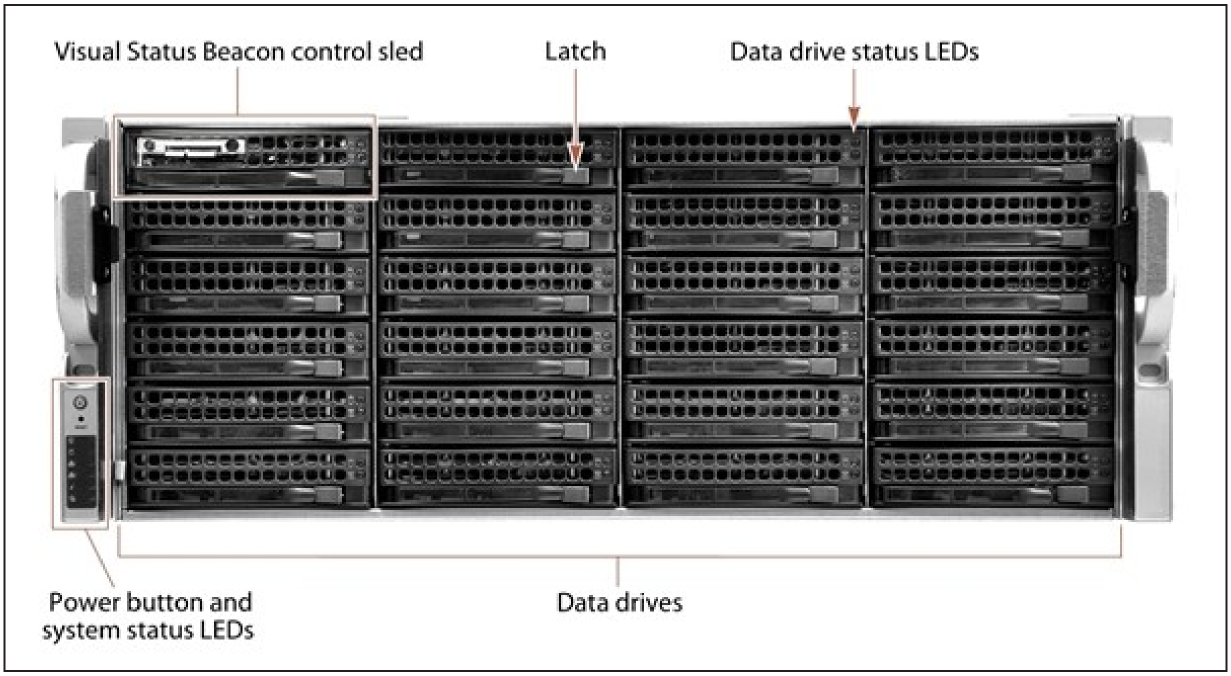

Visual Status Beacon control sled
Latch
Data drive status LEDs
Power button and system status LEDs
Data drives

Figure 11 The front view of the Gen1 S and P Series BlackPearl 4U master node (front bezel removed).

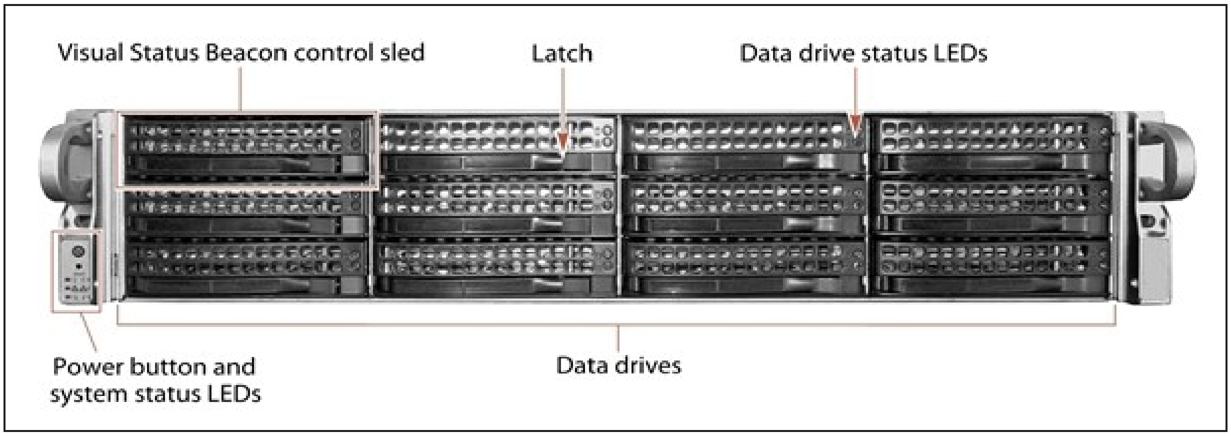

Visual Status Beacon control sled
Latch
Data drive status LEDs
Power button and system status LEDs
Data drives

Figure 12 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 System Status LEDs on page 416 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 13 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 14 shows the major components of the Gen1 V Series BlackPearl master node chassis.

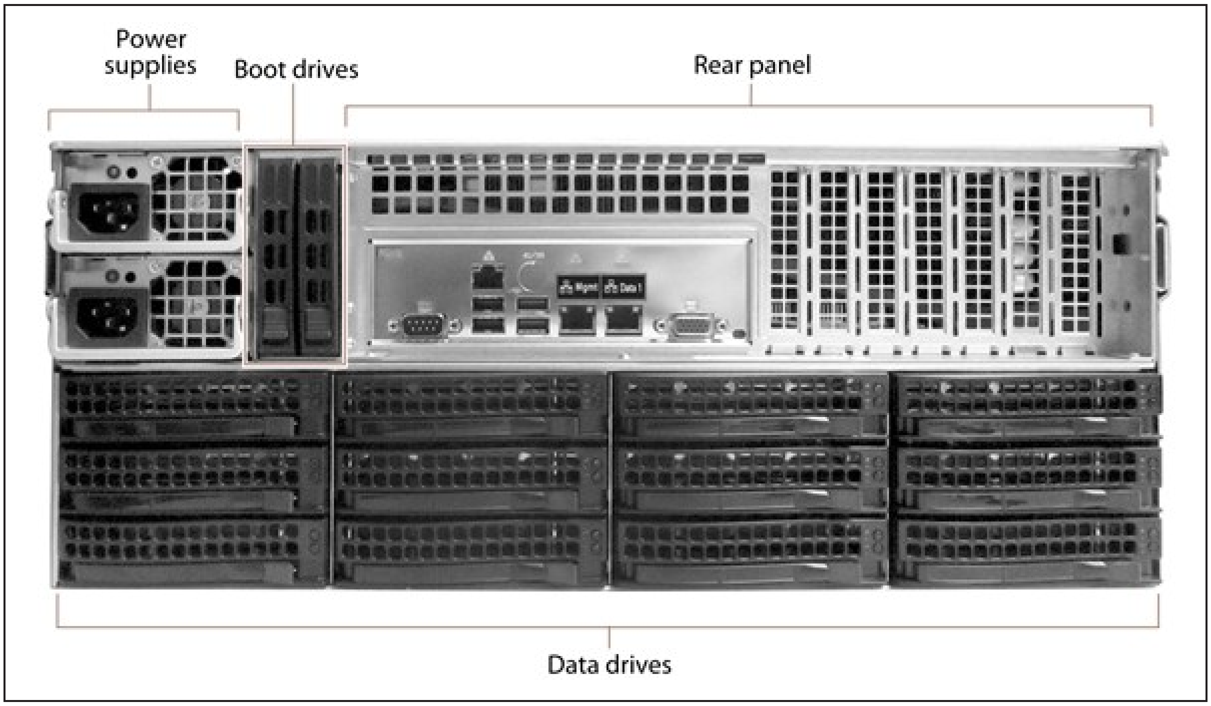


Figure 13 The rear view of the Gen1 S Series BlackPearl 4U master node.

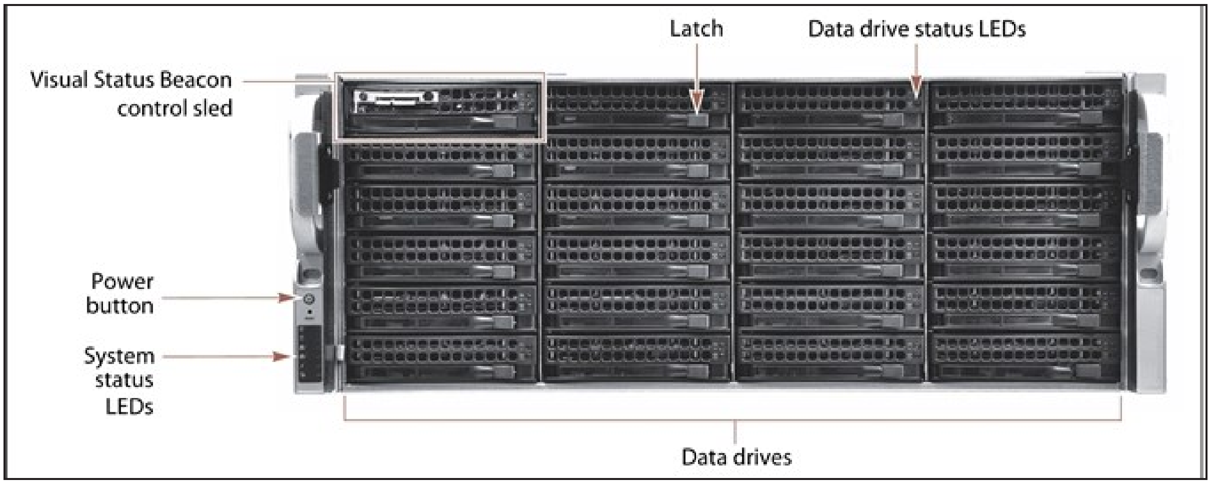


Figure 14 The rear view of the Gen1 V Series BlackPearl 2U master node.

Component	Description
Power supplies	The standard BlackPearl 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 gateway allows for Ethernet, Fibre Channel, SAS, USB, and other connections. See Rear Panel on page 44 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 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 15 shows the components on the rear panel of the BlackPearl 4U and 2U Gen1 S Series chassis.

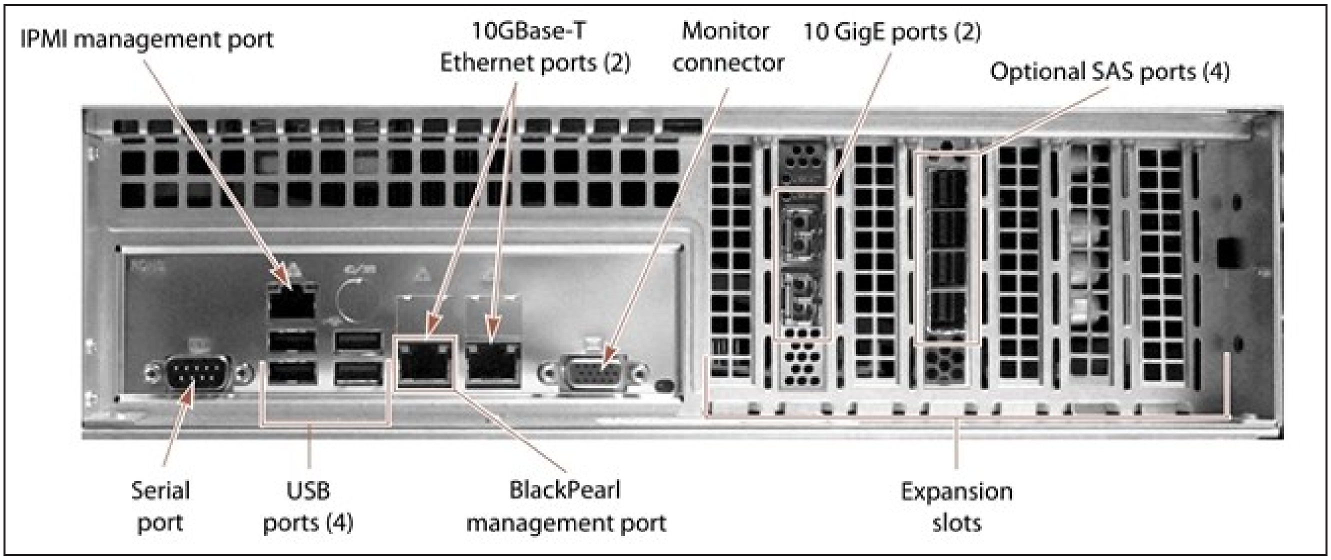


Figure 15 The Gen1 S Series BlackPearl rear panel components.

Component	Description
IPMI management port	See IPMI Configuration on page 553 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 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 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 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 16 shows the major components on the front of the 44-bay expansion node.

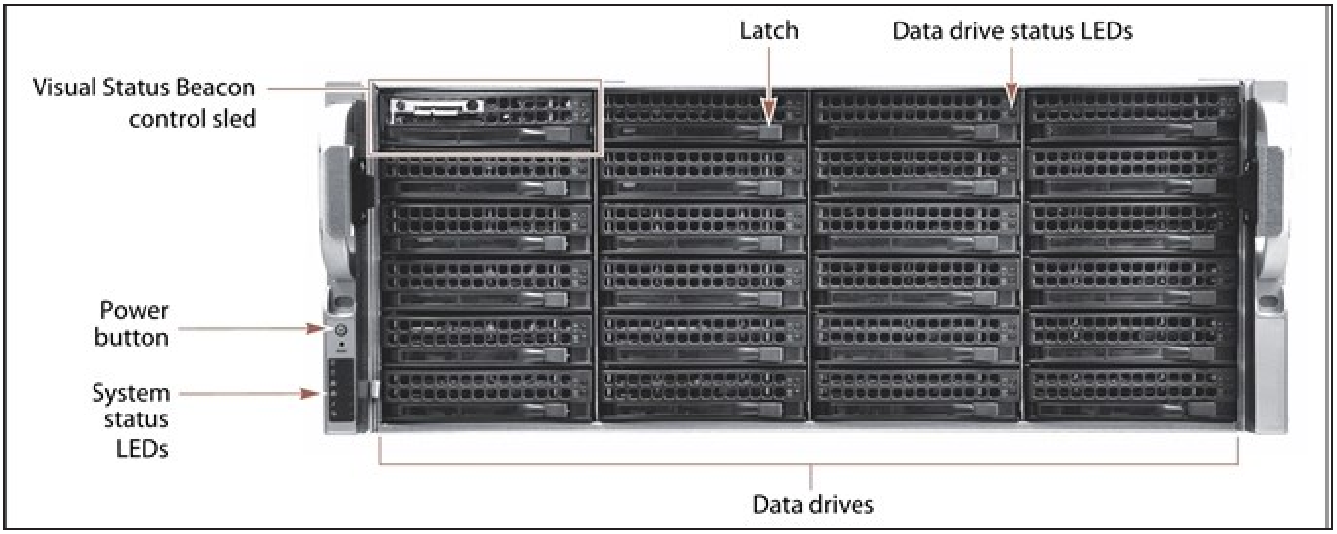


Figure 16 The front view of the 44-bay expansion node (front bezel removed).

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 gateway, including the expansion node.
System status LEDs	The status LEDs indicate power status, disk and network activity, as well as hardware faults. See System Status LEDs on page 416 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.
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.

Component	Description
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 17 shows the major components on the rear of the 44-bay expansion node.

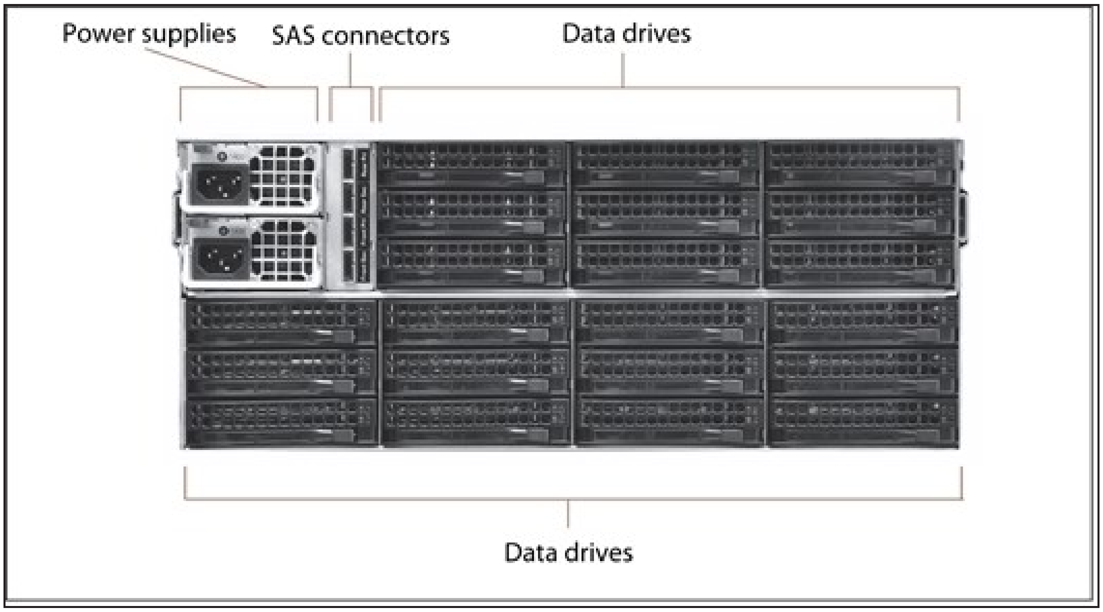


Figure 17 The rear view of the 44-bay expansion node.

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 18 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.

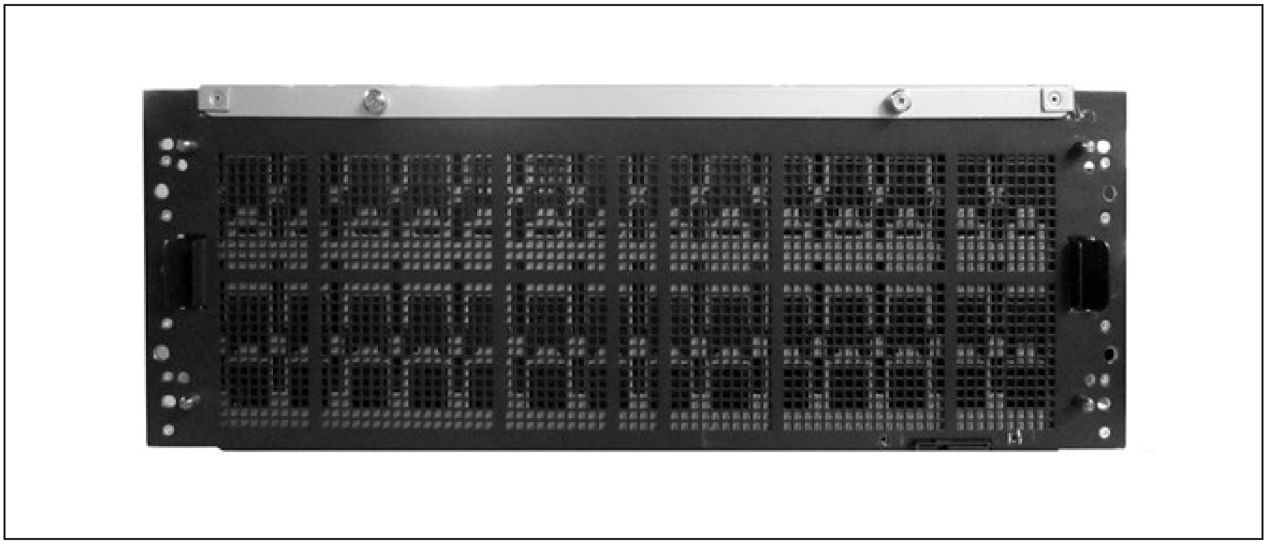


Figure 18 The front view of the 96-bay expansion node (front bezel removed).

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

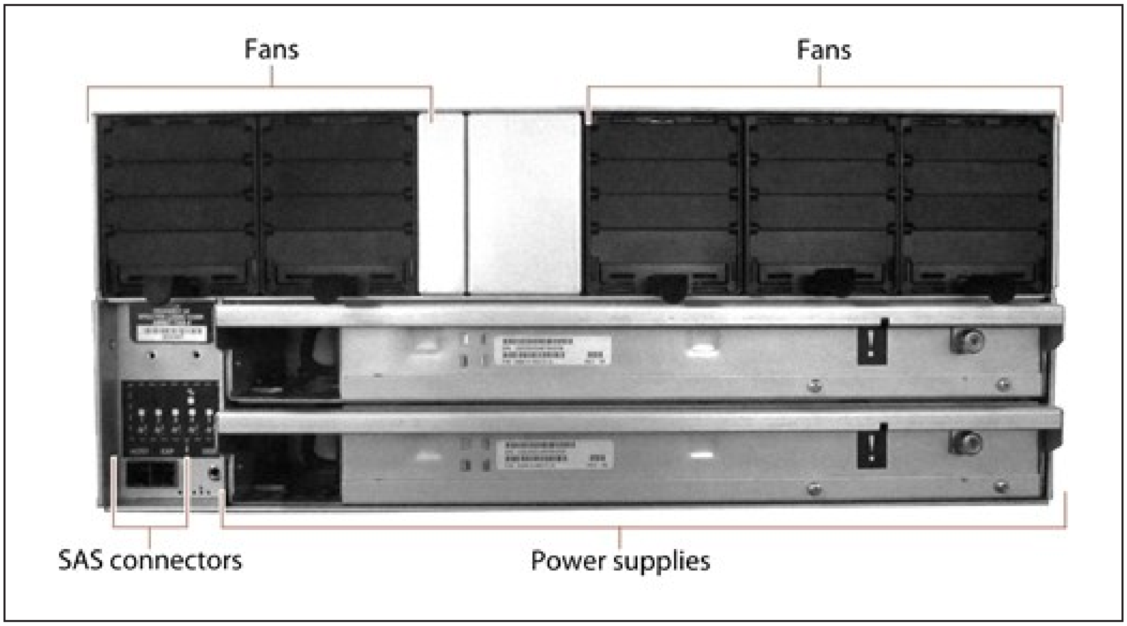


Figure 19 The rear view of the 96-bay expansion node.

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.

USER INTERFACE

The BlackPearl user interface provides browser-based configuration, management, and monitoring of the BlackPearl gateway. The following sections describe the common features that appear in all screens in the user interface.

> **Note:** Prior to BlackPearl OS 5.3, the data storage units displayed in the BlackPearl user interface used base 10 (MB, GB, TB). Starting with BlackPearl OS 5.3, the unit displayed are base 2 (MiB, GiB, TiB) to better reflect actual storage usage. Screen captures used in this guide may not match what is displayed in the BlackPearl user interface.

Menus

The menu bar appears along the top edge of each screen. Use the menu bar drop-down menus to navigate through the interface.

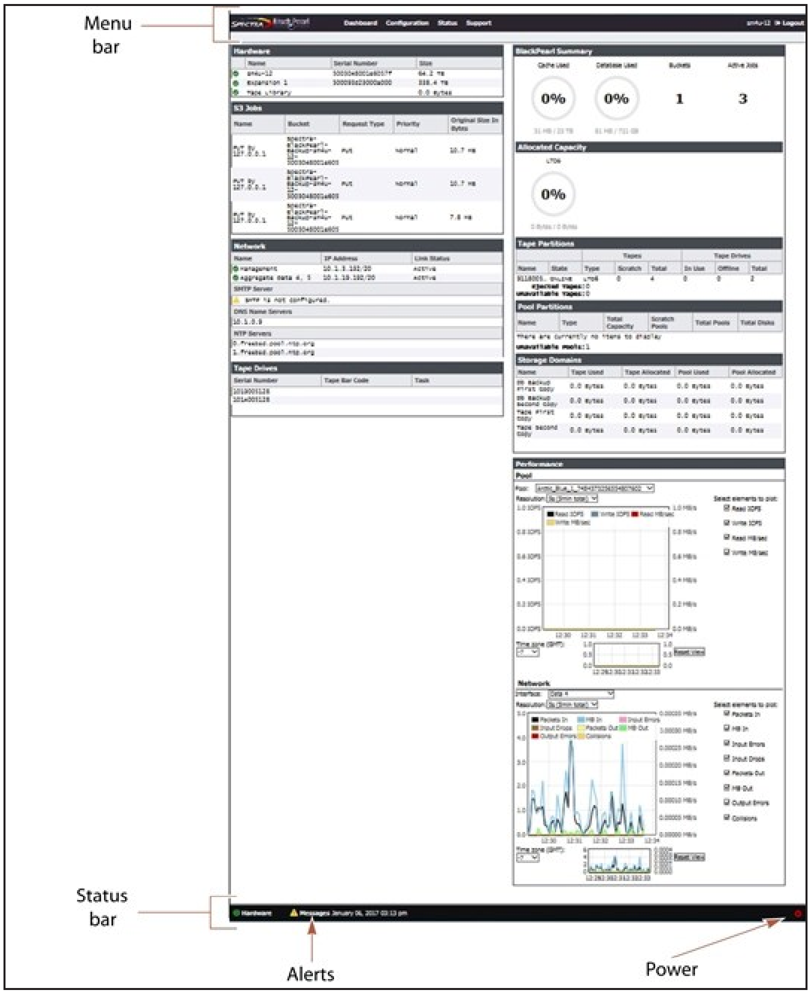


Figure 20 The Dashboard screen of the BlackPearl user interface.

The following table provides an overview of the screens available under each menu. The previously selected screen remains displayed until you select another option.

Note: Some options do not display in the system menu if the corresponding activation key is not installed.

Menu	Available Options
Dashboard	The **Dashboard** navigation link returns you to the Dashboard screen from any other screen. The Dashboard screen displays the general status of the gateway, tape cache, disk pools, volumes, and network connections. Clicking any of the panes on the Dashboard takes you to a details screen for that selection. The Dashboard screen also displays performance metrics for the gateway.
Configuration	The **Configuration** menu provides access to controls for configuring all aspects of gateway operation. • **NAS** • **Pools**—Displays information about any currently configured NAS pools and lets you define new NAS pools, and edit or delete existing NAS pools. • **Volumes**—Displays information about any currently configured NAS volumes on an existing NAS pool and lets you define new NAS volumes, and edit or delete existing NAS volumes. • **Shares > CIFS**—Displays information about any currently configured CIFS shares and lets you define new shares, and edit or delete existing shares. • **Shares > NFS**—Displays information about any currently configured NFS shares and lets you define new shares, and edit or delete existing shares. • **Buckets**—Displays information about the currently configured buckets and lets you add, edit, or delete buckets. You can also view information about the objects contained in a bucket and the physical tape media associated with each bucket. • **Advanced Bucket Management** • **Storage & Policy Management**—Lets you configure partitions, and create new storage domains and data policies. • **Replication Targets**—Lets you configure BlackPearl, Amazon® S3, and Microsoft Azure® targets. • **Database Backup**—Displays information about any currently generated backups on the gateway, as well as allows you to create new backups, either manually or on a schedule. • **Services**—Displays information about the currently configured services and lets you edit existing services. • **Network**—Provides controls for configuring the Ethernet ports on the BlackPearl gateway, configure a static route, Domain Name Servers, date and time, as well as entering SMTP (Simple Mail Transport Protocol) information to allow the gateway to send emails.

Menu	Available Options
	• **Certificates**—Provides controls for installing signed, trusted SSL certificates for your data and management ports so that you do not need to resolve the security certificate warning when accessing these ports. • **Mail Recipients**—Provides controls for configuring mail recipient accounts to receive emails when a message severity threshold is reached, or when AutoSupport Log sets (ASLs) are generated by the gateway. • **Users**—Provides controls for creating new S3 user accounts that act as owners for buckets, editing the login password, and displaying the S3 credentials for each user
Status	The **Status** menu provides access to the tools for monitoring the BlackPearl gateway in your environment. • **Hardware**—Displays information about the gateway, its components, tape libraries and associated tape drives, and disk expansion nodes and associated disk drives. Selecting the tabs on the Hardware screen displays detailed component status information. • **Tape Management**—Provides controls for managing the tape media in the tape library connected to the BlackPearl gateway. • **S3 Jobs**—Displays information about the status of all S3 jobs currently being processed by the gateway. • **NAS > Pools**—Displays information about any currently configured NAS pools. • **NAS > Volumes**—Displays information about any currently configured volumes on an existing NAS pool. • **Messages**—Displays system messages for the gateway. • **Performance**—Displays performance metrics for the tape cache, individual drives, network connections, and the CPUs in the integrated server. • **Reports**—Provides controls for generating reports about the configuration and status of the gateway. Reports can be generated in XML or JSON (JavaScript Object Notation) formats.
Support	The **Support** menu provides access for maintenance and troubleshooting options for the BlackPearl gateway. • **Software**—Provides controls for updating the BlackPearl software. • **Activation Keys**—Provides controls for entering activation keys. • **Logs**—Displays any current ASL sets on the gateway and provides controls for generating a new log set. • **Documentation**—Displays links to BlackPearl documentation. • **Contact Information**—Displays contact information for Spectra Logic Technical Support, as well as the part and serial numbers for the gateway.

Menu	Available Options
	• **Tools > Data Integrity Verification**—Provides a tool for data integrity verification of storage pools.
Logout	Logs the current user out of the BlackPearl user interface and returns to the login screen.

The information in the following table can be found on the Status bar, located at the bottom of all screens.

Status Bar	Available Options
Hardware	Provides an at-a-glance status of the overall health of the BlackPearl gateway. Clicking this link takes you to the Hardware screen. For more information see View the Status of Hardware Components on page 421.
Messages	Displays the severity, date, and time of the highest severity unread message. Clicking this link takes you to the Messages screen. **Note:** This link does not display if there are no current system messages. For more information see Check System Messages on page 420.
Power	Provides controls for rebooting and shutting down the gateway. For more information see Reboot or Shut Down a BlackPearl Gateway on page 451. **Note:** The connection to the user interface is lost after running the reboot command. Wait while the gateway reboots before attempting to reconnect to the user interface.

Status Icons

Icons indicate the status of a component and the highest severity level for any system messages, as described in the following table.

Icon	Meaning
✓	**Component OK** The component is functioning correctly.
ℹ	**Information** An informational message about a system component is available. Check messages to determine the component.
⚠	**Warning** A system component requires attention. Check messages to determine the component.
✖	**Error** A system component experienced an error condition. Check messages to determine the component and its error condition.
?	**Unknown** The status of a system component cannot be determined. Check messages to determine the component and its status.

Supported Browsers

The BlackPearl user interface supports the following standard web browsers:

- Google® Chrome™ version 22 or later
- Mozilla® FireFox® version 27 or later
- Apple® Safari® version 7 or later
- Microsoft Internet Explorer® version 11 or later
- Microsoft Edge® version 79.0.309 or later
- Opera Software Browser version 12 or later

Note: Spectra Logic recommends using Google Chrome to access the BlackPearl user interface.

CHAPTER 2 - INITIAL CONFIGURATION

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

Before You Begin **67**

Rackmount the Chassis **67**

Connect Ethernet Cables **67**

Automatically Import Activation Keys **68**

Power On the Gateway **69**

Configure the BlackPearl Management Port **71**

Log Into the BlackPearl User Interface **74**

Configure the Data Connection **76**

Configure an Aggregate Port Data Connection 76

Configure a Single Port Data Connection 79

Configure a Static Route 80

Create a User **82**

Description of User Types 82

Create a User 83

View S3 Credentials **86**

Next Steps **87**

Before You Begin

If your BlackPearl 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 gateway.

Rackmount the Chassis

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

- For a Gen2 X, S, or V Series see the *BlackPearl Gateway Quick Start Guide*.
- For a Gen1 P, S, or V Series, see the *Spectra BlackPearl Rackmount Installation Guide*.

Connect Ethernet Cables

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

- For a Gen2 X Series see Rear View on page 37.
- For a Gen2 S or V Series see Rear Panel on page 44.
- For a Gen1 P, S, or V Series, see Rear Panel on page 53.

AUTOMATICALLY IMPORT ACTIVATION KEYS

Activation keys enable features on the BlackPearl gateway. They are tied to the serial number of the gateway for which they are issued, and cannot be used on another gateway. There are two types of activation keys; feature keys to enable features like NAS and the Vail application, and capacity keys that determine the amount of disk and tape storage available.

Renewals of expired activation keys are obtained by contacting Spectra Logic Technical Support (see Contacting Spectra Logic on page 9).

The USB device in the BlackPearl documentation kit contains the activation keys for the options that you purchased.

Note: If your BlackPearl documentation kit does not contain a USB device, see Manually Enter Activation Keys on page 338 for instructions for manually entering the activation keys.

Follow these steps to import the keys.

1. Insert the USB device into a USB port on the back of the gateway. See one of the following for the location of the Ethernet ports on the rear of the master node:

- For a Gen2 X Series see Rear View on page 37.
- For a Gen2 S or V Series see Rear Panel on page 44.
- For a Gen1 P, S, or V Series, see Rear Panel on page 53.

   When the BlackPearl gateway detects the USB device it automatically imports the activation keys and power cycles the gateway.

2. Power on the gateway using the instructions in Power On the Gateway on the next page.
3. Wait while the BlackPearl gateway performs its power-on sequence.

⚠ **IMPORTANT** Do not remove the USB device until after the gateway power cycles and the BlackPearl user interface displays a message that it is safe to remove the USB device.

⚠ **IMPORTANT** Do not remove the USB device until after the gateway power cycles and the BlackPearl user interface displays a message that it is safe to remove the USB device.

POWER ON THE GATEWAY

Use the instructions in this section to power on a BlackPearl gateway, and optionally, a 44-bay, 77-bay, 96-bay, or 107-bay expansion node. During the power-on sequence, the BlackPearl 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 19 on page 59 and Figure 10 on page 48), 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.

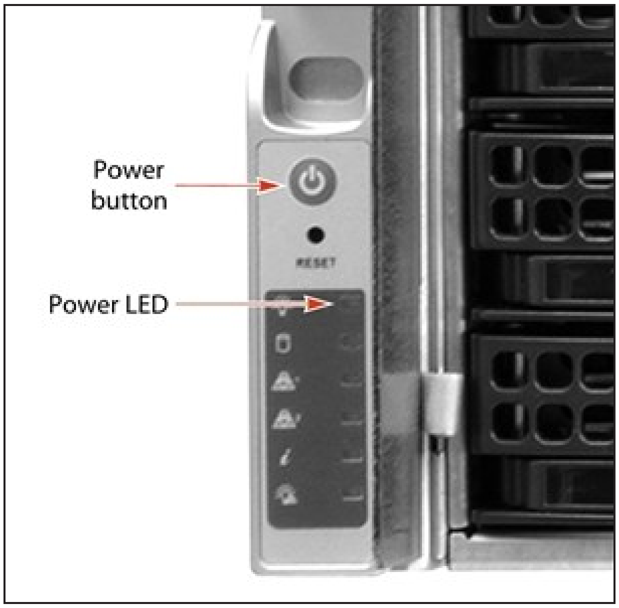


Figure 21 Press the power button.

2. To power on a BlackPearl Gen1 or Gen2 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 Gen2 X Series see Rear View on page 37.
- For a Gen2 S or V Series see Rear Panel on page 44.
- For a Gen1 P, S, or V Series, see Rear Panel on page 53.

Then plug the power cables into power outlets near the chassis. Wait while the BlackPearl 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 Gateway on page 451.

Configure the BlackPearl Management Port

IMPORTANT You must connect Ethernet cables as described in Connect Ethernet Cables on page 67 before either proceeding with the steps below.

IMPORTANT You must connect Ethernet cables as described in Connect Ethernet Cables on page 67 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 the Management Port on page 281

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 536 for an alternate method.

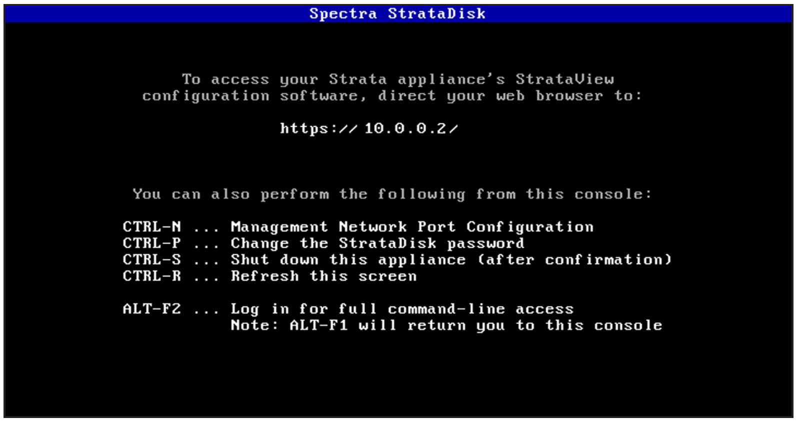
1. Connect a monitor and USB keyboard or KVM switch to the rear of the BlackPearl gateway.

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 Gen2 X Series see Rear View on page 37.
- For a Gen2 S or V Series see Rear Panel on page 44.
- For a Gen1 P, S, or V Series, see Rear Panel on page 53.

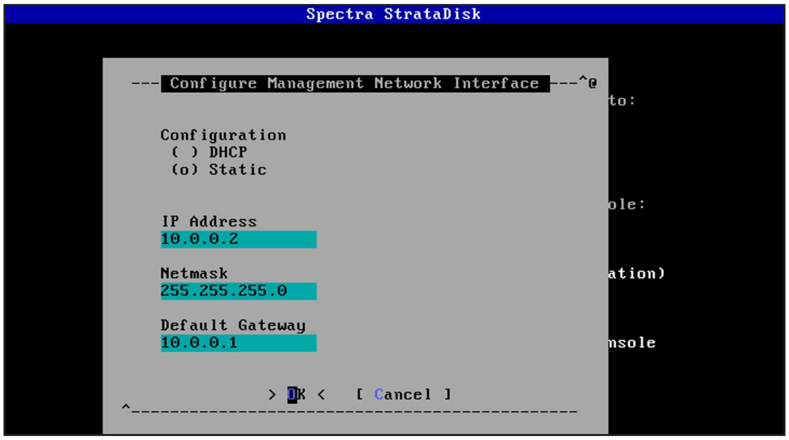
The Console screen displays.



```
                         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 22 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
      10.0.0.1                                          nsole


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

Figure 23 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 gateway.

LOG INTO THE BLACKPEARL USER INTERFACE

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

Note: 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.

Note: To log into the BlackPearl user interface on a system that is configured to use Mult-Factor Authentication, see Log In to a System Configured to Use Multi-Factor Authentication on page 306.

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 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 334.

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.

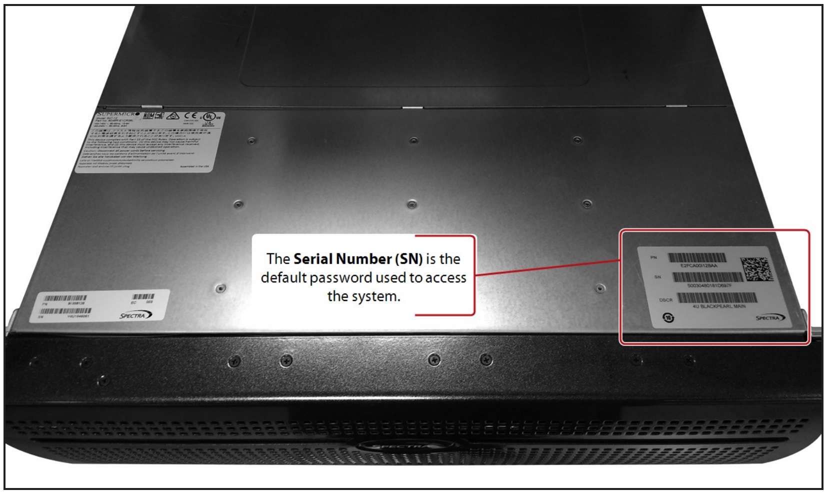

The **Serial Number (SN)** is the default password used to access the system.

Figure 24 The BlackPearl serial number sticker.

Notes:
- Spectra Logic recommends that you change the default password for the primary administrator (see Edit a User on page 323).
- If you are running BlackPearl OS 4.0 through 5.3, the default username is **Administrator** and the default password is **spectra**.
- If this is the first time that you log in after importing activation keys, an informational message displays indicating that you can now safely remove the USB device. See Automatically Import Activation Keys on page 68 for instructions for closing the message.

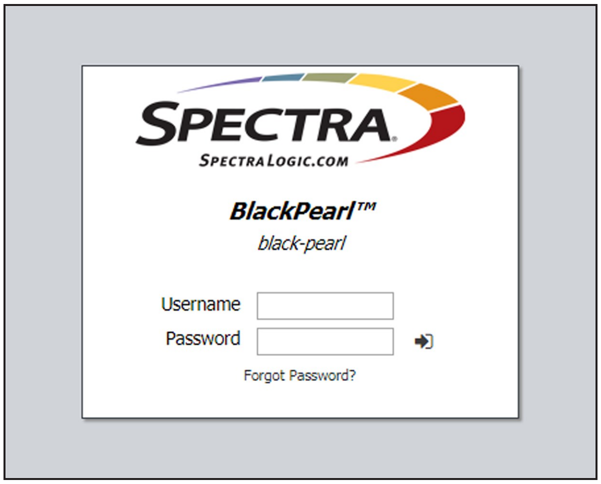


Figure 25 The BlackPearl Login screen.

4. Click ➔ to log in.

IMPORTANT The remainder of this guide assumes that you are logged in to the BlackPearl user interface.

IMPORTANT The remainder of this guide assumes that you are logged in to the BlackPearl user interface.

CONFIGURE THE DATA CONNECTION

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

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 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.
- For a BlackPearl HotPair configuration, see the *Spectra BlackPearl HotPair Installation & Configuration Guide* for information on configuring data connections.

Configure an Aggregate Port Data Connection

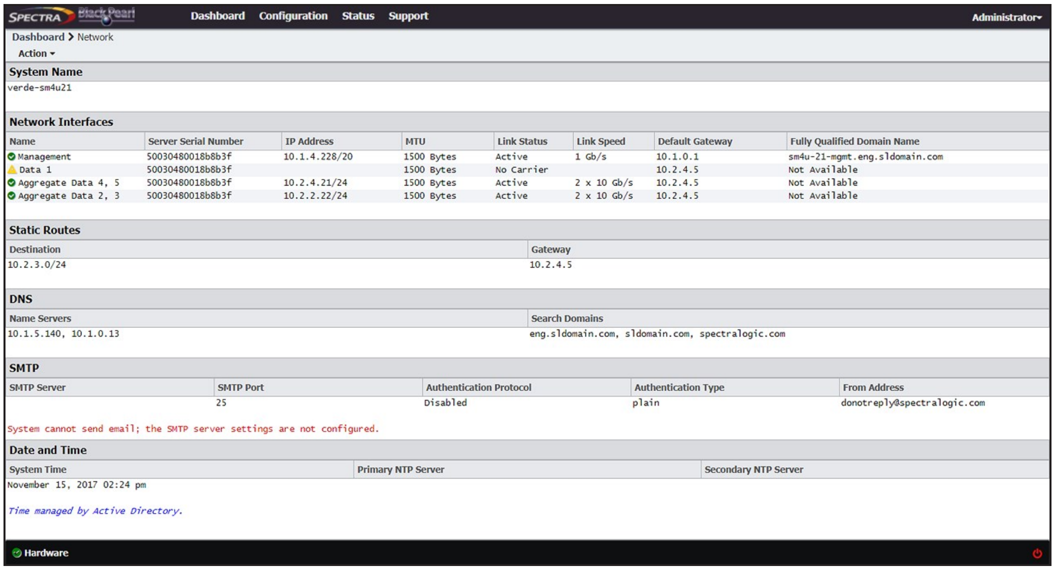
Link aggregation uses multiple Ethernet ports, configured with a single MAC address, to improve data transfer speeds. See Link Aggregation Notes on page 540 for more information.

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

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

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

1. From the menu bar, select **Configuration > Network**, or select the Network pane from the Dashboard screen. 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

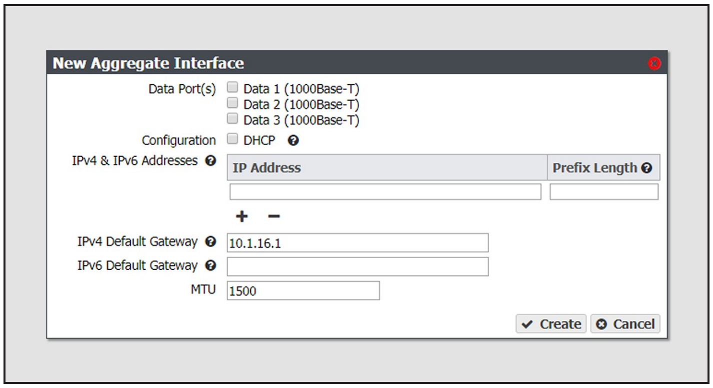
System Time	Primary NTP Server	Secondary NTP Server
November 15, 2017 02:24 pm		

Time managed by Active Directory.

Figure 26 The Network screen.

2. From the menu bar, select **Action > 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.



Data Port(s) □ Data 1 (1000Base-T)
□ Data 2 (1000Base-T)
□ Data 3 (1000Base-T)

Configuration □ DHCP

IPv4 & IPv6 Addresses

IP Address	Prefix Length

IPv4 Default Gateway 10.1.16.1

IPv6 Default Gateway

MTU 1500

Figure 27 The New Aggregate Interface dialog box.

3. Select the **Data Port(s**) you want to configure into an aggregate data interface. 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 **DHCP** 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 in Step 4.

- **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 in Step 4, this option is unavailable.
- The gateway entered for the last configured IPv4 connection sets the default gateway for the BlackPearl gateway.

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

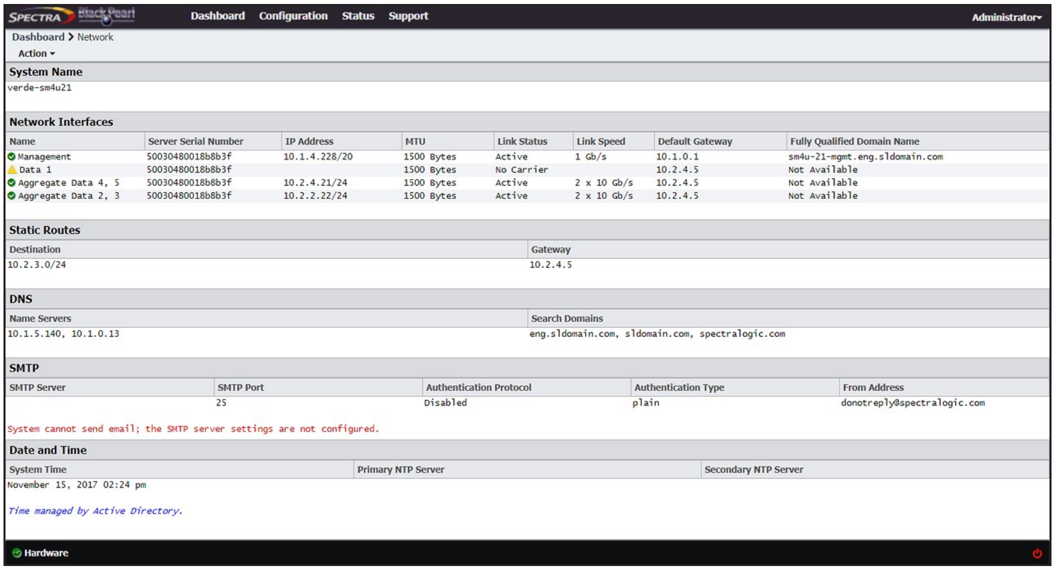
Notes:
- The gateway entered for the last configured IPv6 connection sets the default gateway for the BlackPearl gateway.
- The IPv6 Gateway does not need to be configured when the BlackPearl gateway is connected to a SLACC network.

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 **Create**.

Configure a Single Port Data Connection

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

1. From the menu bar, select **Configuration > Network**, or select the Network pane from the Dashboard screen. 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

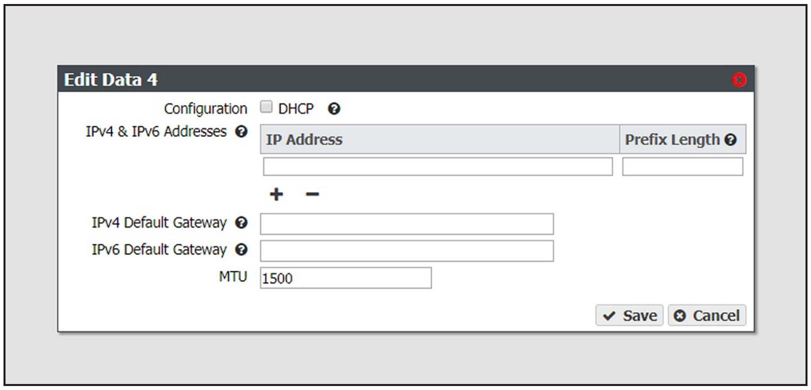
System Time	Primary NTP Server	Secondary NTP Server
November 15, 2017 02:24 pm		

Time managed by Active Directory.

Figure 28 The Network screen.

2. Double-click the Data # row in the Network Interfaces pane for the port you want to configure, or 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.



Configuration □ DHCP

IPv4 & IPv6 Addresses

IP Address	Prefix Length

IPv4 Default Gateway

IPv6 Default Gateway

MTU 1500

Figure 29 The Edit Data # dialog box.

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

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 in Step 3.
   - **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**.

   Notes:
   - If you selected DHCP in Step 3, this option is unavailable.
   - The gateway entered for the last configured IPv4 connection sets the default gateway for the BlackPearl 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 gateway.
   - The IPv6 Gateway does not need to be configured when the BlackPearl gateway is connected to a SLACC network.
7. 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.
8. Click **Save**.

Configure a Static Route

The BlackPearl gateway only supports communication with one default gateway. When configuring a BlackPearl 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 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 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 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 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. From the menu bar, select **Configuration > Network**, or select the Network pane from the Dashboard screen. The Network screen displays (see Figure 28 on page 79).
2. From the menu bar, select **Action > New Static Route**. The Static Route dialog box displays.

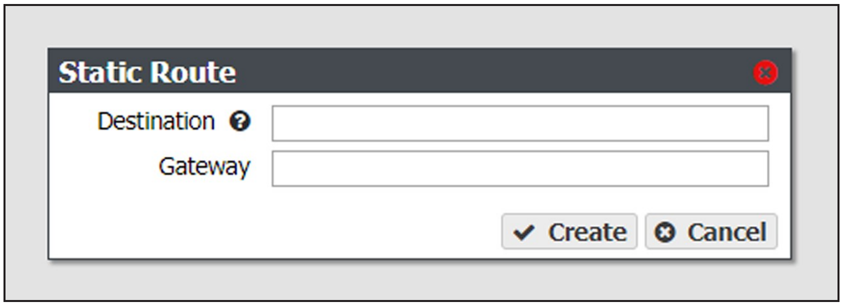


Figure 30 The Static Route dialog box.

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 **Gateway** of the data connection used to communicate with the isolated network.
5. Click **Create**.
6. Repeat Step 2 through Step 5 for each host computer on the isolated network.

CREATE A USER

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

Description of User Types

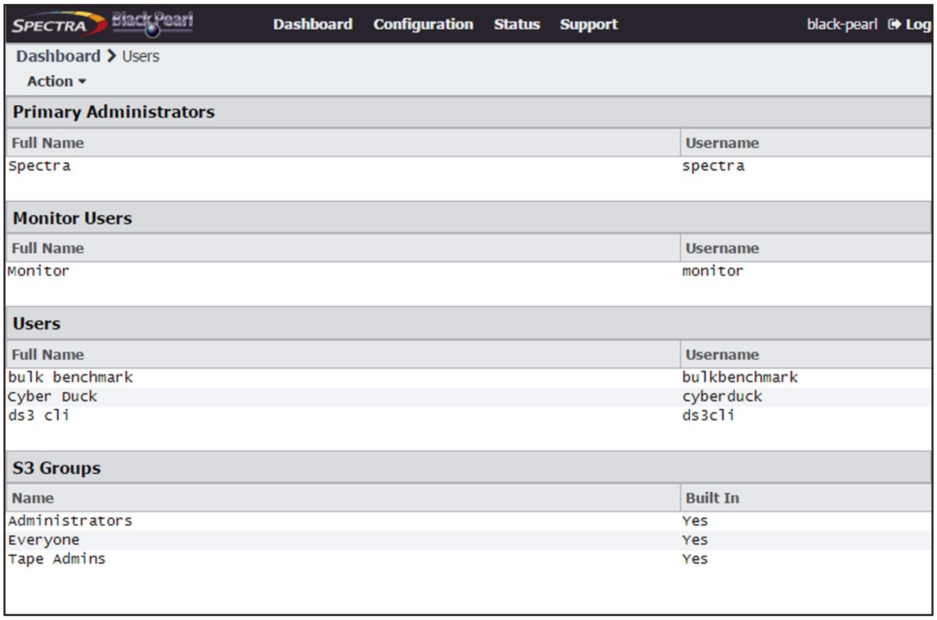
There are four different types of users in the BlackPearl user interface. Administrator users, monitor users, login users, and CIFS users. Additionally, users can be combined with other users into S3 groups, in which all members of the group share the same permissions. Use the table below for a description of the user types.

User	Description
Administrator	An administrator account is created by default. This account can access the BlackPearl user interface and has full control over all user interface functions. The default username for the primary administrator is **Administrator**, and 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 administrator account is automatically created without any permissions. **Notes:** • Spectra Logic recommends changing the password for the primary administrator. See Edit a User on page 323. • If you are running BlackPearl OS 4.0 through 5.3, the default username is **Administrator** and the default password is **spectra**.
Monitor User	The monitor user account is created by default. This account 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 of S3 jobs, or any other aspect of the user interface, or export tapes, or create a snapshot, but do not have access to an administrator account. The default username and password are both **monitor** using all lowercase letters. **Notes:** • Spectra Logic recommends that you change the initial password for the default monitor account. See Edit a User on page 323. • The monitor user can open any menu or function and attempt to edit settings, but these changes are ignored when the monitor user attempts to save the changes.
Login User	A user with Login permissions is able to log into the BlackPearl user interface.

User	Description
	Note: Administrator and Monitor users must also have Login permission in order to log in to the BlackPearl user interface.
CIFS User	A user with CIFS permission is able to access CIFS shares in a Windows workgroup environment.

Create a User

1. From the menu bar, select **Configuration > Users.** The Users screen displays.



Primary Administrators

Full Name	Username
Spectra	spectra

Monitor Users

Full Name	Username
Monitor	monitor

Users

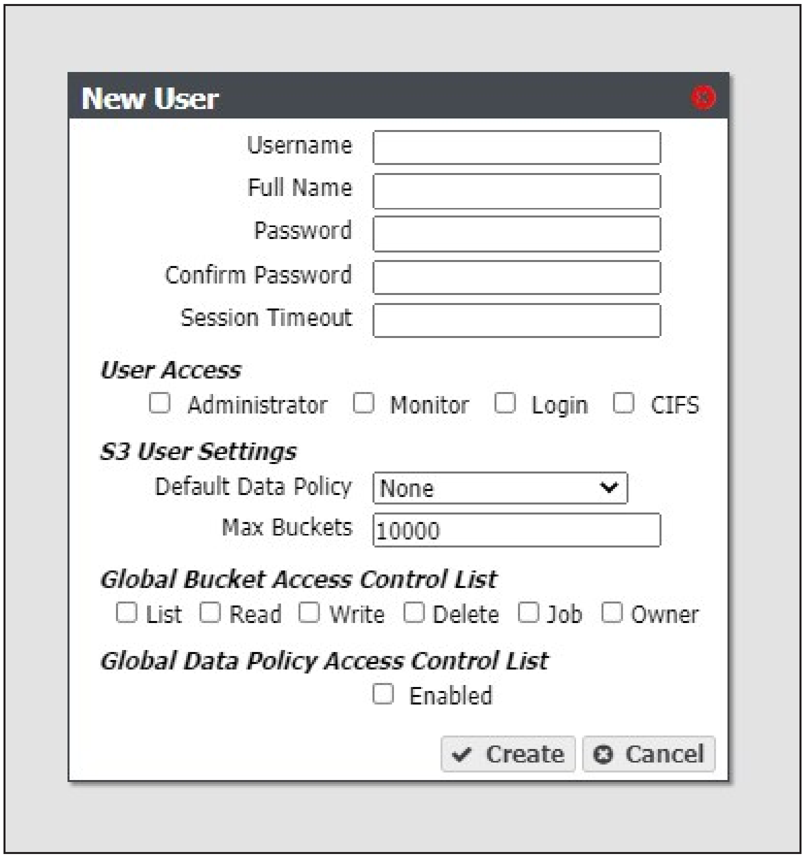
Full Name	Username
bulk benchmark	bulkbenchmark
Cyber Duck	cyberduck
ds3 cli	ds3cli

S3 Groups

Name	Built In
Administrators	Yes
Everyone	Yes
Tape Admins	Yes

Figure 31 The Users screen.

2. Select **Action > New** from the menu bar. The New User dialog box displays.



New User

Username

Full Name

Password

Confirm Password

Session Timeout

User Access

□ Administrator □ Monitor □ Login □ CIFS

S3 User Settings

Default Data Policy: None

Max Buckets: 10000

Global Bucket Access Control List

□ List □ Read □ Write □ Delete □ Job □ Owner

Global Data Policy Access Control List

□ Enabled

Figure 32 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. Select one or more **User Access** permissions. See Description of User Types 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. From the drop-down list, select a **Default 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. The default value of 10000 is pre-entered.

10. 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.

11. If desired, under **Global Data Policy Access Control List**, select the check box to allow the user access to any data policy created on the gateway.

12. Click **Create** to create the new user. The gateway generates a unique S3 Access ID and Secret Key for the user.

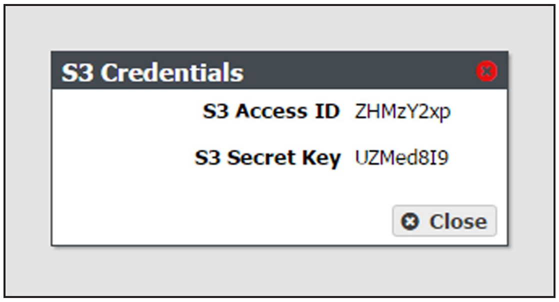
13. If desired, repeat Step 2 on page 84 through Step 12 to create additional users.

View S3 Credentials

There are two methods you can use to view S3 credentials, through the User screen, or the User Profile screen.

Using the User Screen

1. From the menu bar, select **Configuration > Users.** The Users screen displays (see Figure 31 on page 83).
2. Select the user for which you want to view the S3 credentials from the User pane of the Users screen, and then select **Action > Show S3 Credentials**. The S3 Credentials dialog box displays.



S3 Access ID ZHMzY2xp

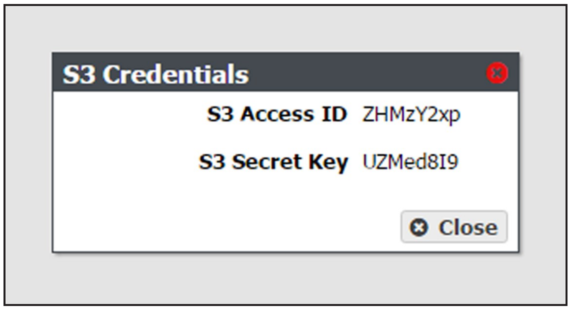
S3 Secret Key UZMed8I9

Figure 33 The S3 Credentials dialog box.

3. Use the **S3 Access ID** and **S3 Secret Key** to access the BlackPearl gateway using a DS3 client, the DS3 API, or Vail sphere.

Using the User Profile Screen

1. From the right side of the menu bar, select ***Current User*** **> User Profile**. The User Profile screen displays.
2. Select **Action > Show S3 Credentials**. The S3 Credentials dialog box displays.



S3 Access ID ZHMzY2xp

S3 Secret Key UZMed8I9

Figure 34 The S3 Credentials dialog box.

3. Use the **S3 Access ID** and **S3 Secret Key** to access the BlackPearl gateway using a DS3 client, DS3 API, or Vail sphere.

NEXT STEPS

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

- See Understanding Advanced Bucket Management on page 88 for information about DS3 and Advanced Bucket Management concepts you need to understand before you begin designing the storage architecture of the BlackPearl gateway.
- See Additional Configuration Options on page 279 for information about the additional options that can be configured on the BlackPearl gateway.
- See Operating the BlackPearl Nearline Gateway on page 407 for information about day-to-day monitoring and operation of the gateway.
- See Using AutoSupport on page 453 to set up AutoSupport to collect and email log sets.
- See Maintaining the BlackPearl Nearline Gateway on page 464 for maintenance options for the gateway.

Chapter 3 - Understanding Advanced Bucket Management

This chapter explains the concepts of the BlackPearl Nearline gateway advanced bucket management. It is important to understand the information in this chapter before you begin designing the storage architecture of the BlackPearl gateway.

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 concepts in this chapter and have thoughtfully planned your data policies and consulted with Spectra Logic Professional Services before you start using the BlackPearlgateway to store data.

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 concepts in this chapter and have thoughtfully planned your data policies and consulted with Spectra Logic Professional Services before you start using the BlackPearl gateway to store data.

Goals of Advanced Bucket Management **90**

DS3 Overview **90**

DS3 Clients 91

BlackPearl Cache **92**

Storage Domains **93**

Data Policies **93**

Data Persistence Rules 93

Data Replication Rules 94

Tape Export Strategy 94

Tape and Disk Partitions **96**

Tape Partitions 96

Tape Drive Reservation 96

Tape Media Inspections 97

Object Storage Disk 98

Storage Disk Pools 98
Special Considerations for Exporting Tapes 99
Tape Export Best Practices 99
Special Considerations for Reading Tapes in a Non-BlackPearl Nearline Gateway Environment 100
Example Configurations 102
Single Copy on Tape 103
Dual Copy on Tape 107
Single Copy on Nearline Object Storage Disk 112
Single Copy on Nearline Object Storage Disk and Tape 116
Single Copy on Nearline Object Storage Disk and Dual Copy on Tape 121
Additional Configurations 127

GOALS OF ADVANCED BUCKET MANAGEMENT

The BlackPearl gateway provides a DS3 front end interface to disk, tape and cloud storage. 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. The BlackPearl gateway delivers seamless data management enabling infinite retention, seamless growth, and unlimited retrieval of data for as low as pennies per Gigabyte.

DS3 OVERVIEW

The Spectra BlackPearl Nearline Gateway allows data to move seamlessly into deep storage in a way not previously possible. DS3 is the first native REST-based interface to deep storage which enables easy archiving of large amounts of bulk data. It enables users to deploy tape, nearline disk, and online disk storage that is cost effective, easy to manage, and scalable to exabytes of data.

DS3 utilizes the standard Amazon S3 operations plus additional operations specifically designed to optimize the transport of data objects to and from deep storage. The additional operations define the job so that BlackPearl gateway interacts with the objects efficiently and define the data policy to customize where and for how long specific data is stored.

The first of these additional operations is called START BULK PUT. It is an HTTP PUT operation that provides BlackPearl gateway with information about the objects that the client wants to send as a single job for storing on tape. The Create Bulk Put command is sent with a payload that is made up of a list of object names and corresponding object sizes. This information allows the BlackPearl gateway to plan the initial storage of the objects in its cache, and how it will store the data on tape. The response to the Create Bulk Put command is a specifically ordered list of how the BlackPearl gateway wants those files (objects) sent.

The second command is called Create Bulk Get. The Create Bulk Get command is actually an HTTP PUT command because it too contains a payload for the BlackPearl gateway. This payload is a list of objects that the client wants to get from the BlackPearl gateway. It is not necessary for the request payload to contain the size of the files because the BlackPearl gateway already knows the sizes of the objects (files). The response to the request is again an ordered list of the objects and information about the objects, including if they are already in the cache and ready to be retrieved from cache by a GET command.

Knowing the files that the client wants to retrieve, the BlackPearl gateway can make the best use of its resources in retrieving the objects. For example, if the list of objects spans across four different tapes and there are four tape drives available, those four tapes can all be loaded into drives and the objects can be read back in parallel, greatly improving the speed at which the client can get all of the objects. Without the Create Bulk Get request, the client would be asking the BlackPearl gateway for those objects in a less efficient manner.

Storing large amounts of bulk data on tape has historically presented challenges. DS3 addresses these challenges:

- Tape drives are sequential block storage devices, with data laid out in a sequential manner along the full length of the tape. This makes it inefficient to retrieve data out of order. DS3 plans and queues a large amount of data to be efficiently written to tape; it logically groups data on tape in a way that reflects how the client is likely to read it back.
- Because of the mechanical nature of the tape media and drives, tape drives demand a large amount of data to be available, via a fast connection. When data is not efficiently streamed for the tape drives to write (due to slow data buffering or a slow connection to the drive), the result is poor write performance. This poor performance is due to a phenomenon referred to as "shoe-shining". When a drive is sent a small amount of data, it writes the data and then is forced to stop. Because the tape cannot stop instantaneously, the drive overshoots a small amount and the tape is not in position for the next write operation. To compensate, the tape drive rewinds to get back to the correct position for the next write. If the next write also has a small amount of data, then the drive writes the next portion and again stops, overshoots, and rewinds, causing a back and forth "shoe-shining" like action. DS3 caches data on the BlackPearl Nearline Gateway before starting the transfer to tape, which prevents the shoe-shining behavior from occurring.
- Classically, different tape storage devices wrote data to tape in unique ways, locking you into a proprietary and single vendor solution to retrieve previously written data. DS3 writes data to tape using the open source Linear Tape File System (LTFS). With LTFS, data is always accessible with any LTFS enabled system.

For more information on the DS3 interface, see the *Spectra BlackPearl DS3 API Reference*.

DS3 Clients

Users can leverage a library of existing DS3 clients available through the *Spectra Logic Developer Program,* or develop their own client. The user moves data through the client to the BlackPearl gateway and then the gateway handles all interaction with the data storage hardware.

BlackPearl Cache

The BlackPearlcache 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 gateway from a client, or transferred from tape storage to the BlackPearl 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', and chunk size can vary.

When writing data to cache destined for tape storage, or restoring data from tape storage to the BlackPearl 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.

STORAGE DOMAINS

A storage domain is a collection of data partitions and, when applicable, media type combinations. Storage domains define the possible places where data sent to the BlackPearl Nearline Gateway can be stored. Data persistence rules and data policies further define where and for how long specific data is stored.

Entire data partition/media type combinations are members of storage domains. When additional capacity is required, a single storage pool or tape is allocated out of the member data partitions to fulfill the capacity requirement.

DATA POLICIES

A data policy defines data integrity policies (checksum type and end-to-end CRC requirements), default job priorities, and data persistence rules, which define where data should be written and for how long it should be kept. A data policy may be used by multiple buckets, but a bucket uses precisely one data policy.

A data policy consists of one or more permanent persistence rules, zero or more temporary persistence rules, and zero or more retired persistence rules. A persistence rule can be 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. Existing permanent and temporary persistence rules may be retired so that the rule is not applied for any new incoming data, but continues to retain data previously written.

Data Persistence Rules

Each data policy must have one or more permanent persistence rules. Each persistence rule targets a specified storage domain. There are three types of persistence rules:

- **Permanent** — A copy of the data is placed in the specified storage domain initially and maintained there permanently.
- **Temporary** — A copy of the data is placed in the specified storage domain initially and maintained there at least until the specified retention period expires.
- **Retired** — The rule is not applied for any new incoming data, but continues to retain data previously written.

Data is written to every storage domain for which there is a persistence rule with the type configured as permanent or temporary.

The same storage domain cannot be specified multiple times using different persistence rules in the same data policy. The same storage domain can be referred to across different data policies.

Data persistence rules must specify the level of physical isolation required for the data retention. There are two types of data retention:

- **Standard** — Data is isolated according to the standard storage domain isolation requirements. When more storage is needed, a tape or pool is assigned to the storage domain. Any buckets using that storage domain can have data on the pool or tape, which can make it difficult to export all of the tapes for a single bucket.
- **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 tape or pool to a bucket when needed. Allocating an entire pool to a bucket may use up resources quickly and is not recommended.

Data Replication Rules

Data policies may also contain data replication rules. The BlackPearl gateway supports replicating data to the following targets:

- BlackPearl target — A BlackPearl gateway remote to the local gateway that stores replicated data.
- Amazon S3 target — An AWS S3 instance remote to the BlackPearl gateway that stores replicated data.
- Microsoft Azure target — A Microsoft Azure instance remote to the BlackPearl gateway that stores replicated data.

Tape Export Strategy

A tape export strategy must be considered as part of a data policy. Spectra recommends keeping at least one copy of all archived data in the tape library at all times. 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 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 Configuring Advanced Bucket Management on page 128 for information on setting up multiple copies and exporting a copy, and Working with Tape Libraries and Media on page 341, or your *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 to transfer the data to another facility. Individual tapes can be exported manually using the BlackPearl user interface (see Export Tapes on page 393).
- **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 to the BlackPearl gateway, in order to free up space in the tape library. After tapes are exported, new tapes are imported to provide the BlackPearl gateway with new media for storage operations.

TAPE AND DISK PARTITIONS

Tape and disk partitions are external data storage targets cabled to the BlackPearl gateway through SAS or Fibre Channel connections. Once created, partitions are assigned to storage domains.

Tape Partitions

Tape partitions refer to data partitions configured on Spectra Logic or other supported tape libraries. When you create a partition on a tape library attached to a BlackPearl gateway, the gateway automatically detects the tape library partition and adds it to the list of available partitions in the BlackPearl user interface. The gateway also automatically creates two commonly used storage domains: tape first copy, and tape second copy. For more information on storage domains, see Storage Domains on page 93.

Notes:

- Cleaning partitions are not added to the BlackPearl user interface.
- Tape drive cleaning is typically handled by the Spectra tape library. For more information on cleaning the library tape drives using the tape library, see your *Tape Library User Guides*.
- Tape drive cleaning is handled automatically by the IBM TS4500 tape library.
- Tape drive cleaning for Spectra Logic libraries can be initiated through the DS3 API. See the *Spectra BlackPearl DS3 API Reference* for more information.
- Tape drive cleaning cannot be initiated through the BlackPearl user interface.
- If the BlackPearl gateway is configured to transfer data to tape, make sure the partitions configured for use by the BlackPearl gateway do not contain WORM (Write Once-Read Many) media. The BlackPearl gateway is not compatible with WORM media.

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 BlackPearl gateways 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 individual tape drive failures, or unavailable drives, from impacting the desired number of drives available for either read or write commands.

Note: Tape drives always allow inspection and verify tasks.

IMPORTANT Spectra Logic does not recommend setting both a minimum reservation priority and reserved task type for the same drive.

IMPORTANT Spectra Logic does not recommend setting both a minimum reservation priority and reserved task type for the same drive.

Tape Media Inspections

When new tape media is added to the BlackPearl gateway, the gateway inspects the tape cartridge as configured in the DS3 service. However, all tapes that are new to the gateway require inspection before they are usable in a managed state. Additionally, under certain circumstances, the gateway may override the configured behavior for inspections on already managed tapes.

Inspection Behavior when the Tape Library is in Standby

With BlackPearl OS 5.2 or earlier, if there was an inventory change in the tape library while in standby, the BlackPearl 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 S3 service is set to "Never Inspect".

Inspection Behavior when the Tape Library is in Active Use

Prior to BlackPearl OS 5.3, if a tape library associated with the BlackPearl gateway goes offline, or is otherwise made unavailable to the BlackPearl gateway, the tapes are marked as "Lost" by the BlackPearl gateway. When this occurs, the tape is considered to be a new tape, and is re-inspected when the tape library is made available. Starting with BlackPearl OS 5.3, the BlackPearl gateway automatically quiesces the tape partition and prevents the tape cartridge being marked "Lost".

Object Storage Disk

Object Storage Disk uses external SAS expansion nodes to provide both Online Storage Disk and Nearline Storage Disk partitions. The disk partitions are behind the BlackPearl DS3 interface, but can also be accessed using the Spectra StorCycle application, or the Spectra Vail application. Nearline Object Storage disk can also be used as a cache for data stored on tape.

Storage Disk Pools

Disk partitions are comprised of disk storage pools on external SAS expansion nodes. There are two types of disk partitions. **Online Storage Disk** partitions are created on Spectra 44-bay expansion nodes, while **Nearline Storage Disk** partitions are created on Spectra 96-bay expansion nodes. Both the 77-bay and 107-bay expansion nodes provide either **Online Storage Disk** or **Nearline Storage Disk** partitions, depending on the type of drives installed.

- **Online Storage Disk** — Is used as a temporary, high-performance storage target for highly transactional data.
- **Nearline Storage Disk** — Is a cost effective storage target for deep storage. Nearline storage is not recommended for frequent reads or writes.

Disk storage pools are manually created using the BlackPearl user interface after you attach an expansion node. See Create a Disk Pool on page 130.

Once storage pools are created, you must manually add them to disk partitions. For information on creating a disk partition, see Create a Disk Partition on page 137.

SPECIAL CONSIDERATIONS FOR EXPORTING TAPES

If you plan to export tapes, Spectra Logic recommends the following storage domain and data policy settings:

- Set the Write Optimization setting to **Capacity** when configuring a storage domain so that data is written to as few tapes as possible.
- Enable **Bucket Isolation** when configuring a data policy. This setting configures the bucket to have its own unique set of tapes. This ensures that tape media containing one bucket of information is not mixed with another bucket, making it easier to export a bucket.

Tape Export Best Practices

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 user 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. Tape media left in the Entry/Exit port may interfere with other automatic tape export operations, or import of new or requested tape media.

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 tape library to complete the GET job.

Note: All **request to import tape media** messages and emails list the required tape cartridge barcode(s), which help you quickly identify the tape cartridges to import.

It is important to not export tape media from the library directly. The BlackPearl Nearline gateway controls the movement of media in the library.

If you are using a Spectra Logic T120 or T50e tape library in with your BlackPearl Nearline gateway, it must be configured with only a single storage partitions. Multiple partitions, including a cleaning partition, are not supported.

Special Considerations for Reading Tapes in a Non-BlackPearl Nearline Gateway Environment

The BlackPearl gateway stores data on LTO-5 or later generation Ultrium, or TS11*xx* technology tape media using the LTFS format. If you plan to export tapes and read them in a non-BlackPearl gateway, you must follow the guidelines for Special Considerations for Exporting Tapes on the previous page as well as the guidelines below when configuring your storage domains and data policies.

- The LTFS file name option should be set to **Object Name** when configuring a storage domain. This setting configures LTFS file names to use the format {*bucket name*}/{*object name*}, for example bucket1/video1.mov. If the tapes are exported from the library attached to the BlackPearl gateway and loaded into a non-BlackPearl gateway, the file names match the object names. If you do not configure this option, object names are assigned a UUID string, which is not human readable, but can be translated back to the actual file name using an external conversion tool.
- Object names must comply with LTFS file naming rules:
    - The colon character (:) is not allowed in LTFS file names and therefore not allowed in BlackPearl object names. The slash character (/) is also technically 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 (for example, 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)

Note: 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.

- **Blobbing Enabled** should be cleared when configuring a data policy. Blobbing allows an object larger than 1 TB to be broken into multiple blobs and then stored on multiple tapes. Tapes created with blobbing disabled are always readable by a non-BlackPearl gateway; tapes created with blobbing enabled may not be readable by a non-BlackPearl gateway when very large objects span across multiple tapes. With blobbing disabled, all files must have a size of 1 TB or less.
- **Minimize Spanning** should be cleared when configuring a data policy. This helps further insure that blobs do not span across tapes and provides great LTFS compatibility.
- The **Keep Latest** setting cannot be used for a data policy which uses a storage domain configured with the **LTFS File Name** option set to **Object Name**.

EXAMPLE CONFIGURATIONS

Below are explanations of the preconfigured data policies on the BlackPearl gateway, which include data persistence rules and storage domain targets.

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 concepts in this chapter and have thoughtfully planned your data policies and consulted with Spectra Logic Professional Services before you start using the BlackPearlgateway to store data.

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 concepts in this chapter and have thoughtfully planned your data policies and consulted with Spectra Logic Professional Services before you start using the BlackPearl gateway to store data.

Note: For information on additional data policy settings that are not available through the BlackPearl user interface, see the *Spectra BlackPearl DS3 API Reference.*

Single Copy on Tape

This data policy is the most basic of the preconfigured data policies on the gateway. This policy creates a single copy of each object sent to the gateway on tape media. Once data is written on tape, it is removed from the BlackPearl cache if the gateway detects that more cache space is needed for incoming data.

Note: This data policy is automatically created when the gateway detects a tape partition.

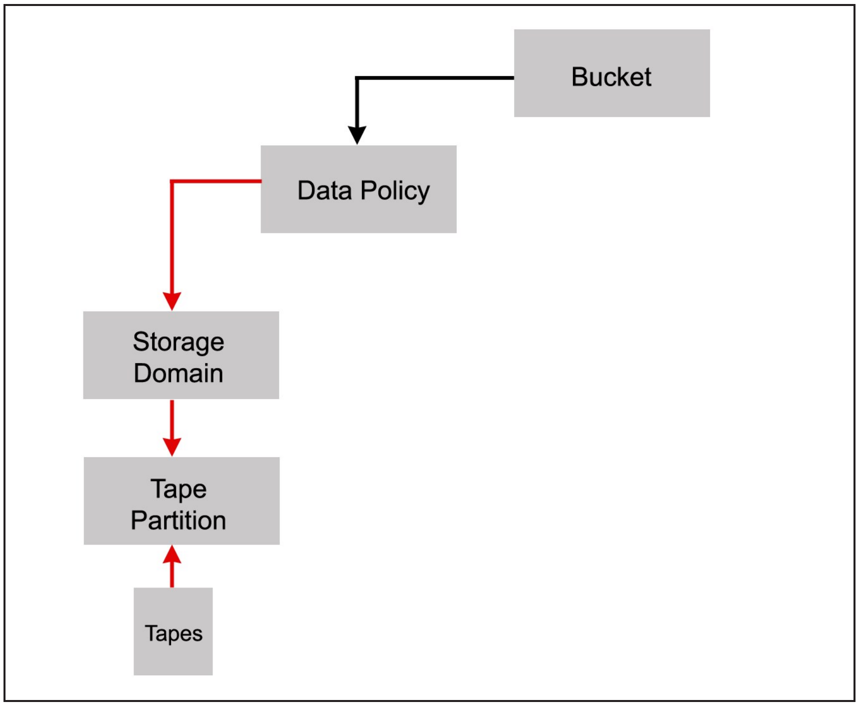


Figure 35 The Single Copy on Tape workflow.

The single copy on tape data policy is configured with the following attributes:

Parameter	Value	Description
Storage Domain - Tape First Copy - Data is written to the primary tape storage domain. This domain is created automatically when the gateway detects the first partition created on the tape library.		
Days to wait before verifying data	**null**	Data integrity verification is not performed automatically.
Secure Media Allocation	**cleared**	Media allocated to the storage domain may be reused by another storage domain if all data is deleted.
Write Optimization	**Capacity**	Job chunks are written across as few pieces of media as possible. Fewer tape drives are used, so performance is lower.
LTFS File Naming	**Object ID**	File names use the format {*bucket name*}/{*object id*}, for example, bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82.
Media Export Allowed	**cleared**	Media export is not allowed.
Storage Domain Member for Tape First Copy - The first tape partition created on the tape library and detected by the gateway.		
Tape Type	***varies***	The tape type matching the latest generation of tape drive in the partition.
Write Preference	**Normal**	The gateway uses the partition after partitions with **High** write preference and before a partition with **Low** or **Never Select** write preference.
Auto Compaction Threshold	**20**	The percentage of a tape with deleted objects at which auto compaction is triggered. The default is 95. The minimum is 10.
Data Policy - Single Copy on Tape		
Blobbing Enabled	**selected**	Allows an object to be broken into multiple blobs.
Minimize Spanning	**cleared**	Jobs larger than 1 TB are allowed to span across multiple tapes or pools as needed to maximize capacity utilization and performance.

Parameter	Value	Description
Default GET Job Priority	**High**	When the storage domain receives a GET job, it is processed with high priority, which is before low and normal priority jobs. Jobs of different types are put in order based on priority. **Note:** When using a DS3 client, this setting can be overridden when sending a GET job by specifying a different priority in the Get Job command. See the *Spectra BlackPearl DS3 API Reference* for more information.
Default PUT Job Priority	**Normal**	When the storage domain receives a PUT job, it is processed with normal priority, which is after high priority jobs but before low and normal priority jobs. Jobs of different types are put in order based on priority. **Note:** When using a DS3 client, this setting can be overridden when sending a PUT job by specifying a different priority in the Put Job command. See the *Spectra BlackPearl DS3 API Reference* for more information.
Default VERIFY Job Priority	**Low**	When the storage domain receives a VERIFY job, it is processed with low priority, which is the lowest setting. **Note:** When using a DS3 client, this setting can be overridden when sending a VERIFY job by specifying a different priority in the Create Verify Job command. See the *Spectra BlackPearl DS3 API Reference* for more information.
Default Verify After Write	**cleared**	Data is not verified after a write.
Rebuild Priority	**Low**	If data is lost from tape media, the data is rebuilt using low priority, which is the lowest setting.
Checksum Type	**MD5**	Data using this storage domain is CRC checked using the MD5 checksum type. Data is CRC checked when it is written to cache with a PUT job, or read back from tape media with a GET job.
End-to-end CRC	**No**	This data policy does not use end-to-end CRC checking.

Parameter	Value	Description
Versioning	**None**	In order to upload a new version of an object already PUT to the gateway, the first version must be deleted.
Always Accept Replicated PUT Jobs	**cleared**	PUT jobs created for this data policy fail if one or more replication targets the gateway must PUT to are unavailable.
Data Persistence Rule for Tape First Copy		
Type	**Permanent**	Data is moved to tape and maintained on tape media until data is deleted from a bucket. **Note:** When data is deleted from a bucket, it is removed from tape media, but individual tape media cartridges are not reclaimed for use until all data is deleted from a tape cartridge.
Bucket Isolation Level	**Standard**	Data from different buckets can be mixed on to the same piece of media.

Dual Copy on Tape

This data policy persists two copies of data for each PUT job the policy receives. Both copies of data are moved to tape media.

This data policy is useful if you want to export one copy of the bucket on tape media for storage off site, which provides enhanced data security in the case of ransomeware attacks or disaster recovery.

Note: This data policy is created automatically when the gateway detects the first and second tape partitions created on the tape library.

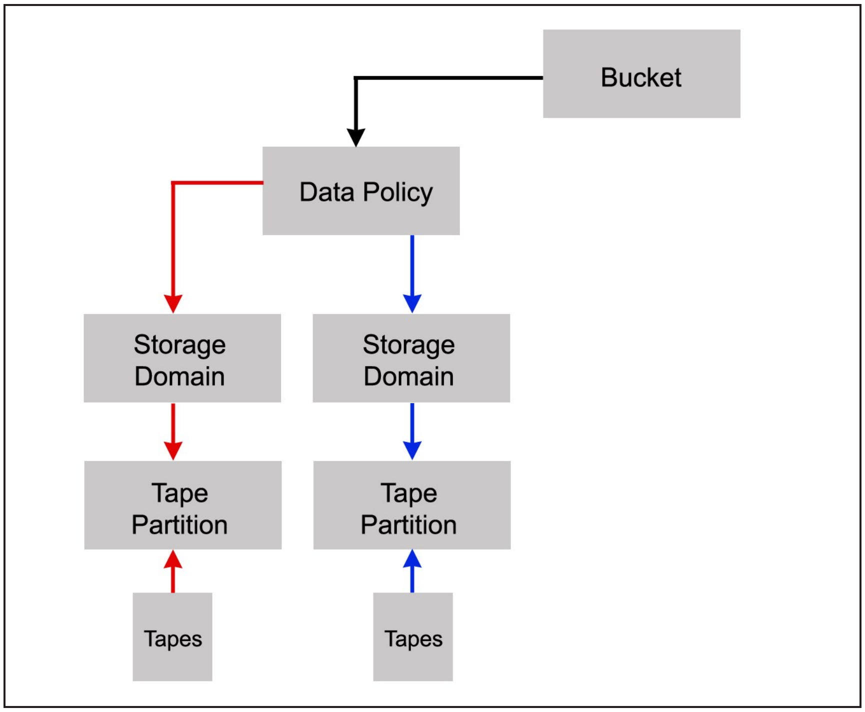


Figure 36 The Dual Copy on Tape workflow.

The dual copy on tape data policy is configured with the following attributes:

Parameter	Value	Description
Storage Domain - Tape First Copy - Data is written to the primary tape storage domain. This domain is created automatically when the gateway detects the first tape partition created on the tape library.		
Days to wait before verifying data	**null**	Data integrity verification is not performed automatically.
Secure Media Allocation	**cleared**	Media allocated to the storage domain may be reused by another storage domain if all data is deleted.
Write Optimization	**Capacity**	Job chunks are written across as few pieces of media as possible. Fewer tape drives are used, so performance is lower.
LTFS File Naming	**Object ID**	File names use the format {*bucket name*}/{*object id*}, for example, bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82.
Media Export Allowed	**cleared**	Media export is not allowed.
Storage Domain Member for Tape First Copy		
Tape Type	***varies***	The tape type matching the latest generation of tape drive in the partition.
Auto Compaction Threshold	**20**	The percentage of a tape with deleted objects at which auto compaction is triggered. The default is 95. The minimum is 10.
Write Preference	**Normal**	The gateway uses the partition after partitions with **High** write preference and before a partition with **Low** or **Never Select** write preference.
Storage Domain - Tape Second Copy - A second copy of the data is written to a tape storage domain optimized for tape export. This domain is created automatically when the gateway detects a tape partition created on the tape library.		
Days to wait before verifying data	**null**	Data integrity verification is not performed automatically.
Secure Media Allocation	**cleared**	Media allocated to the storage domain may be reused by another storage domain if all data is deleted.

Parameter	Value	Description
Write Optimization	**Capacity**	Job chunks are written across as few pieces of media as possible. Fewer tape drives are used, so performance is lower.
LTFS File Naming	**Object ID**	File names use the format {*bucket name*}/{*object id*}, for example, bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82.
Media Exort Allowed	**selected**	Media export is allowed.
Auto Export on Job Completion	**cleared**	Media is not auto exported upon job completion.
Auto Export on Job Cancel	**cleared**	Media is not auto exported upon job cancellation.
Auto Export on Media Full	**cleared**	Media is not auto exported upon media full.
Scheduled Auto Export	**cleared**	Media is not auto exported on a schedule.
Tape Type	***varies***	The tape type matching the latest generation of tape drive in the partition.
Write Preference	**Normal**	The gateway uses the partition after partitions with **High** write preference and before a partition with **Low** or **Never Select** write preference.
Data Policy - Dual Copy on Tape		
Blobbing Enabled	**selected**	Allows an object to be broken into multiple blobs.
Minimize Spanning	**cleared**	Jobs larger than 1 TB are allowed to span across multiple tapes or pools as needed to maximize capacity utilization and performance.

Parameter	Value	Description
Default GET Job Priority	**High**	When the storage domain receives a GET job, it is processed with high priority, which is before low and normal priority jobs. Jobs of different types are put in order based on priority. **Note:** When using a DS3 client, this setting can be overridden when sending a GET job by specifying a different priority in the Get Job command. See the *Spectra BlackPearl DS3 API Reference* for more information.
Default PUT Job Priority	**Normal**	When the storage domain receives a PUT job, it is processed with normal priority, which is after high priority jobs but before low and normal priority jobs. Jobs of different types are put in order based on priority. **Note:** When using a DS3 client, this setting can be overridden when sending a PUT job by specifying a different priority in the Put Job command. See the *Spectra BlackPearl DS3 API Reference* for more information.
Default VERIFY Job Priority	**Low**	When the storage domain receives a VERIFY job, it is processed with low priority, which is the lowest setting. **Note:** When using a DS3 client, this setting can be overridden when sending a VERIFY job by specifying a different priority in the Create Verify Job command. See the *Spectra BlackPearl DS3 API Reference* for more information.
Default Verify After Write	**cleared**	Data is not verified after a write.
Rebuild Priority	**Low**	If data is lost from tape media, the data is rebuilt using low priority, which is the lowest setting.
Checksum Type	**MD5**	Data using this storage domain is CRC checked using the MD5 checksum type. Data is CRC checked when it is written to cache with a PUT job, or read back from media with a GET job.
End-to-end CRC	**No**	This data policy does not use end-to-end CRC checking.

Parameter	Value	Description
Versioning	**None**	In order to upload a new version of an object already PUT to the gateway, the first version must be deleted.
Always Accept Replicated PUT Jobs	**cleared**	PUT jobs created for this data policy fail if one or more replication targets the gateway must PUT to are unavailable.
Data Persistence Rule for Tape First Copy		
Type	**Permanent**	Data is moved to tape and maintained on tape media until data is deleted from a bucket. **Note:** When data is deleted from a bucket, it is removed from tape media, but individual tape media cartridges are not reclaimed for use until all data is deleted from a tape cartridge.
Bucket Isolation Level	**Standard**	Data from different buckets can be mixed on to the same piece of media.
Data Persistence Rule for Tape Second Copy		
Type	**Permanent**	Data is moved to tape and maintained on tape media until data is deleted from a bucket. **Note:** When data is deleted from a bucket, it is removed from tape media, but individual tape media cartridges are not reclaimed for use until all data is deleted from a tape cartridge.
Bucket Isolation Level	**Standard**	Data from different buckets can be mixed on to the same piece of media.

Single Copy on Nearline Object Storage Disk

This data policy persists a single copy of each job sent to the gateway on to nearline object storage disk, which is provided by 77-bay, 96-bay, and 107-bay expansion nodes, or in the Gen2 S Series master node. Once data is written on nearline storage disk, it is removed from the BlackPearl cache if the gateway detects that more cache space is needed for incoming data.

Note: This data policy is automatically created when the gateway detects a nearline storage disk partition.

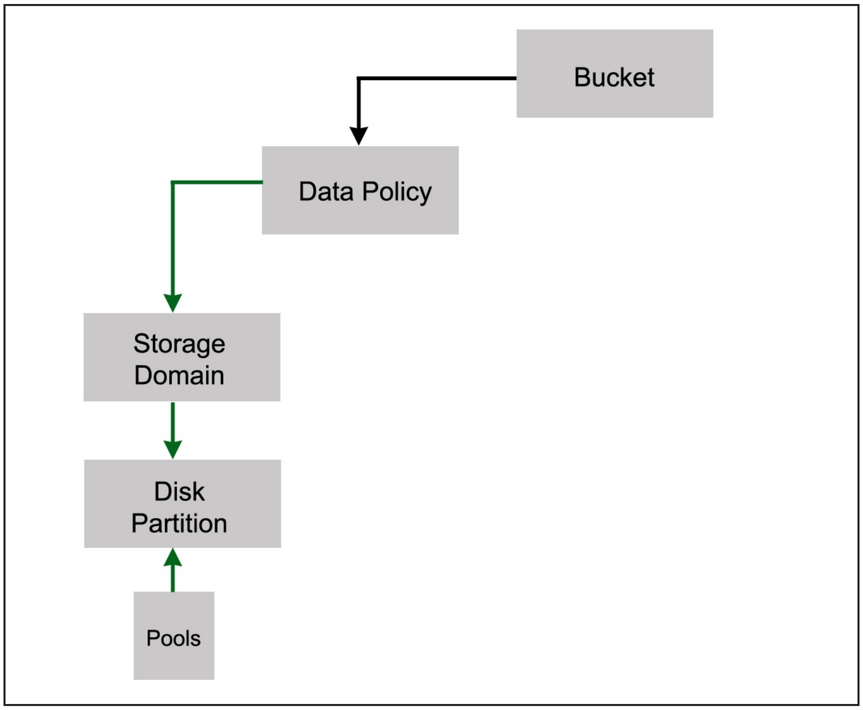


Figure 37 The Single Copy on Nearline Object Storage Disk workflow.

The single copy on nearline storage disk data policy is configured with the following attributes:

Parameter	Value	Description
Storage Domain - Pool First Copy - Data is written to the primary nearline storage domain. This domain is created automatically after you create a nearline object storage disk partition.		
Days to wait before verifying data	**null**	Data integrity verification is not performed automatically.
Secure Media Allocation	**cleared**	Media allocated to the storage domain may be reused by another storage domain if all data is deleted.
Write Optimization	**Capacity**	Job chunks are written across as few pools as possible.
LTFS File Naming	**Object ID**	File names use the format {*bucket name*}/{*object id*}, for example, bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82.
Media Export Allowed	**selected**	Media export is allowed.
Auto Export on Job Completion	**cleared**	Media is not auto exported upon job completion.
Auto Export on Job Cancel	**cleared**	Media is not auto exported upon job cancellation.
Auto Export on Media Full	**cleared**	Media is not auto exported upon media full.
Scheduled Auto Export	**cleared**	Media is not auto exported on a schedule.
Storage Domain Member for Pool First Copy - The first nearline disk partition created.		
Write Preference	**Normal**	The gateway uses the partition after partitions with **High** write preference and before a partition with **Low** or **Never Select** write preference.
Data Policy - Single Copy on Nearline Disk		
Blobbing Enabled	**selected**	Allows an object to be broken into multiple blobs.

Parameter	Value	Description
Minimize Spanning	**cleared**	Jobs larger than 1 TB are allowed to span across multiple tapes or pools as needed to maximize capacity utilization and performance.
Default GET Job Priority	**High**	When the storage domain receives a GET job, it is processed with high priority, which is before low and normal priority jobs. Jobs of different types are put in order based on priority. **Note:** When using a DS3 client, this setting can be overridden when sending a GET job by specifying a different priority in the Get Job command. See the *Spectra BlackPearl DS3 API Reference* for more information.
Default PUT Job Priority	**Normal**	When the storage domain receives a PUT job, it is processed with normal priority, which is after high priority jobs but before low and normal priority jobs. Jobs of different types are put in order based on priority. **Note:** When using a DS3 client, this setting can be overridden when sending a PUT job by specifying a different priority in the Put Job command. See the *Spectra BlackPearl DS3 API Reference* for more information.
Default VERIFY Job Priority	**Low**	When the storage domain receives a VERIFY job, it is processed with low priority, which is the lowest setting. **Note:** When using a DS3 client, this setting can be overridden when sending a VERIFY job by specifying a different priority in the Create Verify Job command. See the *Spectra BlackPearl DS3 API Reference* for more information.
Default Verify After Write	**cleared**	Data is not verified after a write.
Rebuild Priority	**Low**	If data is lost from disk, the data is rebuilt using low priority, which is the lowest setting.
Checksum Type	**MD5**	Data using this storage domain is CRC checked using the MD5 checksum type. Data is CRC checked when it is written to cache with a PUT job, or read back from media with a GET job.

Parameter	Value	Description
End-to-end CRC	**No**	This data policy does not use end-to-end CRC checking.
Versioning	**None**	In order to upload a new version of an object already PUT to the gateway, the first version must be deleted.
Always Accept Replicated PUT Jobs	**cleared**	PUT jobs created for this data policy fail if one or more replication targets the gateway must PUT to are unavailable.
Type	**Permanent**	Data is moved to nearline disk and maintained on nearline disk until data is deleted from a bucket.
Bucket Isolation Level	**Standard**	Data from different buckets can be mixed on to the same piece of media.
Data Persistence Rule for Pool First Copy		
Type	**Permanent**	Data is moved to disk and maintained on disk media until data is deleted from a bucket.
Isolation Level	**Standard**	Data from different buckets can be mixed on to the same piece of media.

Single Copy on Nearline Object Storage Disk and Tape

This data policy persists a single copy of each job sent to the gateway on to both nearline storage disk and tape media. Nearline object storage disk is provided by 77-bay, 96-bay, and 107-bay expansion nodes, or in the Gen2 S Series master node. Tape storage is provided by a Spectra Logic tape library.

Once data is written on both nearline object storage disk and tape, it is removed from the BlackPearl cache if the gateway detects that more cache space is needed for incoming data.

This configuration offers secure glacier storage on tape with the benefit of faster restores of data from nearline object storage disk.

Note: This data policy is automatically created when the gateway detects a nearline disk partition and a tape partition.

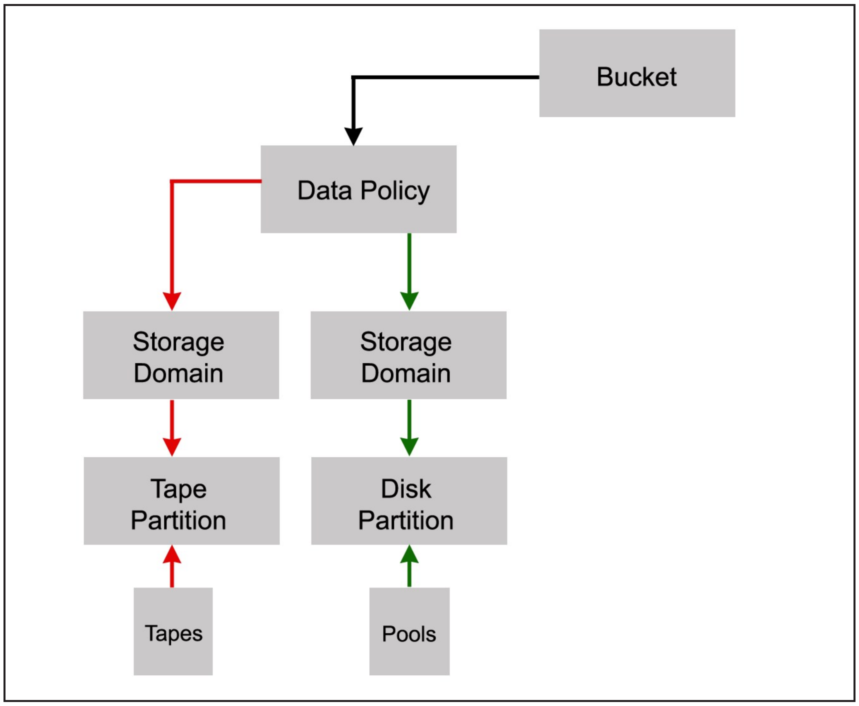


Figure 38 The Single Copy on Nearline Object Storage Disk and Tape workflow.

The single copy on nearline storage disk and tape data policy is configured with the following attributes:

Parameter	Value	Description
Storage Domain - Tape First Copy - Data is written to the primary tape storage domain. This domain is created automatically when the gateway detects the first tape partition created on the tape library.		
Days to wait before verifying data	**null**	Data integrity verification is not performed automatically.
Secure Media Allocation	**cleared**	Media allocated to the storage domain may be reused by another storage domain if all data is deleted.
Write Optimization	**Capacity**	Job chunks are written across as few pieces of media as possible. Fewer tape drives are used, so performance is lower.
LTFS File Naming	**Object ID**	File names use the format {*bucket name*}/{*object id*}, for example, bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82.
Media Export Allowed	**cleared**	Media export is not allowed.
Storage Domain Member for Tape First Copy		
Tape Type	***varies***	The tape type matching the latest generation of tape drive in the partition.
Auto Compaction Threshold	**20**	The percentage of a tape with deleted objects at which auto compaction is triggered. The default is 95. The minimum is 10.
Write Preference	**Normal**	The gateway uses the partition after partitions with **High** write preference and before a partition with **Low** or **Never Select** write preference.
Storage Domain - Pool First Copy- Data is written to the primary nearline storage domain. This domain is created automatically after you create a nearline disk partition.		
Days to wait before verifying data	**null**	Data integrity verification is not performed automatically.

Parameter	Value	Description
Secure Media Allocation	**cleared**	Media allocated to the storage domain may be reused by another storage domain if all data is deleted.
Write Optimization	**Capacity**	Job chunks are written across as few pools as possible.
LTFS File Naming	**Object ID**	File names use the format {*bucket name*}/{*object id*}, for example, bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82.
Media Export Allowed	**selected**	Media export is allowed.
Auto Export on Job Completion	**cleared**	Media is not auto exported upon job completion.
Auto Export on Job Cancel	**cleared**	Media is not auto exported upon job cancellation.
Auto Export on Media Full	**cleared**	Media is not auto exported upon media full.
Scheduled Auto Export	**cleared**	Media is not auto exported on a schedule.
Storage Domain Member for Pool First Copy - The first nearline disk partition created.		
Write Preference	**Normal**	The gateway uses the partition after partitions with **High** write preference and before a partition with **Low** or **Never Select** write preference.
Data Policy - Single Copy on Nearline Disk and Tape		
Blobbing Enabled	**selected**	Allows an object to be broken into multiple blobs.
Minimize Spanning	**cleared**	Jobs larger than 1 TB are allowed to span across multiple tapes or pools as needed to maximize capacity utilization and performance.

Parameter	Value	Description
Default GET Job Priority	**High**	When the storage domain receives a GET job, it is processed with high priority, which is before low and normal priority jobs. Jobs of different types are put in order based on priority. **Note:** When using a DS3 client, this setting can be overridden when sending a GET job by specifying a different priority in the Get Job command. See the *Spectra BlackPearl DS3 API Reference* for more information.
Default PUT Job Priority	**Normal**	When the storage domain receives a PUT job, it is processed with normal priority, which is after high priority jobs but before low and normal priority jobs. Jobs of different types are put in order based on priority. **Note:** When using a DS3 client, this setting can be overridden when sending a PUT job by specifying a different priority in the Put Job command. See the *Spectra BlackPearl DS3 API Reference* for more information.
Default VERIFY Job Priority	**Low**	When the storage domain receives a VERIFY job, it is processed with low priority, which is the lowest setting. **Note:** When using a DS3 client, this setting can be overridden when sending a VERIFY job by specifying a different priority in the Create Verify Job command. See the *Spectra BlackPearl DS3 API Reference* for more information.
Default Verify After Write	**cleared**	Data is not verified after a write.
Rebuild Priority	**Low**	If data is lost from tape media, the data is rebuilt using low priority, which is the lowest setting.
Checksum Type	**MD5**	Data using this storage domain is CRC checked using the MD5 checksum type. Data is CRC checked when it is written to cache with a PUT job, or read back from media with a GET job.
End-to-end CRC	**No**	This data policy does not use end-to-end CRC checking.

Parameter	Value	Description
Versioning	**None**	In order to upload a new version of an object already PUT to the gateway, the first version must be deleted.
Always Accept Replicated PUT Jobs	**cleared**	PUT jobs created for this data policy fail if one or more replication targets the gateway must PUT to are unavailable.
Data Persistence Rule for Tape First Copy		
Type	**Permanent**	Data is moved to tape and maintained on tape media until data is deleted from a bucket. **Note:** When data is deleted from a bucket, it is removed from tape media, but individual tape media cartridges are not reclaimed for use until all data is deleted from a tape cartridge.
Bucket Isolation Level	**Standard**	Data from different buckets can be mixed on to the same piece of media.
Data Persistence Rule for Pool First Copy		
Type	**Permanent**	Data is moved to disk and maintained on disk media until data is deleted from a bucket.
Isolation Level	**Standard**	Data from different buckets can be mixed on to the same media.

Single Copy on Nearline Object Storage Disk and Dual Copy on Tape

This data policy persists a single copy of each job sent to the gateway on to nearline object storage disk, and two copies of the job on to tape media. Nearline storage is provided by 77-bay, 96-bay, and 107-bay expansion nodes, or in the Gen2 S Series master node, while tape storage is provided by a Spectra Logic tape library.

Once data is written on both nearline object storage disk and tape, it is removed from the BlackPearl cache if the gateway detects that more cache space is needed for incoming data.

This configuration offers secure glacier storage on tape with the benefit of faster restores of data from nearline object storage disk.

This data policy is helpful if you want to export one copy of the bucket on tape media for storage off site, which provides enhanced data security in the case of ransomeware attacks or disaster recovery.

Note: This data policy is automatically created when the gateway detects a nearline storage disk partition and two tape partitions.

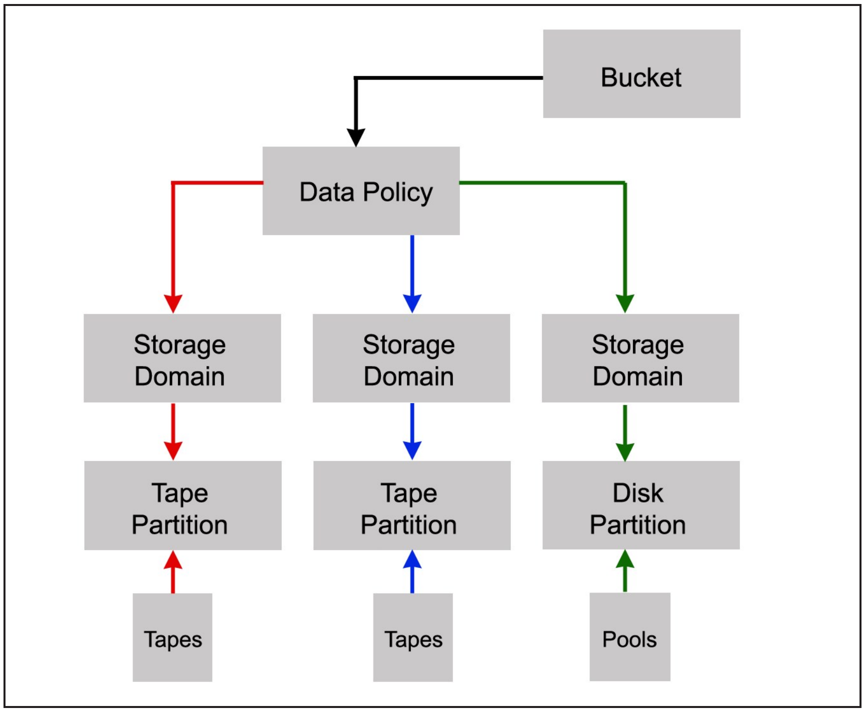


Figure 39 The Single Copy on Nearline Object Storage Disk and Dual Copy on Tape workflow.

The single copy on nearline storage disk and dual copy on tape data policy is configured with the following attributes:

Parameter	Value	Description
Storage Domain - Tape First Copy - Data is written to the primary tape storage domain. This domain is created automatically when the gateway detects the first tape partition created on the tape library.		
Days to wait before verifying data	**null**	Data integrity verification is not performed automatically.
Secure Media Allocation	**cleared**	Media allocated to the storage domain may be reused by another storage domain if all data is deleted.
Write Optimization	**Capacity**	Job chunks are written across as few pieces of media as possible. Fewer tape drives are used, so performance is lower.
LTFS File Naming	**Object ID**	File names use the format {*bucket name*}/{*object id*}, for example, bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82.
Media Export Allowed	**cleared**	Media export is not allowed.
Storage Domain Member for Tape First Copy		
Tape Type	***varies***	The tape type matching the latest generation of tape drive in the partition.
Write Preference	**Normal**	The gateway uses the partition after partitions with **High** write preference and before a partition with **Low** or **Never Select** write preference.
Storage Domain - Tape Second Copy - A second copy of the data is written to a tape storage domain optimized for tape exports. This domain is created automatically when the gateway detects a tape partition created on the tape library.		
Days to wait before verifying data	**null**	Data integrity verification is not performed automatically.
Secure Media Allocation	**cleared**	Media allocated to the storage domain may be reused by another storage domain if all data is deleted.

Parameter	Value	Description
Write Optimization	**Capacity**	Job chunks are written across as few pieces of media as possible. Fewer tape drives are used, so performance is lower.
LTFS File Naming	**Object ID**	File names use the format {*bucket name*}/{*object id*}, for example, bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82.
Media Export Allowed	**selected**	Media export is allowed.
Auto Export on Job Completion	**cleared**	Media is not auto exported upon job completion.
Auto Export on Job Cancel	**cleared**	Media is not auto exported upon job cancellation.
Auto Export on Media Full	**cleared**	Media is not auto exported upon media full.
Scheduled Auto Export	**cleared**	Media is not auto exported on a schedule.
Storage Domain Member for Tape Second Copy		
Tape Type	***varies***	The tape type matching the latest generation of tape drive in the partition.
Auto Compaction Threshold	**20**	The percentage of a tape with deleted objects at which auto compaction is triggered. The default is 95. The minimum is 10.
Write Preference	**Normal**	The gateway uses the partition after partitions with **High** write preference and before a partition with **Low** or **Never Select** write preference.
Storage Domain - Pool First Copy- Data is written to the primary nearline storage domain. This domain is created automatically after you create a nearline storage disk partition.		
Days to wait before verifying data	**null**	Data integrity verification is not performed automatically.
Secure Media Allocation	**cleared**	Media allocated to the storage domain may be reused by another storage domain if all data is deleted.

Parameter	Value	Description
Write Optimization	**Capacity**	Job chunks are written across as few pools as possible.
LTFS File Naming	**Object ID**	File names use the format {*bucket name*}/{*object id*}, for example, bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82.
Media Export Allowed	**selected**	Media export is allowed.
Auto Export on Job Completion	**cleared**	Media is not auto exported upon job completion.
Auto Export on Job Cancel	**cleared**	Media is not auto exported upon job cancellation.
Auto Export on Media Full	**cleared**	Media is not auto exported upon media full.
Scheduled Auto Export	**cleared**	Media is not auto exported on a schedule.
Storage Domain Member for Pool First Copy - The first nearline disk partition created.		
Write Preference	**Normal**	The gateway uses the partition after partitions with **High** write preference and before a partition with **Low** or **Never Select** write preference.
Data Policy - Single Copy on Nearline Disk and Dual Copy on Tape		
Blobbing Enabled	**selected**	Allows an object to be broken into multiple blobs.
Minimize Spanning	**cleared**	Jobs larger than 1 TB are allowed to span across multiple tapes or pools as needed to maximize capacity utilization and performance.
Default GET Job Priority	**High**	When the storage domain receives a GET job, it is processed with high priority, which is before low and normal priority jobs. Jobs of different types are put in order based on priority. **Note:** When using a DS3 client, this setting can be overridden when sending a GET job by specifying a different priority in the Get Job command. See the *Spectra BlackPearl DS3 API Reference* for more information.

Parameter	Value	Description
Default PUT Job Priority	**Normal**	When the storage domain receives a PUT job, it is processed with normal priority, which is after high priority jobs but before low and normal priority jobs. Jobs of different types are put in order based on priority. **Note:** When using a DS3 client, this setting can be overridden when sending a PUT job by specifying a different priority in the Put Job command. See the *Spectra BlackPearl DS3 API Reference* for more information.
Default VERIFY Job Priority	**Low**	When the storage domain receives a VERIFY job, it is processed with low priority, which is the lowest setting. **Note:** When using a DS3 client, this setting can be overridden when sending a VERIFY job by specifying a different priority in the Create Verify Job command. See the *Spectra BlackPearl DS3 API Reference* for more information.
Default Verify After Write	**cleared**	Data is not verified after a write.
Rebuild Priority	**Low**	If data is lost from tape media, the data is rebuilt using low priority, which is the lowest setting.
Checksum Type	**MD5**	Data using this storage domain is CRC checked using the MD5 checksum type. Data is CRC checked when it is written to cache with a PUT job, or read back from media with a GET job.
End-to-end CRC	**No**	This data policy does not use end-to-end CRC checking.
Versioning	**None**	In order to upload a new version of an object already PUT to the gateway, the first version must be deleted.
Always Accept Replicated PUT Jobs	**cleared**	PUT jobs created for this data policy fail if one or more replication targets the gateway must PUT to are unavailable.
Continue to the next page		

Parameter	Value	Description
Data Persistence Rule for Tape First Copy		
Type	**Permanent**	Data is moved to tape and maintained on tape media until data is deleted from a bucket. **Note:** When data is deleted from a bucket, it is removed from tape media, but individual tape media cartridges are not reclaimed for use until all data is deleted from a tape cartridge.
Bucket Isolation Level	**Standard**	Data from different buckets can be mixed on to the same piece of media.
Data Persistence Rule for Tape Second Copy		
Type	**Permanent**	Data is moved to tape and maintained on tape media until data is deleted from a bucket. **Note:** When data is deleted from a bucket, it is removed from tape media, but individual tape media cartridges are not reclaimed for use until all data is deleted from a tape cartridge.
Bucket Isolation Level	**Standard**	Data from different buckets can be mixed on to the same piece of media.
Data Persistence Rule for Pool First Copy		
Type	**Permanent**	Data is moved to disk and maintained on disk media until data is deleted from a bucket.
Isolation Level	**Standard**	Data from different buckets can be mixed on to the same media.

Additional Configurations

In addition to the above standard configurations, many custom configurations can be created for BlackPearl Nearline gateway flash disks, spinning disk, and tape storage.

Contact Spectra Logic Professional Services for assistance. See Contacting Spectra Logic on page 9.

CHAPTER 4 - CONFIGURING ADVANCED BUCKET MANAGEMENT

This chapter provides instructions on how to configure Advanced Bucket Management features.

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 concepts in Understanding Advanced Bucket Management on page 88 and have thoughtfully planned your data policies before you start using the BlackPearlgateway to store data.

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 concepts in Understanding Advanced Bucket Management on page 88 and have thoughtfully planned your data policies before you start using the BlackPearl gateway to store data.

Create a Disk Pool 130
Create a Nearline Storage Disk Pool 131
Create an Online Disk Pool 134
Create a Disk Partition 137
Create a Tape Partition 138
Create a Replication Target 139
Create a BlackPearl Target 139
Create an Amazon S3 Target 143
Create a Microsoft Azure Target 147
Create a Storage Domain 150
Add a Storage Domain Member to a Storage Domain 156
Create a Data Policy 159
Add Data Persistence Rules and Replication Rules to a Data Policy 163
Create Data Policy ACLs 169
Create a Bucket 171
Create a New Bucket ACL for a Group 173

Create a New Bucket ACL for a User 174

Transfer Data 176

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 without I/O, 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. This allows the BlackPearl gateway to store more data.

If desired, select the check box to enable data compression with ZFS to allow the BlackPearl 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 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.

If your BlackPearl gateway does not include disk storage, continue with Create a Tape Partition on page 138.

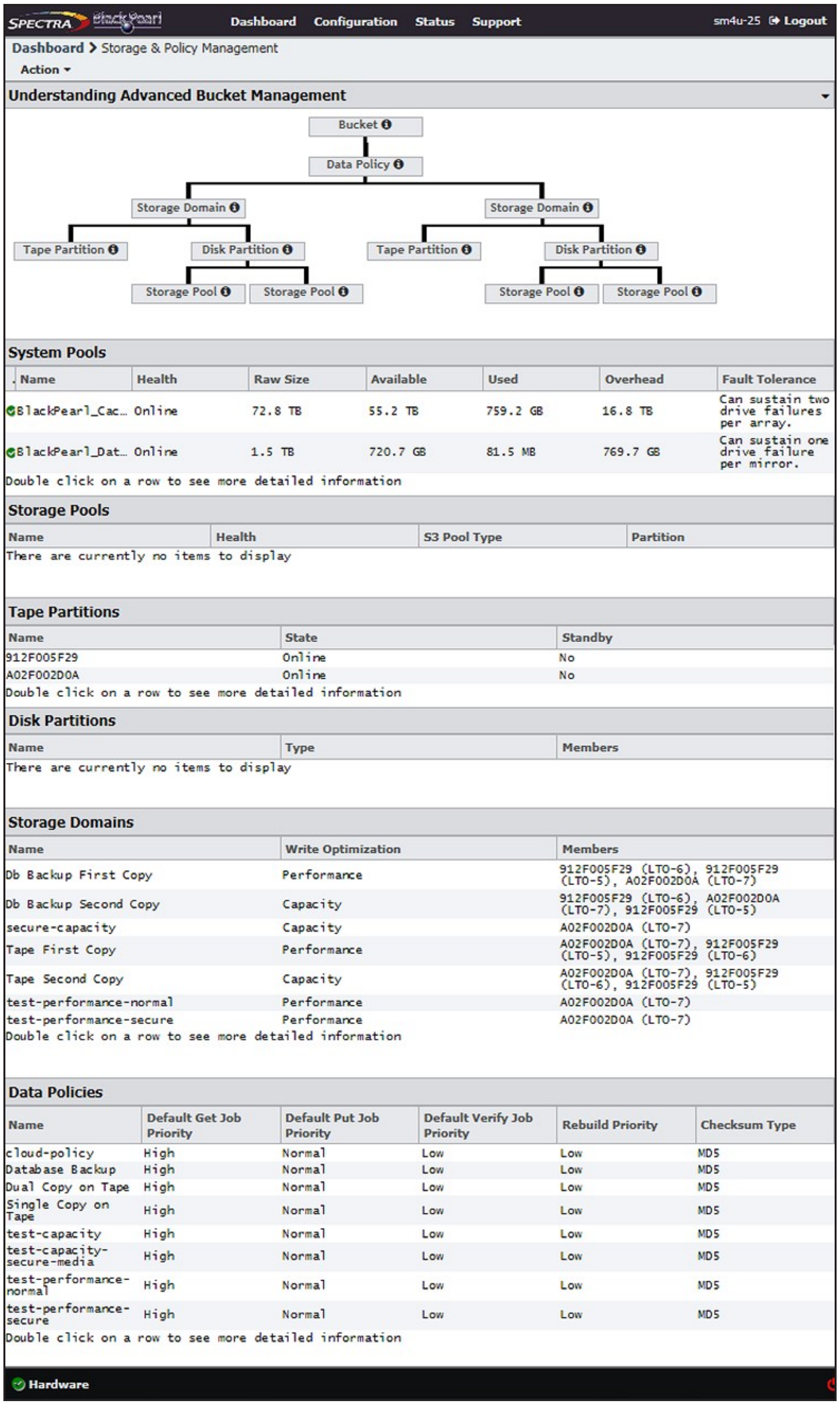
Create a Nearline Storage Disk Pool

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

If you do not want to configure a nearline disk pool, continue with Create an Online Disk Pool on page 134.

Note: Nearline pools created on a 96-bay expansion node have a hard coded capacity utilization limit percentage. On gateways running BlackPearl OS 5.2 or later, this percentage is 95%. On gateways running BlackPearl OS 5.1.x or older, the capacity limit percentage is 87%.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen.



System Pools

Name	Health	Raw Size	Available	Used	Overhead	Fault Tolerance
BlackPearl_Cac…	Online	72.8 TB	55.2 TB	759.2 GB	16.8 TB	Can sustain two drive failures per array.
BlackPearl_Dat…	Online	1.5 TB	720.7 GB	81.5 MB	769.7 GB	Can sustain one drive failure per mirror.

Double click on a row to see more detailed information

Storage Pools

Name	Health	S3 Pool Type	Partition

There are currently no items to display

Tape Partitions

Name	State	Standby
912F005F29	Online	No
A02F002D0A	Online	No

Double click on a row to see more detailed information

Disk Partitions

Name	Type	Members

There are currently no items to display

Storage Domains

Name	Write Optimization	Members
Db Backup First Copy	Performance	912F005F29 (LTO-6), 912F005F29 (LTO-5), A02F002D0A (LTO-7)
Db Backup Second Copy	Capacity	912F005F29 (LTO-6), A02F002D0A (LTO-7), 912F005F29 (LTO-5)
secure-capacity	Capacity	A02F002D0A (LTO-7)
Tape First Copy	Performance	A02F002D0A (LTO-7), 912F005F29 (LTO-5), 912F005F29 (LTO-6)
Tape Second Copy	Capacity	A02F002D0A (LTO-7), 912F005F29 (LTO-6), 912F005F29 (LTO-5)
test-performance-normal	Performance	A02F002D0A (LTO-7)
test-performance-secure	Performance	A02F002D0A (LTO-7)

Double click on a row to see more detailed information

Data Policies

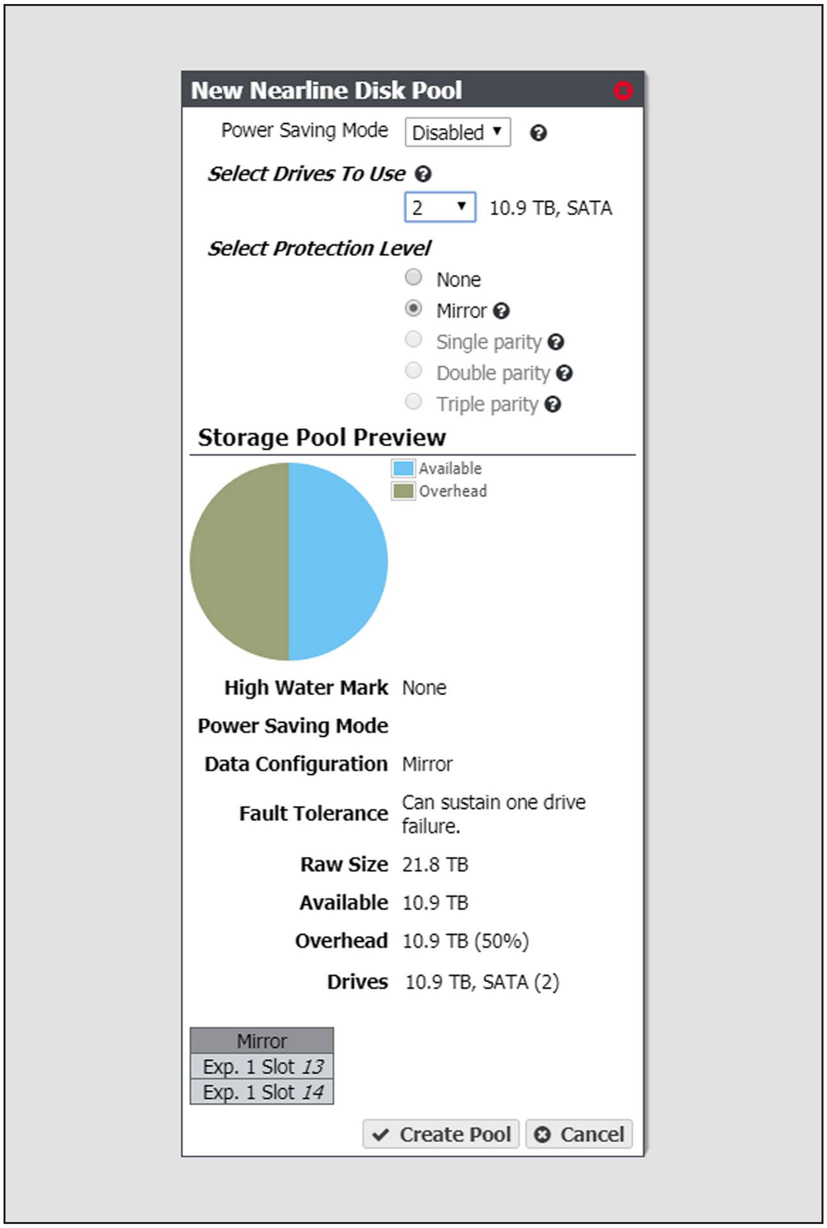
Name	Default Get Job Priority	Default Put Job Priority	Default Verify Job Priority	Rebuild Priority	Checksum Type
cloud-policy	High	Normal	Low	Low	MD5
Database Backup	High	Normal	Low	Low	MD5
Dual Copy on Tape	High	Normal	Low	Low	MD5
Single Copy on Tape	High	Normal	Low	Low	MD5
test-capacity	High	Normal	Low	Low	MD5
test-capacity-secure-media	High	Normal	Low	Low	MD5
test-performance-normal	High	Normal	Low	Low	MD5
test-performance-secure	High	Normal	Low	Low	MD5

Double click on a row to see more detailed information

Figure 40 The Advanced Bucket Management screen.

2. Select **Action > New Nearline Disk Pool**. The New Nearline Disk Pool dialog box displays.

Note: The **Storage Pool Preview** pane does not display until you have selected the disks you want to use in the disk pool.



New Nearline Disk Pool

Power Saving Mode: Disabled ▾

Select Drives To Use

2 ▾ 10.9 TB, SATA

Select Protection Level

○ None
● Mirror
○ Single parity
○ Double parity
○ Triple parity

Storage Pool Preview

High Water Mark	None
Power Saving Mode	
Data Configuration	Mirror
Fault Tolerance	Can sustain one drive failure.
Raw Size	21.8 TB
Available	10.9 TB
Overhead	10.9 TB (50%)
Drives	10.9 TB, SATA (2)

Mirror
Exp. 1 Slot *13*
Exp. 1 Slot *14*

Figure 41 The New Nearline Disk Pool dialog box.

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

For this option....	Do the following...
Power Saving Mode	Using the drop-down menu, select the desired **Power Saving Mode**. Enabling the power saving mode sets the standby timer to 60 minutes for all drives in the pool, but only if all drives in the pool are capable of using a standby timer. When the disk pool is idle for 60 minutes, the drives spin-down to conserve power. **Note:** To use this feature, all drives in the storage pool must be power-saving compatible.
Select Drives To Use	Use the drop-down menu to select the number of drives to include in the pool. If your gateway contains more than one type of disk drive, multiple drop-down menus are present, but only one type can be assigned to a pool. 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.
Select Protection Level	Use the radio buttons to select the protection level for the pool. Only one option can be selected. Use the Storage Pool Preview information to compare the fault tolerance and required overhead for each configuration. **None**—The pool is not configured to provide data protection. Any drive failure results in data loss. **Note:** Spectra Logic doesD 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 parity**—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 parity**—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 parity**—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.

4. Click **Create Pool**. The new nearline disk pool is listed on the Advanced Bucket Management screen.

Create an Online Disk Pool

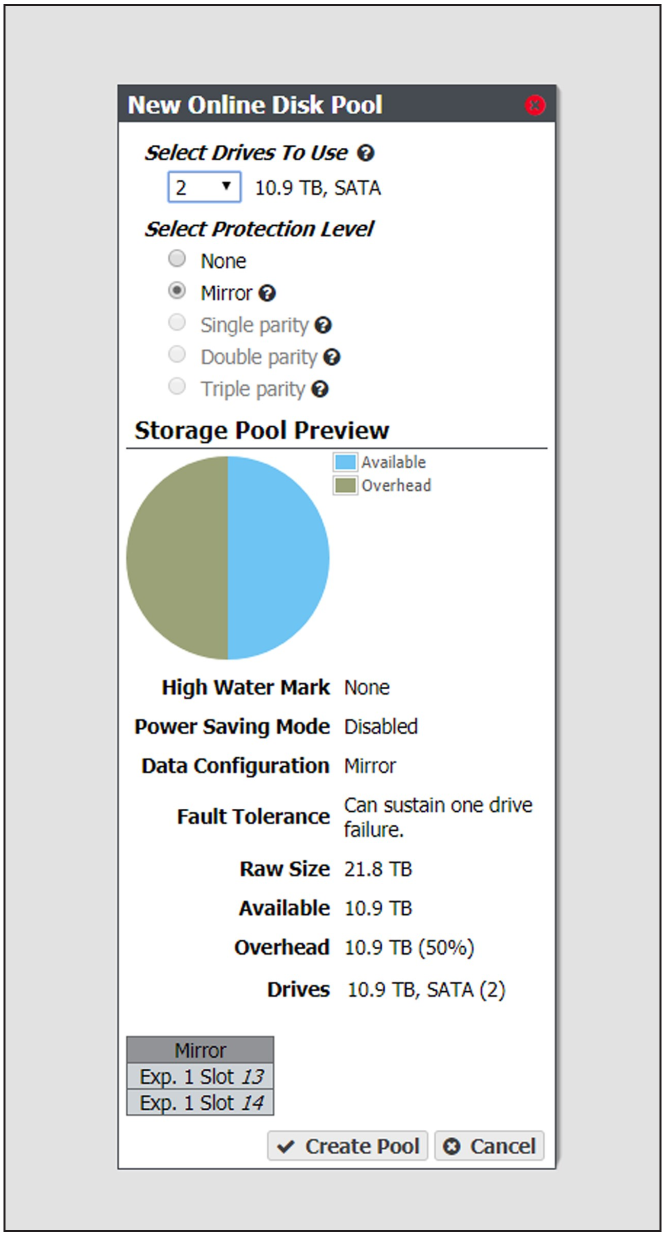
Use the instructions in this section to create an online disk pool.

If you do not want to create an online disk pool, continue with Create a Disk Partition on page 137.

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

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Select **Action > New Online Disk Pool**. The New Online Disk Pool dialog box displays.

Note: The **Storage Pool Preview** pane does not display until you have selected the disks you want to use in the disk pool.



New Online Disk Pool

Select Drives To Use

2 ▾ 10.9 TB, SATA

Select Protection Level

○ None
● Mirror
○ Single parity
○ Double parity
○ Triple parity

Storage Pool Preview

High Water Mark	None
Power Saving Mode	Disabled
Data Configuration	Mirror
Fault Tolerance	Can sustain one drive failure.
Raw Size	21.8 TB
Available	10.9 TB
Overhead	10.9 TB (50%)
Drives	10.9 TB, SATA (2)

Mirror
Exp. 1 Slot *13*
Exp. 1 Slot *14*

Figure 42 The New Online Disk Pool dialog box.

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

For this option....	Do the following...
Select Drives To Use	Use the drop-down menu to select the number of drives to include in the pool. If your gateway contains more than one type of disk drive, multiple drop-down menus are present, but only one type can be assigned to a pool. 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.
Select Protection Level	Use the radio buttons to select the protection level for the pool. Only one option can be selected. Use the Storage Pool Preview information to compare the fault tolerance and required overhead for each configuration. **None**—The pool is not configured to provide data protection. Any drive failure results in data loss. **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 parity**—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 parity**—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 parity**—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.

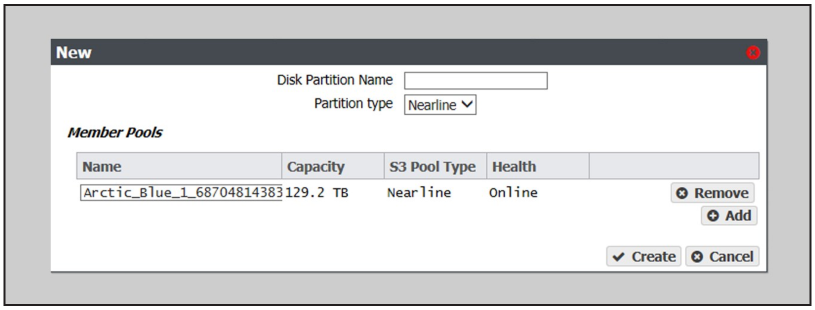
4. Click **Create Pool**. The new online disk pool is listed on the Advanced Bucket Management screen.

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. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management**. The Advanced Bucket Management screen displays (see Figure 40 on page 132).
2. Select **Action > New Disk Partition**. The New Disk Partition dialog box displays.



Disk Partition Name

Partition type: Nearline

Member Pools

Name	Capacity	S3 Pool Type	Health
Arctic_Blue_1_68704814383	129.2 TB	Nearline	Online

Figure 43 The New Disk Partition dialog box.

3. Enter a name for the disk partition in the **Disk Partition Name** field.
4. Use the drop-down menu to select the **Partition type**. You cannot mix different types of disk pools in a disk partition.

- Select **Online** to use a disk pool that is always powered on and available for access.
- Select **Nearline** to use a disk pool that can be configured to spin down after 60 minutes without I/O, for power savings.

5. Add a disk pool to the disk partition.
    a. In the Member Pools pane, click **Add**. A new row appears in the pane.
    b. Use the **Name** drop down menu to select a disk pool from the list of previously configured disk pools. The Capacity, Type, and Health of the disk pool display.

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

    c. If desired, repeat Step a and Step b to add additional disk pools to the disk partition.

6. Click **Create**. The new disk partition displays on the Advanced Bucket Management screen.

Create a Tape Partition

Use the *Tape Library User Guides on page 27* for your Spectra Logic or other supported tape library to create a partition. Once the BlackPearl gateway detects a partition on a tape library connected to it, the tape partition is automatically listed on the Advanced Bucket Management screen.

If your BlackPearl gateway does not have a tape library, continue with Create a Replication Target below.

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

CREATE A REPLICATION TARGET

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

If your BlackPearl gateway does not include the feature to replicate data to cloud targets, continue with Create a Storage Domain on page 150.

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 Services on page 234.

Create a BlackPearl Target

Configuring a BlackPearl target allows a data policy on one BlackPearl gateway to replicate data to a second gateway. If data is sent to a data policy that is not configured for replication, the data is not replicated to the target 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 gateways provides enhanced data security and disaster recovery if the source gateway fails. When you delete data from the source gateway, you can optionally specify to have the data deleted from the target gateway as well.

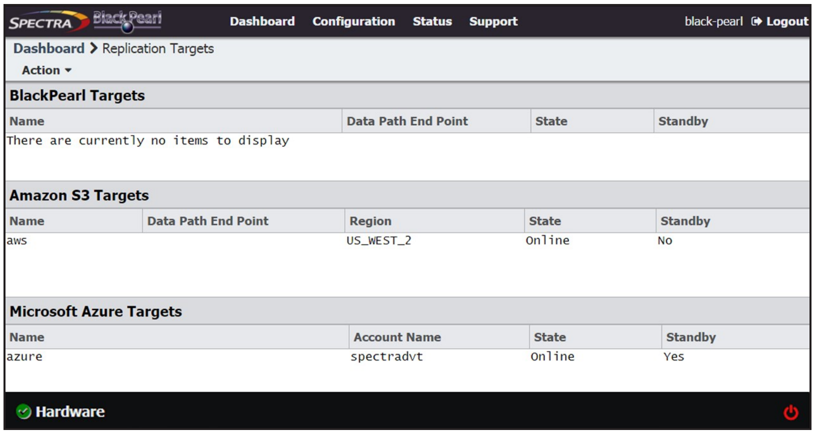
IMPORTANT Spectra Logic recommends using the same versioning settings on both the source and target BlackPearlgateways.

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

Note: If the source BlackPearl gateway uses object versioning but the target BlackPearl 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.

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

1. From the menu bar, select **Configuration > Advanced Bucket Management > Replication Targets** to display the Replication Targets screen.



BlackPearl Targets

Name	Data Path End Point	State	Standby
There are currently no items to display			

Amazon S3 Targets

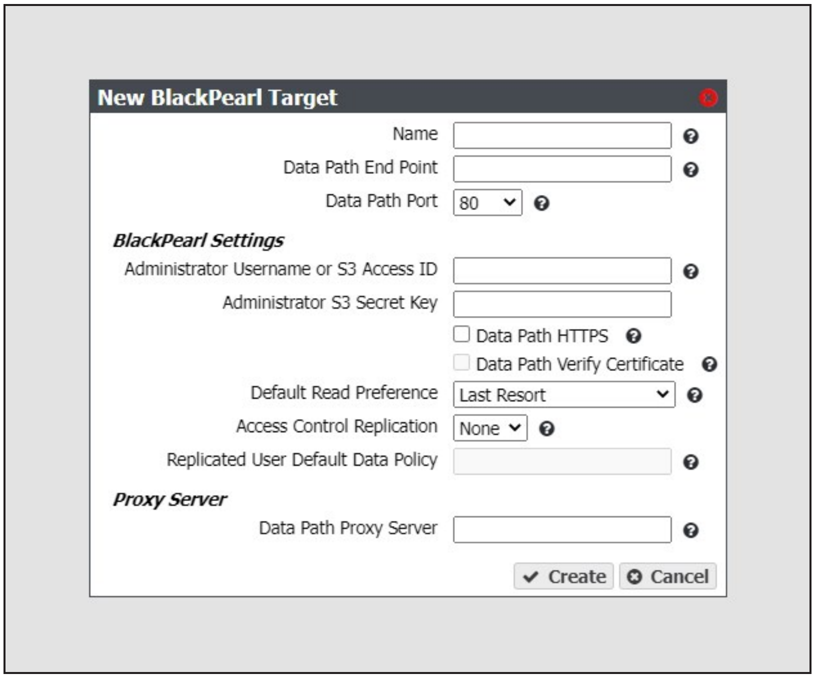
Name	Data Path End Point	Region	State	Standby
aws		US_WEST_2	Online	No

Microsoft Azure Targets

Name	Account Name	State	Standby
azure	spectradvt	Online	Yes

Figure 44 The Replication Targets screen

2. Select **Action > New BlackPearl Target**. The New BlackPearl Target dialog box displays.


New BlackPearl Target

Name

Data Path End Point

Data Path Port: 80

BlackPearl Settings

Administrator Username or S3 Access ID

Administrator S3 Secret Key

☐ Data Path HTTPS

☐ Data Path Verify Certificate

Default Read Preference: Last Resort

Access Control Replication: None

Replicated User Default Data Policy

Proxy Server

Data Path Proxy Server

Figure 45 The New BlackPearl Target dialog box.

3. Enter a name for the BlackPearl target in the **Name** field.

4. 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.

5. Using the drop-down menu, select a value for the **Data Path Port**. Set this to the value of the port on which the target gateway's S3 service is running.

Note: Port selections for secure transfer (443/8443) are grayed-out and not able to be selected until you select Data Path HTTPS in Step 8 below.

6. 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.

7. In the **Administrator S3 Secret Key** field, enter the S3 Secret Key of the user you entered in Step 6.

8. Select **Data Path HTTPS** 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 5 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.

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.

9. If you enabled Data Path HTTPS, you can optionally select **Data Path Verify Certificate** to verify the SSL certificate of the BlackPearl target. This option is not available if you did not enable Data Path HTTPS.

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

10. Using the drop-down menu, select a value for the **Default Read Preference**. Data is normally read from the source gateway whenever possible. This setting determines from what location data is read back from the target gateway, if needed.

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 whether 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-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 gateway.

11. Using the drop-down menu, select a value for **Access Control Replication**.

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 gateways must be identical when setting Access Control Replication to **None**.
Users	User creation, modification, and deletion is replicated to the BlackPearl target.

12. If you selected Users in Step 11, 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.

13. 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.

14. Click **Create**. The new BlackPearl target appears on the Advanced Bucket Management screen.

Create an Amazon S3 Target

Configuring an Amazon S3 target allows a data policy on the BlackPearl 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

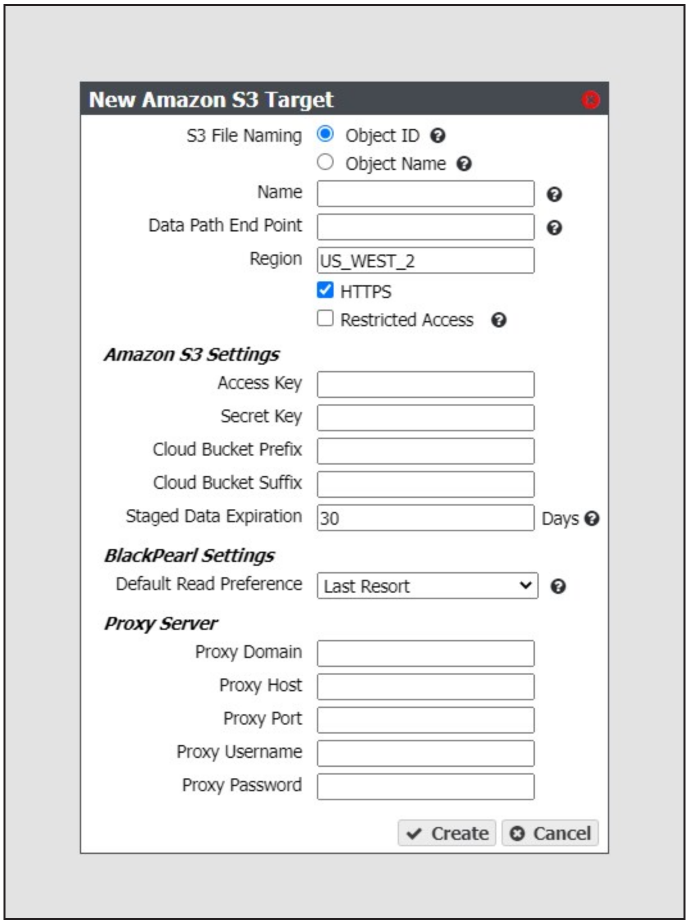
The following restrictions apply to creating an Amazon S3 target:

- 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. From the menu bar, select **Configuration > Advanced Bucket Management > Replication Targets** to display the Replication Targets screen (see Figure 44 on page 140).

2. Select **Action > New Amazon S3 Target**. The New Amazon S3 Target dialog box displays.



New Amazon S3 Target

S3 File Naming ● Object ID ○ Object Name

Name

Data Path End Point

Region US_WEST_2

☑ HTTPS

☐ Restricted Access

Amazon S3 Settings

Access Key

Secret Key

Cloud Bucket Prefix

Cloud Bucket Suffix

Staged Data Expiration 30 Days

BlackPearl Settings

Default Read Preference Last Resort

Proxy Server

Proxy Domain

Proxy Host

Proxy Port

Proxy Username

Proxy Password

Figure 46 The New Amazon S3 Target dialog box.

3. Select the type of **S3 File Naming** to use for the target.

- **Object ID** - objects display a UUID when viewed on the Amazon target.
- **Object Name** - objects display their name when viewed on the Amazon target.

4. Enter a name for the Amazon S3 target in the **Name** field.

5. 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
- us_east_2
- us_west_1
- us_west_2
- eu_west_1
- eu_west_2
- eu_central_1
- ap_south_1
- ap_southeast_1
- ap_southeast_2
- ap_northeast_1
- ap_northeast_2
- sa_east_1
- cn_north_1
- ca_central_1
- gov_cloud

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.

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

7. 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 gateway uses to confirm valid credentials when a data path endpoint and region are entered in Step 5.

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

8. Enter the S3 Access Key of a user with administrator privileges for the Amazon S3 account in the **Access Key** field.

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

9. In the **Secret Key** field, enter the S3 Secret Key of the user you entered in Step 8.

10. Optionally, enter a **Cloud Bucket Prefix** and/or **Cloud Bucket Suffix**. Bucket names on the BlackPearl 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 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.

11. 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 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.

12. Using the drop-down menu, select a value for the **Default Read Preference**. 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.

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.
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.

13. 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.

14. Click **Create**. The new Amazon S3 target appears on the Replication Targets screen.

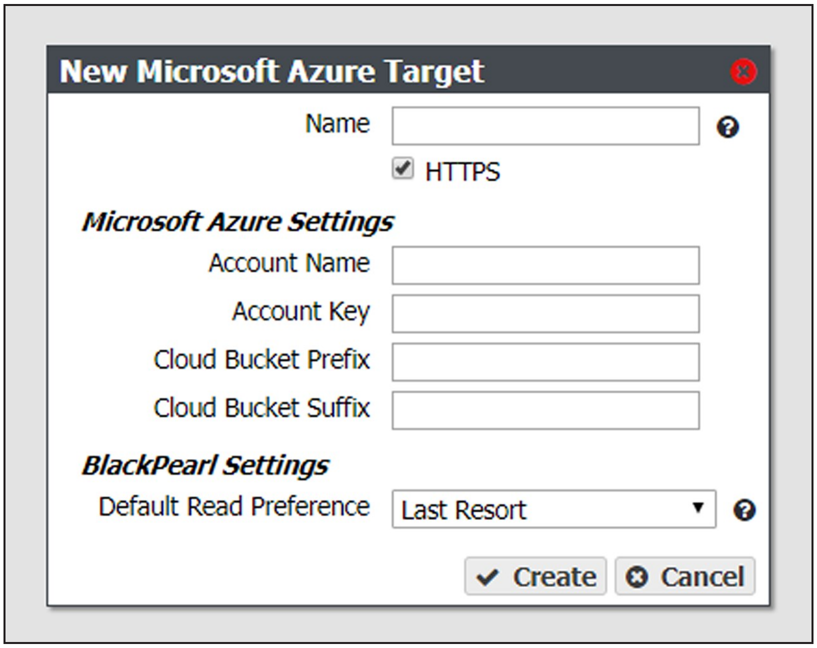
Create a Microsoft Azure Target

Configuring a Microsoft Azure target allows a data policy on the BlackPearl 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. From the menu bar, select **Configuration > Advanced Bucket Management > Replication Targets** to display the Replication Targets screen(see Figure 44 on page 140).

2. Select **Action > New Microsoft Azure Target**. The New Microsoft Azure Target dialog box displays.



New Microsoft 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 47 The New Microsoft Azure Target dialog box.

3. Enter a name for the Microsoft Azure target in the **Name** field.

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

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

6. In the **Account Key** field, enter the account key associated with the account entered in Step 5.
7. Optionally, enter a **Cloud Bucket Prefix** and/or **Cloud Bucket Suffix**. Bucket names on the BlackPearl 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 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.

8. Using the drop-down menu, select a value for the **Default Read Preference**. 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 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.
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.

9. Click **Create**. The new Microsoft Azure target appears on the Replication Targets screen.

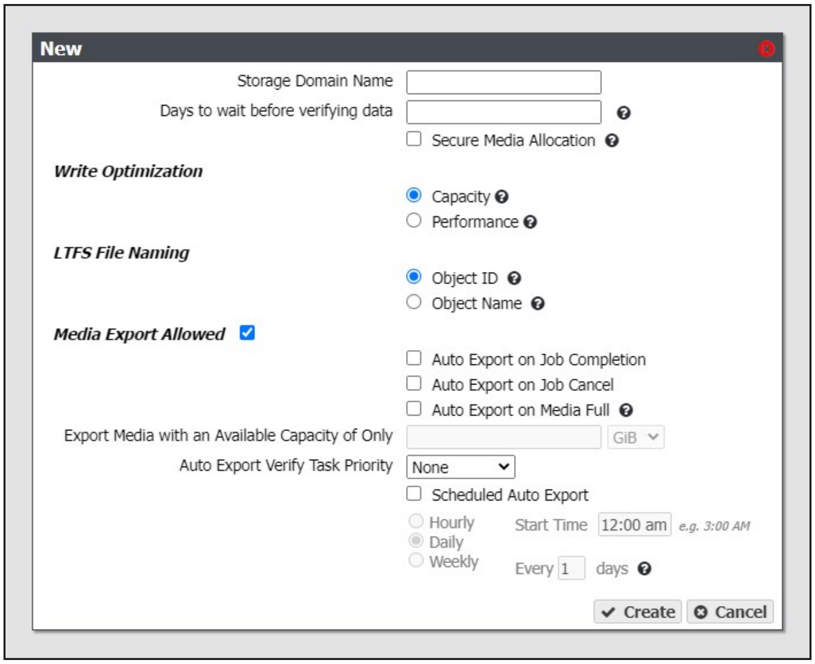
CREATE A STORAGE DOMAIN

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 Nearline 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 is allocated out of the members to fulfill the capacity requirement.

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

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Select **Action > New Storage Domain**. The New Storage Domain dialog box displays.



New

Storage Domain Name

Days to wait before verifying data

□ Secure Media Allocation

Write Optimization

● Capacity

○ Performance

LTFS File Naming

● Object ID

○ Object Name

Media Export Allowed ☑

□ Auto Export on Job Completion

□ Auto Export on Job Cancel

□ Auto Export on Media Full

Export Media with an Available Capacity of Only GiB

Auto Export Verify Task Priority None

□ Scheduled Auto Export

○ Hourly
● Daily
○ Weekly

Start Time 12:00 am *e.g. 3:00 AM*

Every 1 days

Figure 48 The New Storage Domain dialog box.

3. Enter a name for the storage domain in the **Storage Domain Name** field.

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 the DS3 Service on page 292.
- 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 467 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 465 for more information.

5. Select or clear **Secure Media Allocation**. If enabled, Secure Media Allocation 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.

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. Select the **Write Optimization** for the storage domain. This setting specifies whether job chunks are written as quickly as possible or across as few pieces of media as possible.

   The BlackPearl 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 gateway aggregates smaller jobs or smaller chunks into a size of approximately 128 GB for each tape drive read or write task.

   When running in **Capacity** mode, the BlackPearl 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.

   When running in **Performance** mode, the BlackPearl 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.

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

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

For more information on capacity and performance modes, see Capacity Mode versus Performance Mode on page 516.

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 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.

7. Select the **LTFS File Name** option for the storage domain.

Note: This setting only applies to tape media. If the storage domain includes tape partition(s), you must specify the **LTFS File Name** option for the storage domain. This option specifies how the gateway names the file when it writes them to tape.

There are two options for the **LTFS File 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 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.

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.

- **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.

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.

8. Optionally, select the **Media Export Allowed** check box to enable tape media export options for the storage domain. Clear the check box to disallow tape media export for the storage domain. This setting only applies to tape media. See Tape Export Best Practices on page 99 for more information.

   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.

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.

Note: It is important to not export tape media from the library directly. The BlackPearl Nearline gateway controls the movement of media in the library.

If you select to allow media export, configure the following options:

a. Select or clear options for auto media export.

- **Auto Export on Job Completion** — select 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 Nearline gateway.
- **Auto Export on Job Cancel** — select 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** — select 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.

Note: If you select for media to automatically export when the media is full, you can optionally configure the **Export Media with an Available Capacity of Only** setting, which determines when the gateway marks a piece of media as full, and queues the piece of media for export. Select the desired unit size from the drop-down menu and enter a numerical value for the media full threshold in the text box to the left of the unit size drop-down menu.

b. Using the **Auto Export Verify Task Priority** drop-down menu, 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.

c. Select or clear the **Scheduled Auto Export** check box. If enabled, this option 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 capacity of storage remaining on the tape cartridges. Use the instructions below to configure either hourly, daily, or weekly, automatic tape export.

Note: **Scheduled Auto Export** operates independently from the condition-based auto export options discussed in Step a on page 154.

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.

Create an Hourly Schedule

i. Select **Hourly** as the interval for the tape export schedule (see Figure 48 on page 150).

ii. Enter numbers for **Every _ hours on minute _**. These values specify the interval in hours between tape exports and the number of minutes after the top of the hour when the export starts. For example, if the values are set to 4 and 15, tapes are exported every four hours at 15 minutes after the hour. The maximum setting for the **hours** field is 48, where tapes are exported every two days.

Note: Spectra Logic recommends offsetting the minutes after the hour for starting tape exports so that there are not a large number of jobs starting at exactly the same time.

Create a Daily Schedule

i. Select **Daily** as the interval for the tape export schedule (see Figure 48 on page 150).

ii. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.

iii. Enter a number for **Every _ days**. Allowed values are between 1 and 31. This value specifies the interval, in days, between scheduled exports. The value entered is enumerated from the first day of the month. The schedule resets at the beginning of each month. For example, if this value is set to 2, scheduled tape exports occur every two days, starting with the 1st of the month, at the time specified in Step ii. A value of 30 runs on the 1st of the month, and then again on the 31st of the month (for months that have 31 days). To schedule exports on the first of every month, set the interval to 31 days.

Create a Weekly Schedule

i. Select **Weekly** as the interval for the tape export schedule (see Figure 48 on page 150).

ii. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.

iii. Select one or more days for **Every week on:**. This determines the day(s) of each week the gateway exports tapes.

9. Click **Create**. The new storage domain displays on the Advanced Bucket Management screen.

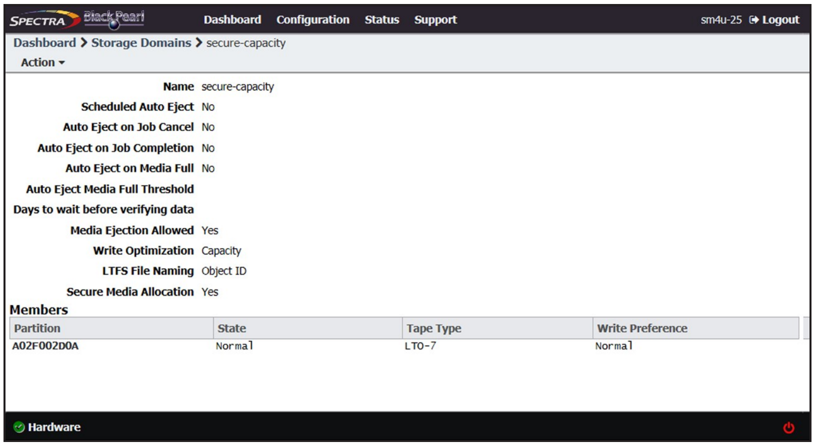
Add a Storage Domain Member to a Storage Domain

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. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).

2. Double-click the storage domain for which you want to add a new storage domain member in the Storage Domains pane, or select the storage domain and select **Action > Show Details** from the menu bar. The Storage Domain details screen displays.



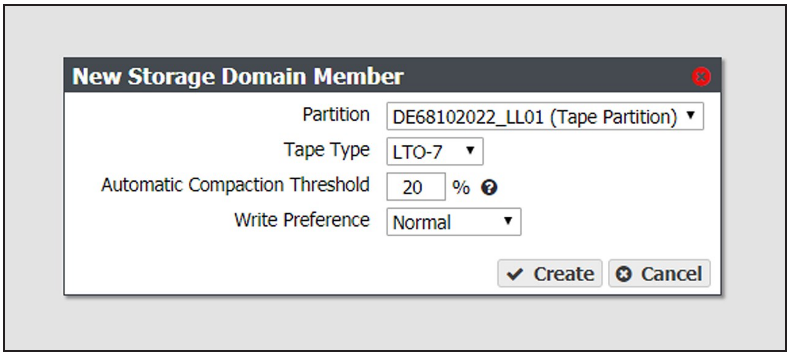
Name	secure-capacity
Scheduled Auto Eject	No
Auto Eject on Job Cancel	No
Auto Eject on Job Completion	No
Auto Eject on Media Full	No
Auto Eject Media Full Threshold	
Days to wait before verifying data	
Media Ejection Allowed	Yes
Write Optimization	Capacity
LTFS File Naming	Object ID
Secure Media Allocation	Yes

Members

Partition	State	Tape Type	Write Preference
A02F002D0A	Normal	LTO-7	Normal

Figure 49 The Storage Domain details screen.

3. Select **Action > New Storage Domain Member**. The New Storage Domain Member dialog box displays.



Partition	DE68102022_LL01 (Tape Partition) ▾
Tape Type	LTO-7 ▾
Automatic Compaction Threshold	20 %
Write Preference	Normal ▾

Figure 50 The New 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 version.
- This option does not display if you selected a disk partition in Step 4 on page 157.

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 on page 157, 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.

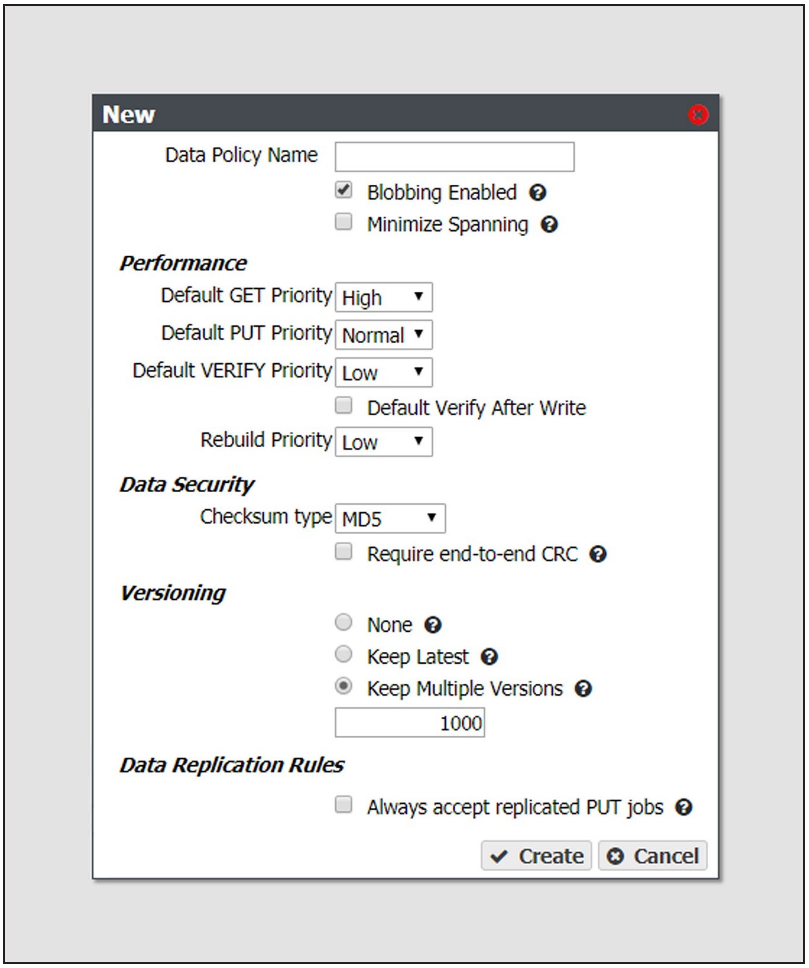
8. Click **Create**. The new storage domain member displays on the Storage Domain details screen.

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.

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

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Select **Action > New Data Policy**. The New Data Policy dialog box displays.



New

Data Policy Name

☑ Blobbing Enabled

□ Minimize Spanning

Performance

Default GET Priority: High

Default PUT Priority: Normal

Default VERIFY Priority: Low

□ Default Verify After Write

Rebuild Priority: Low

Data Security

Checksum type: MD5

□ Require end-to-end CRC

Versioning

○ None

○ Keep Latest

● Keep Multiple Versions

1000

Data Replication Rules

□ Always accept replicated PUT jobs

Figure 51 The New Data Policy dialog box.

3. Enter a name for the data policy in the **Data Policy Name** field.

4. Select or clear the **Blobbing Enabled** check box. When enabled this setting allows an object to be broken into multiple blobs. If disabled, an object must be exactly one blob. 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.

Note: Disabling blobbing guarantees that an object will never span multiple tapes or disk pools, since a blob cannot span multiple media.

5. Select or clear the **Minimize Spanning** check box. When enabled, this setting minimizes the spanning of data across multiple tapes or pools. Jobs less than 1 TB never span media.

Notes:

- When "Minimize Spanning" is enabled, it overrides a storage domain's 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.
- Enabling this option can adversely affect capacity utilization and performance.

6. Select the **Performance** characteristics for the data policy. Each priority determines the resources assigned and the processing order. 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**.
    d. Select or clear **Default Verify After Write**. Clients may specify whether or not to verify data immediately after writes when creating a PUT job. If the client does not specify a policy for verification of data after writes, this selection determines whether a verify is done. If done, the verification uses the checksum type specified in Step 7 on page 161.

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.
- This verification does not update the **Last Verified** field on the tape details screen.
- Selecting **Default Verify After Write** reduces gateway write throughput by up to 50%.
- This setting does not apply to replication targets.

    e. Use the drop-down menu to select the **Rebuild Priority**.

7. Select the **Data Security** options for the data policy.

   a. Use the drop-down menu to select the **Checksum type**. This setting specifies the type of checksum used to verify data integrity for data in any bucket using this data policy, and the type of checksum required for end-to-end CRC, if specified.

Notes:

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

   b. If you want to enable end-to-end security for each GET or PUT job, select the **Require end-to-end CRC** check box.

8. Select the type of **Versioning** you want to use for the data policy. You must select either **None**, **Keep Latest**, or **Keep Multiple Versions**.

IMPORTANT If you select **Keep Multiple Versions**, you are not able to change this setting after the data policy is created.

IMPORTANT If you select **Keep Multiple Versions**, you are not able to change this setting after the data policy is created.

- **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.
- **Keep Multiple Versions** (*default*)—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, are retained and accessible. The default value of 1000 is pre-entered.

Notes:

- You cannot assign a Storage Domain configured with the LTFS option set to **Object Name** when using the **Keep Latest** or **Keep Multiple Versions** setting. See Create a Storage Domain on page 150 for more information.
- 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.

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.

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 BlackPearl gateway believes the latest version to be the same object as the earlier version and rejects it, and only the earlier version is retained.

9. If you plan to configure a data replication target, select or clear the **Always accept replicated PUT jobs** check box. This option controls whether all PUT jobs for this data policy are created even if one or more replication targets the gateway must PUT to are unavailable, or if there are global issues that would likely prevent the completion of the job.

Note: 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.

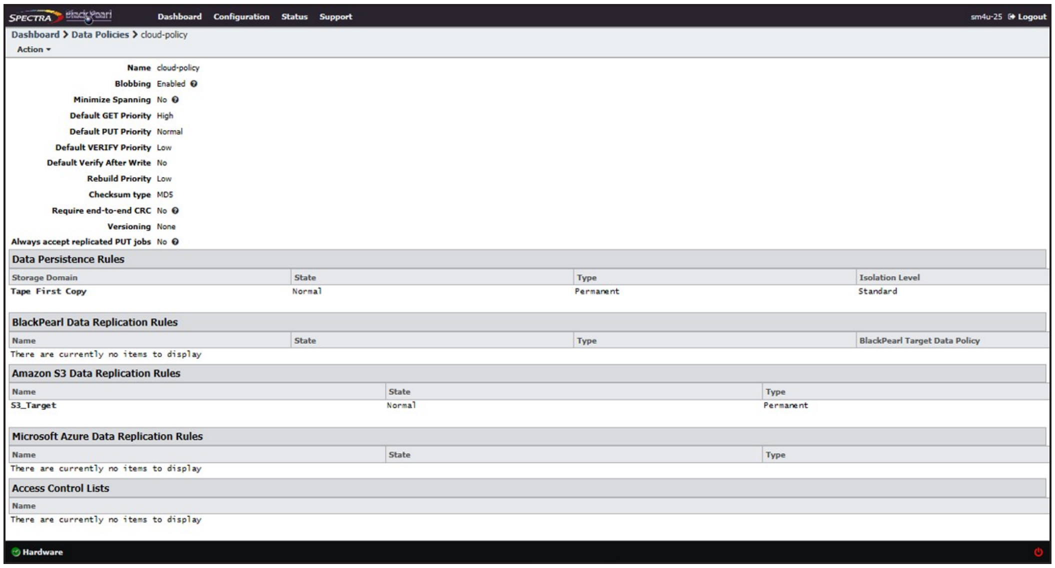
10. Click **Create**. The new data policy displays on the Advanced Bucket Management screen.

Add Data Persistence Rules and Replication Rules to a Data Policy

Once a data policy is created, you must add 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. 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. A data policy must include at least one permanent persistence rule.

Add a Data Persistence Rule to a Data Policy

1. If necessary, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Double-click the data policy in the Data Policies pane, or select the data policy and select **Action > Show Details** from the menu bar. The Data Policy details screen displays.



Name	cloud-policy
Blobbing	Enabled
Minimize Spanning	No
Default GET Priority	High
Default PUT Priority	Normal
Default VERIFY Priority	Low
Default Verify After Write	No
Rebuild Priority	Low
Checksum type	MD5
Require end-to-end CRC	No
Versioning	None
Always accept replicated PUT jobs	No

Data Persistence Rules

Storage Domain	State	Type	Isolation Level
Tape First Copy	Normal	Permanent	Standard

BlackPearl Data Replication Rules

Name	State	Type	BlackPearl Target Data Policy
There are currently no items to display			

Amazon S3 Data Replication Rules

Name	State	Type
S3_Target	Normal	Permanent

Microsoft Azure Data Replication Rules

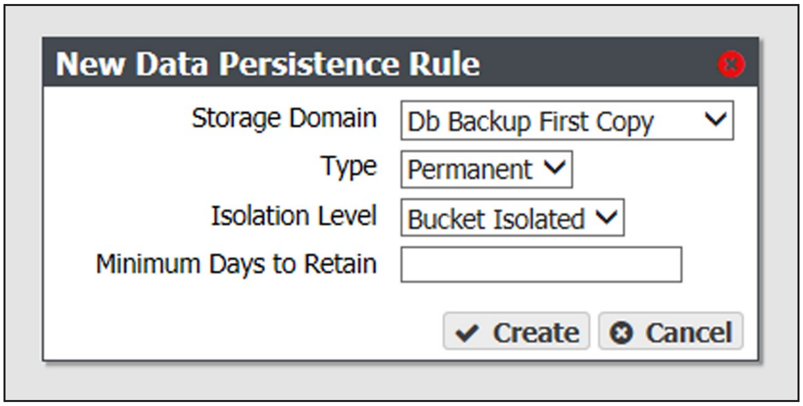
Name	State	Type
There are currently no items to display		

Access Control Lists

Name
There are currently no items to display

Figure 52 The Data Policy details screen.

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



New Data Persistence Rule

Storage Domain: Db Backup First Copy

Type: Permanent

Isolation Level: Bucket Isolated

Minimum Days to Retain:

Figure 53 The New 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 512 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 Edit a Data Persistence Rule on page 195.

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** in the entry field to specify the minimum number of days the gateway should retain data written using a temporary persistence rule.

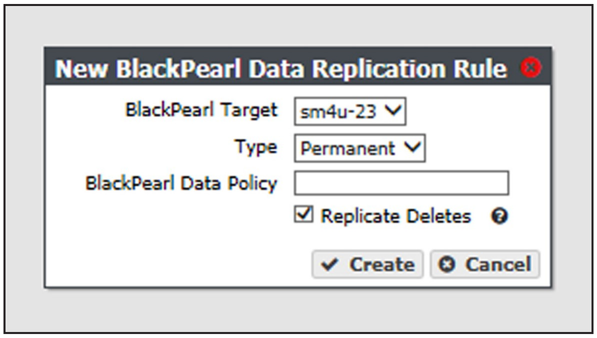
Notes:
- The **Minimum Days to Retain** for a persistence rule targeting a storage domain using a nearline pool (a 77-bay, 96-bay, or 107-bay expansion node) must be 90 days or greater.
- **Minimum Days to Retain** cannot be specified when using a **Type** of **Permanent**.

8. Click **Create**. The new data persistence rule displays on the Data Policy details screen.

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 BlackPearl Target on page 139.

1. If necessary, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Double-click the data policy in the Data Policies pane, or select the data policy and select **Action > Show Details** from the menu bar. The Data Policy details screen displays (see Figure 52 on page 163).
3. Select **Action > New BlackPearl Data Replication Rule**. The New BlackPearl Data Replication Rule dialog box displays.



New BlackPearl Data Replication Rule

BlackPearl Target: sm4u-23

Type: Permanent

BlackPearl Data Policy:

☑ Replicate Deletes

Figure 54 The New BlackPearl Data Replication Rule dialog box.

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

6. In the **BlackPearl Data Policy** entry field, enter the name of the data policy on the target BlackPearl gateway to use when creating the bucket for replicated data. Alternatively, you can leave the field blank.

Notes:
- The data policy name is case sensitive.
- If the field is left blank and the BlackPearl target was configured with the setting "Replicated User Default Data Policy" enabled, and Access Control Replication was set to "Users", the default data policy on the target gateway is used. If no default is set on the target gateway and the target gateway is configured with more than one data policy, the replication fails.

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

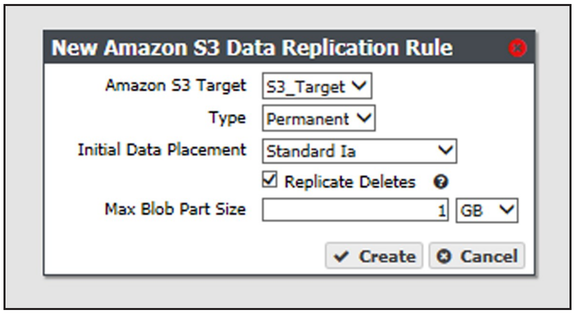
Note: Replicated objects do not immediately delete. Objects are only deleted after running a verify operation on the bucket.

8. Click **Create**. The new BlackPearl data replication rule displays on the Data Policy details screen.

Add an Amazon 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 an Amazon S3 Target on page 143.

1. If necessary, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Double-click the data policy in the Data Policies pane, or select the data policy and select **Action > Show Details** from the menu bar. The Data Policy details screen displays (see Figure 52 on page 163).
3. Select **Action > New Amazon S3 Data Replication Rule**. The New Amazon S3 Data Persistence Rule dialog box displays.



New Amazon S3 Data Replication Rule

Amazon S3 Target: S3_Target

Type: Permanent

Initial Data Placement: Standard Ia

☑ Replicate Deletes

Max Blob Part Size: 1 GB

Figure 55 The New Amazon S3 Data Replication Rule dialog box.

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

5. Use the **Type** drop-down menu to select whether the data persistence rule to use for the for the replication target 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.

6. Use the **Initial Data Placement** drop-down menu to select the storage class for any objects transferred to the AWS S3 instance. See *Storage Classes* for detailed descriptions of the storage classes provided by AWS.

Note: The BlackPearl gateway 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.

- **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.

Note: 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.

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

8. 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 size is 1 GB.

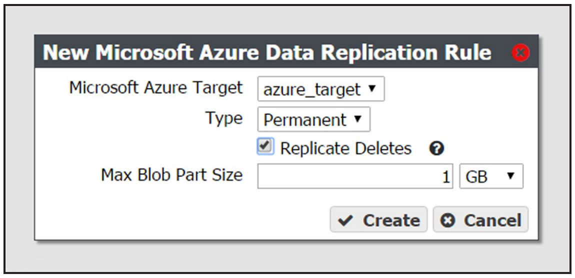
Note: To prevent data transfer failures, it is important that this value not exceed the maximum blob size that the target is able to accept.

9. Click **Create**. The new Amazon S3 replication rule displays on the Data Policy details screen.

Add a Microsoft Azure Data Replication Rule to a Data Policy

A Microsoft Azure replication target must be configured before adding an Microsoft Azure Data Replication Rule to the data policy. See Create a Microsoft Azure Target on page 147.

1. If necessary, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Double-click the data policy in the Data Policies pane, or select the data policy and select **Action > Show Details** from the menu bar. The Data Policy details screen displays (see Figure 52 on page 163).
3. Select **Action > New Microsoft Azure Data Replication Rule**. The New Microsoft Azure Data Replication Rule dialog box displays.



New Microsoft Azure Data Replication Rule

Microsoft Azure Target: azure_target

Type: Permanent

☑ Replicate Deletes

Max Blob Part Size: 1 GB

Figure 56 The New Microsoft Azure Data Replication Rule dialog box.

4. Use the **Microsoft Azure Target** drop-down menu to select a Microsoft Azure replication target from the list of previously created replication targets.
5. Use the **Type** drop-down menu to select whether the data persistence rule to use for the for the replication target 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.

6. Select or clear the **Replicate Deletes** check box. 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.

7. 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 GB.

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.

8. Click **Create**. The new Microsoft Azure replication rule displays on the Data Policy details screen.

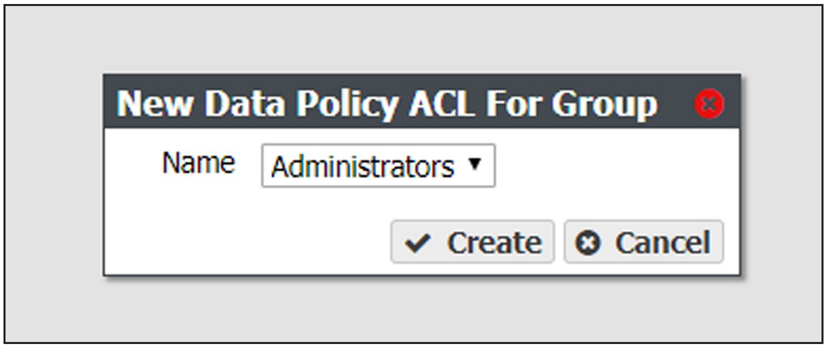
Create Data Policy ACLs

The sections below describe creating Access Control List (ACL) for both a group of user and an individual user.

New Data Policy ACL for a Group

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

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Select the row for the data policy for which you want to create a new ACL for a group, then select **Action > Show Details**. The Data Policy details screen displays.
3. From the menu bar, select **Action > New Data Policy ACL For Group**. The New Data Policy ACL For Group dialog box displays.


New Data Policy ACL For Group

Name: Administrators ▼

Figure 57 The New Data Policy ACL For Group dialog box.

4. Using the **Name** drop-down menu, select the group to be assigned to the data policy ACL.
5. Click **Create**.

New Data Policy ACL for a User

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

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).

2. Select the row for the data policy for which you want to create a new ACL for a user, then select **Action > Show Details**. The Data Policy details screen displays.
3. From the menu bar, select **Action > New Data Policy ACL For User**. The New Data Policy ACL For User dialog box displays.

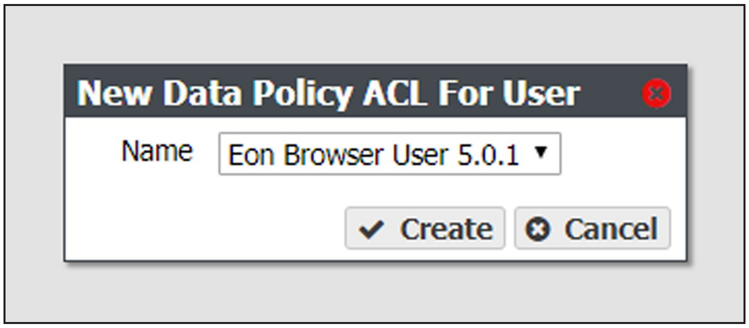


Figure 58 The New Data Policy ACL For User dialog box.

4. Using the **Name** drop-down menu, select the user to be assigned to the data policy ACL.
5. Click **Create**.

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*.

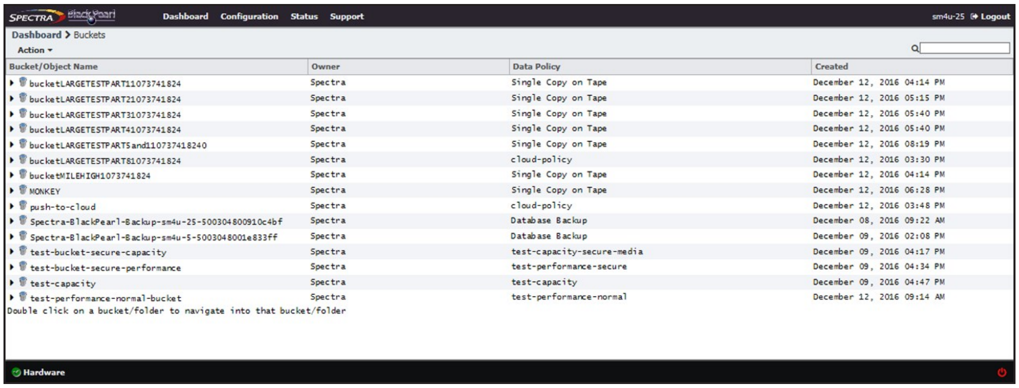
Note: Buckets can also be created using a DS3 client, or the DS3 API.

IMPORTANT If you are creating a bucket that is 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.

IMPORTANT If you are creating a bucket that is 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. From the menu bar, select **Configuration > Buckets**. The Buckets screen displays.

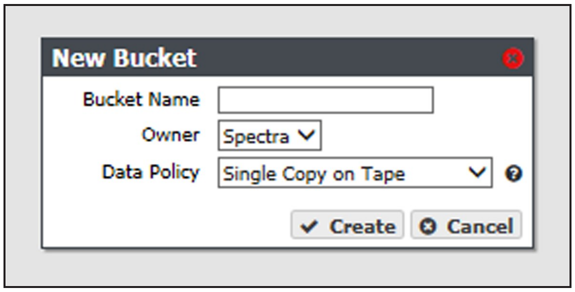


Bucket/Object Name	Owner	Data Policy	Created
bucketLARGETESTPART11073741824	Spectra	Single Copy on Tape	December 12, 2016 04:14 PM
bucketLARGETESTPART21073741824	Spectra	Single Copy on Tape	December 12, 2016 05:15 PM
bucketLARGETESTPART31073741824	Spectra	Single Copy on Tape	December 12, 2016 05:40 PM
bucketLARGETESTPART41073741824	Spectra	Single Copy on Tape	December 12, 2016 05:40 PM
bucketLARGETESTPART5and110737418240	Spectra	Single Copy on Tape	December 12, 2016 08:19 PM
bucketLARGETESTPART81073741824	Spectra	cloud-policy	December 12, 2016 03:30 PM
bucketMILEHIGH1073741824	Spectra	Single Copy on Tape	December 12, 2016 04:14 PM
MONKEY	Spectra	Single Copy on Tape	December 12, 2016 06:28 PM
push-to-cloud	Spectra	cloud-policy	December 12, 2016 03:48 PM
Spectra-BlackPearl-Backup-sm4u-25-500304800910c4bf	Spectra	Database Backup	December 08, 2016 09:22 AM
Spectra-BlackPearl-Backup-sm4u-5-5003048001e833ff	Spectra	Database Backup	December 09, 2016 02:08 PM
test-bucket-secure-capacity	Spectra	test-capacity-secure-media	December 09, 2016 04:17 PM
test-bucket-secure-performance	Spectra	test-performance-secure	December 09, 2016 04:34 PM
test-capacity	Spectra	test-capacity	December 09, 2016 04:47 PM
test-performance-normal-bucket	Spectra	test-performance-normal	December 12, 2016 09:14 AM

Double click on a bucket/folder to navigate into that bucket/folder

Figure 59 The Buckets screen.

2. Select **Action > New** from the menu bar. The New Bucket dialog box displays.



New Bucket

Bucket Name

Owner: Spectra

Data Policy: Single Copy on Tape

Figure 60 The New Bucket dialog box.

3. Enter a name for the bucket in the **Bucket Name** field.

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.

- For **BlackPearl OS 3.5.2 or earlier**, the BlackPearlgateway 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 causing possible data collision and bucket ownership/permission problems.
- For **BlackPearl OS 4.0 or later,** if the bucket name is incompatible with the naming requirements of the cloud target provider, bucket creation fails and an error message displays.

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 BlackPearl gateway 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.

- For **BlackPearl OS 3.5.2 or earlier**, the BlackPearl gateway 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 causing possible data collision and bucket ownership/permission problems.
- For **BlackPearl OS 4.0 or later,** if the bucket name is incompatible with the naming requirements of the cloud target provider, bucket creation fails and an error message displays.

Notes:

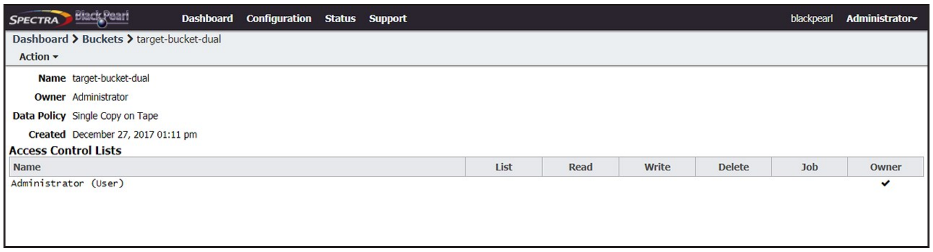
- The bucket name cannot contain a colon (:), forward slash (/), or space.
- The bucket name cannot exceed 255 characters.

4. Using the drop-down menu, select an **Owner** for the bucket from the list of users already created on the gateway.
5. Using the drop-down menu, 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 **Create**. The Buckets screen displays with the newly created bucket listed.

Create a New Bucket ACL for a Group

Use the instructions in this section to create a new Access Control List (ACL) using the specified group for a bucket.

1. From the menu bar, select **Configuration > Buckets**. The Buckets screen displays (see Figure 59 on page 171).
2. Select the bucket for which you want to create an ACL and select **Action > Show Details**. The bucket details screen displays.



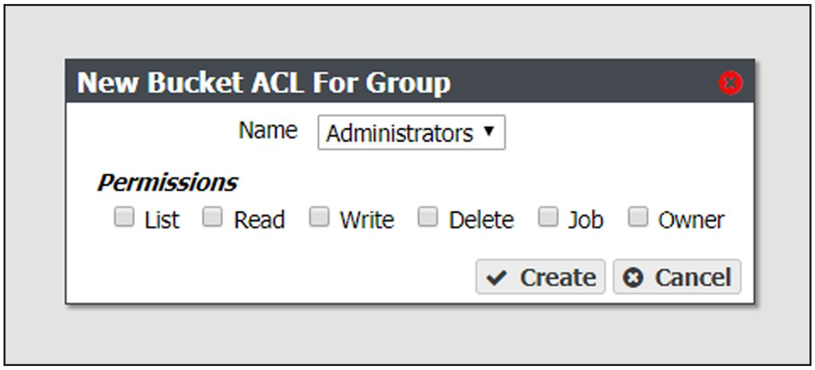
Name target-bucket-dual
Owner Administrator
Data Policy Single Copy on Tape
Created December 27, 2017 01:11 pm

Access Control Lists

Name	List	Read	Write	Delete	Job	Owner
Administrator (User)						✓

Figure 61 The bucket details screen.

3. Select **Action > New Bucket ACL For Group**. The New Bucket ACL For Group dialog box displays.



Name Administrators ▾

Permissions

□ List □ Read □ Write □ Delete □ Job □ Owner

Figure 62 The New Bucket ACL For Group dialog box.

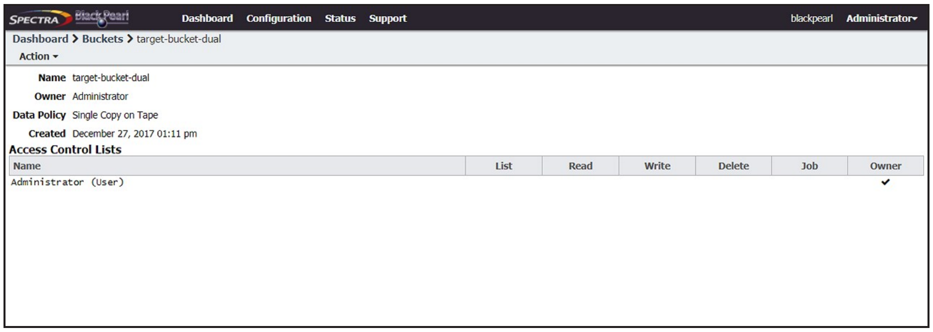
4. Using the **Name** drop-down list, select a group from the list of exiting S3 groups on the BlackPearl gateway.

5. Select the desired **Permissions** for the group ACL.
   - **LIST** — The users in the group can see the bucket in a get buckets request and can list the objects in a bucket. The users can also perform any type of bucket or object get that does not involve returning the actual data for an object.
   - **READ** — The users can get objects and create GET jobs.
   - **WRITE** — The users can put objects and create PUT jobs.
   - **DELETE** — The users can delete objects, but cannot delete the bucket.
   - **JOB** — The group members can modify or cancel jobs that they did not create. The users can also see the details of jobs they did not create. Note that 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 users receives full access to the bucket, including all permissions listed above, and also receives permission to modify bucket ACLs for that bucket.
6. Click **Create**.

Create a New Bucket ACL for a User

Use the instructions in this section to create a new Access Control List (ACL) using the specified user for a bucket.

1. From the menu bar, select **Configuration > Buckets**. The Buckets screen displays (see Figure 59 on page 171).
2. Select the bucket for which you want to create an ACL and select **Action > Show Details**. The bucket details screen displays.



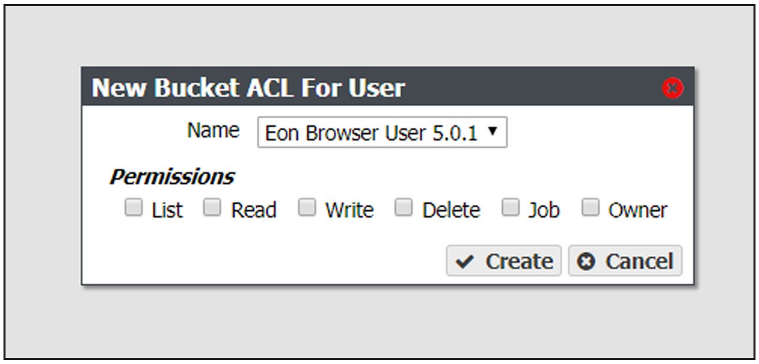
Name target-bucket-dual
Owner Administrator
Data Policy Single Copy on Tape
Created December 27, 2017 01:11 pm

Access Control Lists

Name	List	Read	Write	Delete	Job	Owner
Administrator (User)						✓

Figure 63 The bucket details screen.

3. Select **Action > New Bucket ACL For User**. The New Bucket ACL For User dialog box displays.



New Bucket ACL For User

Name: Eon Browser User 5.0.1

Permissions

□ List □ Read □ Write □ Delete □ Job □ Owner

Figure 64 The New Bucket ACL For User dialog box.

4. Using the **Name** drop-down list, select a user from the list of exiting users on the BlackPearl gateway.

5. Select the desired **Permissions** for the user ACL.

- **LIST** — The user can see the bucket in a get buckets request and can list the objects in a bucket. The user can also perform any type of bucket or object get that does not involve returning the actual data for an object.
- **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 that they did not create. The user can also see the details of jobs they did not create. Note that 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 the bucket, including all permissions listed above, and also receives permission to modify bucket ACLs for that bucket.

6. Click **Create**.

TRANSFER DATA

After completing the above sections of this chapter, you are ready to begin transferring data to, and from, the BlackPearl gateway.

- To transfer data using the EON Browser, consult the *EON Browser User Guide*.
- To transfer data using the Spectra RioBroker® application, consult the *Spectra RioBroker User Guide*.
- To transfer data using the Spectra StorCycle® application, consult the *Spectra StorCycle User Guide*.
- To transfer data using a DS3 client, consult the *Spectra BlackPearl DS3 API Reference*, and documentation specific to each DS3 client.

IMPORTANT Contact Spectra Logic Professional Services for assistance in setting up data transfer. See Contacting Spectra Logic on page 9.

IMPORTANT The Spectra BlackPearlgateway limits the number of simultaneous active jobs. The number of simultaneous jobs differs depending on the software installed on the BlackPearlgateway.

- BlackPearl OS 3.x is limited to 1,000 simultaneous active jobs.
- BlackPearl OS 4.x is limited to 1,000 simultaneous active jobs.
- BlackPearl OS 5.x is limited to 10,000 simultaneous active jobs.

IMPORTANT Contact Spectra Logic Professional Services for assistance in setting up data transfer. See Contacting Spectra Logic on page 9.

IMPORTANT The Spectra BlackPearl gateway limits the number of simultaneous active jobs. The number of simultaneous jobs differs depending on the software installed on the BlackPearl gateway.

- BlackPearl OS 3.x is limited to 1,000 simultaneous active jobs.
- BlackPearl OS 4.x is limited to 1,000 simultaneous active jobs.
- BlackPearl OS 5.x is limited to 10,000 simultaneous active jobs.

Chapter 5 - Managing Advanced Bucket Management Settings

This chapter describes using the BlackPearl user interface to manage storage domains, data policies, disk partitions, and buckets on the gateway after configuring Advanced Bucket Management. For initial Advanced Bucket Management configuration steps, see Configuring Advanced Bucket Management on page 128.

Manage Buckets **179**

Show Bucket Physical Placement 179

Edit a Bucket ACL 179

Delete a Bucket ACL 180

Edit a Bucket 180

Delete a Bucket 182

Manage a Storage Domain **183**

Edit a Storage Domain Member 183

Exclude a Storage Domain Member 184

Cancel Storage Domain Member Exclusion 185

Delete a Storage Domain Member 185

Edit a Storage Domain 186

Delete a Storage Domain 187

Manage Data Replication Rules **189**

Edit a BlackPearl Data Replication Rule 189

Edit an Amazon S3 Data Replication Rule 190

Edit a Microsoft Azure Data Replication Rule 191

Delete a Data Replication Rule 192

Manage a Data Policy **193**

Edit a Data Policy 193

Delete a Data Policy 194

Delete a Data Policy ACL 195

Edit a Data Persistence Rule 195

Delete a Data Persistence Rule 197

Manage Replication Targets **198**

Edit a BlackPearl Replication Target 198
Edit an Amazon Replication Target 199
Edit an Azure Replication Target 200
Verify a Replication Target 200
Put a Replication Target in Standby State 201
Activate a Replication Target 202
Delete a Replication Target 203
Manage a Disk Partition 204
Edit a Disk Partition 204
Delete a Disk Partition 205
Manage Online and Nearline Disk Pools 206
Import a Nearline or Online Disk Pool 206
Delete a Nearline or Online Disk Pool 207
Change the BlackPearl Gateway Cache Configuration 209

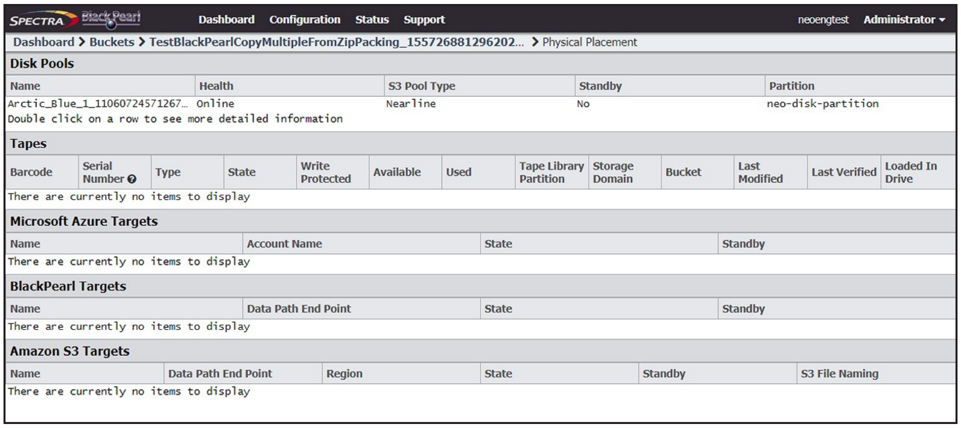
Manage Buckets

Use the instructions in this section to configure ACLs for a bucket, edit, or delete a bucket. For instructions on creating a new bucket, see Create a Bucket on page 171.

Show Bucket Physical Placement

Once data is transferred to the BlackPearl 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. From the menu bar, select **Configuration > Buckets**. The Buckets screen displays (see Figure 59 on page 171).
2. Select the bucket for which you want to view physical placement and select **Action > Show Physical Placement**. The *Bucket* Physical Placement screen displays.



Dashboard > Buckets > TestBlackPearlCopyMultipleFromZipPacking_155726881296202... > Physical Placement

Disk Pools

Name	Health	S3 Pool Type	Standby	Partition
Arctic_Blue_1_11060724571267...	Online	Nearline	No	neo-disk-partition

Double click on a row to see more detailed information

Tapes

Barcode	Serial Number ❓	Type	State	Write Protected	Available	Used	Tape Library Partition	Storage Domain	Bucket	Last Modified	Last Verified	Loaded In Drive

There are currently no items to display

Microsoft Azure Targets

Name	Account Name	State	Standby

There are currently no items to display

BlackPearl Targets

Name	Data Path End Point	State	Standby

There are currently no items to display

Amazon S3 Targets

Name	Data Path End Point	Region	State	Standby	S3 File Naming

There are currently no items to display

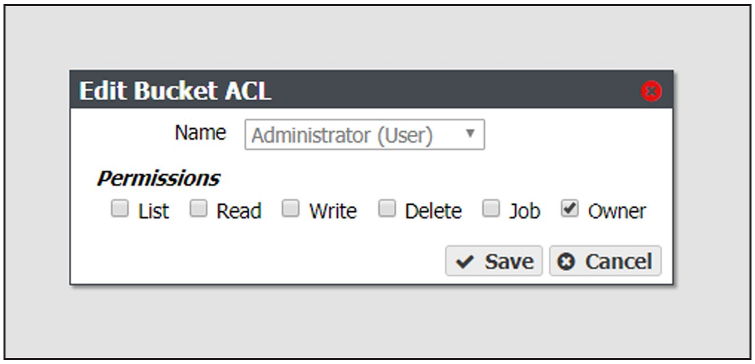
Figure 65 The *Bucket* Physical Placement screen.

Edit a Bucket ACL

Use the instructions in this section to edit an Access Control List (ACL) for a bucket.

1. From the menu bar, select **Configuration > Buckets**. The Buckets screen displays (see Figure 59 on page 171).
2. Select the bucket for which you want to edit an ACL and select **Action > Show Details**. The bucket details screen displays (see Figure 61 on page 173).

3. Select the Access Control List you want to edit and select **Action > Edit Bucket ACL**. The Edit Bucket ACL dialog box displays.


Edit Bucket ACL

Name: Administrator (User)

Permissions

□ List □ Read □ Write □ Delete □ Job ☑ Owner

Figure 66 The Edit Bucket ACL dialog box.

Note: You cannot change the user of an existing bucket ACL list. The **Name** drop-down list is unavailable.

4. Select or clear the desired **Permissions** for the bucket ACL.
5. Click **Save**.

Delete a Bucket ACL

Use the instructions in this section to delete an Access Control List (ACL) for a bucket.

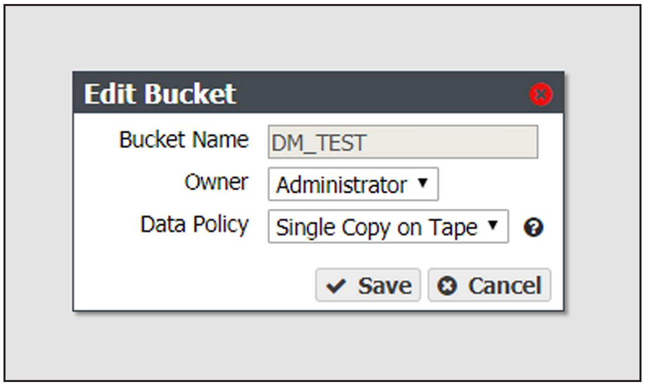
1. From the menu bar, select **Configuration > Buckets**. The Buckets screen displays (see Figure 59 on page 171).
2. Select the bucket for which you want to delete an ACL and select **Action > Show Details**. The bucket details screen displays (see Figure 61 on page 173).
3. Select the Access Control List you want to delete and select **Action > Delete Bucket ACL**. The Delete Bucket ACL confirmation dialog box displays.
4. Click **Delete**.

Edit a Bucket

Use the instructions in this section to change the owner of a bucket or to change the data policy used by the bucket.

1. From the menu bar, select **Configuration > Buckets**. The Buckets screen displays (see Figure 59 on page 171).

2. Select the bucket you want to edit and select **Action > Edit**. The Edit Bucket dialog box displays.



Bucket Name: DM_TEST
Owner: Administrator
Data Policy: Single Copy on Tape

Figure 67 The Edit Bucket dialog box.

3. The **Bucket Name** is unavailable and cannot be changed.
4. From the drop-down list, change the **Owner** assigned to the bucket.

IMPORTANT After changing bucket owners, you may need to reconfigure your client application to access the bucket.

IMPORTANT After changing bucket owners, you may need to reconfigure your client application to access the bucket.

5. Use the **Data Policy** drop down menu to change the data policy assigned to the bucket. For more information on data policies, see Data Policies on page 93.
6. Click **Save**.

Delete a Bucket

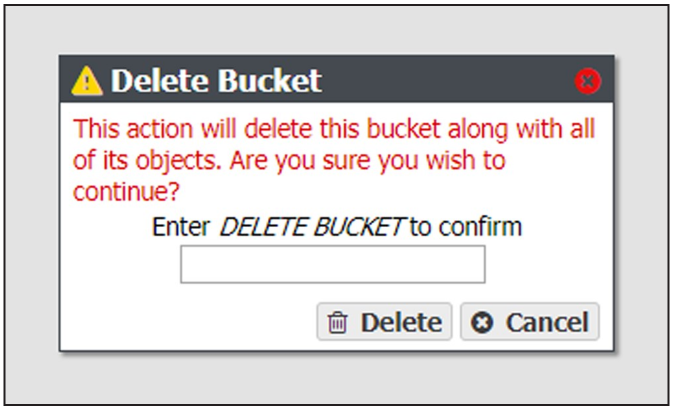
Use the instructions in this section to delete a bucket.

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.

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. From the menu bar, select **Configuration > Buckets**. The Buckets screen displays (see Figure 59 on page 171).
2. Select the bucket you want to delete and select **Action > Delete**. A confirmation dialog box displays.



Delete Bucket

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 68 The bucket delete confirmation dialog box.

3. Type `DELETE BUCKET` into the entry field, and then click **Delete**.

Manage a Storage Domain

Use the instructions in this section to edit or delete a storage domain member or a storage domain.

Edit a Storage Domain Member

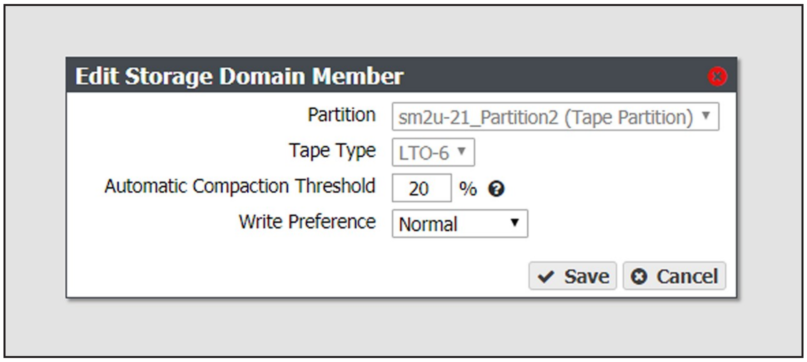
Use the instructions in this section to change the write preference for a storage domain member.

Note: For every storage domain, at least one storage domain member must have a write preference other than **Never_Select**.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Double-click the row for the storage domain with the storage domain member that you want to edit, or select the storage domain row and then select **Action > Show Details**. The Storage Domain details screen displays (see Figure 49 on page 157).
3. Select the storage domain member row and then select **Action > Edit Storage Domain Member**.

Note: Do not click the partition name when selecting the data persistence rule row or the Partition details screen will open.

The Edit Storage Domain Member dialog box displays.



Edit Storage Domain Member

Partition: sm2u-21_Partition2 (Tape Partition)

Tape Type: LTO-6

Automatic Compaction Threshold: 20 %

Write Preference: Normal

Figure 69 The Edit Storage Domain Member dialog box.

4. If desired, edit the percentage for the **Automatic Compaction Threshold**. Automatic compaction occurs when the percentage of deleted objects on a tape cartridge exceeds this value.
5. If desired, using the drop down menu, edit the **Write Preference** field as necessary. See Add a Storage Domain Member to a Storage Domain on page 156 for a description of each field.

Note: When editing a storage domain member, the **Partition** and **Tape Type** settings are unavailable.

6. Click **Save**. The edited storage domain member displays on the Storage Domain details screen.

Exclude a Storage Domain Member

Use the instructions in this section to exclude a storage domain member. This command migrates data off of the selected storage domain member before deleting the storage domain member.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Double-click the row for the storage domain with the storage domain member that you want to exclude, or select the storage domain row and then select **Action > Show Details**. The Storage Domain details screen displays (see Figure 49 on page 157).
3. Select the desired storage domain member row and then select **Action > Exclude Storage Domain Member**.

Note: Do not click the partition name when selecting the data persistence rule row or the Partition details screen will open.

The Exclude Storage Domain Member dialog box displays.

4. Type `EXCLUDE` in the entry field and then click **Exclude**.

Cancel Storage Domain Member Exclusion

Use the instructions in this section to cancel a storage domain member exclusion in process.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Double-click the row for the storage domain with the storage domain member that is currently being excluded, or select the storage domain row and then select **Action > Show Details**. The Storage Domain details screen displays (see Figure 49 on page 157).
3. Select the desired storage domain member row and then select **Action > Cancel Storage Domain Member Exclusion**.

   Note: Do not click the partition name when selecting the data persistence rule row or the Partition details screen will open.

   The Cancel Storage Domain Member Exclusion dialog box displays.
4. Type `CANCEL` in the entry field and then click **Cancel**.

Delete a Storage Domain Member

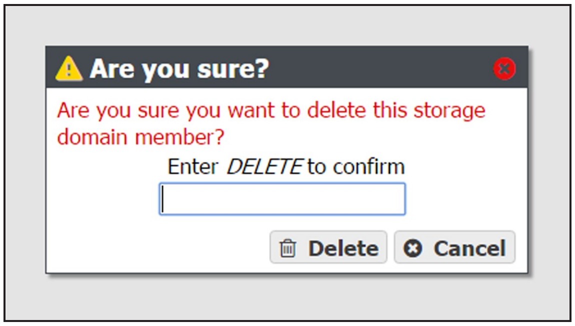
Use the instructions in this section to delete a storage domain.

Notes:
- You cannot delete a storage domain member that has a tape or pool assigned to the storage domain.
- You cannot delete the last storage domain member of a storage domain assigned to a data policy.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Double-click the row for the storage domain with the storage domain member that you want to edit, or select the storage domain row and then select **Action > Show Details**. The Storage Domain details screen displays (see Figure 49 on page 157).
3. Select the storage domain member row and then select **Action > Delete Storage Domain Member**.

   Note: Do not click the partition name when selecting the data persistence rule row or the Partition details screen will open.

   A confirmation dialog box displays.


Are you sure?

Are you sure you want to delete this storage domain member?

Enter *DELETE* to confirm

Figure 70 The delete storage domain member confirmation dialog box.

4. Type `DELETE` into the entry field, and then click **Delete**.

Edit a Storage Domain

Use the instructions in this section to change the parameters for a storage domain.

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.

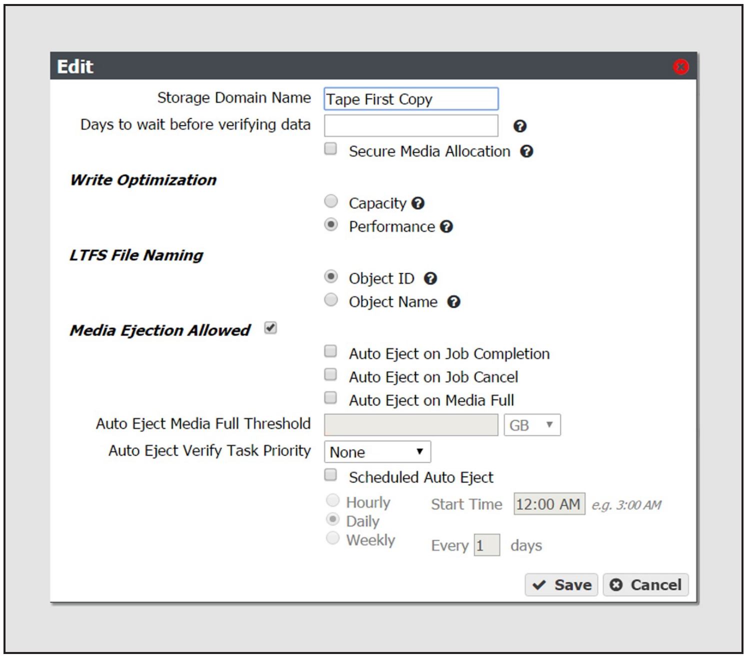
IMPORTANT If this storage domain is assigned to a data policy that uses versioning, after data is persisted, you cannot change this setting from Object ID to Object Name.

Note: If an edit you select is not allowed, the gateway generates an error message when you click **Save**, explaining why the edit is not allowed.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).

2. Select the row for the storage domain that you want to edit and then select **Action > Edit**. The Edit storage domain screen displays

Note: Alternatively, select **Action > Edit Storage Domain** from the storage domain details screen.



Edit

Storage Domain Name: Tape First Copy

Days to wait before verifying data:

□ Secure Media Allocation

Write Optimization

○ Capacity

● Performance

LTFS File Naming

● Object ID

○ Object Name

Media Ejection Allowed ☑

□ Auto Eject on Job Completion

□ Auto Eject on Job Cancel

□ Auto Eject on Media Full

Auto Eject Media Full Threshold: GB

Auto Eject Verify Task Priority: None

□ Scheduled Auto Eject

○ Hourly ● Daily ○ Weekly

Start Time: 12:00 AM *e.g. 3:00 AM*

Every 1 days

Figure 71 The Edit Storage Domain dialog box.

3. Edit the fields as necessary. See Create a Storage Domain on page 150 for a description of each field.

4. Click **Save**. The edited storage domain displays on the Advanced Bucket Management screen.

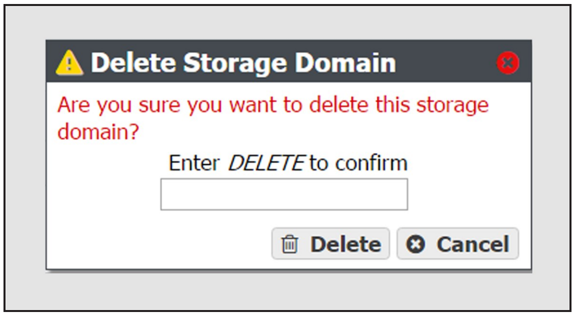
Delete a Storage Domain

Use the instructions in this section to delete a storage domain.

Note: You cannot delete a storage domain if it is used by a data policy. See Delete a Data Replication Rule on page 192 for instructions on removing the storage domain from a data policy.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).

2. Select the row for the storage domain that you want to delete and then select **Action > Delete**. A confirmation dialog box displays.



Are you sure you want to delete this storage domain?

Enter *DELETE* to confirm

Figure 72 The delete storage domain confirmation dialog box.

3. Type `DELETE` into the entry field, and then click **Delete**.

MANAGE DATA REPLICATION RULES

Edit a BlackPearl Data Replication Rule

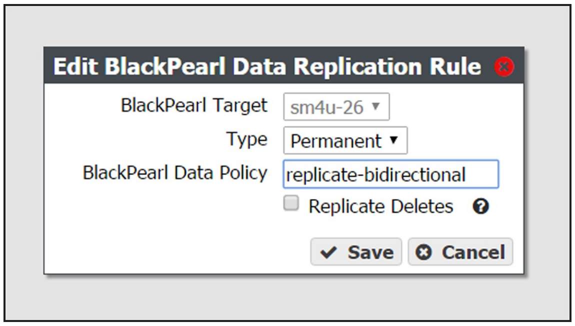
Use the instructions in this section to change the type, data policy, or whether to replicate deletes, for a BlackPearl data replication rule.

Note: Some edits are restricted based on whether a bucket is currently using the data policy. If an edit is not allowed, an error message displays when you click **Save**.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Double-click the data policy with the BlackPearl data replication rule that you want to edit, or select the data policy and then select **Action > Show Details**. The Data Policy details screen displays (see Figure 52 on page 163).
3. Double-click the row of the BlackPearl data replication rule that you want to edit, or select the row for the replication rule and then select **Action > Edit Rule**.

Note: Do not click the target name when selecting the data persistence rule row or the Replication Targets screen will open.

The Edit BlackPearl Data Replication Rule dialog box displays.



Edit BlackPearl Data Replication Rule

BlackPearl Target: sm4u-26

Type: Permanent

BlackPearl Data Policy: replicate-bidirectional

☐ Replicate Deletes

Figure 73 The Edit BlackPearl Data Replication Rule dialog box.

4. The BlackPearl target name is unavailable and cannot be changed.
5. Edit the fields as necessary. See Add a BlackPearl Data Replication Rule to a Data Policy on page 165 for a description of each field.
6. Click **Save**. The edited BlackPearl data replication rule displays on the Data Policy details screen.

Edit an Amazon S3 Data Replication Rule

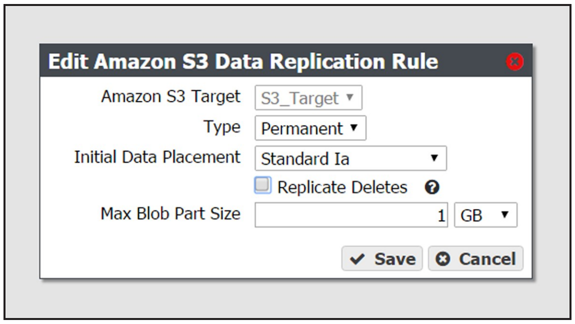
Use the instructions in this section to change the type, Initial Data Placement, whether to Replicate Deletes, or the Max Blob Size for an Amazon S3 data replication rule.

Note: Some edits are restricted based on whether a bucket is currently using the data policy. If an edit is not allowed, an error message displays when you click **Save**.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Double-click the data policy with the Amazon S3 replication rule that you want to edit, or select the data policy and then select **Action > Show Details**. The Data Policy details screen displays (see Figure 52 on page 163).
3. Double-click the row of the Amazon S3 data replication rule that you want to edit, or select the row for the replication rule and then select **Action > Edit Rule**.

Note: Do not click the target name when selecting the data persistence rule row or the Replication Targets screen will open.

The Edit Amazon S3 Data Replication Rule dialog box displays.


Edit Amazon S3 Data Replication Rule

Amazon S3 Target: S3_Target

Type: Permanent

Initial Data Placement: Standard Ia

□ Replicate Deletes

Max Blob Part Size: 1 GB

Figure 74 The Edit Amazon S3 Data Replication Rule dialog box.

4. The Amazon S3 target name is unavailable and cannot be changed.
5. Edit the fields as necessary. See Add an Amazon S3 Data Replication Rule to a Data Policy on page 166 for a description of each field.

Note: 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.

6. Click **Save**. The edited Amazon S3 data replication rule displays on the Data Policy details screen.

Edit a Microsoft Azure Data Replication Rule

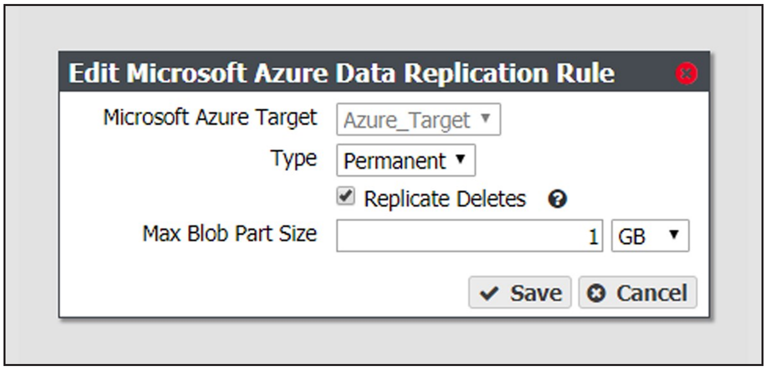
Use the instructions in this section to change the type, whether to Replicate Deletes, or the Max Blob Size for a Microsoft Azure data replication rule.

Note: Some edits are restricted based on whether a bucket is currently using the data policy. If an edit is not allowed, an error message displays when you click **Save**.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Double-click the data policy with the Microsoft Azure replication rule that you want to edit, or select the data policy and then select **Action > Show Details**. The Data Policy details screen displays (see Figure 52 on page 163).
3. Double-click the row of the Microsoft Azure data replication rule that you want to edit, or select the row for the replication rule and then select **Action > Edit Rule**.

Note: Do not click the target name when selecting the data persistence rule row or the Replication Targets screen will open.

The Edit Microsoft Azure Data Replication Rule dialog box displays.



Edit Microsoft Azure Data Replication Rule

Microsoft Azure Target: Azure_Target

Type: Permanent

☑ Replicate Deletes

Max Blob Part Size: 1 GB

Figure 75 The Edit Microsoft Azure Data Replication Rule dialog box.

4. The Microsoft Azure target name is unavailable and cannot be changed.
5. Edit the fields as necessary. See Add a Microsoft Azure Data Replication Rule to a Data Policy on page 168 for a description of each field.
6. Click **Save**. The edited Microsoft Azure data replication rule displays on the Data Policy details screen.

Delete a Data Replication Rule

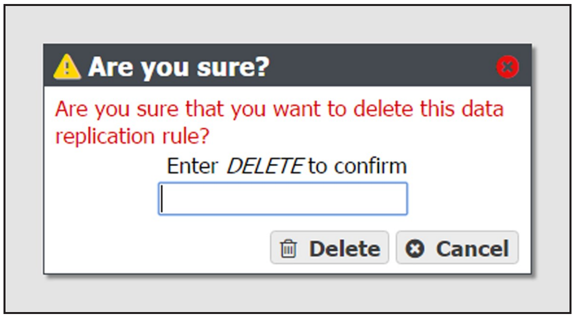
Use the instructions in this section to delete a data replication rule for any type of target from a data policy.

Note: You cannot delete a data replication rule if the data policy is used by a bucket. See Delete a Bucket on page 182 for instructions for deleting buckets using a data policy.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Double-click the data policy with the replication rule that you want to delete, or select the data policy and then select **Action > Show Details**. The Data Policy details screen displays (see Figure 52 on page 163).
3. Select the row for the replication rule and then select **Action > Delete Rule**.

Note: Do not click the target name when selecting the data persistence rule row or the Replication Targets screen will open.

A confirmation dialog box displays.



Are you sure that you want to delete this data replication rule?

Enter *DELETE* to confirm

Figure 76 The delete data replication rule confirmation dialog box.

4. Type `DELETE` into the entry field, and then click **Delete**.

MANAGE A DATA POLICY

Use the instructions in this section to manage access control lists (ACLs), and to edit or delete persistence rules, replication rules, and data policies.

Edit a Data Policy

Use the instructions in this section to edit a data policy.

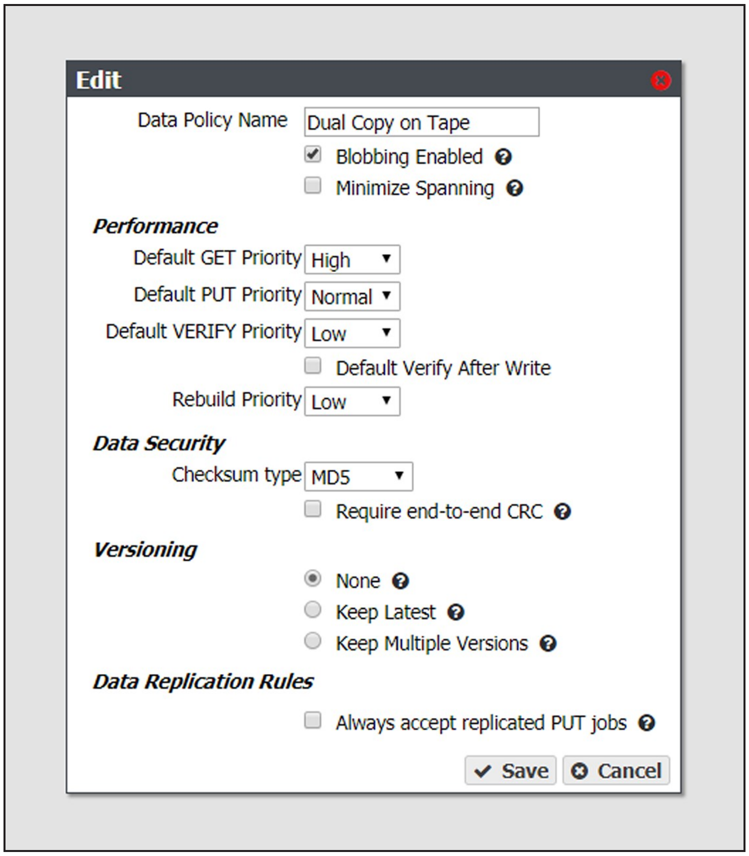
IMPORTANT If you previously configured the data policy Versioning setting to **Keep Multiple Versions**, you are not able to change this setting after the data policy was created.

IMPORTANT If you previously configured the data policy Versioning setting to **Keep Multiple Versions**, you are not able to change this setting after the data policy was created.

Note: If an edit you selected is not allowed, the gateway generates an error message, when you click **Save**, explaining why the edit is not allowed. For example, you cannot change the **Checksum type** if the data policy is used by a bucket.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).

2. Select the row for the data policy that you want to edit and then select **Action > Edit**. The Edit Data Policy screen displays.



Edit

Data Policy Name: Dual Copy on Tape

☑ Blobbing Enabled

□ Minimize Spanning

Performance

Default GET Priority: High

Default PUT Priority: Normal

Default VERIFY Priority: Low

□ Default Verify After Write

Rebuild Priority: Low

Data Security

Checksum type: MD5

□ Require end-to-end CRC

Versioning

● None

○ Keep Latest

○ Keep Multiple Versions

Data Replication Rules

□ Always accept replicated PUT jobs

Figure 77 The Edit Data Policy dialog box.

3. Edit the fields as necessary. See Create a Data Policy on page 159 for a description of each field.
4. Click **Save**. The edited data policy displays on the Advanced Bucket Management screen.

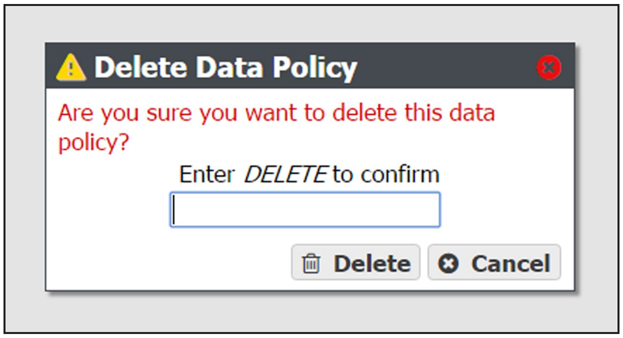
Delete a Data Policy

Use the instructions in this section to delete a data policy.

Note: You cannot delete a data policy if any buckets exist that use the specified data policy. See Delete a Bucket on page 182 for instructions for deleting buckets using a data policy.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).

2. Select the row for the data policy that you want to delete and then select **Action > Delete**. A confirmation dialog box displays.



Delete Data Policy

Are you sure you want to delete this data policy?

Enter *DELETE* to confirm

Figure 78 The delete data policy confirmation dialog box.

3. Type DELETE into the entry field, and then click **Delete**.

Delete a Data Policy ACL

Use the instruction in this section to delete a data policy ACL.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Select the row for the data policy for which you want to delete an ACL, then select **Action > Show Details**. The Data Policy details screen displays.
3. Select the row for the data policy ACL which you want to delete.
4. From the menu bar, select **Action > Delete Data Policy ACL**. A confirmation window displays.
5. Click **Delete**.

Edit a Data Persistence Rule

Use the instructions in this section to change the type, Isolation Level, or Minimum Days to Retain for a data persistence rule.

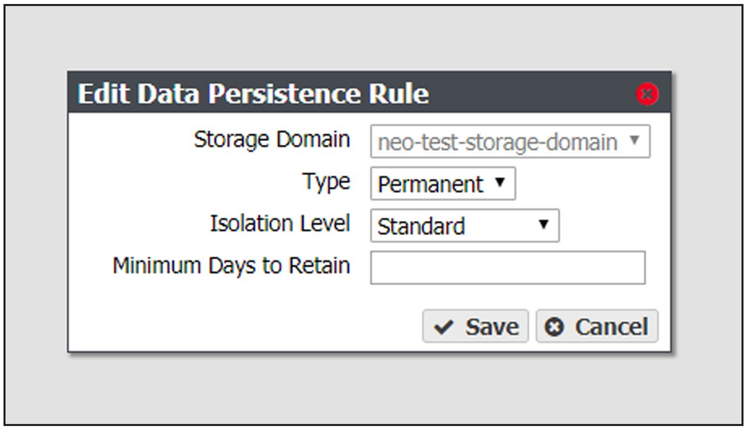
Note: Some edits are restricted based on whether a bucket is currently using the data policy. If an edit is not allowed, an error message displays when you click **Save**.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Double-click the data policy with the persistence rule that you want to edit, or select the data policy and then select **Action > Show Details**. The Data Policy details screen displays (see Figure 52 on page 163).

3. Double-click the row of the persistence rule that you want to edit, or select the row for the persistence rule and then select **Action > Edit Rule**.

Note: Do not click the storage domain name when selecting the data persistence rule row or the Storage Domain details screen will open.

The Edit Data Persistence Rule dialog box displays.



Edit Data Persistence Rule

Storage Domain	neo-test-storage-domain ▾
Type	Permanent ▾
Isolation Level	Standard ▾
Minimum Days to Retain	

Figure 79 The Edit Data Persistence Rule dialog box.

4. The **Storage Domain** setting is unavailable and cannot be changed.
5. Edit the fields as necessary. See Add Data Persistence Rules and Replication Rules to a Data Policy on page 163 for a description of each field.
6. Click **Save**. The edited data persistence rule displays on the Data Policy details screen.

Delete a Data Persistence Rule

Use the instructions in this section to delete a data persistence rule from a data policy.

CAUTION Deleting a persistence rule deletes all data associated with the rule.

CAUTION Deleting a persistence rule deletes all data associated with the rule.

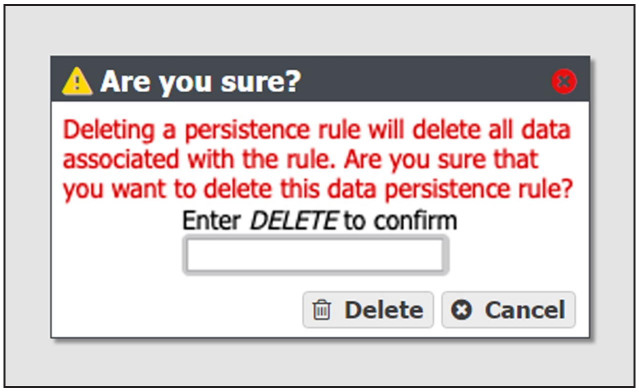
Notes:

- You cannot delete a data persistence rule if the data policy is used by a bucket. See Delete a Bucket on page 182 for instructions for deleting buckets using a data policy.
- You cannot delete a persistence rule if it is the last permanent persistence rule for a data policy.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Double-click the data policy with the persistence rule that you want to delete, or select the data policy and then select **Action > Show Details**. The Data Policy details screen displays (see Figure 52 on page 163).
3. Select the row for the persistence rule and then select **Action > Delete Rule**.

Note: Do not click the storage domain name when selecting the data persistence rule row or the Storage Domain details screen will open.

A confirmation dialog box displays.



Are you sure?

Deleting a persistence rule will delete all data associated with the rule. Are you sure that you want to delete this data persistence rule?

Enter *DELETE* to confirm

Figure 80 The delete data persistence rule confirmation dialog box.

4. Type `DELETE` into the entry field, and then click **Delete**.

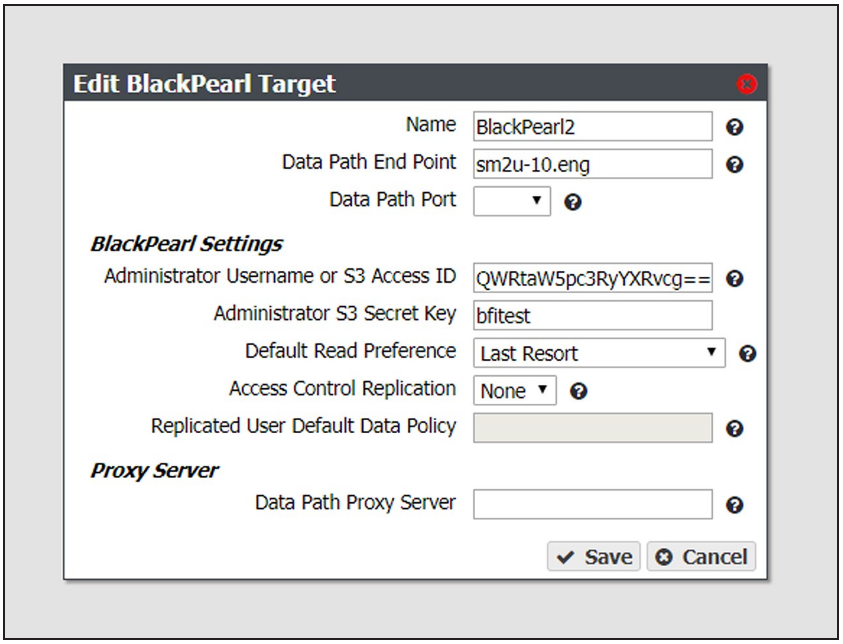
MANAGE REPLICATION TARGETS

Use the instruction in this section to manage existing replication targets.

Edit a BlackPearl Replication Target

Use the instructions in this section to modify the configuration of an existing BlackPearl replication target.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Replication Targets** to display the Replication Targets screen (see Figure 40 on page 132).
2. Double-click the BlackPearl replication target that you want to edit, or select the replication target and then select **Action > Edit**. The Edit BlackPearl Target dialog box displays.



Edit BlackPearl Target

Name: BlackPearl2

Data Path End Point: sm2u-10.eng

Data Path Port:

BlackPearl Settings

Administrator Username or S3 Access ID: QWRtaW5pc3RyYXRvcg==

Administrator S3 Secret Key: bfitest

Default Read Preference: Last Resort

Access Control Replication: None

Replicated User Default Data Policy:

Proxy Server

Data Path Proxy Server:

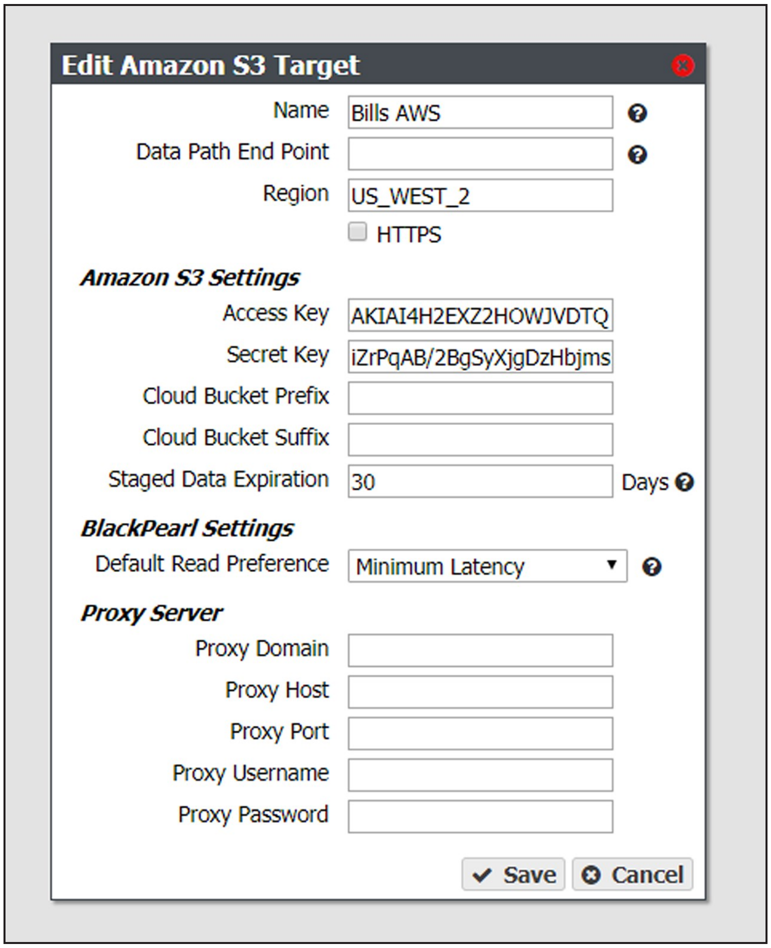
Figure 81 The Edit BlackPearl Target dialog box.

3. Edit the fields as necessary. See Create a BlackPearl Target on page 139 for a description of each field.
4. Click **Save**. The edited BlackPearl replication target displays on the Replication Targets screen.

Edit an Amazon Replication Target

Use the instructions in this section to modify the configuration of an existing Amazon replication target.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Replication Targets** to display the Replication Targets screen (see Figure 40 on page 132).
2. Double-click the Amazon replication target that you want to edit, or select the replication target and then select **Action > Edit**. The Edit Amazon S3 Target dialog box displays.



Edit Amazon S3 Target

Name	Bills AWS
Data Path End Point	
Region	US_WEST_2
	□ HTTPS

Amazon S3 Settings

Access Key	AKIAI4H2EXZ2HOWJVDTQ
Secret Key	iZrPqAB/2BgSyXjgDzHbjms
Cloud Bucket Prefix	
Cloud Bucket Suffix	
Staged Data Expiration	30 Days

BlackPearl Settings

Default Read Preference	Minimum Latency ▾

Proxy Server

Proxy Domain	
Proxy Host	
Proxy Port	
Proxy Username	
Proxy Password	

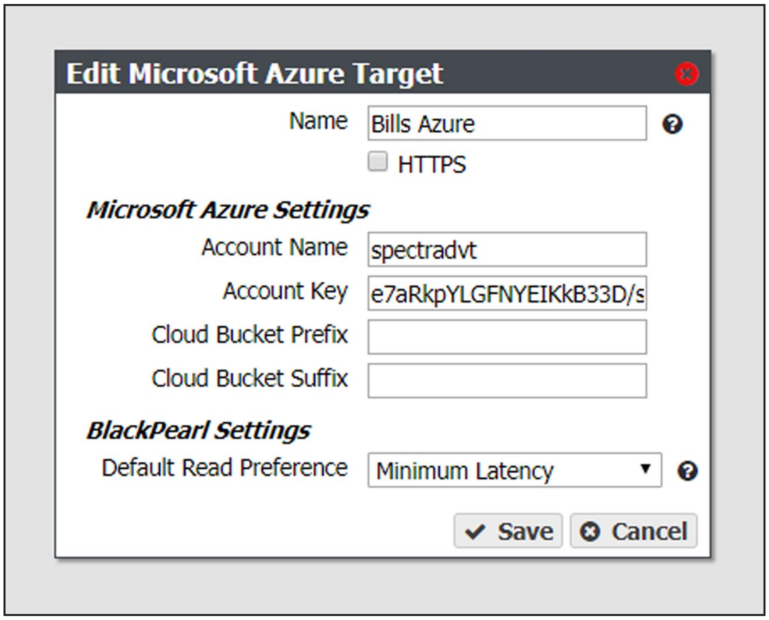
Figure 82 The Edit Amazon S3 Target dialog box.

3. Edit the fields as necessary. See Create an Amazon S3 Target on page 143 for a description of each field.
4. Click **Save**. The edited Amazon replication target displays on the Replication Targets screen.

Edit an Azure Replication Target

Use the instructions in this section to modify the configuration of an existing Azure replication target.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Replication Targets** to display the Replication Targets screen (see Figure 40 on page 132).
2. Double-click the Azure replication target that you want to edit, or select the replication target and then select **Action > Edit**. The Edit Microsoft Azure Target dialog box displays.



Edit Microsoft Azure Target

Name: Bills Azure

□ HTTPS

Microsoft Azure Settings

Account Name: spectradvt

Account Key: e7aRkpYLGFNYEIKkB33D/s

Cloud Bucket Prefix:

Cloud Bucket Suffix:

BlackPearl Settings

Default Read Preference: Minimum Latency

Figure 83 The Edit Microsoft Azure Target dialog box.

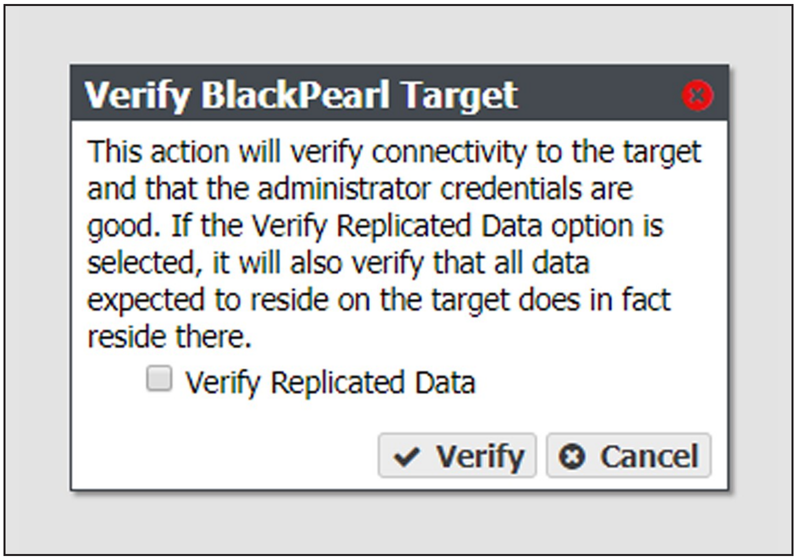
3. Edit the fields as necessary. See Create a Microsoft Azure Target on page 147 for a description of each field.
4. Click **Save**. The edited Azure replication target displays on the Replication Targets screen.

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. From the menu bar, select **Configuration > Advanced Bucket Management > Replication Targets** to display the Replication Targets screen (see Figure 40 on page 132).

2. Double-click the replication target for which you want to verify connectivity, or select the replication target and then select **Action > Verify Data**. The Verify *target type* Target dialog box displays.



Verify BlackPearl 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 84 The Verify *target type* Target dialog box.

3. 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.

4. Click **Verify**. The gateway confirms connectivity to the target and optionally verifies the replicated data.

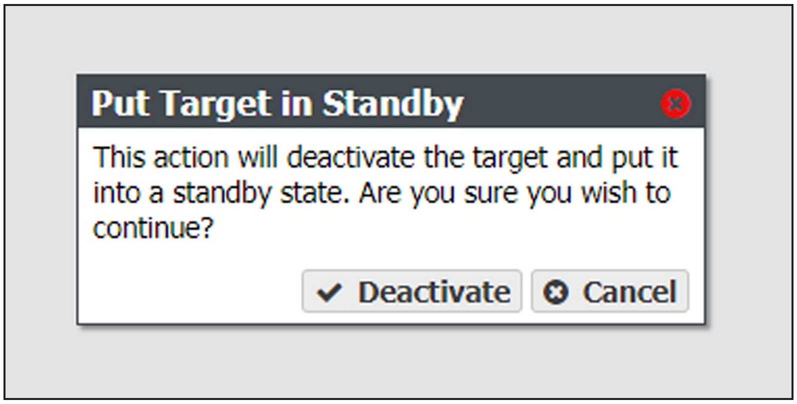
Put a Replication Target in Standby State

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 gateway may attempt to use the target while it is in service.

Use the instructions in this section to place a replication target into a standby state. No data is transferred to the replication target while in standby.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Replication Targets** to display the Replication Targets screen (see Figure 40 on page 132).

2. Select the replication target that you want to put into standby and then select **Action > Put Target in 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?

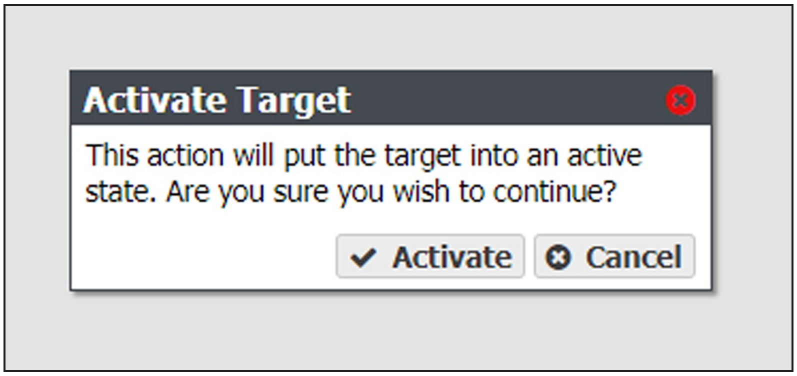
Figure 85 The Put Target in Standby dialog box.

3. 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. From the menu bar, select **Configuration > Advanced Bucket Management > Replication Targets** to display the Replication Targets screen (see Figure 40 on page 132).
2. Select the replication target that you want to activate and then select **Action > Activate Target**. The Activate Target dialog box displays.



Activate Target

This action will put the target into an active state. Are you sure you wish to continue?

Figure 86 The Activate Target dialog box.

3. Click **Activate**. The target is now in an active state.

Delete a Replication Target

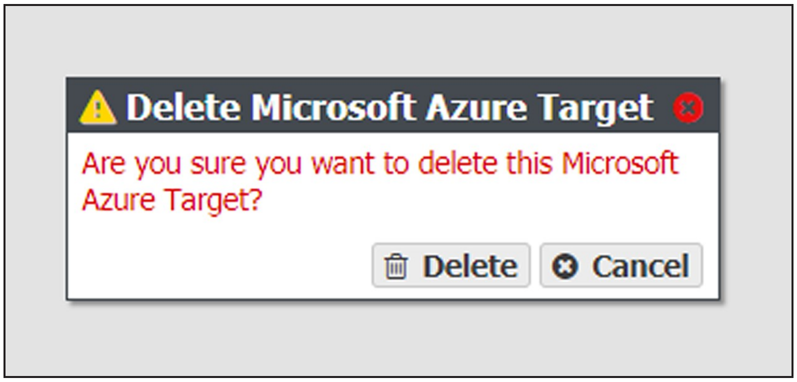
Use the instructions to delete an existing replication target.

CAUTION If you delete a replication target, all data on the target is deleted.

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 Delete a Data Replication Rule on page 192 for instructions on removing a replication target from a data policy.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Replication Targets** to display the Replication Targets screen (see Figure 40 on page 132).
2. Select the replication target that you want to delete and then select **Action > Delete**. The Delete *target type* Target dialog box displays.



Delete Microsoft Azure Target

Are you sure you want to delete this Microsoft Azure Target?

Figure 87 The Delete *target type* Target dialog box.

3. Click **Delete** to delete the selected replication target.

Manage a Disk Partition

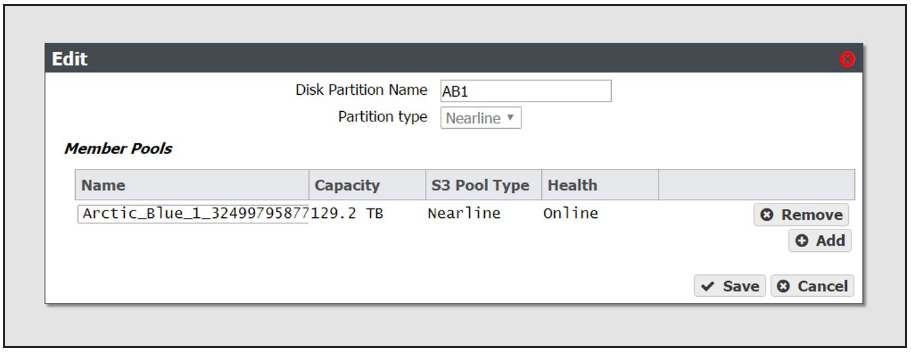
Use the instructions in this section to edit or delete a disk partition.

Edit a Disk Partition

Use the instructions in this section to change the parameters for a disk partition.

Notes:
- You cannot remove a member pool that contains data.
- You cannot remove the last member pool of a disk partition assigned to a storage domain.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Select the disk partition row and then select **Action > Edit**. The Edit Disk Partition dialog box displays.



Edit

Disk Partition Name: AB1

Partition type: Nearline

Member Pools

Name	Capacity	S3 Pool Type	Health
Arctic_Blue_1_32499795877	129.2 TB	Nearline	Online

Figure 88 The Edit Disk Partition dialog box.

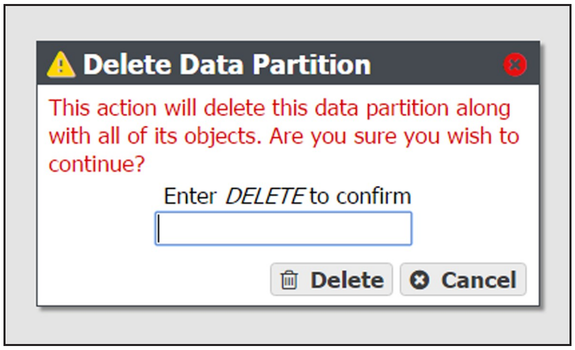
3. Edit the fields as necessary. See Create a Disk Pool on page 130 for a description of each field.
4. Click **Save**. The edited disk partition displays on the Advanced Bucket Management screen.

Delete a Disk Partition

Use the instructions in this section to delete a disk partition.

Note: You cannot delete a disk partition that is a member of any storage domain. See Delete a Storage Domain Member on page 185 for information on deleting the disk partition from a storage domain.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Select the row of the disk partition you want to delete and then select **Action > Delete**. A confirmation dialog box displays.



Delete Data Partition

This action will delete this data partition along with all of its objects. Are you sure you wish to continue?

Enter *DELETE* to confirm

Figure 89 The Delete Disk Partition confirmation dialog box.

3. Type `DELETE` into the entry field, and then click **Delete**.

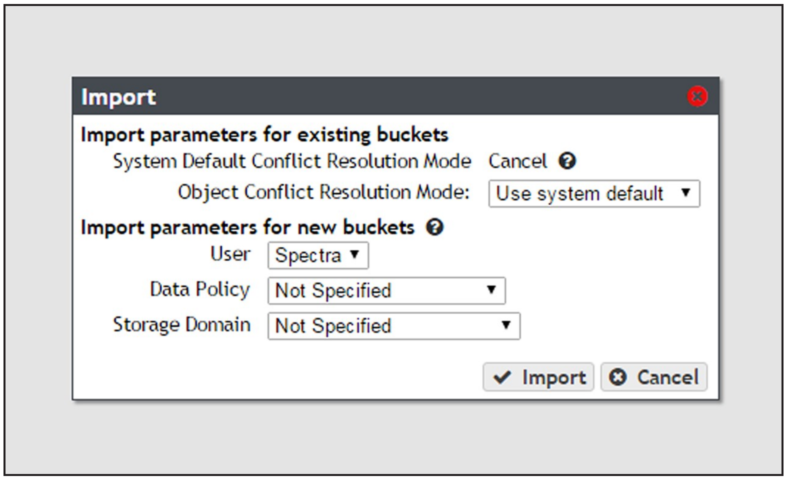
Manage Online and Nearline Disk Pools

Use the instructions in this section to manage nearline and online disk pools. For information on managing network attached storage (NAS) disk pools, see Manage Storage Pools on page 248.

Import a Nearline or Online Disk Pool

Data present on storage pools on expansion nodes can be moved from one BlackPearl gateway to another, either to increase name space redundancy, or as part of disaster prevention. Use the instructions in this section to import a pool.

1. Ensure the expansion node containing the pool you want to import is cabled to the BlackPearl gateway master node.
2. Ensure the settings for the DS3 service **Default Conflict Resolution Mode** are set to your preference. See Configure the DS3 Service on page 292 for more information.
3. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
4. Disk pools eligible for import display with a health of **Foreign**. Select the nearline pool you want to import in the Storage Pools pane, and select **Action > Import Pool**. The Import dialog box displays.



Import parameters for existing buckets
System Default Conflict Resolution Mode Cancel
Object Conflict Resolution Mode: Use system default
Import parameters for new buckets
User Spectra
Data Policy Not Specified
Storage Domain Not Specified

Figure 90 The Import dialog box.

5. Configure the import parameters for existing buckets present on the storage pool.
   a. The **System Default Conflict Resolution Mode** is configured when editing the DS3 service and is not editable in this dialog box. See Configure the DS3 Service on page 292 for more information.

b. Using the drop-down menu, select a behavior for **Object Conflict Resolution Mode**. This setting configures how the gateway handles a file name conflict when importing foreign objects on the storage pool to an existing bucket.

Value	Description
Use system default	The gateway uses the behavior displayed in the **System Default Conflict Resolution Mode** row of the Import dialog box.
Cancel	Abort the import process if a file name conflict is discovered.
Accept Most Recent	Keep the file with the most recent creation date.
Accept Existing	Keep the file currently in the BlackPearl database.

6. Configure the import parameters for new buckets present on the storage pool.
    a. Using the drop-down menu, select the **User** to be the owner of the imported bucket (s).
    b. Using the drop-down menu, select the **Data Policy** to use for the imported bucket (s).
    c. Using the drop-down menu, select the **Storage Domain** to use for the imported bucket(s).
7. Click **Import.**

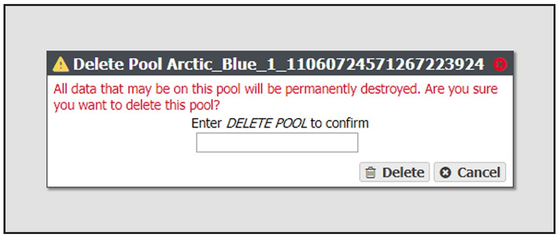
Delete a Nearline or Online Disk Pool

If you want to delete an online or nearline disk pool (for example, to create a larger pool after adding additional disks to the gateway) use the instructions in this section to delete a disk pool.

Note: You must delete all objects contained in the disk pool before you can delete the pool.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).

2. Select the pool you want to delete in the Storage Pools pane, and select **Action > Delete**. A confirmation dialog box displays.

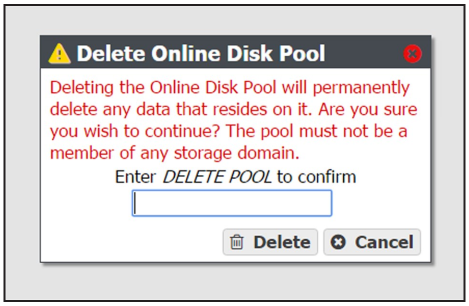


Delete Pool Arctic_Blue_1_11060724571267223924

All data that may be on this pool will be permanently destroyed. Are you sure you want to delete this pool?

Enter *DELETE POOL* to confirm

Figure 91 The Delete Nearline Disk Pool confirmation dialog box.



Delete Online Disk Pool

Deleting the Online Disk Pool will permanently delete any data that resides on it. Are you sure you wish to continue? The pool must not be a member of any storage domain.

Enter *DELETE POOL* to confirm

Figure 92 The Delete Online Disk Pool confirmation dialog box.

3. Enter `DELETE POOL` into the entry field and click **Delete**. The disk pool is deleted.

Change the BlackPearl Gateway Cache Configuration

If desired, you can change the configuration of the BlackPearl gateway cache to allow for better performance, or create a larger or smaller cache suitable for your workflow environment. You can also add new disks installed in the gateway to the system cache.

Note: Changing the system cache should only be done after careful consideration of your desired workflow.

After changing the BlackPearl cache configuration, all data in the cache is deleted, and the system reboots.

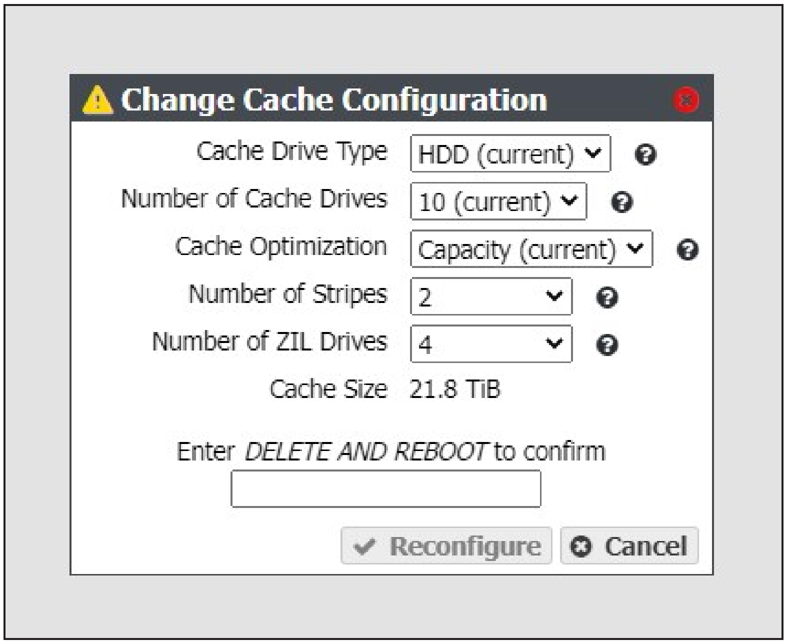
CAUTION All data currently in the system cache is deleted. As long as all jobs are complete before you change the system cache configuration, no data is lost.

CAUTION All data currently in the system cache is deleted. As long as all jobs are complete before you change the system cache configuration, no data is lost.

Use the instructions in this section to change the system cache configuration.

1. Discontinue data transfers to the BlackPearl gateway and ensure that all jobs complete (see View DS3 Jobs Information on page 431). Migrate any data you want to keep off of the system cache.
2. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).

3. In the Storage Pools pane, select the BlackPearl_Cache, and then select **Action > Edit**. The Change Cache Configuration dialog box displays.



Change Cache Configuration

Cache Drive Type: HDD (current)

Number of Cache Drives: 10 (current)

Cache Optimization: Capacity (current)

Number of Stripes: 2

Number of ZIL Drives: 4

Cache Size: 21.8 TiB

Enter *DELETE AND REBOOT* to confirm

Figure 93 The Change Cache Configuration dialog box.

4. If desired, change the **Cache Drive Type**. You cannot mix drive types in the system cache.
5. If desired, change the **Number of Cache Drives**. The number of drives selected affects the number of stripes that can be used in Capacity mode.
6. Select the method of **Cache Optimization**. The default is Performance mode. Use Capacity mode to create a larger cache capable of storing a greater number of objects.
7. If you selected Capacity mode in Step 6, select the **Number of Stripes** to use for the cache.
8. Select the **Number of ZIL Drives** (high-performance drives) to assign to the BlackPearl cache.
9. Enter `DELETE AND REBOOT` in the dialog box, and click **Reconfigure**.

CAUTION All data currently in the system cache is deleted. As long as all jobs are complete before you change the system cache configuration, no data is lost.

CAUTION All data currently in the system cache is deleted. As long as all jobs are complete before you change the system cache configuration, no data is lost.

10. The BlackPearl gateway creates a new system cache and reboots.

CHAPTER 6 - CONFIGURING NETWORK ATTACHED STORAGE

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

Overview of NAS Storage Pools, Volumes, and Shares **212**

Storage Pools 212

Volumes and Shares 212

Naming Considerations 212

Create a NAS Storage Pool **213**

Create a Volume **217**

Create a Share **226**

Create a CIFS Share 226

Create an NFS Share 231

Create a Vail S3 Share 232

Configure NAS Services **234**

Configure the CIFS Service 234

Configure the NFI Service 235

Configure the NFS Service 237

Configure NAS Replication **239**

Configure the NAS Replication Service 239

Configure the Target System 241

Configure Volumes for NAS Replication 241

Overview of NAS Storage Pools, Volumes, and Shares

Storage pools, volumes, and shares are the logical components used to interact with the data storage capacity provided by NAS.

Storage Pools

A storage pool groups a set of physical drives together to create a virtual drive that the operating system treats as a single physical drive. Depending on how it is configured, a storage pool can provide mirrored, single-parity, double-parity, or triple-parity data protection. Higher levels of protection allow for more individual drives to fail before the data is compromised. The costs of higher protection are reduced storage availability and reduced performance.

Volumes and Shares

Volumes are located on each storage pool. Volumes can be configured with a minimum size and thin provisioned with a maximum size. When you create a volume, you can specify whether it uses compression, and whether the time stamp for files is updated when the file is read (access time). After the volume is created, it can be shared (made available for use by other computers on the network) via either the NFS service or the CIFS service.

Naming Considerations

When a volume is shared, the volume mount path uses a combination of the storage pool name and volume name. The combined name must be less than 78 ASCII characters, or the volume fails to mount. Additionally, storage pool names are limited to 48 characters, and volume names are limited to 62 characters. Even if the storage pool name is a single character, you are still restricted to 62 characters in the volume name.

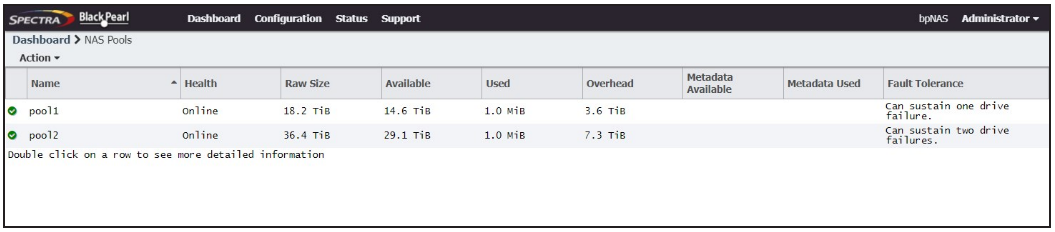
CREATE A NAS STORAGE POOL

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 as described in Delete a Storage Pool on page 251. 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. From the menu bar, select **Configuration > NAS > Pools**, or click the Pools pane on the Dashboard. The NAS Pools screen displays.



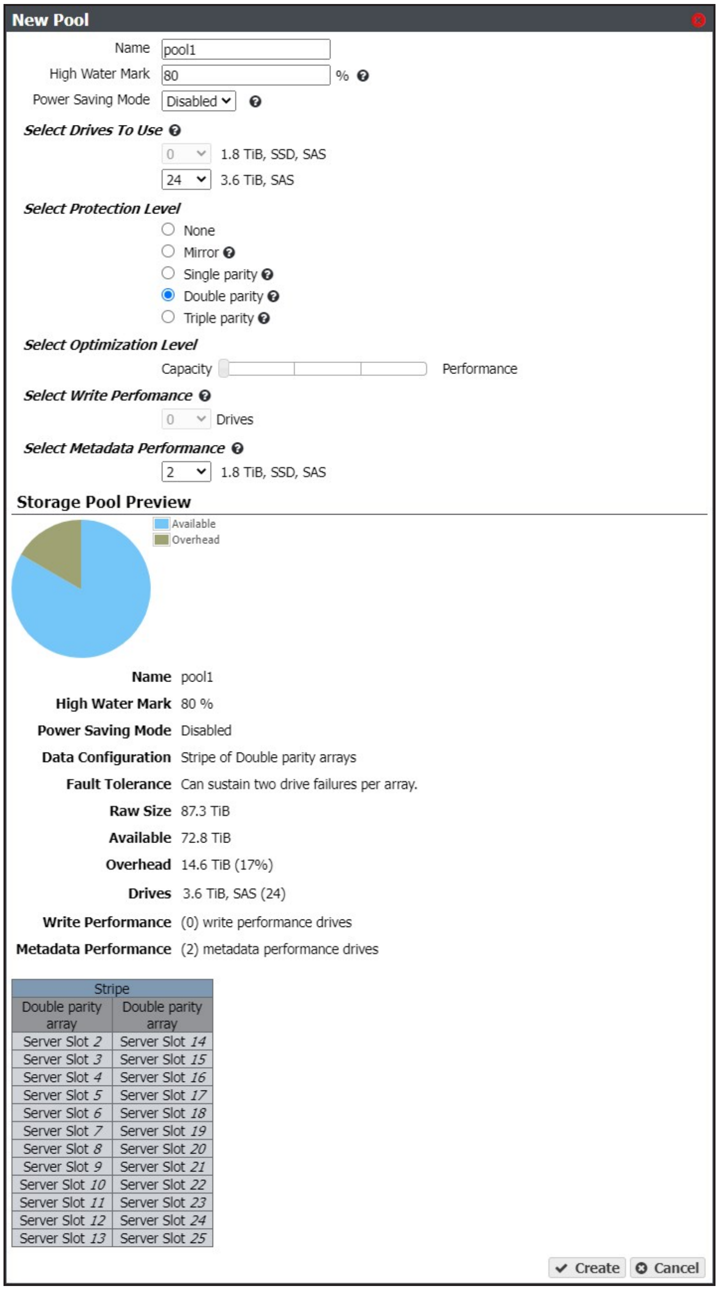
	Name	Health	Raw Size	Available	Used	Overhead	Metadata Available	Metadata Used	Fault Tolerance
✓	pool1	Online	18.2 TiB	14.6 TiB	1.0 MiB	3.6 TiB			Can sustain one drive failure.
✓	pool2	Online	36.4 TiB	29.1 TiB	1.0 MiB	7.3 TiB			Can sustain two drive failures.

Double click on a row to see more detailed information

Figure 94 The NAS Pools screen.

2. Select **Action > New.** A dialog box opens to show the default configuration options for the new pool.

Note: The **Storage Pool Preview** pane does not display until you have selected the disks you want to use in the storage pool



New Pool

Name: pool1

High Water Mark: 80 %

Power Saving Mode: Disabled

Select Drives To Use

0 — 1.8 TiB, SSD, SAS

24 — 3.6 TiB, SAS

Select Protection Level

○ None
○ Mirror
○ Single parity
● Double parity
○ Triple parity

Select Optimization Level

Capacity — Performance

Select Write Perfomance

0 Drives

Select Metadata Performance

2 — 1.8 TiB, SSD, SAS

Storage Pool Preview

Name	pool1
High Water Mark	80 %
Power Saving Mode	Disabled
Data Configuration	Stripe of Double parity arrays
Fault Tolerance	Can sustain two drive failures per array.
Raw Size	87.3 TiB
Available	72.8 TiB
Overhead	14.6 TiB (17%)
Drives	3.6 TiB, SAS (24)
Write Performance	(0) write performance drives
Metadata Performance	(2) metadata performance drives

Stripe	
Double parity array	Double parity array
Server Slot 2	Server Slot 14
Server Slot 3	Server Slot 15
Server Slot 4	Server Slot 16
Server Slot 5	Server Slot 17
Server Slot 6	Server Slot 18
Server Slot 7	Server Slot 19
Server Slot 8	Server Slot 20
Server Slot 9	Server Slot 21
Server Slot 10	Server Slot 22
Server Slot 11	Server Slot 23
Server Slot 12	Server Slot 24
Server Slot 13	Server Slot 25

Figure 95 The New 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.

For this option....	Do the following...
Name	Enter a name for the pool. Pool names are 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(.).
High Water Mark	Enter a percentage. 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.
Power Saving Mode	Using the drop-down menu, select the desired **Power Saving Mode**. Enabling the power saving mode sets the standby timer to 60 minutes for all drives in the pool, but only if all drives in the pool are capable of using a standby timer. When the disk pool is idle for 60 minutes, the drives spin-down to conserve power. **Notes:** • Spectra Logic recommends leaving power saving mode **disabled**. • To use this feature, all drives in the storage pool must be power-saving compatible.
Select Drives To Use	Use the drop-down menu to select the number of drives to include in the pool. If your gateway contains more than one type of disk drive, multiple drop-down menus are present, but only one type can be assigned to a pool. Any drive not in a storage pool acts as a global spare. A global spare drive is activated as soon as a drive configured in a storage pool fails.

For this option....	Do the following...
Select Protection Level	Use the radio buttons to select the protection level for the pool. Only one option can be selected. Use the Storage Pool Preview information to compare the fault tolerance and required overhead for each configuration. **None**—The pool is not configured to provide data protection. Any drive failure results in data loss. **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 parity**—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 parity**—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 parity**—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.
Select Optimization Level	Use the slider to maximize either pool capacity or performance, or to mix the two options. Greater capacity means more storage space but slower performance. Higher performance means the pool is faster at reading or writing data with less overall capacity. **Note:** The Storage Pool Preview pane of the New Pool screen changes as you move the slider between Capacity and Performance to show the impact your changes have on the storage pool.
Select Write Performance	Use the drop-down menu to select the number of drives to use to increase write performance when the pool is shared using NFS. This feature is only intended for storage pools with NFS shares and typically has little impact on CIFS share performance.
Select Metadata Performance	Use the drop-down menu to select the number of drives to use to 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. **Note:** Metadata Performance drives can only be selected in multiples of three. **Note:** These drives are permanently part of the storage pool and cannot be removed.

4. Click **Create**. The NAS Pools screen displays. The storage pool is automatically created and is available for use immediately.

Create a Volume

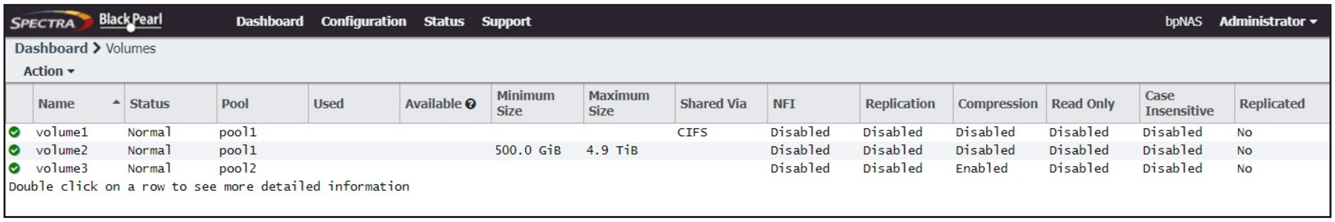
Before you begin using a disk pool to store data, you must create one or more volumes to organize how the information is stored on the pool. After you create a volume, you can share the volume using NFS or CIFS, but you cannot share a volume using more than one method.

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

Note: If you want to configure the volume to use the NFI service (Network File Interface) to automatically transfer files from the NAS storage to the local gateway's storage domains or to a remote BlackPearl Nearline gateway, configure the NFI service before configuring the volume. See Configure the NFI Service on page 235.

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

1. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays.

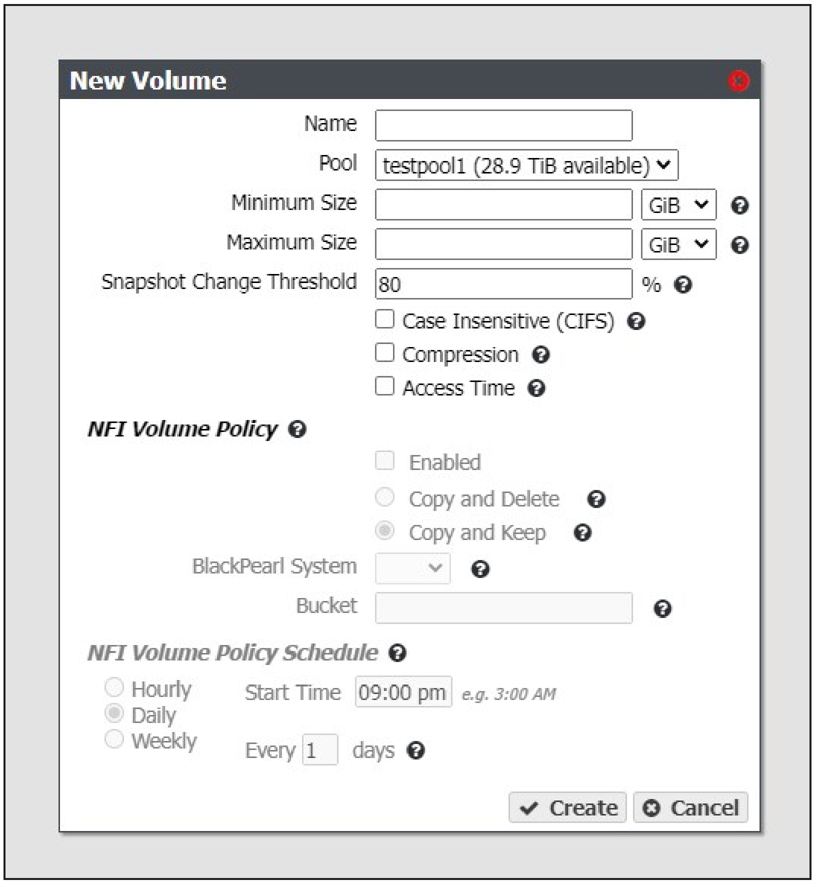


	Name	Status	Pool	Used	Available	Minimum Size	Maximum Size	Shared Via	NFI	Replication	Compression	Read Only	Case Insensitive	Replicated
✓	volume1	Normal	pool1					CIFS	Disabled	Disabled	Disabled	Disabled	Disabled	No
✓	volume2	Normal	pool1			500.0 GiB	4.9 TiB		Disabled	Disabled	Disabled	Disabled	Disabled	No
✓	volume3	Normal	pool2						Disabled	Disabled	Enabled	Disabled	Disabled	No

Double click on a row to see more detailed information

Figure 96 The Volumes screen.

2. Select **Action > New**. The New Volume dialog box displays.



New Volume

Name

Pool testpool1 (28.9 TiB available)

Minimum Size GiB

Maximum Size GiB

Snapshot Change Threshold 80 %

□ Case Insensitive (CIFS)

□ Compression

□ Access Time

NFI Volume Policy

□ Enabled

○ Copy and Delete

● Copy and Keep

BlackPearl System

Bucket

NFI Volume Policy Schedule

○ Hourly

● Daily

○ Weekly

Start Time 09:00 pm *e.g. 3:00 AM*

Every 1 days

Figure 97 The New Volume dialog box.

3. Configure the volume as required for your environment.

For this option....	Do the following...
Name	Enter a name for the new volume. 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.

For this option....	Do the following...
Pool	Select the disk pool on which to create the volume. If there are multiple disk pools configured on the gateway, use the drop-down menu to select the **Pool** where you want to create the volume.
Minimum Size	Select the desired unit size from the drop-down menu and enter a numerical value for the minimum size in the 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.
Maximum Size	Select the desired unit size from the drop-down menu and enter a numerical value for the maximum size in the 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.
Snapshot Change Threshold	Specify 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. • Allowed values are between 0 and 99. **Note:** Spectra Logic recommends configuring the Administrator user to receive emails when a warning event occurs. **Note:** The BlackPearl Nearline 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.
Case Insensitive (CIFS)	If desired, select this option 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.

For this option....	Do the following...
	- Case-insensitive volumes are useful for Commvault® targets. ⚠ CAUTION **DO NOT** enable this setting if you plan to share the volume using NFS. ⚠ CAUTION **DO NOT** enable this setting if you plan to share the volume using NFS.
Compression	If desired, select the check box to enable data compression using ZFS to allow the BlackPearl gateway 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 master nodes.
Access Time	If desired, select the check box to configure the gateway to update the time stamp of a file when it is read from the volume. Selecting **Access Time** may slow performance.

Configure the 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 Nearline gateway. If you do not want to configure NFI for this volume, continue with Step 4 on page 225.

1. Select the **Enabled** check box to enable the **NFI Volume Policy**.
2. Select either **Copy and Keep**, or **Copy and Delete**.

This option....	Does 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. Using the drop-down menu, select a **BlackPearl System** configured in Configure the NFI Service on page 235.

4. Enter the name of the **Bucket** to use to store the data on the BlackPearl 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 159.
- 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.

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.

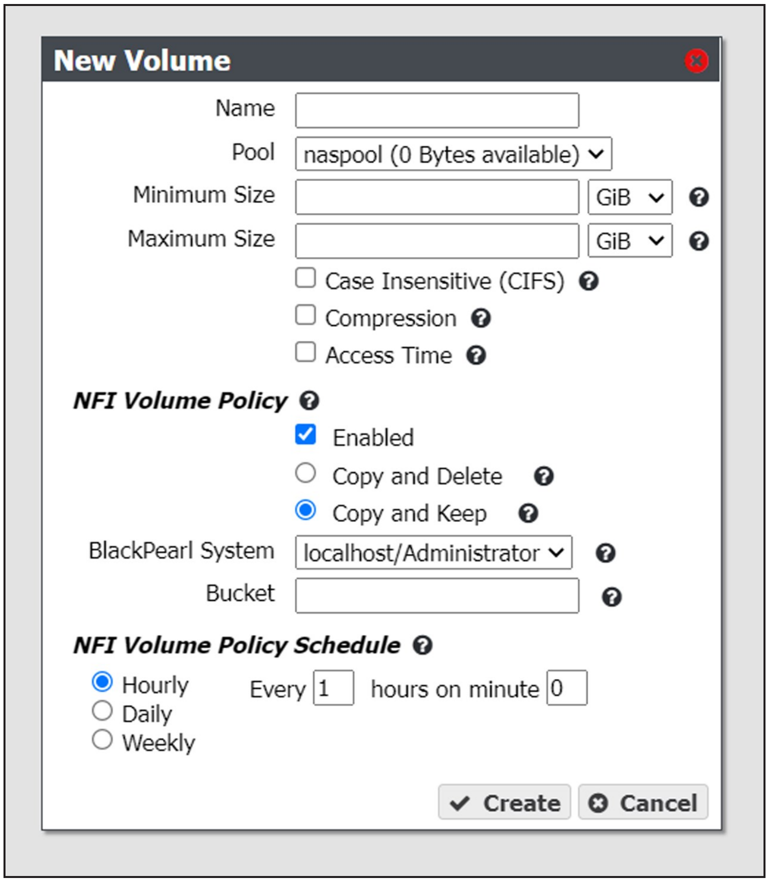
5. Configure the **NFI Volume Policy Schedule**:

   The NFI Volume Policy Schedule transfers data from the NAS volume to a BlackPearl gateway at intervals based on number of hours, days, or days of the week. Decide which interval to use for the schedule and follow the appropriate instructions.

- Create an Hourly Schedule below—Transfer data every selected number of hours.
- Create a Daily Schedule on page 224—Transfer data every selected number of days.
- Create a Weekly Schedule on page 225—Transfer data on certain days of the week.

Create an Hourly Schedule

1. In the New Volume dialog box, select **Hourly** as the interval for the policy schedule. The dialog box changes to display options for the hourly interval setting.



New Volume

Name

Pool naspool (0 Bytes available)

Minimum Size GiB

Maximum Size GiB

□ Case Insensitive (CIFS)

□ Compression

□ Access Time

NFI Volume Policy

☑ Enabled

○ Copy and Delete

● Copy and Keep

BlackPearl System localhost/Administrator

Bucket

NFI Volume Policy Schedule

● Hourly
○ Daily
○ Weekly

Every 1 hours on minute 0

Figure 98 The New Volume dialog box showing the hourly interval options.

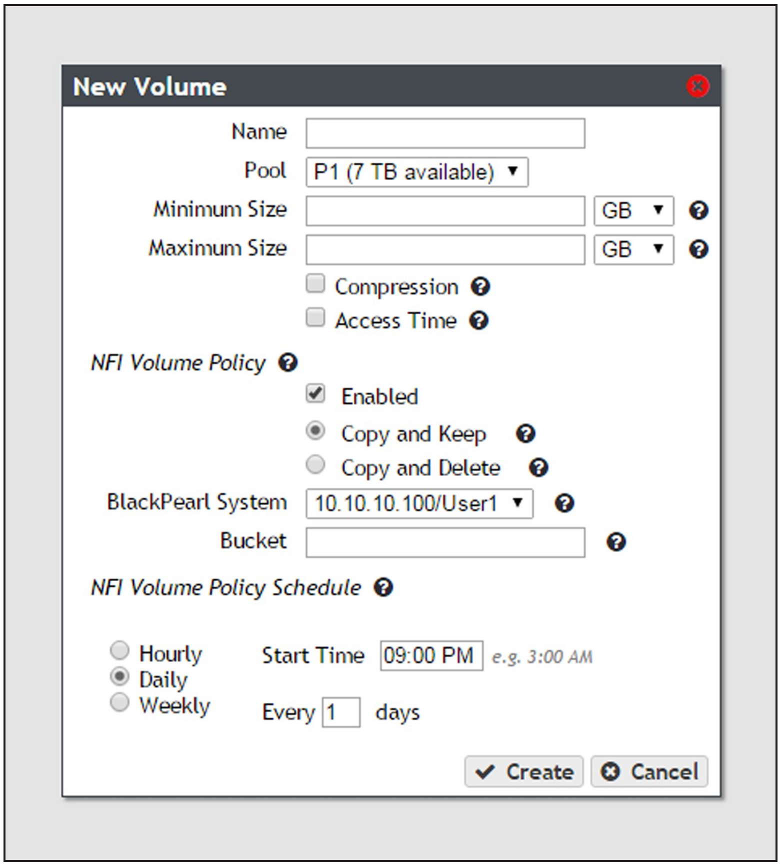
2. Enter numbers for **Every _ hours on minute _**. These values specify the interval in hours between data transfers and the number of minutes after the top of the hour when the job starts. For example, if the values are set to 4 and 15, the NAS volume transfers data to the target BlackPearl gateway every four hours at 15 minutes after the hour. The maximum setting for the **hours** field is 48, where the NAS volume transfers data every two days. The maximum setting for the **minute** field is 59.

Note: Spectra Logic recommends offsetting the minutes after the hour for starting NFI transfers so that there are not a large number of jobs starting at exactly the same time.

3. Continue to Step 4 on page 225.

Create a Daily Schedule

1. In the New Volume dialog box, select **Daily** as the interval for the policy schedule. The dialog box changes to display options for the daily interval setting.



New Volume

Name

Pool P1 (7 TB available) ▼

Minimum Size GB ▼

Maximum Size GB ▼

□ Compression

□ Access Time

NFI Volume Policy

☑ Enabled

● Copy and Keep

○ Copy and Delete

BlackPearl System 10.10.10.100/User1 ▼

Bucket

NFI Volume Policy Schedule

○ Hourly
● Daily
○ Weekly

Start Time 09:00 PM *e.g. 3:00 AM*

Every 1 days

Figure 99 The New Volume dialog box showing the daily interval options.

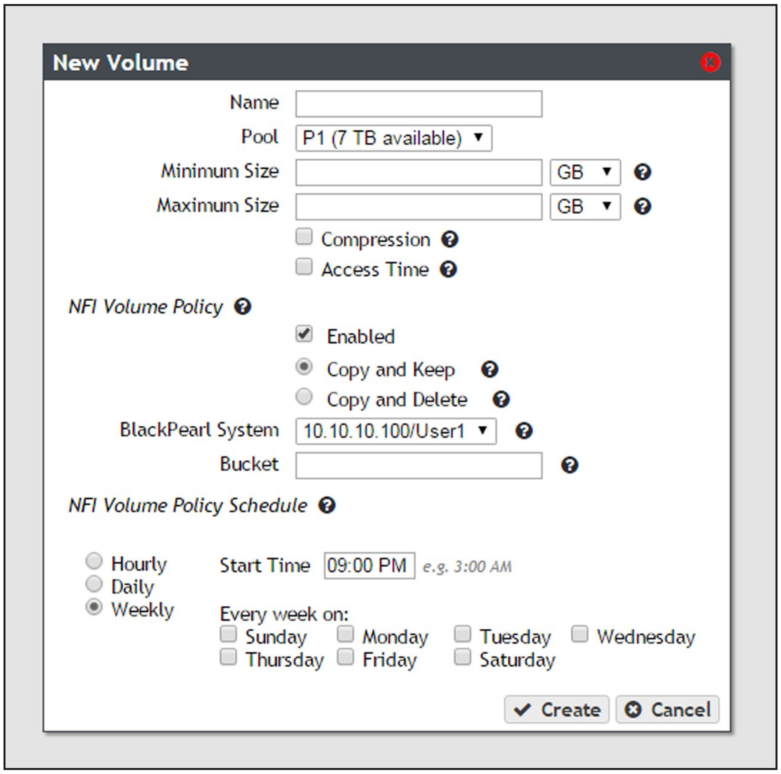
2. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.

3. Enter a number for **Every _ days**. This value specifies the interval, in days, between data transfers to the BlackPearl gateway. The value entered is enumerated from the first day of the month. The schedule resets at the beginning of each month. For example, if this value is set to 2, the NAS volume transfers data every two days, starting with the 1st of the month, at the time specified in Step 2. A value of 30 runs on the 1st of the month, and then again on the 31st of the month (for months that have 31 days). To schedule data transfers on the first of every month, set the interval to 31 days.

4. Continue to Step 4 on page 225.

Create a Weekly Schedule

1. In the New Volume dialog box, select **Weekly** as the interval for the policy schedule. The dialog box changes to display options for the weekly interval setting.



New Volume

Name

Pool: P1 (7 TB available) ▼

Minimum Size: GB ▼

Maximum Size: GB ▼

□ Compression

□ Access Time

NFI Volume Policy

☑ Enabled

● Copy and Keep

○ Copy and Delete

BlackPearl System: 10.10.10.100/User1 ▼

Bucket

NFI Volume Policy Schedule

○ Hourly
○ Daily
● Weekly

Start Time: 09:00 PM *e.g. 3:00 AM*

Every week on:
□ Sunday □ Monday □ Tuesday □ Wednesday
□ Thursday □ Friday □ Saturday

Figure 100 The New Volume dialog box showing the weekly interval options.

2. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.
3. Select one or more days for **Every week on:**. This determines the day(s) of each week the NAS volume copies data to the BlackPearl gateway.
4. Click **Create**. The Volumes screen refreshes to show the new volume.

CREATE A SHARE

After you create one or more volumes, you can share a volume using either the NFS or CIFS service. Decide which method to use for sharing and follow the appropriate instructions below.

- Create a CIFS Share, below
- Create an NFS Share on page 231

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

Create a CIFS Share

Spectra Logic recommends using Active Directory to control access to CIFS shares on the BlackPearl gateways. To do this, continue with Join an Active Directory Domain, below.

However, if your Windows operating system environment does not use Active Directory, you can enable 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 gateway are used to access the CIFS shares when using a Windows workgroup environment. To do this, continue with Enable Local Administrator Status.

Join an Active Directory Domain

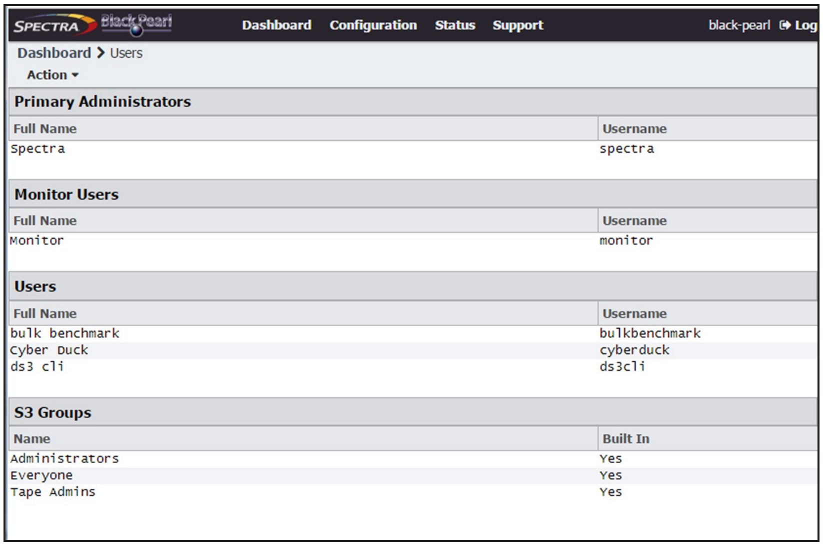
If your Windows environment uses Active Directory, you must join an Active Directory domain before creating a CIFS share. See Configure the Active Directory Service on page 296 for more information. After joining the Active Directory domain, continue with Create a CIFS Share on page 228.

Enable Local Administrator Status

If your Windows environment does not use Active Directory, you must edit a user to enable local administrator status.

> **Note:** Alternatively, you can create a new user with local administrator status. See Create a User on page 82.

1. From the menu bar, select **Configuration > Users**. The Users screen displays.



Primary Administrators

Full Name	Username
Spectra	spectra

Monitor Users

Full Name	Username
Monitor	monitor

Users

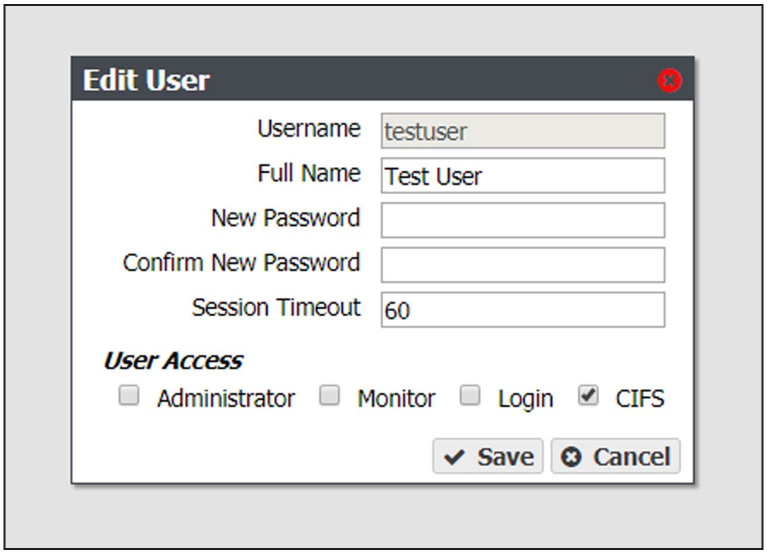
Full Name	Username
bulk benchmark	bulkbenchmark
Cyber Duck	cyberduck
ds3 cli	ds3cli

S3 Groups

Name	Built In
Administrators	Yes
Everyone	Yes
Tape Admins	Yes

Figure 101 The Users screen.

2. Double-click the row for the user for which you want to enable local administrator status, or select the user, and then select **Action > Edit**. The Edit User dialog box displays.



Edit User

Username: testuser

Full Name: Test User

New Password:

Confirm New Password:

Session Timeout: 60

User Access

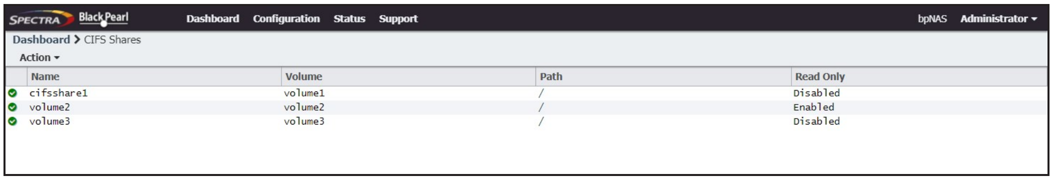
□ Administrator □ Monitor □ Login ☑ CIFS

Figure 102 The Edit User dialog box.

3. Select the **CIFS** checkbox to enable the user to access CIFS shares in a Windows workgroup environment.
4. If desired, change other settings as described in Edit a User on page 323.
5. Click **Save**.

Create a CIFS Share

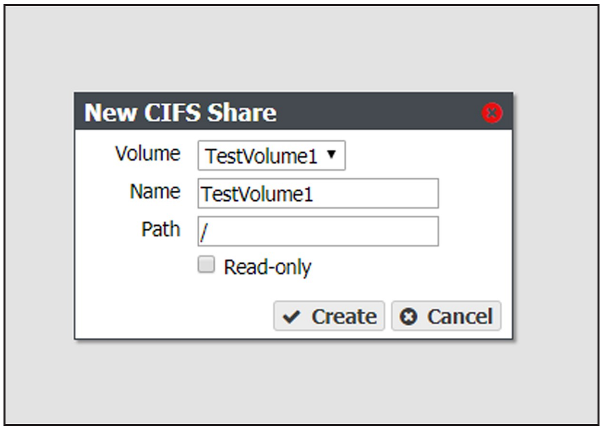
1. From the menu bar, select **Configuration > NAS > Shares > CIFS**. The CIFS Shares screen displays.



Name	Volume	Path	Read Only
cifsshare1	volume1	/	Disabled
volume2	volume2	/	Enabled
volume3	volume3	/	Disabled

Figure 103 The CIFS Shares screen.

2. Select **Action > New**. The New CIFS Share dialog box displays to show the options for creating a new share.



Volume TestVolume1 ▾
Name TestVolume1
Path /
□ Read-only

Figure 104 The New CIFS Share dialog box.

3. Use the drop-down menu to select the **Volume** you want to share.

Note: Creating a CIFS share on a case-sensitive volume reduces performance.

4. Set the **Name** for the CIFS share. This is the name that is displayed in Active Directory configurations.

5. The network address displayed for **Path** is the address of the share you are currently configuring. The default path allows access to the root of the volume.

Notes:

- After creating the CIFS share, you can connect to it using your Windows-based host and create subdirectories in the share. You can then edit the share and use the **Path** field to allow access to specific directories by specifying the exact subdirectory (see Edit a CIFS Share on page 267).

  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.

- If you use a path that starts with two slashes (for example \\path) you are unable to edit permissions after the share is created.

6. If desired, select **Read-only** to configure the CIFS share as read only.

7. Click **Create**. The newly created share is listed on the CIFS Shares screen.

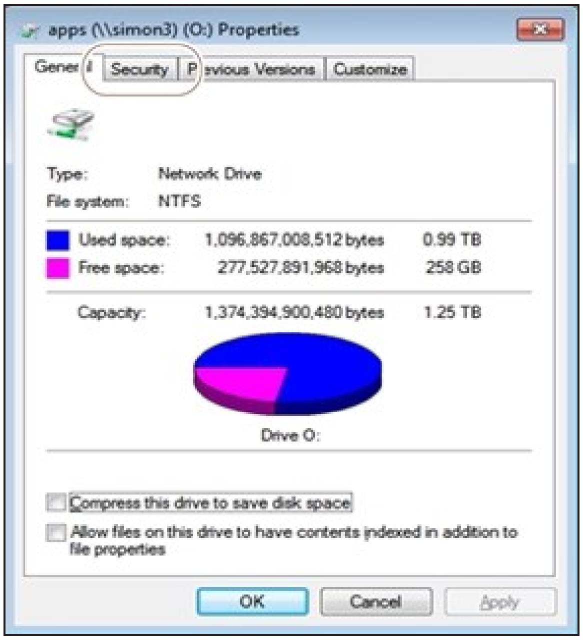
Set Permissions for a CIFS Share

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.



Type: Network Drive

File system: NTFS

🟦	Used space:	1,096,867,008,512 bytes	0.99 TB
🟪	Free space:	277,527,891,968 bytes	258 GB
	Capacity:	1,374,394,900,480 bytes	1.25 TB

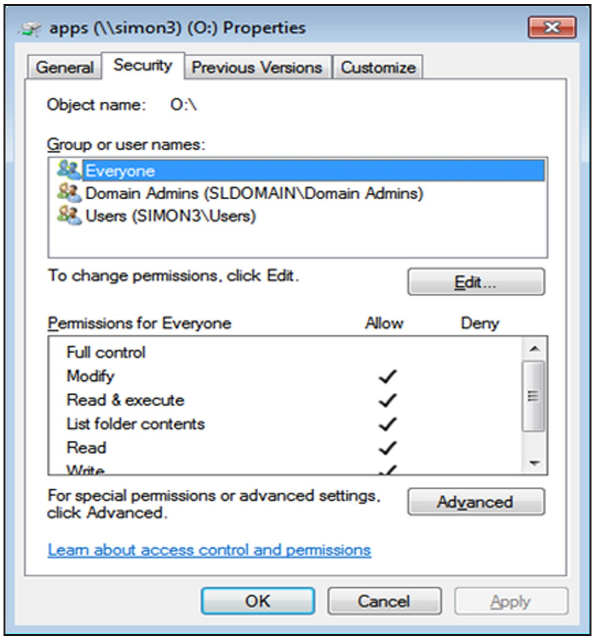
Drive O:

□ Compress this drive to save disk space

□ Allow files on this drive to have contents indexed in addition to file properties

Figure 105 The Properties window.

3. Click **Security**. The Security tab displays.


apps (\\simon3) (O:) Properties
General
Security
Previous Versions
Customize
Edit...
Advanced
Learn about access control and permissions
OK
Cancel
Apply

Object name: O:\

Group or user names:

- Everyone
- Domain Admins (SLDOMAIN\Domain Admins)
- Users (SIMON3\Users)

To change permissions, click Edit.

Permissions for Everyone	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

Figure 106 The Security tab.

4. Add, or remove users, or modify permissions for users as needed for your storage environment.

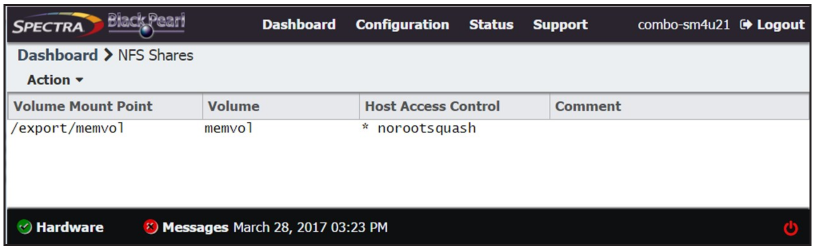
5. Click **OK**.

Note: Starting with BlackPearl OS 5.4, 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.

Create an NFS Share

Use the following steps to create an NFS share.

1. From the menu bar, select **Configuration > NAS > Shares > NFS**. The NFS Shares screen displays.

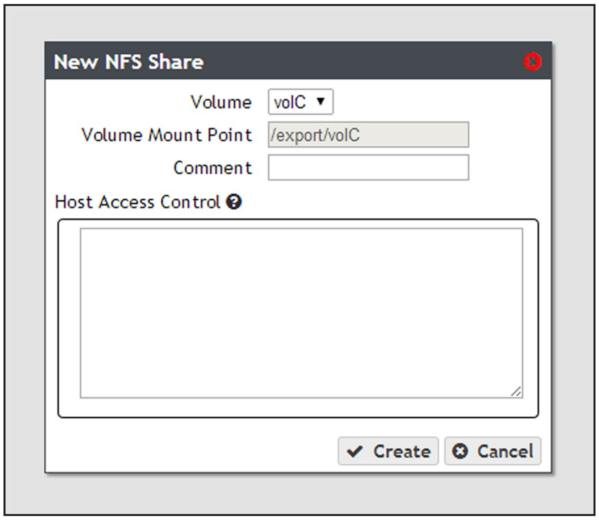


Volume Mount Point	Volume	Host Access Control	Comment
/export/memvol	memvol	* norootsquash	

Messages March 28, 2017 03:23 PM

Figure 107 The NFS Shares screen.

2. Select **Action > New**. The New NFS Share dialog box displays.



Volume: volC ▾

Volume Mount Point: /export/volC

Comment:

Figure 108 The New NFS Share dialog box.

3. Use the drop-down menu to select the **Volume** you want to share.
4. 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.

5. If desired, enter a comment in the **Comment** field. This comment only displays on the BlackPearl Nearline user interface.

6. 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 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	**StandardAccess**—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.

7. Click **Create**. The newly created share is listed on the NFS Shares screen.

Create a Vail S3 Share

Use the following information to create a Vail S3 share.

Note: You can only create a Vail S3 share after registering the BlackPearl gateway to a Vail sphere. See Configure a Vail Sphere on page 310 for more information.

1. From the menu bar, select **Configuration > NAS > Shares > Vail S3**. The Vail S3 Shares screen displays.

2. Select **Action > New**. The New Vail S3 Share dialog box displays.

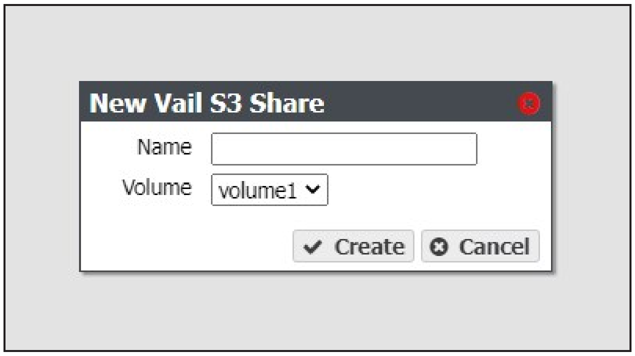


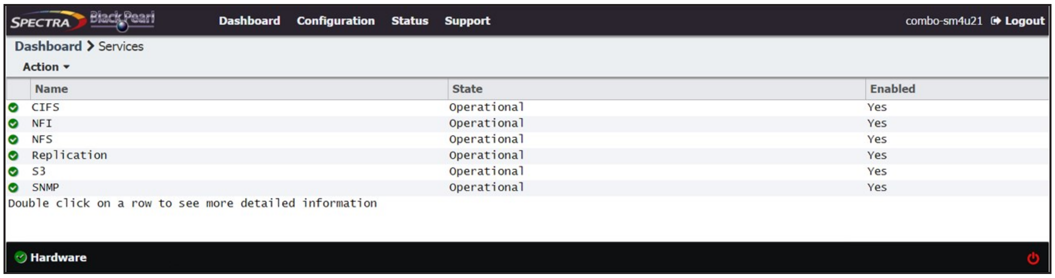
Figure 109 The New Vail S3 Share dialog box.

3. Enter the desired **Name** of the Vail S3 share.
4. Click **Create**.

CONFIGURE NAS SERVICES

The NAS Services - CIFS, NFI, NFS, and Replication - are methods of sharing NAS volumes for use by other computers on the network.

Note: For information about networking services see Configure Network Connections and Settings on page 280.



Name	State	Enabled
CIFS	Operational	Yes
NFI	Operational	Yes
NFS	Operational	Yes
Replication	Operational	Yes
S3	Operational	Yes
SNMP	Operational	Yes

Double click on a row to see more detailed information

Figure 110 The Services screen.

Configure the CIFS Service

There are no configurable settings for the CIFS service at this time, but you can add an advanced parameter, if desired.

Note: For information about using CIFS shares and joining an Active Directory domain, see Create a CIFS Share on page 226.

Add Advanced Parameter

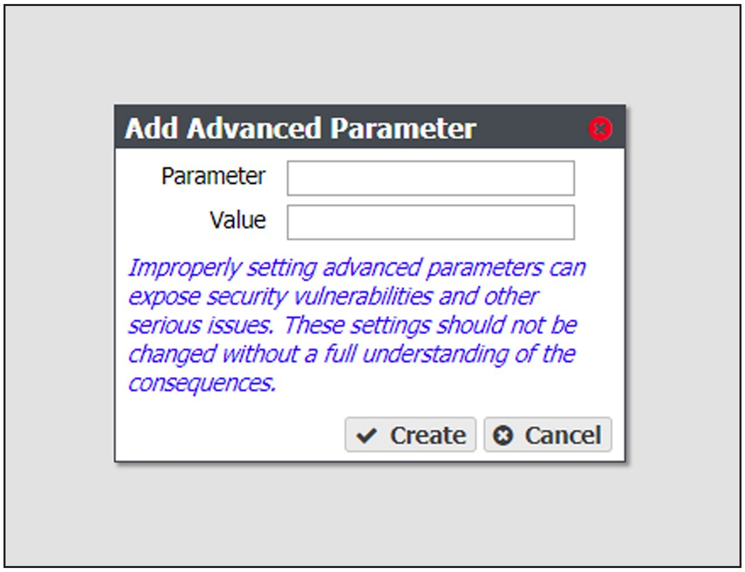
Advanced parameters are used to adjust/set global or share specific Samba parameters.

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.

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. From the menu bar, select **Configuration > Services**. The Services screen displays (see Figure 110 on page 234).
2. Double-click the **CIFS** row, or select the **CIFS** row and select **Action > Show Details**. The CIFS details screen displays.

3. Select **Action > Add Advanced Parameter**. The Add Advanced Parameter dialog box displays.



Improperly setting advanced parameters can expose security vulnerabilities and other serious issues. These settings should not be changed without a full understanding of the consequences.

Figure 111 The Add Advanced Parameter dialog box.

4. Enter the desired **Parameter** and **Value**.
5. Click **Create**.

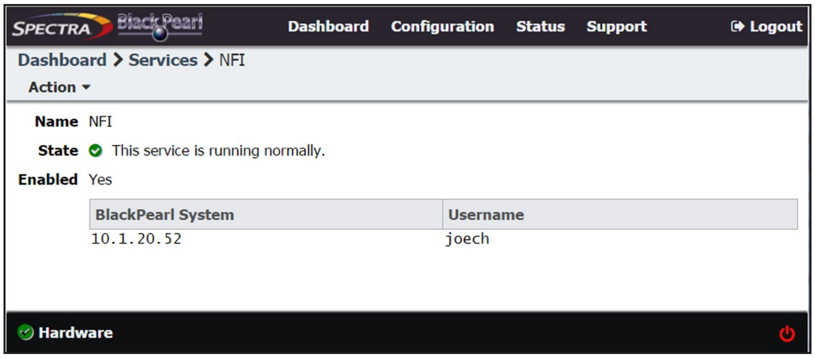
Configure the NFI Service

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 gateway.

> **Note:** This service is only for transferring files from NAS volumes on the gateway to BlackPearl managed object storage. To replicate NAS volumes to other BlackPearl gateways with NAS enabled or to BlackPearl NAS solutions use the NAS replication service (see Configure NAS Services on the previous page).

1. From the menu bar, select **Configuration > Services** to display the Services screen.

2. Double-click the NFI service, or select the service, and then select **Action > Show Details**. The details screen for the NFI service displays.



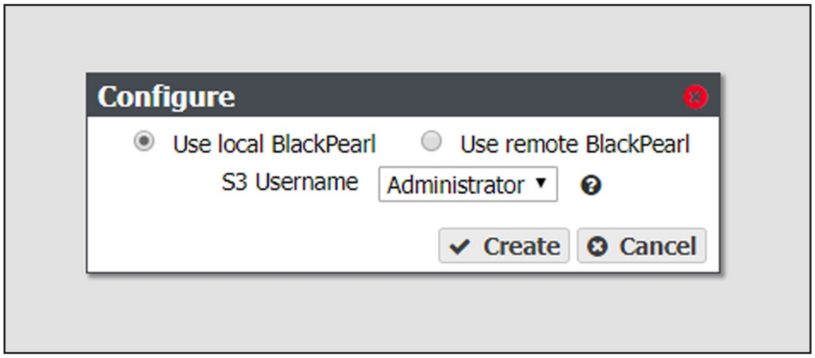
Name NFI
State ✓ This service is running normally.
Enabled Yes

BlackPearl System	Username
10.1.20.52	joech

Figure 112 The NFI service details screen.

3. Select **Action > Configure**. The Configure dialog box displays.

Configure the NFI Service to Use a Local BlackPearl Gateway



● Use local BlackPearl ○ Use remote BlackPearl
S3 Username Administrator

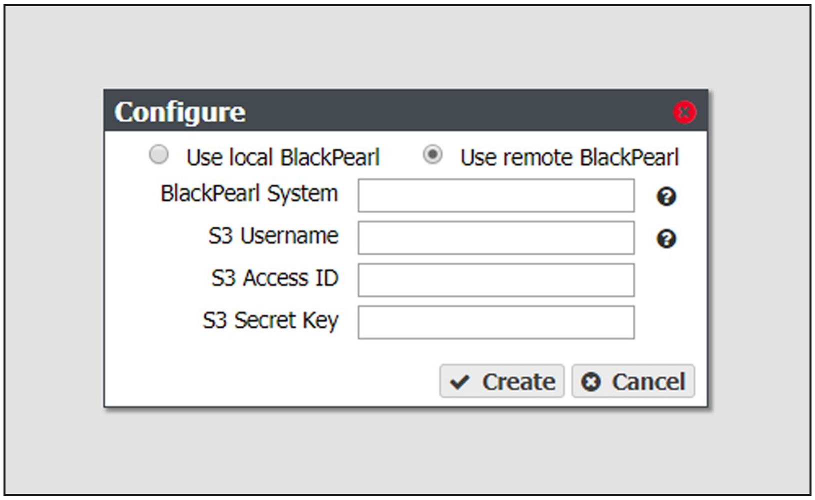
Figure 113 The Configure dialog box for a local BlackPearl gateway.

a. Select **Use local BlackPearl**.

b. Using the drop-down menu, select the **S3 Username** to use for the NFI service.

c. Click **Create**.

Configure the NFI Service to Use a Remote BlackPearl Gateway



Configure

○ Use local BlackPearl ● Use remote BlackPearl

BlackPearl System

S3 Username

S3 Access ID

S3 Secret Key

Figure 114 The Configure dialog box for a BlackPearl gateway.

a. Select **Use remote BlackPearl**.

b. Enter the IP address or the DNS name of the data port of the BlackPearl gateway to which you want to connect in the **BlackPearl System** entry field. If you do not know the IP address or DNS name of the data port on the BlackPearl gateway, select **Configuration > Network** to view the Network screen.

Note: If your BlackPearl gateway is running BlackPearl OS 3.5.3, or later, all BlackPearl NFI targets must use BlackPearl OS 3.3.0, or later.

c. Enter a value for the **S3 Username**. The S3 Username helps you identify the user credentials provided for the BlackPearl gateway.

d. Enter the S3 security credentials of a user previously created on the BlackPearl gateway in the **S3 Access ID** and **S3 Secret Key** fields. See View S3 Credentials on page 86.

e. Click **Create**.

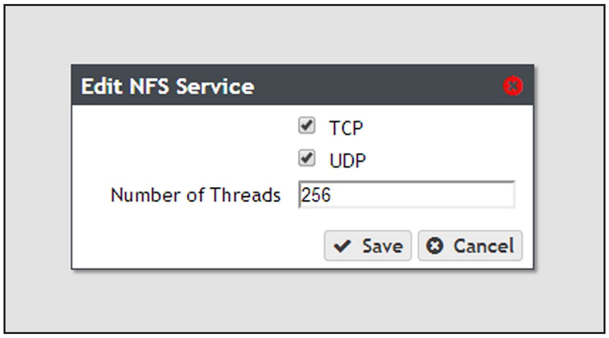
If desired, repeat the appropriate section to configure additional BlackPearl gateways or additional S3 security credentials.

Configure the NFS Service

The BlackPearl user interface lets you configure the transmission protocols and number of threads used by the NFS service. Use the following steps to edit the NFS service.

1. Select **Configuration > Services** to display the Services screen (see Figure 110 on page 234).

2. Double-click the NFS service, or select the service, and then select **Action > Show Details**. The NFS service details screen displays.
3. On the NFS service details screen, select **Action > Edit**. The Edit NFS Service dialog box displays.



Edit NFS Service

☑ TCP

☑ UDP

Number of Threads 256

Figure 115 The Edit NFS Service dialog box.

4. Select or clear the **TCP** and **UDP** transmission protocols to enable or disable them, respectively.
5. Set the number of **Threads** for use by the service.

Note: The default setting is sufficient for most network configurations.

6. Click **Save**.

Configure NAS Replication

If the BlackPearl gateway is on a network with Verde arrays, BlackPearl NAS solutions, or other BlackPearl 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 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. Use the instructions in this section to configure the replication service and to configure volumes for replication.

Notes:

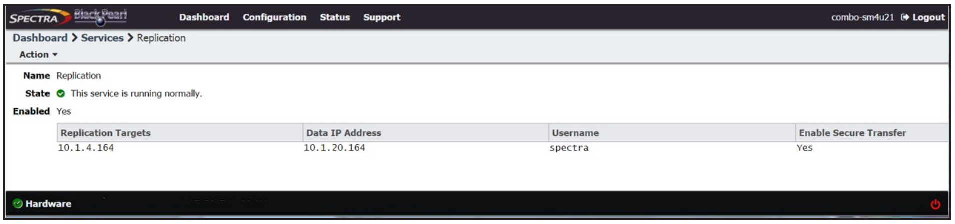
- This replication service is only for replicating NAS volumes on the gateway to other BlackPearl gateways with NAS enabled or BlackPearl NAS solutions. To replicate NAS volumes to BlackPearl managed object storage use NFI (see Configure NAS Replication above).
- There must be enough space on the target 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 Ethernet Ports on page 281).
- 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.

Configure the NAS Replication Service

Note: For both the source gateway and the targets, make sure you have completed the steps in Initial Configuration on page 66.

Use the instruction in this section to configure the NAS replication service.

1. In the source gateway's BlackPearl user interface, select **Configuration > Services** to display the Services screen (see on page 239).
2. Double-click the Replication service, or select the service, and then select **Action > Show Details**. The Replication service details screen displays.



Name Replication

State This service is running normally.

Enabled Yes

Replication Targets	Data IP Address	Username	Enable Secure Transfer
10.1.4.164	10.1.20.164	spectra	Yes

Figure 116 The Replication service details screen.

3. Select **Action > Create**. The Add Replication Target dialog box displays.

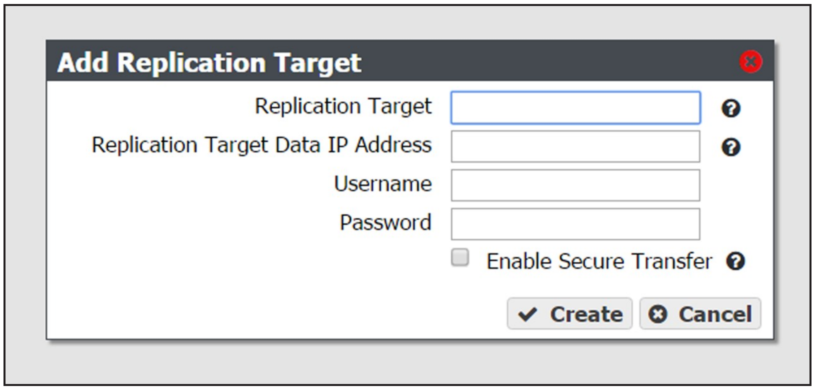


Figure 117 The Add Replication Target dialog box.

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** check box 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 **Save**.

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 213.
3. Create one or more volumes as described in Create a Volume on page 217. You must create one volume on the **target system** for each volume you want to replicate on the **source system**. Otherwise, you can create volumes when performing the steps in Configure Volumes for NAS Replication, below.

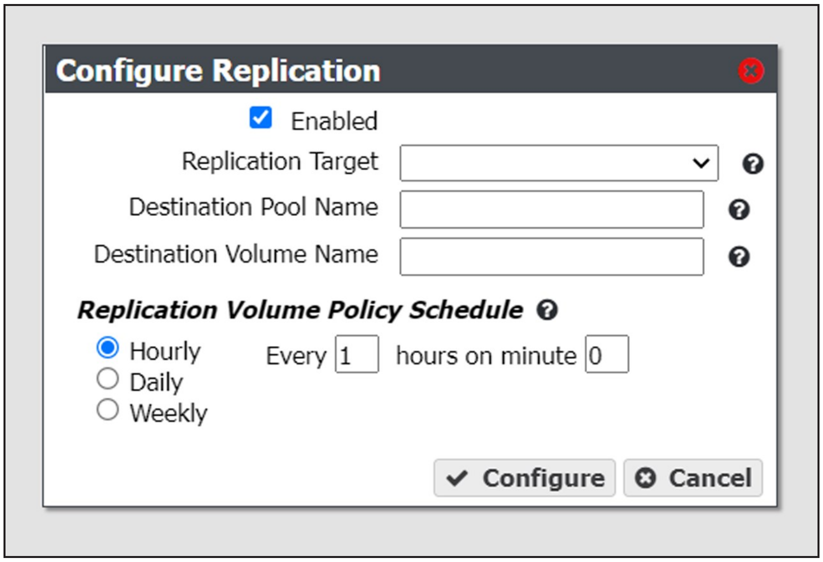
CAUTION You cannot use this volume for normal data storage operations, it can only be used as a replication target. Any data in the specified target volume is deleted each time the source system replicates data to the target system.

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. In the source gateway’s BlackPearl user interface, select **Configuration > NAS > Volumes**. The Volumes screen displays.
2. Double-click the volume name you want to configure to replicate, or select the volume and select **Action > Show Details**. The details screen for the volume displays.

3. Select **Action > Configure Replication**. The Configure Replication dialog box displays.



☑ Enabled

Replication Target

Destination Pool Name

Destination Volume Name

Replication Volume Policy Schedule

● Hourly
○ Daily
○ Weekly

Every 1 hours on minute 0

Figure 118 The Configure Replication dialog box.

4. Select the **Enabled** check box. The options below are unavailable and not configurable until this check box is selected.
5. Select the **Replication Target** from the drop-down menu. The targets are listed by the IP address or hostname entered in Step 4 on page 240. If you only configured the gateway to replicate to a single target, the target is preselected.
6. Enter the name of the storage pool on the target you want to use for replication in the **Destination Pool Name**. This field is case sensitive.
7. Enter the name of a volume that resides on the target storage pool you selected in Step 6 in the **Destination Volume Name** field, or enter the 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.

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.

8. Select the Hourly, Daily, or Weekly radial button for the **Replication Volume Policy Schedule**. The dialog box changes to show the configuration options for your selection. Use one of the sections below to complete the replication configuration for this volume.

- Create an Hourly Schedule below— Replicate data every selected number of hours.
- Create a Daily Schedule on the next page — Replicate data every selected number of days.
- Create a Weekly Schedule on page 245 — Replicate data on certain days of the week.

Create an Hourly Schedule

Creating an hourly schedule for NAS replication is helpful in the case of a ransomware attack. With an hourly snapshot schedule, only data written in the last hour or less can be compromised by the ransomware attack. Data older than one hour can be restored from the most recent snapshot.

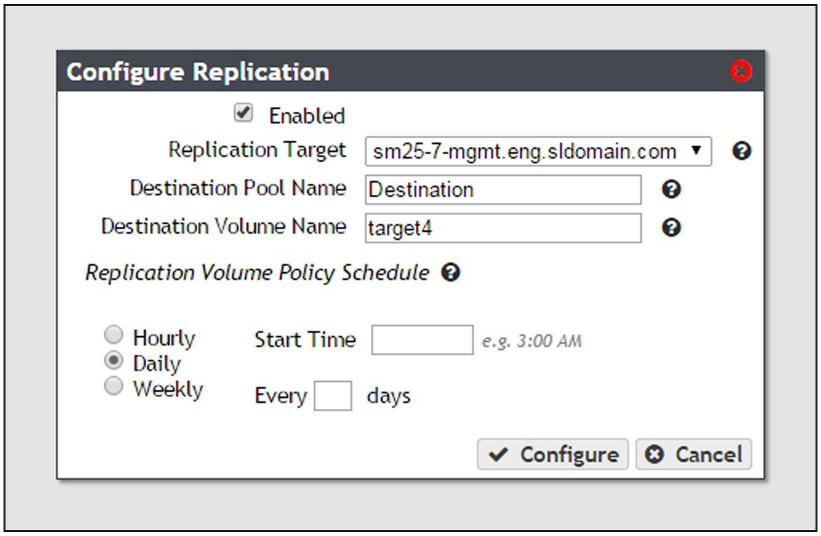
1. Select Hourly as the interval for the replication schedule (see Figure 118 on page 242).
2. Enter numbers for **Every _ hours on minute _**. These values specify the interval in hours between replicating data and the number of minutes after the top of the hour when the job starts. For example, if the values are set to 4 and 15, the data is replicated every four hours at 15 minutes after the hour. The maximum setting for the **hours** field is 48, where the data replicates every two days. The maximum setting for the **minute** field is 59.

Note: Spectra Logic recommends offsetting the minutes after the hour for starting replications so that there are not a large number of jobs starting at exactly the same time.

3. Click **Create**.

Create a Daily Schedule

1. Select **Daily** as the interval for the replication schedule. The dialog box changes to display options for the daily interval setting.



Configure Replication

☑ Enabled

Replication Target: sm25-7-mgmt.eng.sldomain.com ▼

Destination Pool Name: Destination

Destination Volume Name: target4

Replication Volume Policy Schedule

○ Hourly
● Daily
○ Weekly

Start Time: *e.g. 3:00 AM*

Every □ days

Figure 119 The Configure Replication dialog box showing the daily interval options.

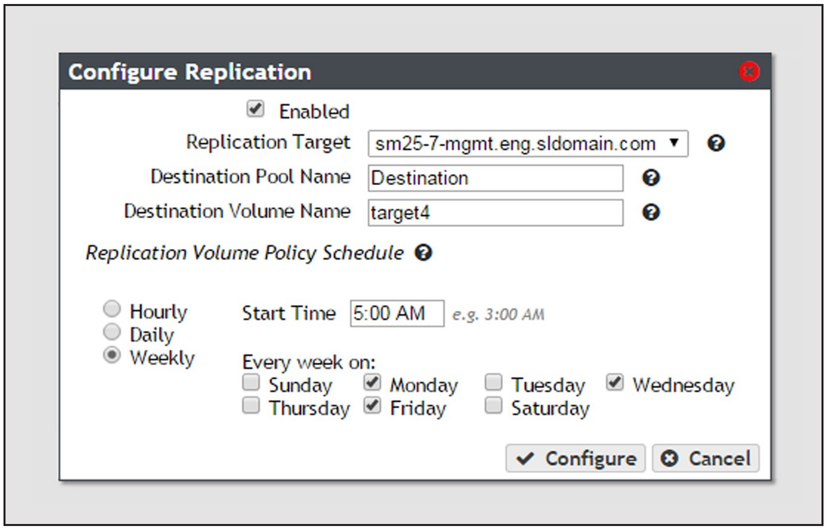
2. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.

3. Enter a number for **Every _ days**. This value specifies the interval, in days, between data replications. The value entered is enumerated from the first day of the month. The schedule resets at the beginning of each month. For example, if this value is set to 2, the NAS volume replicates data every two days, starting with the 1st of the month, at the time specified in Step 2. A value of 30 runs on the 1st of the month, and then again on the 31st of the month (for months that have 31 days). To schedule data replication on the first of every month, set the interval to 31 days.

4. Click **Create**.

Create a Weekly Schedule

1. Select **Weekly** as the interval for the replication schedule. The dialog box changes to display options for the weekly interval setting.



Configure Replication

☑ Enabled

Replication Target: sm25-7-mgmt.eng.sldomain.com ▼

Destination Pool Name: Destination

Destination Volume Name: target4

Replication Volume Policy Schedule

○ Hourly
○ Daily
● Weekly

Start Time: 5:00 AM *e.g. 3:00 AM*

Every week on:
□ Sunday ☑ Monday □ Tuesday ☑ Wednesday
□ Thursday ☑ Friday □ Saturday

Figure 120 The Configure Replication dialog box showing the weekly interval options.

2. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.
3. Select one or more days for **Every week on:**. This determines the day(s) of each week the NAS volume replicates data. For example, based on the selections in Figure 120, the NAS volume replicates data every Monday, Wednesday, and Friday at 5:00 AM.
4. Click **Create**.

Chapter 7 - Managing Network Attached Storage

This chapter describes using the BlackPearl user interface to manage storage pools, volumes, and shares on the gateway after configuring NAS. For initial NAS configuration steps, see Configuring Network Attached Storage on page 211.

Manage Storage Pools **248**

Edit a Storage Pool 248

Expand a Storage Pool 249

Delete a Storage Pool 251

Manage Volumes **252**

Move a Volume 252

Cancel a Volume Move 252

Edit a Volume 253

Delete a Volume 256

Volume Snapshots **257**

Create a Snapshot 257

Create a Snapshot Schedule 259

Delete a Snapshot Schedule 262

Delete Snapshots 262

Restore to a Snapshot 264

Retrieve a Single File from a Snapshot 265

Manage Shares **267**

Edit a CIFS Share 267

Edit an NFS Share 267

Delete a Share 268

Manage NAS Replication **270**

Manually Start NAS Replication 270

Cancel a NAS Replication In Progress 271

Restoring Files from a NAS Replication Target 271

Disable NAS Replication for a Volume 272

Edit the NAS Replication Service 273
Delete the NAS Replication Service Configuration 274
Manage NFI Replication 276
Edit the NFI Service 276
Delete the NFI Service Configuration 276
Manually Starting an NFI Replication 277
Reinitialize NFI Replication 277
Edit the NFI Volume Policy 278
Restoring Files From an NFI Target BlackPearl Gateway 278

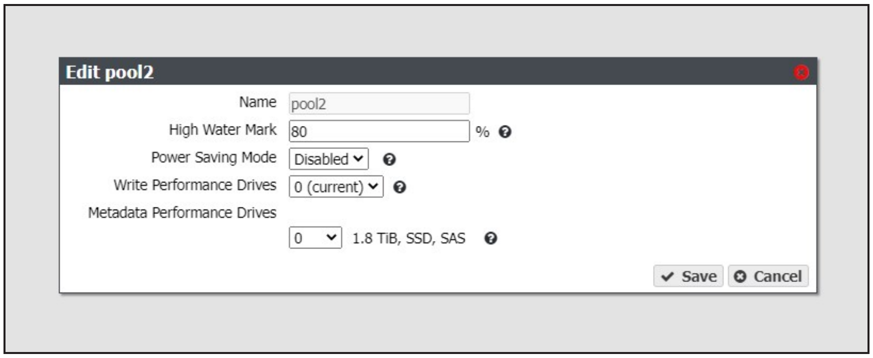
Manage Storage Pools

After creating one or more storage pools, use the instructions in this section to edit, expand, or delete a pool.

Edit a Storage Pool

You can edit an existing storage pool to change the value of the high water mark and the number of write performance drives. Use the following steps to edit a storage pool.

1. From the menu bar, select **Configuration > NAS > Pools**, or click the Pools pane on the Dashboard. The NAS Pools screen displays (see Figure 94 on page 213).
2. Select the pool you want to edit and select **Action > Edit**. The Edit *Pool Name* dialog box displays.



Edit pool2

Name: pool2

High Water Mark: 80 %

Power Saving Mode: Disabled

Write Performance Drives: 0 (current)

Metadata Performance Drives: 0 1.8 TiB, SSD, SAS

Figure 121 The Edit *Pool Name* dialog box.

Note: The **Name** field is unavailable and cannot be changed.

3. If desired, enter a percentage for the **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.
4. If desired, enable or disable **Power Saving Mode** for the storage pool. Enabling this feature configures the standby timer to 60 minutes. When there is no I/O to the storage pool for 60 minutes, the drives in the pool spin down and use minimal power.

Notes:
- Spectra Logic recommends leaving power saving mode **disabled**.
- To use this feature, all drives in the storage pool must be power-saving compatible.

5. If desired, use the **Write Performance Drives** drop-down menu to select the number of write performance drives to allocate to the storage pool.
6. If desired, use the **Metadata Performance Drives** drop-down menu to select the number of metatdata performance drives to allocate to the storage pool.

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

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

7. Click **Save**.

Expand a Storage Pool

You can resize an existing storage pool to include more physical drives present in the gateway. This is useful if you just purchased and installed additional drives.

Additionally, expanding a storage pool is used when you want to include different drive types than the type used when creating the pool.

Notes:
- Drive types must be the same block size.
- The number of drives to be added to the storage pool must match the minimum number of drives for the existing stripe size.
- Self-Encrypting Drives (SED) that are unused can be added to a non-encrypted partition.

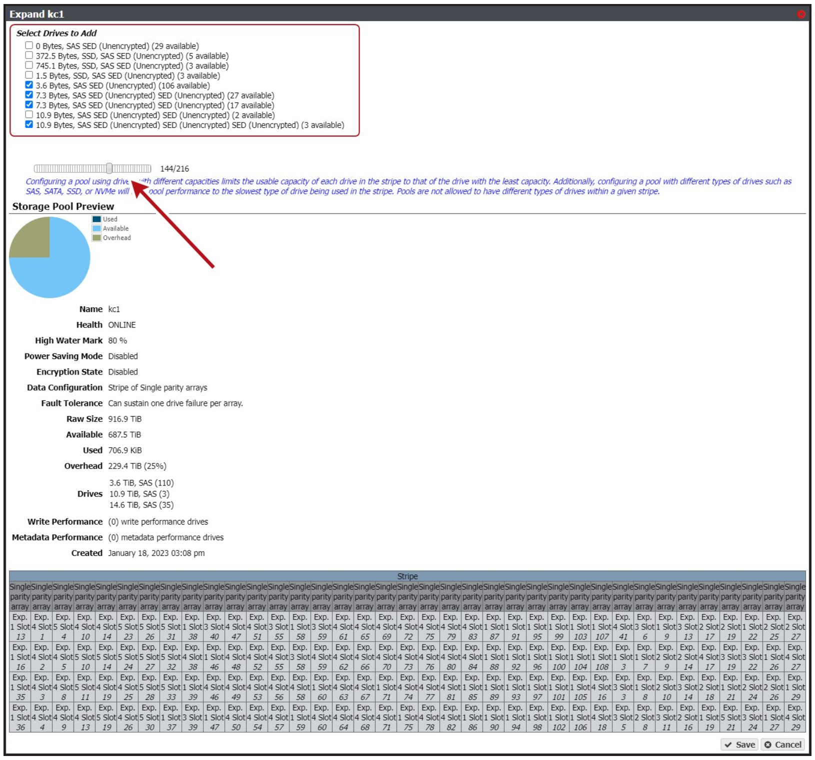
IMPORTANT Contact your solutions architect before including multiple drive types in a storage pool.

IMPORTANT Contact your solutions architect before including multiple drive types in a storage pool.

Use the following steps to expand a storage pool.

1. From the menu bar, select **Configuration > NAS > Pools**, or click the Pools pane on the Dashboard. The NAS Pools screen displays (see Figure 94 on page 213).

2. From the list of existing storage pools, select the storage pool you want to expand, and then select **Action > Expand**. The Expand Pool screen displays options for adding additional drives to the storage pool.



Expand kc1

Select Drives to Add

☐ 0 Bytes, SAS SED (Unencrypted) (29 available)
☐ 372.5 Bytes, SSD, SAS SED (Unencrypted) (5 available)
☐ 745.1 Bytes, SSD, SAS SED (Unencrypted) (3 available)
☐ 1.5 Bytes, SSD, SAS SED (Unencrypted) (3 available)
☑ 3.6 Bytes, SAS SED (Unencrypted) (106 available)
☑ 7.3 Bytes, SAS SED (Unencrypted) SED (Unencrypted) (27 available)
☑ 7.3 Bytes, SAS SED (Unencrypted) SED (Unencrypted) (17 available)
☐ 10.9 Bytes, SAS SED (Unencrypted) SED (Unencrypted) (2 available)
☑ 10.9 Bytes, SAS SED (Unencrypted) SED (Unencrypted) SED (Unencrypted) (3 available)

144/216

Configuring a pool using drive with different capacities limits the usable capacity of each drive in the stripe to that of the drive with the least capacity. Additionally, configuring a pool with different types of drives such as SAS, SATA, SSD, or NVMe will pool performance to the slowest type of drive being used in the stripe. Pools are not allowed to have different types of drives within a given stripe.

Storage Pool Preview

Name	kc1
Health	ONLINE
High Water Mark	80 %
Power Saving Mode	Disabled
Encryption State	Disabled
Data Configuration	Stripe of Single parity arrays
Fault Tolerance	Can sustain one drive failure per array.
Raw Size	916.9 TiB
Available	687.5 TiB
Used	706.9 KiB
Overhead	229.4 TiB (25%)
Drives	3.6 TiB, SAS (110) 10.9 TiB, SAS (3) 14.6 TiB, SAS (35)
Write Performance	(0) write performance drives
Metadata Performance	(0) metadata performance drives
Created	January 18, 2023 03:08 pm

Stripe																																				
Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array	Single parity array
Exp. 1 Slot 13	Exp. 4 Slot 1	Exp. 5 Slot 4	Exp. 4 Slot 10	Exp. 4 Slot 14	Exp. 5 Slot 23	Exp. 5 Slot 26	Exp. 5 Slot 31	Exp. 1 Slot 38	Exp. 3 Slot 40	Exp. 4 Slot 47	Exp. 4 Slot 51	Exp. 3 Slot 55	Exp. 1 Slot 58	Exp. 3 Slot 59	Exp. 4 Slot 61	Exp. 4 Slot 65	Exp. 4 Slot 69	Exp. 4 Slot 72	Exp. 4 Slot 75	Exp. 4 Slot 79	Exp. 4 Slot 83	Exp. 1 Slot 87	Exp. 1 Slot 91	Exp. 1 Slot 95	Exp. 1 Slot 99	Exp. 1 Slot 103	Exp. 1 Slot 107	Exp. 4 Slot 41	Exp. 3 Slot 6	Exp. 1 Slot 9	Exp. 3 Slot 13	Exp. 2 Slot 17	Exp. 2 Slot 19	Exp. 1 Slot 22	Exp. 2 Slot 25	Exp. 2 Slot 27
Exp. 1 Slot 16	Exp. 4 Slot 2	Exp. 4 Slot 5	Exp. 5 Slot 10	Exp. 5 Slot 14	Exp. 5 Slot 24	Exp. 5 Slot 27	Exp. 5 Slot 32	Exp. 4 Slot 38	Exp. 1 Slot 46	Exp. 4 Slot 48	Exp. 4 Slot 52	Exp. 4 Slot 55	Exp. 3 Slot 58	Exp. 4 Slot 59	Exp. 4 Slot 62	Exp. 4 Slot 66	Exp. 4 Slot 70	Exp. 4 Slot 73	Exp. 4 Slot 76	Exp. 4 Slot 80	Exp. 4 Slot 84	Exp. 1 Slot 88	Exp. 1 Slot 92	Exp. 1 Slot 96	Exp. 1 Slot 100	Exp. 1 Slot 104	Exp. 1 Slot 108	Exp. 1 Slot 3	Exp. 1 Slot 7	Exp. 2 Slot 9	Exp. 2 Slot 14	Exp. 4 Slot 17	Exp. 3 Slot 19	Exp. 3 Slot 22	Exp. 1 Slot 26	Exp. 4 Slot 27
Exp. 1 Slot 35	Exp. 4 Slot 3	Exp. 4 Slot 8	Exp. 5 Slot 11	Exp. 4 Slot 19	Exp. 4 Slot 25	Exp. 5 Slot 28	Exp. 5 Slot 33	Exp. 1 Slot 39	Exp. 4 Slot 46	Exp. 4 Slot 49	Exp. 4 Slot 53	Exp. 4 Slot 56	Exp. 4 Slot 58	Exp. 1 Slot 60	Exp. 4 Slot 63	Exp. 4 Slot 67	Exp. 1 Slot 71	Exp. 4 Slot 74	Exp. 4 Slot 77	Exp. 4 Slot 81	Exp. 1 Slot 85	Exp. 1 Slot 89	Exp. 1 Slot 93	Exp. 1 Slot 97	Exp. 1 Slot 101	Exp. 1 Slot 105	Exp. 4 Slot 16	Exp. 3 Slot 3	Exp. 1 Slot 8	Exp. 2 Slot 10	Exp. 3 Slot 14	Exp. 2 Slot 18	Exp. 1 Slot 21	Exp. 2 Slot 24	Exp. 2 Slot 26	Exp. 1 Slot 29
Exp. 1 Slot 36	Exp. 4 Slot 4	Exp. 4 Slot 9	Exp. 4 Slot 13	Exp. 5 Slot 19	Exp. 4 Slot 26	Exp. 5 Slot 30	Exp. 1 Slot 37	Exp. 3 Slot 39	Exp. 1 Slot 47	Exp. 4 Slot 50	Exp. 4 Slot 54	Exp. 4 Slot 57	Exp. 1 Slot 59	Exp. 4 Slot 60	Exp. 4 Slot 64	Exp. 4 Slot 68	Exp. 4 Slot 71	Exp. 1 Slot 75	Exp. 4 Slot 78	Exp. 4 Slot 82	Exp. 1 Slot 86	Exp. 1 Slot 90	Exp. 1 Slot 94	Exp. 1 Slot 98	Exp. 1 Slot 102	Exp. 1 Slot 106	Exp. 4 Slot 18	Exp. 3 Slot 5	Exp. 2 Slot 8	Exp. 3 Slot 11	Exp. 2 Slot 16	Exp. 1 Slot 19	Exp. 5 Slot 21	Exp. 3 Slot 24	Exp. 1 Slot 27	Exp. 4 Slot 29

Figure 122 The Expand Pool screen.

3. Select the check box next to the type of drive(s) you want to add to the storage pool. By default, the check box for any drive type present in the gateway is automatically selected.

4. Use the slider to increase the number of drives to use in the storage pool. As you make changes, the graphics beneath the slider update to show the impact your changes have on the storage pool.

Note: If you are mixing drive types, the number of drives to be added to the storage pool must match the minimum number of drives for the existing stripe size.

5. When you are satisfied with the new configuration, click **Save**. It may take up to three minutes for pool expansion to complete. Multiple expansions of the same storage pool may increase the time to complete.

Note: If you are adding self-encrypting drives to an encrypted storage pool, the drives are automatically encrypted and then added to the storage pool.

Delete a Storage Pool

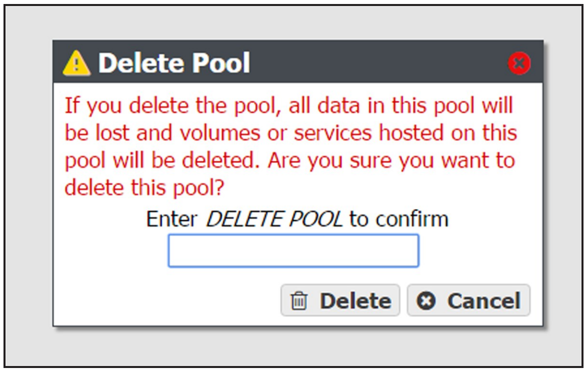
If you want to create a new storage pool and existing storage pools use all of the available drives, you must delete an existing storage pool to make drives available for the new storage pool.

CAUTION When you delete a storage pool, all data on it is lost. If you want to keep the data, migrate it to another location before deleting the pool.

CAUTION When you delete a storage pool, all data on it is lost. If you want to keep the data, migrate it to another location before deleting the pool.

Use the following steps to delete a storage pool.

1. From the menu bar, select **Configuration > NAS > Pools**, or click the Pools pane on the Dashboard. The NAS Pools screen displays (see Figure 94 on page 213).
2. From the list of existing storage pools, select the storage pool you want to delete, and then select **Action > Delete**. A dialog box displays asking you to confirm the deletion.



Delete Pool

If you delete the pool, all data in this pool will be lost and volumes or services hosted on this pool will be deleted. Are you sure you want to delete this pool?

Enter *DELETE POOL* to confirm

Figure 123 Confirm the storage pool deletion.

3. Type `DELETE`in the entry field and click **Delete** to delete the storage pool. Expanded pools may take up three minutes to delete.

Note: If you deleted an encrypted pool, the drives in the pool are automatically erased and reset.

4. If desired, create a new storage pool that includes the disks no longer in use, as described in Create a NAS Storage Pool on page 213.

MANAGE VOLUMES

After creating one or more volumes, use the instructions in this section to move, edit, or delete a volume.

Move a Volume

If desired, you can move a volume from one storage pool to another. There must be sufficient space for the volume on the destination storage pool.

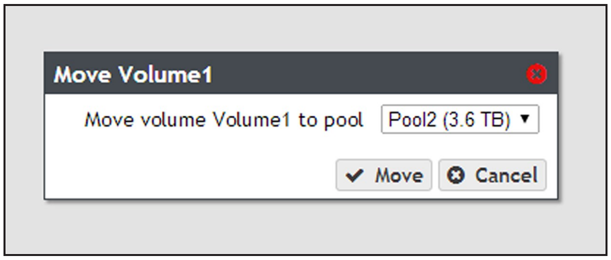
IMPORTANT Access to CIFS shares is lost when moving the share while simultaneously transferring data to or from the share.

IMPORTANT Access to CIFS shares is lost when moving the share while simultaneously transferring data to or from the share.

Note: There is a decrease in performance in file storage operations on a volume that is being moved.

Use the following steps to move a volume to a different storage pool.

1. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 96 on page 217).
2. Select the volume you want to move to a different storage pool, and then select **Action > Move**. The Move Volume dialog box displays.
3. Use the drop-down menu to select the destination pool for the volume.



Move Volume1

Move volume Volume1 to pool Pool2 (3.6 TB) ▾

Figure 124 Select the destination pool for the volume.

4. Click **Move**. The volume is moved to the selected pool.

Cancel a Volume Move

If desired, you can cancel the move of a volume from one storage pool to another.

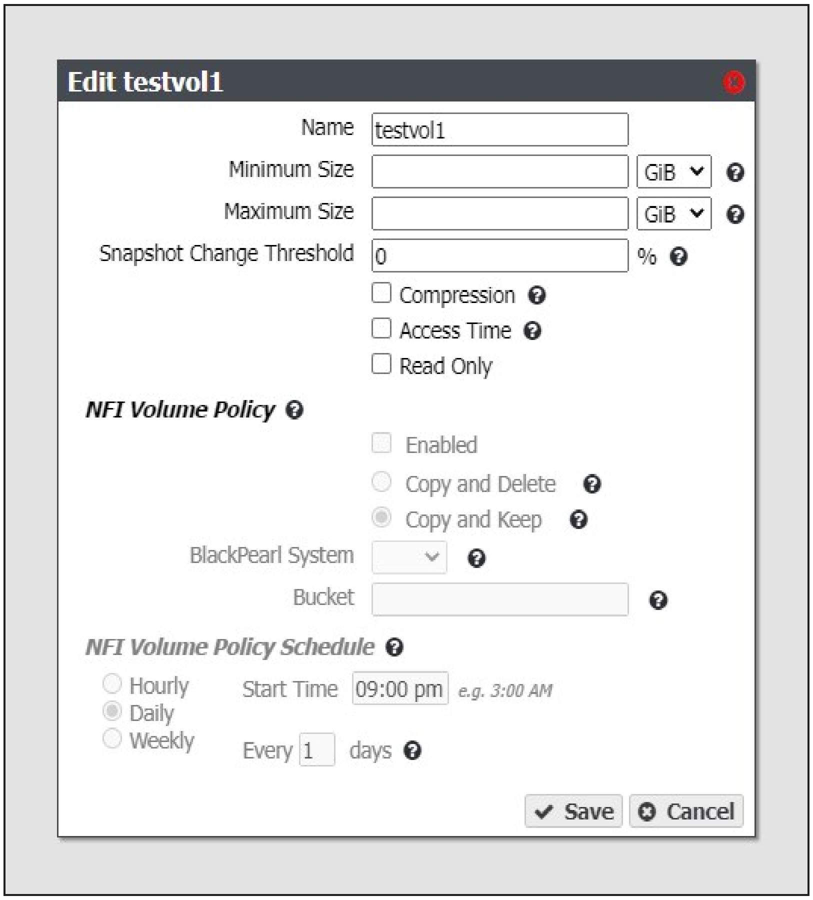
1. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 96 on page 217).
2. Select the volume you want to cancel moving to a different storage pool, and then select **Action > Cancel Move**. The Cancel Move Volume dialog box displays.
3. Click **Cancel Move** to cancel the in-progress volume move.

Note: The data on the target pool is deleted. Data on the source pool is unaffected and persists on the source pool after canceling the move.

Edit a Volume

After creating a volume, you can edit it to change the volume configuration. Use the following steps to edit a volume.

1. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 96 on page 217).
2. Double-click the volume you want to edit, or select the volume and then select **Action > Edit**. The Edit *Volume name* screen displays.



Edit testvol1

Name: testvol1

Minimum Size: GiB

Maximum Size: GiB

Snapshot Change Threshold: 0 %

□ Compression

□ Access Time

□ Read Only

NFI Volume Policy

□ Enabled

○ Copy and Delete

● Copy and Keep

BlackPearl System:

Bucket:

NFI Volume Policy Schedule

○ Hourly

● Daily

○ Weekly

Start Time: 09:00 pm e.g. 3:00 AM

Every 1 days

Figure 125 The Edit Volume screen.

3. Change the configuration of the volume as required for your environment.

For this option....	Do the following...
Name	Enter a new name for the volume. Volume names are limited to 62 characters or fewer. **IMPORTANT** **DO NOT**rename a volume that is used by the Spectra Vail application. **IMPORTANT** **DO NOT**rename a volume that is used by the Spectra Vail application. **Notes:** • The combined storage 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. • If you change the name of a volume that is being shared, the share point is maintained after the volume name change.
Minimum Size	Select the desired unit size from the drop-down menu and enter a numerical value for the minimum size in the 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 storage pool. If there is insufficient space available, saving the modified volume fails.
Maximum Size	• Select the desired unit size from the drop-down menu and enter a numerical value for the maximum size in the text box to the left of the unit size drop-down menu. **Notes:** • The maximum size must be greater than the current amount of used space on the volume. • Volumes are thin provisioned, so it is possible for the combined allocated maximum storage of all volumes to exceed the physical space available.

For this option....	Do the following...
Snapshot Change Threshold	Specify 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. • Allowed values are between 0 and 99. **Note:** Spectra Logic recommends configuring the Administrator user to receive emails when a warning event occurs. **Note:** The BlackPearl Nearline gateway uses unique data to detect the specified percentage change when data is deleted. If you enable compression for this volume, it is possible that the volume may contain compressed data that is not unique. When data is deleted it may not reach the specified threshold, which does not trigger a warning when the deletion occurs.
Compressio n	If desired, select the check box to enable the gateway to compress data stored in NAS. If desired, select the check box to enable data compression using ZFS to allow the BlackPearl gateway 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 filesdepends 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 master nodes. **Note:** Changing the compression setting only affects data written to the volume after the compression setting is changed. It does not affect data already on the volume.
Access Time	If desired, select the check box to configure the gateway to update the time stamp of a file when it is read from the volume. Selecting **Access Time** may slow performance.
Read Only	If desired, select the check box to configure the volume so that data can be read, but not written to the volume.
NFI Volume Policy	If desired, edit the NFI Volume policy configurations. See Configure the NFI Volume Policy on page 221.

4. Click **Save**.

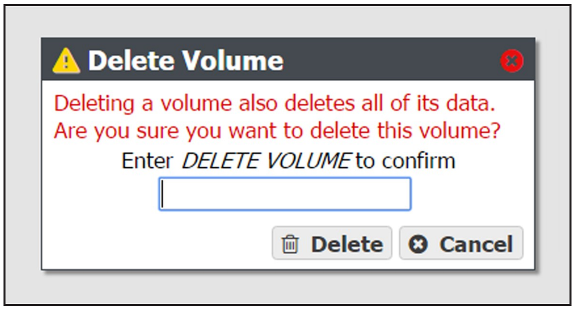
Delete a Volume

Use the following steps to delete a volume.

1. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The **Volumes screen** displays (see Figure 96 on page 217).
2. Select the volume you want to delete and then select **Action > Delete**. A dialog box displays asking you to codsfsdfsdfdsfsnfirm the deletion.

CAUTION Deleting a volumes deletes all data in the volume. This action cannot be undone.

CAUTION Deleting a volumes deletes all data in the volume. This action cannot be undone.



Delete Volume

Deleting a volume also deletes all of its data.
Are you sure you want to delete this volume?
Enter *DELETE VOLUME* to confirm

Figure 126 Confirm the volume deletion.

3. Type `DELETE VOLUME` in the entry field and click **Delete** to delete the volume.

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 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.

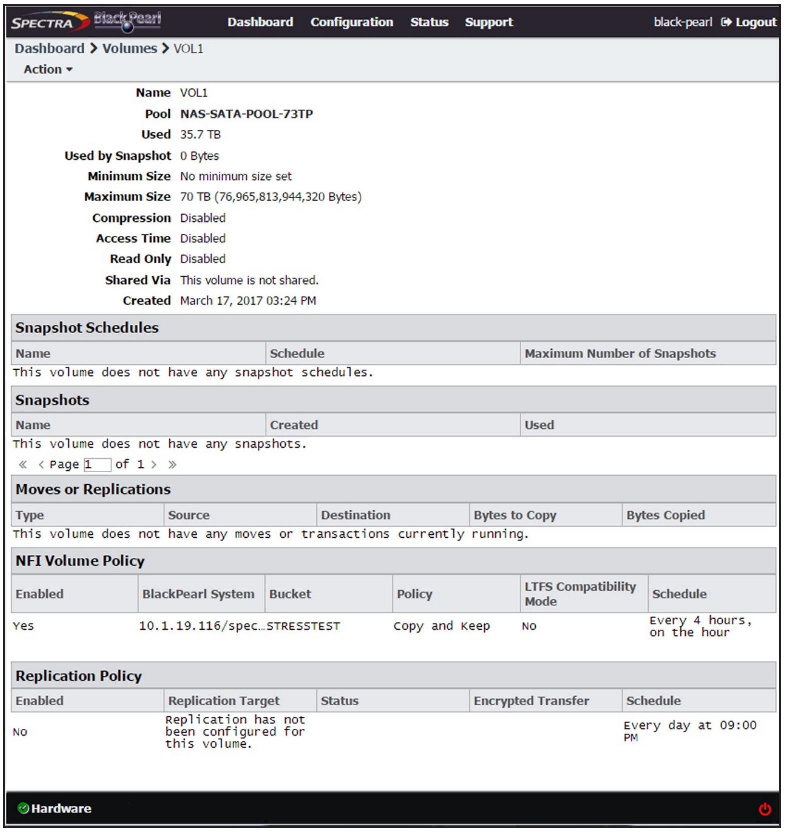
For example, if you write 100 GB to the volume, and then make a snapshot of that data, the snapshot is 0 bytes in size, as it simply points to the existing data. However, if that 100 GB is deleted, the snapshot grows to 100 GB, because it must retain the data. When the snapshot containing the 100 GB 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

Use the following steps to create a snapshot.

1. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 96 on page 217).

2. Double-click the volume you want to use to create a snapshot, or select the volume, and then select **Action > Show Details**. The details screen for that volume displays.



Name	VOL1
Pool	NAS-SATA-POOL-73TP
Used	35.7 TB
Used by Snapshot	0 Bytes
Minimum Size	No minimum size set
Maximum Size	70 TB (76,965,813,944,320 Bytes)
Compression	Disabled
Access Time	Disabled
Read Only	Disabled
Shared Via	This volume is not shared.
Created	March 17, 2017 03:24 PM

Snapshot Schedules

Name	Schedule	Maximum Number of Snapshots
This volume does not have any snapshot schedules.		

Snapshots

Name	Created	Used
This volume does not have any snapshots.		

« ‹ Page 1 of 1 › »

Moves or Replications

Type	Source	Destination	Bytes to Copy	Bytes Copied
This volume does not have any moves or transactions currently running.				

NFI Volume Policy

Enabled	BlackPearl System	Bucket	Policy	LTFS Compatibility Mode	Schedule
Yes	10.1.19.116/spec…	STRESSTEST	Copy and Keep	No	Every 4 hours, on the hour

Replication Policy

Enabled	Replication Target	Status	Encrypted Transfer	Schedule
No	Replication has not been configured for this volume.			Every day at 09:00 PM

Figure 127 The Volume details screen.

3. On the Volume details screen, select **Action > New Snapshot**. The New Snapshot dialog box displays.

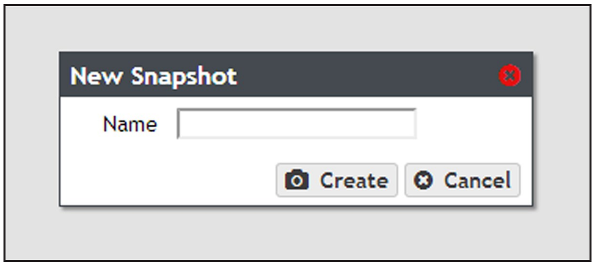


Figure 128 The New Snapshot dialog box.

4. Enter a name for the snapshot in the **Name** field.

5. Click **Create**. The Volume details screen displays showing the newly created snapshot.

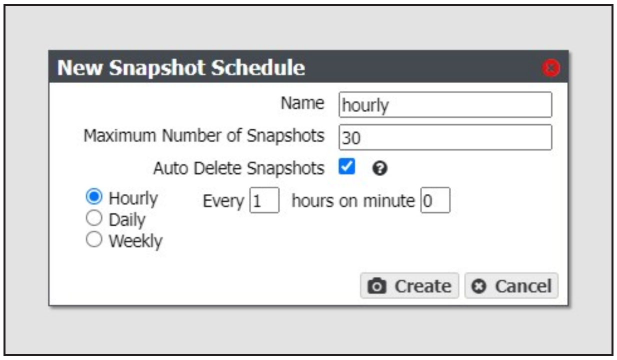
Create a Snapshot Schedule

Snapshot schedules can be configured at intervals based on hours, number of days, or days of the week. Decide which interval to use for the schedule and follow the appropriate instructions.

- Create an Hourly Schedule below — Create snapshots every selected number of hours.
- Create a Daily Schedule on the next page — Create snapshots every selected number of days.
- Create a Weekly Schedule on page 261 — Create snapshots on certain days of the week.

Create an Hourly Schedule

1. On the Volume details screen (see Figure 127 on page 258), select **Action > New Snapshot Schedule**. The New Snapshot Schedule dialog box displays.
2. Select **Hourly** as the interval for the snapshot schedule. The dialog box changes to display options for the hourly interval setting.



New Snapshot Schedule

Name: hourly

Maximum Number of Snapshots: 30

Auto Delete Snapshots ☑

● Hourly
○ Daily
○ Weekly

Every 1 hours on minute 0

Figure 129 The New Snapshot Schedule dialog box showing the hourly interval options.

3. Change the default name of the snapshot schedule, if desired.

Note: Snapshot schedule names must be unique.

4. Enter a number for the **Maximum Number of Snapshots**. When the maximum number is reached, the gateway deletes the oldest snapshot.
5. If desired, select **Auto Delete Snapshots** to allow the BlackPearl Nearline gateway to automatically delete the oldest snapshot when the gateway reaches the specified **Maximum Number of Snapshots**. If you do not enable this feature, when the system reaches the specified **Maximum Number of Snapshots**, the gateway stops creating snapshots until snapshots are manually deleted.

Note: Spectra Logic recommends enabling this feature.

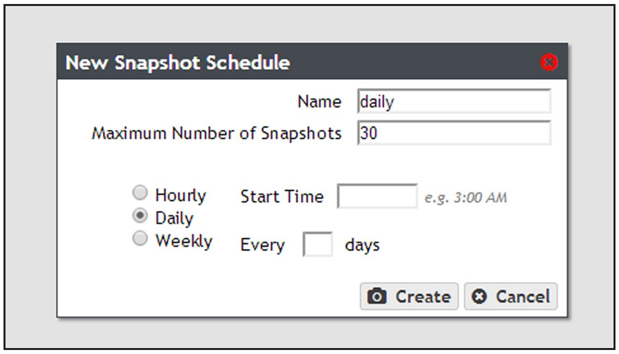
6. Enter numbers for **Every _ hours on minute _**. These values specify the interval in hours between generating snapshots and the number of minutes after the top of the hour when the job starts. For example, if the values are set to 4 and 15, the NAS volume creates a snapshot every four hours at 15 minutes after the hour. The maximum setting for the **hours** field is 48, where the NAS volume creates a snapshot every two days. The maximum setting for the **minute** field is 59.

Note: Spectra Logic recommends offsetting the minutes after the hour for starting snapshots so that there are not a large number of jobs starting at exactly the same time.

7. Click **Create**.

Create a Daily Schedule

1. On the Volume details screen (see Figure 127 on page 258), select **Action > New Snapshot Schedule**. The New Snapshot Schedule dialog box displays.
2. Select **Daily** as the interval for the snapshot schedule. The dialog box changes to display options for the daily interval setting.



New Snapshot Schedule

Name: daily

Maximum Number of Snapshots: 30

○ Hourly
● Daily
○ Weekly

Start Time: e.g. 3:00 AM

Every days

Figure 130 The New Snapshot Schedule dialog box showing the daily interval options.

3. Change the default name of the snapshot schedule, if desired.

Note: Snapshot schedule names must be unique.

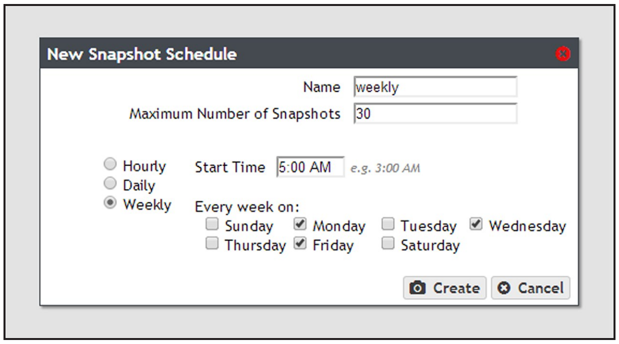
4. Enter a number for the **Maximum Number of Snapshots**. When the maximum number is reached, the gateway deletes the oldest snapshot.
5. If desired, select **Auto Delete Snapshots** to allow the BlackPearl Nearline gateway to automatically delete the oldest snapshot when the gateway reaches the specified **Maximum Number of Snapshots**. If you do not enable this feature, when the system reaches the specified **Maximum Number of Snapshots**, the gateway stops creating snapshots until snapshots are manually deleted.

Note: Spectra Logic recommends enabling this feature.

6. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.
7. Enter a number for **Every _ days**. This value specifies the interval, in days, between generating snapshots. The value entered is enumerated from the first day of the month. The schedule resets at the beginning of each month. For example, if this value is set to 2, the NAS volume creates a snapshot every two days, starting with the 1st of the month, at the time specified in Step 6. A value of 30 runs on the 1st of the month, and then again on the 31st of the month (for months that have 31 days). To schedule generating snapshots on the first of every month, set the interval to 31 days.
8. Click **Create**.

Create a Weekly Schedule

1. On the Volume details screen (see Figure 127 on page 258), select **Action > New Snapshot Schedule**. The New Snapshot Schedule dialog box displays.
2. Select **Weekly** as the interval for the snapshot schedule. The dialog box changes to display options for the weekly interval setting.



New Snapshot Schedule

Name: weekly

Maximum Number of Snapshots: 30

○ Hourly
○ Daily
● Weekly

Start Time: 5:00 AM *e.g. 3:00 AM*

Every week on:
☐ Sunday ☑ Monday ☐ Tuesday ☑ Wednesday
☐ Thursday ☑ Friday ☐ Saturday

Figure 131 The New Snapshot Schedule dialog box showing the weekly interval options.

3. Change the default name of the snapshot schedule, if desired.

Note: Snapshot schedule names must be unique.

4. Enter a number for the **Maximum Number of Snapshots**. When the maximum number is reached, the gateway deletes the oldest snapshot.
5. If desired, select **Auto Delete Snapshots** to allow the BlackPearl Nearline gateway to automatically delete the oldest snapshot when the gateway reaches the specified **Maximum Number of Snapshots**. If you do not enable this feature, when the system reaches the specified **Maximum Number of Snapshots**, the gateway stops creating snapshots until snapshots are manually deleted.

Note: Spectra Logic recommends enabling this feature.

6. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.
7. Select one or more days for **Every week on:**. This determines the day(s) of each week the NAS volume generates snapshots. For example, based on the selections in Figure 131, the NAS volume creates a snapshot every Monday, Wednesday, and Friday at 5:00 AM.
8. Click **Create**.

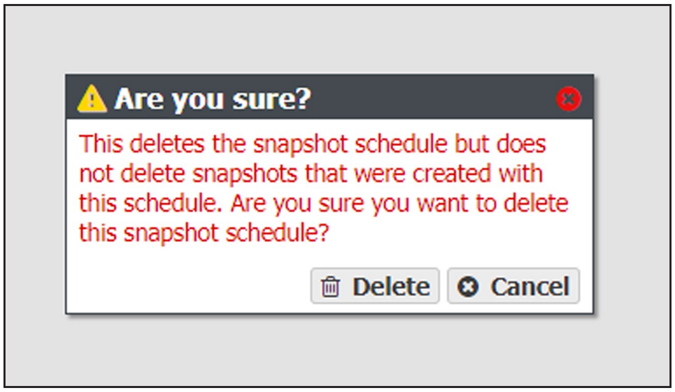
Delete a Snapshot Schedule

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 below.

Use the instructions in this section to delete a snapshot schedule.

1. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 96 on page 217).
2. Double-click the volume for which you want to delete the snapshot schedule, or select the volume, and then select **Action > Show Details**. The details screen for that volume displays.
3. Select the snapshot schedule you want to delete and select **Action > Delete Snapshot Schedule**. A confirmation window displays.



Are you sure?

This deletes the snapshot schedule but does not delete snapshots that were created with this schedule. Are you sure you want to delete this snapshot schedule?

Figure 132 Confirm the snapshot schedule deletion.

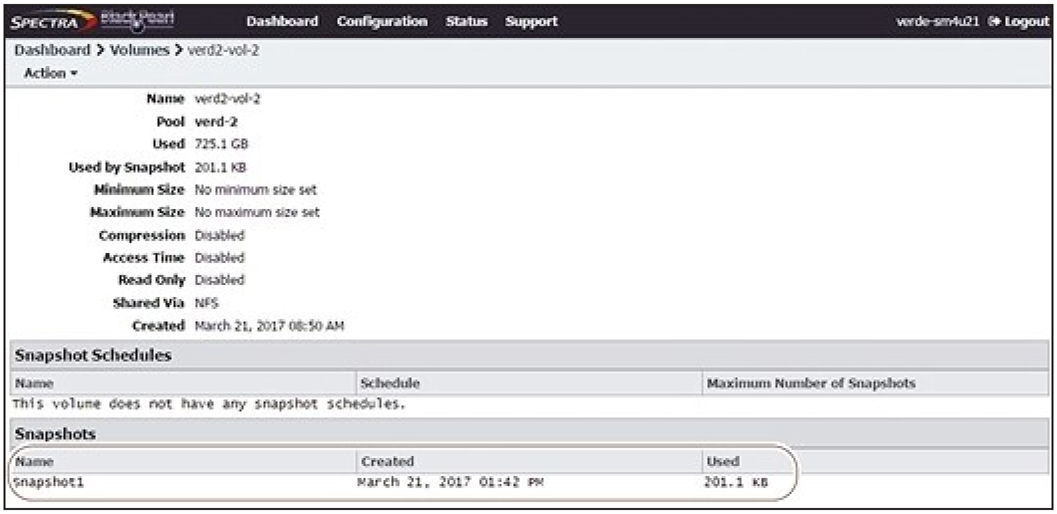
4. Click **Delete**.

Delete Snapshots

Use the following steps to delete a one or more snapshots.

1. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 96 on page 217).

2. Double-click the volume you for which you want to delete snapshot, or select the volume, and then select **Action > Show Details**. The details screen for that volume displays.



Name	verd2-vol-2
Pool	verd-2
Used	725.1 GB
Used by Snapshot	201.1 KB
Minimum Size	No minimum size set
Maximum Size	No maximum size set
Compression	Disabled
Access Time	Disabled
Read Only	Disabled
Shared Via	NFS
Created	March 21, 2017 08:50 AM

Snapshot Schedules

Name	Schedule	Maximum Number of Snapshots
This volume does not have any snapshot schedules.		

Snapshots

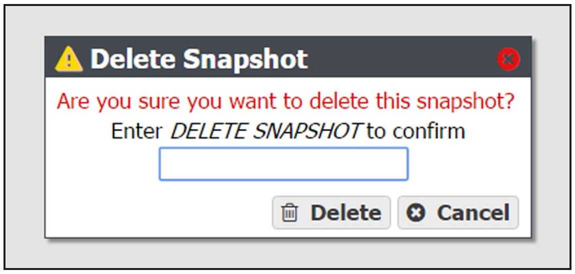
Name	Created	Used
snapshot1	March 21, 2017 01:42 PM	201.1 KB

Figure 133 The Volume details screen showing a snapshot.

3. Delete the snapshot(s):

- To delete a single snapshot, select the snapshot you want to delete, and then select **Action > Delete Snapshot**.
- To delete all snapshots select **Action > Delete All Snapshots.**

A confirmation window displays.


Delete Snapshot

Are you sure you want to delete this snapshot?

Enter *DELETE SNAPSHOT* to confirm

Figure 134 Confirm the snapshot deletion (Delete Snapshot window shown).

4. Type the indicated text in the entry field and click **Delete** to delete the selected snapshot, or all snapshots.

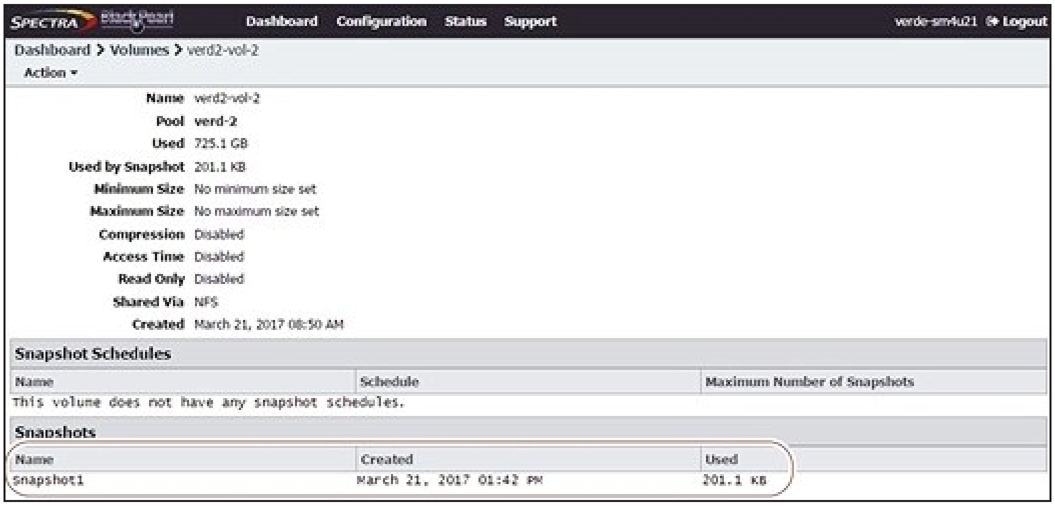
Restore to a Snapshot

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 Retrieve a Single File from a Snapshot on the next page.
- 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. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 96 on page 217).
2. Double-click the volume you want to restore using a previously generated snapshot, or select the volume, and then select **Action > Show Details**. The details screen for that volume displays.



Name verd2-vol-2
Pool verd-2
Used 725.1 GB
Used by Snapshot 201.1 KB
Minimum Size No minimum size set
Maximum Size No maximum size set
Compression Disabled
Access Time Disabled
Read Only Disabled
Shared Via NFS
Created March 21, 2017 08:50 AM

Snapshot Schedules

Name	Schedule	Maximum Number of Snapshots
This volume does not have any snapshot schedules.		

Snapshots

Name	Created	Used
snapshot1	March 21, 2017 01:42 PM	201.1 KB

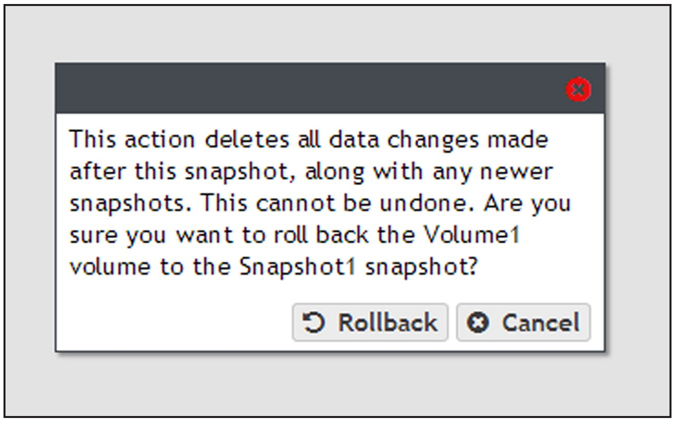
Figure 135 The Volume details screen.

3. In the snapshots list, select the snapshot you want to use to restore the volume and then select **Action > Rollback**.

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.

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.

4. A dialog box displays, asking you to confirm the rollback. Select **Rollback** to restore the volume to its state when the snapshot was created.



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 Volume1 volume to the Snapshot1 snapshot?

Figure 136 Confirm the volume snapshot 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.

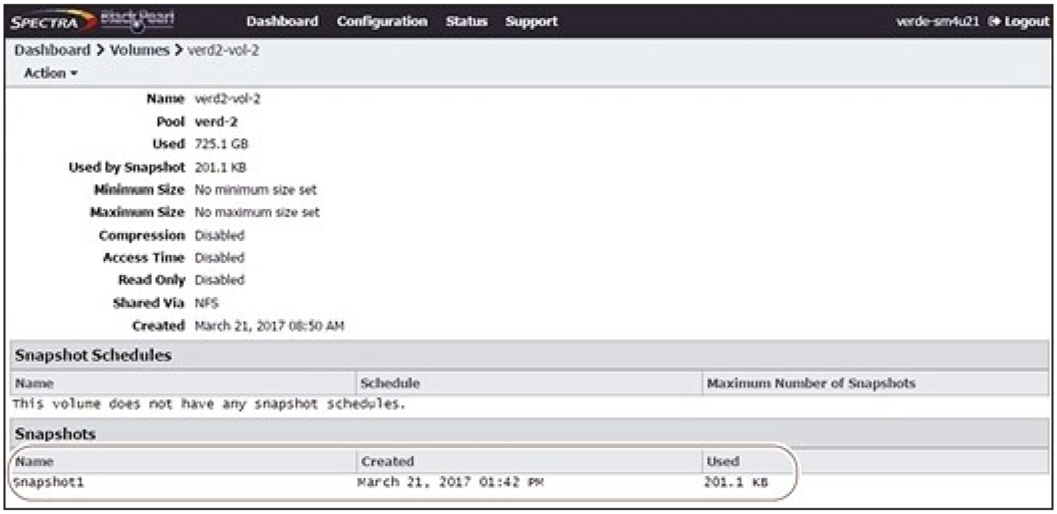
Note: Use Windows Explorer or Linux/Unix command line to complete this procedure.

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. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 96 on page 217).

   b. Double-click the volume you for which you want to delete snapshot, or select the volume, and then select **Action > Show Details**. The details screen for that volume displays.



Name	verd2-vol-2
Pool	verd-2
Used	725.1 GB
Used by Snapshot	201.1 KB
Minimum Size	No minimum size set
Maximum Size	No maximum size set
Compression	Disabled
Access Time	Disabled
Read Only	Disabled
Shared Via	NFS
Created	March 21, 2017 08:50 AM

Snapshot Schedules

Name	Schedule	Maximum Number of Snapshots
This volume does not have any snapshot schedules.		

Snapshots

Name	Created	Used
snapshot1	March 21, 2017 01:42 PM	201.1 KB

Figure 137 The Volume details screen showing a snapshot.

   c. Locate the snapshot from which you want to restore a file and record the name, if desired.

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.

MANAGE SHARES

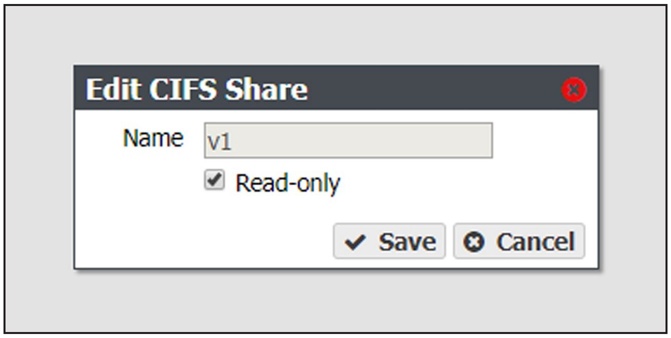
After creating one or more shares, use the instructions in this section to edit, or delete a share.

Note: You cannot edit a Vail S3 share.

Edit a CIFS Share

After creating a CIFS share, you can edit it to change the configuration.

1. From the menu bar, select **Configuration > Shares > CIFS**. The CIFS Shares screen displays.
2. Select the share you want to edit, and then select **Action > Edit**. The Edit CIFS Share screen displays.



Name v1

☑ Read-only

Figure 138 The Edit NFS Share dialog box.

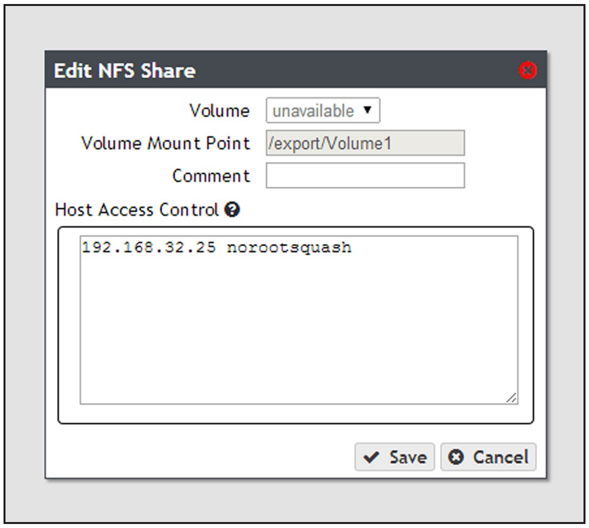
3. Select or clear the **Read-only** check box. You cannot change the name once the CIFS share is created.
4. Click **Save**.

Edit an NFS Share

After creating an NFS share, you can edit it to change the configuration.

1. From the menu bar, select **Configuration > Shares > NFS**. The NFS Shares screen displays.

2. Select the share you want to edit, and then select **Action > Edit**. The NFS Share Edit screen displays.



Volume: unavailable

Volume Mount Point: /export/Volume1

Comment:

Host Access Control

```
192.168.32.25 norootsquash
```

Figure 139 The Edit NFS Share dialog box.

3. Make the desired changes (see Create a Share on page 226 for more information), and click **Save**.

Delete a Share

If you do not want to continue sharing a volume (that is, you do not want users accessing the NAS over a network connection to access the volume), you can delete the share.

Use the following steps to delete the share.

1. If you need to delete a CIFS share, from the menu bar, select **Configuration > Shares > CIFS**. The CIFS Shares screen displays.

   —OR—

   If you need to delete an NFS share, from the menu bar, select **Configuration > Shares > NFS**. The NFS Shares screen displays.

   —OR—

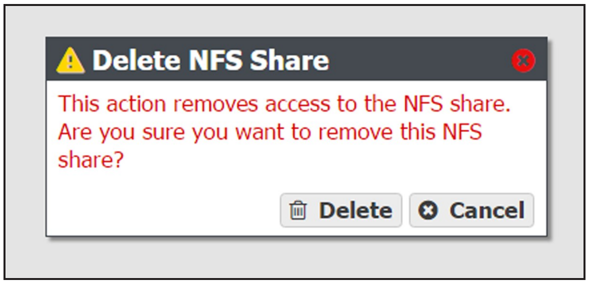
   If you need to delete a Vail share, from the menu bar, select **Configuration > Shares > Vail S3**. The Vail S3 Shares screen displays.

2. Select the share you want to delete, and then select **Action > Delete**.

Note: You cannot delete a Vail S3 share with data persisted to the volume. You must first delete the share as Storage in the Vail management console, then delete the share in the BlackPearl user interface.

3. A dialog box displays asking you to confirm the deletion. Click **Delete** to remove the share.

Note: Clicking **Delete** does not delete the volume. It only removes the volume from the list of shares and makes it inaccessible to remote hosts. The volume is still listed present on the gateway and listed on the Volumes screen.



Delete NFS Share

This action removes access to the NFS share. Are you sure you want to remove this NFS share?

Figure 140 Confirm removing the share.

MANAGE NAS REPLICATION

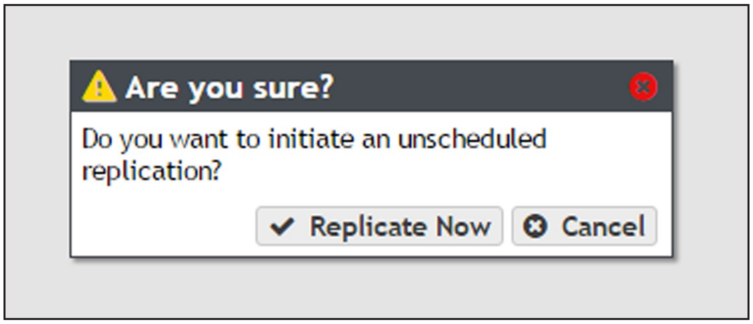
After configuring replication (see Configure NAS Services on page 234), use the instructions in this section to manually start or cancel a volume replication, edit or delete the NAS replication configuration, and to restore replicated files.

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.

Note: If the gateway is in the process of replicating data on a preconfigured schedule, the manual replication begins when the scheduled replication completes. To stop any replication in progress, see Cancel a NAS Replication In Progress below.

1. On the source system's BlackPearl user interface, select **Configuration > NAS > Volumes**. The Volumes screen displays.
2. Double-click the volume name you want to replicate, or select the volume and select **Action > Show Details**. The details screen for the volume displays.
3. Select **Action > Replicate Now**. A confirmation window displays.



Are you sure?

Do you want to initiate an unscheduled replication?

Figure 141 The Replicate Now confirmation window.

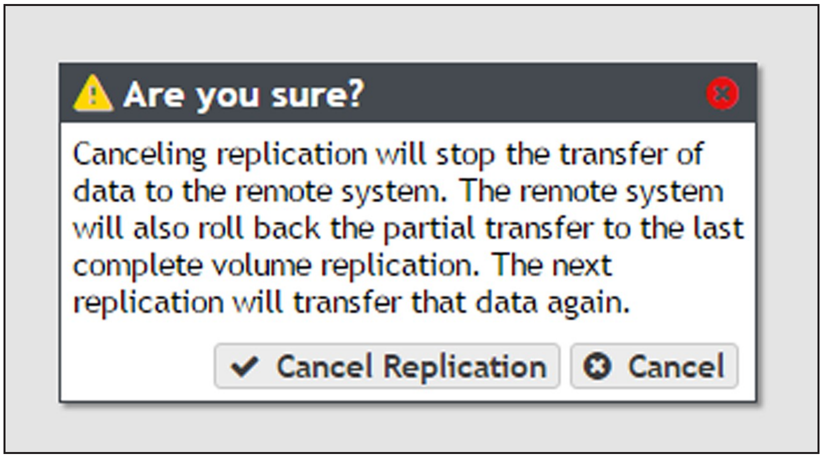
4. Click **Replicate Now** to begin a manual NAS replication.

Cancel a NAS Replication In Progress

If desired, you can cancel any NAS replications currently in progress. Canceling replication stops the replication and deletes any data the target received during the replication. Use the steps in this section to cancel a NAS replication.

Note: Starting with BlackPearl OS 5.4, you can no longer cancel an in-progress NAS replication. After starting a NAS replication, you must wait for it to complete.

1. On the source system's BlackPearl user interface, select **Configuration > NAS > Volumes**. The Volumes screen displays.
2. Double-click the volume name for which you want to cancel replication, or select the volume and select **Action > Show Details**. The details screen for the volume displays.
3. Select **Action > Cancel Replication**. A confirmation window displays.



Canceling replication will stop the transfer of data to the remote system. The remote system will also roll back the partial transfer to the last complete volume replication. The next replication will transfer that data again.

Figure 142 The Cancel Replication confirmation window.

4. Click **Cancel Replication** to stop the NAS replication in progress. Any data that was transferred to the target is deleted.

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. From the menu bar, 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** check box.

   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 Share on page 226 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. From the menu bar, 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** check box.

   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. See Delete a Share on page 268.

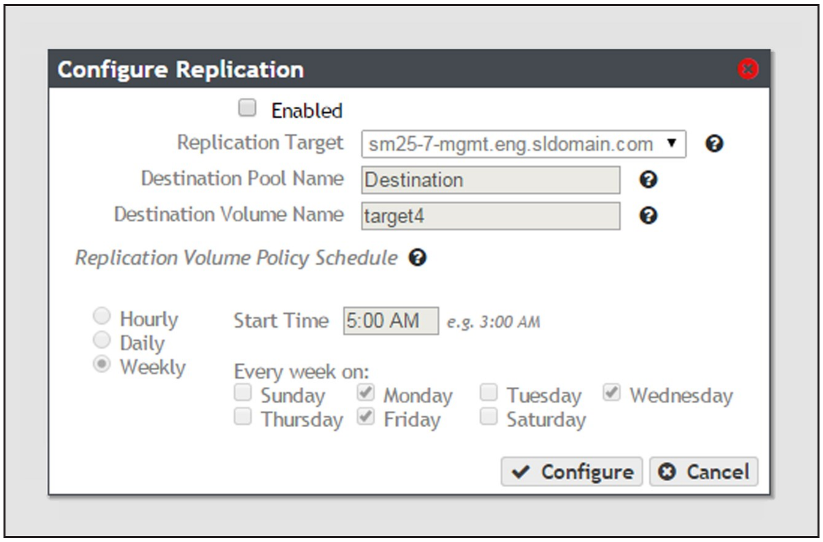
Disable NAS Replication for a Volume

Use the instructions in this section to prevent any further replication from a volume currently configured to use NAS replication.

1. On the source system's BlackPearl user interface, select **Configuration > NAS > Volumes**. The Volumes screen displays.

2. Double-click the volume name you want to stop replicating, or select the volume and select **Action > Show Details**. The details screen for the volume displays.

3. Select **Action > Configure Replication**. The Configure Replication dialog box displays.



Configure Replication

□ Enabled

Replication Target: sm25-7-mgmt.eng.sldomain.com

Destination Pool Name: Destination

Destination Volume Name: target4

Replication Volume Policy Schedule

○ Hourly
○ Daily
● Weekly

Start Time: 5:00 AM *e.g. 3:00 AM*

Every week on:
□ Sunday ☑ Monday □ Tuesday ☑ Wednesday
□ Thursday ☑ Friday □ Saturday

Figure 143 The Configure Replication dialog box.

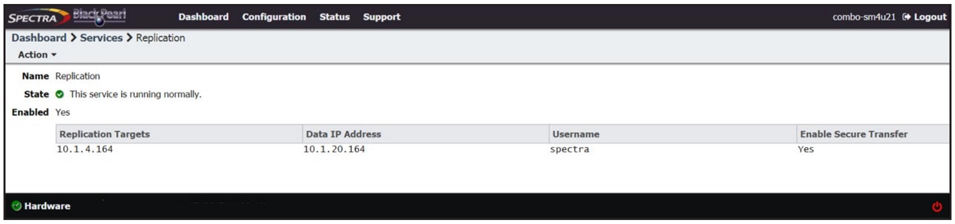
4. Clear the **Enabled** check box. The other options on the dialog box grey out and become un-editable.

5. Click **Configure**. The volume no longer replicates to the target.

Edit the NAS Replication Service

1. On the source gateway's BlackPearl user interface, select **Configuration > Services** to display the Services screen (see Figure 161 on page 292).

2. Double-click the Replication service, or select the service, and then select **Action > Show Details**. The Replication service details screen displays.

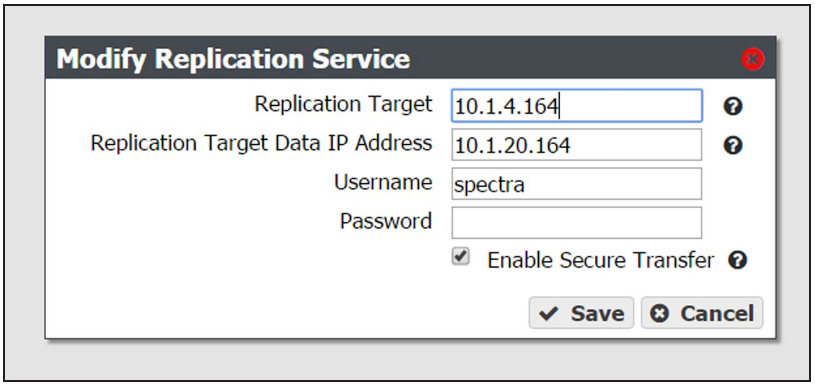


Name Replication
State ✓ This service is running normally.
Enabled Yes

Replication Targets	Data IP Address	Username	Enable Secure Transfer
10.1.4.164	10.1.20.164	spectra	Yes

Figure 144 The Replication service details screen.

3. Select the replication target in the Replication service details screen, and select **Action > Edit**. The Modify Replication Service dialog box displays.



Modify Replication Service

Replication Target: 10.1.4.164

Replication Target Data IP Address: 10.1.20.164

Username: spectra

Password:

☑ Enable Secure Transfer

Figure 145 The Modify Replication Service dialog box.

4. If desired, modify the IP address or hostname of the management port of the target in the **Replication Target** field.

Note: Do not use http:// or https:// to precede the IP address or hostname.

5. If desired, modify the IP address of the target’s data port in the **Replication Target Data IP Address** field.

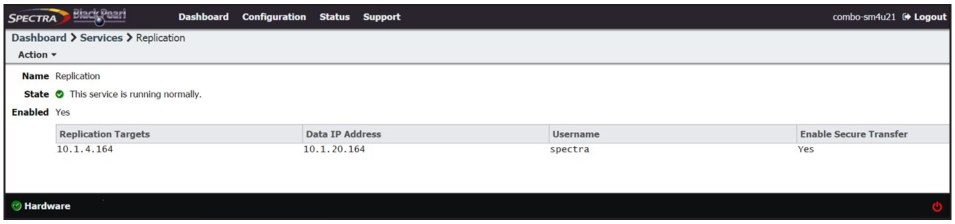
Note: Do not use http:// or https:// to precede the IP address or hostname.

6. If desired, modify the username of a user configured on the target in the **Username** field.
7. Enter the user password in the **Password** field, if one is set. Otherwise, leave the field blank.
8. If desired, select the **Enable Secure Transfer** check box to configure the gateway to encrypt the replicated data before transferring it to the target, or clear the check box to transfer data without encryption. Data is encrypted using Secure Socket Layer (SSL).
9. Click **Save**.

Delete the NAS Replication Service Configuration

1. On the source gateway’s BlackPearl user interface, select **Configuration > Services** to display the Services screen (see Figure 161 on page 292).

2. Double-click the Replication service, or select the service, and then select **Action > Show Details**. The Replication service details screen displays.



Name Replication

State ✓ This service is running normally.

Enabled Yes

Replication Targets	Data IP Address	Username	Enable Secure Transfer
10.1.4.164	10.1.20.164	spectra	Yes

Figure 146 The Replication service details screen.

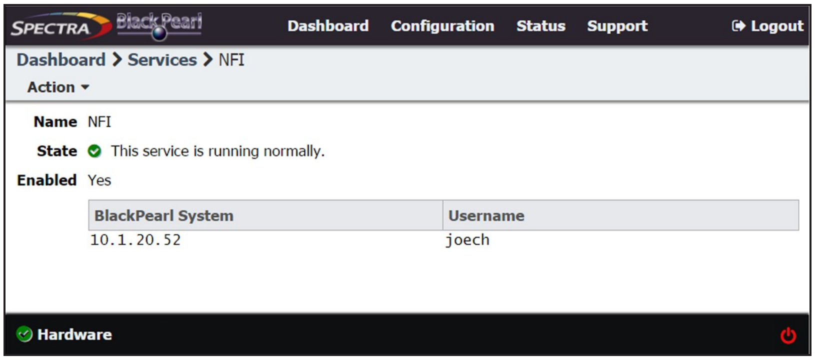
3. Select the replication target in the Replication service details screen, and select **Action > Delete**. The Delete Replication Target dialog box displays.
4. Click **Delete** to remove the NAS replication target. The gateway no longer replicates data to the target.
5. Repeat Step 3 and Step 4 to delete additional NAS replication targets, if desired.

MANAGE NFI REPLICATION

Edit the NFI Service

If desired, you can change the configuration of the previously configured NFI service.

1. From the menu bar, select **Configuration > Services** to display the Services screen.
2. Double-click the NFI service, or select the service, and then select **Action > Show Details**. The details screen for the NFI service displays.



Name NFI
State ✓ This service is running normally.
Enabled Yes

BlackPearl System	Username
10.1.20.52	joech

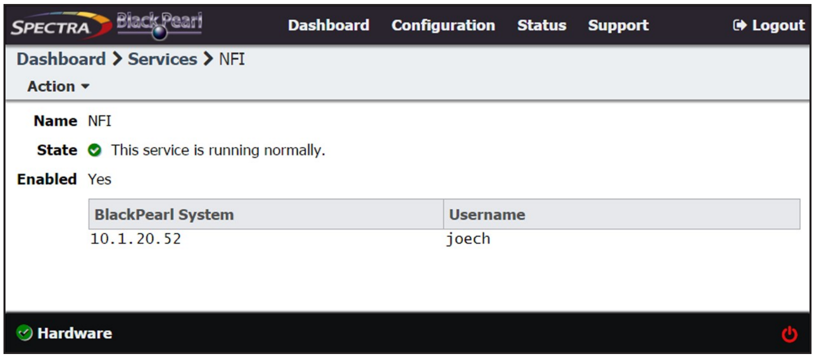
Figure 147 The NFI service details screen.

3. Select **Action > Edit**. The Edit NFI dialog box displays.
4. Edit the settings as described in Configure the NFI Service on page 235.
5. Click **Save**.

Delete the NFI Service Configuration

If desired, you can delete (clear) the NFI service configuration.

1. From the menu bar, select **Configuration > Services** to display the Services screen.
2. Double-click the NFI service, or select the service, and then select **Action > Show Details**. The details screen for the NFI service displays.



Name NFI
State ✓ This service is running normally.
Enabled Yes

BlackPearl System	Username
10.1.20.52	joech

Figure 148 The NFI service details screen.

3. Select **Action > Delete**. A confirmation window displays.
4. Confirm the deletion of the NFI service configuration.

Manually Starting an NFI Replication

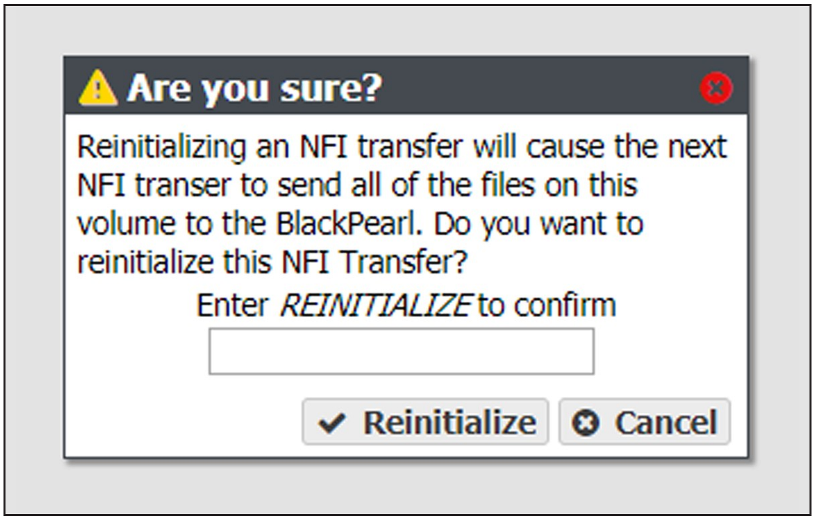
If desired, you can manually initiate an NFI replication to the target gateway.

1. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 96 on page 217).
2. Double-click the volume for which you want to manually start an NFI replication, or select the volume, and then select **Action > Show Details**. The details screen for that volume displays.
3. Select **Action > Initiate NFI Transfer**.
4. Click **Initiate NFI Transfer** to begin the replication.

Reinitialize NFI Replication

If desired, you can elect to reinitialize an NFI replication, which transfers all the files in the volume to the BlackPearl target during the next NFI replication.

1. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 96 on page 217).
2. Double-click the volume for which you want to manually start an NFI replication, or select the volume, and then select **Action > Show Details**. The details screen for that volume displays.
3. Select **Action > Reinitialize NFI Transfer**. A confirmation window displays.



Are you sure?

Reinitializing an NFI transfer will cause the next NFI transer to send all of the files on this volume to the BlackPearl. Do you want to reinitialize this NFI Transfer?

Enter *REINITIALIZE* to confirm

Figure 149 The Reinitialize NFI Transfer confirmation window.

4. Type `REINITIALIZE` in the entry field and click **Reinitialize** to reinitialize the NFI transfer.

Edit the NFI Volume Policy

Use the instructions in Configure the NFI Volume Policy on page 221 to change how data is copied from the NAS volume to a BlackPearl gateway.

Restoring Files From an NFI Target BlackPearl Gateway

If files copied to the BlackPearl gateway using the NFI service are deleted from the NAS system, you can retrieve the files from the BlackPearl storage domains using the Spectra EON Browser, Spectra Deep Storage Browser, or a DS3 client. If you only need to retrieve a small number of files, Spectra Logic recommends using the EON Browser.

- For instructions for installing, configuring, and using the EON Browser, see the *BlackPearl Eon Browser User Guide*.
- For instructions for installing, configuring, and using the Deep Storage Browser, use the documentation provided to you when you installed the program.

Note: To retrieve a file you must use the S3 credentials for the user configured in the NFI service when starting a session in the EON Browser or Deep Storage Browser.

If you do not know which user is configured in the NFI service, see Configure the NFI Service on page 235.

If you do not know the S3 credentials of the user, see View S3 Credentials on page 86. It is helpful to leave the S3 Credentials dialog box open in the BlackPearl user interface, so that you can easily copy and paste the credential values when configuring the EON Browser or Deep Storage Browser.

CHAPTER 8 - ADDITIONAL CONFIGURATION OPTIONS

This chapter describes using the BlackPearl user interface to configure additional options for the Spectra BlackPearl Nearline Gateway.

Configure Network Connections and Settings 280

Configure Ethernet Ports 281

Configure DNS Settings 287

Configure SMTP Settings 288

Configure Date and Time 290

Edit the System Name 291

Configure Networking Services 292

Configure the DS3 Service 292

Configure the Active Directory Service 296

Configure the SNMP Service 300

Multi-Factor Authentication 303

Enable the Attack Hardened Service 303

Enable Multi-Factor Authentication for a User 304

Log In to a System Configured to Use Multi-Factor Authentication 306

Update Multi-Factor Authentication for a User 307

Disable Multi-Factor Authentication for a User 309

Disable the Attack Hardened Service 309

Configure a Vail Sphere 310

Register with a Vail Sphere 310

Edit the Vail Service 310

Configure and Use Encryption 311

Configure the Encryption Service 312

Export Encryption Key to USB Drive 316

Change the Encryption Password 318

Unlock the Self-Encrypting Drives 319

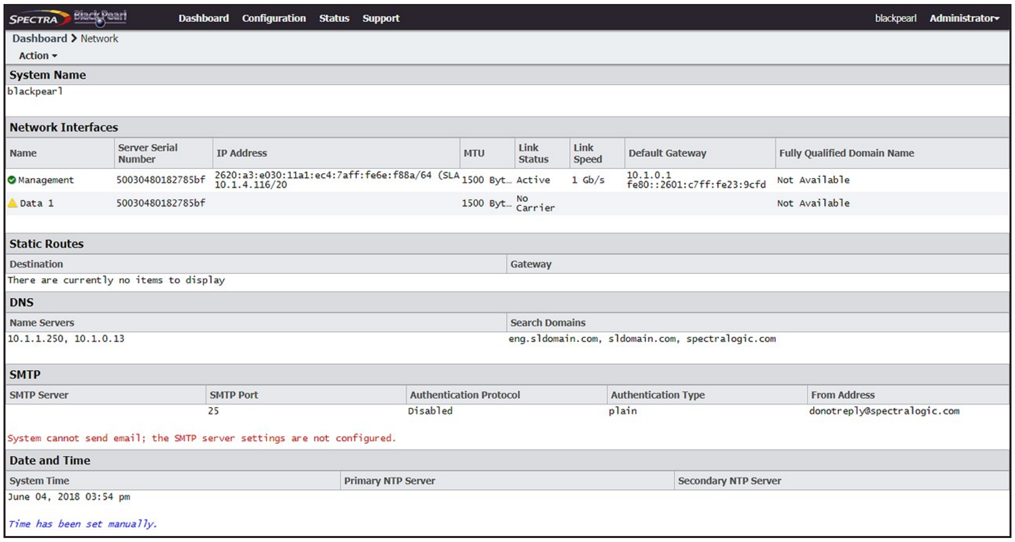
Encrypt or Decrypt a Storage Pool 320

PSID Erase an Encryption Drive 321
Configure Users 323
Description of User Types 323
Create a User 323
Edit a User 323
Change S3 Secret Key 326
Delete a User 327
Configure S3 Groups 329
Create an S3 Group 329
Remove an S3 Group Member 331
Edit an S3 Group 332
Delete an S3 Group 332
Configure Certificates 334
Enable Remote Logging 336
Manually Enter Activation Keys 338

Configure Network Connections and Settings

Use the Network screen to edit the system name, configure Ethernet ports and DNS settings, and to enter SMTP and NTP information.

Note: If configuring a HotPair system, see the *Spectra BlackPearl HotPair Installation & Configuration Guide* for instructions on configuring network connections.



System Name

blackpearl

Network Interfaces

Name	Server Serial Number	IP Address	MTU	Link Status	Link Speed	Default Gateway	Fully Qualified Domain Name
✓ Management	50030480182785bf	2620:a3:e030:11a1:ec4:7aff:fe6e:f88a/64 (SLA 10.1.4.116/20	1500 Byt...	Active	1 Gb/s	10.1.0.1 fe80::2601:c7ff:fe23:9cfd	Not Available
⚠ Data 1	50030480182785bf		1500 Byt...	No Carrier			Not Available

Static Routes

Destination	Gateway
There are currently no items to display	

DNS

Name Servers	Search Domains
10.1.1.250, 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
June 04, 2018 03:54 pm		

Time has been set manually.

Figure 150 The Network screen.

Configure Ethernet Ports

This section describes using the BlackPearl user interface to configure the IP addressing for the Ethernet ports in the BlackPearl 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 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.
- 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 Initial Configuration on page 66. Use the instructions in this section to configure network settings after initial setup is complete.

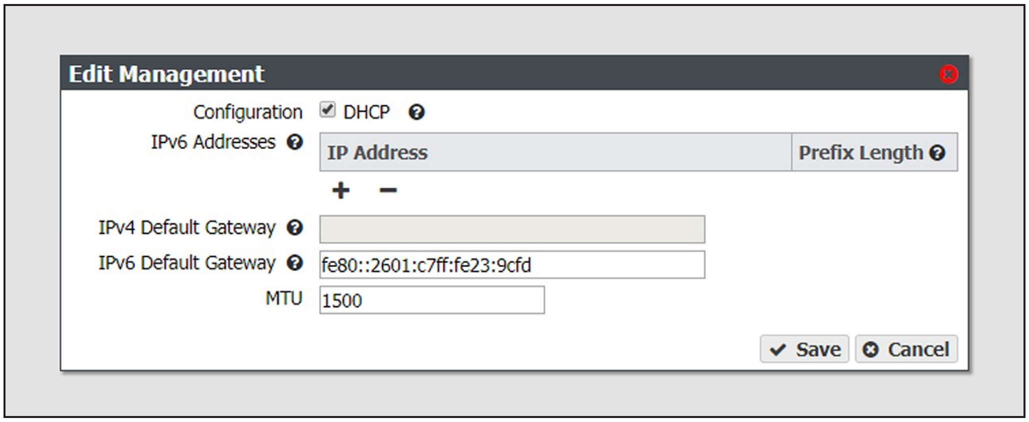
The next steps depend on if you are configuring the data connection, the management port, or want to delete (clear) a network configuration.

- Configure the Data Connection on page 76
- Configure the Management Port below
- Edit an Aggregate Data Connection on page 283
- Edit a Static Route on page 286
- Clear a Data Port Configuration on page 287

Configure the Management Port

1. From the menu bar, select **Configuration > Network**, or click the Network pane from the Dashboard screen. The Network screen displays (see Figure 150 on page 280).

2. In the Network Interfaces pane, double-click the Management row, or select the Management row and then select **Action > Edit**. The Edit Management dialog box displays.



Edit Management

Configuration ☑ DHCP

IPv6 Addresses

IP Address	Prefix Length

IPv4 Default Gateway:

IPv6 Default Gateway: fe80::2601:c7ff:fe23:9cfd

MTU: 1500

Figure 151 The Edit Management dialog box.

3. Select **DHCP** 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.

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 in Step 3 on page 282.

- **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 **IPv4Default Gateway**.

Notes:
- If you selected DHCP in Step 3 on page 282, this option is unavailable.
- The gateway entered for the last configured IPv4 connection sets the default gateway for the BlackPearl gateway.

6. If applicable, enter the **IPv6Default Gateway**.

Notes:
- The gateway entered for the last configured IPv6 connection sets the default gateway for the BlackPearl gateway.
- The IPv6 Gateway does not need to be configured when the BlackPearl 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, ensure that your switch configuration supports larger MTU settings, as well as all the hosts on the network.

8. Click **Save**.

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.

Edit an Aggregate Data Connection

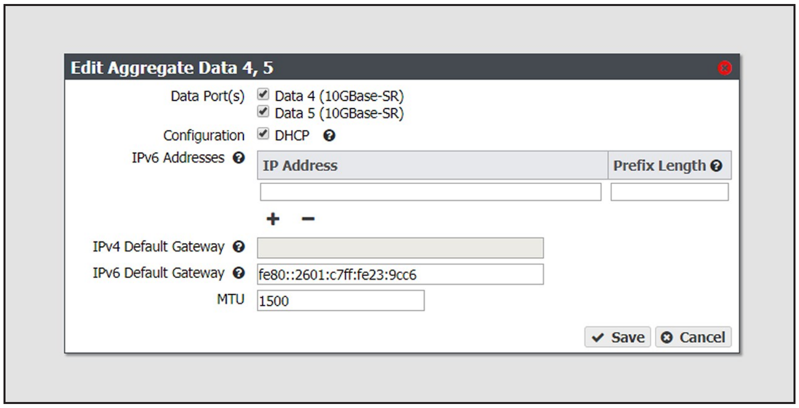
If desired, you can edit an aggregate data connection after it is created.

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

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

1. From the menu bar, select **Configuration > Network**, or click the Network pane from the Dashboard screen. The Network screen displays (see Figure 150 on page 280).

2. Select the row of the data connection you want to edit and select **Action > Edit**. The Edit Aggregate *Data Connection* dialog box displays.



Edit Aggregate Data 4, 5

Data Port(s) ☑ Data 4 (10GBase-SR)
☑ Data 5 (10GBase-SR)

Configuration ☑ DHCP

IPv6 Addresses

IP Address	Prefix Length

IPv4 Default Gateway:

IPv6 Default Gateway: fe80::2601:c7ff:fe23:9cc6

MTU: 1500

Figure 152 The Edit Aggregate *Data* dialog box.

3. Select or clear the **Data Port(s)** you want to configure into an aggregate data interface. 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 **DHCP** to configure the gateway to automatically acquire an IPv4 address using DHCP. This setting does not apply to IPv6.

5. To configure a static 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 in Step 4.

- **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.

To remove an existing static address, click the **-** button.

6. If applicable, enter the **IPv4Default 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 gateway.

7. If applicable, enter the **IPv6Default Gateway**.

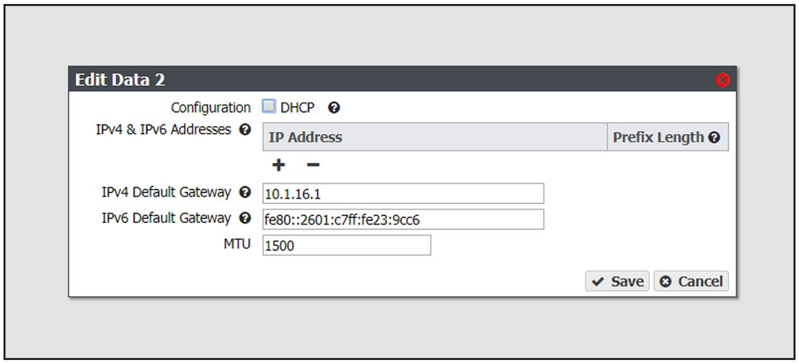
Notes:
- The gateway entered for the last configured IPv6 connection sets the default gateway for the BlackPearl gateway.
- The IPv6 Gateway does not need to be configured when the BlackPearl gateway is connected to a SLACC network.

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**.

Edit a Data Connection

If desired, you can edit a data connection after it is created.

1. From the menu bar, select **Configuration > Network**, or click the Network pane from the Dashboard screen. The Network screen displays (see Figure 150 on page 280).
2. Select the row of the data connection you want to edit and select **Action > Edit**. The Edit *Data Connection* dialog box displays.



Edit Data 2

Configuration □ DHCP

IPv4 & IPv6 Addresses

IP Address	Prefix Length

IPv4 Default Gateway: 10.1.16.1

IPv6 Default Gateway: fe80::2601:c7ff:fe23:9cc6

MTU: 1500

Figure 153 The Edit *Data* # dialog box.

3. Select **DHCP** to configure the gateway to automatically acquire an IPv4 address using DHCP. This setting does not apply to IPv6.
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 IP address if you selected DHCP in Step 4.

- **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.

To remove an existing static address, click the **-** button.

5. If applicable, enter the **IPv4Default 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 gateway.

6. If applicable, enter the **IPv6Default Gateway**.

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

7. 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.
8. Click **Save**.

Edit a Static Route

1. From the menu bar, select **Configuration > Network**, or select the Network pane from the Dashboard screen. The Network screen displays (see Figure 28 on page 79).
2. Double-click the static route you want to edit. The Static Route dialog box displays.

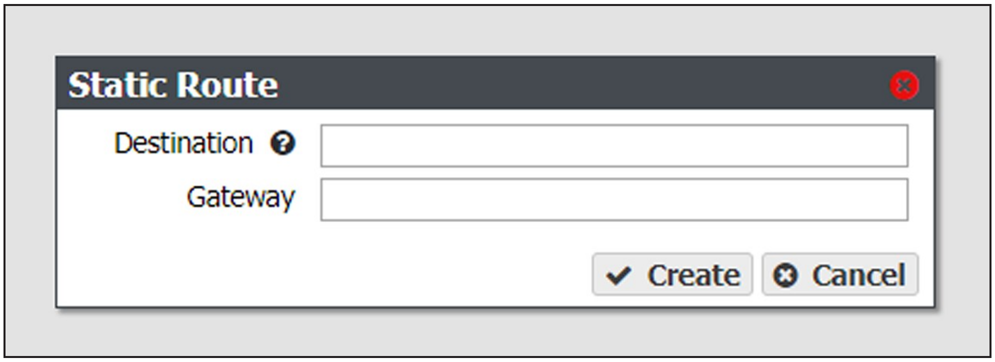


Figure 154 The Static Route dialog box.

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 **Gateway** of the data connection used to communicate with the isolated network.
5. Click **Create**.

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.

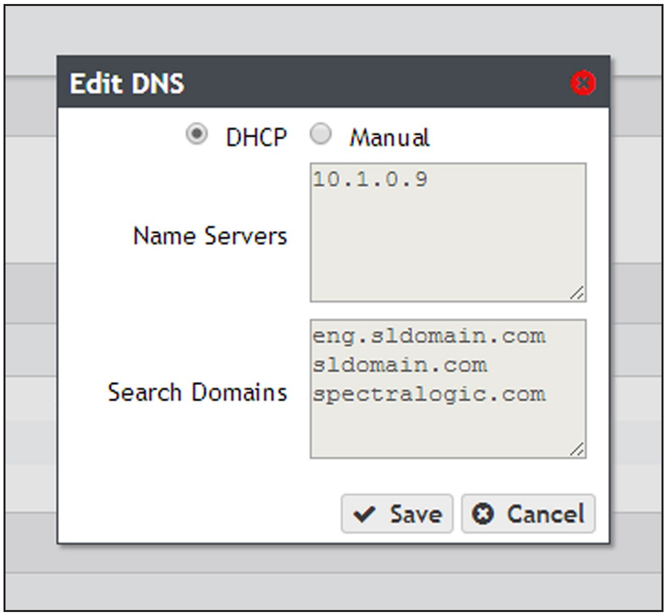
> **Note:** The management port cannot be cleared. See Configure the Management Port on page 281 to change the management port settings.

1. From the menu bar, select **Configuration > Network**, or click the Network pane from the Dashboard screen. The Network screen displays (see Figure 150 on page 280).
2. Select the row of the configuration you want to clear and select **Action > Clear** from the menu bar. A confirmation window displays.
3. Click **Delete** to clear the Ethernet configuration.

Configure DNS Settings

The DNS settings on the BlackPearl gateway are used to allow domain name lookup on the gateway. Use the following instructions to enter DNS information on the gateway.

1. From the menu bar, select **Configuration > Network**, or click the Network pane from the Dashboard screen. The Network screen displays (see Figure 150 on page 280).
2. In the DNS pane of the Network screen, double-click the single row, or select the row and then select **Action > Edit**. The Edit DNS screen displays.



● DHCP ○ Manual

Name Servers: 10.1.0.9

Search Domains: eng.sldomain.com
sldomain.com
spectralogic.com

Figure 155 Edit DNS information.

3. Select **DHCP** to have the gateway determine the address of name servers and search domains automatically.

   —OR—

   Select **Manual** to enter information for name servers and search domains manually.

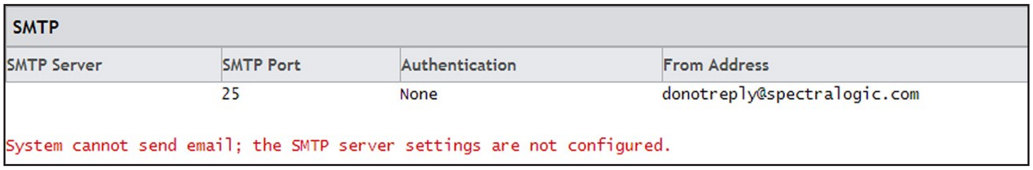
Note: The buttons for **DHCP** and **Manual** are only usable when the BlackPearl management port is configured as DHCP. If the management interface is set to a static IP address, the buttons are unavailable, and the information must be entered manually.

4. If the BlackPearl management port is configured with a static IP address, or 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 **Save**.

Configure SMTP Settings

Use the Email settings to associate the BlackPearl gateway with a mail server. The gateway uses this SMTP server to send emails whenever ASLs or certain types of messages are generated.

1. From the menu bar, select **Configuration > Network**, or select the Network pane from the Dashboard screen. The Network screen displays.



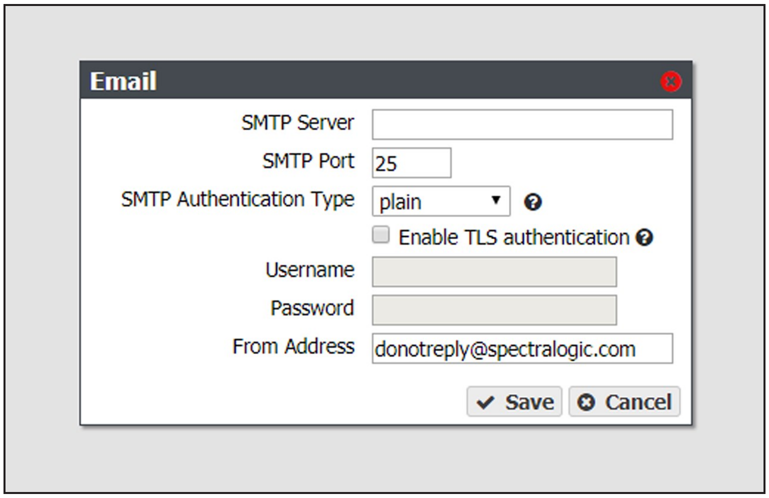
SMTP

SMTP Server	SMTP Port	Authentication	From Address
	25	None	donotreply@spectralogic.com

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

Figure 156 The SMTP pane of the Network screen.

2. Double-click the name of the SMTP server, or select the name of the SMTP server and then click **Action > Edit**. The Email dialog box displays.



Email

SMTP Server

SMTP Port 25

SMTP Authentication Type plain

□ Enable TLS authentication

Username

Password

From Address donotreply@spectralogic.com

Figure 157 The Email dialog box.

3. Enter the **SMTP Server** and **SMTP Port** information.
4. Using the drop-down menu, select the **SMTP Authentication Type** required by your mail server.
5. If your SMTP server uses TLS (Transport Layer Security) authentication, select the **Enable TLS Authentication** check box 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 gateway to assist in troubleshooting and be recognized by the SMTP server as a valid domain address.
7. Click **Save**.

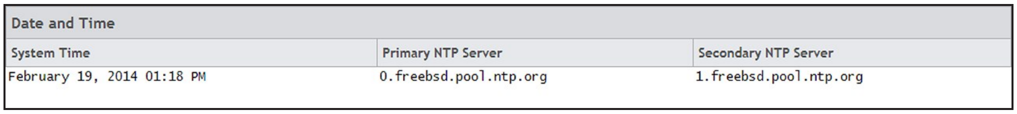
Configure Date and Time

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 gateway.

Note: If you plan to join an Active Directory domain, you must configure the BlackPearl 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. From the menu bar, select **Configuration > Network**, or select the Network pane from the Dashboard screen. The Network screen displays.

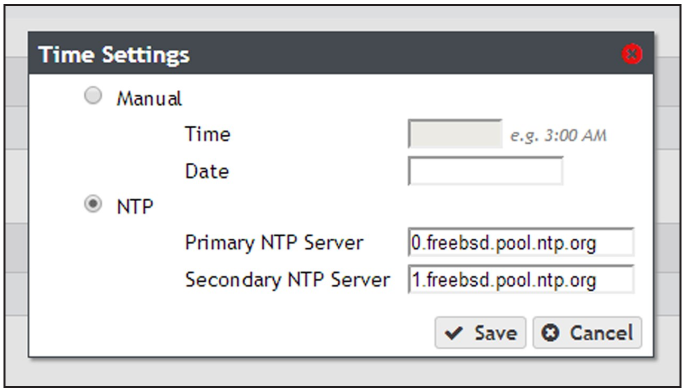


Date and Time

System Time	Primary NTP Server	Secondary NTP Server
February 19, 2014 01:18 PM	0.freebsd.pool.ntp.org	1.freebsd.pool.ntp.org

Figure 158 The Date and Time pane of the Network screen.

2. Double-click the System Time to edit the date and time, or select the System Time row and select **Action > Edit**. The Time Settings dialog box displays.



Time Settings

○ Manual

Time: e.g. 3:00 AM

Date:

● NTP

Primary NTP Server: 0.freebsd.pool.ntp.org

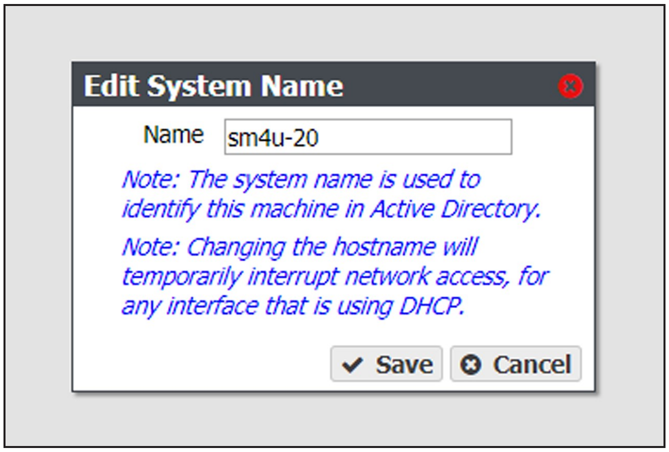
Secondary NTP Server: 1.freebsd.pool.ntp.org

Figure 159 The Time Settings dialog box.

3. Select **Manual** or **NTP**.
   a. If you select **Manual**, enter the current time in the **Time** field. Enter either 12-hour time values and include AM or PM, or use 24-hour time values. Click the empty **Date** field. A calendar appears. Select the current date.
   b. If you select **NTP**, enter the NTP server information for the **Primary NTP Server**. If desired, enter the NTP server information for the **Secondary NTP Server**.
4. Click **Save**.

Edit the System Name

1. From the menu bar, select **Configuration > Network**, or click the Network pane from the Dashboard screen. The Network screen displays.
2. In the Network Interfaces pane, double-click the system name, or select the system name and then select **Action > Edit**. The Edit System Name dialog box displays.



Name: sm4u-20

Note: The system name is used to identify this machine in Active Directory.

Note: Changing the hostname will temporarily interrupt network access, for any interface that is using DHCP.

Figure 160 The Edit System Name dialog box.

3. Enter the desired **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
- If your gateway is using BlackPearl OS 3.2.2, or earlier, there are no character restrictions on system names. However, Spectra Logic recommends limiting system names to letters, numbers, and hyphens to maintain compatibility with the RFC 1123 standard.
- The gateway does not change previously configured system names using special characters when upgrading to BlackPearl OS 3.3, or later.

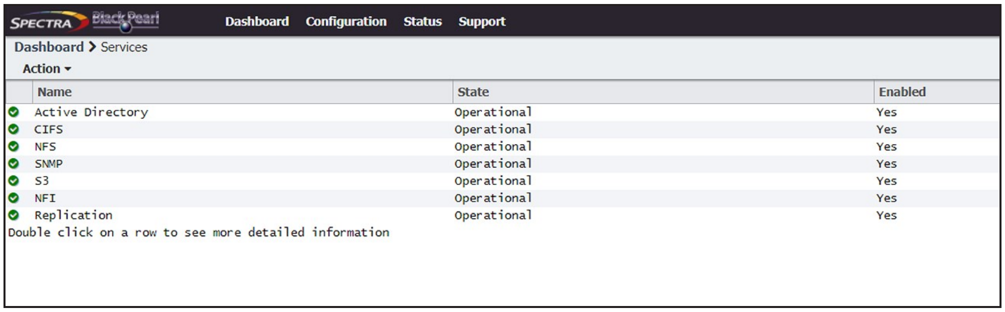
4. Click **Save**.

Configure Networking Services

Use the following instructions to configure networking services on the BlackPearl gateway.

For instructions on configuring NAS services, see Configure NAS Services on page 234.

To display the services screen, from the menu bar, select **Configuration > Services**.



	Name	State	Enabled
✓	Active Directory	Operational	Yes
✓	CIFS	Operational	Yes
✓	NFS	Operational	Yes
✓	SNMP	Operational	Yes
✓	S3	Operational	Yes
✓	NFI	Operational	Yes
✓	Replication	Operational	Yes

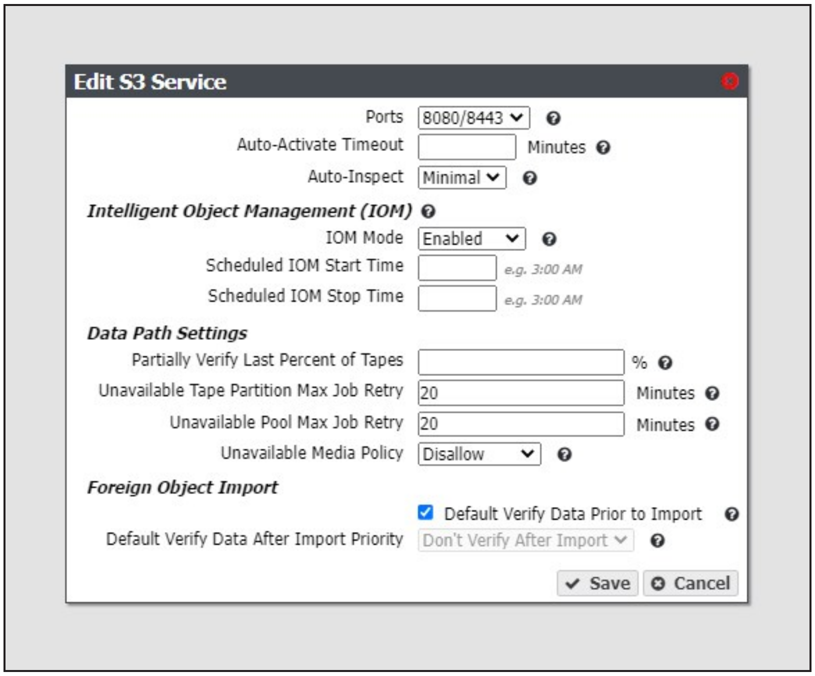
Double click on a row to see more detailed information

Figure 161 The Services screen.

Configure the DS3 Service

1. From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 93 on page 164).
2. Double-click the S3 service, or select the S3 service and select **Action > Show Details**. The S3 details screen displays.

3. On the S3 service details screen, select **Action > Edit**. The Edit S3 Service dialog box displays.



Edit S3 Service

Ports	8080/8443
Auto-Activate Timeout	Minutes
Auto-Inspect	Minimal

Intelligent Object Management (IOM)

IOM Mode	Enabled
Scheduled IOM Start Time	e.g. 3:00 AM
Scheduled IOM Stop Time	e.g. 3:00 AM

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

Default Verify Data After Import Priority	Don't Verify After Import

Figure 162 The Edit S3 Service dialog box.

4. Using the drop-down list, select the pair of **Ports** used for the HTTP and HTTPS connections to the S3 service.

5. Enter a value in minutes in the **Auto-Activate Timeout** entry field. This value specifies the amount of time that must pass between the S3 data path backend shutdown and the restart before it will not be auto-activated. For example, if the gateway is powered off for longer than the specified timeout value, you must manually restart the S3 data path backend after powering on the gateway.

Notes:

- To manually start the data path backend, see Reboot or Shut Down a BlackPearl Gateway on page 451.
- If the **Auto-Activate Timeout** is set to 0, the data path backend never auto-activates.
- If the BlackPearl Nearline gateway is powered off longer than the configured timeout value, when the system is powered on, the **Auto-Activate Timeout** value is set to "None".

6. Using the drop-down menu, select a behavior for **Auto-Inspect**. 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 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.

Notes:

- All tapes new to the BlackPearl gateway are inspected regardless of the auto-inspect setting.
- With BlackPearl OS 5.2 or earlier, if there was an inventory change in the tape library while in standby, the BlackPearl 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 S3 service is set to "Never Inspect".

7. 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 512 for information on IOM.

Value	Description
Enabled	The BlackPearl 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 **IOM Start Time** and **IOM Stop Time**. **Note:** If you set the start and stop time to the same value, IOM operations do not run.
Disabled	The BlackPearl 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 Partition Drive Reservation on page 350 for more information).

- Data migration is initiated manually. See Data Migration on page 367 for more information.
- If this option is currently enabled, when the setting is disabled, any in-progress IOM operations are suspended.

8. 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 467 for information about on demand tape media data integrity verification.

9. 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.
10. 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.
11. Using the drop-down menu, select a behavior for **Unavailable Media Policy**. This setting configures how the gateway behaves where there is 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 fail.

12. Select or clear **Default Verify Data Prior to Import**. Selecting this option verifies data on imported tape media before it makes the data available to the gateway.

13. Using the drop-down menu, select a priority for **Default Verify Data After Import Priority**. This option makes imported foreign options available, and schedules a verify job with the selected priority at a later time.

Note: This option is unavailable if you selected **Default Verify Data Prior to Import** in Step 12 on page 296.

14. 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 gateway to use NTP. See Configure Date and Time on page 290.

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

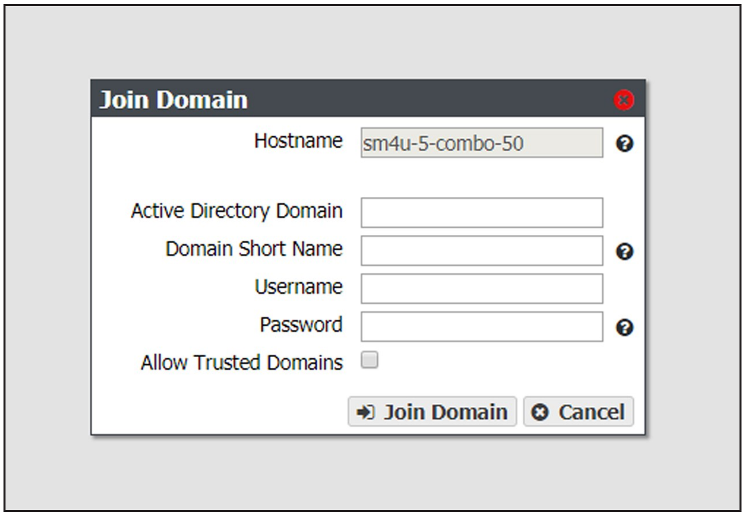
Use the instructions in this section to join or leave an Active Directory domain.

Join Domain

1. From the menu bar, select **Configuration > Services**. The Services screen displays (see Figure 161 on page 292).

2. Double-click the **Active Directory** row, or select the **Active Directory** row and select **Action > Show Details**. The Active Directory details screen displays.

3. On the Active Directory service details screen, select **Action > Join Domain**. The Join Domain dialog box displays.



Hostname: sm4u-5-combo-50

Figure 163 The Join Domain dialog box.

4. The **Hostname** identifies the BlackPearl 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 Edit the System Name on page 291).

5. Enter the name of the **Active Directory Domain** you want to join.

6. Optionally, enter the **Domain Short Name** if your domain uses a non-standard workgroup name.

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

Notes:
- The BlackPearl 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 gateway joins an Active Directory domain. The gateway does not save this information.

8. If desired, select **Allow Trusted Domains** if the Active Directory domain you want to join is a trusted domain.

9. Click **Join Domain**.

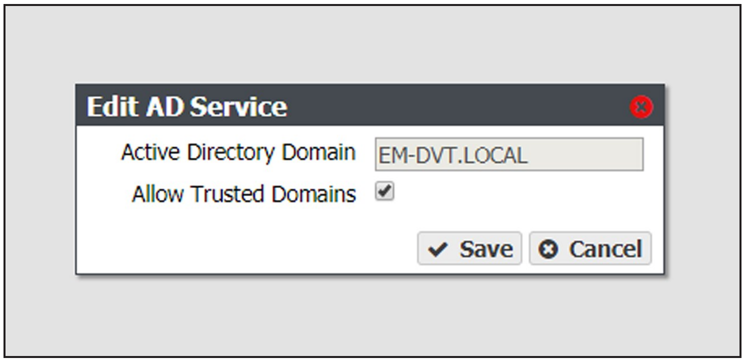
Edit Domain

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

1. From the menu bar, select **Configuration > Services**. The Services screen displays (see Figure 161 on page 292).

2. Double-click the **Active Directory** row, or select the **Active Directory** row and select **Action > Show Details**. The Active Directory details screen displays.

3. Select **Action > Edit**. The Edit AD Service dialog box displays.



Edit AD Service

Active Directory Domain: EM-DVT.LOCAL

Allow Trusted Domains ☑

Figure 164 The Join Domain dialog box.

Note: The **Active Directory Domain** name is unavailable and cannot be changed.

4. Select or clear **Allow Trusted Domains**.

5. Click **Save**.

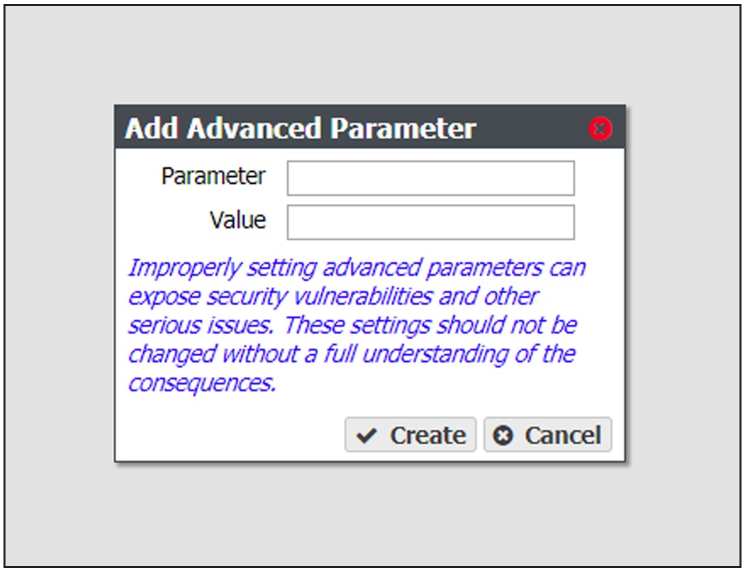
Add Advanced Parameter

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.

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. From the menu bar, select **Configuration > Services**. The Services screen displays (see Figure 161 on page 292).
2. Double-click the **Active Directory** row, or select the **Active Directory** row and select **Action > Show Details**. The Active Directory details screen displays.
3. Select **Action > Add Advanced Parameter**. The Add Advanced Parameter dialog box displays.



Add Advanced Parameter

Improperly setting advanced parameters can expose security vulnerabilities and other serious issues. These settings should not be changed without a full understanding of the consequences.

Figure 165 The Add Advanced Parameter dialog box.

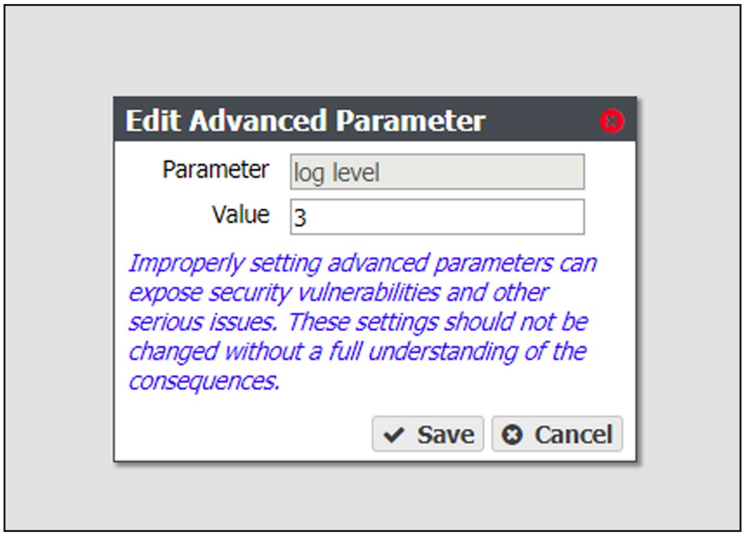
4. Enter the desired **Parameter** and **Value**.
5. Click **Create**.

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.

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. From the menu bar, select **Configuration > Services**. The Services screen displays (see Figure 161 on page 292).
2. Double-click the **Active Directory** row, or select the **Active Directory** row and select **Action > Show Details**. The Active Directory details screen displays.
3. Select the advanced parameter which you want to edit, then select **Action > Edit Advanced Parameter**. The Edit Advanced Parameter dialog box displays.



Edit Advanced Parameter

Parameter: log level

Value: 3

Improperly setting advanced parameters can expose security vulnerabilities and other serious issues. These settings should not be changed without a full understanding of the consequences.

Figure 166 The Edit Advanced Parameter dialog box.

4. The **Parameter** field is greyed-out and cannot be changed.
5. Enter the desired **Value**.
6. Click **Save**.

Delete Advanced Parameter

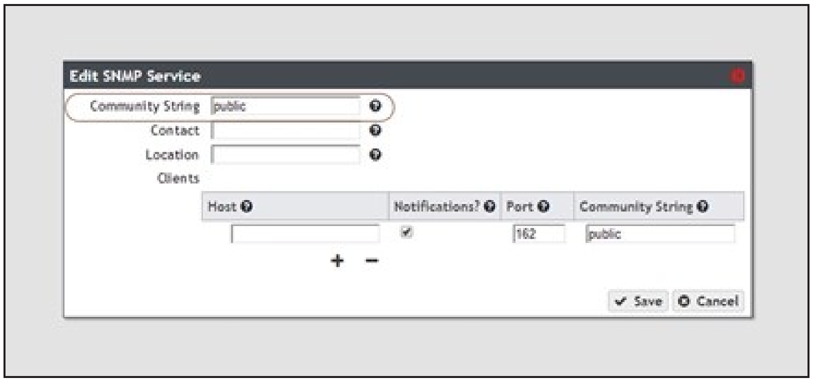
1. From the menu bar, select **Configuration > Services**. The Services screen displays (see Figure 161 on page 292).
2. Double-click the **Active Directory** row, or select the **Active Directory** row and select **Action > Show Details**. The Active Directory details screen displays.
3. Select the advanced parameter which you want to delete, then select **Action > Delete Advanced Parameter**. The Edit Advanced Parameter confirmation window displays.
4. Click **Delete**.

Leave Domain

1. From the menu bar, select **Configuration > Services**. The Services screen displays (see Figure 161 on page 292).
2. Double-click the **Active Directory** row, or select the **Active Directory** row and select **Action > Show Details**. The Active Directory details screen displays.
3. Select **Action > Leave Domain**. A confirmation window displays.
4. Click **Leave Domain**.

Configure the SNMP Service

1. From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 161 on page 292).
2. Double-click the SNMP service, or select the SNMP service and select **Action > Show Details**. The SNMP details screen displays.
3. On the SNMP details screen, select **Action > Edit**. The Edit SNMP Service dialog box displays.



Community String: public

Contact:

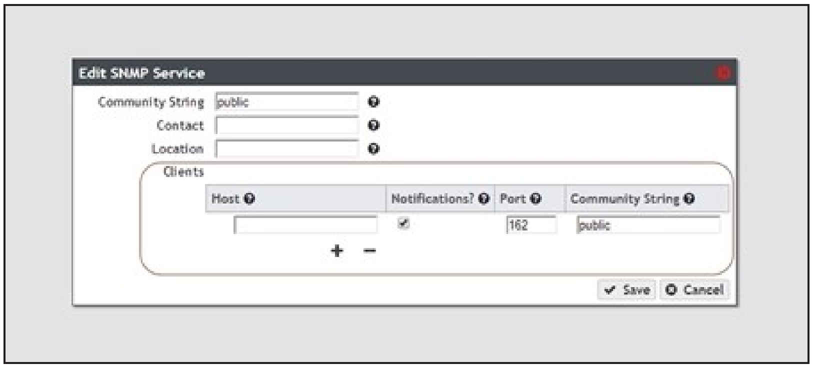
Location:

Clients

Host	Notifications?	Port	Community String
	☑	162	public

Figure 167 The Edit SNMP Service dialog box.

4. 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 gateway responds to all SNMP queries.
5. Enter the primary contact for the BlackPearl gateway in the **Contact** field.
6. Enter the physical location of the gateway in the **Location** field.
7. If desired, add clients that are allowed to access the gateway using SNMP.



Edit SNMP Service

Community String: public

Contact:

Location:

Clients

Host	Notifications?	Port	Community String
	☑	162	public

Figure 168 The Edit SNMP Service dialog box.

a. Click the **+** sign to add a client.
b. Enter the host IP address in the **Host** field.
c. If desired, select the **Notifications** check box to indicate that the SNMP client should receive outgoing notifications.
d. Enter the port number to be used for SNMP communication in the **Port** field.
e. 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.
f. Repeat Step a through Step e as needed to add additional clients.

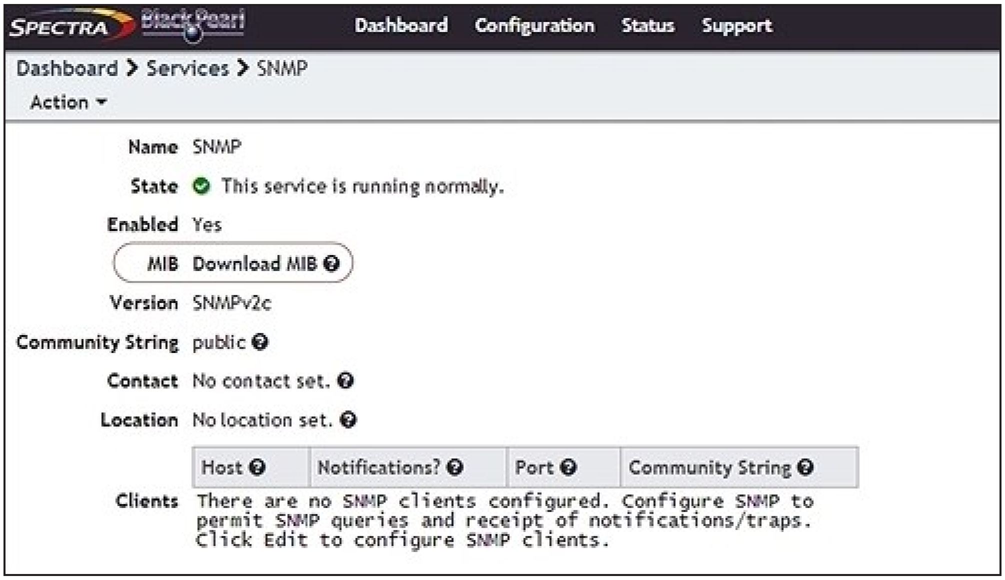
8. Click **Save**.

Download the MIB File

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

1. Select **Configuration > Services** to display the Services screen (see Figure 161 on page 292).
2. Double-click the SNMP service row, or select the SNMP service row and select **Action > Show Details**. The SNMP details screen displays.

3. Click **Download MIB**. Using your web browser, save the file to your local host.



Name SNMP

State ✓ This service is running normally.

Enabled Yes

MIB Download MIB ?

Version SNMPv2c

Community String public ?

Contact No contact set. ?

Location No location set. ?

Clients

Host ?	Notifications? ?	Port ?	Community String ?

```
There are no SNMP clients configured. Configure SNMP to
permit SNMP queries and receipt of notifications/traps.
Click Edit to configure SNMP clients.
```

Figure 169 Download the MIB file.

4. Load the file into the network node manager program.

5. You can now use your network node manager program to communicate with the BlackPearl gateway, using the settings configured in Configure the SNMP Service on page 300.

MULTI-FACTOR AUTHENTICATION

The Spectra BlackPearl Nearline gateway offers multi-factor authentication as part of Attack Hardened storage, which enhances the security of your gateway by using Google Authenticator to confirm the identity of any user trying to log in to the BlackPearl 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 Google Authenticator to complete the account creation. After the QR code is scanned, Google Authenticator generates a six-digit number every 30 seconds, and does not require cell or internet access to generate these codes.

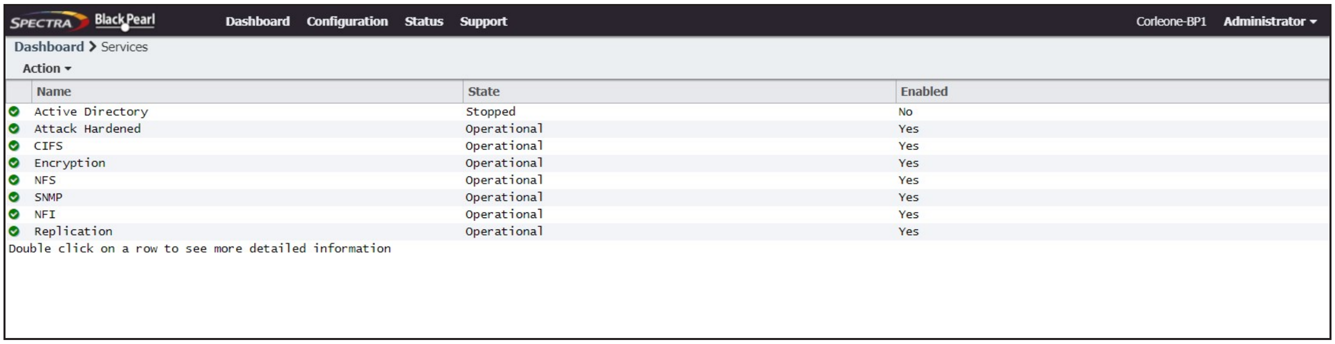
After multi-factor authentication is enabled, when the user attempts to log in to the BlackPearl user interface, after entering their username and password, they must enter the six-digit number generated by Google Authenticator within 30 seconds to complete the log in.

Note: Only Administrator users can configure the Attack Hardened Service and enable Multi-Factor authentication for a user.

Enable the Attack Hardened Service

Before you can enable multi-factor authentication for users, you must enable the Attack Hardened service.

1. Select **Configuration > Services**. The Services screen displays.



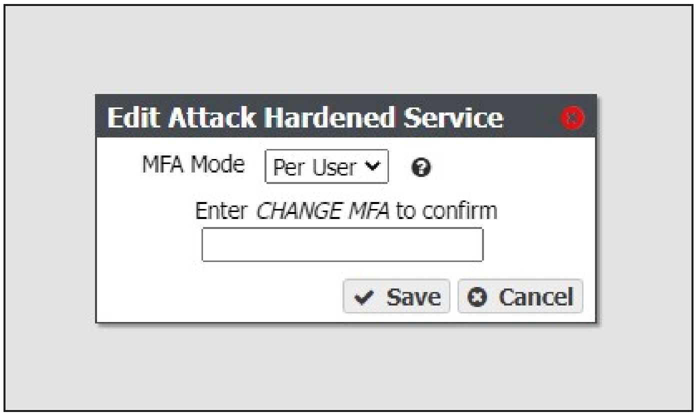
	Name	State	Enabled
✓	Active Directory	Stopped	No
✓	Attack Hardened	Operational	Yes
✓	CIFS	Operational	Yes
✓	Encryption	Operational	Yes
✓	NFS	Operational	Yes
✓	SNMP	Operational	Yes
✓	NFI	Operational	Yes
✓	Replication	Operational	Yes

Double click on a row to see more detailed information

Figure 170 The Services screen.

2. Select the Attack Hardened service row, then select **Action > Edit**. The Edit Attack Hardened Service dialog box displays.

Note: You can also **double-click** the service row to edit the service.



Edit Attack Hardened Service

MFA Mode Per User

Enter *CHANGE MFA* to confirm

Figure 171 The Edit Attack Hardened Service dialog box.

3. Using the **MFA Mode** drop-down menu, select **Per User**.

4. In the dialog box, enter `CHANGE MFA`, then click **Save**.

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.

CAUTION After enabling the service, you must configure each user to use Multi-Factor Authentication before MFA is required for the user to log in to the BlackPearl user interface.

Enable Multi-Factor Authentication for a User

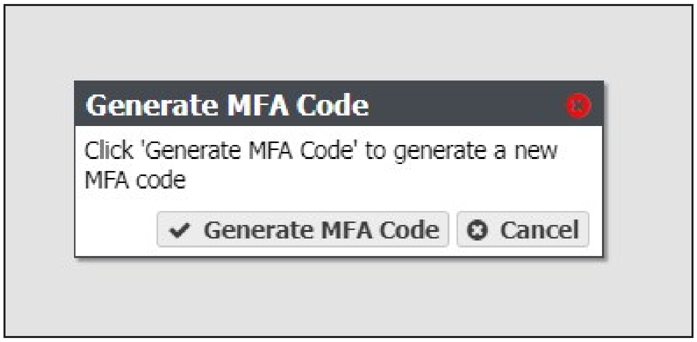
Note: The user account on the target system configured for NAS replication cannot use multi-factor authentication.

1. If necessary, download and install Google Authenticator on your mobile phone.

2. In the BlackPearl user interface, select **Configuration > Users**. The Users screen displays.

3. If necessary, create a new user (see Create a User on page 82), then continue with Step 4.

4. Select the user and then select **Action > Enable MFA**. The Generate MFA Code dialog box displays.

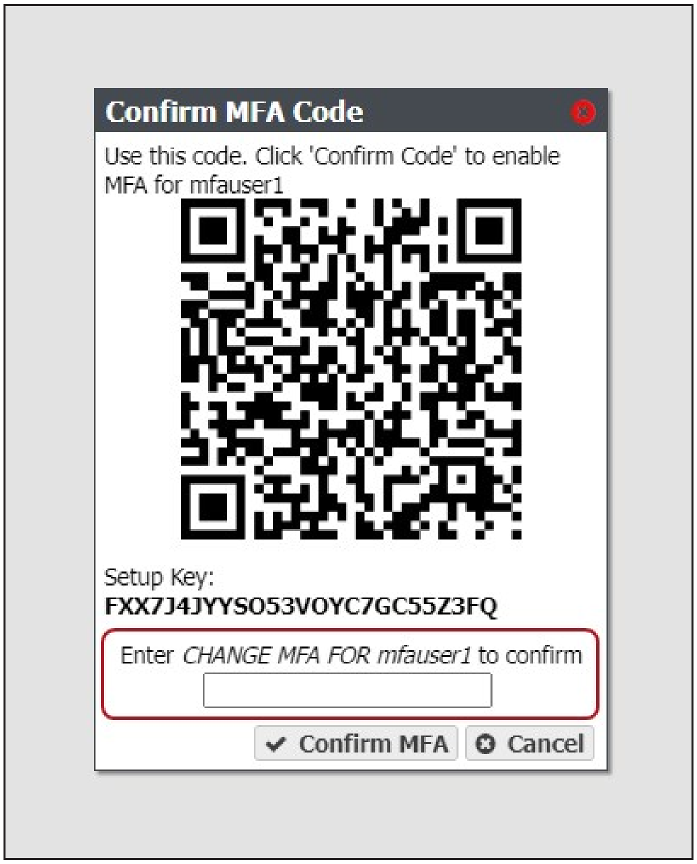


Generate MFA Code

Click 'Generate MFA Code' to generate a new MFA code

Figure 172 The Generate MFA Code dialog box.

5. Click **Generate MFA Code**. The Confirm MFA Code dialog box displays.



Confirm MFA Code

Use this code. Click 'Confirm Code' to enable MFA for mfauser1

Setup Key:
FXX7J4JYYSO53VOYC7GC55Z3FQ

Enter *CHANGE MFA FOR mfauser1* to confirm

Figure 173 The Confirm MFA Code dialog box displaying a users QR code.

6. Use Google Authenticator on your phone to **scan** the QR code displayed in the BlackPearl user interface. The username and BlackPearl system name display in Google Authenticator, and the authenticator begins generating codes for the user.

Note: If you cannot scan the QR code, enter the **Setup Key** into Google Authenticator.

7. In the BlackPearl user interface, in the Confirm MFA Code dialog box, enter `CHANGE MFA FOR` *`user's full name`*, and click **Confirm MFA**.

   The next time the user logs into the BlackPearl user interface, they must use the code generated by Google Authenticator 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 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 334.

3. Enter the **Username** and **Password**.

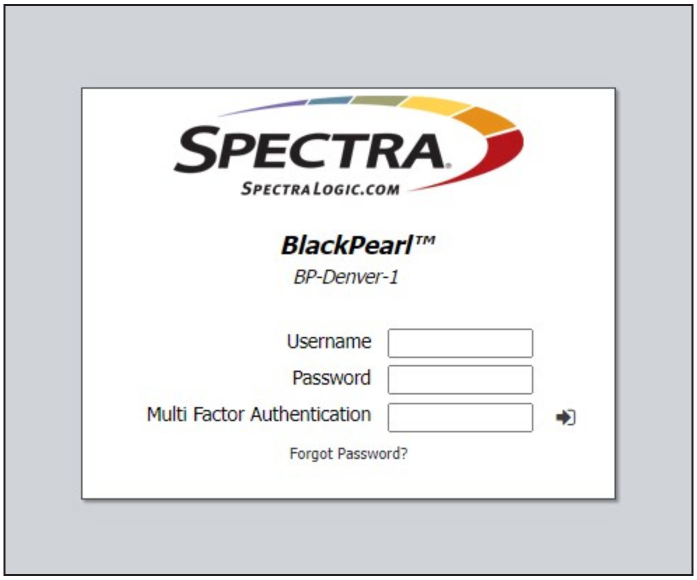


Figure 174 The Login screen with Multi-Factor Authentication enabled on the system.

4. Using Google Authenticator on your phone, enter the six-digit **Multi Factor Authentication** code for the user.

Note: 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.

Note: If you have more than one user or BlackPearl system 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.

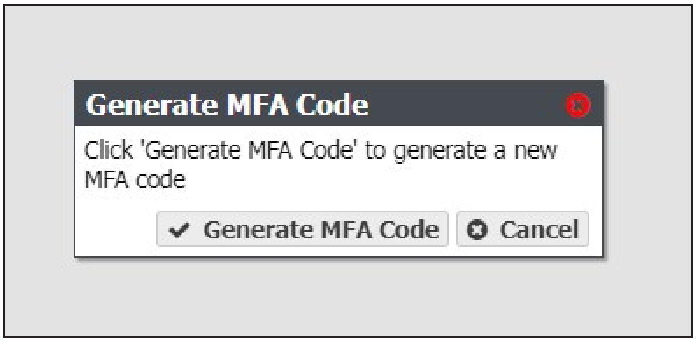
5. Click ➔ to log in.

Update Multi-Factor Authentication for a User

If desired, you can update the token that Google Authenticator 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. In the BlackPearl user interface, select **Configuration > Users**. The Users screen displays.

2. Select the user and then select **Action > Update MFA**. The Generate MFA Code dialog box displays.

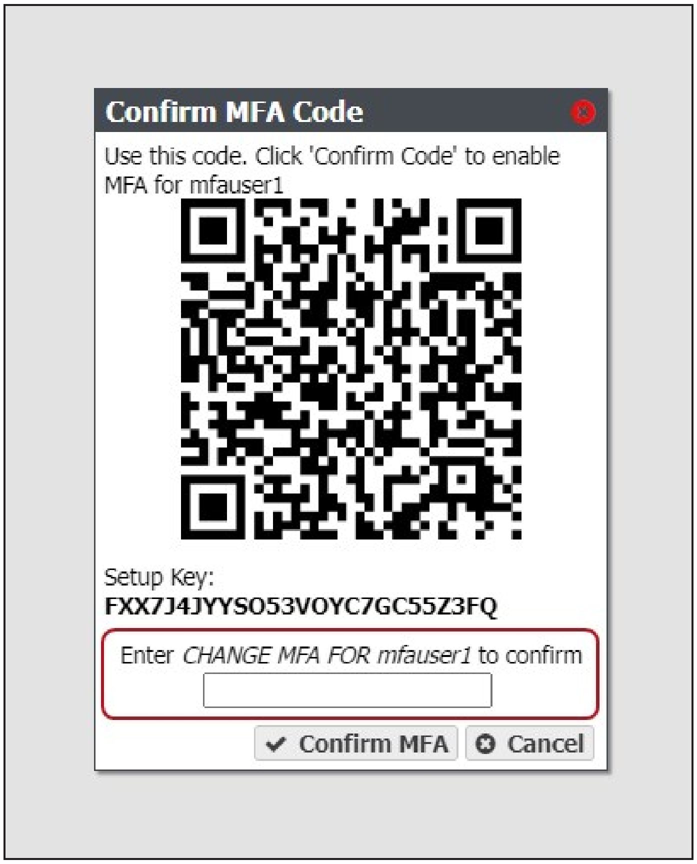


Generate MFA Code

Click 'Generate MFA Code' to generate a new MFA code

Figure 175 The Generate MFA Code dialog box.

3. Click **Generate MFA Code**. The Confirm MFA Code dialog box displays.



Confirm MFA Code

Use this code. Click 'Confirm Code' to enable MFA for mfauser1

Setup Key:
FXX7J4JYYSO53VOYC7GC55Z3FQ

Enter *CHANGE MFA FOR mfauser1* to confirm

Figure 176 The Confirm MFA Code dialog box displaying a users QR code.

4. Use Google Authenticator on your phone to **scan** the QR code displayed in the BlackPearl user interface. The username and BlackPearl system name display in Google Authenticator, and the authenticator begins generating codes for the user.

Note: If you cannot scan the QR code, enter the **Setup Key** into Google Authenticator.

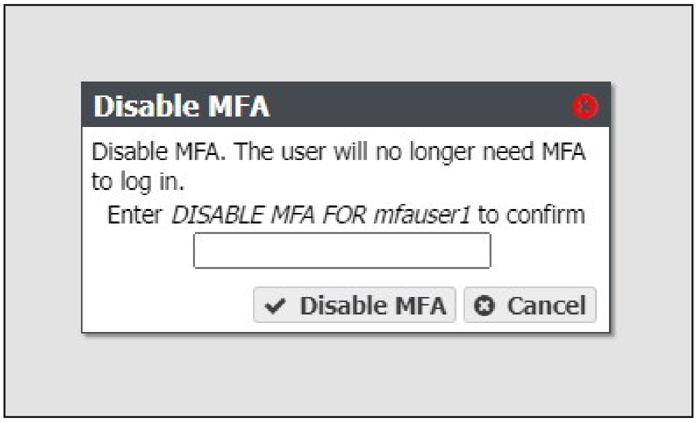
5. In the BlackPearl user interface, in the Confirm MFA Code dialog box, enter `CHANGE MFA FOR` *`user's full name`*, and click **Confirm MFA**.

   The next time the user logs into the BlackPearl user interface, they must use the code generated by Google Authenticator to complete the login.

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. In the BlackPearl user interface, select **Configuration > Users**. The Users screen displays.
2. Select the user and then select **Action > Disable MFA**. The Disable MFA dialog box displays.



Disable MFA

Disable MFA. The user will no longer need MFA to log in.

Enter *DISABLE MFA FOR mfauser1* to confirm

Figure 177 The Disable MFA dialog box.

3. In the dialog box, enter `DISABLE MFA FOR` *`user's full name`*, and click **Disable MFA**.

   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 BlackPearlgateway.

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 Update Multi-Factor Authentication for a User on page 307)

1. Select **Configuration > Services**. The Services screen displays (see Figure 170 on page 303).

2. Select the Attack Hardened service row, then select **Action > Edit**. The Edit Attack Hardened Service dialog box displays (see Figure 171 on page 304).

Note: You can also **double-click** the service row to edit the service.

3. Using the **MFA Mode** drop-down menu, select **Off**.
4. In the dialog box, enter `CHANGE MFA`, and then click **Save**.

Configure a Vail Sphere

Use the instructions in this section to configure the BlackPearl gateway to communicate with a Vail sphere. After registering with a Vail sphere, you can create S3 buckets or NAS-based Vail S3 shares on the BlackPearl gateway.

Notes:

- You can only register or edit a Vail sphere after entering a Vail activation key. See Manually Enter Activation Keys on page 338.
- All other aspects of the Vail application are controlled in the Vail management console. See the *Vail User Guide* for information on configuring and using the Vail application.

Register with a Vail Sphere

The Vail service configures a BlackPearl gateway for use with a Spectra Vail sphere. The Vail service only displays in the Services menu after an activation key is entered. Use the instructions in this section to register a Vail sphere with a BlackPearl gateway.

See the *Vail Online Help* for information about registering the BlackPearl Nearline gateway with a Vail sphere.

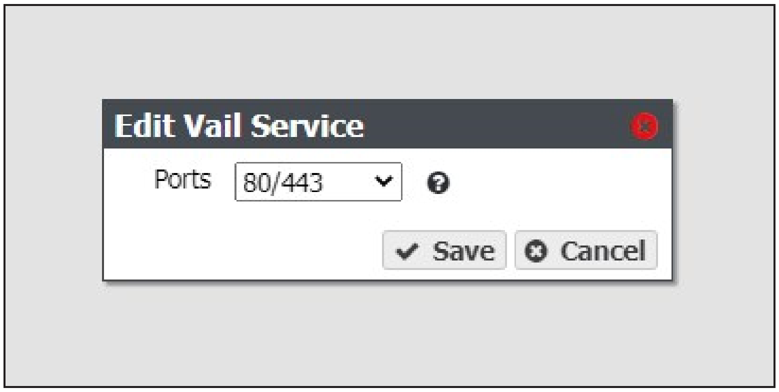
Note: These instructions will be updated in the next revision of the BlackPearl User Guide.

Edit the Vail Service

If desired, you can change the ports that the BlackPearl gateway uses to communicate with a Vail sphere.

1. From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 161 on page 292).
2. Double-click the Sphere service, or select the service, and then select **Action > Show Details**. The details screen for the Sphere service displays.

3. Select **Action > Edit**. The Edit Vail Service dialog box displays.



Edit Vail Service

Ports 80/443

Figure 178 The Edit Vail Service dialog box.

4. Use the **Ports** drop-down menu to select the desired ports.
5. Click **Save**.

Configure and Use Encryption

If your BlackPearl gateway includes disk or flash 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 27* 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.

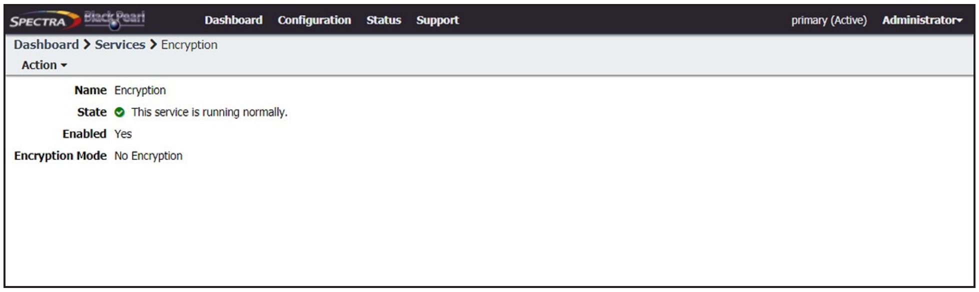
Configure the Encryption Service

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.

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 338.
2. From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 161 on page 292).
3. Double-click the Encryption service, or select the service, and then select **Action > Show Details**. The details screen for the Encryption service displays.

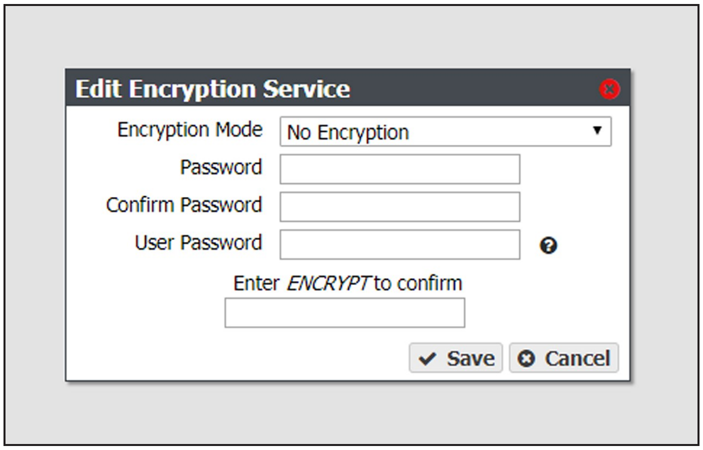


Name Encryption
State This service is running normally.
Enabled Yes
Encryption Mode No Encryption

Figure 179 The Encryption service details screen.

4. Select **Action > Edit Service**.The Edit Encryption Service dialog box displays.

Note: If multi-factor authorization is enabled for the user currently logged in to the BlackPearl user interface, an additional entry field displays in the Edit Encryption Service dialog box.



Edit Encryption Service

Encryption Mode: No Encryption

Password

Confirm Password

User Password

Enter *ENCRYPT* to confirm

Figure 180 The Edit Encryption Service dialog box.

5. Use the **Encryption Mode** drop-down menu to set the encryption mode.

Parameter	Description
No Encryption	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 Encrypt or Decrypt a Storage Pool on page 320 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 gateway. The drives are automatically unlocked when the BlackPearl 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 systems to the storage architecture that may access the encrypted drives. Spectra Logic recommends storing multiple copies of the password. ⚠ 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 systems to the storage architecture that may access the encrypted drives. Spectra Logic recommends storing multiple copies of the password.

Parameter	Description
Encrypt and Don't Store Password	The self-encrypting drives encrypt data transferred to them, but the BlackPearlgateway does not store the password to unlock the drives. You must manually enter the password each time the BlackPearlgateway initializes. **Note:** This option is no longer available starting with BlackPearl OS 5.6. This setting is also allows you to create a USB device with the encryption password. You can use the USB device when the gateway initializes to unlock the drives. Store the USB device in a safe location, not attached to the BlackPearlgateway, at all other times. ⚠ **CAUTION** Since the password is not stored on the system, you must record and store multiple copies of the password using either USB drives and/or manual records to avoid losing access to the encrypted data. ⚠ **CAUTION** Since the password is not stored on the system, you must record and store multiple copies of the password using either USB drives and/or manual records to avoid losing access to the encrypted data.

6. Enter a **Password** to unlock the self-encrypting drives, and then **Confirm** the password.
7. Enter the **User Password** of the user currently logged in to the BlackPearl user interface.
8. If necessary, enter the **Multi Factor Authentication** code for the user. See Multi-Factor Authentication on page 303 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.

9. Enter `ENCRYPT` into the confirmation dialog box.
10. Click **Save**.

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.

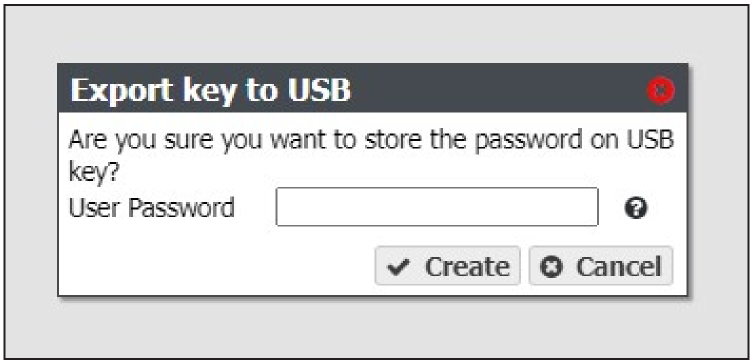
CAUTION Spectra Logic recommends creating and storing multiple copies of the password used to encrypt data to avoid losing access to encrypted data. Additionally, Spectra Logic recommends exporting the encryption key to multiple types of storage media. See Email the Encryption Key on the next page

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 Email the Encryption Key on the next page

If your BlackPearl system is running BlackPearl OS 5.5 or earlier, and if the encryption service is configured to not store the password on the BlackPearl gateway, the USB key can be used to unlock the encrypted drives when the BlackPearl system initializes. Insert the USB key when the gateway initializes to unlock the drives. Remove it from the gateway USB port and store it in a safe location at all other times.

Note: This feature is no longer available starting with BlackPearl OS 5.6.

1. From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 161 on page 292).
2. Double-click the Encryption service, or select the service, and then select **Action > Show Details**. The details screen for the Encryption service displays.
3. Select **Action > Export Key to USB**. The Export key to USB confirmation window displays.



Export key to USB

Are you sure you want to store the password on USB key?

User Password

Figure 181 The Export key to USB confirmation window.

4. Enter the **User Password** of the user currently logged into the BlackPearl user interface.
5. Click **Create**.

Note: Once created, remove the USB key from the gateway and store it in a safe location until it is needed.

Email the Encryption Key

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.

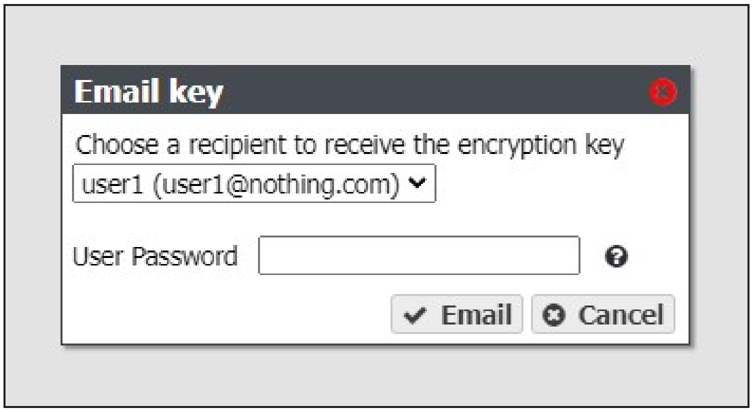
CAUTION Spectra Logic recommends creating and storing multiple copies of the password used to encrypt data to avoid losing access to encrypted data. Additionally, Spectra Logic recommends exporting the encryption key to multiple types of storage media. See Export Encryption Key to USB Drive on the previous page

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 Export Encryption Key to USB Drive on the previous page

You must configure an email recipient and an SMTP server before you can email the encryption key. If necessary, use the instructions in the sections below.

- **Configure Mail Recipients on page 455**
- **Configure SMTP Settings on page 288**

1. From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 161 on page 292).
2. Double-click the Encryption service, or select the service, and select **Action > Show Details**. The details screen for the Encryption service displays.
3. Select **Action > Email key**. The Email key confirmation window displays.



Email key

Choose a recipient to receive the encryption key

user1 (user1@nothing.com)

User Password

Figure 182 The Email key confirmation window.

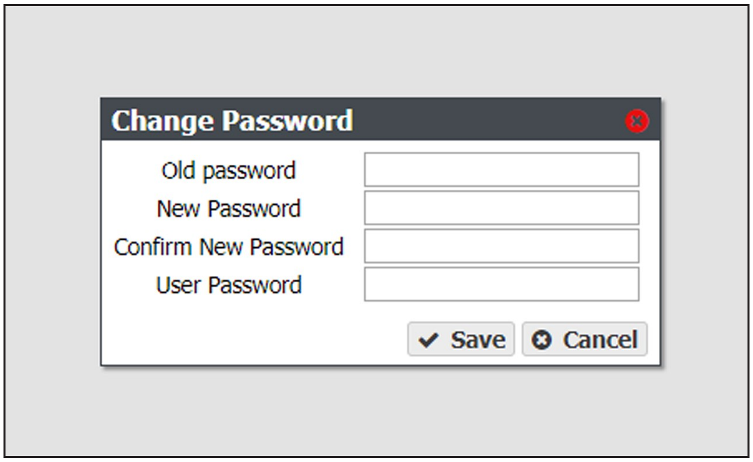
4. Use the drop-down menu to select an **email recipient** to receive the encryption key.
5. Enter the **User Password** for the currently logged into the BlackPearl user interface.
6. Click **Email**.

Change the Encryption Password

If desired, you can change the password used to unlock the self-encrypting drives.

1. From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 161 on page 292).
2. Double-click the Encryption service, or select the service, and then select **Action > Show Details**. The details screen for the Encryption service displays.
3. Select **Action > Change Password**. The Change 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 Password dialog box.



Change Password

Old password

New Password

Confirm New Password

User Password

Figure 183 The Change Password dialog box.

4. Enter the (current) **Old Password**.

5. Enter the desired **New Password**, and then **Confirm** the new 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. See Multi-Factor Authentication on page 303 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. Click **Save**.

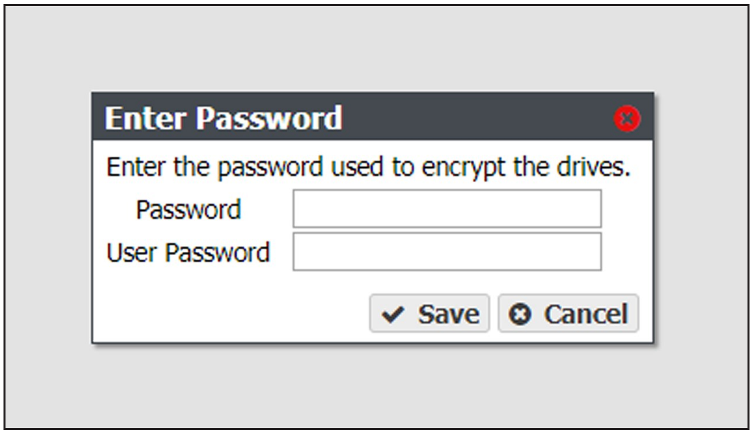
IMPORTANT After changing the password, update the USB keys and/or manual records stored in secure locations. See Export Encryption Key to USB Drive on page 316.

IMPORTANT After changing the password, update the USB keys and/or manual records stored in secure locations. See Export Encryption Key to USB Drive on page 316.

Unlock the Self-Encrypting Drives

If necessary, use the instructions below to manually unlock the self-encrypting drives after the gateway initializes.

1. From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 161 on page 292).
2. Double-click the Encryption service, or select the service, and then select **Action > Show Details**. The details screen for the Encryption service displays.
3. Select **Action > Unlock Drives**. The Enter Password dialog box displays.



Enter Password

Enter the password used to encrypt the drives.

Password

User Password

Figure 184 The Enter Password dialog box.

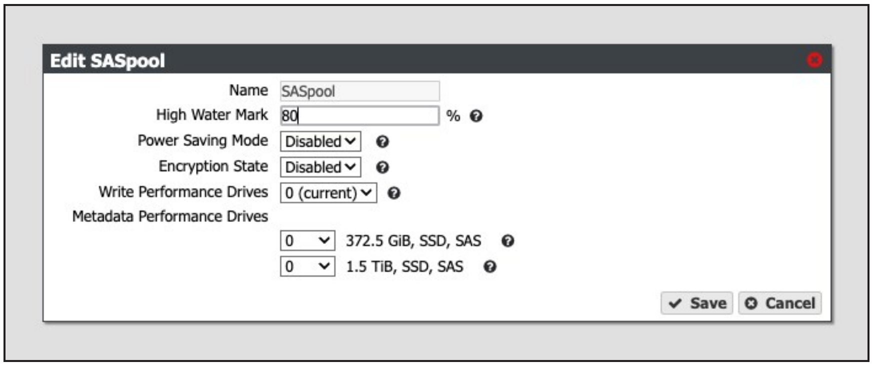
4. Enter the encryption **Password**.

5. Enter the **User Password** of the user currently logged in to the BlackPearl user interface.
6. Click **Save**.

Encrypt or Decrypt a Storage Pool

Use the steps in this section to encrypt or decrypt the drives in a storage pool after creating the pool.

1. From the menu bar, select **Configuration > NAS > Pools**.
2. Select the disk pool for which you want to enable encryption, then select **Action > Edit**.



Edit SASpool

Name: SASpool
High Water Mark: 80 %
Power Saving Mode: Disabled
Encryption State: Disabled
Write Performance Drives: 0 (current)
Metadata Performance Drives:
0 372.5 GiB, SSD, SAS
0 1.5 TiB, SSD, SAS

Figure 185 The Edit *storage pool* dialog box.

3. Using the **Encryption State** drop-down menu, select **Enabled** to encrypt the drives in the pool or **Disabled** to decrypt the drives.
4. If desired, make any other changes as described in Edit a Storage Pool on page 248.
5. Click **Save**.

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.

CAUTION Performing a PSID Erase on a drive makes all data on the drive permanently inaccessible.

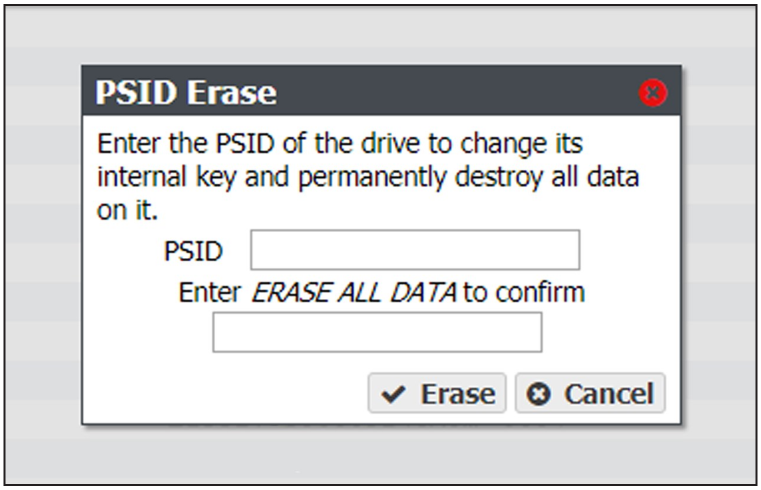
Use the instructions in this section to perform a PSID erase on the drive.

1. From the menu bar, select **Status > Hardware** or click the Hardware pane on the Dashboard, or click the Hardware link on the status bar. The Hardware screen displays (see Figure 262 on page 422).
2. Click **Data Drives**. The hardware screen refreshes and displays all disk drives present in the gateway.
3. Record the slot number and serial number for each drive you want to PSID erase.
4. Power down the gateway as described in Reboot or Shut Down a BlackPearl Gateway on page 451.
5. Locate the drive(s) in the chassis using the slot number and verify the serial number(s) you recorded in Step 3.
6. Locate the PSID value on the drive label and record the value.
7. Repeat Step 5 and Step 6 for any additional drives you want to erase.
8. Power on the gateway as described in Power On the Gateway on page 69.
9. Log into the gateway as described in Log Into the BlackPearl User Interface on page 74.

10. From the menu bar, select **Status > Hardware** or click the Hardware pane on the Dashboard, or click the Hardware link on the status bar. The Hardware screen displays (see Figure 262 on page 422).

11. Click **Data Drives**. The hardware screen refreshes and displays all disk drives present in the gateway.

12. 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 186 The PSID Erase dialog box.

13. Enter the PSID value you recorded in Step 6 on page 321 in the **PSID** entry field.

14. Type `ERASE ALL DATA` in the confirmation entry field.

CAUTION Performing a PSID Erase on a drive permanently erases all data on the drive.

CAUTION Performing a PSID Erase on a drive permanently erases all data on the drive.

15. Click **Erase**.

16. Repeat Step 12 through Step 15 for any additional drives you want to erase.

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 Types 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

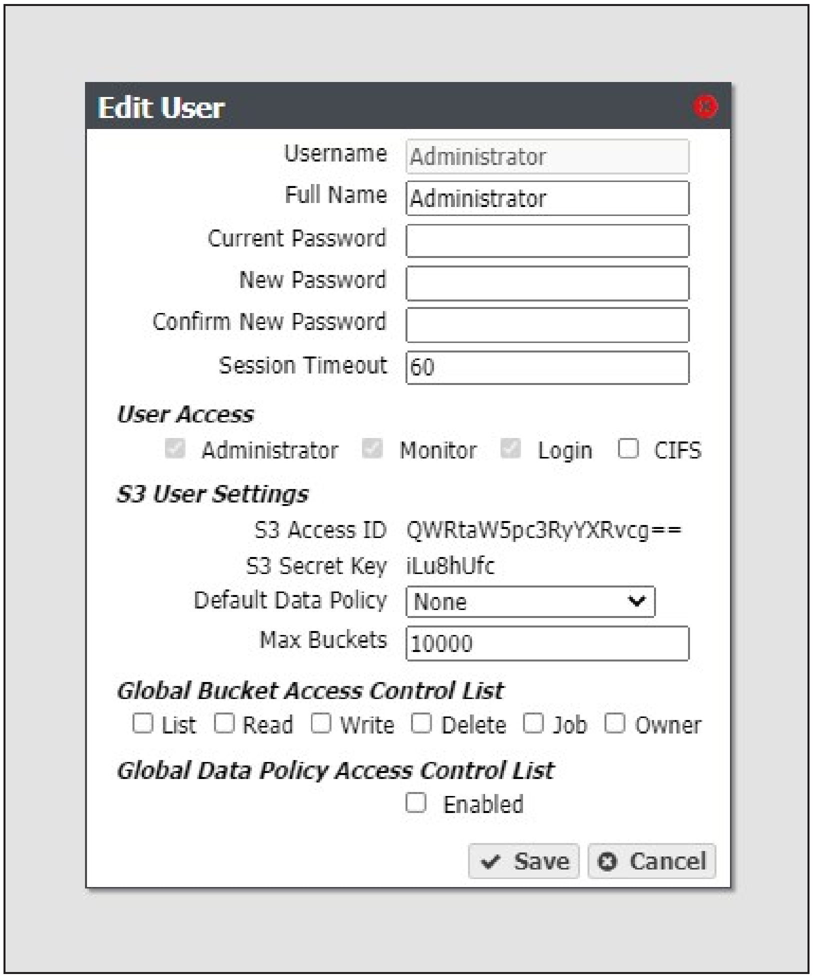
There are two methods you can use to edit a user, through the User screen, or the User Profile screen.

Note: If you use the User Profile screen to edit a user, you are only able to change the password, session timeout, and full name of the user.

Using the Users Screen

1. From the menu bar, select **Configuration > Users**. The Users screen displays a list of all configured users (see Figure 31 on page 83).

2. Double-click the name of the user you want to edit, or select the user and then select **Action > Edit**. The Edit Users dialog box displays.



Username: Administrator
Full Name: Administrator
Current Password:
New Password:
Confirm New Password:
Session Timeout: 60

User Access
☑ Administrator ☑ Monitor ☑ Login □ CIFS

S3 User Settings
S3 Access ID: QWRtaW5pc3RyYXRvcg==
S3 Secret Key: iLu8hUfc
Default Data Policy: None
Max Buckets: 10000

Global Bucket Access Control List
□ List □ Read □ Write □ Delete □ Job □ Owner

Global Data Policy Access Control List
□ Enabled

Figure 187 The Edit User dialog box.

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 desired **New Password**, then **Confirm New 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 450).

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 Types on page 82 for information on each level of user access permission.

8. The **S3 Access ID** and **S3 Secret Key** fields are unavailable cannot be changed when editing a user. To change the S3 secret key, see Change S3 Secret Key on page 326.

9. If desired, using the drop-down menu, select a different **Default 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.

10. If desired, edit the value for the **Max Buckets** the user is allowed to create.

11. 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.

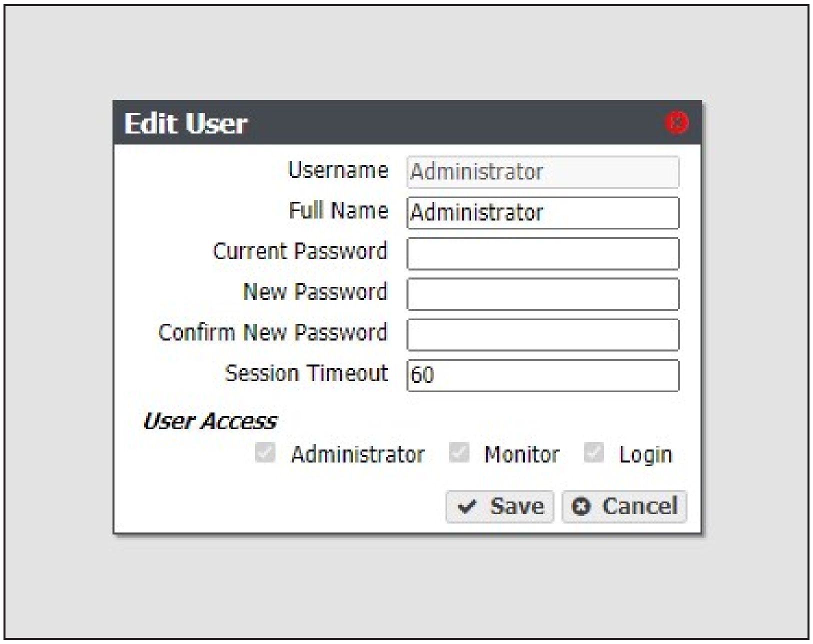
12. Under **Global Data Policy Access Control List**, select the **Enabled** to allow the user access to any data policy created on the gateway.

13. Click **Save**.

Using the User Profile Screen

1. From the right side of the menu bar, select ***Current User*>** **User Profile**. The User Profile screen displays.

2. Select **Action >Edit**. The Edit User Screen displays.



Edit User

Username	Administrator
Full Name	Administrator
Current Password	
New Password	
Confirm New Password	
Session Timeout	60

User Access

☑ Administrator ☑ Monitor ☑ Login

Figure 188 The Edit User dialog box.

3. If desired, edit the user’s **Full Name**.
4. If you are changing the password, enter the desired **New Password**, then **Confirm New 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 450).

5. If desired, edit the value for the **Session Timeout** in minutes. This value cannot exceed 999 minutes.
6. Click **Save**.

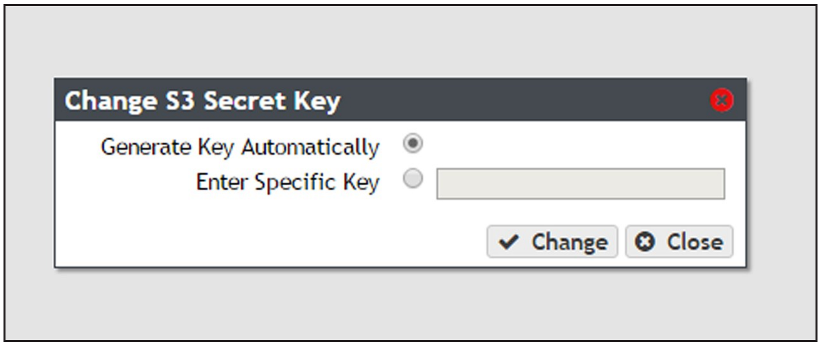
Change S3 Secret Key

If an S3 secret key is compromised, or you otherwise want to change it, use the instructions in this section to change an S3 secret key for a user. There are two methods you can use to change S3 credentials, through the User screen, or the User Profile screen.

Using the Users Screen

1. From the menu bar, select **Configuration > Users**. The Users screen displays a list of all configured users (see Figure 31 on page 83).

2. Select the user for which you want to change the S3 secret key, and then select **Action > Change S3 Secret Key**. The Change S3 Secret Key window displays.



Change S3 Secret Key

Generate Key Automatically ●

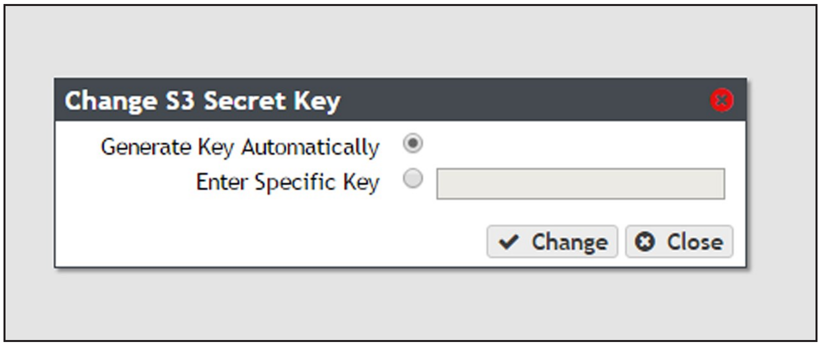
Enter Specific Key ○

Figure 189 The Change S3 Secret Key dialog box.

3. Select either **Generate Key Automatically** or **Enter Specific Key**.
4. Optionally, if you selected **Enter Specific Key**, enter the desired key in the entry box.
5. Click **Change** to change the S3 secret key for the user.

Using the User Profile Screen

1. From the right side of the menu bar, select ***Current User*> User Profile**. The User Profile screen displays.
2. Select **Action > Change S3 Secret Key**. The Change S3 Secret Key window displays.



Change S3 Secret Key

Generate Key Automatically ●

Enter Specific Key ○

Figure 190 The Change S3 Secret Key dialog box.

3. Select either **Generate Key Automatically** or **Enter Specific Key**.
4. Optionally, if you selected **Enter Specific Key**, enter the desired key in the entry box.
5. Click **Change** to change the S3 secret key for the user.

Delete a User

1. From the menu bar, select **Configuration > Users**. The Users screen displays a list of all configured users and S3 groups (see Figure 31 on page 83).

2. Select the user you want to delete, and then select **Action > Delete**. A confirmation window displays.
3. Click **Delete** to delete the user.

CONFIGURE S3 GROUPS

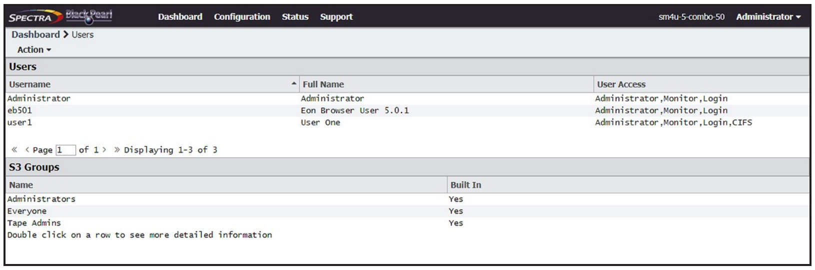
Use the instructions in this section to create, edit, or delete an S3 user group.

Create an S3 Group

An S3 group on the BlackPearl gateway is a group of previously created 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 S3 group.

1. From the menu bar, select **Configuration > Users.** The Users screen displays.



Users

Username	Full Name	User Access
Administrator	Administrator	Administrator,Monitor,Login
eb501	Eon Browser User 5.0.1	Administrator,Monitor,Login
user1	User One	Administrator,Monitor,Login,CIFS

« ‹ Page 1 of 1 › » Displaying 1-3 of 3

S3 Groups

Name	Built In
Administrators	Yes
Everyone	Yes
Tape Admins	Yes

Double click on a row to see more detailed information

Figure 191 The Users screen.

2. Select **Action > New S3 Group** from the menu bar. The New S3 Group dialog box displays.

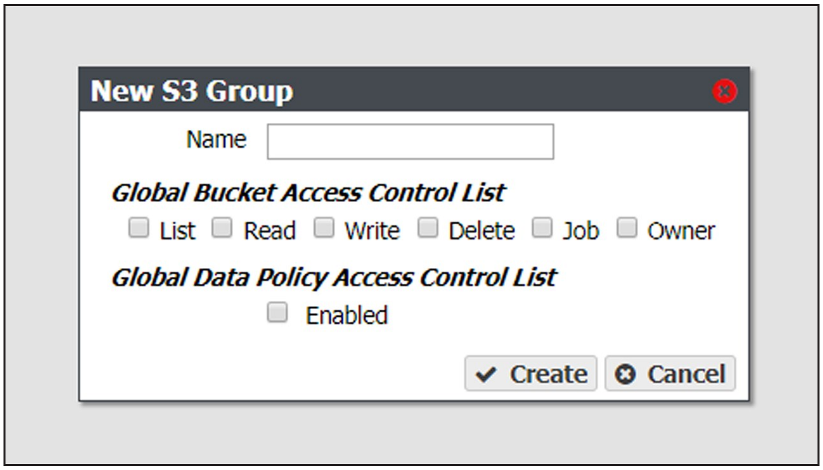

New S3 Group
Name
Global Bucket Access Control List
□ List □ Read □ Write □ Delete □ Job □ Owner
Global Data Policy Access Control List
□ Enabled
✓ Create
Cancel

Figure 192 The New S3 Group dialog box.

3. Enter the desired **Name** for the group.

4. Select or clear options for the **Global Bucket Access Control List**. 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 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 S3 group that has Write permission, the user now has both Read and Write permissions.

Name	Description
List	The S3 group can see the bucket and can list the objects in a bucket.
Read	The S3 group can get objects and create GET jobs.
Write	The S3 group can put objects and create PUT jobs.
Delete	The S3 group can delete objects, but cannot delete the bucket.
Job	The S3 group can modify or cancel jobs created by other users. The 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 S3 group receives full access to all buckets, including all permissions listed above.

5. Under **Global Data Policy Access Control List**, select **Enabled** to allow the user access to any data policy created on the gateway.

6. Click **Create** to create the new S3 group.

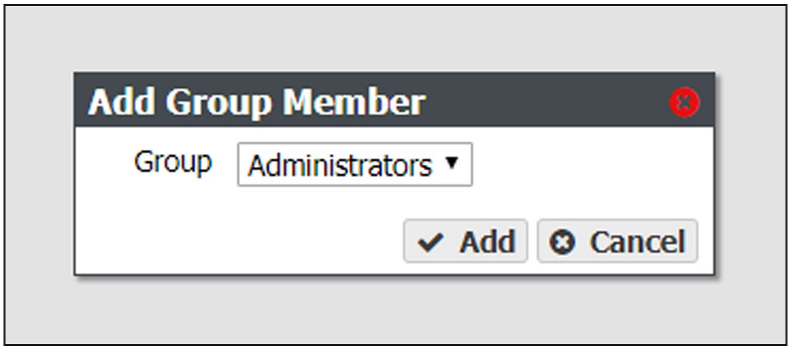
   Use the instructions below to add groups or individual users to the S3 group.

Add a Group Member to an S3 Group

1. From the menu bar, select **Configuration > Users**. The Users screen displays (see Figure 191 on page 329).

2. Double-click the S3 group to which you want to add a different S3 group as a member, or select the group and from the menu bar select **Action > Show Details**.

3. From the menu bar, select **Action > Add Group Member**. The Add Group Member dialog box displays.



Add Group Member

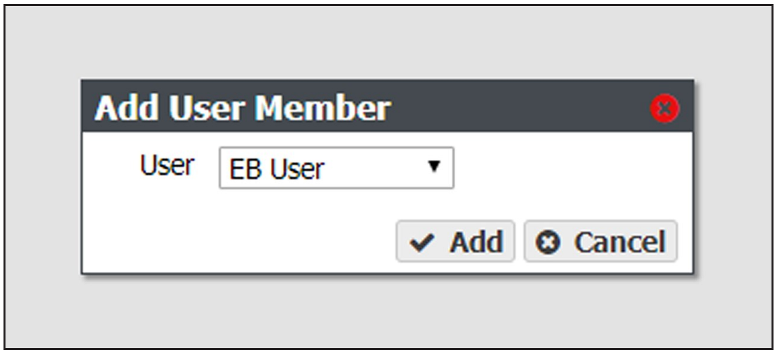
Group Administrators

Figure 193 The Add Group Member dialog box.

4. Using the **Group** drop-down menu, select the S3 group to add as a member.
5. Click **Add**.

Add a User Member to an S3 Group

1. From the menu bar, select **Configuration > Users**. The Users screen displays (see Figure 191 on page 329).
2. Double-click the S3 group to which you want to add an individual user as a member, or select the group and from the menu bar select **Action > Show Details.**
3. From the menu bar, select **Action > Add User Member**. The Add Group Member dialog box displays.



Add User Member

User EB User

Figure 194 The Add User Member dialog box.

4. Using the **User** drop-down menu, select the user to add as a member.
5. Click **Add**.

Remove an S3 Group Member

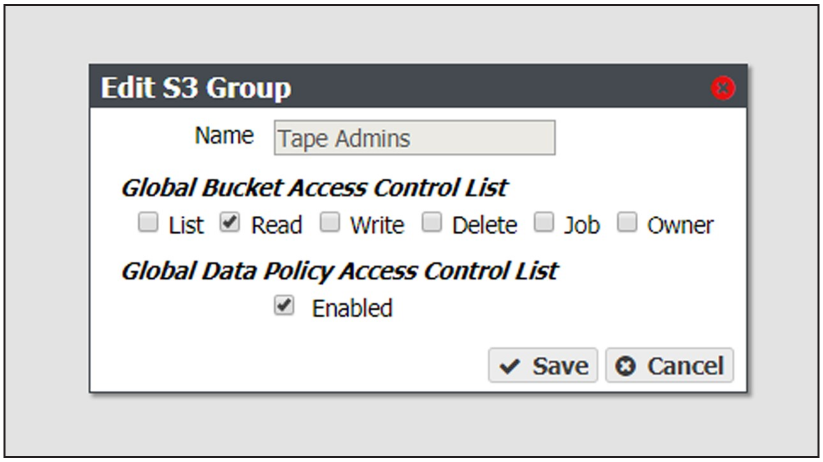
Use the following instructions to remove a group or user from an S3 group.

1. From the menu bar, select **Configuration > Users**. The Users screen displays (see Figure 191 on page 329).
2. Double-click the S3 group from which you want to remove an individual user or group as a member, or select the group and from the menu bar select **Action > Show Details**.
3. From the menu bar, select **Action > Remove Member**. The Remove Member confirmation screen displays.
4. Click **Delete**.

Edit an S3 Group

Use the following instructions to edit an S3 group.

1. From the menu bar, select **Configuration > Users**. The Users screen displays (see Figure 191 on page 329).
2. Select the S3 group which you want to edit and from the menu bar select **Action > Edit**. The Edit S3 Group dialog box displays.



Edit S3 Group

Name: Tape Admins

Global Bucket Access Control List

□ List ☑ Read □ Write □ Delete □ Job □ Owner

Global Data Policy Access Control List

☑ Enabled

Figure 195 The Edit S3 Group dialog box.

3. If desired, select or clear options for the **Global Bucket Access Control List**. 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. See Create an S3 Group on page 329 for a description of each user type.
4. Under **Global Data Policy Access Control List**, select **Enabled** to allow the user access to any data policy created on the gateway.
5. Click **Save**.

Delete an S3 Group

1. From the menu bar, select **Configuration > Users**. The Users screen displays a list of all configured users and S3 groups (see Figure 31 on page 83).

2. Select the S3 group you want to delete, and then select **Action > Delete**. A confirmation window displays.
3. Click **Delete** to delete the S3 group.

CONFIGURE CERTIFICATES

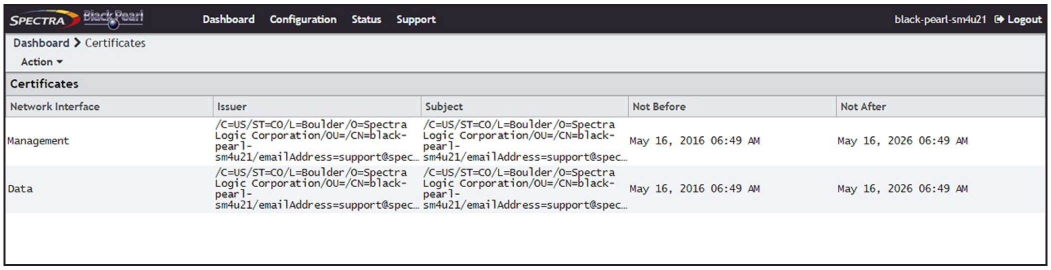
The BlackPearl gateway ships with non-signed SSL certificates for both the data and management ports on the gateway. Because the certificates are not signed, you must pass a security check every time you attempt to access the management port to view the BlackPearl user interface, or when you attempt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

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

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

1. From the menu bar, select **Configuration > Certificates**. The Certificates screen displays.



Certificates

Network Interface	Issuer	Subject	Not Before	Not After
Management	/C=US/ST=CO/L=Boulder/O=Spectra Logic Corporation/OU=/CN=black-pearl-sm4u21/emailAddress=support@spec…	/C=US/ST=CO/L=Boulder/O=Spectra Logic Corporation/OU=/CN=black-pearl-sm4u21/emailAddress=support@spec…	May 16, 2016 06:49 AM	May 16, 2026 06:49 AM
Data	/C=US/ST=CO/L=Boulder/O=Spectra Logic Corporation/OU=/CN=black-pearl-sm4u21/emailAddress=support@spec…	/C=US/ST=CO/L=Boulder/O=Spectra Logic Corporation/OU=/CN=black-pearl-sm4u21/emailAddress=support@spec…	May 16, 2016 06:49 AM	May 16, 2026 06:49 AM

Figure 196 The Certificates screen.

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

3. Select **Action > Import Certificate**. The Import Certificate dialog box displays.

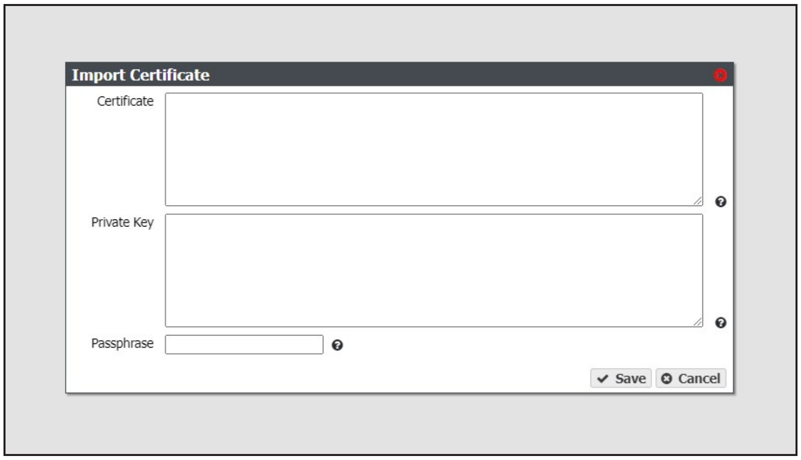


Figure 197 The Import Certificate dialog box.

4. From your source SSL certificate file, copy the certificate portion of the file into your host's cache, and then 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 into your host's cache, and then 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.

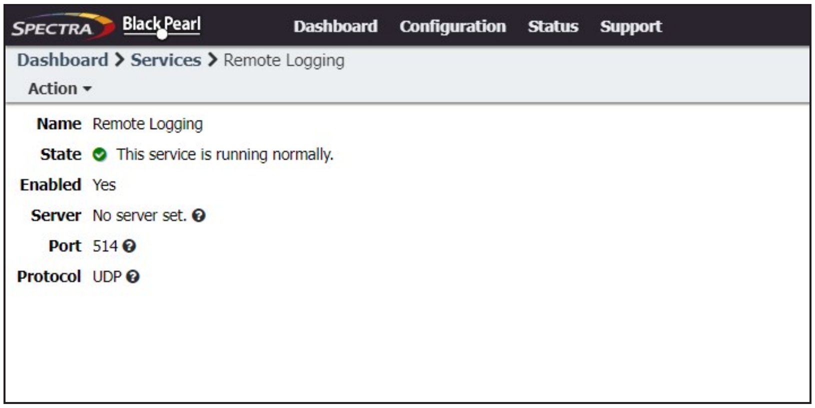
7. Click **Save**.

ENABLE REMOTE LOGGING

Remote Logging is a feature that allows the BlackPearl system to send any messages generated by the system to a syslog server.

Use the instructions in this section to enable remote logging.

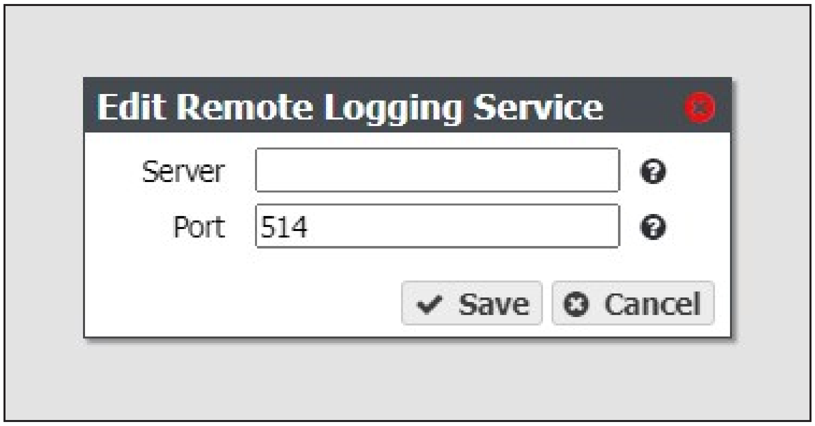
1. Enter the Remote Logging activation key as described in Manually Enter Activation Keys on page 338.
2. From the menu bar, select **Configuration > Services**. The Services screen displays.
3. Double-click the **Remote Logging** service, or select the service and then select **Action > Show Details**. The details screen for the remote logging service displays.



Name Remote Logging
State This service is running normally.
Enabled Yes
Server No server set.
Port 514
Protocol UDP

Figure 198 The Remote Logging Service details screen.

4. Select **Action > Edit**. The Edit Remote Logging Service dialog box displays.


Edit Remote Logging Service

Server

Port 514

Figure 199 The Edit Remote Logging Service dialog box.

5. Enter a hostname or IP address for the remote logging **Server**.
6. Enter the **Port** used to communicate with the remote logging server.

Note: The default port is 514.

7. Click **Save**.

Manually Enter Activation Keys

If this is an initial installation and your BlackPearl documentation kit included a USB device, see Automatically Import Activation Keys on page 68 for instructions for importing activation keys.

Note: After entering certain Product keys, the system automatically reboots. Starting with BlackPearl OS 5.4.2, after the system initializes, you are automatically logged into the BlackPearl management interface and do not need to enter login information.

Use the following instructions to manually enter activation keys.

1. Determine the order for installing the activation keys.

- If this is not an initial installation, you can enter activation keys in any order. Proceed with Step 2 on page 340.
- If you want to manually enter the activation keys for an initial installation, they must be entered in the following order

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.

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.

a. Capacity keys

Key Type	Description
NAS/S3 SAS Count	Enables the specified number of SAS drives present in the system for NAS storage and S3 pools.
NAS/S3 SATA Count	Enables the specified number of SATA drives present in the system for NAS storage and S3 pools.
NAS/S3 SSD Count	Enables the specified number of SSDs present in the system for NAS storage and S3 pools.
DS3 & on premise Glacier SAS Count	Enables the specified number of SAS drives present in the system for cache, database, OSD.

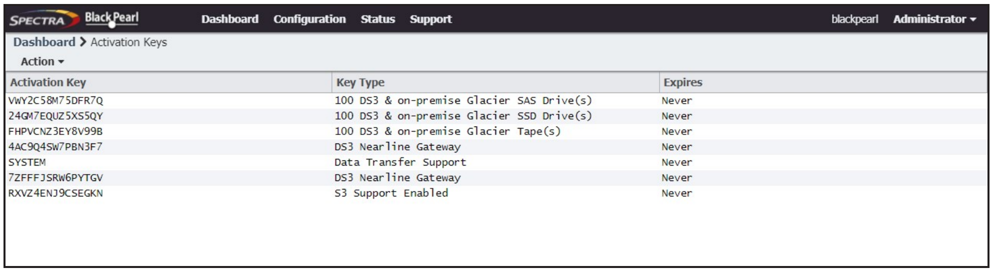
Key Type	Description
DS3 & on premise Glacier SATA Count	Enables the specified number of SATA drives present in the system for cache, database, OSD.
DS3 & on premise Glacier SSD Count	Enables the specified number of SSDs present in the system for cache, database, OSD.
DS3 & on-premise Glacier Tape Count	Enables the specified number of tape slots present in the attached Spectra Logic or supported tape library.

b. Product key(s)

Key Type	Description
DS3 Nearline 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.
S3 Support Enabled	Enables BlackPearl S3. **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 for a BlackPearl S3.
Third party tape library enabled	Enables object storage on a non-Spectra library.

c. All other keys - Any additional keys included on the Software Activation Key Certificate, such as the Product Key, Software Update key, or the NAS and Pools product key, can be entered in any order.

2. Select **Support > Activation Keys** to display the Activation Keys screen. Any previously entered keys are listed.



Activation Key	Key Type	Expires
VWY2C58M75DFR7Q	100 DS3 & on-premise Glacier SAS Drive(s)	Never
24GM7EQUZ5XS5QY	100 DS3 & on-premise Glacier SSD Drive(s)	Never
FHPVCNZ3EY8V99B	100 DS3 & on-premise Glacier Tape(s)	Never
4AC9Q4SW7PBN3F7	DS3 Nearline Gateway	Never
SYSTEM	Data Transfer Support	Never
7ZFFFJSRW6PYTGV	DS3 Nearline Gateway	Never
RXVZ4ENJ9CSEGKN	S3 Support Enabled	Never

Figure 200 The Activation Keys screen.

3. Select **Action > New**. The Enter Activation Key dialog box displays.

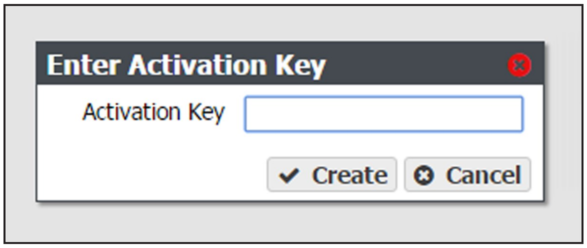


Figure 201 The Enter Activation Key dialog box.

4. Enter the key, exactly as provided, in the Activation Key field and click **Create** to save the key on the gateway. The Activation Keys screen displays with the newly entered key listed.

5. If necessary, repeat Step 3 through Step 4 to add additional keys.

CHAPTER 9 - 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 **343**

Tape Library Barcode Reporting 343

WORM Media 343

Available TeraPack Magazines 343

BlackPearl System Memory 343

Moving a BlackPearl Nearline to a New Tape Library 344

Tape Terminology 344

Tape Library Support **345**

Tape Library Options **346**

Activate a Tape Library Partition 346

Put a Tape Library Partition into Standby 347

Delete a Tape Partition 348

Tape Drive Options **349**

Tape Drive Reservation 349

Offline a Tape Drive 353

Online a Tape Drive 354

Remove a Tape Drive from a Tape Partition 356

Test Tape Drive **357**

Collect Drive Diagnostic Logs **359**

Compact a Tape Cartridge **360**

Format Managed BlackPearl Tapes **362**

Cancel Tape Format 364

Inspect Tapes **365**

Manage Tapes Not in Inventory **366**

Mark Tape as Exported 366

Delete Lost or Exported Tape 366

Data Migration 367

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 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.

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 Nearline gateway is configured to transfer data to tape, make sure the partitions configured for use by the BlackPearl gateway do not contain WORM (Write Once-Read Many) media. The BlackPearl 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 Nearline 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 Nearline gateway.

Moving a BlackPearl Nearline to a New Tape Library

If you need to move your BlackPearl Nearline gateway and the associate tape partition to a new tape library, you must contact Spoectra 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 system and made available for use.
- **Export** - Removing tape media from the BlackPearl system 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 eccentricity port are inspected by the BlackPearl system and moved to storage chambers. During export, tapes are moved from storage chambers to the eccentricity port before they are physically removed from the library.
- **Storage Chamber** - Chambers used to store tape media while in use by the BlackPearl Nearline gateway.

TAPE LIBRARY SUPPORT

The BlackPearl Nearline 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 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.

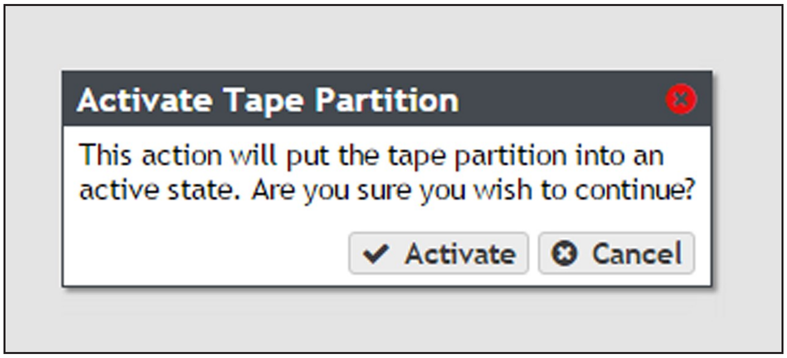
Notes:

- With BlackPearl OS 5.2 or earlier, if there was an inventory change in the tape library while in standby, the BlackPearl gateway may 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 S3 service is set to "Never Inspect".
- Spectra Logic recommends upgrading to BlackPearl OS 5.3 or later.

Use the instructions in this section to activate a tape library.

Note: If you are activating a new tape library, you must create a partition on the library so that the BlackPearl gateway can automatically detect the new tape library. See your *Library User Guide* for information on creating a partition in a tape library.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 221 on page 372).
2. Select the tape partition in the Tape Partitions pane, and select **Action > Activate Tape Partition**. The Activate Tape Partition confirmation window displays.


Activate Tape Partition

This action will put the tape partition into an active state. Are you sure you wish to continue?

Figure 202 The Activate Tape Partition confirmation window.

3. Click **Activate**. The tape partition is activated and is usable by the BlackPearl gateway.

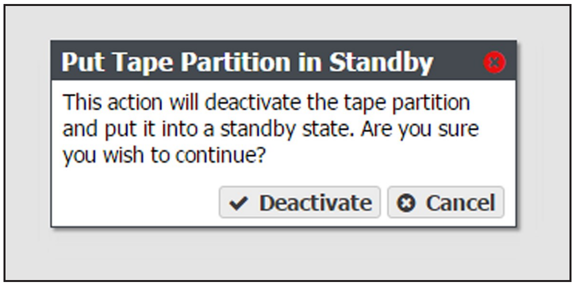
Put a Tape Library Partition into Standby

If you need to perform service on the tape library associated with your BlackPearl gateway, or with the BlackPearl gateway itself, you must first put the tape library into a standby state. Otherwise, the BlackPearl 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 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. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 40 on page 132).
2. Select the tape partition in the Tape Partitions pane, and select **Action > Put Tape Partition in Standby**. The Put Tape Partition in Standby confirmation window displays.



Put Tape Partition in Standby

This action will deactivate the tape partition and put it into a standby state. Are you sure you wish to continue?

Figure 203 The Put Tape Partition in Standby confirmation window.

3. Click **Deactivate**. The tape partition enters the standby state.

Note: If you have multiple partitions in the same tape library configured for use by the BlackPearl gateway, you must repeat steps Step 2 and Step 3 for each partition in the tape library that requires service.

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.

Once you complete service on the tape library and/or the BlackPearl gateway, return the tape library to service using the steps in Activate a Tape Library Partition on the previous page.

Delete a Tape Partition

If desired, you can delete a specified existing tape partition from the BlackPearl gateway. Any tapes in the partition that contain data are disassociated from the partition. Any tapes without data on them and all tape drives associated with the partition are deleted from the BlackPearl gateway configuration. This request is useful if the partition should never have been associated with the BlackPearl gateway or if the partition was deleted from the library.

Note: You must put the tape partition into standby before you can delete the tape partition. See Put a Tape Library Partition into Standby on the previous page for more information.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 221 on page 372).
2. Select the tape partition that you want to delete and select **Action > Delete**. A confirmation window displays.
3. Enter `DELETE` in the entry box.
4. Click **Delete**.

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 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.

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 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 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 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 gateway to a single tape drive (or two drives for dual copy), making the effective sustained write performance on the BlackPearl 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 gateway can utilize to restore subsets of data spread across a large number of tapes.

Tape Partition Drive Reservation

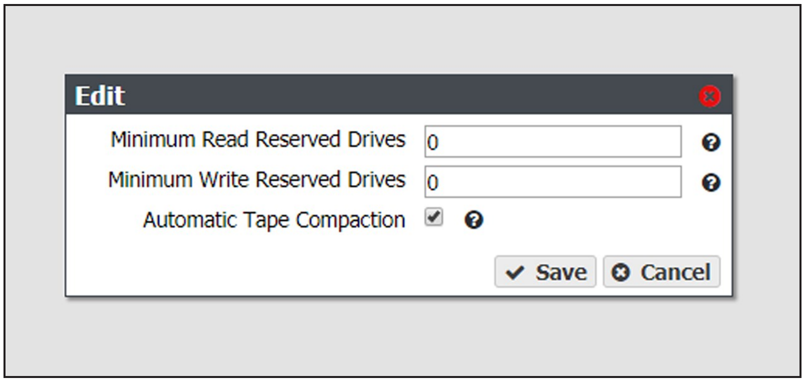
If desired, you can reserve a specified number of tape drives for read or write operations by editing the library partition.

By setting drive reservation on the tape partition instead of individual drives, it can prevent unavailable drives, or drives experiencing a tape drive failure, from impacting the desired number of drives reserved for either read or write commands.

Note: Reserving drives in a tape partition does not allow you to specify which specific drive(s) are reserved for read or write operations. To reserve a specific drive in the library, see Individual Tape Drive Reservation on page 352.

Use the instructions in this section to reserve drives in a partition.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 221 on page 372).
2. Select the tape partition that contains the drive(s) you want to reserve or make available in the Tape Partitions pane, and select **Action > Show Details**. The Tape Partition details screen displays.
3. Select **Action > Edit**. The Edit dialog box displays.



Edit

Minimum Read Reserved Drives 0

Minimum Write Reserved Drives 0

Automatic Tape Compaction ☑

Figure 204 The Edit dialog box.

4. If desired, edit the number of drives you want to reserve for read operations in the **Minimum Read Reserved Drives**. Alternatively, click the up and down arrows in the entry field (not shown).

Note: Drives reserved for read operations are occasionally used for background operations or tape inspection, but are never used for write operations.

5. If desired, edit the number of drives you want to reserve for write operations in the **Minimum Write Reserved Drives**. Alternatively, click the up and down arrows in the entry field.

Note: Drives reserved for a write operations are occasionally used for background operations or tape inspection, but are never used for read operations.

6. Select or clear **Automatic Tape Compaction**. When selected, the gateway automatically reclaims unused tape space caused by deleted objects that still reside on a tape.

Note: In addition to selecting Automatic Tape Compaction, IOM must be enabled for the automatic tape compaction process to run. See Configure the DS3 Service on page 292 for information on configuring IOM.

7. Click **Save**.

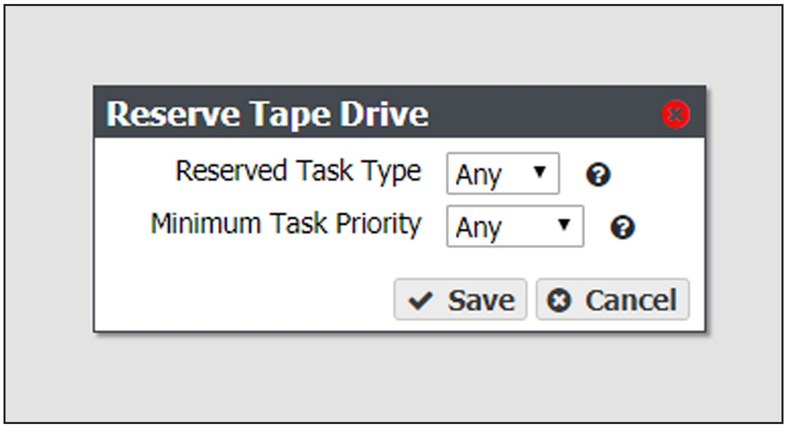
Individual Tape Drive Reservation

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.

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. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 221 on page 372).
2. Select the tape partition that contains the drive(s) you want to reserve in the Tape Partitions pane, and select **Action > Show Details**. The Tape Partition details screen displays.
3. Select the tape drive you want to reserve in the Tape Drives pane, and select **Action > Reserve Tape Drive**. The Reserve Tape Drive dialog box displays.



Reserve Tape Drive

Reserved Task Type: Any

Minimum Task Priority: Any

Figure 205 The Reserve Tape Drive dialog box.

4. Using the **Reserve Task Type** drop-down menu, select the type of operation for which you want to reserve the tape drive:

- 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.
- Select **Any** to make the drive available for both read and write operations.

Note: Tape drives always allow inspection and verify tasks.

IMPORTANT Spectra Logic does not recommend setting both a minimum task priority and reserved task type for the same drive.

IMPORTANT Spectra Logic does not recommend setting both a minimum task priority and reserved task type for the same drive.

5. Using the **Minimum Task Priority** drop-down menu, select the Minimum Task Priority; the drive is reserved for tasks at or above the selected priority.

Notes:

- 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, 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 Minimum Task Priority of Any or Low. If only one drive is configured for Any or Low, you cannot change the tape drive reservation.

6. Click **Save**.

Offline a Tape Drive

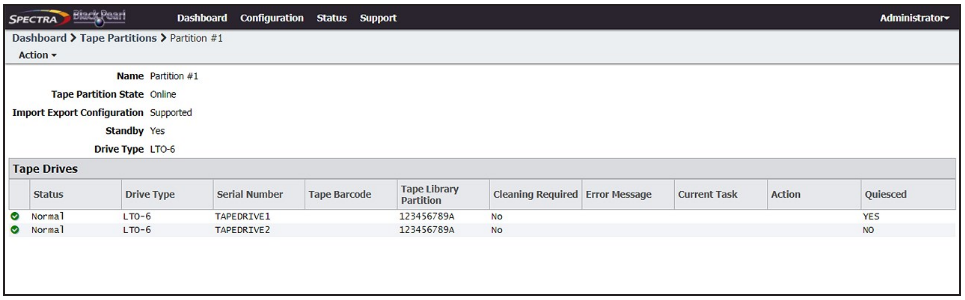
If you need to perform service on a tape drive in the tape library associated with your BlackPearl gateway, you must first offline the tape drive. Otherwise, the BlackPearl gateway may attempt to use the tape drive while it is in service.

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. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 221 on page 372).

2. Select the tape partition that contains the drive you want to offline in the Tape Partitions pane, and select **Action > Show Details**. The Tape Partition details screen displays.



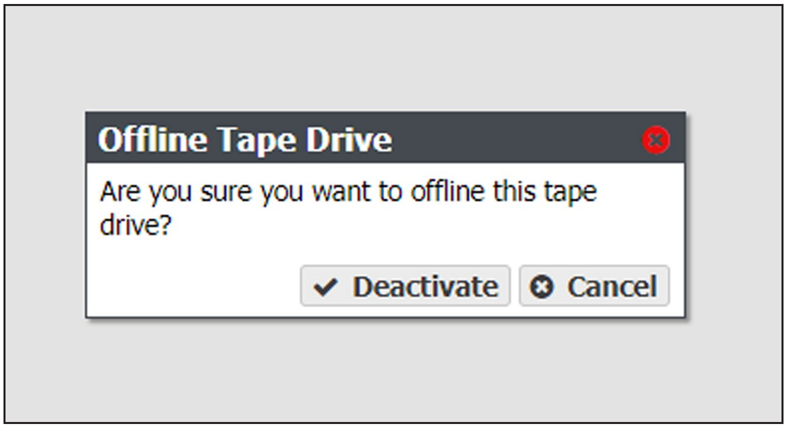
Name Partition #1
Tape Partition State Online
Import Export Configuration Supported
Standby Yes
Drive Type LTO-6

Tape Drives

	Status	Drive Type	Serial Number	Tape Barcode	Tape Library Partition	Cleaning Required	Error Message	Current Task	Action	Quiesced
✓	Normal	LTO-6	TAPEDRIVE1		123456789A	No				YES
✓	Normal	LTO-6	TAPEDRIVE2		123456789A	No				NO

Figure 206 The Tape Partition details screen.

3. Select the tape drive you want to offline in the Tape Drives pane and select **Action > Offline Tape Drive**. The Offline Tape Drive confirmation window displays.



Are you sure you want to offline this tape drive?

Figure 207 The Offline Tape Drive confirmation window.

4. Click **Deactivate**. The tape drive is now offline.

Once you complete service on the tape drive, make the tape drive available to the BlackPearl 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.

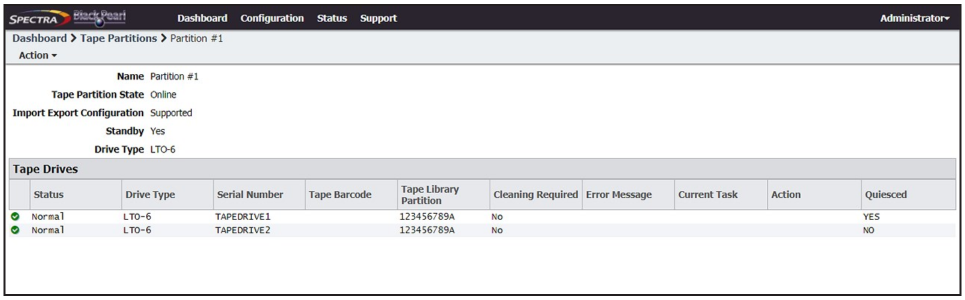
Tape drives appear offline for two different reasons. Either a user set a drive to be offline in the BlackPearl user interface, or the BlackPearl gateway is unable to communicate with the drive in the tape library.

- Drives that are offline with a Quiesced value of "Yes" were either manually set to offline by a user, or the BlackPearl gateway detected an error condition that was caused by a drive failure, and marked the drive as offline and quiesced it to prevent further use by the BlackPearl gateway.
- Offline drives with a Quiesced value of "No" indicate that the BlackPearl gateway cannot communicate with the drive. Examine your tape library to determine the cause of the problem, or contact Spectra Logic Technical Support (see Figure 221 on page 372).

Use the instructions in this section to online a 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.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 221 on page 372).
2. Select the tape partition that contains the drive you want to online in the Tape Partitions pane, and select **Action > Show Details**. The Tape Partition details screen displays.



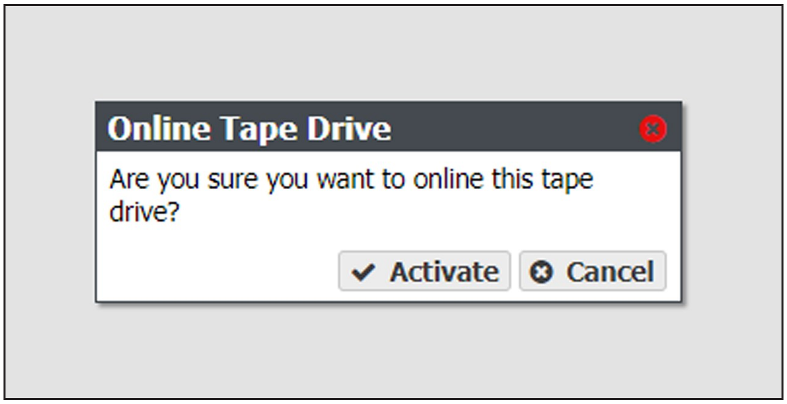
Name	Partition #1
Tape Partition State	Online
Import Export Configuration	Supported
Standby	Yes
Drive Type	LTO-6

Tape Drives

	Status	Drive Type	Serial Number	Tape Barcode	Tape Library Partition	Cleaning Required	Error Message	Current Task	Action	Quiesced
✓	Normal	LTO-6	TAPEDRIVE1		123456789A	No				YES
✓	Normal	LTO-6	TAPEDRIVE2		123456789A	No				NO

Figure 208 The Tape Partition details screen.

3. Select the tape drive you want to online in the Tape Drives pane, and select **Action > Online Tape Drive**. The Online Tape Drive confirmation window displays.



Online Tape Drive

Are you sure you want to online this tape drive?

Figure 209 The Online Tape Drive confirmation window.

4. Click **Activate**. The tape partition is now online and is usable by the BlackPearl gateway.

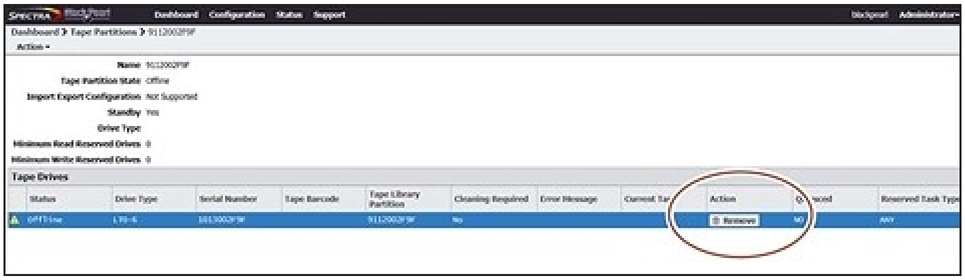
Remove a Tape Drive from a Tape Partition

If desired, you can delete a specified tape drive in a tape library partition.

Note: Removing a drive makes the drive inaccessible to the BlackPearl gateway. It has no effect on the tape library configuration.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 221 on page 372).

2. Select the tape partition that contains the drive you want to remove in the Tape Partitions pane, and select **Action > Show Details**. The Tape Partition details screen displays.



Name 9112002F9F
Tape Partition State Offline
Import Export Configuration Not Supported
Standby Yes
Drive Type
Minimum Read Reserved Drives 0
Minimum Write Reserved Drives 0

Tape Drives

	Status	Drive Type	Serial Number	Tape Barcode	Tape Library Partition	Cleaning Required	Error Message	Current Ta	Action	Q..ced	Reserved Task Type
⚠	Offline	LTO-6	1013002F9F		9112002F9F	No			Remove	NO	ANY

Figure 210 The Tape Partition details screen.

3. Click **Remove** on the row of the tape drive you want to remove from the tape partition. A confirmation window displays.

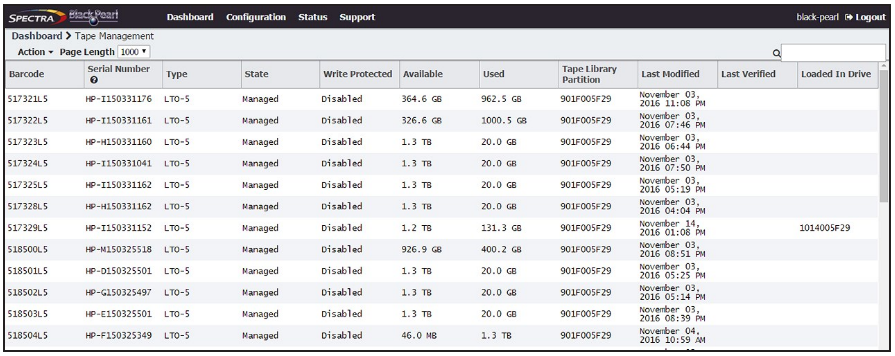
4. Click **Delete**.

TEST TAPE DRIVE

Starting with BlackPearl OS 5.6, 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.

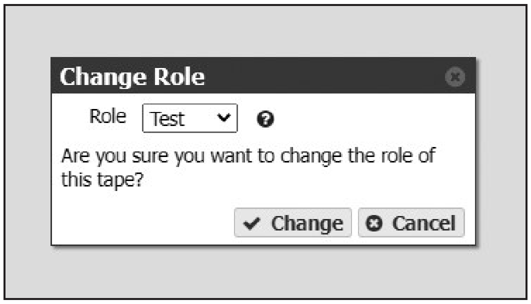
1. If necessary, import a tape cartridge to use for the drive test as described in Importing Tape Media in to a TeraPack-Based Library on page 379.
2. If necessary, configure a tape cartridge to use for the drive test.
   - **a.** In the BlackPearl user interface, select **Status > Tape Management**.



Barcode	Serial Number	Type	State	Write Protected	Available	Used	Tape Library Partition	Last Modified	Last Verified	Loaded In Drive
517321L5	HP-I150331176	LTO-5	Managed	Disabled	364.6 GB	962.5 GB	901F005F29	November 03, 2016 11:08 PM		
517322L5	HP-I150331161	LTO-5	Managed	Disabled	326.6 GB	1000.5 GB	901F005F29	November 03, 2016 07:46 PM		
517323L5	HP-H150331160	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 06:44 PM		
517324L5	HP-I150331041	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 07:50 PM		
517325L5	HP-I150331162	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 05:19 PM		
517328L5	HP-H150331162	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 04:04 PM		
517329L5	HP-I150331152	LTO-5	Managed	Disabled	1.2 TB	131.3 GB	901F005F29	November 14, 2016 01:08 PM		1014005F29
518500L5	HP-M150325518	LTO-5	Managed	Disabled	926.9 GB	400.2 GB	901F005F29	November 03, 2016 08:51 PM		
518501L5	HP-D150325501	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 05:25 PM		
518502L5	HP-G150325497	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 05:14 PM		
518503L5	HP-E150325501	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 08:39 PM		
518504L5	HP-F150325349	LTO-5	Managed	Disabled	46.0 MB	1.3 TB	901F005F29	November 04, 2016 10:59 AM		

Figure 211 The Tape Management screen.

   - **b.** Select the desired tape and select **Action > Change Role**.

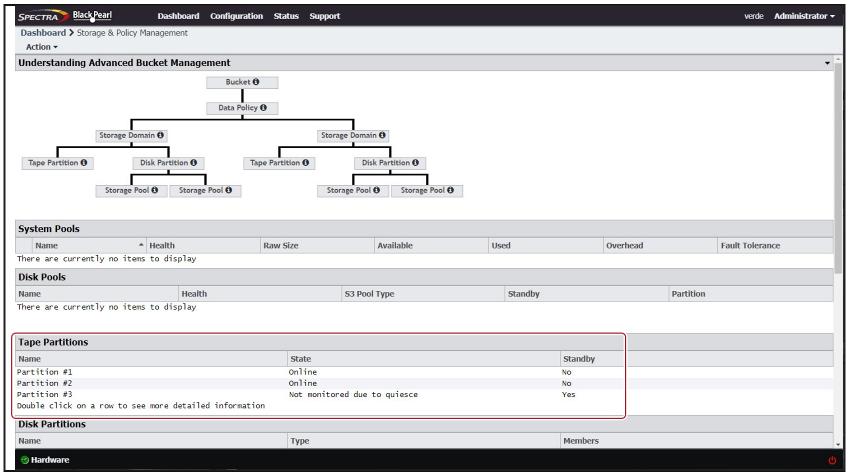


Role: Test

Are you sure you want to change the role of this tape?

Figure 212 The Change Role window.

   - **c.** Using the **Role** drop-down menu, select **Test**.
   - **d.** Click **Change**.
3. Select **Configuration > Advanced Bucket Management > Storage & Policy Management**.
4. Under the **Tape Partitions** banner, double-click the partition containing the drive you want to test.



System Pools

Name	Health	Raw Size	Available	Used	Overhead	Fault Tolerance

There are currently no items to display

Disk Pools

Name	Health	S3 Pool Type	Standby	Partition

There are currently no items to display

Tape Partitions

Name	State	Standby
Partition #1	Online	No
Partition #2	Online	No
Partition #3	Not monitored due to quiesce	Yes

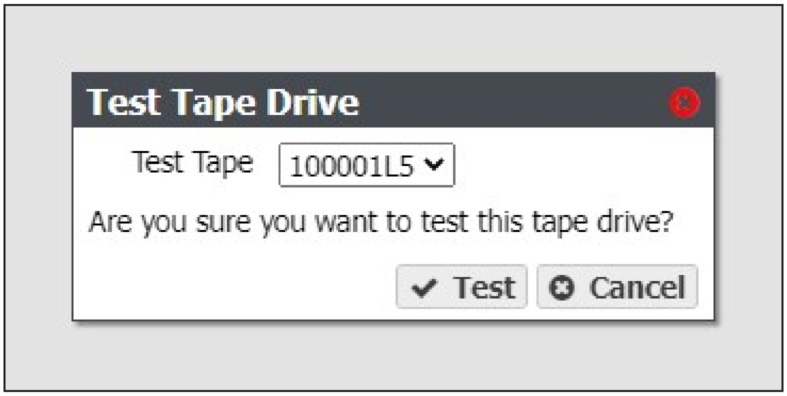
Double click on a row to see more detailed information

Disk Partitions

Name	Type	Members

Figure 213 The Storage & Policy Management screen.

5. Select the drive you want to test, and select **Action > Reserve Tape Drive**.
6. Select the drive to test and select **Action > Test Tape Drive**.
7. Using the **Test Tape** drop-down menu, select a tape cartridge configured as a test tape.



Test Tape: 100001L5

Are you sure you want to test this tape drive?

Figure 214 The Test Tape Drive window.

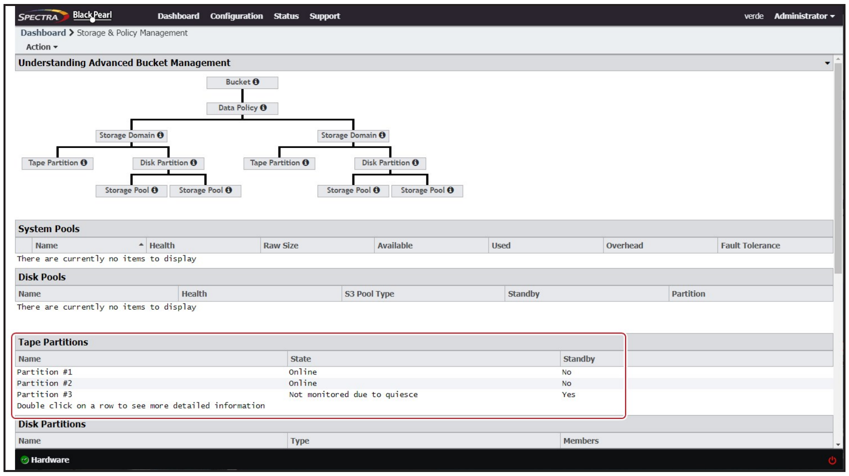
8. Click **Test**.

- If the drive test passes, return the drive to service.
    a. Select the tape drive and select **Action > Reserve Tape Drive**.
    b. Using the **Reserved Task Type** drop-down menu, select the role for the drive, and click **Save**.
- If the drive test failed, collect drive diagnostic logs as described in Collect Drive Diagnostic Logs on page 506 and contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 9).

Collect 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.

1. Select **Configuration > Advanced Bucket Management > Storage & Policy Management**.
2. Under the **Tape Partitions** banner, double-click the partition containing the drive for which you want to save logs.



System Pools

Name	Health	Raw Size	Available	Used	Overhead	Fault Tolerance

There are currently no items to display

Disk Pools

Name	Health	S3 Pool Type	Standby	Partition

There are currently no items to display

Tape Partitions

Name	State	Standby
Partition #1	Online	No
Partition #2	Online	No
Partition #3	Not monitored due to quiesce	Yes

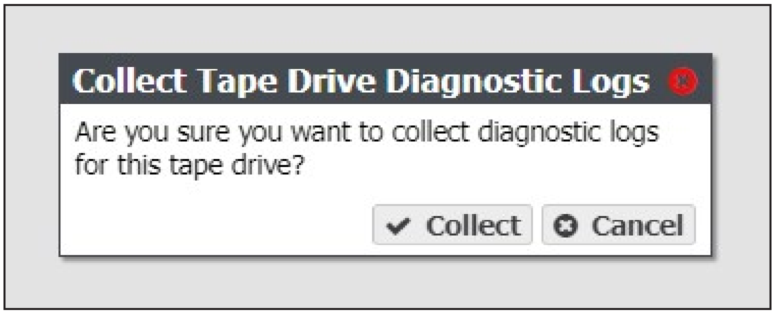
Double click on a row to see more detailed information

Disk Partitions

Name	Type	Members

Figure 215 The Storage & Policy Management screen.

3. Select the drive, and select **Action > Collect Tape Drive Diagnostic Logs**.


Collect Tape Drive Diagnostic Logs

Are you sure you want to collect diagnostic logs for this tape drive?

Figure 216 The Collect Tape Drive Diagnostic Logs window

4. Click **Collect**. The process takes approximately 30 seconds.

   After the drive log collection completes, download the log as described in Download a Log Set on page 462.

Compact a Tape Cartridge

The BlackPearl Nearline 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.

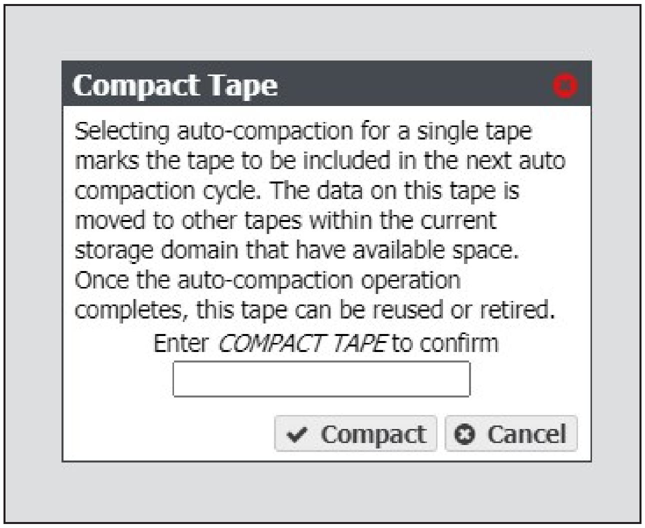
This is helpful if you want to retire or repurpose specific pieces of media while still maintaining a copy of the data on the tape in your BlackPearl ecosystem.

> **Note:** Tape compaction does not create a direct 1:1 copy of a tape cartridge. The BlackPearl system 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 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. Select **Status > Tape Management** from the menu bar. The Tape Management screen displays (see Figure 217 on page 363).
2. Select the tape cartridge you want to add to the compaction cycle, and select **Action > Compact Tape**. 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

3. In the entry field, enter `COMPACT TAPE`, and click **Compact**. 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 system for use as new data storage, use the instructions in this section to format tapes. During formatting, the BlackPearl Nearline 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.

CAUTION Any data currently on the tape media is lost during the format operation.

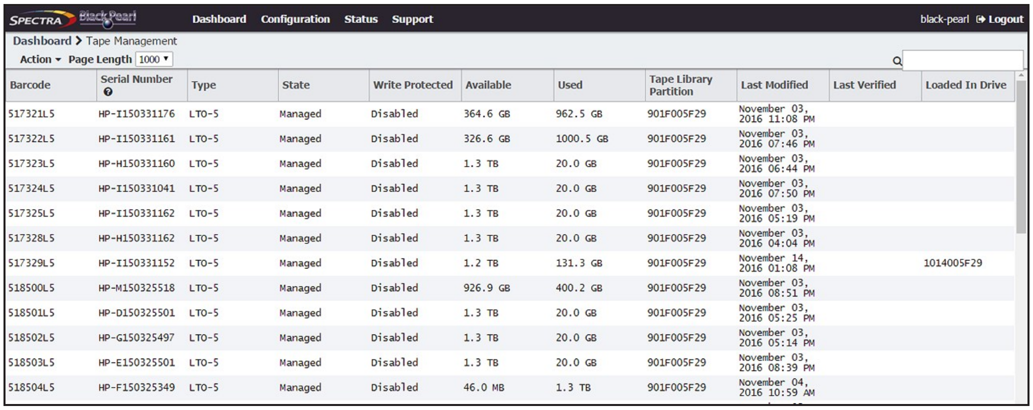
For information on increasing library capacity see your *Tape Library User Guides.*

The **Force** parameter must be used to format a tape if any of the below conditions are met:

- To Format a tape that contains data written by a BlackPearl gateway.
- To format a tape before it is inspected.
- To format a tape that currently has reads or writes scheduled.
- To format a tape that has already been formatted by a BlackPearl gateway,

Note: Tapes are not eligible for formatting if they have a state of EXPORTED, LOST, EXPORT_ PENDING, or OFFLINE.

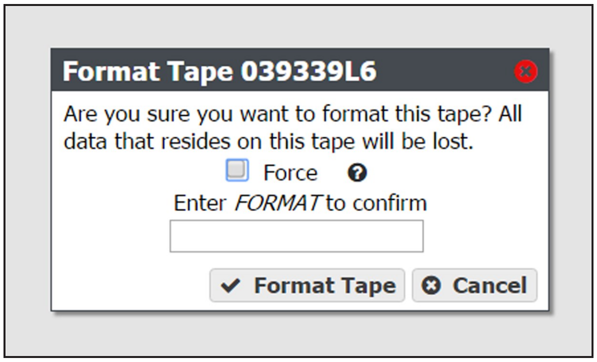
1. From the menu bar, select **Status > Tape Management**. The Tape Management screen displays. Any unformatted tapes display a state of Unknown on the Tape Management screen.



Barcode	Serial Number	Type	State	Write Protected	Available	Used	Tape Library Partition	Last Modified	Last Verified	Loaded In Drive
517321L5	HP-I150331176	LTO-5	Managed	Disabled	364.6 GB	962.5 GB	901F005F29	November 03, 2016 11:08 PM		
517322L5	HP-I150331161	LTO-5	Managed	Disabled	326.6 GB	1000.5 GB	901F005F29	November 03, 2016 07:46 PM		
517323L5	HP-H150331160	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 06:44 PM		
517324L5	HP-I150331041	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 07:50 PM		
517325L5	HP-I150331162	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 05:19 PM		
517328L5	HP-H150331162	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 04:04 PM		
517329L5	HP-I150331152	LTO-5	Managed	Disabled	1.2 TB	131.3 GB	901F005F29	November 14, 2016 01:08 PM		1014005F29
518500L5	HP-M150325518	LTO-5	Managed	Disabled	926.9 GB	400.2 GB	901F005F29	November 03, 2016 08:51 PM		
518501L5	HP-D150325501	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 05:25 PM		
518502L5	HP-G150325497	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 05:14 PM		
518503L5	HP-E150325501	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 08:39 PM		
518504L5	HP-F150325349	LTO-5	Managed	Disabled	46.0 MB	1.3 TB	901F005F29	November 04, 2016 10:59 AM		

Figure 217 The Tape Management screen.

2. Select the tape cartridge you want to format and select **Action > Format Tape**, or to format all tapes with a state of Unknown, select **Action > Format All Unmanaged Tapes**. A confirmation dialog box displays.



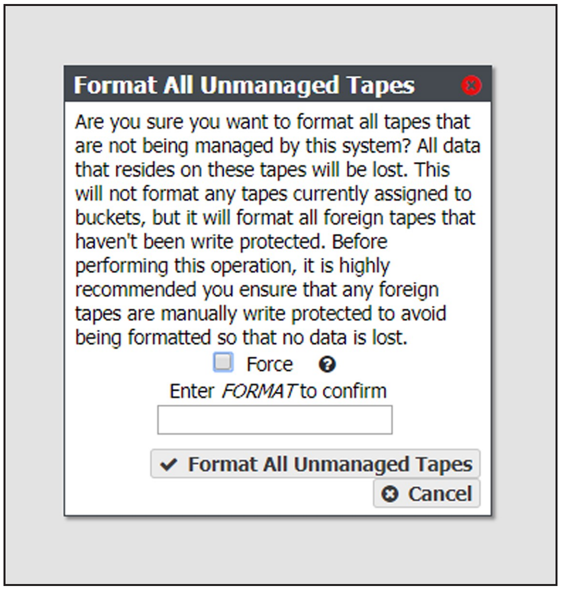
Format Tape 039339L6

Are you sure you want to format this tape? All data that resides on this tape will be lost.

☐ Force

Enter *FORMAT* to confirm

Figure 218 The Format Tape confirmation dialog box.



Format All Unmanaged Tapes

Are you sure you want to format all tapes that are not being managed by this system? All data that resides on these tapes will be lost. This will not format any tapes currently assigned to buckets, but it will format all foreign tapes that haven't been write protected. Before performing this operation, it is highly recommended you ensure that any foreign tapes are manually write protected to avoid being formatted so that no data is lost.

☐ Force

Enter *FORMAT* to confirm

Figure 219 The Format All Unmanaged Tapes confirmation dialog box.

3. If desired, select the **Force** option.

Note: If the selected tape contains data from a BlackPearl 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.

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.

4. Enter `FORMAT` in the entry field and click **Format Tape**, or **Format All Unmanaged Tapes**. 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 gateway. This process can take up to five minutes per tape.

Cancel Tape Format

If desired, you can cancel a queued tape format, or cancel all queued tape formats. Use the instructions in this section to cancel one or more tape formats.

1. From the menu bar, select **Status > Tape Management**. The Tape Management screen displays (see Figure 217 on page 363).
2. Cancel tape format(s):

- To cancel a single tape format:
  - **a.** Select the tape row, then select **Action > Cancel Tape Format**. A confirmation window displays.
  - **b.** Click **Cancel Tape Format**.
- To cancel all queued tape formats:
  - **a.** select **Action > Cancel All Tape Formats**. A confirmation window displays.
  - **b.** Click **Cancel All Tape Formats**.

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 gateway, the tape may transition to the Pending Inspection state (see State on page 423) 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.

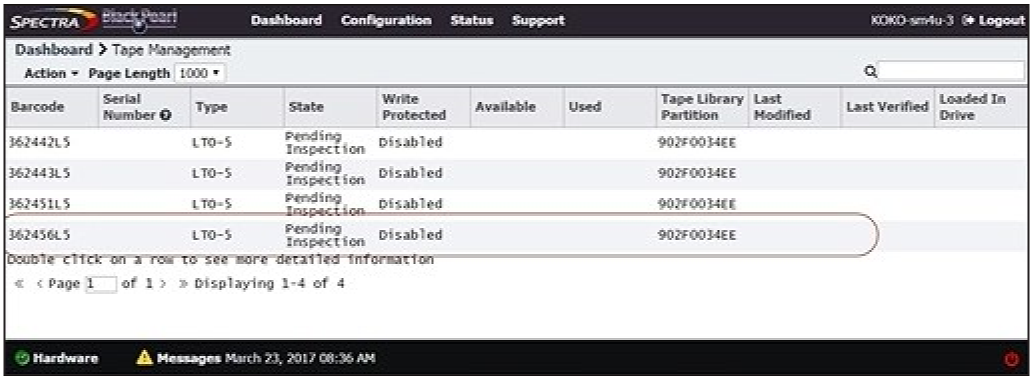
Inspecting a tape manually is useful if the tape cartridge transitions to a state of "Unknown" or "Bad". Inspecting the tape cartridge while in these states may recover the cartridge for use.

IMPORTANT Tape inspection may take several hours or days depending on the number of tapes to be inspected.

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. From the menu bar, select **Status > Tape Management**. The Tape Management screen displays. Any tapes requiring inspection display a state of Pending Inspection on the Tape Management screen.



Barcode	Serial Number	Type	State	Write Protected	Available	Used	Tape Library Partition	Last Modified	Last Verified	Loaded In Drive
362442L5		LTO-5	Pending Inspection	Disabled			902F0034EE			
362443L5		LTO-5	Pending Inspection	Disabled			902F0034EE			
362451L5		LTO-5	Pending Inspection	Disabled			902F0034EE			
362456L5		LTO-5	Pending Inspection	Disabled			902F0034EE			

Double click on a row to see more detailed information

« ‹ Page 1 of 1 › » Displaying 1-4 of 4

Figure 220 The Tape Management screen.

2. Select the tape you want to inspect, and then select **Action > Inspect**. The Inspect Tape dialog box displays.

3. Click **Inspect** to begin inspecting the tape.

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 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”.

1. Select **Status > Tape Management** from the menu bar. The Tape Management screen displays (see Figure 217 on page 363).
2. If desired, edit the tape export information as described in Edit Tape Export Information Without Exporting Tape Media on page 395.
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 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 370 for more information.

Use the instruction in this section to delete a lost or exported tape from the BlackPearl database.

1. Select **Status > Tape Management** from the menu bar. The Tape Management screen displays (see Figure 217 on page 363).
2. Select the tape with a status of “Not in Inventory” and select **Action > Delete Lost or Exported Tape**. A confirmation window displays.
3. 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 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 BlackPearlgateway. If you need to create any of the above, see Configuring Advanced Bucket Management on page 128.

IMPORTANT This process assumes that all required data policies, data persistence rules, storage domains, and storage partitions are already configured on the BlackPearl gateway. If you need to create any of the above, see Configuring Advanced Bucket Management on page 128.

1. If necessary, create a tape partition that contains the new media technology (see Create a Tape Partition on page 138). This is the **target tape** partition.
2. 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.
3. Add the **target tape** partition to the storage domain as a storage domain member (see Add a Storage Domain Member to a Storage Domain on page 156).
4. 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”.
5. 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.
6. Manually create a database backup (see Manually Generate a Database Backup on page 446). The data migration is now complete.

7. If desired, using the list of tapes you recorded in Step 2, export tapes from the **source tape** partition (see Export Tapes on page 393).

CHAPTER 9 - 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 370
Imported Tape Object Name Restrictions for Amazon S3 Replication 371
Import Tape Media 371
Import BlackPearl Foreign Tape(s) 373
Import LTFS Foreign Tape(s) 375
Import Requested Tape Media 378
Importing Tape Media in to a TeraPack-Based Library 379
Log Into the User Interface 380
Import the Magazines 381
Import Requested Tape Media 392
Export Tapes 393
Export a Single Tape 394
Cancel Tape Export 395
Edit Tape Export Information Without Exporting Tape Media 395
Export Tapes from a T50e or T120 Library with Multiple Partitions 396
Exporting Tape Media from a TeraPack-Based Library 397
Log Into the User Interface 398
Export the Magazines 399

IMPORT TAPES

Use the instructions in this section to import tape media physically into a tape library partition and logically into the BlackPearl 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 Tapes above.

Importing tape media into a BlackPearl gateway is a multi-step processes and depends on the characteristics of the tape library. First, media is physically imported into the eccentricity pool in the tape library, if necessary. Second, the media in the eccentricity pool is moved by the BlackPearl gateway to the storage pool. Lastly the media is moved tape drives for inspection.

During the inspection, the BlackPearl 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 gateway before it is available for use.
- Media previously exported by the BlackPearl 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.

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 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 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 BlackPearlgateway. Tapes not set to write-protected are not imported.

IMPORTANT LTFS foreign tapes must have the physical write-protect tab set in the "write-protected" position before you import them into the BlackPearl 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 S3 solution, 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 (//)

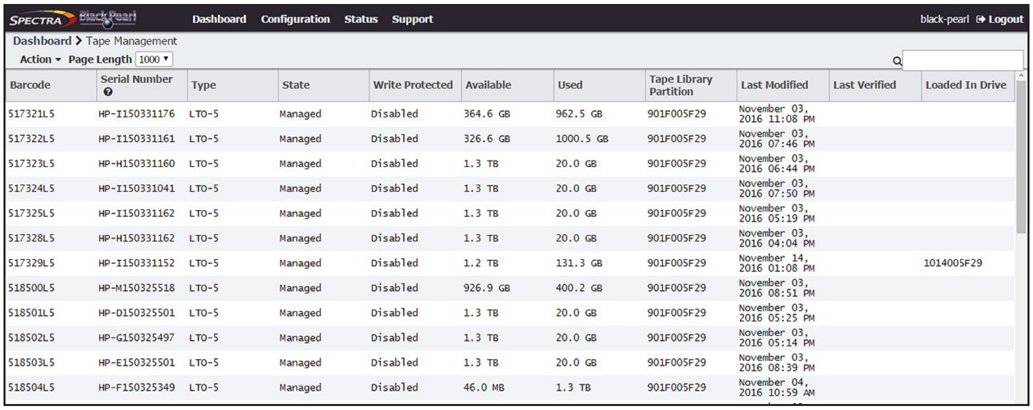
Import Tape Media

Use the instructions in this section to import tape media into the BlackPearl gateway database.

1. Use the instructions in Importing Tape Media in to a TeraPack-Based Library on page 379 to import the requested tape media into the Entry/Exit pool of a Spectra Logic tape library associated with the BlackPearl gateway.

Note: For instructions on importing tape media in to the I/O slots of an IBM tape library, see Tape Library User Guides on page 27.

2. Select **Status > Tape Management** from the menu bar. The Tape Management screen displays.



Barcode	Serial Number	Type	State	Write Protected	Available	Used	Tape Library Partition	Last Modified	Last Verified	Loaded In Drive
517321L5	HP-I150331176	LTO-5	Managed	Disabled	364.6 GB	962.5 GB	901F005F29	November 03, 2016 11:08 PM		
517322L5	HP-I150331161	LTO-5	Managed	Disabled	326.6 GB	1000.5 GB	901F005F29	November 03, 2016 07:46 PM		
517323L5	HP-H150331160	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 06:44 PM		
517324L5	HP-I150331041	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 07:50 PM		
517325L5	HP-I150331162	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 05:19 PM		
517328L5	HP-H150331162	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 04:04 PM		
517329L5	HP-I150331152	LTO-5	Managed	Disabled	1.2 TB	131.3 GB	901F005F29	November 14, 2016 01:08 PM		1014005F29
518500L5	HP-M150325518	LTO-5	Managed	Disabled	926.9 GB	400.2 GB	901F005F29	November 03, 2016 08:51 PM		
518501L5	HP-D150325501	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 05:25 PM		
518502L5	HP-G150325497	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 05:14 PM		
518503L5	HP-E150325501	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 08:39 PM		
518504L5	HP-F150325349	LTO-5	Managed	Disabled	46.0 MB	1.3 TB	901F005F29	November 04, 2016 10:59 AM		

Figure 221 The Tape Management screen.

3. Select **Action > Online All Tapes**. A confirmation window displays.

4. Click **Online All Tapes**. 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 Nearline 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. LTO-9 media is supported starting in BlackPearl OS 5.4.1.

- If you imported media previously exported from the BlackPearl 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.

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.

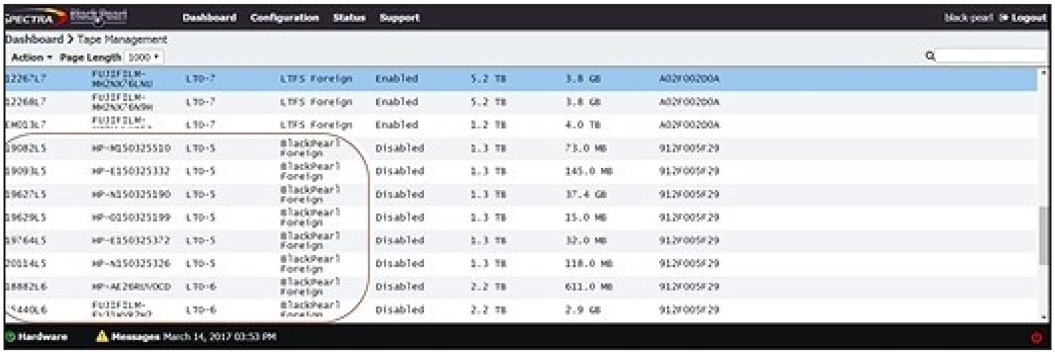
- To reclaim previously-used media for new data storage, see Format Managed BlackPearl Tapes on page 362.
- If you imported foreign media, use the appropriate instructions below to complete the import process:
  - Import BlackPearl Foreign Tape(s) below
  - Import LTFS Foreign Tape(s) on page 375

Import BlackPearl Foreign Tape(s)

After importing tapes into a tape library and allowing the BlackPearl 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. Select **Status > Tape Management** from the menu bar. The Tape Management screen displays.



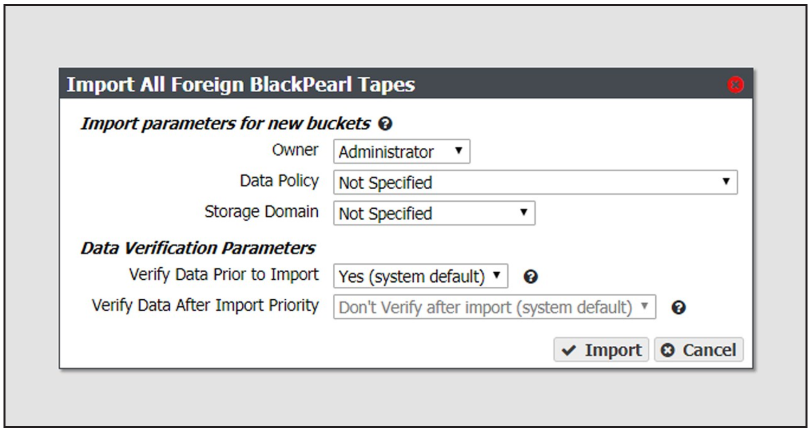
12267L7	FUJIFILM-MH2NX76LNU	LTO-7	LTFS Foreign	Enabled	5.2 TB	3.8 GB	A02F00200A
12268L7	FUJIFILM-MH2NX76N9H	LTO-7	LTFS Foreign	Enabled	5.2 TB	3.8 GB	A02F00200A
EM013L7	FUJIFILM-	LTO-7	LTFS Foreign	Enabled	1.2 TB	4.0 TB	A02F00200A
19082L5	HP-M150325510	LTO-5	BlackPearl Foreign	Disabled	1.3 TB	73.0 MB	912F005F29
19093L5	HP-E150325332	LTO-5	BlackPearl Foreign	Disabled	1.3 TB	145.0 MB	912F005F29
19627L5	HP-A150325190	LTO-5	BlackPearl Foreign	Disabled	1.3 TB	37.4 GB	912F005F29
19629L5	HP-G150325199	LTO-5	BlackPearl Foreign	Disabled	1.3 TB	15.0 MB	912F005F29
19764L5	HP-E150325372	LTO-5	BlackPearl Foreign	Disabled	1.3 TB	32.0 MB	912F005F29
20014L5	HP-A150325326	LTO-5	BlackPearl Foreign	Disabled	1.3 TB	118.0 MB	912F005F29
18882L6	HP-AE26RUVOCD	LTO-6	BlackPearl Foreign	Disabled	2.2 TB	611.0 MB	912F005F29
5440L6	FUJIFILM-[illegible]	LTO-6	BlackPearl Foreign	Disabled	2.2 TB	2.9 GB	912F005F29

March 14, 2017 03:53 PM

Figure 222 The Tape Management screen with BlackPearl foreign tapes listed.

2. Select **Action > Import All Foreign BlackPearl Tapes**, or select the individual BlackPearl foreign tape that you want to import, and select **Action > Import Foreign Tape**. The Import Foreign BlackPearl Tape or Import All Foreign BlackPearl Tapes dialog box displays.

Note: The import settings are the same for importing a single tape or all BlackPearl foreign tapes.



Import All Foreign BlackPearl 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 (system default)

Verify Data After Import Priority: Don't Verify after import (system default)

Figure 223 The Import Foreign BlackPearl Tape dialog box.

3. Using the **Owner** drop-down list, 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.
4. Using the **Data Policy** drop-down list, select a data policy from the list of previously created data policies to use for all buckets on the foreign tape(s). 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.
5. Using the **Storage Domain** drop-down list, select a storage domain from the list of previously created storage domains to use for all buckets on the foreign tape(s). 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 NearlineGateway stores data that is sent to it.
6. Using the **Verify Data Prior to Import** drop-down list, select whether or not to perform a data verification the data on the foreign tape(s) before importing. Data verification ensures the data on the tape is still viable.
7. Using the **Verify Data After Import Priority** drop-down list, select whether or not to perform data verification on the media after importing. 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.

Note: This option is grayed-out if you selected **Verify Data Prior to Import** in Step 6.

8. Click **Import**. The foreign tape(s) are imported into the BlackPearl gateway.

Import LTFS Foreign Tape(s)

After importing tapes into a tape library and allowing the BlackPearl gateway to online and inspect the tape, use the instructions in this section to complete the import of LTFS foreign tapes.

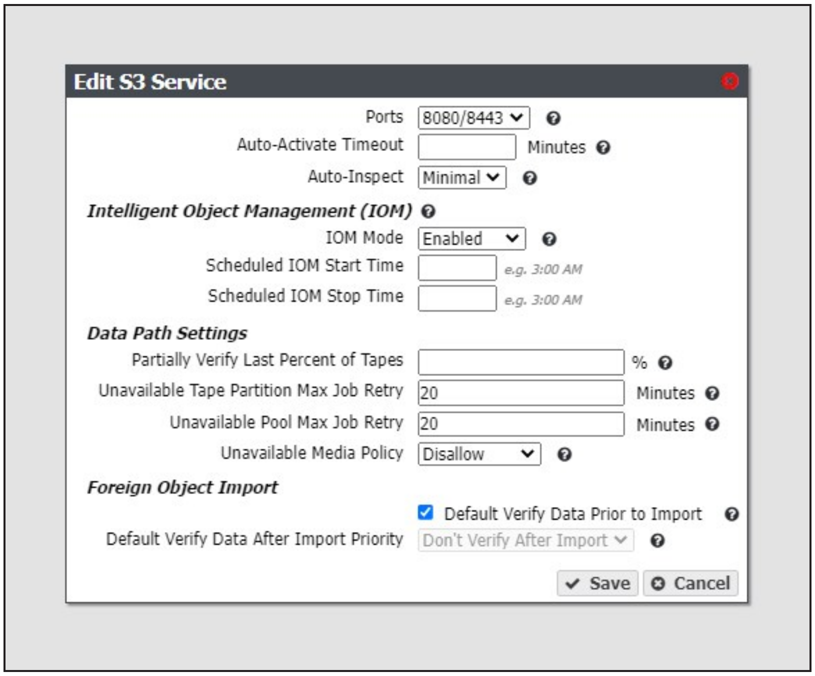
> **Note:** Importing LTFS tape media must be done while the Intelligent Object Management (IOM) service is disabled. After you finish importing foreign LTFS tape media, you can re-enable IOM, which may trigger the creation of missing copies of files as required by the associated data policy. After the LTFS import completes, you can manually start an IOM migration.

1. **Disable** the IOM service.

   a. From the menu bar, select **Configuration > Services** to display the Services screen.

   b. Double-click the S3 service, or select the S3 service and select **Action > Show Details**. The S3 Service details screen displays.

   c. On the S3 service details screen, select **Action > Edit**. The Edit S3 Service dialog box displays.



Edit S3 Service

Ports: 8080/8443

Auto-Activate Timeout: Minutes

Auto-Inspect: Minimal

Intelligent Object Management (IOM)

IOM Mode: Enabled

Scheduled IOM Start Time: e.g. 3:00 AM

Scheduled IOM Stop Time: e.g. 3:00 AM

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

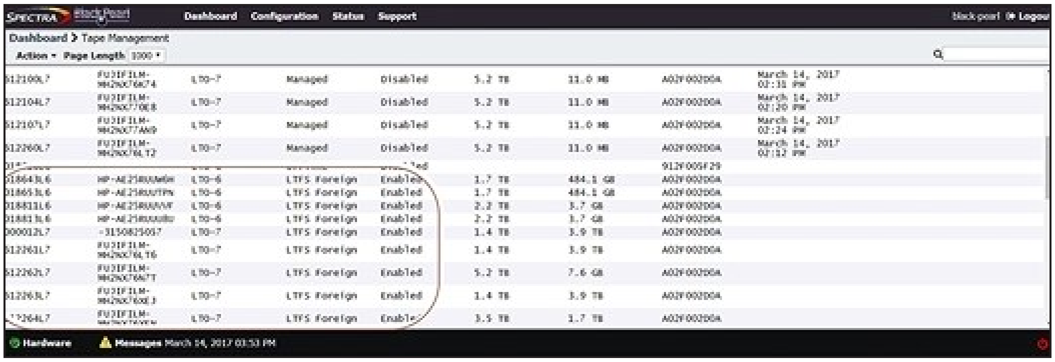
Default Verify Data After Import Priority: Don't Verify After Import

Figure 224 The Edit S3 Service dialog box.

   d. Use the **IOM Mode** drop-down menu to select the behavior for Intelligent Object Management to **Disabled**.

   e. Leave all other settings unchanged, and click **Save**.

2. Select **Status > Tape Management** from the menu bar. The Tape Management screen displays.



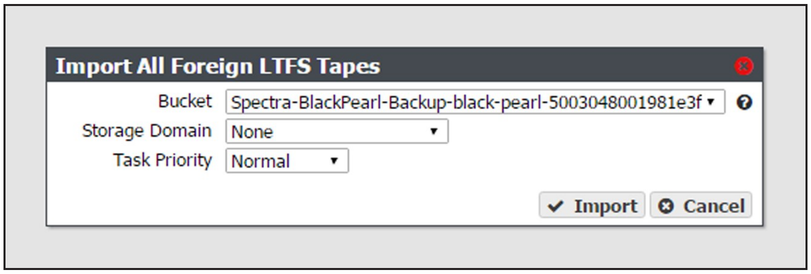
512100L7	FUJIFILM-9M2NX76A74	LTO-7	Managed	Disabled	5.2 TB	11.0 MB	A02F002D0A	March 14, 2017 02:31 PM
512104L7	FUJIFILM-9M2NX770E8	LTO-7	Managed	Disabled	5.2 TB	11.0 MB	A02F002D0A	March 14, 2017 02:20 PM
512107L7	FUJIFILM-9M2NX77AN9	LTO-7	Managed	Disabled	5.2 TB	11.0 MB	A02F002D0A	March 14, 2017 02:24 PM
512260L7	FUJIFILM-9M2NX76L72	LTO-7	Managed	Disabled	5.2 TB	11.0 MB	A02F002D0A	March 14, 2017 02:12 PM
91[illegible]				[illegible]led			912F005F29	
018643L6	HP-AE2[illegible]	LTO-6	LTFS Foreign	Enabled	1.7 TB	484.1 GB	A02F002D0A	
018653L6	HP-AE2[illegible]	LTO-6	LTFS Foreign	Enabled	1.7 TB	484.1 GB	A02F002D0A	
018811L6	HP-AE2[illegible]	LTO-6	LTFS Foreign	Enabled	2.2 TB	3.7 GB	A02F002D0A	
018813L6	HP-AE2[illegible]	LTO-6	LTFS Foreign	Enabled	2.2 TB	3.7 GB	A02F002D0A	
000012L7	-3150825037	LTO-7	LTFS Foreign	Enabled	1.4 TB	3.9 TB	A02F002D0A	
512261L7	FUJIFILM-9M2NX76LT6	LTO-7	LTFS Foreign	Enabled	1.4 TB	3.9 TB	A02F002D0A	
512262L7	FUJIFILM-9M2NX76A7T	LTO-7	LTFS Foreign	Enabled	5.2 TB	7.6 GB	A02F002D0A	
512263L7	FUJIFILM-9M2NX76XEJ	LTO-7	LTFS Foreign	Enabled	1.4 TB	3.9 TB	A02F002D0A	
[illegible]264L7	FUJIFILM-[illegible]	LTO-7	LTFS Foreign	Enable[illegible]	3.5 TB	1.7 TB	A02F002D0A	

Figure 225 The Tape Management screen with LTFS foreign tapes listed.

3. Import the tape(s) using one of the methods below:

- If you want to import all foreign LTFS tapes into one bucket on the BlackPearl gateway, select **Action > Import All Foreign LTFS Tapes**. The Import All Foreign LTFS Tape dialog box displays.
- If you want to import different foreign LTFS tapes into multiple buckets, select the individual foreign tape that you want to import, and select **Action > Import Foreign Tape**. The Import Foreign LTFS Tape dialog box displays.

Note: The import settings are the same for importing a single tape or all LTFS foreign tapes.



Bucket: Spectra-BlackPearl-Backup-black-pearl-5003048001981e3f

Storage Domain: None

Task Priority: Normal

Figure 226 The Import All Foreign LTFS Tapes dialog box.

4. Using the **Bucket** drop-down list, 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.

5. If the bucket's data policy includes dual copy on tape, use the **Storage Domain** drop-down list to specify into which storage domain to import the foreign LTFS tape. Otherwise, continue with Step 6.

6. Using the **Task Priority** drop-down list, 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.

7. Click **Import**. The foreign LTFS tape(s) are imported into the BlackPearl gateway.
8. After the import completes, enable the IOM service.
   a. From the menu bar, select **Configuration > Services** to display the Services screen.
   b. Double-click the S3 service, or select the S3 service and select **Action > Show Details**. The S3 Service details screen displays.
   c. On the S3 service details screen, select **Action > Edit**. The Edit S3 Service dialog box displays (see Figure 224 on page 375).
   d. Use the **IOM Mode** drop-down menu to select the behavior for Intelligent Object Management to **Enabled**.
   e. 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.

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 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 370

1. Refer to system messages or emails sent to the administrator account for a list of tape barcode(s) to import. See How Does a User Know What Tape Cartridge(s) to Import in Response to a GET Request for Objects on Exported Media? on page 500 for more information.
2. Use the instructions in Importing Tape Media in to a TeraPack-Based Library on the next page to import the requested tape media into the Entry/Exit pool of a Spectra Logic tape library associated with the BlackPearl gateway.

Note: For instructions on importing tape media in to the I/O slots of an IBM tape library, see Tape Library User Guides on page 27.

3. In the BlackPearl user interface, select **Status > Tape Management** from the menu bar. The Tape Management screen displays (see Figure 221 on page 372).
4. Select **Action > Online All Tapes**. A confirmation window displays.
5. Click **Online All Tapes**. 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.

CAUTION If the bucket associated with the imported tape media no longer exists, the tape cartridges are marked for formatting and reclaimed by the BlackPearlNearlinegateway.

CAUTION If the bucket associated with the imported tape media no longer exists, the tape cartridges are marked for formatting and reclaimed by the BlackPearl Nearline gateway.

IMPORTING TAPE MEDIA IN TO A TERAPACK-BASED LIBRARY

Use the instructions in this section to import tape media into a TeraPack-based library 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 Nearline gateway.
- These instructions describe a simplified workflow for importing tape media for use by a BlackPearl Nearline 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 Spectra Stack, T120, and T50e, see your *Library User Guide*.

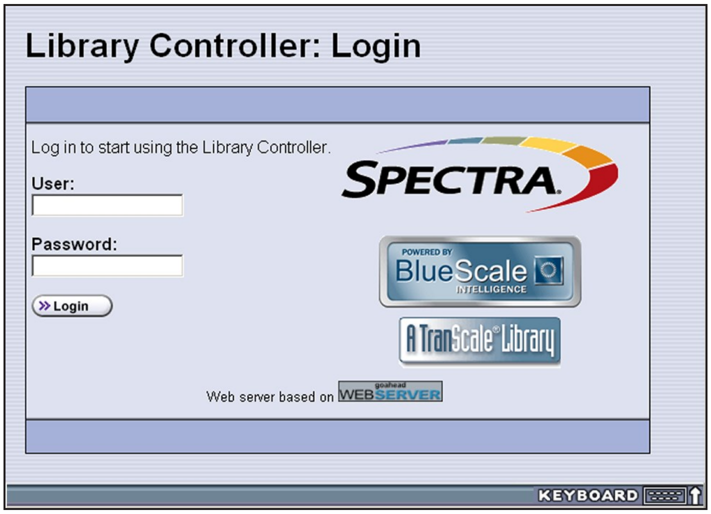
Log Into the User Interface

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:

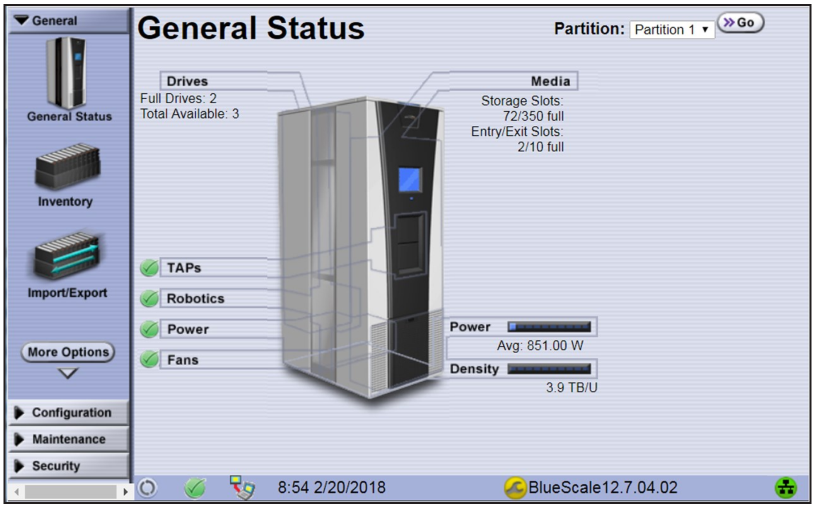
Password:

Login
SPECTRA
POWERED BY BlueScale INTELLIGENCE
A TranScale Library
Web server based on goahead WEBSERVER
KEYBOARD

Figure 227 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

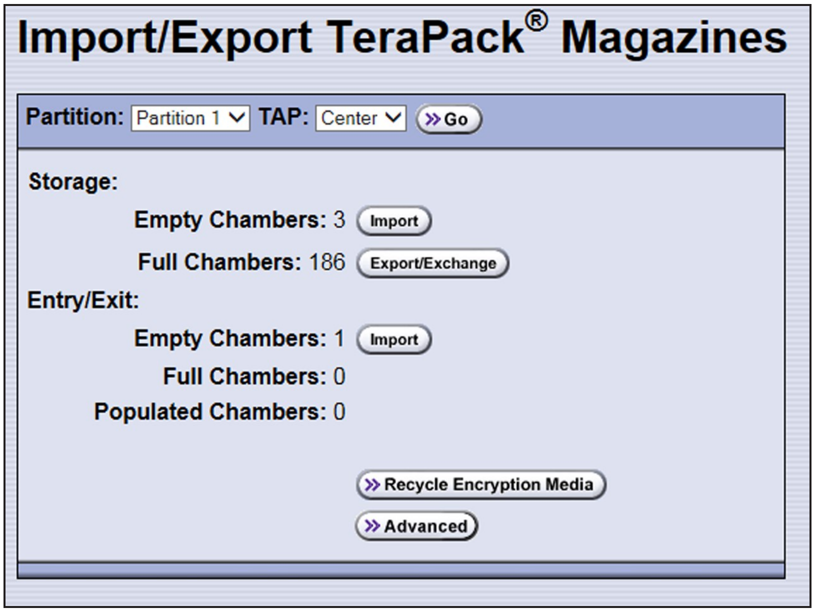
Figure 228 The BlueScale user interface General Status screen for a Spectra TeraPack-based tape library.

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

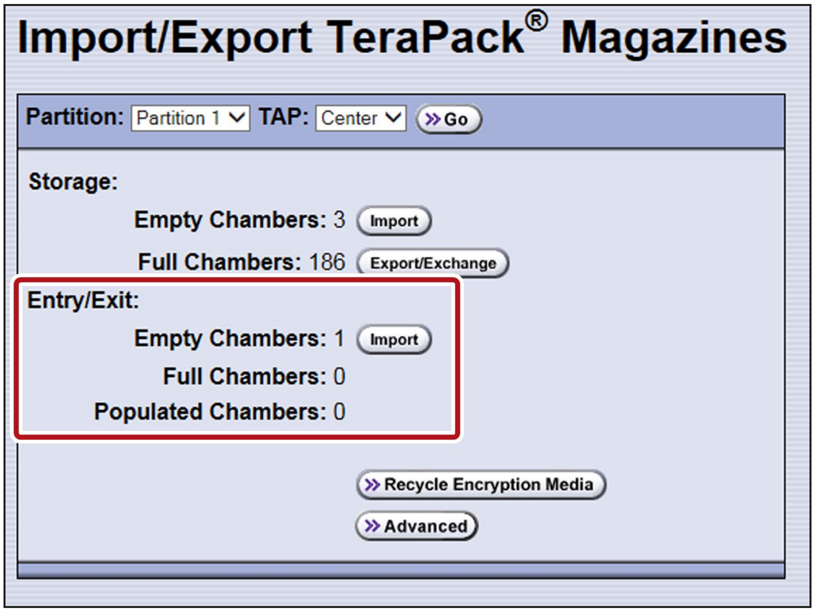
Figure 229 Select the partition and the TAP.

4. Under Entry/Exit, click the **Import** button.

IMPORTANT Only import tape cartridges into the Entry/Exit port. The BlackPearl system controls the movement of tape media inside the library.

IMPORTANT Only import tape cartridges into the Entry/Exit port. The BlackPearl system 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 230 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 on the next page
   - Center TAP in a T680, T380, or T200 Library on page 385
   - Bulk TAP on page 388

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 Figure 231 on page 384.

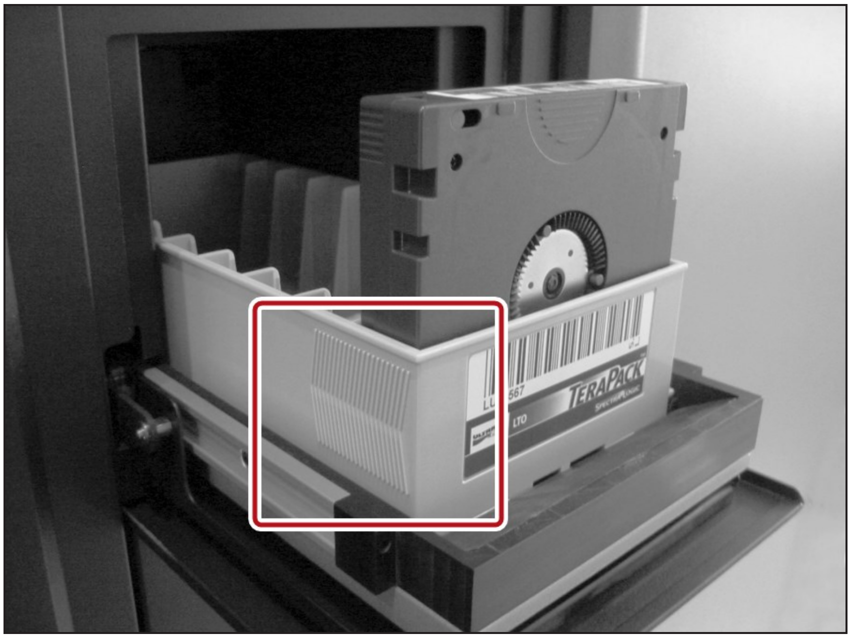


Figure 231 Insert a magazine into the TAP, making sure that it is correctly oriented.

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 eccentricity pool. **2.** If there are still empty chambers available in the eccentricity 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 eccentricity 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 Figure 231.

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.

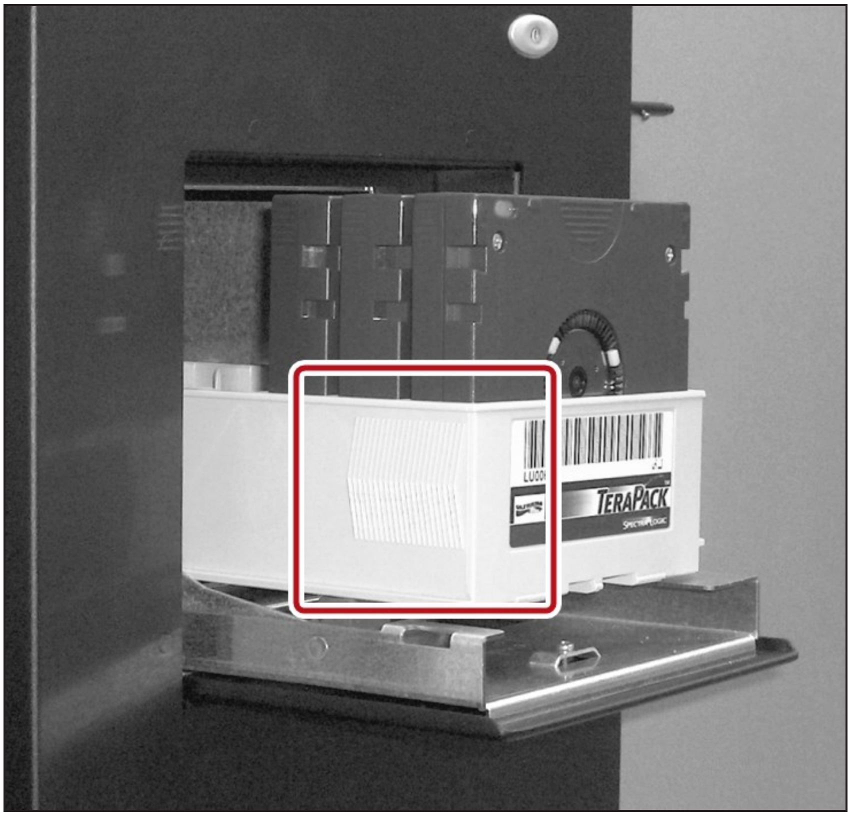


Figure 232 Insert a magazine into the TAP, making sure that it is correctly oriented.

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.

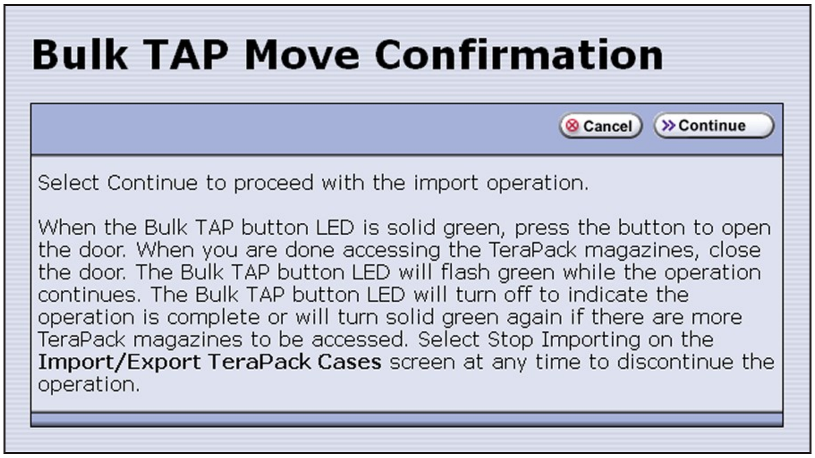
c. Return to the operator panel and select the appropriate option on the Feedback Required screen.

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 eccentricity pool. **2.** If there are still empty chambers available in the eccentricity 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 eccentricity 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 233 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.

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.

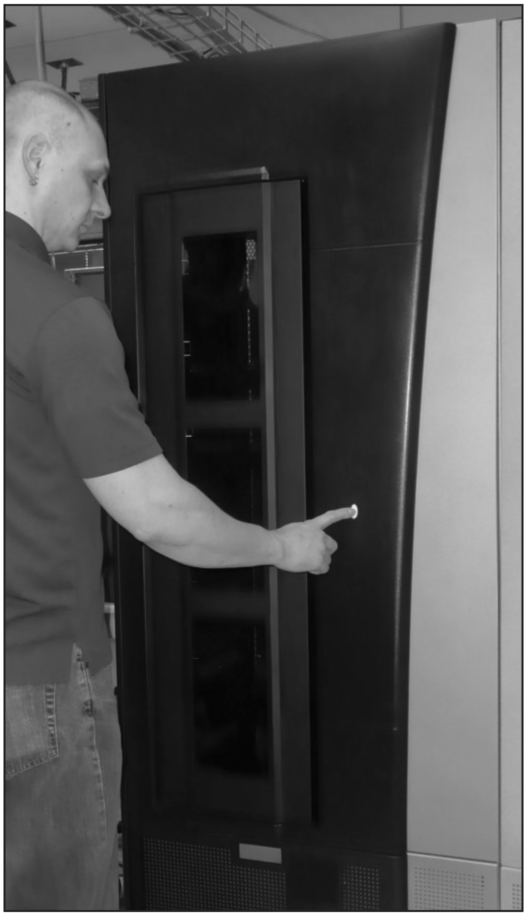


Figure 234 Press the door release button to open the door.

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 235 on page 390. Loading the magazines incorrectly or at an angle can result in damage to the carousel or the robotics.

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 235 on page 390. 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.

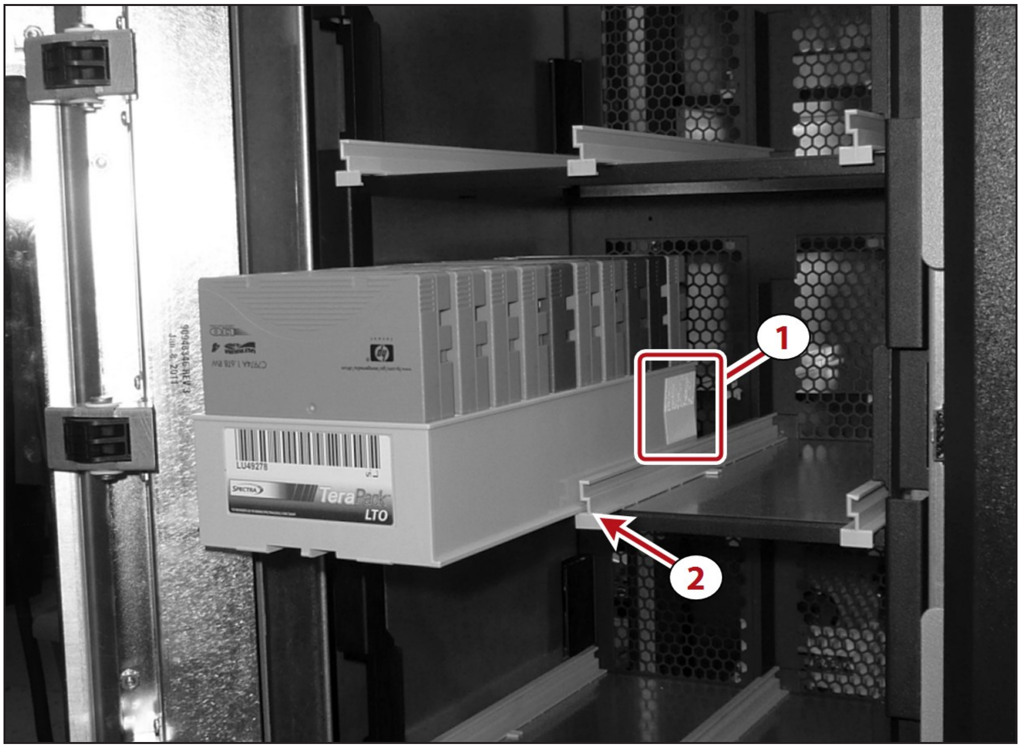
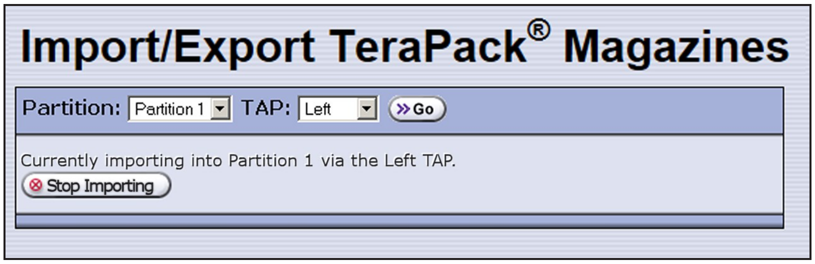


Figure 235 Insert the magazine into the bulk TAP carousel, making sure that it is correctly positioned.

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 eccentricity 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.



Import/Export TeraPack® Magazines

Partition: Partition 1 TAP: Left

Currently importing into Partition 1 via the Left TAP.

Figure 236 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 eccentricity pool** — The operation ends when the destination is full. If the eccentricity 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.

IMPORT REQUESTED TAPE MEDIA

Use the instructions in this section to import tape media into the BlackPearl 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 Requested Tape Media above

1. Refer to system messages or emails sent to the administrator account for a list of tape barcode(s) to import. See How Does a User Know What Tape Cartridge(s) to Import in Response to a GET Request for Objects on Exported Media? on page 500 for more information.
2. Use the instructions in Importing Tape Media in to a TeraPack-Based Library on page 379 to import the requested tape media into the Entry/Exit pool of a Spectra Logic tape library associated with the BlackPearl 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 Tape Library User Guides on page 27.

3. In the BlackPearl user interface, select **Status > Tape Management** from the menu bar. The Tape Management screen displays (see on page 392).
4. Select **Action > Online All Tapes**. A confirmation window displays.
5. Click **Online All Tapes**. 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.

CAUTION If the bucket associated with the imported tape media no longer exists, the tape cartridges are marked for formatting and reclaimed by the BlackPearlNearlinegateway.

CAUTION If the bucket associated with the imported tape media no longer exists, the tape cartridges are marked for formatting and reclaimed by the BlackPearl Nearline gateway.

EXPORT TAPES

Tape media and the data they contain can be removed from the BlackPearl 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 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 BlackPearlgateway.

If you suspect that a tape was exported from the library without being exported from the BlackPearl gateway using the BlackPearl user interface, see What Happens if a User Exports a Tape From the Library Before Exporting the Tape in the BlackPearl User Interface? on page 502

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 gateway.

If you suspect that a tape was exported from the library without being exported from the BlackPearl gateway using the BlackPearl user interface, see What Happens if a User Exports a Tape From the Library Before Exporting the Tape in the BlackPearl User Interface? on page 502

Notes:

- The BlackPearl 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 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 Exporting Tapes on page 99 for important information on how to configure your BlackPearl 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 *Tape Library User Guides* for more information.

- For instructions on storing tape media exported from an IBM TS4500 tape library, see the *TS4500 User Guide*.

Notes:

- Spectra T50e and T120 libraries must be configured in Standard Entry/Exit Port mode in order for the BlackPearl gateway to automatically export tapes. If your library has only one partition, it is already in Standard Entry/Exit Port mode.

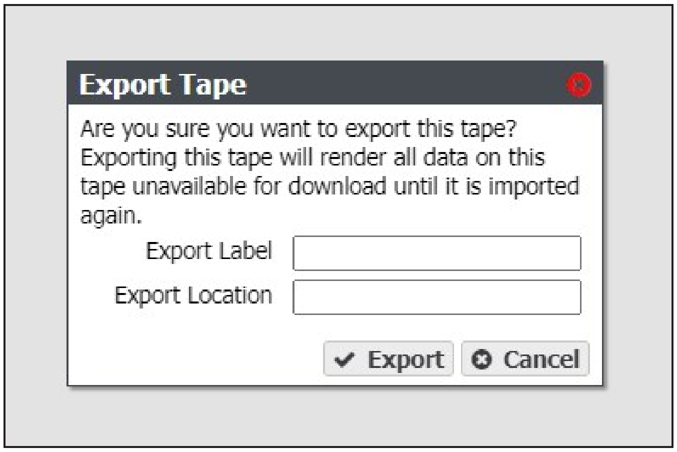
  If there is more than one partition, including a cleaning partition, in order for the BlackPearl gateway to automatically export tapes you must delete partitions until only one remains, and then edit the remaining partition to use Standard mode. See your Spectra Logic *Tape Library User Guides* for more 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 396.

Export a Single Tape

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 gateway.

1. Select **Status > Tape Management** to display the Tape Management screen (see Figure 217 on page 363).
2. Select the tape you want to export, and then select **Action > Export Tape**. The Export Tape dialog box displays.



Export Tape

Are you sure you want to export this tape? Exporting this tape will render all data on this tape unavailable for download until it is imported again.

Export Label

Export Location

Figure 237 The Export Tape dialog box.

3. 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 gateway. You are not required to enter this information.

4. Click **Export**. The tape is marked as exported in the BlackPearl 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.
5. Repeat Step 2 through Step 4 as necessary to export additional tapes.
6. Once you have exported the desired tape(s) in the BlackPearl user interface, use the instructions in Exporting Tape Media from a TeraPack-Based Library on page 397 to export the requested tape media into the Entry/Exit pool of a Spectra Logic tape library associated with the BlackPearl gateway.

Note: For instructions on importing tape media in to the I/O slots of an IBM tape library, see Tape Library User Guides on page 27.

Cancel Tape Export

If you requested a tape export but it has not yet started, you can cancel the export in progress. Any tapes not already moved to the Entry/Exit pool of a Spectra Logic tape library, or the I/O slots of an IBM tape library are left in the storage partition and are usable by the BlackPearl gateway. Any tapes that were moved to the Entry/Exit pool or I/O slots must be exported from the library and re-imported as described in Import Tapes on page 370.

1. Select **Status > Tape Management** to display the Tape Management screen (see Figure 217 on page 363).
2. Cancel the export:

- To cancel all tape exports, select **Action > Cancel All Tape Exports**.
- To cancel a single tape export, select the tape for which you want to cancel the export, and then select **Action > Cancel Tape Export**.

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. Select **Status > Tape Management** to display the Tape Management screen (see Figure 217 on page 363).

2. Select the tape you want to export, and then select **Action > Edit**. The Edit Tape dialog box displays.

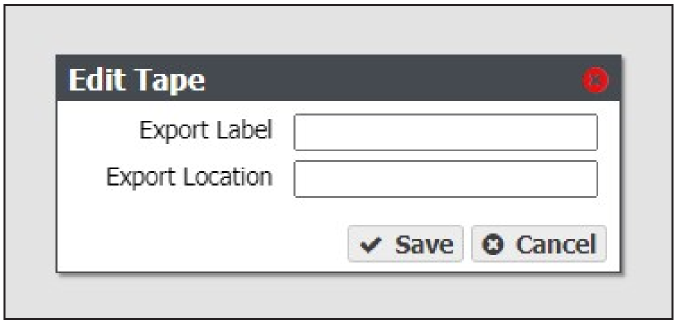


Figure 238 The Edit Tape dialog box.

3. Enter information in the **Export Label** and **Export Location** fields. This information is stored on the BlackPearl database and is visible when re-importing the tape into a BlackPearl 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 gateway, you cannot use the BlackPearl 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 Mark Tape as Exported on page 366.

EXPORTING TAPE MEDIA FROM A TERAPACK-BASED LIBRARY

Use the instructions in this section to export tape media into a TeraPack-based library 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 Nearline gateway.
- These instructions describe a simplified workflow for exporting tape media for use by a BlackPearl Nearline gateway. For advanced export options, see your *Library User Guide* for instructions.
- For instructions on exporting tapes from a Spectra Stack, T120, and T50e, see your *Library User Guide*.

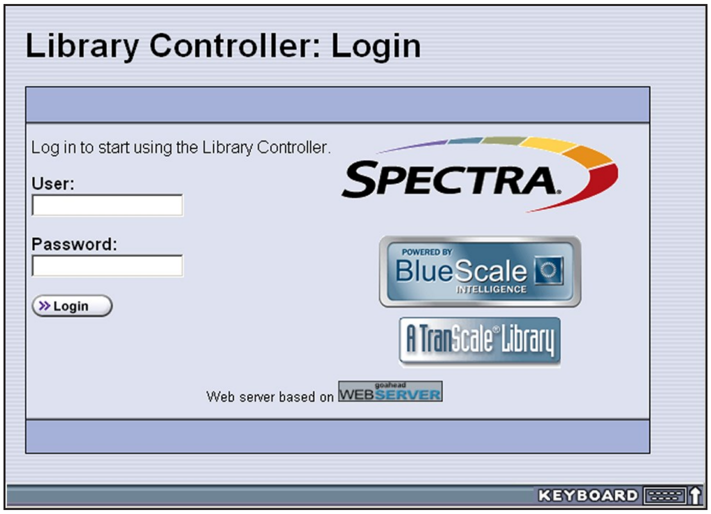
Log Into the User Interface

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 239 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.

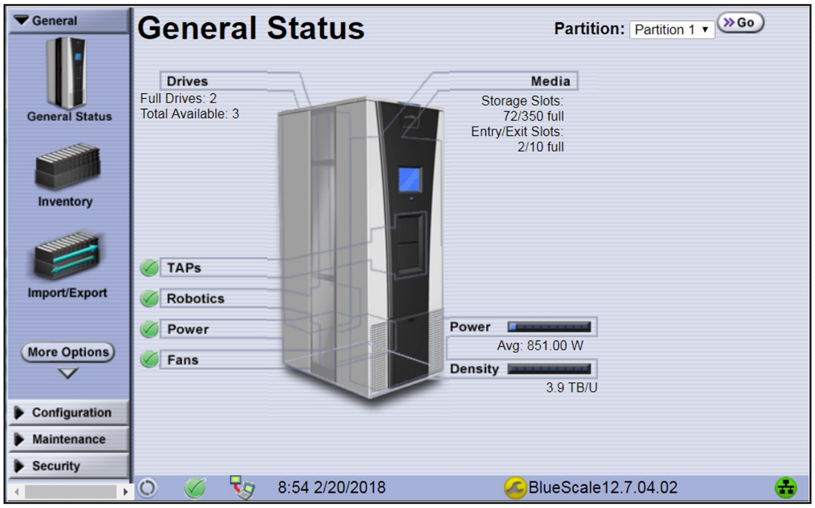


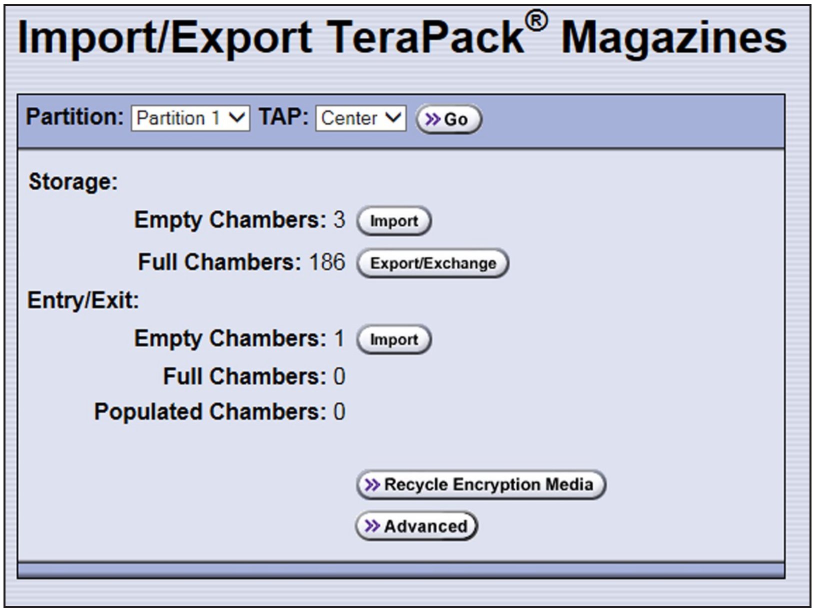
Figure 240 The BlueScale user interface General Status screen for a Spectra TeraPack-based tape library.

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

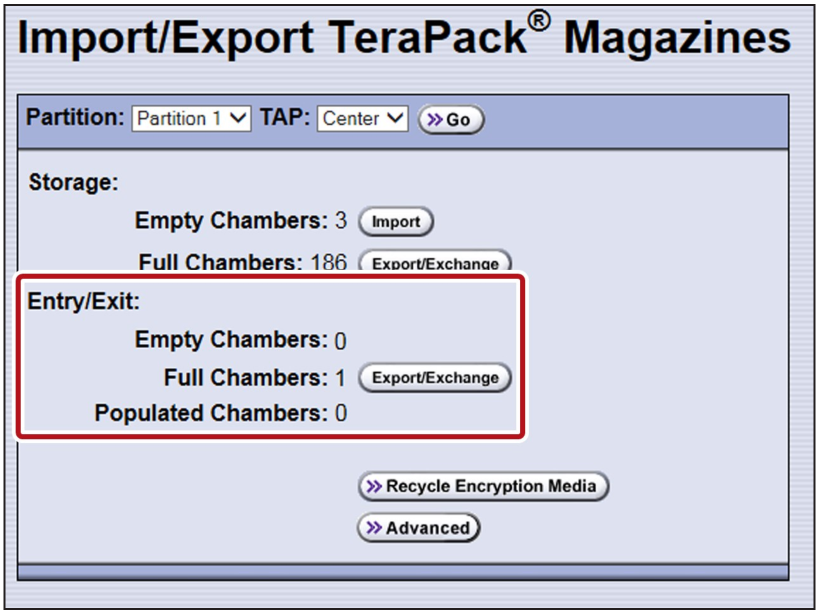
Populated Chambers: 0

Figure 241 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 system controls the movement of tape media inside the library.

IMPORTANT Only export tape cartridges from the Entry/Exit port. The BlackPearl system 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 242 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 d. 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.

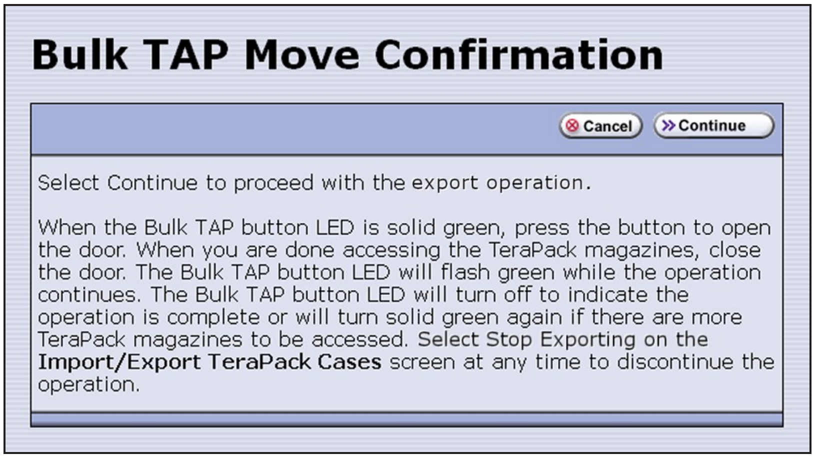
Select...	If...
Continue	You want to export another magazine. The process continues as follows: **1.** After the TAP door closed either manually or automatically, the TeraPorter retrieves the next magazine and delivers it to the center TAP. **Note:** On TFinity, T950, and T680 libraries, the TAP doors alternate as you continue to export magazines. **2.** The export process continues as long as there are magazines in the eccentricity 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 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.

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.



Bulk TAP Move Confirmation

Select Continue to proceed with the export operation.

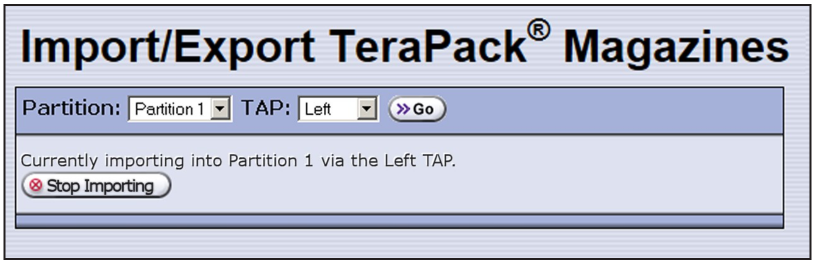
When the Bulk TAP button LED is solid green, press the button to open the door. When you are done accessing the TeraPack magazines, close the door. The Bulk TAP button LED will flash green while the operation continues. The Bulk TAP button LED will turn off to indicate the operation is complete or will 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 243 Read the instructions on the Bulk TAP Move Confirmation screen, then click **Continue**.

Click **Continue**. The TeraPorter retrieves magazines from the eccentricity 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.

b. 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 244 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.

c. 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.

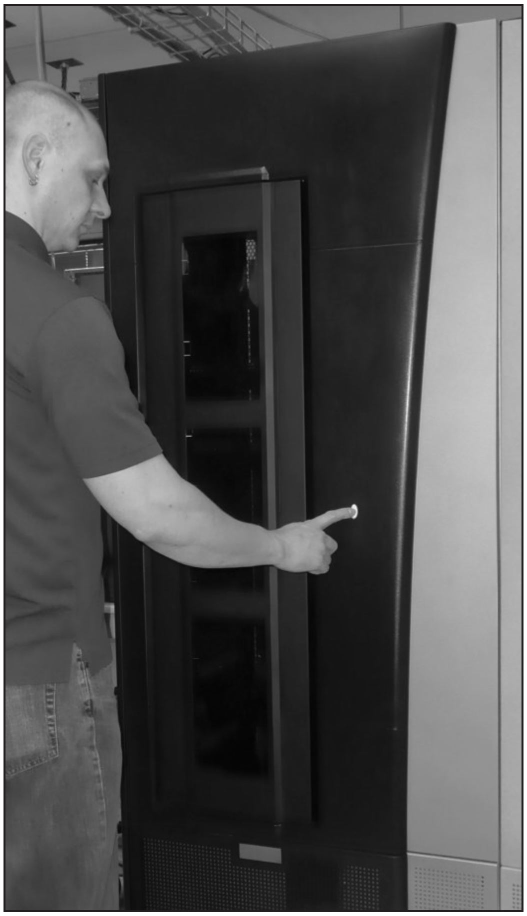


Figure 245 Press the door release button to open the door.

d. Remove the TeraPack magazines from the carousel(s) and set them aside.

e. 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.

f. If the bulk TAP could not accommodate all of the magazines in the eccentricity pool, the TeraPorter moves the next set of magazines from the eccentricity pool to the carousel. The process continues as long as there are magazines in the eccentricity 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 10 - Operating the BlackPearl Nearline Gateway

This chapter describes procedures for day-to-day monitoring and operation of the Spectra BlackPearl Nearline Gateway.

S3 Operations 409

Download an Object 409

Cancel DS3 Jobs 410

Edit an S3 Job 410

Clear All Canceled or Completed Jobs 411

Manually Starting the S3 Data Path Backend 412

Disallow New Jobs 412

Allow New Jobs 413

Monitor the BlackPearl Gateway 414

Front Bezel Visual Status Beacon 415

Configuring the Visual Status Beacon Color 416

System Status LEDs 416

Check System Messages 420

View the Status of Hardware Components 421

View the Status of Services 423

View the Status of NAS Pools 423

View the Status of NAS Volumes 426

View the Status of NAS Shares 426

View the Status of the System Pools 428

View Bucket Contents 430

View DS3 Jobs Information 431

View Tape Media Information 433

View Performance Metrics 438

View Reports 440

Database Backup & Restore 441

Create a Database Backup Schedule 442

Manually Generate a Database Backup 446
Restore from a Database Backup 446
Delete Backup 448
Edit Backup Data Policy 449
Show Backup Physical Placement 449
Exit the BlackPearl User Interface 450
Reboot or Shut Down a BlackPearl Gateway 451
Using the BlackPearl User Interface 451
Power-Cycle Reset 452

S3 OPERATIONS

Use the instructions in this section to manually download an object, cancel an S3 job, or to manually start the datapath backend.

Download an Object

Objects present on the BlackPearl 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.*

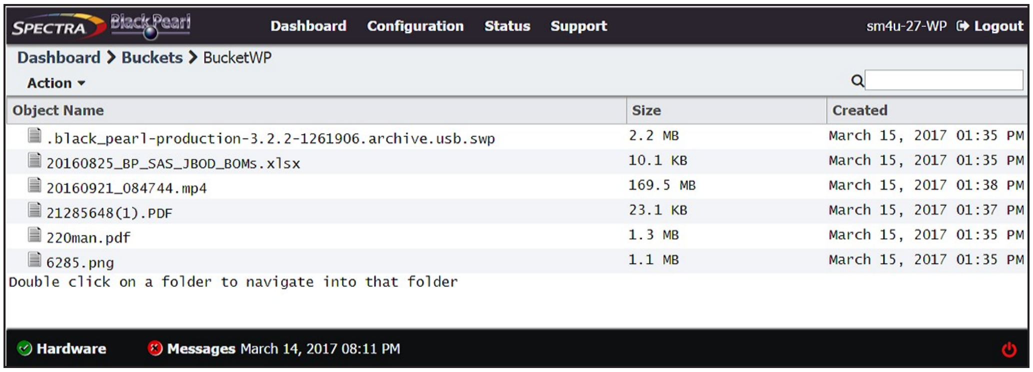
Use the instructions in this section to download an object through the BlackPearl user interface.

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.

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. From the menu bar, select **Configuration > Buckets**. The Buckets screen displays (see Figure 59 on page 171).
2. Double-click the bucket that contains the object you want to download. The Bucket Details screen displays a list of all objects in the bucket.



Object Name	Size	Created
.black_pearl-production-3.2.2-1261906.archive.usb.swp	2.2 MB	March 15, 2017 01:35 PM
20160825_BP_SAS_JBOD_BOMs.xlsx	10.1 KB	March 15, 2017 01:35 PM
20160921_084744.mp4	169.5 MB	March 15, 2017 01:38 PM
21285648(1).PDF	23.1 KB	March 15, 2017 01:37 PM
220man.pdf	1.3 MB	March 15, 2017 01:35 PM
6285.png	1.1 MB	March 15, 2017 01:35 PM

Double click on a folder to navigate into that folder

Figure 246 The Bucket details screen.

3. Select the object you want to download, and select **Action > Download**. The object begins downloading through your web server.

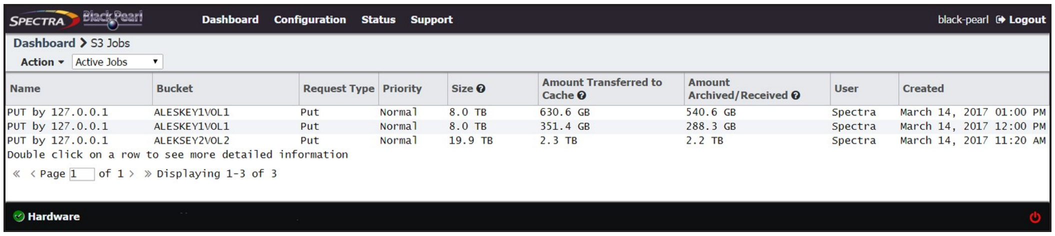
Cancel DS3 Jobs

You can use the BlackPearl user interface to cancel an in-progress DS3 job, or to cancel all S3 jobs, instead of using your DS3 client.

Note: You cannot cancel a PUT or GET job initiated by the Vail application associated with the BlackPearl Nearline gateway.

Use the instructions in this section to cancel a DS3 job(s).

1. From the menu bar, select **Status > S3 Jobs** to display the S3 Jobs screen.



Name	Bucket	Request Type	Priority	Size	Amount Transferred to Cache	Amount Archived/Received	User	Created
PUT by 127.0.0.1	ALESKEY1VOL1	Put	Normal	8.0 TB	630.6 GB	540.6 GB	Spectra	March 14, 2017 01:00 PM
PUT by 127.0.0.1	ALESKEY1VOL1	Put	Normal	8.0 TB	351.4 GB	288.3 GB	Spectra	March 14, 2017 12:00 PM
PUT by 127.0.0.1	ALEKSEY2VOL2	Put	Normal	19.9 TB	2.3 TB	2.2 TB	Spectra	March 14, 2017 11:20 AM

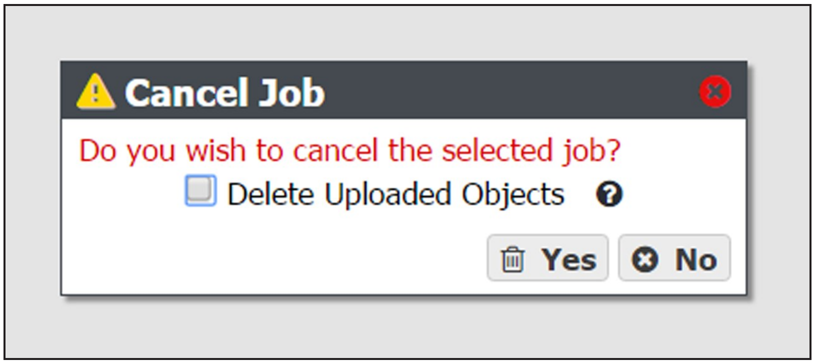
Double click on a row to see more detailed information

« ‹ Page 1 of 1 › » Displaying 1-3 of 3

Figure 247 The S3 Jobs screen.

2. Cancel one or more in-progress jobs.

   a. Select the job to cancel and then select **Action > Cancel** or select **Action > Cancel All Jobs**. The Cancel Job or Cancel All Jobs screen displays.



Cancel Job

Do you wish to cancel the selected job?

□ Delete Uploaded Objects

Figure 248 The Cancel Job screen.

   b. Optionally, select **Delete Uploaded Objects** to delete any objects associated with a current in-progress PUT job that are already uploaded to the gateway.

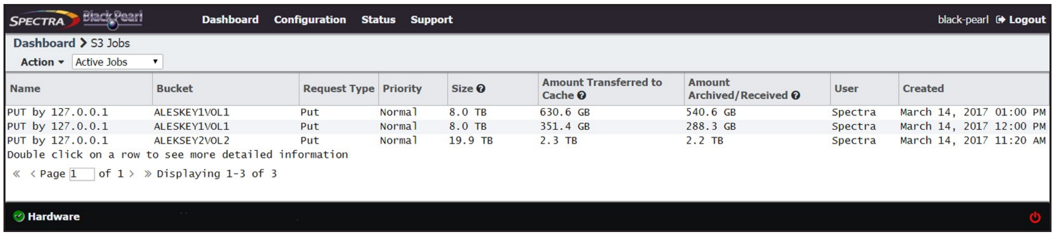
   c. Click **Yes** to cancel all S3 jobs, or the individual selected S3 job.

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. From the menu bar, select **Status > S3 Jobs** to display the S3 Jobs screen.



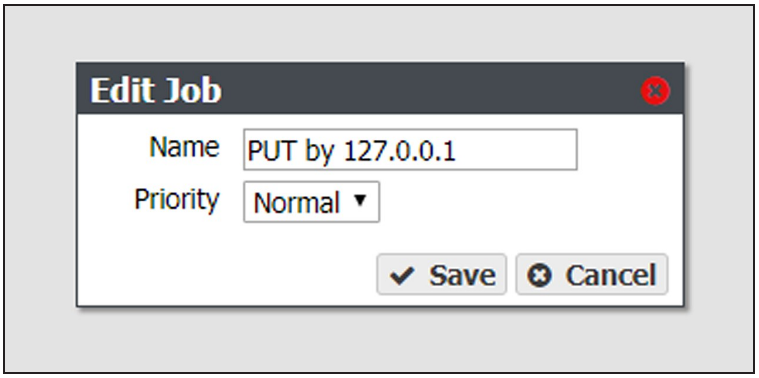
Name	Bucket	Request Type	Priority	Size	Amount Transferred to Cache	Amount Archived/Received	User	Created
PUT by 127.0.0.1	ALESKEY1VOL1	Put	Normal	8.0 TB	630.6 GB	540.6 GB	Spectra	March 14, 2017 01:00 PM
PUT by 127.0.0.1	ALESKEY1VOL1	Put	Normal	8.0 TB	351.4 GB	288.3 GB	Spectra	March 14, 2017 12:00 PM
PUT by 127.0.0.1	ALEKSEY2VOL2	Put	Normal	19.9 TB	2.3 TB	2.2 TB	Spectra	March 14, 2017 11:20 AM

Double click on a row to see more detailed information

« ‹ Page 1 of 1 › » Displaying 1-3 of 3

Figure 249 The S3 Jobs screen.

2. Select the row of the S3 job for which you want to change the name, and select **Action > Edit Job**. The Edit Job dialog box displays.



Name: PUT by 127.0.0.1

Priority: Normal

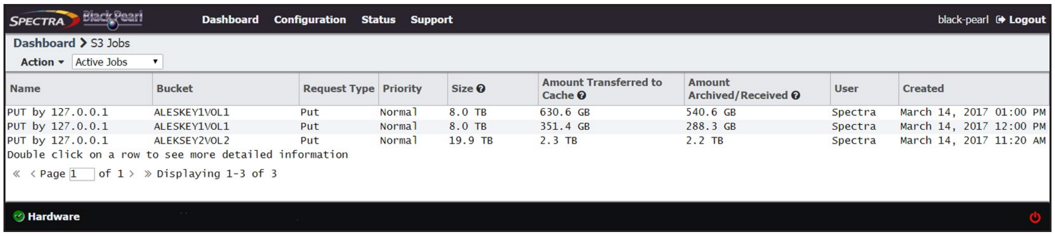
Figure 250 The Edit Job dialog box.

3. Enter the desired **Name**.
4. Using the drop-down menu, select the job **Priority**.
5. Click **Save**.

Clear All Canceled or Completed Jobs

If desired, you can clear completed or canceled jobs from the BlackPearl user interface.

1. From the menu bar, select **Status > S3 Jobs** to display the S3 Jobs screen.



Name	Bucket	Request Type	Priority	Size	Amount Transferred to Cache	Amount Archived/Received	User	Created
PUT by 127.0.0.1	ALESKEY1VOL1	Put	Normal	8.0 TB	630.6 GB	540.6 GB	Spectra	March 14, 2017 01:00 PM
PUT by 127.0.0.1	ALESKEY1VOL1	Put	Normal	8.0 TB	351.4 GB	288.3 GB	Spectra	March 14, 2017 12:00 PM
PUT by 127.0.0.1	ALEKSEY2VOL2	Put	Normal	19.9 TB	2.3 TB	2.2 TB	Spectra	March 14, 2017 11:20 AM

Double click on a row to see more detailed information

« ‹ Page 1 of 1 › » Displaying 1-3 of 3

Figure 251 The S3 Jobs screen.

2. Clear canceled or completed jobs:

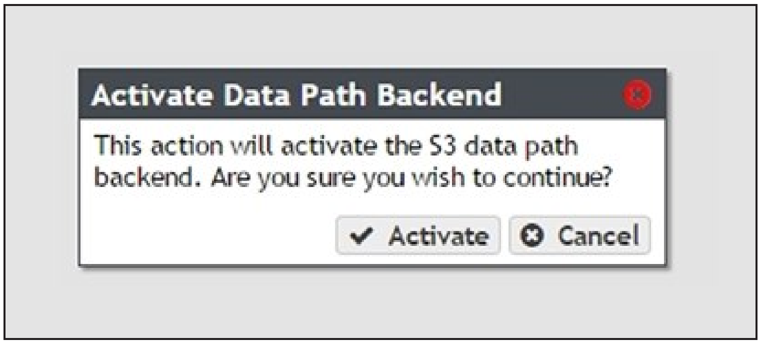
- To clear all canceled jobs, select **Action > Clear All Canceled Jobs.**
- To clear all completed jobs, select **Action > Clear All Completed Jobs.**

3. A confirmation window displays. Click **Clear** to confirm clearing the jobs.

Manually Starting the S3 Data Path Backend

If the BlackPearl gateway is powered off for longer than the timeout value specified in the 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. From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 161 on page 292).
2. Double-click the S3 service, or select the S3 service and select **Action > Show Details**. The S3 details screen displays.
3. On the S3 service details screen, select **Action > Activate Data Path Backend**. The Activate Data Path Backend confirmation window displays.



Activate Data Path Backend

This action will activate the S3 data path backend. Are you sure you wish to continue?

Figure 252 The Activate Data Path Backend screen.

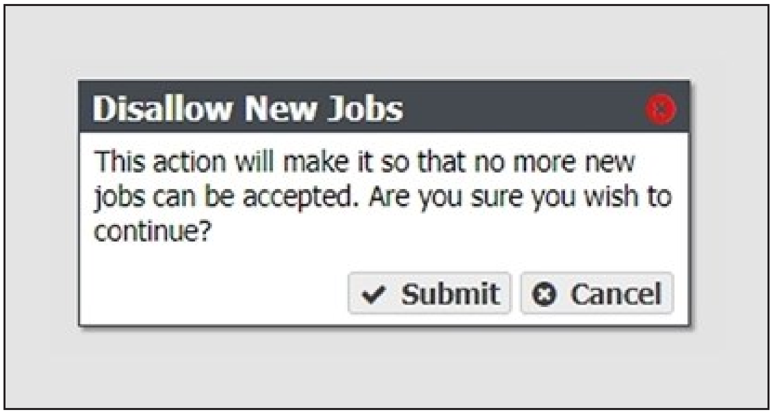
4. Click **Activate**.

Disallow New Jobs

If desired, you can stop the BlackPearl gateway from accepting new S3 jobs.

1. From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 161 on page 292).
2. Double-click the S3 service, or select the S3 service and select **Action > Show Details**. The S3 details screen displays.

3. On the 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?

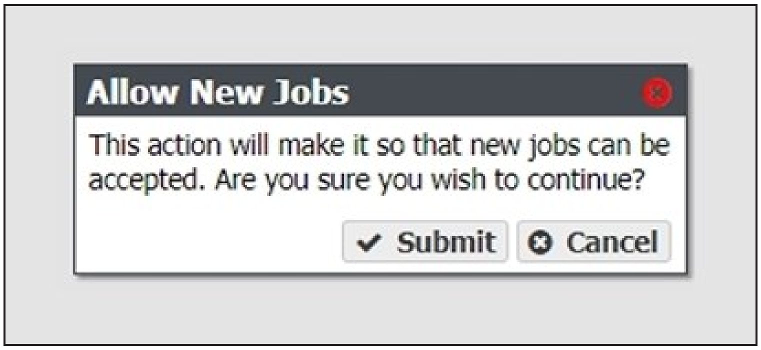
Figure 253 The Disallow New Jobs confirmation window.

4. Click **Submit**.

Allow New Jobs

If you have configured the BlackPearl gateway to no longer accept new S3 jobs, use the instructions in this section to configure the gateway to allow new jobs.

1. From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 161 on page 292).
2. Double-click the S3 service, or select the S3 service and select **Action > Show Details**. The S3 details screen displays.
3. On the 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 254 The Allow New Jobs confirmation window.

4. Click **Submit**.

MONITOR THE BLACKPEARL GATEWAY

The Visual Status Beacon on the front bezel, and the BlackPearl user interface, combine to provide a number of tools for monitoring the health and performance of the BlackPearl gateway and its components.

- 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 on the next page).

  Note: The front bezels in BlackPearl Gen1 2U master nodes, and some Gen1 4U chassis, do not include a Visual Status Beacon light bar.

- System messages provide important information about the BlackPearl gateway and its operation (see Check System Messages on page 420 for more information).
- Icons on the Hardware screen provide overall status of the hardware components in each group (see View the Status of Hardware Components on page 421 for more information). Clicking the text next to each icon displays detailed status information for the components in the group.
- You can also use the BlackPearl user interface to do the following:
  - View the status of services (see View the Status of Services on page 423).
  - View the status of NAS pools, volumes, and shares (see View the Status of NAS Pools on page 423, View the Status of NAS Volumes on page 426, and "View the Status of NAS Shares" on page 426).
  - View the status of the database and cache (see View the Status of the System Pools on page 428).
  - View performance metrics for the drives, CPUs, cache, and network (see View Performance Metrics on page 438).
  - View the current network configuration settings (see Configure Network Connections and Settings on page 280).
  - View the status of any DS3 jobs running on the gateway (see View DS3 Jobs Information on page 431).
  - View the status of media in the associated tape library (see View Tape Media Information on page 433).
  - Reboot or shutdown the gateway (see Reboot or Shut Down a BlackPearl Gateway on page 451).

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.

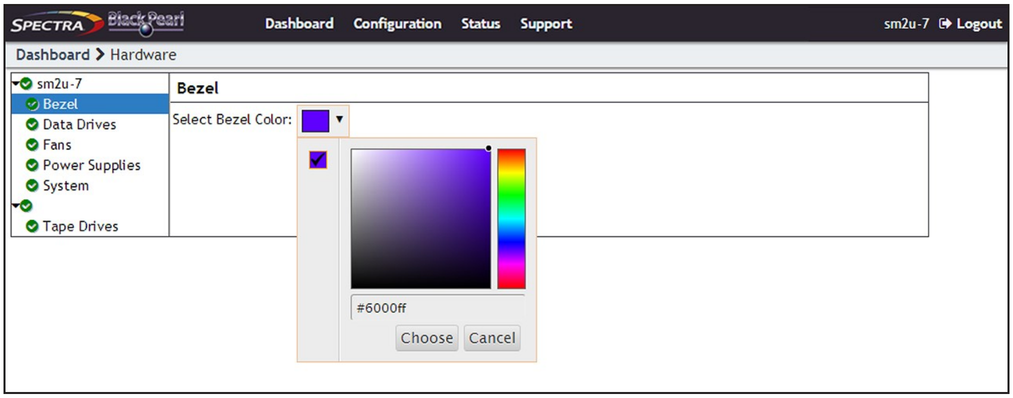
Color Display	Condition
Purple Scroll	The gateway is operating normally. **Note:** The color displayed when the gateway is operating normally can be changed on the Hardware screen. See Configuring the Visual Status Beacon Color on the next page for more information.
Yellow Scroll	The gateway is experiencing 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.
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 View the Status of Hardware Components on page 421 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 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 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.

1. From the menu bar, select **Status > Hardware**, or click the Hardware pane on the Dashboard, or click the Hardware link on the status bar. The Hardware screen displays.
2. Click **Bezel**. The Bezel pane of the Hardware screen displays.
3. Click the colored box next to **Select Bezel Color**. The color picker window displays.



Select Bezel Color:

#6000ff

Figure 255 Use the color picker to set the color of the Visual Status Beacon when the gateway is operating normally.

4. 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 or red, so that you can more easily determine if the gateway is in a warning or error state.

5. Click **Choose** to set the color of the Visual Status Beacon.

System Status LEDs

The system status LEDs provide information about the status of the gateway, its fans, network connections, and power supplies.

Gen2 X Series Chassis

The table below lists each system status LED, in order from left to right, and its function.

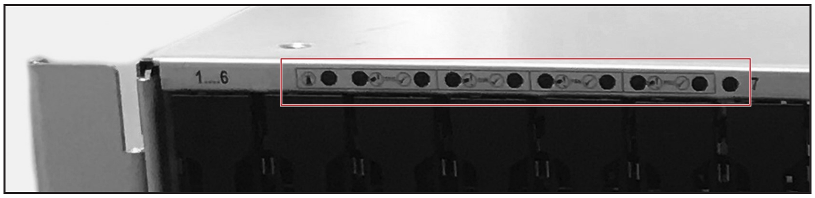


Figure 256 The top left section of the front of the Gen2 X chassis (front bezel removed) showing system status LEDs.

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 Identify the Failed Component on page 489 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.

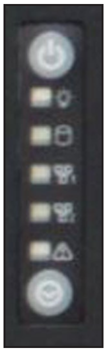


Figure 257 The top right section of the front of the Gen2 S Series chassis, with the front bezel removed, showing system status LEDs.

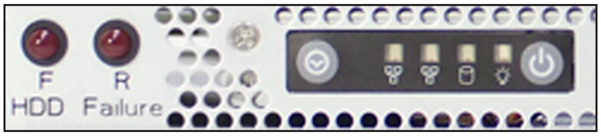


Figure 258 The top left section of the front of the Gen2 V Series chassis, with the front bezel removed, showing system status LEDs.

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.

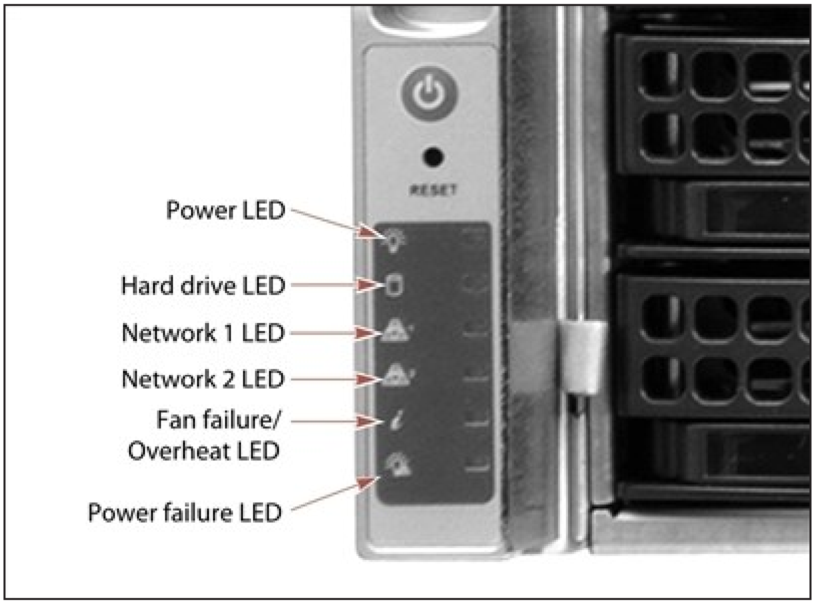


Figure 259 The left side of the front of the Gen1 S Series chassis showing system status LEDs.

LED	Function
Power	Indicates if the unit is powered on or off.
Hard Drive	Indicates boot drive activity. To see the activity of a data drive, see Data drive status LEDs on page 36.
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 9.
Power Failure	Indicates a power supply failure. Check the BlackPearl user interface to determine which power supply failed.

Check System Messages

Check the system messages regularly. These messages provide important information about the BlackPearl 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 gateway may occur.
Warning	Notifies the user of a failure that may adversely impact the BlackPearl gateway.
Critical	Notifies the user of a failure that caused significant adverse impact to the BlackPearl gateway.

If any system messages are generated by the gateway, the status bar displayed at the bottom of all BlackPearl screens shows the severity, date, and time of the highest severity unread message. If there are no system messages, this text does not display.

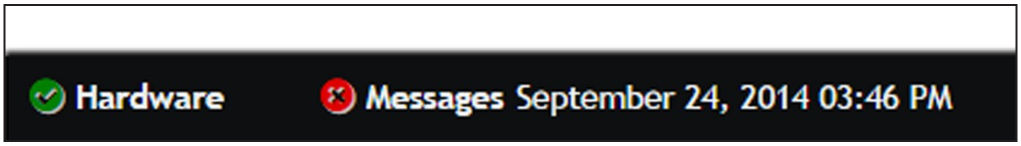
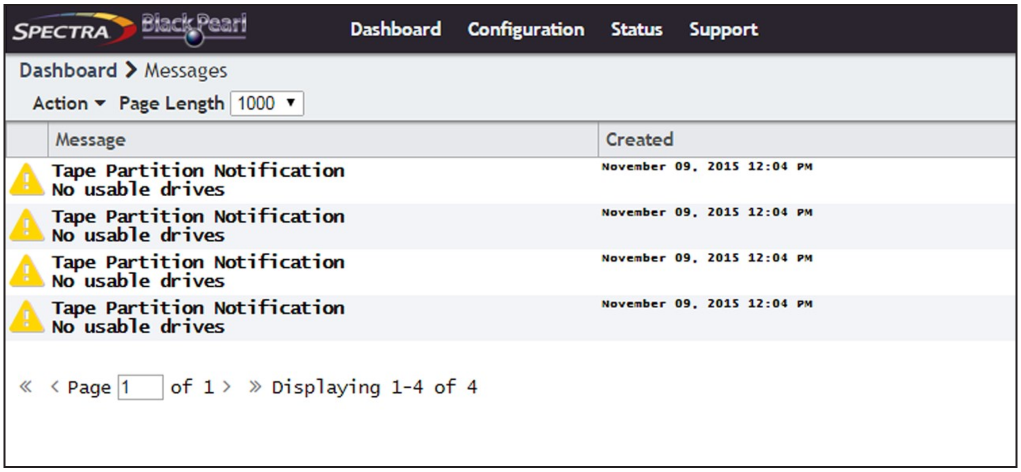


Figure 260 A system message displayed on the BlackPearl user interface status bar.

Use the instructions in this section to check system messages.

1. From the menu bar, select **Status > Messages**, or click the Messages link on the status bar, to display the Messages screen.



	Message	Created
⚠	Tape Partition Notification No usable drives	November 09, 2015 12:04 PM
⚠	Tape Partition Notification No usable drives	November 09, 2015 12:04 PM
⚠	Tape Partition Notification No usable drives	November 09, 2015 12:04 PM
⚠	Tape Partition Notification No usable drives	November 09, 2015 12:04 PM

« ‹ Page 1 of 1 › » Displaying 1-4 of 4

Figure 261 The Messages screen.

Pay extra attention to any messages flagged with the Warning or Error icon (see Status Icons on page 64), and follow any recommended steps. Contact Spectra Logic Technical Support if you need assistance (see Contacting Spectra Logic on page 9).

Note: 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.

2. If desired, use the **Page Length** 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 select **Action > Mark as read**. To mark all messages as read, select **Action >Mark all as read**.

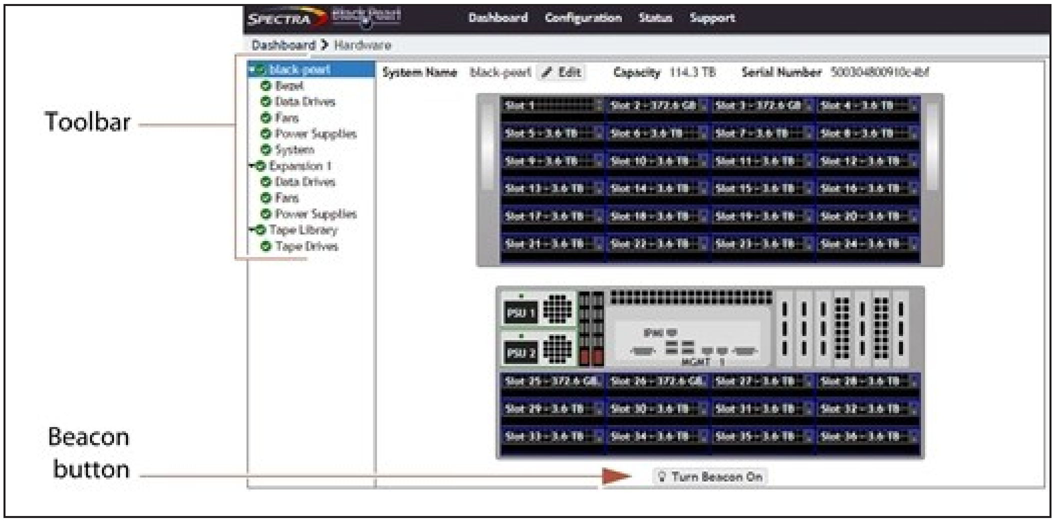
Note: Messages can also be marked as **Unread** using the **Action** menu.

View the Status of Hardware Components

The BlackPearl user interface lets you monitor the status of hardware components in the gateway, and the connected library tape drives, without having direct physical access. This is especially useful when your BlackPearl 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. From the menu bar, 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 262 The Hardware screen. Gen1 S Series 4U chassis shown.

2. Use the toolbar menu on the left-hand side of the screen to view detailed information about component groups. The following table describes the types of information on each details screen. An icon next to each component indicates the status (see Status Icons on page 64 for a description of the icons).

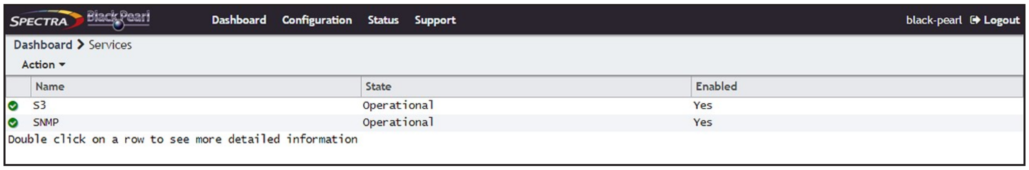
Clicking...	Shows the...
Bezel	Color of the Visual Status Beacon that is displayed during normal operation. See Front Bezel Visual Status Beacon on page 415 for more information about the colors displayed by the Visual Status Beacon.
Data Drives	• Slot number of each drive • Status of each drive • Drive size, serial number, and firmware level • The name of the cache to which the drive is assigned
Fans	• Status of midplane fans
Power Supplies	• Power supply status and wattage **Note:** Power supply information is not available for the 77-bay or 107-bay expansion node.
System	• CPU status and temperature • System memory status and size • Status, manufacturer, model, size, and serial number for each boot drive

Clicking...	Shows the...
Tape Drives	• Status of tape drives in the tape library connected to the gateway
Turn Beacon On (*Below chassis graphic*)	Click **Turn Beacon On** to cause the Visual Status Beacon light on a BlackPearl gateway to flash blue. This is useful when you have multiple gateways and need to locate a specific one, for example to replace a component. Click the button a second time to stop the light from flashing.

View the Status of Services

The Services screen provides status information about services that are currently installed on the BlackPearl gateway.

From the menu bar, select **Configuration > Services** to display the Services screen.



	Name	State	Enabled
✓	S3	Operational	Yes
✓	SNMP	Operational	Yes

Double click on a row to see more detailed information

Figure 263 The Services screen.

The Services screen displays the following information:

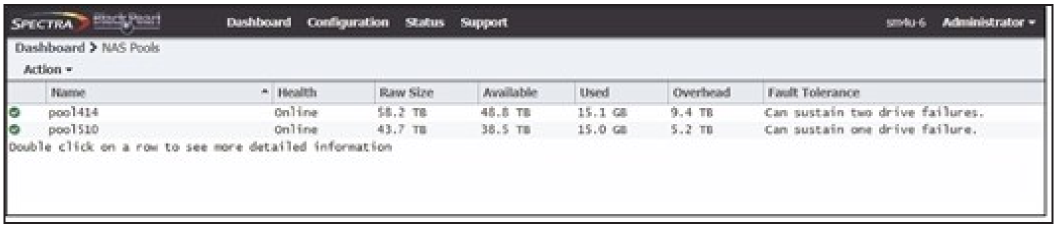
This column...	Shows...
Name	The name of the service running on the gateway.
State	The status of the service on the BlackPearl Nearline gateway. • **Starting**—The service is starting up. • **Operational**—The service is running. • **Stopped**—The service is not running.
Enabled	Whether or not the service is enabled at system startup. • **Yes**—Service automatically starts when the gateway is powered on. • **No**—Service does not start when the gateway is powered on.

View the Status of NAS Pools

The Pools screen provides status information about all NAS storage pools that are configured on the gateway.

1. From the menu bar, select **Status > NAS > Pools** to display the Pools screen.

2. The status of each storage pool is indicated by the status icons on the left side of the screen.



	Name	Health	Raw Size	Available	Used	Overhead	Fault Tolerance
●	pool414	Online	58.2 TB	48.8 TB	15.1 GB	9.4 TB	Can sustain two drive failures.
●	pool510	Online	43.7 TB	38.5 TB	15.0 GB	5.2 TB	Can sustain one drive failure.

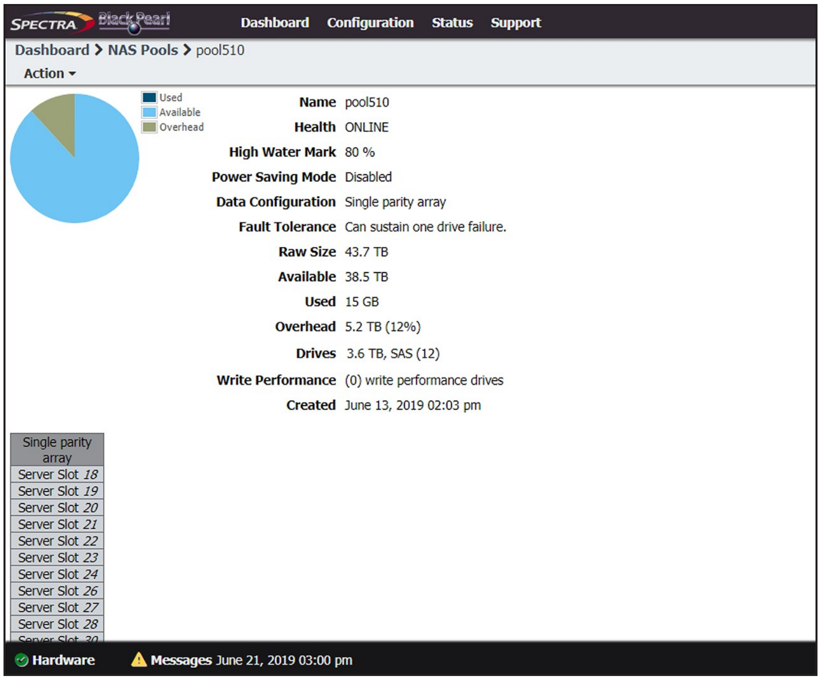
Double click on a row to see more detailed information

Figure 264 The Pools screen.

The Pools screen 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.
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.
Fault Tolerance	The fault tolerance setting for each pool.

3. To view additional information about a NAS pool, select the pool and then select **Action > Show Details**. The *pool name* details screen displays.



Name pool510
Health ONLINE
High Water Mark 80 %
Power Saving Mode Disabled
Data Configuration Single parity array
Fault Tolerance Can sustain one drive failure.
Raw Size 43.7 TB
Available 38.5 TB
Used 15 GB
Overhead 5.2 TB (12%)
Drives 3.6 TB, SAS (12)
Write Performance (0) write performance drives
Created June 13, 2019 02:03 pm

Single parity array
Server Slot *18*
Server Slot *19*
Server Slot *20*
Server Slot *21*
Server Slot *22*
Server Slot *23*
Server Slot *24*
Server Slot *26*
Server Slot *27*
Server Slot *28*
Server Slot *30*

Figure 265 A NAS Pool details screen.

The *pool name* details screen displays the following information:

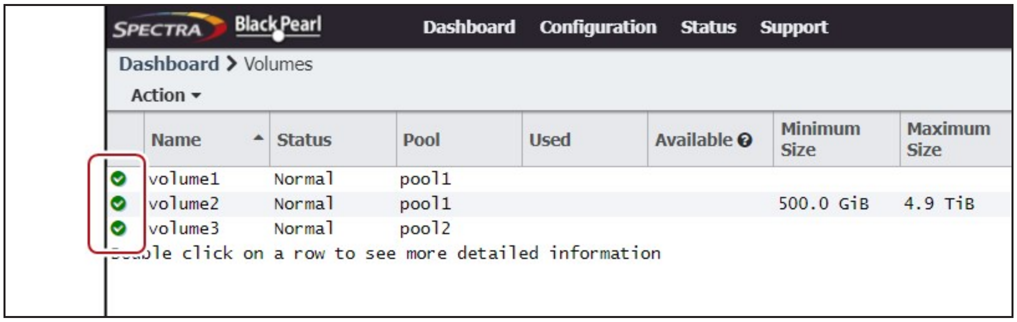
This row...	Shows...
Name	The name of the pool.
Health	The current health of the pool.
High Water Mark	When the used space on the pool reaches this percentage, an alert is generated. No alert is generated when the percentage is set to zero.
Power Saving Mode	Indicates if power saving mode is enabled or disabled.
Data Configuration	The protection level for the pool.
Fault Tolerance	The number of drives that can fail before data is lost.
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.

This row…	Shows…
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.
Stripe	The location of all disks included in the pool.

View the Status of NAS Volumes

The Volumes screen provides status information about all NAS volumes that are configured on the gateway.

1. From the menu bar, select **Status > NAS > Volumes** to display the Volumes screen.
2. The status of each volume is indicated by the status icons on the left side of the screen.



	Name	Status	Pool	Used	Available	Minimum Size	Maximum Size
✓	volume1	Normal	pool1				
✓	volume2	Normal	pool1			500.0 GiB	4.9 TiB
✓	volume3	Normal	pool2				

Double click on a row to see more detailed information

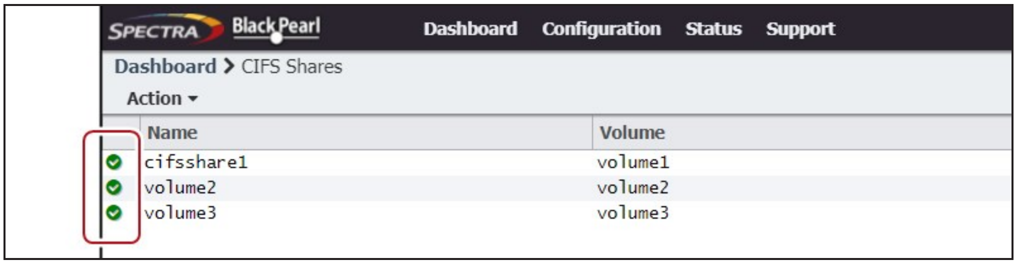
Figure 266 The Volumes screen.

View the Status of NAS Shares

The Shares screen provides status information about all NAS shares that are configured on the gateway.

1. From the menu bar, select **Configuration > NAS > Shares > CIFS** to display the CIFS Shares screen, select **Configuration > NAS > Shares > NFS** to display the NFS Shares screen, or select **Configuration > NAS > Shares > Vail S3** to display Vail Shares.

2. The status of each share is indicated by the status icons on the left side of the screen.



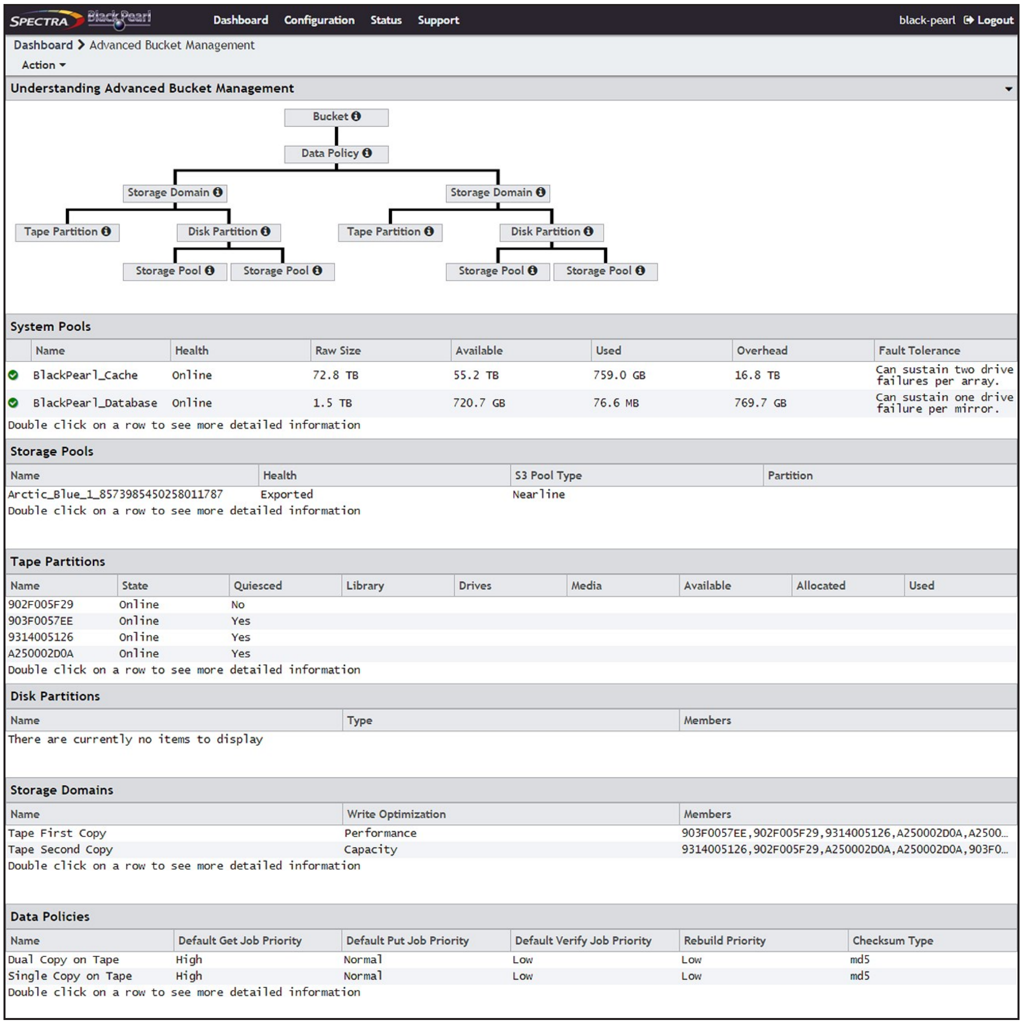
	Name	Volume
✓	cifsshare1	volume1
✓	volume2	volume2
✓	volume3	volume3

Figure 267 The CIFS Shares screen.

View the Status of the System Pools

The System Pools pane of the Advanced Bucket Management screen provides status information about the database and cache pools configured on the BlackPearl gateway, as well as status information for each system pool.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen.



System Pools

	Name	Health	Raw Size	Available	Used	Overhead	Fault Tolerance
✓	BlackPearl_Cache	Online	72.8 TB	55.2 TB	759.0 GB	16.8 TB	Can sustain two drive failures per array.
✓	BlackPearl_Database	Online	1.5 TB	720.7 GB	76.6 MB	769.7 GB	Can sustain one drive failure per mirror.

Double click on a row to see more detailed information

Storage Pools

Name	Health	S3 Pool Type	Partition
Arctic_Blue_1_8573985450258011787	Exported	Nearline	

Double click on a row to see more detailed information

Tape Partitions

Name	State	Quiesced	Library	Drives	Media	Available	Allocated	Used
902F005F29	Online	No						
903F0057EE	Online	Yes						
9314005126	Online	Yes						
A250002D0A	Online	Yes						

Double click on a row to see more detailed information

Disk Partitions

Name	Type	Members

There are currently no items to display

Storage Domains

Name	Write Optimization	Members
Tape First Copy	Performance	903F0057EE,902F005F29,9314005126,A250002D0A,A2500…
Tape Second Copy	Capacity	9314005126,902F005F29,A250002D0A,A250002D0A,903F0…

Double click on a row to see more detailed information

Data Policies

Name	Default Get Job Priority	Default Put Job Priority	Default Verify Job Priority	Rebuild Priority	Checksum Type
Dual Copy on Tape	High	Normal	Low	Low	md5
Single Copy on Tape	High	Normal	Low	Low	md5

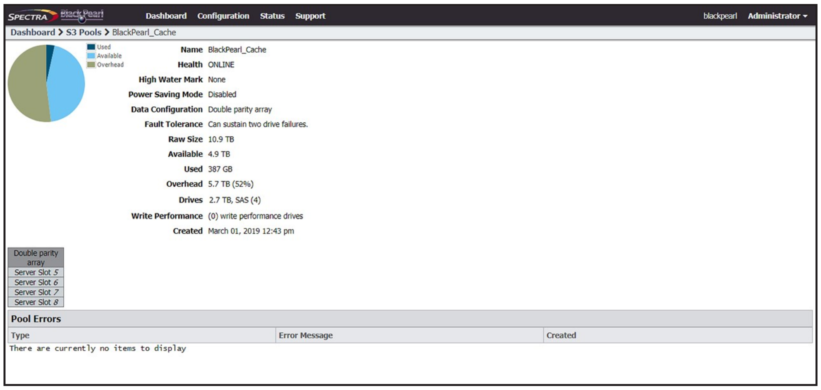
Double click on a row to see more detailed information

Figure 268 The System Pools pane of the Advanced Bucket Management screen.

The System Pools pane displays the following information.

This column...	Shows...
Name	The name of each system pool. This name cannot be edited.
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.
Fault Tolerance	The fault tolerance setting for each system pool.

2. To view additional information about a system pool, select the system pool and then select **Action > Show Details**. The *system pool name* details screen displays.



Name	BlackPearl_Cache
Health	ONLINE
High Water Mark	None
Power Saving Mode	Disabled
Data Configuration	Double parity array
Fault Tolerance	Can sustain two drive failures.
Raw Size	10.9 TB
Available	4.9 TB
Used	387 GB
Overhead	5.7 TB (52%)
Drives	2.7 TB, SAS (4)
Write Performance	(0) write performance drives
Created	March 01, 2019 12:43 pm

Pool Errors

Type	Error Message	Created
There are currently no items to display		

Figure 269 The BlackPearl_Cache details screen.

The *system pool name* details screen displays the following information:

This row...	Shows...
Name	The name of the pool. This name cannot be edited.
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.

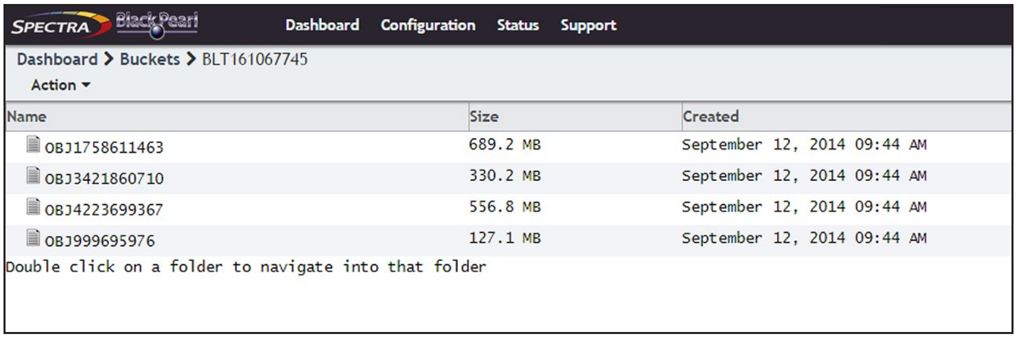
This row...	Shows...
Power Saving Mode	Indicates if power saving mode is enabled or disabled.
Data Configuration	The protection level for the pool.
Fault Tolerance	The number of drives that can fail before data is lost.
Raw Size	The total amount of storage space assigned to the pool.
Available	The amount 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.
Stripe	The location of all disks included in the pool.
Pool Errors	Gives details of pool errors if any.

View Bucket Contents

Use the instructions in this section to view the contents of a bucket configured on the BlackPearl gateway.

1. From the menu bar, select **Configuration > Buckets**. The Buckets screen displays (see Figure 59 on page 171).

2. Double-click the name of the bucket for which you want to view the contents. The details screen for the bucket displays.



Name	Size	Created
OBJ1758611463	689.2 MB	September 12, 2014 09:44 AM
OBJ3421860710	330.2 MB	September 12, 2014 09:44 AM
OBJ4223699367	556.8 MB	September 12, 2014 09:44 AM
OBJ999695976	127.1 MB	September 12, 2014 09:44 AM

Double click on a folder to navigate into that folder

Figure 270 The details screen for a selected bucket.

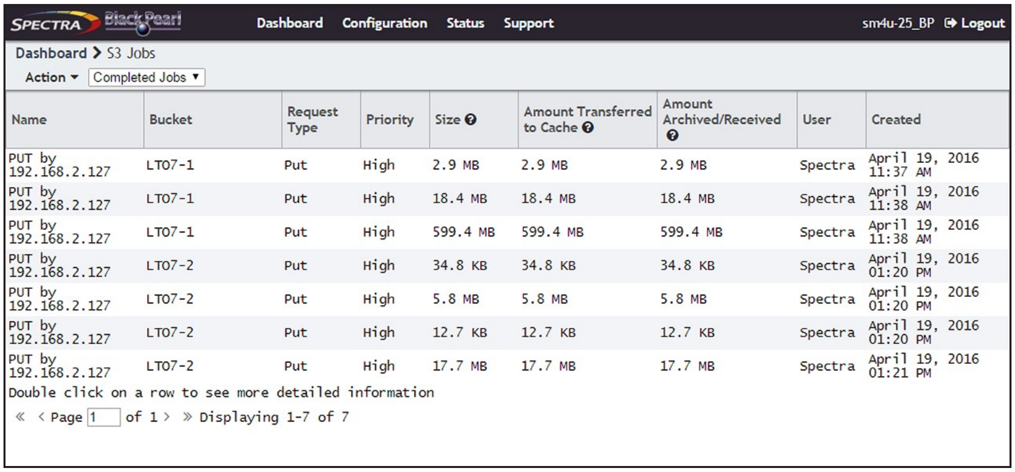
The bucket details screen displays the following information for each object contained in the bucket:

This row...	Shows...
Object Name	The name of an object in the specified bucket.
Size	The size of the object.
Created	The timestamp of when the object was written to the bucket.

View DS3 Jobs Information

The S3 Jobs screen displays the status of all DS3 jobs the gateway is currently processing, all canceled jobs, and all completed jobs.

From the menu bar, select **Status > S3 Jobs** to display the S3 Jobs screen.



Name	Bucket	Request Type	Priority	Size	Amount Transferred to Cache	Amount Archived/Received	User	Created
PUT by 192.168.2.127	LT07-1	Put	High	2.9 MB	2.9 MB	2.9 MB	Spectra	April 19, 2016 11:37 AM
PUT by 192.168.2.127	LT07-1	Put	High	18.4 MB	18.4 MB	18.4 MB	Spectra	April 19, 2016 11:38 AM
PUT by 192.168.2.127	LT07-1	Put	High	599.4 MB	599.4 MB	599.4 MB	Spectra	April 19, 2016 11:38 AM
PUT by 192.168.2.127	LT07-2	Put	High	34.8 KB	34.8 KB	34.8 KB	Spectra	April 19, 2016 01:20 PM
PUT by 192.168.2.127	LT07-2	Put	High	5.8 MB	5.8 MB	5.8 MB	Spectra	April 19, 2016 01:20 PM
PUT by 192.168.2.127	LT07-2	Put	High	12.7 KB	12.7 KB	12.7 KB	Spectra	April 19, 2016 01:20 PM
PUT by 192.168.2.127	LT07-2	Put	High	17.7 MB	17.7 MB	17.7 MB	Spectra	April 19, 2016 01:21 PM

Double click on a row to see more detailed information

« ‹ Page 1 of 1 › » Displaying 1-7 of 7

Figure 271 The S3 Jobs screen.

Use the job status drop-down menu to select **Active Jobs**, **Canceled Jobs**, or **Completed Jobs** as desired.

The S3 Jobs screen displays the following information:

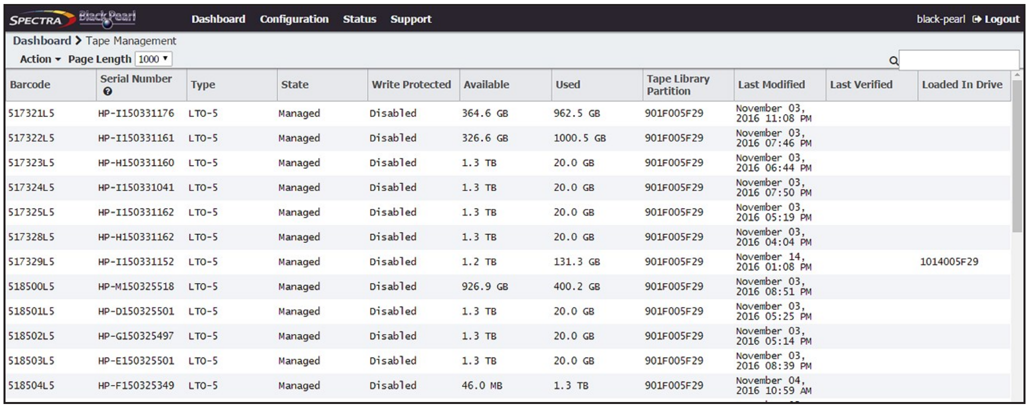
This column...	Shows...
Name	The name of the job request, which is generated automatically using the job request type and IP address of the source or destination host. **Note:** Multiple jobs of the same request type from the same host IP address all have the same name.
Bucket	The name of the bucket that is acted on by the job request. **Note:** Jobs created from standard S3 PUT and GET requests do not display a bucket name in the S3 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**.
Size	The amount of data to be transferred by the job.
Amount 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.
Amount Archived/Received	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.
User	The S3 user that initiated the job.
Created	The timestamp of when the job was created.
Date Canceled (Canceled jobs only)	The timestamp of when the job was canceled.
Date Completed (Completed jobs only)	The timestamp of when the job completed.

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, or in a specified bucket.

1. Display the Tape Management Screen:

- To view the status of all tapes in the associated tape library, from the menu bar, select **Status > Tape Management.** The Tape Management screen displays.



Dashboard > Tape Management

Action ▾ Page Length 1000 ▾

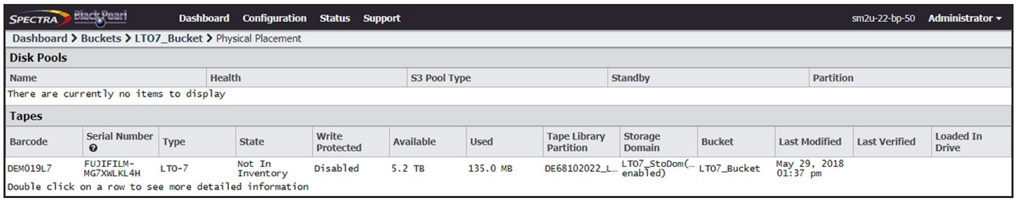
Barcode	Serial Number	Type	State	Write Protected	Available	Used	Tape Library Partition	Last Modified	Last Verified	Loaded In Drive
517321L5	HP-I150331176	LTO-5	Managed	Disabled	364.6 GB	962.5 GB	901F005F29	November 03, 2016 11:08 PM		
517322L5	HP-I150331161	LTO-5	Managed	Disabled	326.6 GB	1000.5 GB	901F005F29	November 03, 2016 07:46 PM		
517323L5	HP-H150331160	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 06:44 PM		
517324L5	HP-I150331041	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 07:50 PM		
517325L5	HP-I150331162	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 05:19 PM		
517328L5	HP-H150331162	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 04:04 PM		
517329L5	HP-I150331152	LTO-5	Managed	Disabled	1.2 TB	131.3 GB	901F005F29	November 14, 2016 01:08 PM		1014005F29
518500L5	HP-M150325518	LTO-5	Managed	Disabled	926.9 GB	400.2 GB	901F005F29	November 03, 2016 08:51 PM		
518501L5	HP-D150325501	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 05:25 PM		
518502L5	HP-G150325497	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 05:14 PM		
518503L5	HP-E150325501	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 08:39 PM		
518504L5	HP-F150325349	LTO-5	Managed	Disabled	46.0 MB	1.3 TB	901F005F29	November 04, 2016 10:59 AM		

Figure 272 The Tape Management screen.

- To view the status of the tapes associated with a bucket:

   a. From the menu bar, select **Configuration > Buckets**. The Buckets screen displays.

   b. Select the bucket for which you want to view the tape media information, and select **Action > Show Physical Placement**. The Physical Placement screen displays.



Dashboard > Buckets > LTO7_Bucket > Physical Placement

Disk Pools

Name	Health	S3 Pool Type	Standby	Partition
There are currently no items to display				

Tapes

Barcode	Serial Number	Type	State	Write Protected	Available	Used	Tape Library Partition	Storage Domain	Bucket	Last Modified	Last Verified	Loaded In Drive
DEM019L7	FUJIFILM-MG7XWLKL4H	LTO-7	Not In Inventory	Disabled	5.2 TB	135.0 MB	DE68102022_L…	LTO7_StoDom(… enabled)	LTO7_Bucket	May 29, 2018 01:37 pm		

Double click on a row to see more detailed information

Figure 273 The Physical Placement screen showing the storage pools and tapes for a specified bucket.

The Tape Management and Physical Placement screens display the following information:

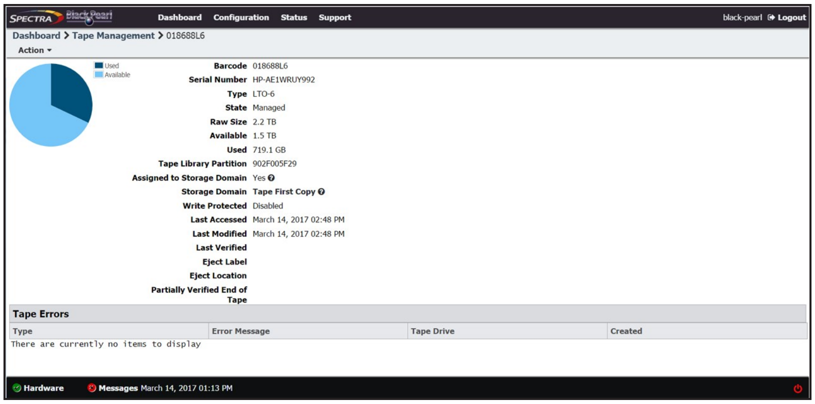
This column…	Shows…
Barcode	The barcode label on the tape cartridge.
Serial Number	The tape manufacturer serial number for the tape cartridge.

This column...	Shows...
Type	The media type. Values: **LTO-5, LTO-6, LTO-7, LTO-7 Type M, LTO-8, LTO-9, TS1140, TS1150, TS1155, TS1160**
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. • **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. • **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 BlackPearlgateway, 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 BlackPearlgateway, 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 BlackPearlgateway, 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.

This column...	Shows...
State *(continued)*	• **FOREIGN**— A tape from another BlackPearl gateway. This data must be copied into a bucket on this gateway before it is accessible. • **FORMAT IN PROGRESS**— The tape is currently being formatted. • **FORMAT PENDING**— A format was requested for the tape but has not yet started. **Note:** A tape that is physically write protected cannot be formatted and always displays a status of Format Pending. • **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 BlackPearl gateway. • **LOST** — The tape was removed from the tape library without first exporting it from a bucket. • **LTFS WITH FOREIGN DATA**— An LTFS formatted tape not associated with a BlackPearl 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 gateway is being imported into the BlackPearl gateway. • **RAW IMPORT PENDING** — An LTFS formatted tape not associated with a BlackPearl gateway is queued to have the data it contains imported into the BlackPearl gateway. • **SERIAL NUMBER MISMATCH**— The tape serial number does not match the one stored in the BlackPearl gateway. • **UNKNOWN**— The tape contains unknown data or is otherwise unavailable to the BlackPearl gateway.
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 for data on the tape cartridge.

This column...	Shows...
Used	The amount of space on the tape cartridge containing data.
Tape Library Partition	The serial number of the partition on the Spectra Logic or 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 Modified	The timestamp of the last time data was written to 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	The BlueScale serial number of the tape drive in which the tape cartridge is loaded.

2. To display detailed information about a tape cartridge, double click the tape cartridge row. A details screen for the selected tape displays.



Barcode 018688L6
Serial Number HP-AE1WRUY992
Type LTO-6
State Managed
Raw Size 2.2 TB
Available 1.5 TB
Used 719.1 GB
Tape Library Partition 902F005F29
Assigned to Storage Domain Yes
Storage Domain Tape First Copy
Write Protected Disabled
Last Accessed March 14, 2017 02:48 PM
Last Modified March 14, 2017 02:48 PM
Last Verified
Eject Label
Eject Location
Partially Verified End of Tape

Tape Errors

Type	Error Message	Tape Drive	Created
There are currently no items to display			

Figure 274 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.

This row...	Shows...
Type	The media type. Values: **LTO-5, LTO-6, LTO-7, LTO-7 Type M, LTO-8, LTO-9, TS1140, TS1150, TS1155, TS1160**
State	The status of the tape. See State on page 435 for a list of tape cartridge states.
Raw Size	The raw size of the tape.
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.
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.
Write Protected	The status of the write-protect switch on the cartridge.
Last Accessed	The timestamp of the last time the tape was loaded into a tape drive.
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.
Export Label	A user-defined label entered when the tape is exported.
Export Location	A user-defined label entered when the tape is exported.
Partially Verified End of Tape	The timestamp of the last time the gateway verified the data on the specified percentage of the tape before the end of data.

If there are any tape errors associated with the specified cartridge, they display in the **Tape Errors** pane of the details screen.

The following commands are available from the **Action** menu on the tape cartridge details screen. Use the links below for more detailed information about each command.

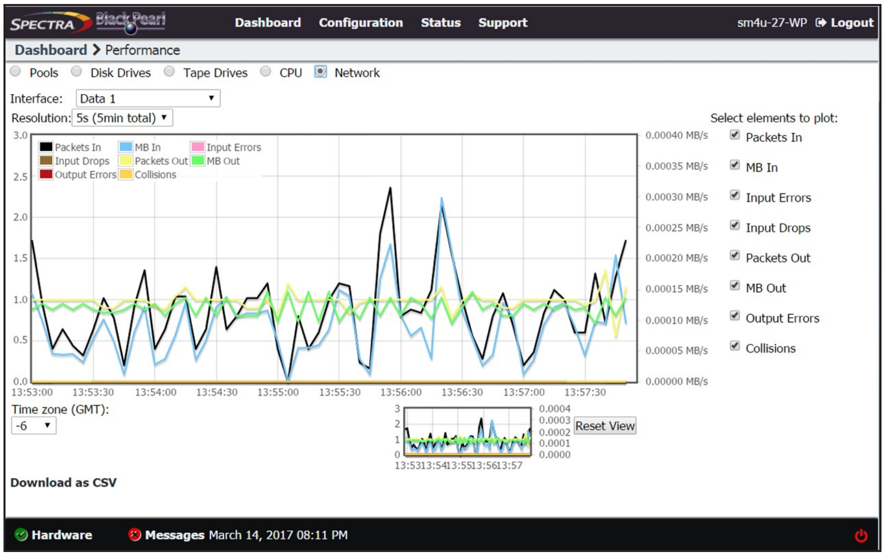
- **Edit** - See Edit Tape Export Information Without Exporting Tape Media on page 395.
- **Export Tape** - See Export Tapes on page 393.
- **Cancel Tape Export** - See Cancel Tape Export on page 395.
- **Format Tape** - See Format Managed BlackPearl Tapes on page 362.

View Performance Metrics

The Performance screen displays performance metrics for the BlackPearl cache, individual data drives, network traffic, and CPUs. Performance graphs can be configured to display either the last 5 minutes of activity, or the last 25 hours.

Use the instructions in this section to view performance metrics.

1. From the menu bar, select **Status > Performance** or click the Performance pane on the Dashboard. The Performance screen displays. The Performance screen displays.



○ Pools ○ Disk Drives ○ Tape Drives ○ CPU ● Network

Interface: Data 1

Resolution: 5s (5min total)

Select elements to plot:
☑ Packets In
☑ MB In
☑ Input Errors
☑ Input Drops
☑ Packets Out
☑ MB Out
☑ Output Errors
☑ Collisions

Time zone (GMT): -6

Messages March 14, 2017 08:11 PM

Figure 275 The Performance screen.

2. Select **Pools, Disk Drives, Tape Drives, CPU,** or **Network** to display performance information about the selected component.

Note: If you select **Pools**, **Disk Drives**, **Tape Drives,** or **Network**, use the **Pool**, **DiskDrive**, **Tape Drive**, or **Interface** drop-down menu to select a specific pool, disk drive, tape drive, or network connection to monitor.

3. Select the time interval using the **Resolution** drop-down menu. The data can be displayed in 1 second increments (5 minutes total) or 1 hour increments (25 hours total).

4. Select or clear options under **Select elements to plot** to indicate which graph lines to display. The graph updates as soon as you select or clear an option.
5. Set the performance graph's time values to your local time zone using the **Time zone (GMT)** menu. All entries are listed in +/- GMT.
6. If desired, click **Download as CSV** on the lower, left side of the panel, 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.
7. To see the performance data in greater detail, select the desired section you want to magnify in either the main or range indicator graph. Using the mouse, 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 main graph.

   The range indicator graph continues to display the original range of data, with the section that is currently being shown on the main graph highlighted.

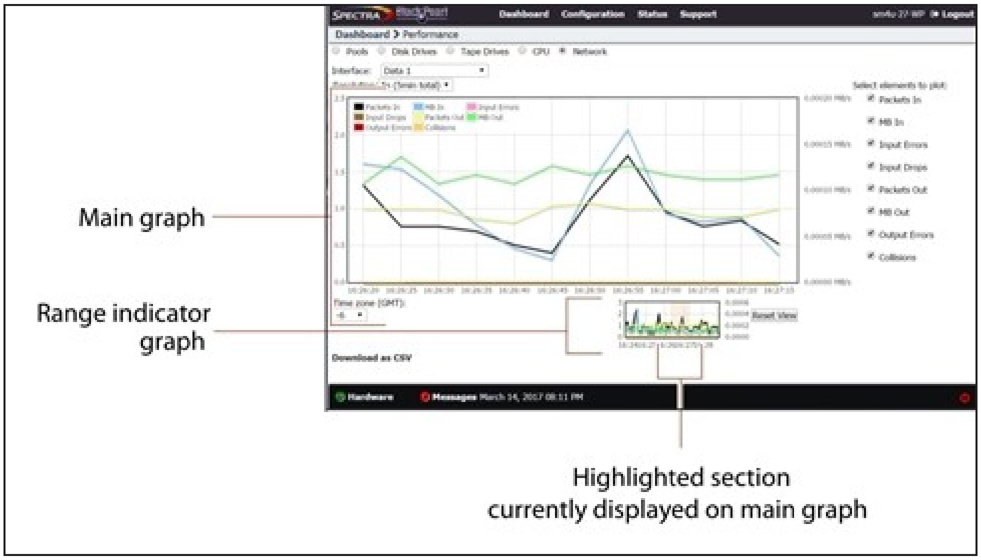


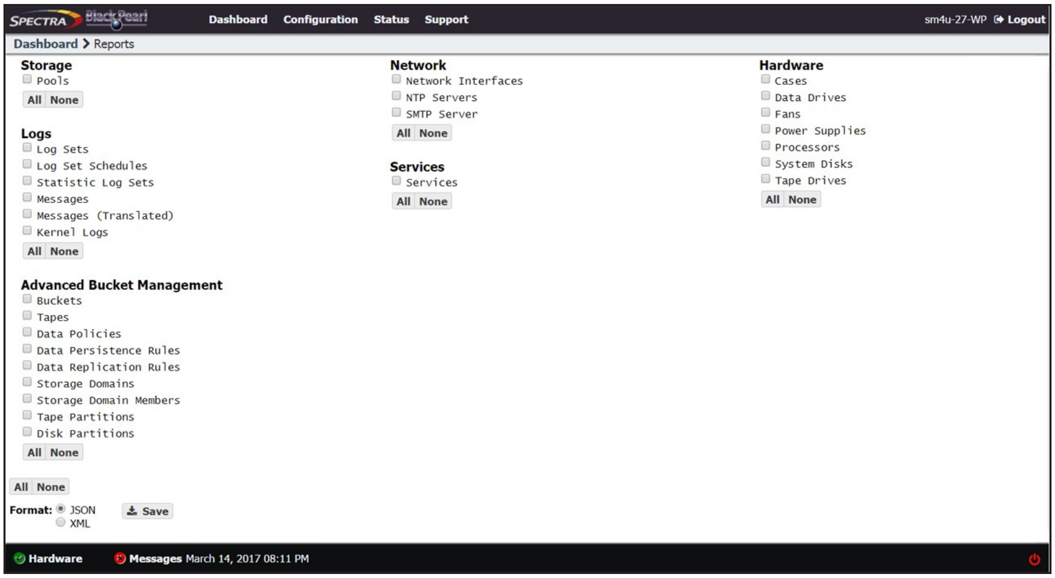
Figure 276 Highlight a section of data to show in greater detail.

8. Click **Reset View** to reset the main graph to the default view.

View Reports

The Reports screen allows you to generate reports on all aspects of the BlackPearl gateway, including component status, and configuration. Reports can be saved in either JSON or XML format.

1. From the menu bar, select **Status > Reports** to display the Reports screen.



Format: ● JSON ○ XML

Figure 277 The Reports screen.

2. Select check boxes next to the report(s) you want to generate.

Note: Use the **All** or **None** buttons at the bottom of each report group to select or clear that group of reports. The **All** and **None** buttons at the bottom of the screen select or clear all reports shown on the screen.

3. Select the **Format** for the report(s). Only one format can be selected.
4. Click **Save**. The selected reports are saved to your local host.
5. Open the report using a compatible program.

DATABASE BACKUP & RESTORE

The BlackPearl 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.

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.

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 gateway, and kept based on the settings of a preconfigured data policy named “Database Backup”.

Note: If your BlackPearl gateway does not contain a tape library, the database backup policy must be manually created.

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 159). If you create a new data policy, you will need to edit the database backup configuration to use the new policy (see Edit Backup Data Policy on page 449).

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 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.

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 gateway does not contain any permanent local storage, the database backup file must be downloaded manually to your host computer.

Create a Database Backup Schedule

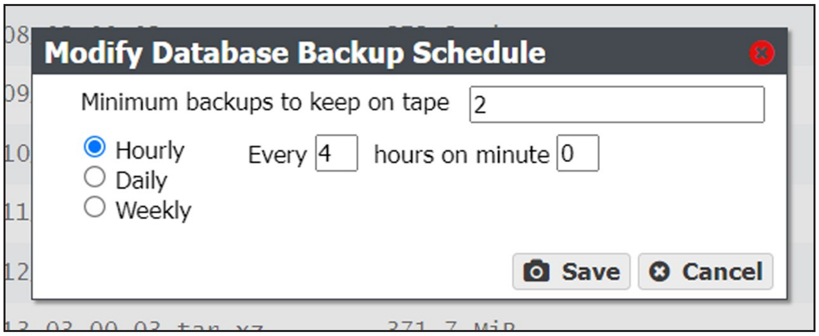
Database backup schedules can be configured at intervals based on hours, number of days, or days of the week. Decide which interval to use for the schedule and follow the appropriate instructions.

- Create an Hourly Schedule below—Create backups every selected number of hours.
- Create a Daily Schedule on the next page—Create backups every selected number of days.
- Create a Weekly Schedule on page 444—Create backups on certain days of the week.

Create an Hourly Schedule

1. From the menu bar, select **Configuration > Database Backup.** The Database Backup screen displays (see Figure 281 on page 446).
2. Select **Action > Change Schedule**. The Modify Database Backup Schedule screen displays.

3. Select **Hourly**. The Modify Database Backup Schedule screen changes to display the options for an hourly backup schedule.



Modify Database Backup Schedule

Minimum backups to keep on tape: 2

● Hourly
○ Daily
○ Weekly

Every 4 hours on minute 0

Figure 278 The Modify Database Backup Schedule screen.

4. 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.

5. Enter numbers for **Every _ hours on minute _**. These values specify the interval in hours between 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, the database is backed up every four hours at 15 minutes after the hour. The maximum setting for the **hours** field is 48, where the database is backed up every two days. The maximum setting for the **minute** field is 59.

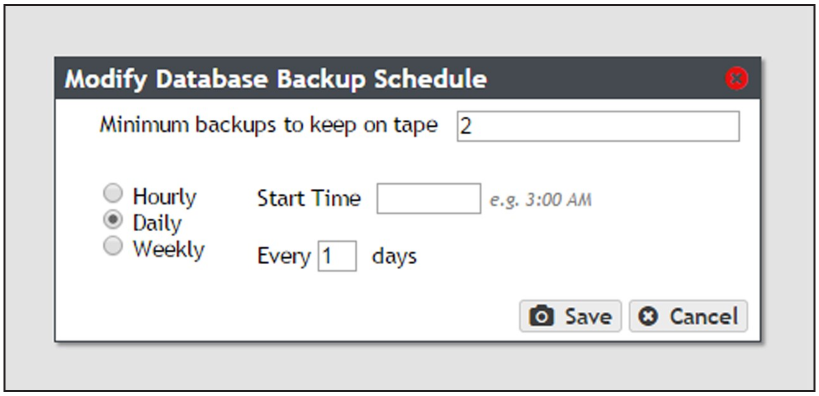
Note: Spectra Logic recommends offsetting the minutes after the hour for starting database backups so that there are not a large number of jobs starting at exactly the same time.

6. Click **Save**.

Create a Daily Schedule

1. From the menu bar, select **Configuration > Database Backup.** The Database Backup screen displays (see Figure 281 on page 446).
2. Select **Action > Change Schedule**. The Modify Database Backup Schedule screen displays.

3. Select **Daily**. The Modify Database Backup Schedule screen changes to display the options for a daily backup schedule.



Modify Database Backup Schedule

Minimum backups to keep on tape 2

○ Hourly
● Daily
○ Weekly

Start Time e.g. 3:00 AM

Every 1 days

Figure 279 The Modify Database Backup Schedule screen.

4. 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.

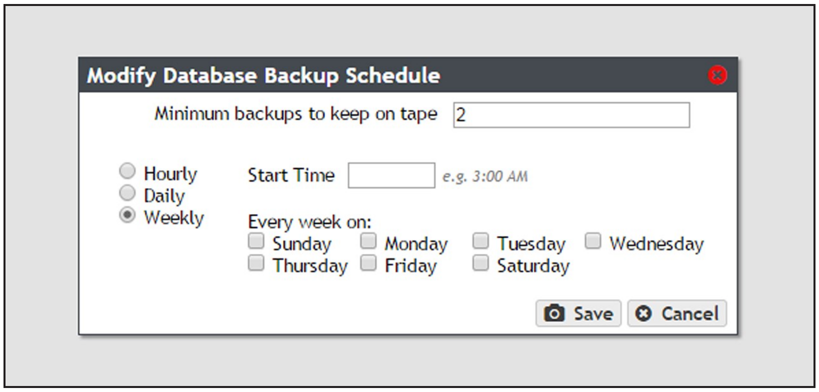
Note: Although the minimum number of backups is always respected, at some times there may be more than the minimum present on the gateway.

5. Enter a time value for **Start Time**, and include AM or PM after the value. this field is not case sensitive.
6. Enter a number for **Every_days**. This value specifies the interval, in days, between generating database backups. For example, if this value is set to 2, the gateway generates a backup every two days at the time specified in Step 5.
7. Click **Save**.

Create a Weekly Schedule

1. From the menu bar, select **Configuration > Database Backup.** The Database Backup screen displays (see Figure 281 on page 446).
2. Select **Action > Change Schedule**. The Modify Database Backup Schedule screen displays.

3. Select **Weekly**. The Modify Database Backup Schedule screen changes to display the options for a daily backup schedule.



Modify Database Backup Schedule

Minimum backups to keep on tape: 2

○ Hourly
○ Daily
● Weekly

Start Time: e.g. 3:00 AM

Every week on:
□ Sunday □ Monday □ Tuesday □ Wednesday
□ Thursday □ Friday □ Saturday

Figure 280 The Modify Database Backup Schedule screen.

4. 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.

5. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.

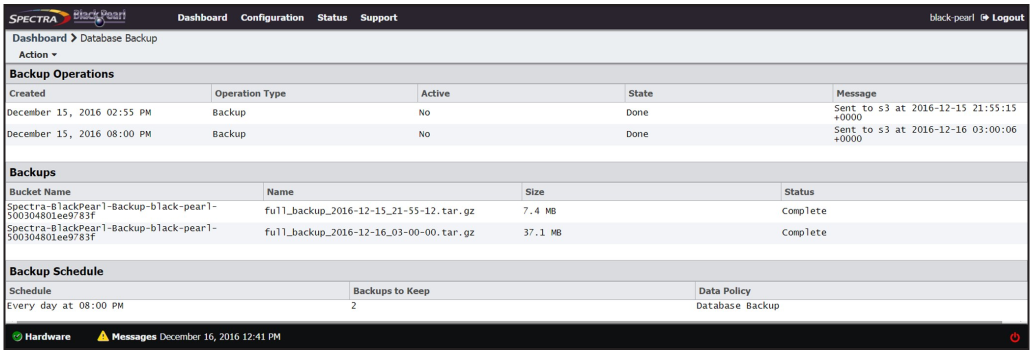
6. Select one or more days for **Every week on:**. This determines the day(s) of each week the gateway generates database backups.

7. Click **Save**.

Manually Generate a Database Backup

Use the instructions in this section to create a database backup manually.

1. From the menu bar, select **Configuration > Database Backup.** The Database Backup screen displays.



Backup Operations

Created	Operation Type	Active	State	Message
December 15, 2016 02:55 PM	Backup	No	Done	Sent to s3 at 2016-12-15 21:55:15 +0000
December 15, 2016 08:00 PM	Backup	No	Done	Sent to s3 at 2016-12-16 03:00:06 +0000

Backups

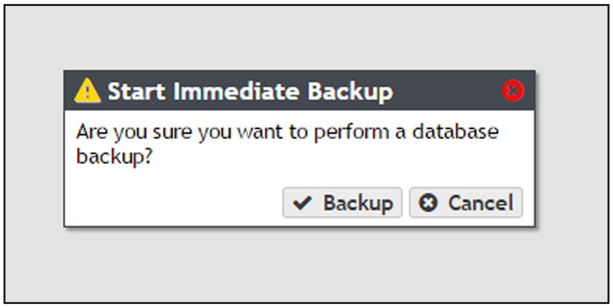
Bucket Name	Name	Size	Status
Spectra-BlackPearl-Backup-black-pearl-500304801ee9783f	full_backup_2016-12-15_21-55-12.tar.gz	7.4 MB	Complete
Spectra-BlackPearl-Backup-black-pearl-500304801ee9783f	full_backup_2016-12-16_03-00-00.tar.gz	37.1 MB	Complete

Backup Schedule

Schedule	Backups to Keep	Data Policy
Every day at 08:00 PM	2	Database Backup

Figure 281 The Database Backup screen.

2. Select **Action > Start Immediate Backup**. A confirmation window displays.


Start Immediate Backup

Are you sure you want to perform a database backup?

Figure 282 The Start Immediate Backup confirmation window.

3. Click **Backup**.

Restore from a Database Backup

Restoring a database backup returns the gateway to the state it was in when the backup was created. All objects written to the gateway after the backup was created are inaccessible.

CAUTION Restoring a database backup deletes all data changes made after the backup was created, and deletes any backups that were saved after the one you are using for the restore process. This action cannot be undone.

CAUTION Restoring a database backup deletes all data changes made after the backup was created, and deletes any backups that were saved after the one you are using for the restore process. This action cannot be undone.

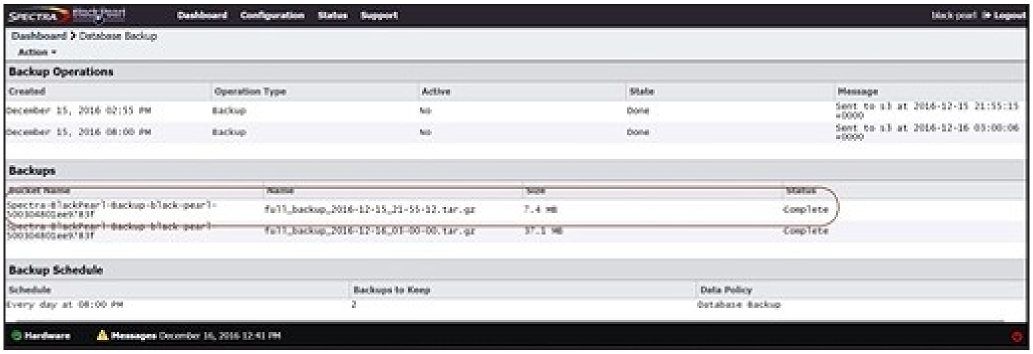
There are two ways to restore from a database backup; restoring from a manual or automatic database backup, or restoring from an arbitrary file. Restoring from an arbitrary file is useful if you have copied your database backup files to another bucket.

Note: If you are restoring using a database backup that resides on an 96-bay expansion node, after restoring the backup, when the gateway completes initialization, you must re-import the pool on the 96-bay expansion node containing the backup file used to restore the database.

Restore Using a Database Backup

Use the following instructions to restore a database backup.

1. From the menu bar, select **Configuration > Database Backup**. The Database Backup screen displays.



Backup Operations

Created	Operation Type	Active	State	Message
December 15, 2016 02:55 PM	Backup	No	Done	Sent to s3 at 2016-12-15 21:55:15 +0000
December 15, 2016 08:00 PM	Backup	No	Done	Sent to s3 at 2016-12-16 03:00:06 +0000

Backups

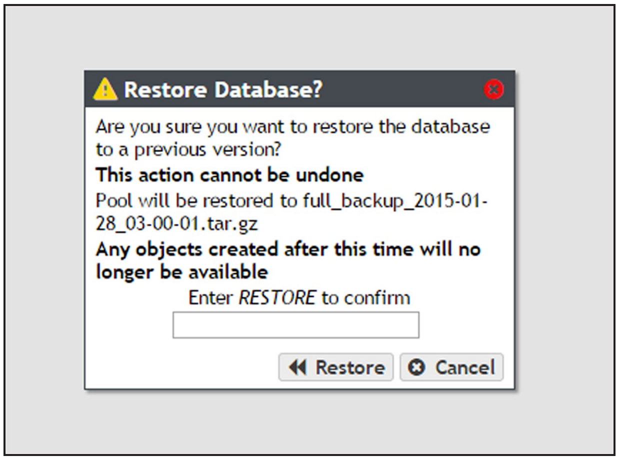
Bucket Name	Name	Size	Status
Spectra-BlackPearl-Backup-black-pearl-500304801ee9f83f	full_backup_2016-12-15_21-55-12.tar.gz	7.4 MB	Complete
Spectra-BlackPearl-Backup-black-pearl-500304801ee9f83f	full_backup_2016-12-16_03-00-00.tar.gz	37.1 MB	Complete

Backup Schedule

Schedule	Backups to Keep	Data Policy
Every day at 08:00 PM	2	Database Backup

Figure 283 The Database Backup screen.

2. Select the backup you want to restore in the Backups pane, and then select **Action > Restore from Backup**. A confirmation dialog box displays.



Are you sure you want to restore the database to a previous version?

This action cannot be undone

Pool will be restored to full_backup_2015-01-28_03-00-01.tar.gz

Any objects created after this time will no longer be available

Enter *RESTORE* to confirm

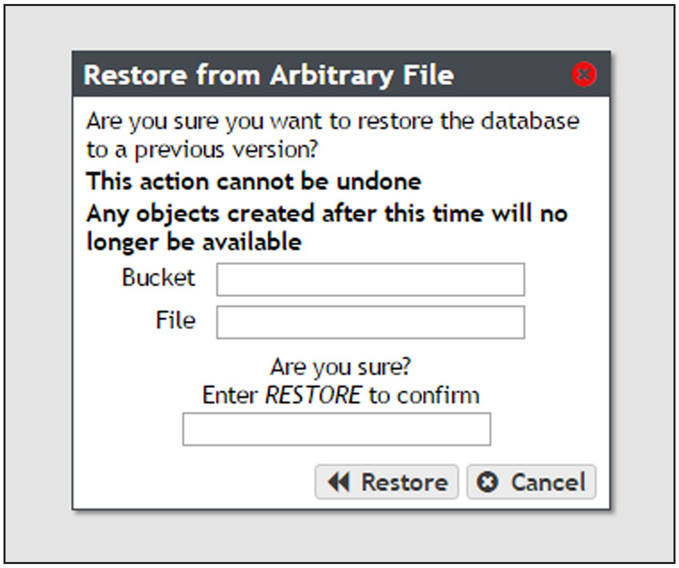
Figure 284 The Restore Database? confirmation dialog box.

3. Enter `RESTORE` in the entry field, and then click **Restore**. The database is restored to the state it was in when the backup was generated.

Restore Using an Arbitrary File

Use the instructions in this section to restore a database backup using an arbitrary file, such as a database backup that was copied to a different bucket than the one normally used for database backups.

1. From the menu bar, select **Configuration > Database Backup**. The Database Backup screen displays (see Figure 283 on page 447).
2. Select **Action > Restore from Arbitrary File**. A confirmation window displays.



Restore from Arbitrary File

Are you sure you want to restore the database to a previous version?

This action cannot be undone

Any objects created after this time will no longer be available

Bucket

File

Are you sure?
Enter *RESTORE* to confirm

Figure 285 The Restore from Arbitrary File confirmation dialog box.

3. Enter the name of the bucket containing the file in the **Bucket** field.
4. Enter the filename of the file in the **File** field.
5. Enter `RESTORE` in the entry field, and then click **Restore**. The database is restored to the state it was in when the backup was generated.

Delete Backup

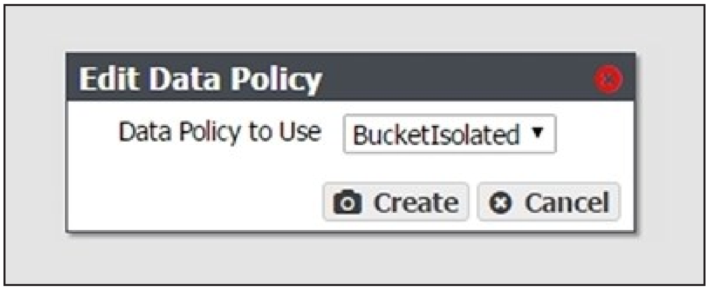
Use the following instructions to delete a database backup.

1. From the menu bar, select **Configuration > Database Backup.** The Database Backup screen displays (see Figure 283 on page 447).
2. Select the backup you want to delete in the Backups pane, and then select **Action > Delete**. A confirmation dialog box displays.
3. Enter `DELETE BACKUP` in the entry field and click **Delete**. The backup is deleted.

Edit Backup Data Policy

Use the following instructions to edit the data policy used for the database backup bucket.

1. From the menu bar, select **Configuration > Database Backup**. The Database Backup screen displays.
2. From the menu bar select **Action > Edit Data Policy**. The Edit Data Policy screen displays.



Data Policy to Use: BucketIsolated

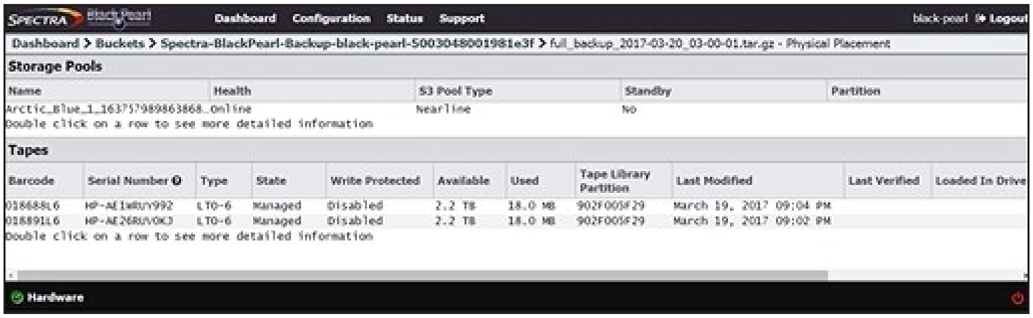
Figure 286 The Edit Data Policy screen.

3. Use the **Data Policy to Use** drop-down menu to select a new data policy for the database backup bucket.

Show Backup Physical Placement

Use the following instructions to display what piece(s) of tape media or what storage pool is used by a database backup.

1. From the menu bar, select **Configuration > Database Backup**. The Database Backup screen displays (see Figure 281 on page 446).
2. From the list of existing backups, select the backup for which you want to view physical placement and select **Action > Show Backup Physical Placement**. The screen refreshes to show you the storage pool or tape media the backup currently occupies.



Dashboard > Buckets > Spectra-BlackPearl-Backup-black-pearl-5003048001981e3f > full_backup_2017-03-20_03-00-01.tar.gz - Physical Placement

Storage Pools

Name	Health	S3 Pool Type	Standby	Partition
Arctic_Blue_1_1637579898638868	Online	Nearline	No	

Double click on a row to see more detailed information

Tapes

Barcode	Serial Number	Type	State	Write Protected	Available	Used	Tape Library Partition	Last Modified	Last Verified	Loaded In Drive
018688L6	HP-AE1WRUY992	LTO-6	Managed	Disabled	2.2 TB	18.0 MB	902F005F29	March 19, 2017 09:04 PM		
018891L6	HP-AE26RUVOKJ	LTO-6	Managed	Disabled	2.2 TB	18.0 MB	902F005F29	March 19, 2017 09:02 PM		

Double click on a row to see more detailed information

Figure 287 The Database Backup Physical Placement screen.

EXIT THE BLACKPEARL USER INTERFACE

To exit the BlackPearl user interface, close the browser or click **Logout** on the right side of the menu bar. This ends the session.

If the active session is idle for more than the set session timeout, the current user is automatically logged out. This setting can be configured on the Accounts screen. The default is 60 minutes. See Configure Users on page 323.

REBOOT OR SHUT DOWN A BLACKPEARL GATEWAY

This section discusses rebooting or shutting down a gateway.

Using the BlackPearl User Interface

Use the following instructions to reboot or shutdown a gateway using the BlackPearl user interface.

1. Click the power icon in the lower right-hand corner of any screen in the BlackPearl user interface. The Power screen displays.

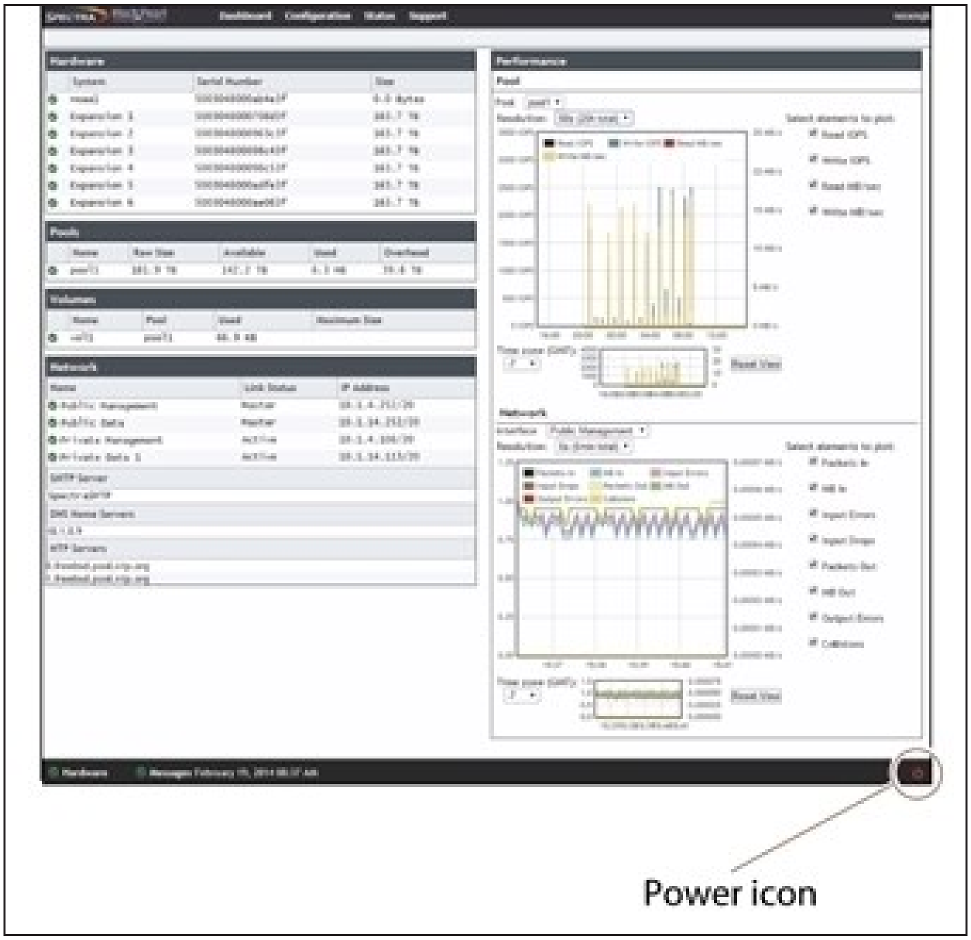


Figure 288 The Power icon.

2. Click either **Reboot** or **Shutdown**.
3. A confirmation screen appears. Confirm the selection to perform the reboot or shutdown.

Power-Cycle Reset

Under some circumstances, Spectra Logic Technical Support may direct you to perform a power-cycle reset of a BlackPearl gateway to recover from an error. To power-cycle reset a BlackPearl gateway, remove the front bezel, and then press and hold the front panel power button (Figure 21 on page 69) 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 BlackPearlgateway unless you are specifically instructed to do so by Spectra Logic Technical Support.

CAUTION Do not use the power button to turn off a BlackPearl gateway unless you are specifically instructed to do so by Spectra Logic Technical Support.

Chapter 11 - Using AutoSupport

This chapter describes using the BlackPearl user interface to configure the support features of the Spectra BlackPearl Nearline Gateway.

About AutoSupport 454

Enter Contact Information 454

Configure Mail Recipients 455

Create a New Mail Recipient 455

Edit a Mail Recipient 456

Send a Test Email 457

Delete a Mail Recipient 458

Log Sets 459

Configure a Log Set Schedule 459

Manually Generate Log Sets 460

Email a Log Set 461

Download a Log Set 462

Delete Log Sets 462

ABOUT AUTOSUPPORT

AutoSupport lets the BlackPearl 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.

ENTER CONTACT INFORMATION

Contact information helps Spectra Logic in contacting the administrator of the BlackPearl gateway during troubleshooting. Entering the contact information is typically a one-time-only process.

1. From the menu bar, select **Support > Contact Information** to display the Contact Information screen.
2. Click **New** in the Customer Contact Information pane. The New Contact Information dialog box displays.

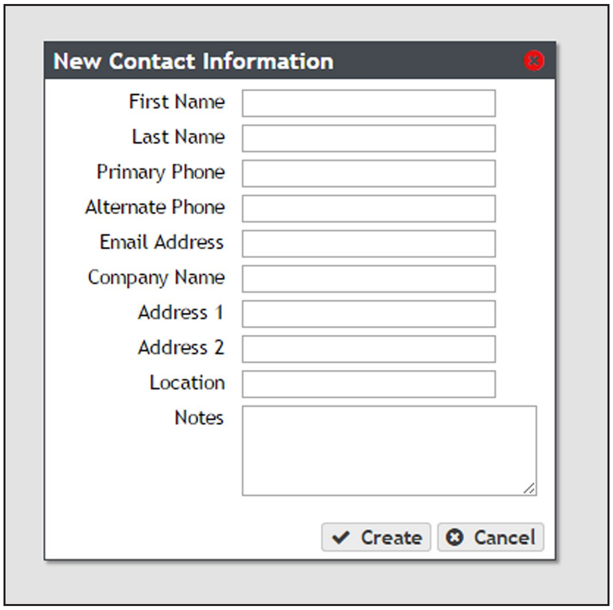
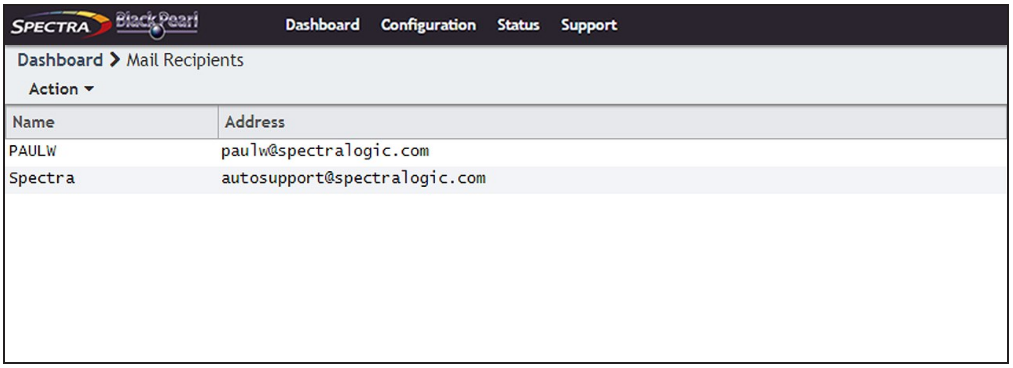


Figure 289 The New Contact Information dialog box.

3. Enter the requested information and click **Create**.

Configure 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.

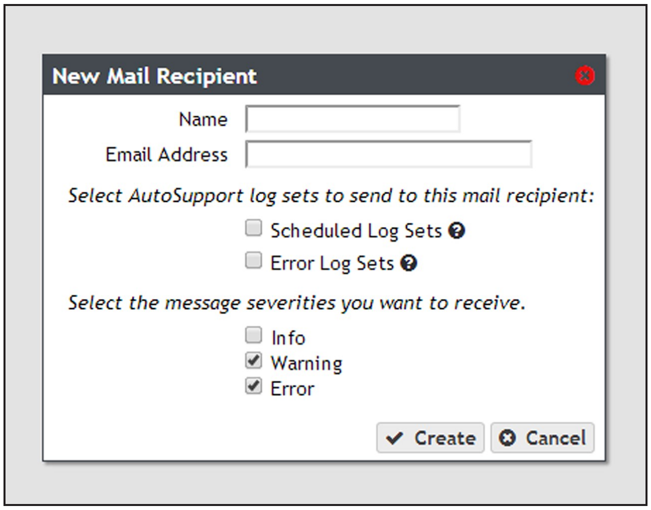


Name	Address
PAULW	paulw@spectralogic.com
Spectra	autosupport@spectralogic.com

Figure 290 The Mail Recipients screen.

Create a New Mail Recipient

1. From the menu bar, select **Configuration > Mail Recipients**. The Mail Recipients screen displays.
2. Select **Action > 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

Figure 291 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 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 Nearline 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.

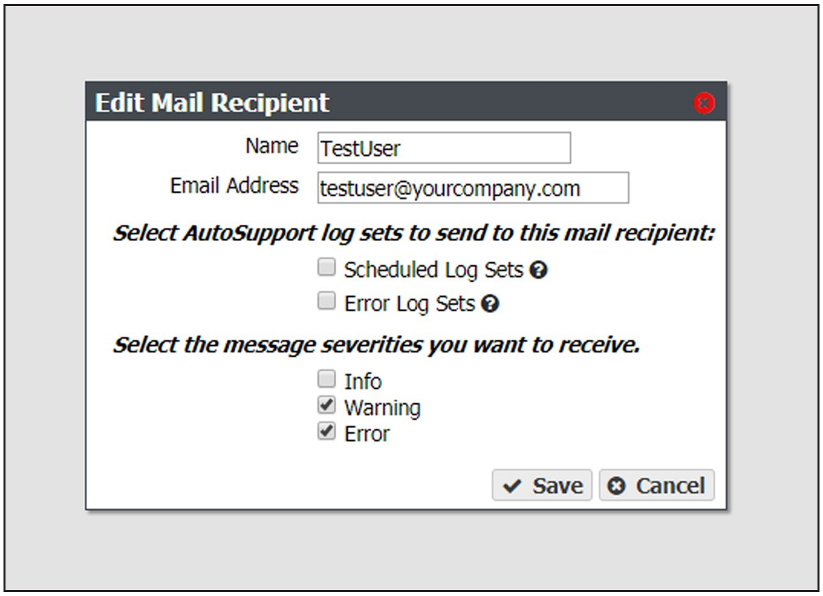
4. Click **Create** to save the information. The Mail Recipients screen re-displays with the new mail recipient added to the list of mail recipients.
5. Repeat Step 1 on page 455 through Step 4 to configure additional mail recipients.

Edit a Mail Recipient

Use the following steps to edit a mail recipient account.

1. From the menu bar, select **Configuration > Mail Recipients**. The Mail Recipients screen displays with any already configured mail recipients listed (see Figure 290 on page 455).

2. From the list of mail recipients, double-click the name of the recipient whose information you want to edit, or select the name and then select **Action > Edit**. The Edit Mail Recipient dialog box displays.



Edit Mail Recipient

Name: TestUser

Email Address: testuser@yourcompany.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

Figure 292 Edit the information for the selected mail recipient.

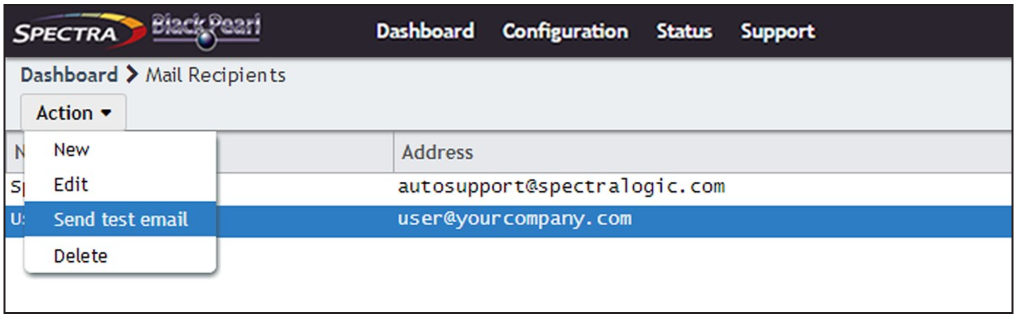
3. Change the information for the recipient as required and then click **Save**. See Step 3 on page 456 for a description of each setting.

Send a Test Email

Use the following steps to send a test email to a mail recipient.

1. From the menu bar, select **Configuration > Mail Recipients**. The Mail Recipients screen displays with any already configured mail recipients listed (see Figure 290 on page 455).

2. From the list of mail recipients, select the name of the recipient you want to receive a test email, and then select **Action > Send test email**.



N	Address
S	autosupport@spectralogic.com
U:	user@yourcompany.com

Figure 293 The Mail Recipients screen.

The BlackPearl gateway immediately sends a test email to the selected account.

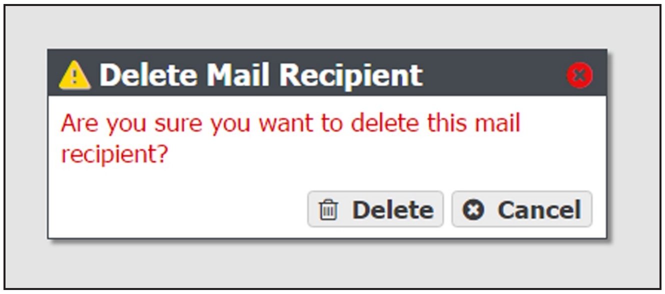
3. Verify the user received the email from the BlackPearl gateway. If the email is not received, verify that you entered the SMTP server settings correctly (see Configure SMTP Settings on page 288).

Delete a Mail Recipient

Use the following steps to delete a mail recipient account.

1. From the menu bar, select **Configuration > Mail Recipients** to display the Mail Recipients screen with any already configured mail recipients listed (see Figure 290 on page 455).
2. From the list of mail recipients, select the name of the recipient whose account you want to delete and then select **Action > Delete**. A dialog box displays asking you to confirm the deletion of the mail recipient.

Note: The default **Spectra** mail recipient cannot be deleted.



Are you sure you want to delete this mail recipient?

Figure 294 Delete the selected mail recipient.

3. Click **Delete** to confirm the deletion.

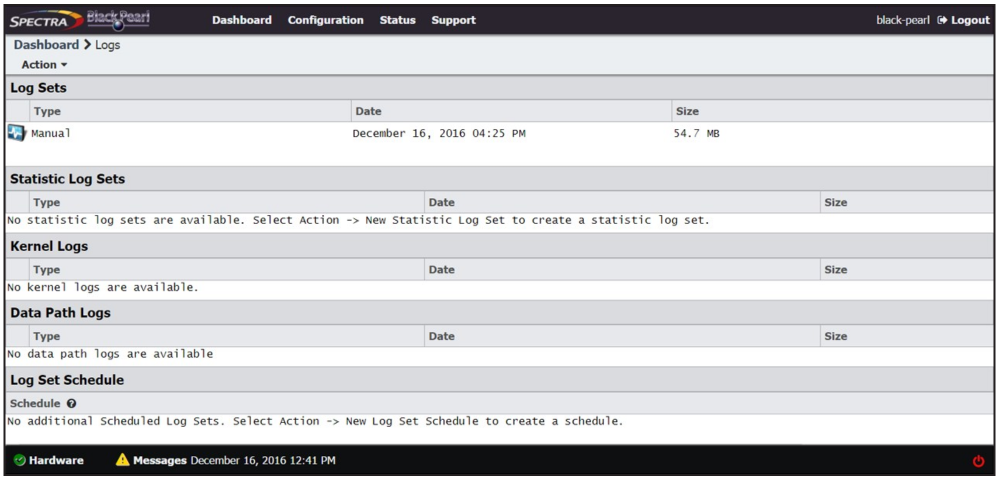
Log Sets

The BlackPearl gateway automatically generates log sets when errors occur. Log sets can also be generated manually, or generated on a schedule. The gateway generates three types of log sets:

- **Log Sets** contain information about the configuration and status of the BlackPearl 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.
- **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 Drive Diagnostic Logs on page 506.



Log Sets

Type	Date	Size
Manual	December 16, 2016 04:25 PM	54.7 MB

Statistic Log Sets

Type	Date	Size

```
No statistic log sets are available. Select Action -> New Statistic Log Set to create a statistic log set.
```

Kernel Logs

Type	Date	Size

```
No kernel logs are available.
```

Data Path Logs

Type	Date	Size

```
No data path logs are available
```

Log Set Schedule

Schedule

```
No additional Scheduled Log Sets. Select Action -> New Log Set Schedule to create a schedule.
```

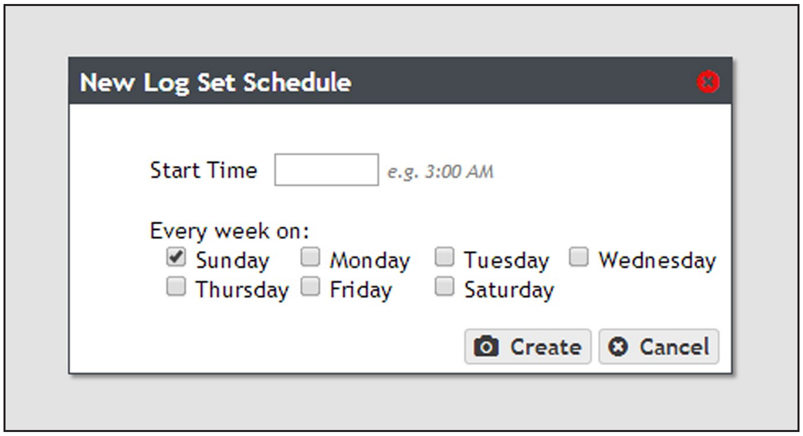
Figure 295 The Logs screen.

Configure a Log Set Schedule

Use the instructions in this section to configure a log set schedule.

1. From the menu bar, select **Support > Logs.** The Logs screen displays (see Figure 295).

2. Select **Action > New Log Set Schedule**. The New Log Set Schedule dialog box displays.



Start Time e.g. 3:00 AM

Every week on:
☑ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday
☐ Thursday ☐ Friday ☐ Saturday

Figure 296 The New Log Set Schedule dialog box.

3. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.

4. Select one or more days for **Every week on:**. This determines the day(s) of the week the gateway generates log sets.

5. Click **Create**. The Logs screen displays showing the newly created Log Set Schedule.

Manually Generate Log Sets

Although the BlackPearl 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. From the menu bar, select **Support > Logs**. The Logs screen displays.

2. Create the desired log set:

- Select **Action > New Log Set** to generate a log set for use in general troubleshooting.

  —OR—

- Select **Action > New Statistic Log Set** to generate a log set used for in-depth troubleshooting. This log is not human readable. To see performance statistics in a human readable form, see View Performance Metrics on page 438.

  —OR—

- Select **Action > New Data Path Log** to generate a log set used for troubleshooting the data communication path to the gateway and its associated tape library. The New Data Path Log dialog box displays.

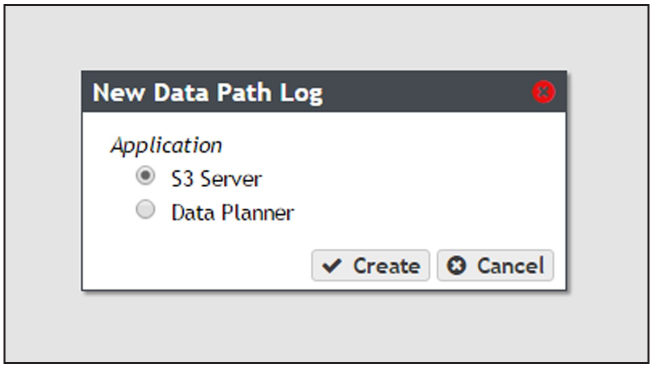


Figure 297 The New Data Path Log dialog box.

3. If you are generating a data path log, select the **Application** for which you want to generate a log set. Otherwise continue to Step 4.

Application	Description
S3 Server	The 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.

4. Click **Create**.
5. Continue with Email a Log Set below or Download a Log Set on the next page.

Email a Log Set

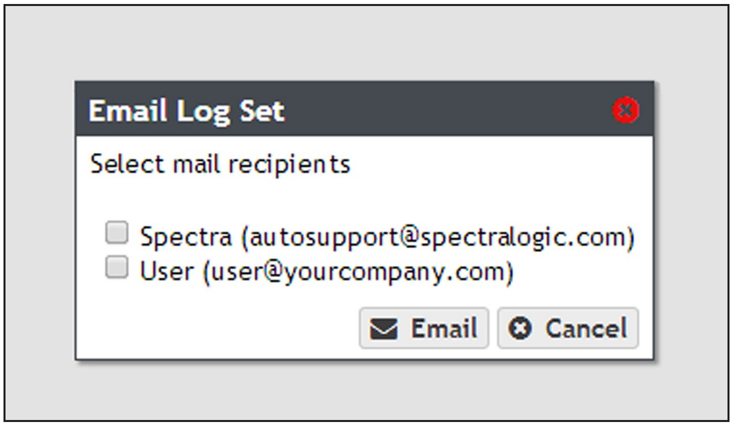
Use the instructions in this section to email a log set.

Note: You must configure the SMTP settings on the gateway before you can send emails. See Configure SMTP Settings on page 288 to configure the SMTP settings.

1. From the menu bar, select **Support > Logs.** The Logs screen displays (see Figure 295 on page 459).

2. Select the log set you want to email, and then select **Action > Email**. The Email Log Set dialog box displays.

Note: Statistic Log Sets are too large to be emailed from the gateway, and must be downloaded. See Download a Log Set, below.



Email Log Set

Select mail recipients

□ Spectra (autosupport@spectralogic.com)
□ User (user@yourcompany.com)

Figure 298 The Email Log Set dialog box.

3. Select the mail recipients you want to receive the log set, and click **Email**.

Download a Log Set

Use the instructions in this section to download a log set.

1. From the menu bar, select **Support > Logs.** The Logs screen displays (see Figure 295 on page 459).
2. Select the log set you want to download, and then select **Action > Download**. The log set begins downloading to your host computer.

Delete Log Sets

Use the instructions in this section to delete a log set.

1. From the menu bar, select **Support > Logs**. The Logs screen displays (see Figure 295 on page 459).
2. Select the log set you want to delete, and then select **Action > Delete**. A confirmation window displays asking you to confirm the action.
3. Click **Delete** to remove the log set.
4. Optionally, use one of the following to delete multiple log sets:

Command	Description
Action > Delete All Log Sets	Deletes all log sets present on the gateway.

Command	Description
Action > Delete All Statistic Log Sets	Deletes all statistic log sets on the gateway.
Action > Delete All Kernel Logs	Deletes all kernel log sets on the gateway.
Action > Delete All Data Path Logs	Deletes all data path log sets on the gateway.

CHAPTER 12 - MAINTAINING THE BLACKPEARL NEARLINE GATEWAY

This chapter describes the maintenance procedures for the Spectra BlackPearl Nearline Gateway.

Data Integrity Verification - Disk Media 465

Cancel Data Integrity Verification 466

Data Integrity Verification - Tape Media 467

Cancel Tape Media Verification 468

Initiate RSC Backup 469

Access the Technical Support Portal 470

Create an Account 470

Log Into the Portal 471

Configure Automated Software Upload 472

Update the Software 474

Considerations for Updating to BlackPearl OS 5.4 475

Check the Current Software Version 475

Check the Currently Released Software Version 477

Download and Stage the Updated Software 478

Install the Update 479

Installing Data Drives 481

Ensure ESD Protection 481

Install a Drive in a Gen2 S Series Chassis 482

Install a Drive in a Gen2 V Series Chassis 483

Install a Drive in a Gen2 X Series Chassis 484

Install a Drive in a Gen1 Chassis 486

Replace a Failed Component 489

Identify the Failed Component 489

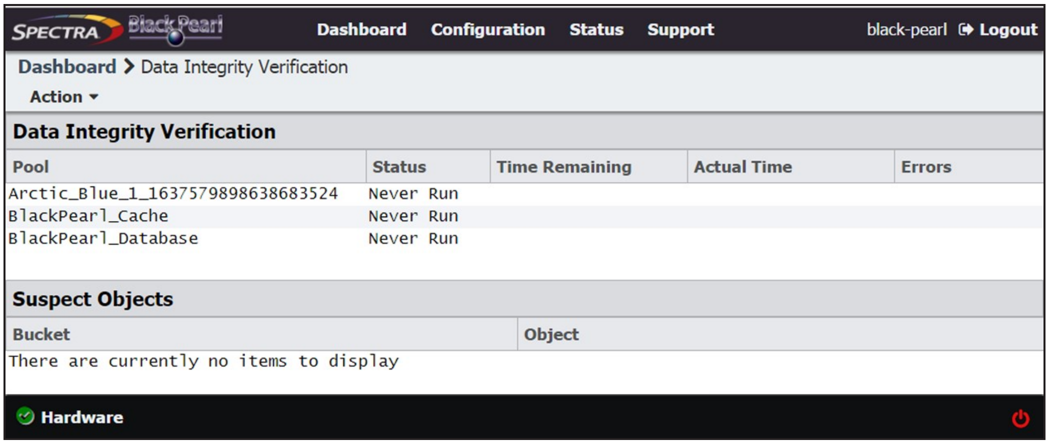
DATA INTEGRITY VERIFICATION - DISK MEDIA

The BlackPearl 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.

Use the instructions in this section to perform a data integrity verification on a disk pool.

1. From the menu bar, select **Support > Tools > Data Integrity Verification.** The Data Integrity Verification screen displays.



Data Integrity Verification

Pool	Status	Time Remaining	Actual Time	Errors
Arctic_Blue_1_1637579898638683524	Never Run			
BlackPearl_Cache	Never Run			
BlackPearl_Database	Never Run			

Suspect Objects

Bucket	Object
There are currently no items to display	

Figure 299 The Data Integrity Verification screen.

2. Select the disk pool for which you want to start the data integrity verification, and select **Action > 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. delete and then reimport the object, The affected files cannot be retrieved from the storage pool, and may need to be transferred to the BlackPearlgateway 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.

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. delete and then reimport the object, The affected files cannot be retrieved from the storage pool, and may need to be transferred to the BlackPearl 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 Data Integrity Verification

If desired, you can stop a data integrity verification while it is in progress.

1. From the menu bar, select **Support > Tools > Data Integrity Verification.** The Data Integrity Verification screen displays.
2. Select the pool for which you want to stop verification in the Data Integrity Verification screen, and then select **Action > Cancel**.
3. A confirmation screen displays. Click **OK** to stop the verification.

DATA INTEGRITY VERIFICATION - TAPE MEDIA

The BlackPearl gateway automatically performs data integrity verification for any tape cartridge that is unchanged for the number of days specified in a given storage domain. See Create a Storage Domain on page 150 for more information.

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 gateway and store off-site.

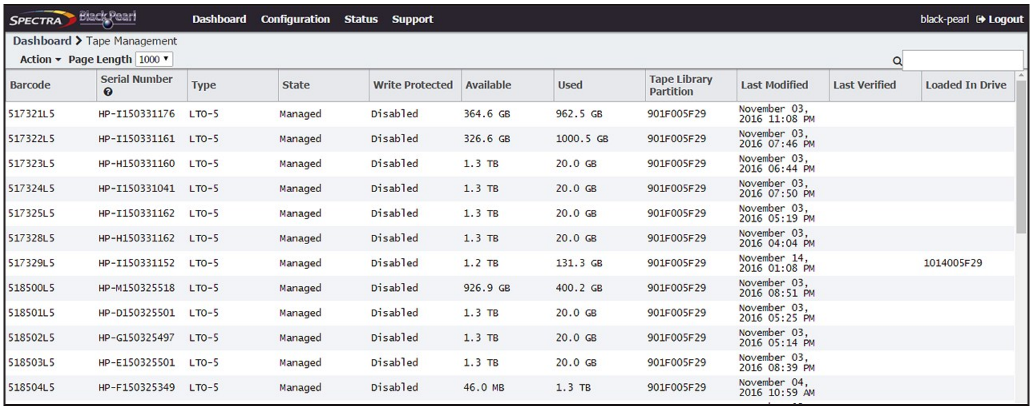
You can configure the gateway to verify the entire tape, or a specified percentage of the total reported capacity of the tape cartridge. If you specify a percentage, the gateway starts the scan the specified percentage of the tape capacity before the EOD (End of Data) marker and ends the scan at the EOD marker. This is useful when you only want to validate the most recent data written to the tape. See Configure the DS3 Service on page 292 for more information.

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.

Use the instruction in this section to verify data on tape media.

1. From the menu bar, select **Status > Tape Management.** The Tape Management screen displays.



Barcode	Serial Number	Type	State	Write Protected	Available	Used	Tape Library Partition	Last Modified	Last Verified	Loaded In Drive
517321L5	HP-I150331176	LTO-5	Managed	Disabled	364.6 GB	962.5 GB	901F005F29	November 03, 2016 11:08 PM		
517322L5	HP-I150331161	LTO-5	Managed	Disabled	326.6 GB	1000.5 GB	901F005F29	November 03, 2016 07:46 PM		
517323L5	HP-H150331160	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 06:44 PM		
517324L5	HP-I150331041	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 07:50 PM		
517325L5	HP-I150331162	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 05:19 PM		
517328L5	HP-H150331162	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 04:04 PM		
517329L5	HP-I150331152	LTO-5	Managed	Disabled	1.2 TB	131.3 GB	901F005F29	November 14, 2016 01:08 PM		1014005F29
518500L5	HP-M150325518	LTO-5	Managed	Disabled	926.9 GB	400.2 GB	901F005F29	November 03, 2016 08:51 PM		
518501L5	HP-D150325501	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 05:25 PM		
518502L5	HP-G150325497	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 05:14 PM		
518503L5	HP-E150325501	LTO-5	Managed	Disabled	1.3 TB	20.0 GB	901F005F29	November 03, 2016 08:39 PM		
518504L5	HP-F150325349	LTO-5	Managed	Disabled	46.0 MB	1.3 TB	901F005F29	November 04, 2016 10:59 AM		

Figure 300 The Tape Management screen.

2. To verify data on an individual tape, select the tape in the Tape Management screen, and then select **Action > Verify Tape**. To verify data on all tapes in the tape library, select **Action > Verify All Tapes.**

Note: The time required to **Verify All Tapes** varies based on the number of tapes in the library. Large libraries can take a very long time to complete the verification.

A confirmation window displays. 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 9) 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 BlackPearlgateway 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.

CAUTION In the event that the data integrity verification fails, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 9) 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 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 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.

1. From the menu bar, select **Support > Tools > Data Integrity Verification.** The Data Integrity Verification screen displays.
2. 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.**

3. 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 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 gateway, Spectra Logic recommends that you backup the configuration manually.

Use the instructions in this section to manually backup the replicated system configuration.

1. From the menu bar, select **Support > Tools > Data Integrity Verification.** The Data Integrity Verification screen displays (see Figure 299 on page 465).
2. Select **Action > Initiate RSC Backup.** A confirmation screen displays.
3. Click **Initiate RSC Backup** to manually backup the current gateway configuration.

ACCESS THE TECHNICAL SUPPORT PORTAL

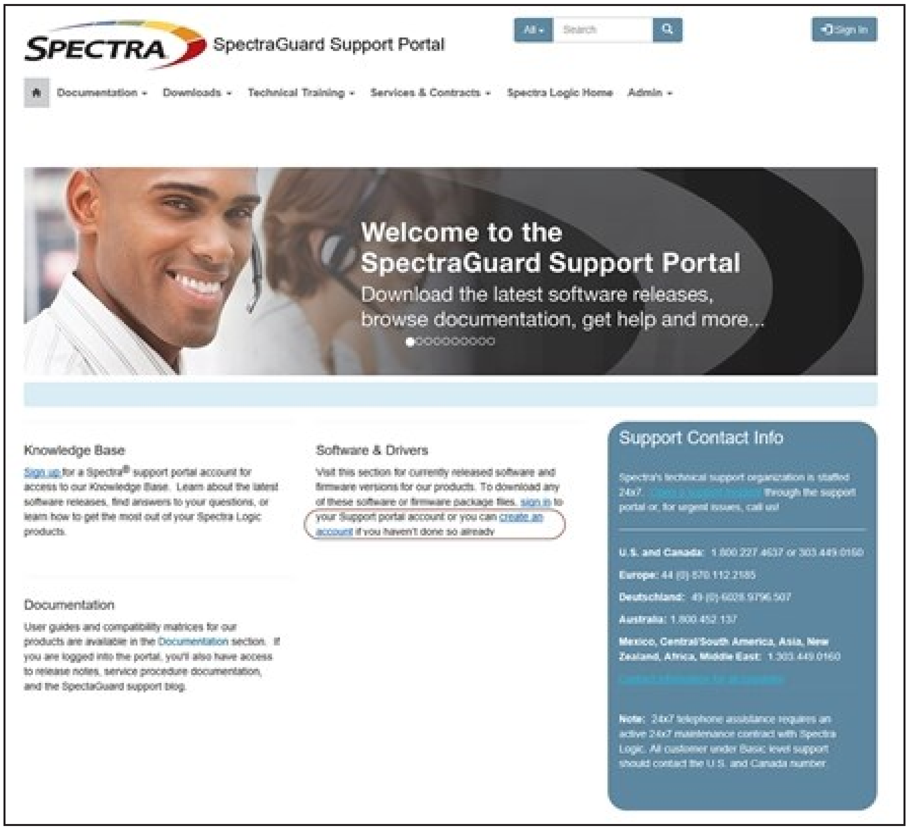
The Spectra Logic Technical Support portal provides access to the Knowledge Base, the current version of BlackPearl software for the gateway, and additional service and support tools. You can also open or update a support incident and upload log files.

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 9).

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. 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

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

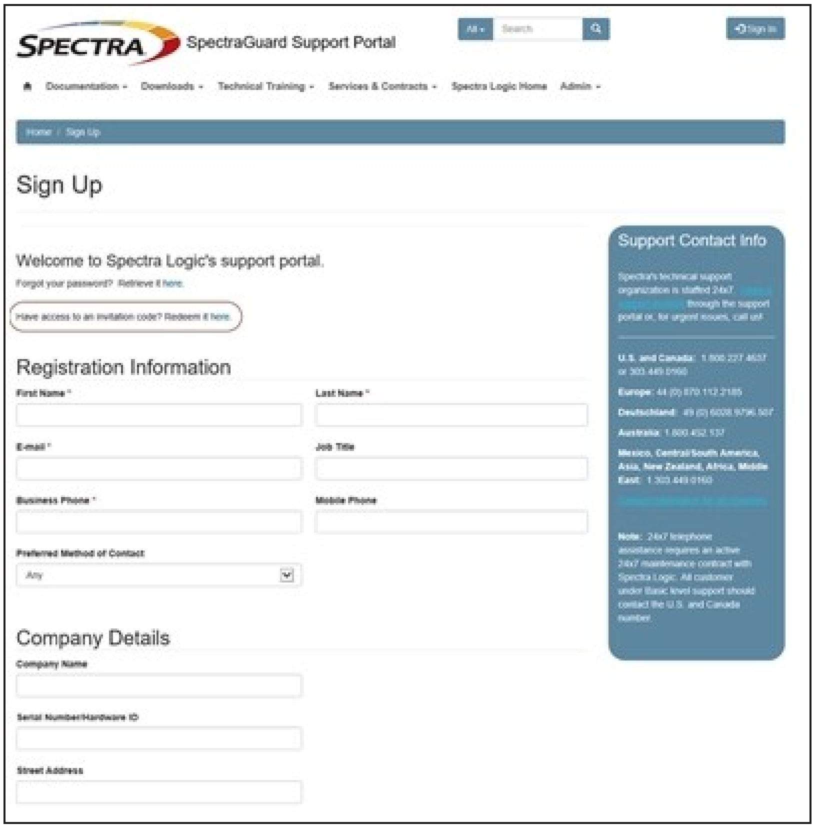
Contact information for all countries

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 301 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

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 302 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.

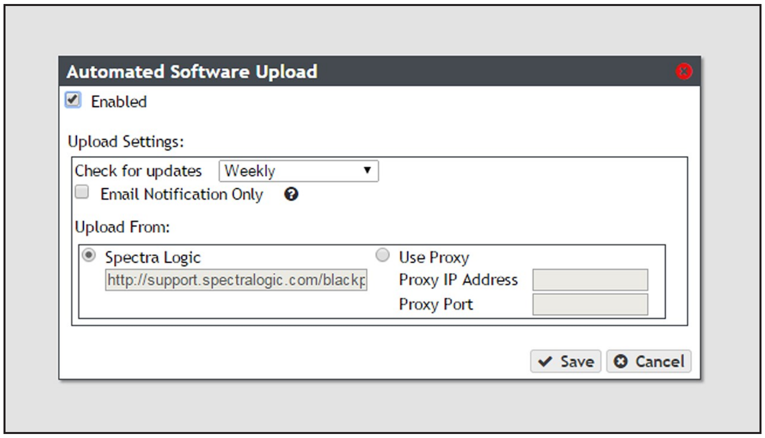
Configure Automated Software Upload

Automated Software Upload is a feature that allows the gateway to periodically check a specified server to determine if updated software is available for the gateway. The feature can also be used to automatically download the updated software package to the gateway.

Note: You must have a current software update key entered in the gateway you want to configure to use Automated Software Upload. See Manually Enter Activation Keys on page 338 for more information.

Use the instructions in this section to configure Automated Software Upload.

1. From the menu bar, select **Support > Software.** The Software screen displays.
2. Select **Action > Edit Automated Software Upload**. The Automated Software Upload dialog box displays.



Automated Software Upload

☑ Enabled

Upload Settings:

Check for updates: Weekly

□ Email Notification Only

Upload From:

● Spectra Logic: http://support.spectralogic.com/blackp

○ Use Proxy

Proxy IP Address:

Proxy Port:

Figure 303 The Automated Software Upload dialog box.

3. Select the **Enabled** check box to enable the feature.
4. Use the drop-down menu to select the **Check for updates** frequency.
5. Optionally, select the **Email Notifications Only** check box to only receive an email when an updated software package is available instead of automatically download the file.
6. Select either **Spectra Logic** or **Use Proxy** as the **Upload From** location.

IMPORTANT Spectra Logic recommends using the **Spectra Logic** package server.

IMPORTANT Spectra Logic recommends using the **Spectra Logic** package server.

If you select **Use Proxy**, enter the following information:

- **Proxy IP Address**—Enter a valid IPv4 address.
- **Proxy Port**—Enter the port used to access the proxy server.

7. Click **Save**.

UPDATE THE SOFTWARE

Some problems with the BlackPearl gateway may be fixed by updating the gateway's software. Spectra Logic provides complete support for the most current release of software and one revision back. Customers using previously released software packages are asked to update to the current release as soon as possible.

Note: You must have a current software update key entered in the gateway you want to update. See Manually Enter Activation Keys on page 338 for more information.

If Automated Software Upload is enabled, the gateway sends an email to all users configured to receive Warning or Informational emails (see Configure Mail Recipients on page 455) and posts a system message to the Messages screen. If configured to do so, the gateway also downloads the updated software.

The method used to update the gateway depends on if the Automated Software Upload feature is enabled or not, and if enabled, whether it is configured to download the updated software.

- If the update package downloaded automatically, skip to Install the Update on page 479.
- If you were notified that an update is required, but the update did not download automatically, skip to Download and Stage the Updated Software on page 478.
- If you do not know if the gateway needs an update installed, continue with Check the Current Software Version below.

Considerations for Updating to BlackPearl OS 5.4

If your BlackPearl Nearline gateway includes a tape library, please read the below before upgrading to BlackPearl OS 5.4.x or later.

Note: Once you have upgraded to BlackPearl OS 5.4.x or later, the below issue no longer occurs.

The BlackPearl system now enumerates the ports in Fibre Channel HBAs to resolve certain issues. As a result of this, the second byte of the WWPN for the BlackPearl Fibre Channel HBAs increments by 1.

For example, if a current HBA WWPN is

WPN 50:00:e1:11:c8:10:e0:b6, it would change to

WPN 51:00:e1:11:c8:10:e0:b6

IMPORTANT When upgrading to OS 5.4.x or later, if you connect to a tape library through a fabric switch which has zoning configured to use WWPNs, make sure to update the switch zoning configuration to include the updated HBA WWPNs. This zoning configuration update must be done prior to upgrading the BlackPearl system to avoid a forced full tape inspection of all tape media.

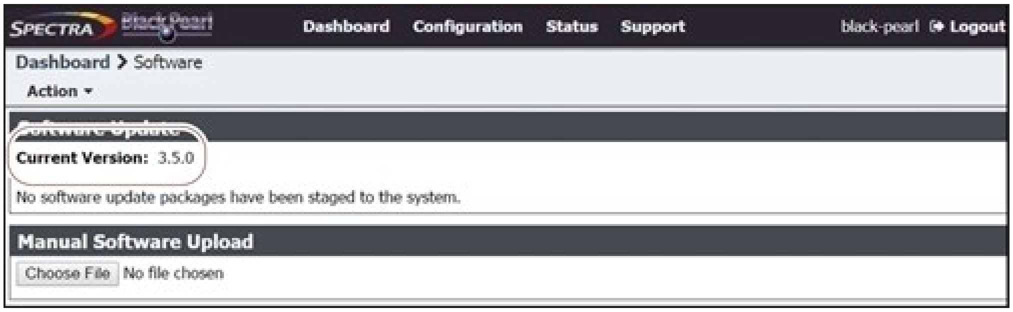
IMPORTANT When upgrading to OS 5.4.x or later, if you connect to a tape library through a fabric switch which has zoning configured to use WWPNs, make sure to update the switch zoning configuration to include the updated HBA WWPNs. This zoning configuration update must be done prior to upgrading the BlackPearl system to avoid a forced full tape inspection of all tape media.

Prior to upgrading, on your fabric switch, change the WWPN for each HBA port to the WWPN currently used by the drives and tape library.

Check the Current Software Version

Use the following steps to determine the current software version running on your BlackPearl gateway.

1. From the menu bar, select **Support > Software.** The Software screen displays.
2. The current software version is listed next to **Current Version** in the Software Update pane.



Current Version: 3.5.0

No software update packages have been staged to the system.

No file chosen

Figure 304 The current BlackPearl software version.

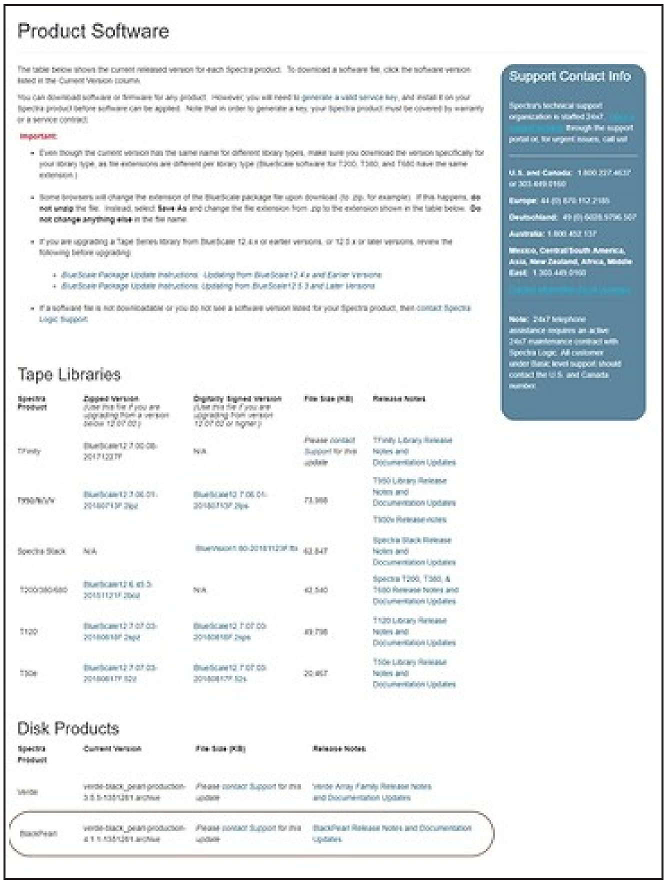
Check the Currently Released Software Version

Follow these steps to check the currently recommended BlackPearl software version:

1. Log into your user account on the Technical Support portal at *support.spectralogic.com*.

Note: See Create an Account on page 470 for information about creating an account and accessing the Technical Support portal.

2. Select **Downloads > Product Software**.
3. On the Product Software page, locate the BlackPearl gateway in the **Spectra Product** column. The currently released BlackPearl software version is listed in the **Current Version** column.



Product Software

The table below shows the current released version for each Spectra product. To download a software file, click the software version listed in the Current Version column.

You can download software or firmware for any product. However, you will need to generate a valid service key, and install it on your Spectra product before software can be applied. Note that in order to generate a key, your Spectra product must be covered by warranty or a service contract.

Important:

- Even though the current version has the same name for different library types, make sure you download the version specifically for your library type, as the extensions are different per library type (BlueScale software for T200, T380, and T680 have the same extension.)
- Some browsers will change the extension of the BlueScale package file upon download (to .zip, for example). If this happens, **do not unzip** the file. Instead, select **Save As** and change the file extension from .zip to the extension shown in the table below. **Do not change anything else** in the file name.
- If you are upgrading a Tape Series library from BlueScale 12.4.x or earlier versions, or 12.5.x or later versions, review the following before upgrading:
  - *BlueScale Package Update Instructions: Updating from BlueScale12.4.x and Earlier Versions*
  - *BlueScale Package Update Instructions: Updating from BlueScale12.5.3 and Later Versions*
- If a software file is not downloadable or you do not see a software version listed for your Spectra product, then contact Spectra Logic Support.

Tape Libraries

Spectra Product	Zipped Version *(Use this file if you are upgrading from a version below 12.07.00.)*	Digitally Signed Version *(Use this file if you are upgrading from version 12.07.00 or higher.)*	File Size (KB)	Release Notes
TFinity	BlueScale12.7.00.08-20171227F	N/A	Please contact Support for this update	TFinity Library Release Notes and Documentation Updates
T950/N/V	BlueScale12.7.06.01-20180713F.2bz	BlueScale12.7.06.01-20180713F.2bs	73,988	T950 Library Release Notes and Documentation Updates T950v Release notes
Spectra Stack	N/A	BlueVision1.80-20181123F.fls	62,847	Spectra Stack Release Notes and Documentation Updates
T200/380/680	BlueScale12.6.45.3-20151121F.2bz2	N/A	42,540	Spectra T200, T380, & T680 Release Notes and Documentation Updates
T120	BlueScale12.7.07.03-20180618F.2apz	BlueScale12.7.07.03-20180618F.2aps	49,798	T120 Library Release Notes and Documentation Updates
T50e	BlueScale12.7.07.03-20180617F.52z	BlueScale12.7.07.03-20180617F.52s	20,857	T50e Library Release Notes and Documentation Updates

Disk Products

Spectra Product	Current Version	File Size (KB)	Release Notes
Verde	verde-black_pearl-production-3.5.5-1351281.archive	Please contact Support for this update	Verde Array Family Release Notes and Documentation Updates
BlackPearl	verde-black_pearl-production-4.1.1-1351281.archive	Please contact Support for this update	BlackPearl Release Notes and Documentation Updates

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: 1.800.492.137

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 customers under Basic level support should contact the U.S. and Canada number.

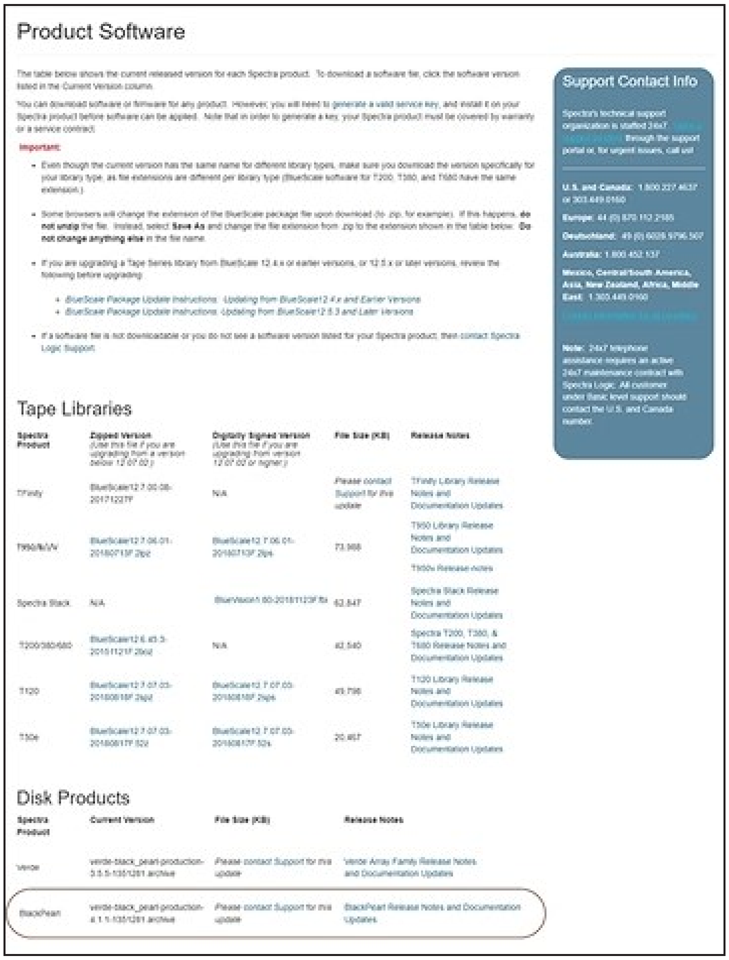
Figure 305 The Product Software screen.

4. Compare the Current Version available for the BlackPearl gateway to the version installed on the gateway.

Download and Stage the Updated Software

Use the instructions in this section to download and stage the updated software for the BlackPearl gateway.

1. Log into your account on the Technical Support portal at *support.spectralogic.com*.
2. Select **Downloads > Product Software**. The Product Software Screen displays.



Product Software

The table below shows the current released version for each Spectra product. To download a software file, click the software version listed in the Current Version column.

You can download software or firmware for any product. However, you will need to generate a valid service key, and install it on your Spectra product before software can be applied. Note that in order to generate a key, your Spectra product must be covered by warranty or a service contract.

Important:

- Even though the current version has the same name for different library types, make sure you download the version specifically for your library type, as file extensions are different per library type (BlueScale software for T200, T380, and T680 have the same extension.)
- Some browsers will change the extension of the BlueScale package file upon download (to .zip, for example). If this happens, **do not unzip** the file. Instead, select **Save As** and change the file extension from .zip to the extension shown in the table below. **Do not change anything else** in the file name.
- If you are upgrading a Tape Series library from BlueScale 12.4.x or earlier versions, or 12.5.x or later versions, review the following before upgrading:
  - *BlueScale Package Update Instructions: Updating from BlueScale12.4.x and Earlier Versions*
  - *BlueScale Package Update Instructions: Updating from BlueScale12.5.3 and Later Versions*
- If a software file is not downloadable or you do not see a software version listed for your Spectra product, then contact Spectra Logic Support.

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.

Tape Libraries

Spectra Product	Zipped Version (Use this file if you are upgrading from a version below 12.07.02.)	Digitally Signed Version (Use this file if you are upgrading from version 12.07.02 or higher.)	File Size (KB)	Release Notes
TFinity	BlueScale12.7.00.08-20171227F	N/A	Please contact Support for the update	TFinity Library Release Notes and Documentation Updates
T950/N/V	BlueScale12.7.06.01-20180713F.2ipz	BlueScale12.7.06.01-20180713F.2ips	73,988	T950 Library Release Notes and Documentation Updates T950v Release notes
Spectra Stack	N/A	BlueVision1.00-20181123F.tis	62,847	Spectra Stack Release Notes and Documentation Updates
T200/380/680	BlueScale12.6.45.3-20151121F.2bxz	N/A	42,540	Spectra T200, T380, & T680 Release Notes and Documentation Updates
T120	BlueScale12.7.07.03-20180816F.2spz	BlueScale12.7.07.03-20180816F.2sps	45,798	T120 Library Release Notes and Documentation Updates
T50e	BlueScale12.7.07.03-20180817F.52z	BlueScale12.7.07.03-20180817F.52s	20,467	T50e Library Release Notes and Documentation Updates

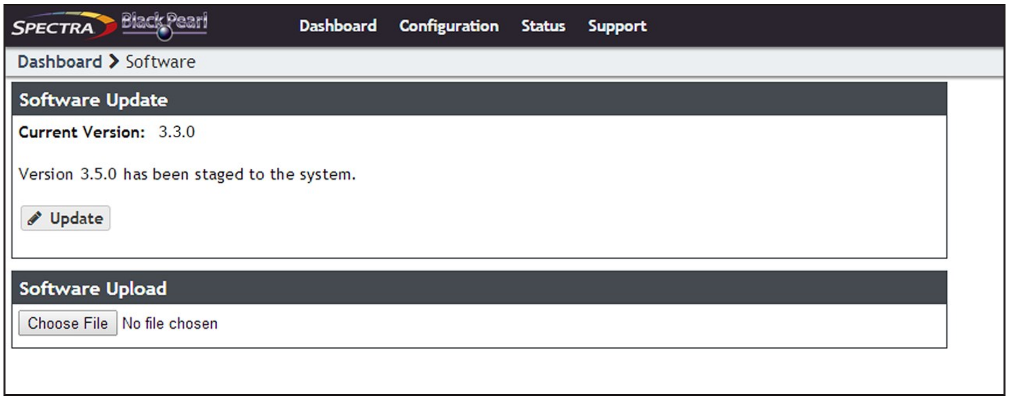
Disk Products

Spectra Product	Current Version	File Size (KB)	Release Notes
Verde	verde-black_pearl-production-3.5.5-135/1281.archive	Please contact Support for this update	Verde Array Family Release Notes and Documentation Updates
BlackPearl	verde-black_pearl-production-4.1.1-135/1281.archive	Please contact Support for this update	BlackPearl Release Notes and Documentation Updates.

Figure 306 The Product Software screen.

3. Locate the BlackPearl gateway in the **SpectraProduct** column. The currently released BlackPearl software version is listed in the **Current Version** column.
4. Click the name of the BlackPearl package. The package begins downloading through your web browser. Do not unzip the downloaded file.

5. From the BlackPearl menu bar, select **Support > Software** to display the Software screen. Click **Choose File.** Using your web browser, browse to the location of the update file and select the file to upload. The file is staged to the gateway.



Current Version: 3.3.0

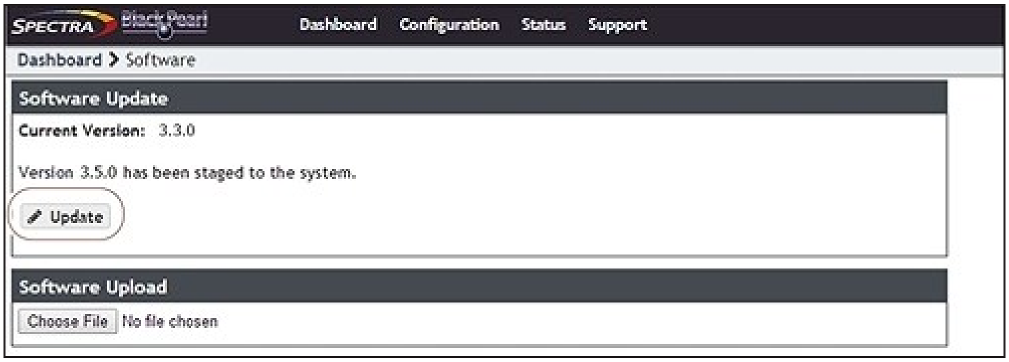
Version 3.5.0 has been staged to the system.

No file chosen

Figure 307 The Software Update screen with an available software package listed.

Install the Update

1. Discontinue all file storage operations on the BlackPearl gateway. The gateway automatically reboots as part of the update process.
2. From the menu bar, select **Support > Software** to display the Software screen. The Software screen displays with the software upload file staged to the gateway.



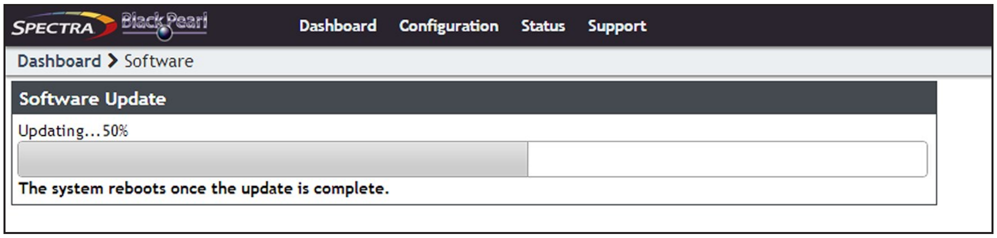
Current Version: 3.3.0

Version 3.5.0 has been staged to the system.

No file chosen

Figure 308 The Software Update screen with a software package staged to the gateway.

3. Click **Update**. A progress bar shows the progress of the update.



Software Update

Updating…50%

The system reboots once the update is complete.

Figure 309 The Software Update screen showing the progress of an update.

4. When the update is complete, the BlackPearl gateway automatically reboots to begin using the latest software.

5. Restart file storage operations.

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.

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 Gen2 S Series Chassis, below.
- Install a Drive in a Gen2 V Series Chassis on page 483
- Install a Drive in a Gen2 X Series Chassis on page 484
- Install a Drive in a Gen1 Chassis on page 486

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.

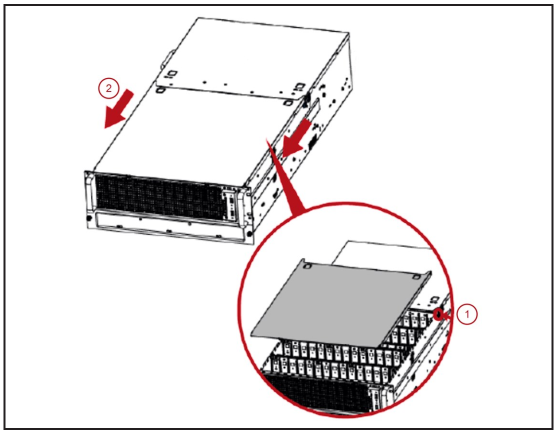


Figure 310 Remove the front top cover.

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**).

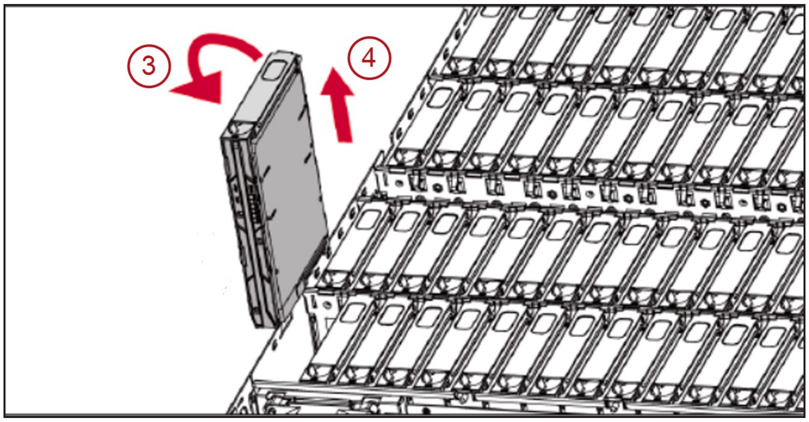


Figure 311 Remove the drive from the BlackPearl chassis.

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.

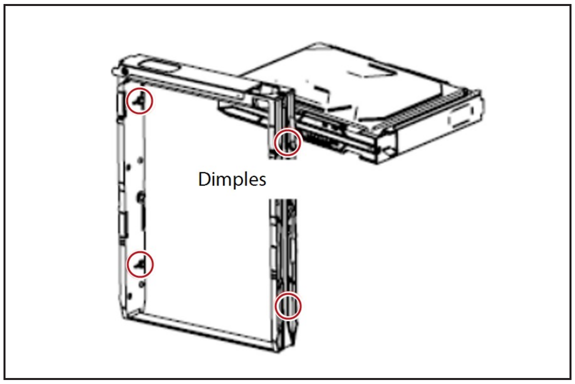


Figure 312 Match the dimples on the drive sled to the dimples on the drive.

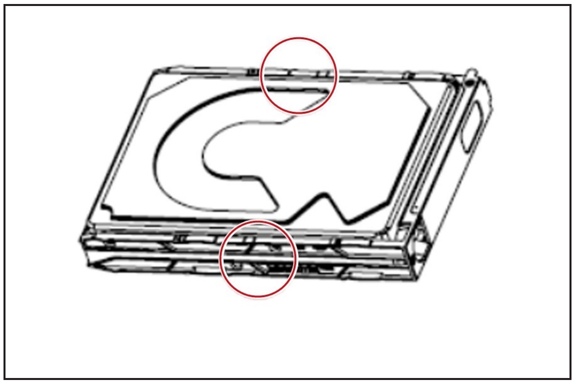


Figure 313 The drive installed in the drive sled.

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 482 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**).

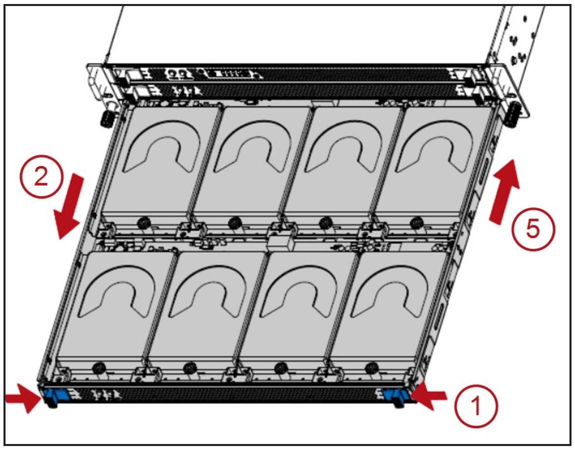


Figure 314 Remove the drive tray.

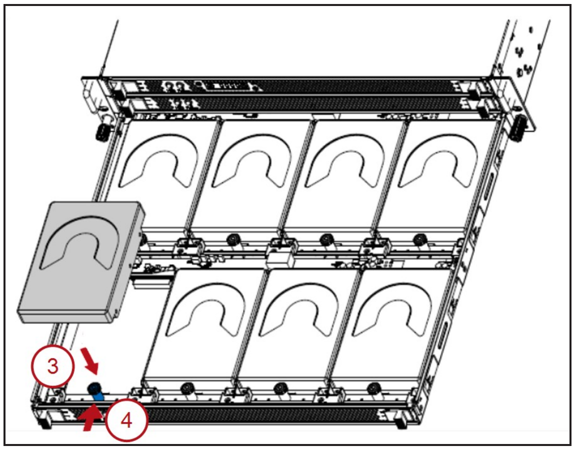


Figure 315 Install the drive.

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 4 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 483 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.

CAUTION Use care to avoid damaging the release latch and drive sled handle.

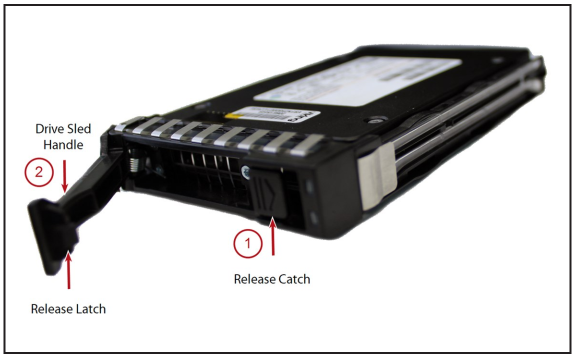


Figure 316 Drive sled parts.

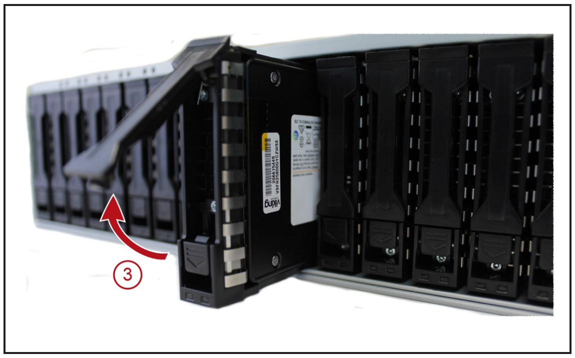


Figure 317 Remove the drive sled with drive blank and insert the drive sled with drive.

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.

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 316 on page 485) 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 484 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 gateway are mounted on drive sleds that ensure proper data and electrical connection with the backplane inside the BlackPearl 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.

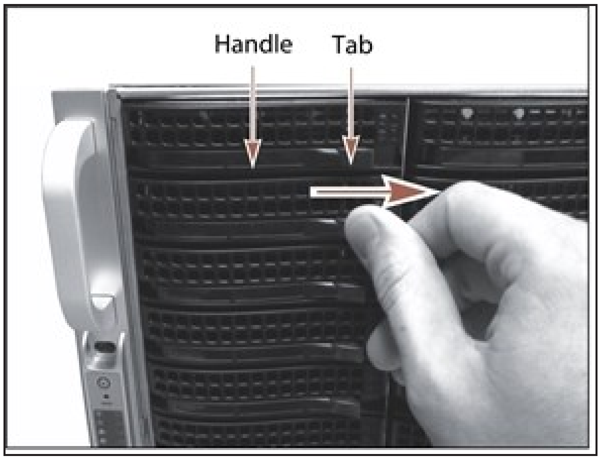


Figure 318 Slide the tab to the right to release the drive sled handle.

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.

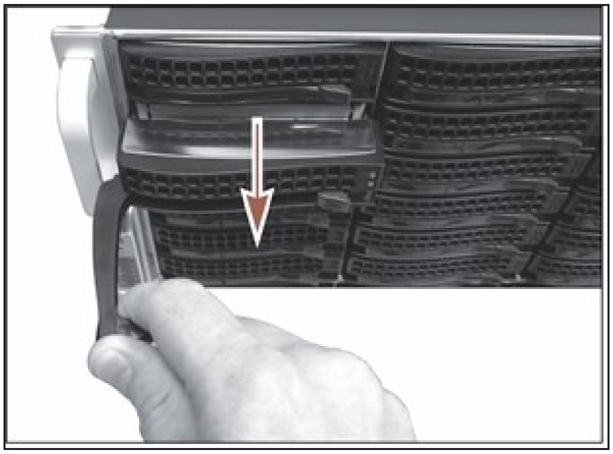


Figure 319 Pull the sled out of the gateway.

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.

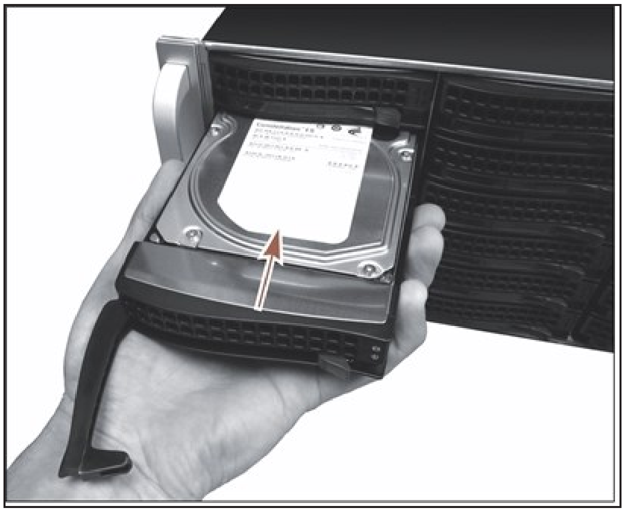


Figure 320 Install the drive into the BlackPearl gateway.

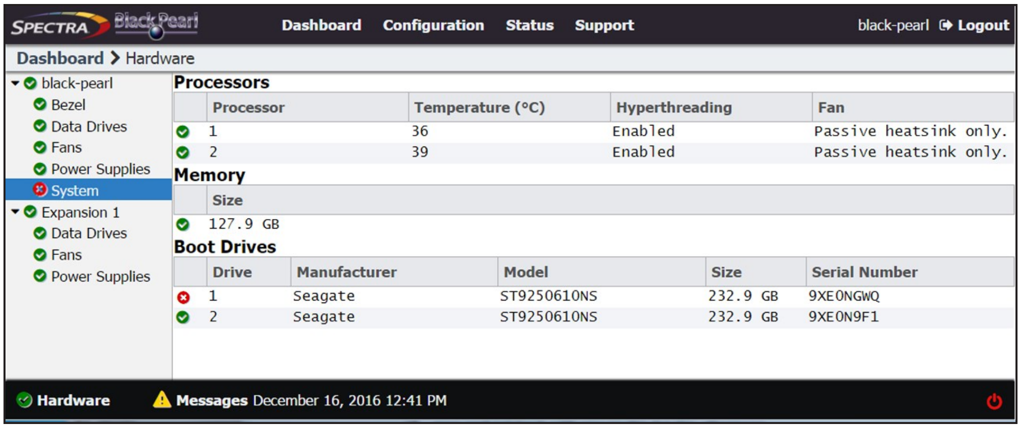
3. When the drive sled is in position, push the handle inward and to the right until the locking tab secures it in place. An audible click indicates that the drive sled is locked into position.
4. If necessary, reinstall the front bezel.

Replace a Failed Component

If a component in a BlackPearl 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 on page 64).

Identify the Failed Component

1. From the menu bar, select **Status > Hardware**. The Hardware screen displays. The malfunctioning component is indicated by an error icon.



Processors

	Processor	Temperature (°C)	Hyperthreading	Fan
✓	1	36	Enabled	Passive heatsink only.
✓	2	39	Enabled	Passive heatsink only.

Memory

	Size
✓	127.9 GB

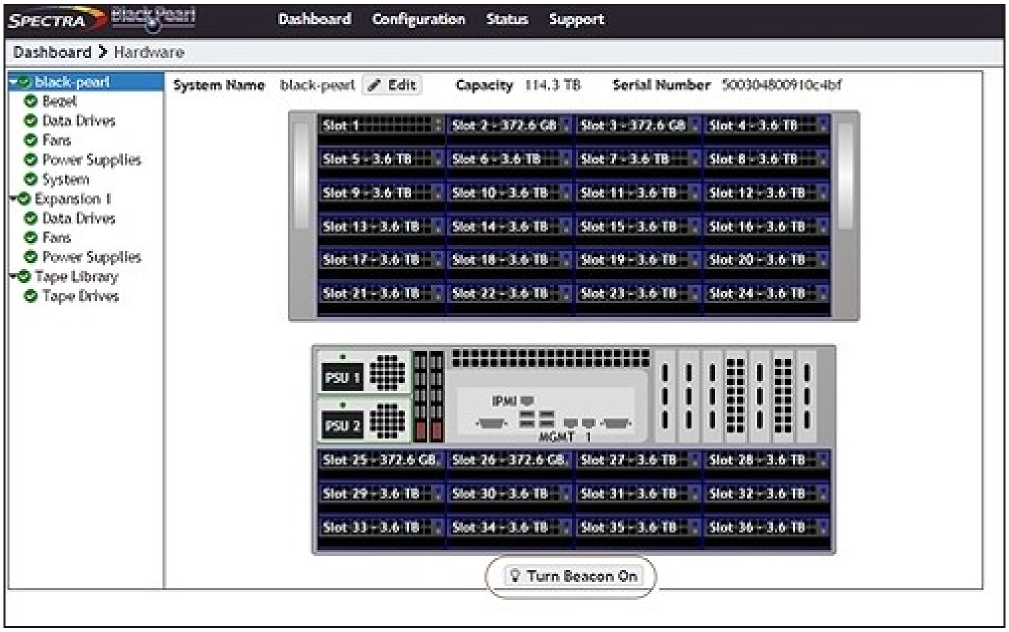
Boot Drives

	Drive	Manufacturer	Model	Size	Serial Number
⊗	1	Seagate	ST9250610NS	232.9 GB	9XE0NGWQ
✓	2	Seagate	ST9250610NS	232.9 GB	9XE0N9F1

Messages December 16, 2016 12:41 PM

Figure 321 The Hardware screen showing a failed component.

2. If you have multiple BlackPearl gateways, you can use the beacon feature to help locate the gateway with the failed component. 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 322 The Hardware screen. Gen1 S Series 4U chassis shown.

3. Click **Turn Beacon On**. The BlackPearl 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.

5. 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 12- & 36-Drive Chassis HBA Installation Guide* provides instructions for installing an HBA in a Gen1 master node.
- The *Spectra 12- & 36-Drive Chassis Boot Drive Replacement Guide* provides instructions for replacing a failed boot drive in a Gen1 master node.
- The *Spectra 12-, 36- & 45-Drive Chassis Drive Replacement Guide* provides instructions for replacing a failed data drive in a Gen1 master node or 44-bay expansion node.
- The *Spectra 12-, 36- & 45-Drive Chassis Fan Replacement Guide* provides instructions for replacing a failed fan in a Gen1 master node or 44-bay expansion node.
- The *Spectra 12-, 36- & 45-Drive Chassis Power Supply Replacement Guide* provides instructions for replacing a failed power supply in a Gen1 master node or 44-bay expansion node.
- The *Spectra 12-Drive Chassis HBA Replacement Guide* and *Spectra 36-Drive Chassis HBA Replacement Guide* provide instructions for replacing a failed HBA in a Gen1 master node.

- 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.

CHAPTER 13 - FAQ, TROUBLESHOOTING, AND SUPPORT

Use the information in this appendix to troubleshoot problems on the Spectra BlackPearl Nearline Gateway as they arise, before contacting Spectra Logic Technical Support.

BlackPearl Cache 495

How is Cache Used and Allocated? 495

Why Does the BlackPearl User Interface Display 80% Cache Usage? 495

Tape Partitions 497

How Does a User Upgrade to Later Generations of Media in the Same Tape Library? 497

What Happens When a Tape Partition is Placed in Standby/Quiesced? 497

What Happens When a Tape Partition is Re-Activated? 498

How do I Change the Tape Library Used by the BlackPearl gateway While Minimizing the Impact, Management Time, and System Downtime? 498

Tape Media 499

How Does a User Know if Tape Media is Running Out of Space? 499

Can Data be Overwritten on Existing Tapes? 499

Can WORM Media be Used With the BlackPearl Gateway? 499

Tape Media Import 500

How Does a User Know What Tape Cartridge(s) to Import in Response to a GET Request for Objects on Exported Media? 500

Tape Media Export 501

What Happens if a User Exports a Tape From the Library Before Exporting the Tape in the BlackPearl User Interface? 502

How Does a User Configure Their T50e or T120 Library to Support Exporting Tapes From the BlackPearl Gateway? 502

Tape Drive Cleaning 503

How Does a User Know Their Cleaning Media is Expired? 503

How Does a User Use Cleaning Media in a T50e or T120 Library That Does Not Have a Cleaning Partition? 504

Tape Drive Test 505

How Does a User Test a Tape Drive in a Spectra Logic Library? 505

Collect Drive Diagnostic Logs **506**

Write to Tape Drive Test **507**

How Does a User Test That Data is Being Written to Tape Media? 507

BlackPearl Database Backup **508**

How Does a User Verify the Database Backup Schedule? 508

How Does a User Create a Bucket Isolated Data Policy for the Database Backup Tapes? 508

BlackPearl Disk Storage Data Retention **509**

BlackPearl Component Hardware **511**

How Does a User Know if a Component of the BlackPearl Gateway Has an Error? 511

Why Do Drives Added to an Expansion Node Fail to Display in the BlackPearl Management Interface? 511

Intelligent Object Management (IOM) **512**

Best Practices 512

Using a BlackPearl Gateway with the Vail Application **514**

Why Do Vail Jobs Show as Canceled in the BlackPearl User Interface? 514

What Ports Does the BlackPearl Gateway Use to Connect to a Vail Sphere? 514

Special Firewall Feature for Connecting to the BlueScale User Interface **515**

Introduction 515

Warning 515

Basic Steps 515

Capacity Mode versus Performance Mode **516**

Chunks 516

Performance Mode 516

Capacity Mode 516

Tape Handling Refactor Starting with BlackPearl OS 5.3 .... **518**

General BlackPearl Notes 518

Tape Drive Failure Modes 518

Move Failures/Tape Stuck in Drive 519

Library, Drive, and Tape Failure Behavior in BlackPearl version 5.3 519

Enabling iSCSI For Use With the Spectra Swarm **522**

Tape Library Errors **525**

What is a Data Checkpoint Failure? 525

Troubleshooting **526**

Resolve a BlackPearl Management Port IP Address Conflict **536**

Using the Console 536

Using a Separate Computer 536

Network Setup Tips **539**

Configuration 539

Connectivity to the Network 539

Troubleshooting 541

Tools 542

Spectra Logic Technical Support **544**

Before Contacting Support 544

Determine the Gateway Serial Number 544

Opening a Support Ticket **545**

Remote Support **550**

Enabling Remote Support 550

Disabling Remote Support 551

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 gateway from a client, or transferred from tape storage to the BlackPearl 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 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 S3 service allows you to set a schedule to minimize downtime.

Why Does the BlackPearl User Interface Display 80% Cache Usage?

BlackPearl OS 5.2 or Earlier

After the gateway is in use, the Cache Used circle graph on the user interface dashboard hovers around 80% used capacity. When a task for a chunk, or the full job, completes, the data planner does not immediately delete those objects, but leaves them in the cache, available for reclaiming. Data from completed tasks remains in cache until more capacity is needed, or the used capacity exceeds 80%. When this threshold is reached, the BlackPearl gateway proactively deletes some of the data from completed tasks. The user interface dashboard only displays the actual data bytes in cache. It does not reflect cache capacity used by active jobs. To see how much cache capacity is currently used by active jobs, on the Jobs page of the user interface, select **Active Jobs**, and calculate the difference between "Amount Transferred to Cache" and "Amount Received/Archived".

BlackPearl OS 5.3 or Later

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 either the Advanced Bucket Management screen, or the Hardware page by double-clicking 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 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 gateway does not issue any internal tape task commands. The BlackPearl 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 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 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 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 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 S3 service is set to "Never Inspect".

How do I Change the Tape Library Used by the BlackPearl gateway While Minimizing the Impact, Management Time, and System Downtime?

If you plan to upgrade the library used by the BlackPearl 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 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.

IMPORTANT Create a manual database backup before changing to a new tape library or partition.

With BlackPearl OS 5.1 or earlier, moving tapes to a new partition may require a BlackPearl foreign import, which must be done for each storage domain. You will need to export the tapes in batches, by storage domain, from the old partition, and import them into the new partition using a foreign import into storage domains associated with each exported batch. If necessary, repeat the process for additional storage domains.

If any tapes that have been exported from the BlackPearl gateway are not stored on-site, those tapes must be rotated back on-site and imported through the new partition, or Spectra Logic Technical Support must manually update the database to re-associate those external tapes with the new 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 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 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 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.

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 Gateway?

The BlackPearl gateway is not compatible with WORM (Write Once-Read Many) media. If the BlackPearl gateway is configured to transfer data to tape, make sure the partitions configured for use by the BlackPearl 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 370.

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 Understanding Advanced Bucket Management on page 88. For additional information about exporting and importing tapes, see Working with Tape Libraries and Media on page 341.

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 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 Understanding Advanced Bucket Management on page 88 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 393).
- **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 393).

"Export" has multiple definitions within the gateway:

- From the BlackPearl 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.

Note: For instructions on exporting a tape from an IBM TS4500 tape library, see the see the *TS4500 User Guide*.

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 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. For instructions on importing a tape into an IBM TS4500 tape library, see the see the *TS4500 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 370. 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. For instructions on importing a tape into an IBM TS4500 tape library, see the see the *TS4500 User Guide*. 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 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 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 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.

Expired cleaning media is automatically exported from an IBM TS4500 tape library.

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 *Tape Library User Guides*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 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, use the steps in this section to test the tape drive.

Note: Starting with BlackPearl OS 5.6, you can test a tape drive using the BlackPearl user interface. See Test Tape Drive on page 357. Only use the process below if you cannot use the BlackPearl user interface to test a tape drive.

1. In the BlackPearl management interface, select **Configuration > Advanced Bucket Management > Storage & Policy Management**.
2. Under the Tape Partitions heading, **double-click** the partition containing the drive you want to test.
3. Select the row of the drive, select **Action > Offline Tape Drive**, then click **Deactivate**.
4. Select **Action > Reserve Tape Drive**.
5. Using the **Reserved Task Type** drop-down menu, 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.
6. Using the tape library BlueScale user interface, edit the tape partition to remove the drive you want to test. See your tape library *User Guide* for instructions.

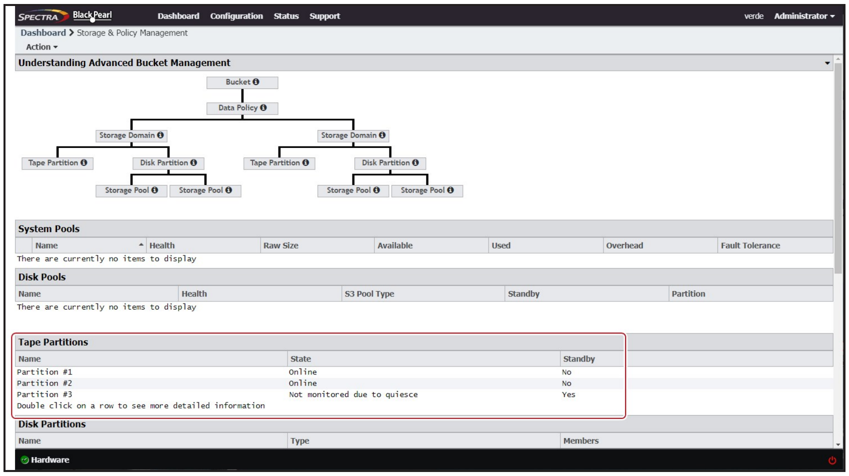
Note: Continue to see your tape library User Guide for the remainder of the test process.

7. Create a new partition with the drive to test as the only drive in the partition.
8. Import a scratch tape and a cleaning cartridge into the Entry/Exit port of the new partition.
9. Test the drive using the tape library MLM Drive Test feature.
10. After the drive test completes, delete the partition you created in Step 7.
    - If the drive passed the drive test, edit the tape partition used by the BlackPearl Nearline 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 Drive Diagnostic Logs on the next page and contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 9).

Collect 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.

1. Select **Configuration > Advanced Bucket Management > Storage & Policy Management**.
2. Under the **Tape Partitions** banner, double-click the partition containing the drive for which you want to save logs.



System Pools

Name	Health	Raw Size	Available	Used	Overhead	Fault Tolerance

There are currently no items to display

Disk Pools

Name	Health	S3 Pool Type	Standby	Partition

There are currently no items to display

Tape Partitions

Name	State	Standby
Partition #1	Online	No
Partition #2	Online	No
Partition #3	Not monitored due to quiesce	Yes

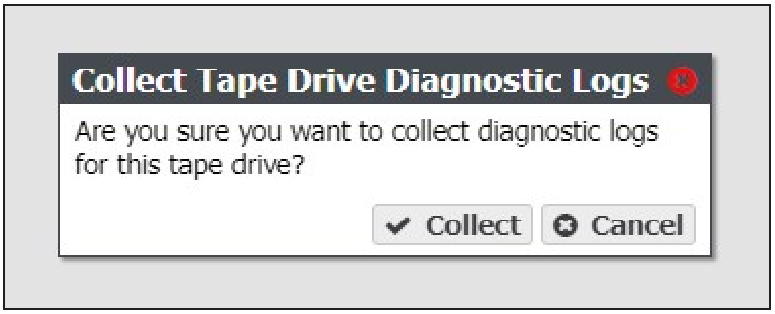
Double click on a row to see more detailed information

Disk Partitions

Name	Type	Members

Figure 323 The Storage & Policy Management screen.

3. Select the drive, and select **Action > Collect Tape Drive Diagnostic Logs**.



Collect Tape Drive Diagnostic Logs

Are you sure you want to collect diagnostic logs for this tape drive?

Figure 324 The Collect Tape Drive Diagnostic Logs window

4. Click **Collect**. The process takes approximately 30 seconds.

   After the drive log collection completes, download the log as described in Download a Log Set on page 462.

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 system 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**.
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.

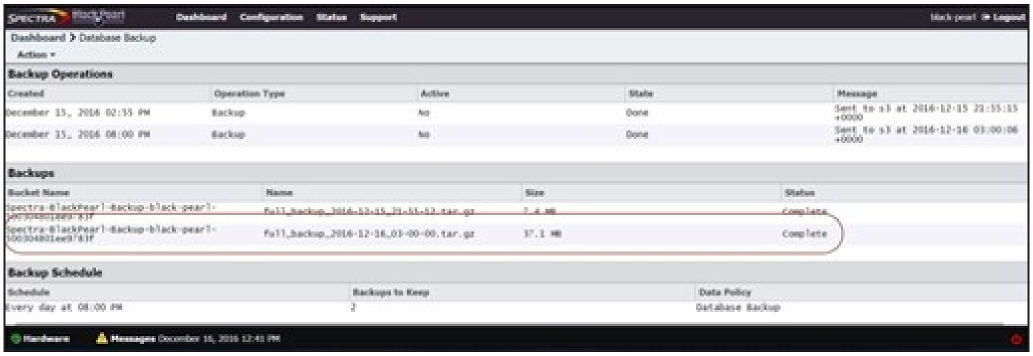
BlackPearl Database Backup

The BlackPearl database is contained on a set of flash (SSD) drives within BlackPearl 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 > Database Backup**. The Database Backup screen displays. In the Backup Schedule pane, view the current schedule. In the Backups pane, view the date code in the name of the complete backups available to verify the most recent backups.



Backup Operations

Created	Operation Type	Active	State	Message
December 15, 2016 02:55 PM	Backup	No	Done	Sent to s3 at 2016-12-15 21:55:15 +0000
December 15, 2016 08:00 PM	Backup	No	Done	Sent to s3 at 2016-12-16 03:00:06 +0000

Backups

Bucket Name	Name	Size	Status
Spectra-BlackPearl-Backup-black-pearl-5003048001ee9783F	full_backup_2016-12-15_21-55-12.tar.gz	7.4 MB	Complete
Spectra-BlackPearl-Backup-black-pearl-5003048001ee9783F	full_backup_2016-12-16_03-00-00.tar.gz	37.1 MB	Complete

Backup Schedule

Schedule	Backups to Keep	Data Policy
Every day at 08:00 PM	2	Database Backup

Figure 325 The Database Backup screen.

Note: See Database Backup & Restore on page 441 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 150 to create a new storage domain for the database backups.
2. Follow the instructions in Create a Data Policy on page 159 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. Using the **Data Policy to Use** drop-down menu, 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 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 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 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 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 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 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 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 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 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 Gateway Has an Error?

During installation of the BlackPearl gateway, users are configured to receive emails if the BlackPearl gateway or the tape library issues a warning or error message. See “Configure Mail Users” in your *Tape Library User Guide* and Configure Mail Recipients on page 455 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 526 section to correct any issues.

Note: For instructions on messaging and error reporting on an IBM TS4500 tape library, see the *TS4500 User Guide*.

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 system and all expansion nodes.
2. Power-on all expansion nodes
3. Wait approximately four minutes
4. Power-on the BlackPearl Nearline gateway.

INTELLIGENT OBJECT MANAGEMENT (IOM)

With IOM, the BlackPearl 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 systems are configured for replication, and a bucket is deleted on the target BlackPearl nearline 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 Add a Storage Domain Member to a Storage Domain on page 156 and Exclude a Storage Domain Member on page 184 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 159 and Edit a Data Policy on page 193.

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 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 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 gateway, it initiates a Start Bulk Get job on the BlackPearl gateway. However, the Vail application has a back-door path to read objects from the BlackPearl cache. The BlackPearl 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 gateway.

What Ports Does the BlackPearl Gateway Use to Connect to a Vail Sphere?

In order to use a BlackPearl 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 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 S3 endpoint nodes.

SPECIAL FIREWALL FEATURE FOR CONNECTING TO THE BLUESCALE USER INTERFACE

Introduction

The BlackPearl gateway can act as a gateway for a Spectra Logic tape library network management interface. This feature enables a private network behind the BlackPearl gateway, where Proxy/NAT information is entered into the BlackPearl gateway to allow a connection to either a BlueScale library or BlueVision library with the BlackPearl 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 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 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 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.

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 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 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 STARTING WITH BLACKPEARL OS 5.3

Use the information in this section to understand the changes to tape handling in BlackPearl OS 5.3.

General BlackPearl Notes

- Tape drives can be taken offline and new drives brought online without restarting the BlackPearl 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 gateway is using it.
- Most drive sense is handled by the sa(4) driver and LTFS. The tape drivers used by the BlackPearl 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 gateway does not issue reset tape drive commands.

Tape Drive Failure Modes

The BlackPearl 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 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 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 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 gateway detects these events through the tape library management subsystem. Currently, the BlackPearl 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 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 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 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 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 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 gateway receives Unit Attention conditionals from the library that tell the BlackPearl 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 gateway. For each attempt that fails, the BlackPearl 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 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 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 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 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 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 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 gateway will not automatically quiesce the tape drive.

4. An LTFS Encryption error, or 500 Hardware error from tape drive causes the BlackPearl 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 gateway to stop monitoring or reconciling a tape library change (tape inspections are not eliminated). Instead, the BlackPearl 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.

7. If a tape library disappears unexpectedly (for example a RIM or robot connection is accidentally disconnected), the BlackPearl 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".

   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".

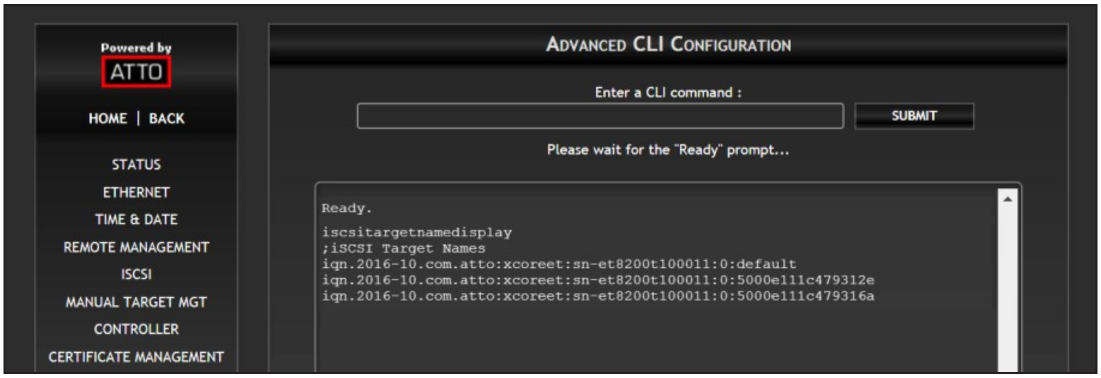
ENABLING iSCSI FOR USE WITH THE SPECTRA SWARM

The BlackPearl 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 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 9).

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.

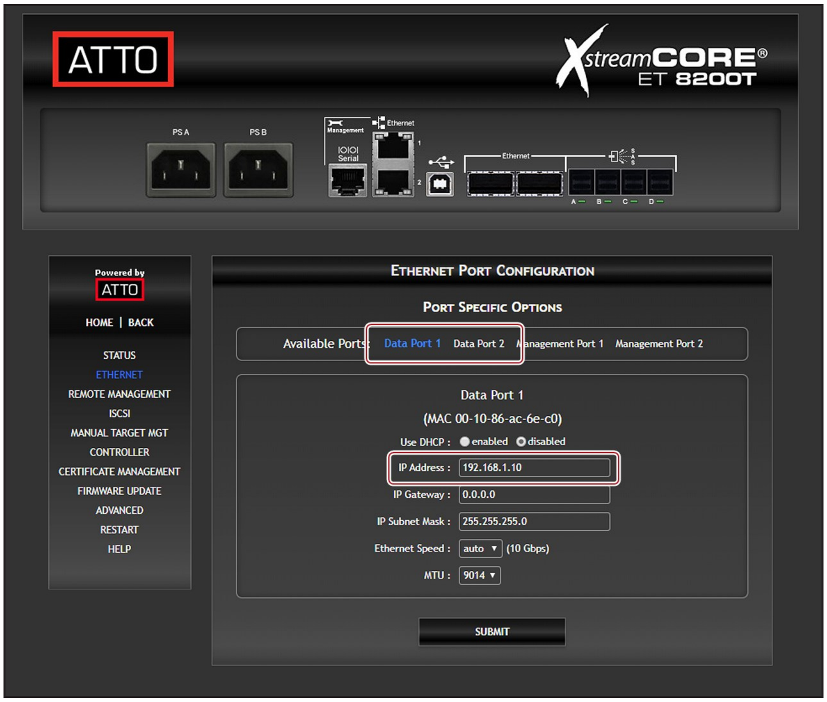
IMPORTANT Using the default target may cause drive reservation errors with other appliances connected to the Spectra Swarm.

Note: The default target is a collection of all iSCSI targets attached to the bridge, and is not recommended for use with the BlackPearl 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

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 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 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 gateway must be restarted for this change to take effect. During system initialization, the BlackPearl 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 9).

Tape Library Errors

What is a Data Checkpoint Failure?

A data checkpoint failure results from the BlackPearl Nearline 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 Nearline 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 Nearline 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 gateway is trying to locate is missing.

If a data checkpoint failure occurs, both system messages in the BlackPearl 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.

TROUBLESHOOTING

This section helps you troubleshoot problems with the Spectra BlackPearl 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 9).

Issue	Resolution
An email is sent from the tape library indicating that drives need cleaning	If the BlackPearl gateway is connected to a **Spectra T200, T380, T680, T950, or TFinity library**, the library should be configured with a cleaning partition, which automatically cleans drives when cleaning is requested by the drive. If the BlackPearl 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 gateways' export function. If there is cleaning media in the data partition, the BlackPearl 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. **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.** Using the **Partition** drop-down menu, select **Total Library**. **4.** Using the **Report** drop-down menu, 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 9).

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.** From the menu bar, select **Configuration > DLM**. The DLM screen displays. **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 9).
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 9).
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 9).

Issue	Resolution
An email is sent from the tape library indicating a tape cartridge experienced a read or write error	If the BlackPearl 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 9). **5.** In the BlackPearl user interface, 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 gateway. **8.** Click **Export**. The tape is marked as exported in the BlackPearl 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 your *Tape Library User Guide*. **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 9).
The BlackPearl 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 9).

Issue	Resolution
A system message on the BlackPearl gateway reports "No tapes available" for a storage domain	When the BlackPearl 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 gateway before exporting the tapes from the tape library. See Export Tapes on page 393.
The BlackPearl 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 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 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 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 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 gateway. **1.** In the BlackPearl user interface, select **Configuration > Services**. The Services screen displays. **2.** Select the S3 Service and select **Action > Show Details**. The S3 Service details screen displays. **3.** On the 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 9).

Issue	Resolution
An email is sent from the BlackPearl 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 370. 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 gateway indicating a hardware failure	Over time, replaceable components in the BlackPearl gateway may wear down and fail. Use the instructions in this section to determine the failed component. **1.** In the BlackPearl user interface, select **Status > Hardware**. 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 9). 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 • Tape Drives (installed in the tape library)

Issue	Resolution
An email is sent from the BlackPearl 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.** In the BlackPearl user interface, select **Configuration > Services**. The Services screen displays. **2.** Select the S3 service, and select **Action > Show Details**. **3.** On the service detail screen, ensure the status of **Data Path Backend Activated** is **Yes**. If the data path is not enabled, select **Action > Activate Data Path Backend**. Check to make sure that no tape libraries are in standby state. **1.** From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management**. The Advanced Bucket Management screen displays. **2.** Under Tape Partitions, make sure all tape partitions listed show a **State** of **Online** and a **Standby** status of **No**. If any tape partitions are in standby state, select the tape partition, and then select **Action > Activate Tape Partition**. Check for system messages that indicate the partition is out of space. See A system message on the BlackPearl gateway reports “No tapes available” for a storage domain on page 530. • 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 BlackPearl user interface, select **Status > S3 Jobs**. The S3 Jobs screen displays. **2.** Select the job you want to cancel and select **Action > Cancel Job**.
An email is sent from the BlackPearl gateway indicating that the database is full	If the database reaches full capacity, the BlackPearl 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 9).

Issue	Resolution
A system message on the BlackPearl gateway indicates that the database is not being backed up	The BlackPearl gateway reports a failure to backup the database in the system messages. Check the system messages to determine the cause. **1.** In the BlackPearl user interface, select **Status > Messages**. The Messages screen displays. **2.** Examine the list of messages for additional information about the failure. If the database backup schedule is not configured, the BlackPearl 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 & Restore on page 441 for more information.
The BlackPearl 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 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 gateway automatically inspects and uses the tapes as needed.

Issue	Resolution
The BlackPearl Tape Management screen shows media in the attached tape library as "Inspect Failed"	The BlackPearl 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 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. **1.** In the BlackPearl user interface, 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 gateway. **5.** Click **Export**. The tape is marked as exported in the BlackPearl 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*.
The BlackPearl gateway displays a system message that a "Job did not complete in a 24 hour period"	If the BlackPearl 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 Network Setup Tips on page 539 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. **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.** In the BlackPearl user interface, select **Support > Logs**. The Logs screen displays.

Issue	Resolution
	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 544.
The BlackPearl user interface does not appear to update correctly	The BlackPearl 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.

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 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 gateway to your network.

Using the Console

Using the BlackPearl Nearline 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 gateway. See Rear Panel on page 44 to locate the management port.
3. Open a web browser on the computer. For a list of compatible browsers, see Supported Browsers on page 65.
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.

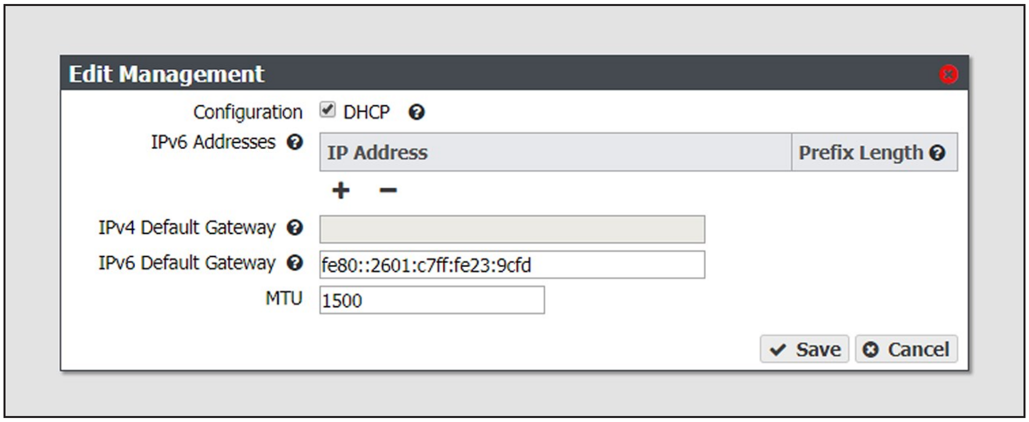
6. Enter the login username and password.

   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 fields are case sensitive.

Note: If you are running BlackPearl OS 4.0 through 5.3, the default username is **Administrator** and the default password is **spectra**. Starting with BlackPearl OS 5.4, the default password is the Serial Number (SN) printed on the front-right corner on the top of the chassis.

7. From the menu bar, select **Configuration > Network**, or click the Network pane from the Dashboard screen. The Network screen displays.

8. In the Network Interfaces pane, double-click the Management row, or select the Management row and then select **Action > Edit**. The Edit Management dialog box displays.



Edit Management

Configuration ☑ DHCP

IPv6 Addresses

IP Address	Prefix Length

IPv4 Default Gateway:

IPv6 Default Gateway: fe80::2601:c7ff:fe23:9cfd

MTU: 1500

Figure 326 The Edit Management dialog box.

9. Select **DHCP** 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.

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.

10. 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 in Step 9.

- **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.

11. Enter the **IPv4 Default Gateway**.

Note: If you selected DHCP in Step 9 on page 538, this option is unavailable.

12. Enter the **IPv6 Default Gateway**.

13. Change the **MTU** 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.

14. Click **Save**.

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.

15. Disconnect the Ethernet cable from the BlackPearl management port.

16. Connect a cable from your network to the management port on the BlackPearl gateway. You are now able to connect to the gateway with the IP address configured.

NETWORK SETUP TIPS

The BlackPearl management port is separated from the data ports. The management port and data ports have their own default routes. This does not prevent a user from having the management and data ports utilizing the same network, if desired.

The basic steps for configuring the management and data ports for access to the 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 gateway and utilize the Ethernet interfaces correctly.

Configuration

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

Connectivity to the Network

The following configurations are supported for the data path:

Recommended:

- **For the 10 GigE optical card (Gen1 only):**
  - Single 10 GigE logical connection using one of the 10 GigE physical ports

    —OR—

  - Single 20 GigE logical connection using two 10 GigE physical ports (link aggregation)
- **For the 40 GigE optical card: (Gen1 only):**
  - Single 40 GigE logical connection using one of the 40 GigE physical ports

    —OR—

  - Single 80 GigE logical connection using two 40 GigE physical ports (link aggregation)
- **For the 10GBase-T card (Gen1 only):**
  - Single 20 gigabit logical connection using two 10GBase-T physical ports (link aggregation)

    —OR—

  - Single 30 gigabit logical connection using three 10GBase-T physical ports (the two ports on the card and the one spare on-board port) (link aggregation)

- **For the 25 GigE optical card: (Gen2 only):**
    - Single 25 GigE logical connection using one of the 25 GigE physical ports

      —OR—
    - Single 50 GigE logical connection using two 25 GigE physical ports (link aggregation)
- **For the 100 GigE optical card: (Gen2 only):**
    - Single 100 GigE logical connection using one of the 100 GigE physical ports

      —OR—
    - Single 200 GigE logical connection using two 100 GigE physical ports (link aggregation)

Not Recommended:

- Single gigabit logical connection utilizing one of the 10GBase-T physical ports and a Category 5e Ethernet cable

Assign the appropriate IP address to the management and data ports either statically or using DHCP. If you are setting the MTU to something other than 1500, ensure that your switch configuration, as well as all the hosts on the network, support larger MTU settings. The BlackPearl gateway can support jumbo frames (MTU=9000), but all switches and hosts on the network must be configured to support jumbo frames if this is selected, or performance might be degraded.

Link Aggregation Notes

Switches use different methods of routing traffic from hosts to NAS servers. There are also many different network configurations to move data from hosts to NAS servers. For example, some Cisco switches route traffic based on the MAC address and the IP address. The BlackPearl gateway presents only one MAC address and one IP address when the data ports are aggregated via DHCP; if static link aggregation is chosen, the BlackPearl gateway presents only one MAC address, but can have up to 16 IP addresses aliased to the MAC address. It is up to the switch to rotate data transfers among the physical ports on the BlackPearl gateway in order to achieve the highest throughput possible.

Additionally, if link aggregation is configured for the BlackPearl gateway, then switches must also be able to support link aggregation to aggregate or “trunk” the data ports together to provide higher bandwidth into the gateway. Switches must support link aggregation using LACP (Link Aggregation Control Protocol), and the switches must hash the destination IP addresses. Manually configure LACP on the switch ports. LACP does not get enabled automatically.

For example, if only a single host is connected to the BlackPearl gateway through a link aggregated 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 mounted two times using different IP addresses and transfers are started to that share from two separate hosts, the resulting throughput would be approximately twice that of a single host connection. You may need to configure more than two IP addresses on the BlackPearl gateway to force the switch hashing algorithm to utilize all physical ports to maximize performance.

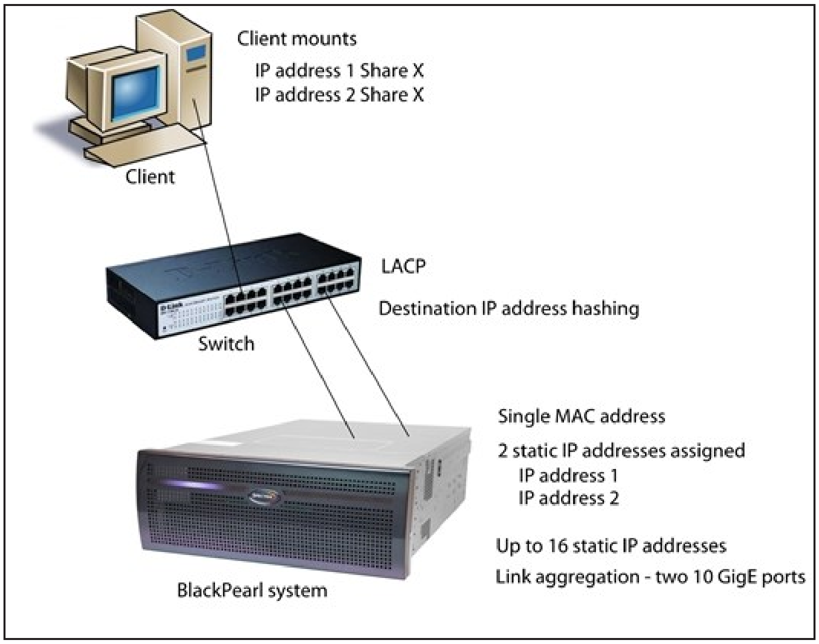


Figure 327 Connection example utilizing two IP addresses assigned to a single share.

Once configured correctly and attached to the network, the status in the user interface indicates the speed of the connection and whether the port is active. The link lights on the network ports should be on and active at both the BlackPearl gateway and the network switch.

From your network, use the "ping" command (see Ping on the next page) to test the assigned IP address for the BlackPearl management port or data port. If this is not successful, use the following troubleshooting tips to ascertain if the problem is a network setup issue.

Troubleshooting

Port Link LED Does Not Light

- Check the port configuration on the network switch. The BlackPearl gateway only supports auto-negotiation. Make sure the switch is configured to match speeds on both ends of the connection.

- Check the cables that connect the port to the other device. Make sure that they are connected. Verify that you are using the correct cable type and connectors. This is especially critical for 10 GigE and 40 GigE connections utilizing SFPs.
- Verify that the switch ports are not administratively disabled. Consult the switch *User Guide* for more information.

Port Link LED is Lit, But I Cannot Ping the BlackPearl Gateway

- Check the LACP settings on the switch. If you are using link aggregation on the BlackPearl gateway, the switch MUST be configured to use LACP on those ports. If you are not using link aggregation, the switch must be configured NOT to 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.

Tools

Ping

The ping command is a simple tool, based on a request-response mechanism, to verify connectivity to a remote network node. The ping command is based on ICMP (Internet Control Message Protocol). The request is an ICMP Echo request packet and the reply is an ICMP Echo Reply. Like a regular IP packet, an ICMP packet is forwarded based on the intermediate routers' routing table, until it reaches the destination. After it reaches the destination, the ICMP Echo Reply packet is generated and returned to the originating node.

For example, to verify the connectivity from the switch to the 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. A response of 0 msec means that the time was less than 1 ms. If the request times out, then check the settings on the switch to which the BlackPearl gateway is connected.

Traceroute

You can use the traceroute command, if it is available, or something similar, to not only verify connectivity to a remote network node, but to track the responses from intermediate nodes as well. The traceroute command sends a UDP packet to a port that is likely to not be used on a remote node with a TTL of 1. After the packet reaches the intermediate router, the TTL is decremented, and the ICMP time-exceeded message is sent back to the originating node, which increments the TTL to 2, and the process repeats. After the UDP packet reaches a destination host, an ICMP port-unreachable message is sent back to the sender. This action provides the sender with information about all intermediate routers on the way to the destination.

For example, for a BlackPearl gateway at IP address 192.168.2.10, the output of the command shown below,

```
traceroute 192.168.2.10
```

shows a numbered list indicating the number of hops encountered when tracing the packet from the switch to the BlackPearl gateway.

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 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 Check System Messages on page 420) 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.

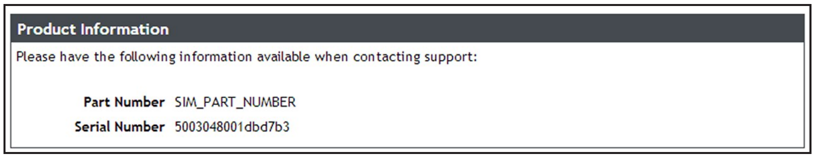
Contact Support

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 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. From the menu bar, select **Support > Contact Information**. The Contact Information screen displays.
2. The gateway serial number is listed in the Product Information pane.



Product Information

Please have the following information available when contacting support:

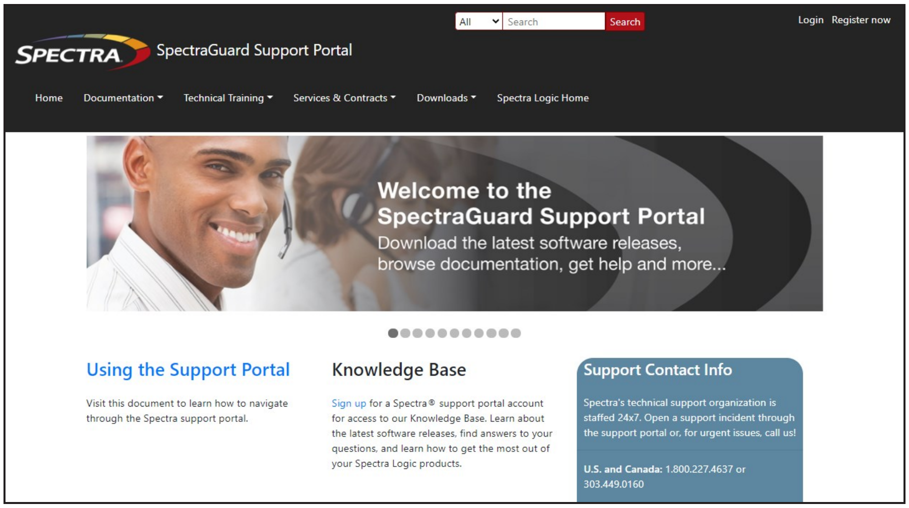
Part Number	SIM_PART_NUMBER
Serial Number	5003048001dbd7b3

Figure 328 The gateway serial number.

Opening a Support Ticket

You can open a support incident using the Spectra Logic Technical Support portal or telephone.

- Use the following instructions to open a support incident hrough the portal, or skip to Contact Spectra Logic Technical Support by Phone on page 549.



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!

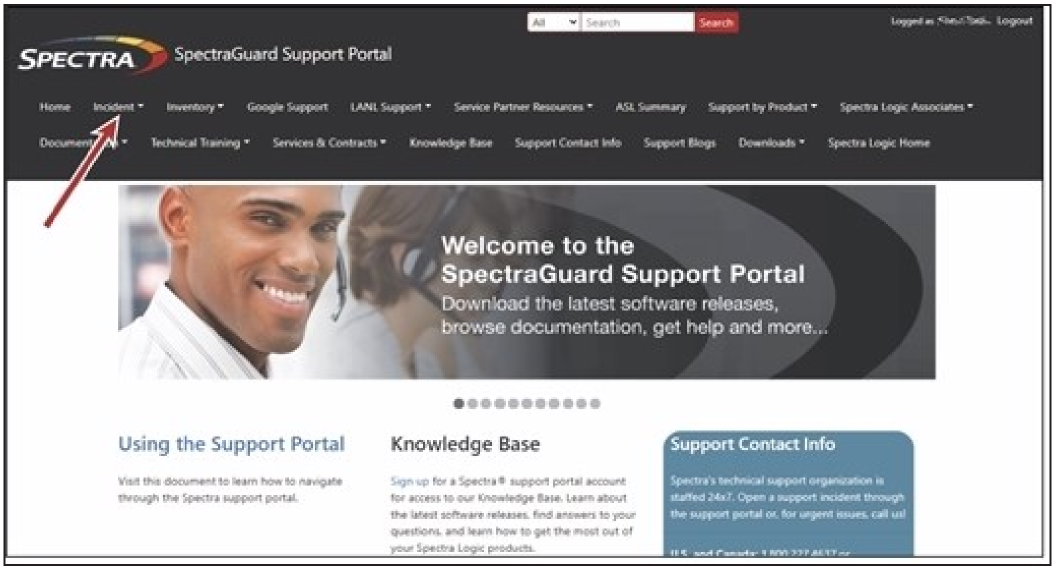
U.S. and Canada: 1.800.227.4637 or 303.449.0160

Figure 329 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 Library Serial Number)
   - 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 Spectra Logic Technical Support on the previous page if you have not previously created an account on the Technical Support portal.
4. Submit a support incident.
   - Use the following instructions to search for help before submitting a ticket, or skip to Submit an Incident Directly on page 547.

i. 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.

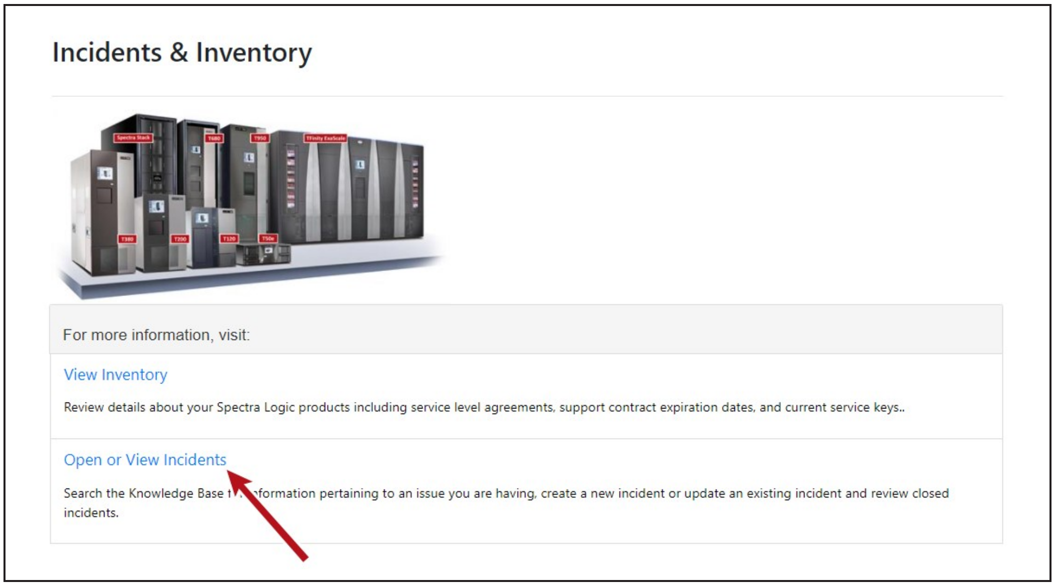
Support Contact Info

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 330 Select **Incidents>Incidents & Inventory**.

ii. Select **Open or View Incidents**.



Incidents & Inventory

For more information, visit:

View Inventory

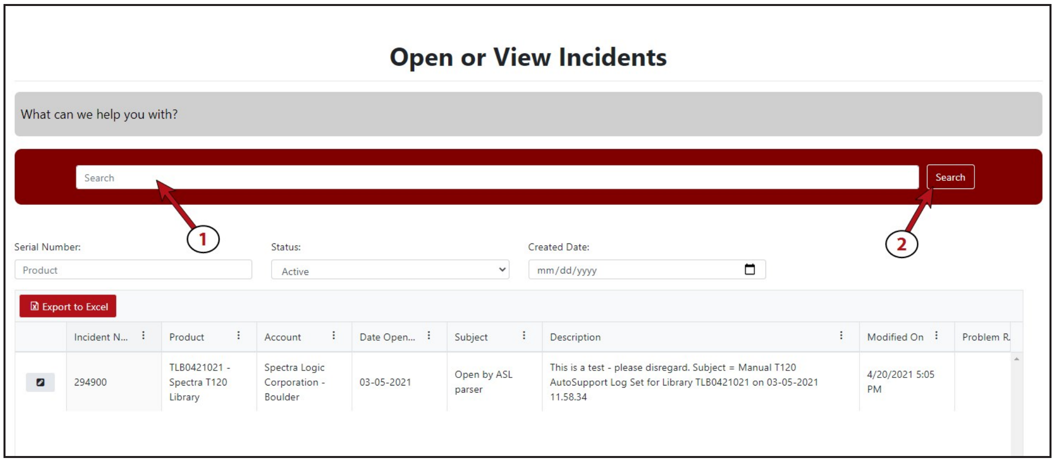
Review details about your Spectra Logic products including service level agreements, support contract expiration dates, and current service keys..

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 331 Select **Open or View Incidents**.

iii. In the Search dialog box, enter a term or phrase about your problem (**1**) and click **Search** (**2**).



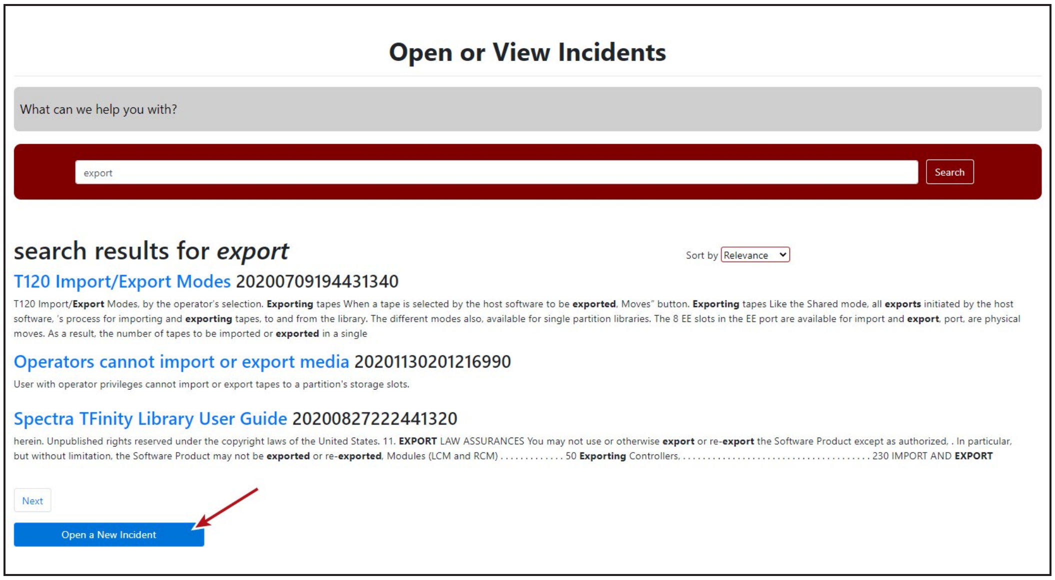
Open or View Incidents

What can we help you with?

	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 332 Enter a search phrase and click **Search**.

iv. If the search does not provide an answer, click **Open a New Incident**.



Open or View Incidents

What can we help you with?

search results for *export*

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**

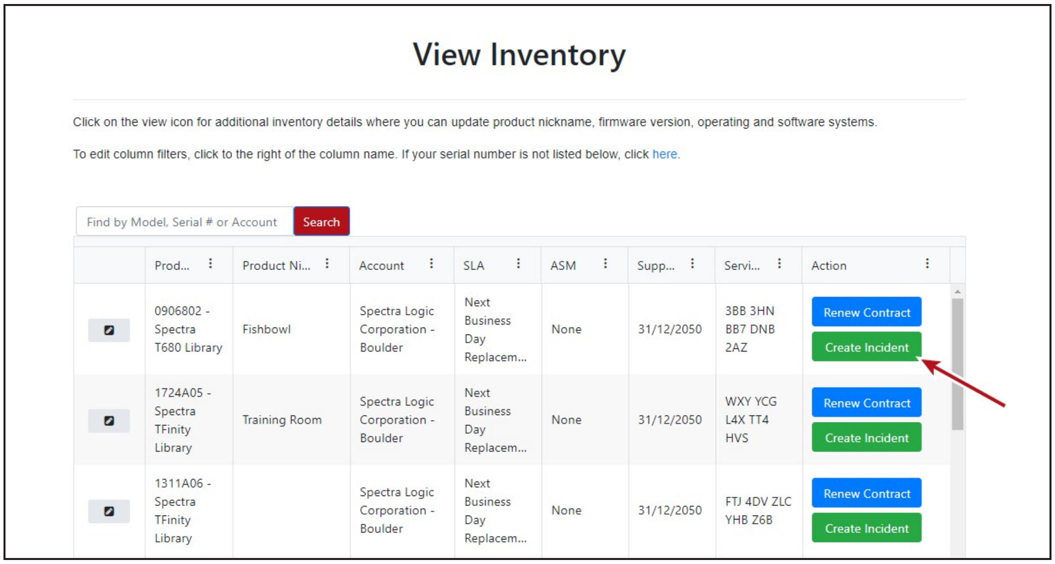
Figure 333 Click **Open a New Incident**.

v. Continue with Step 5 on page 548.

- Submit an Incident Directly

  i. From any page, select **Inventory>My Inventory**.

  ii. 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.

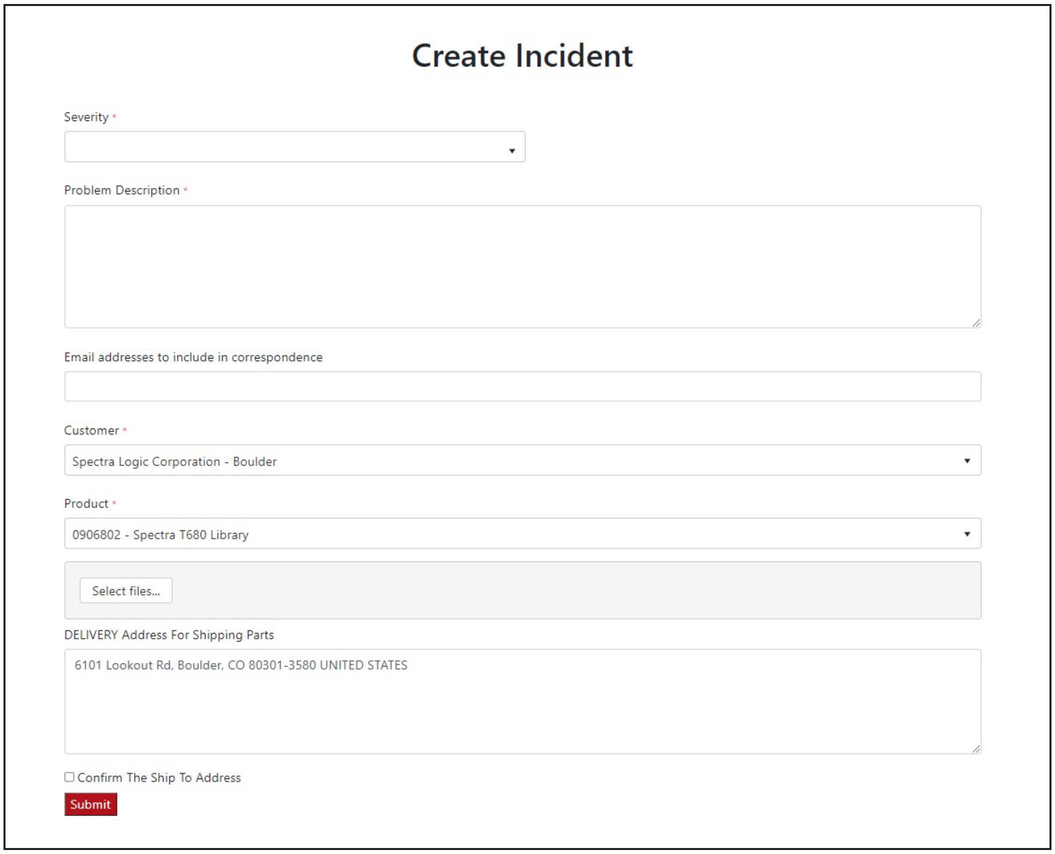
Find by Model, Serial # or Account

	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 334 Click **Create Incident**.

iii. Continue with Step 5 on page 548.

5. 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

DELIVERY Address For Shipping Parts

6101 Lookout Rd, Boulder, CO 80301-3580 UNITED STATES

□ Confirm The Ship To Address

Figure 335 Enter information about your incident and click **Submit**.

Notes:

- If you have multiple libraries and need to determine the serial number of the affected library, see Determine the Library Serial Number.
- If the serial number of the affected library is not listed, contact Technical Support (see Contacting Spectra Logic).

- Contact Spectra Logic Technical Support by Phone

  To contact Spectra Logic Technical Support by telephone, see Contacting Spectra Logic.

REMOTE SUPPORT

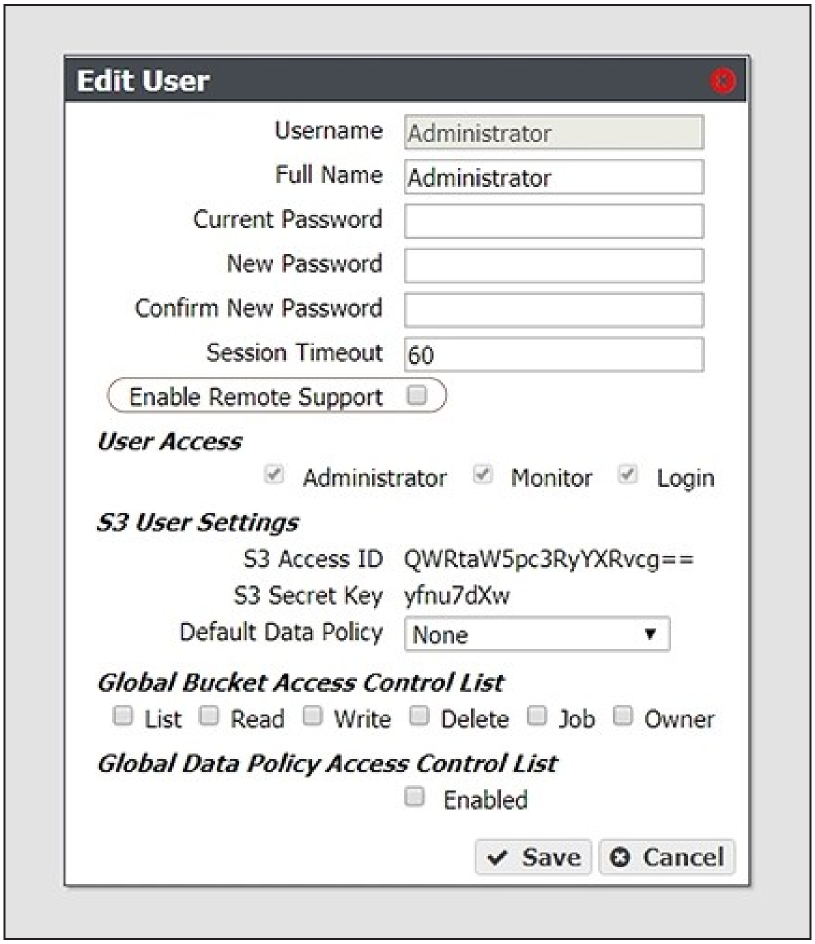
Remote Support is an option that allows Spectra Logic Technical Support personnel to access the root console of the gateway. This option is for troubleshooting purposes only.

Enabling Remote Support

1. Enter the Remote Support activation key as described in Configure Network Connections and Settings on page 280.

Note: The Remote Support activation key is only valid for 24 hours. When the key expires, remote access is automatically disabled.

2. From the menu bar, select **Configuration > Users**. The Users screen displays a list of all configured users.
3. Double-click the **Administrator** account, or select the **Administrator** account, and then select **Action > Edit**. The Edit User dialog box displays.



Username: Administrator
Full Name: Administrator
Current Password:
New Password:
Confirm New Password:
Session Timeout: 60
Enable Remote Support □

User Access
☑ Administrator ☑ Monitor ☑ Login

S3 User Settings
S3 Access ID: QWRtaW5pc3RyYXRvcg==
S3 Secret Key: yfnu7dXw
Default Data Policy: None

Global Bucket Access Control List
□ List □ Read □ Write □ Delete □ Job □ Owner

Global Data Policy Access Control List
□ Enabled

Figure 336 The Edit User dialog box.

4. Select the **Enable Remote Support** check box.

Note: The Enable Remote Support check box does not display until you enter a Remote Support activation key. See Configure Network Connections and Settings on page 280 for more information.

5. Click **Save**.

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. See Disabling Remote Support for more information.

The Remote Support activation key is only valid for 24 hours. When the key expires, remote access is automatically disabled.

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. See Disabling Remote Support for more information.

The Remote Support activation key is only valid for 24 hours. When the key expires, remote access is automatically disabled.

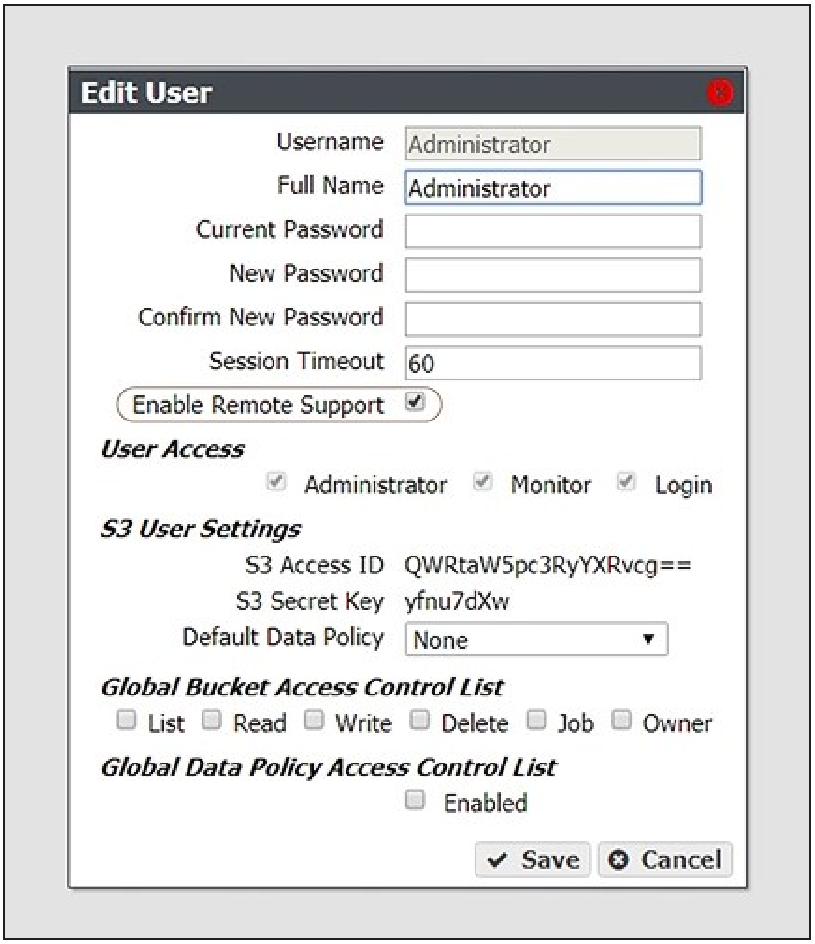
Disabling Remote Support

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. From the menu bar, select **Configuration > Users**. The Users screen displays a list of all users configured on the gateway.

2. Double-click the **Administrator** account, or select the **Administrator** account, and then select **Action > Edit**. The Edit User dialog box displays.



Edit User

Username: Administrator

Full Name: Administrator

Current Password:

New Password:

Confirm New Password:

Session Timeout: 60

Enable Remote Support ☑

User Access

☑ Administrator ☑ Monitor ☑ Login

S3 User Settings

S3 Access ID: QWRtaW5pc3RyYXRvcg==

S3 Secret Key: yfnu7dXw

Default Data Policy: None

Global Bucket Access Control List

□ List □ Read □ Write □ Delete □ Job □ Owner

Global Data Policy Access Control List

□ Enabled

Figure 337 The Edit User dialog box.

3. Clear the **Enable Remote Support** check box.

4. Click **Save**.

APPENDIX A - IPMI CONFIGURATION

This appendix provides instructions for configuring IPMI for the BlackPearl 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 gateway is currently powered on, shut down the gateway as described in Reboot or Shut Down a BlackPearl Gateway on page 451.
2. Connect a monitor and USB keyboard to the rear of the BlackPearl gateway. See Rear Panel on page 44 to locate the monitor and USB connectors.
3. Power on the gateway as described in Power On the Gateway on page 69.
4. 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.

5. If necessary, log into the IPMI interface. The username is **admin**. 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 fields are case sensitive.

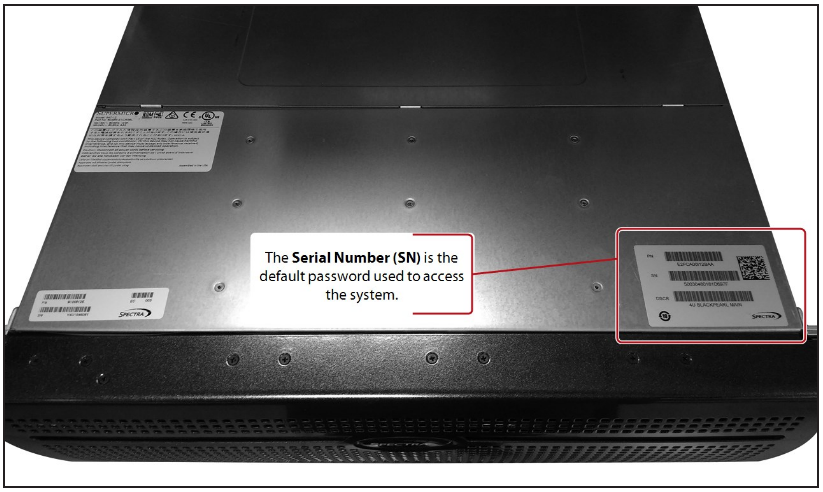
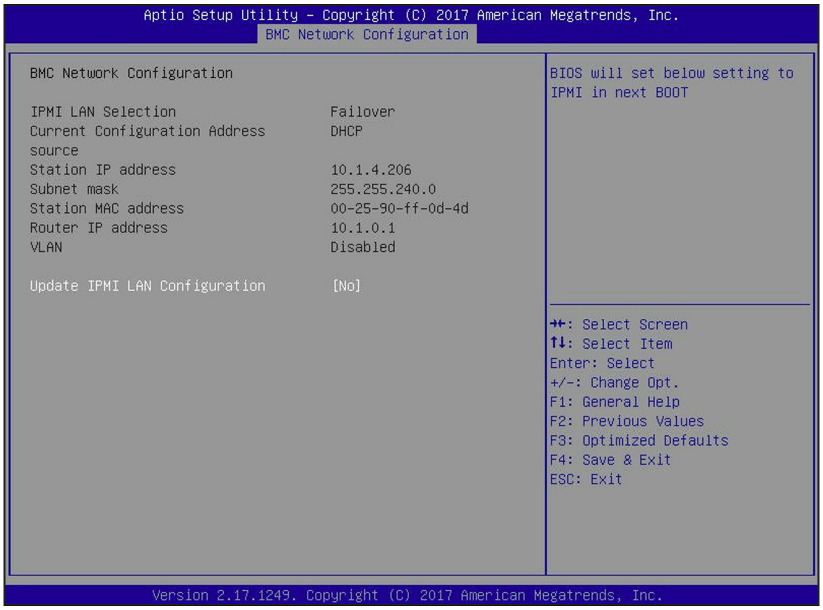

The **Serial Number (SN)** is the default password used to access the system.

Figure 338 The BlackPearl serial number sticker.

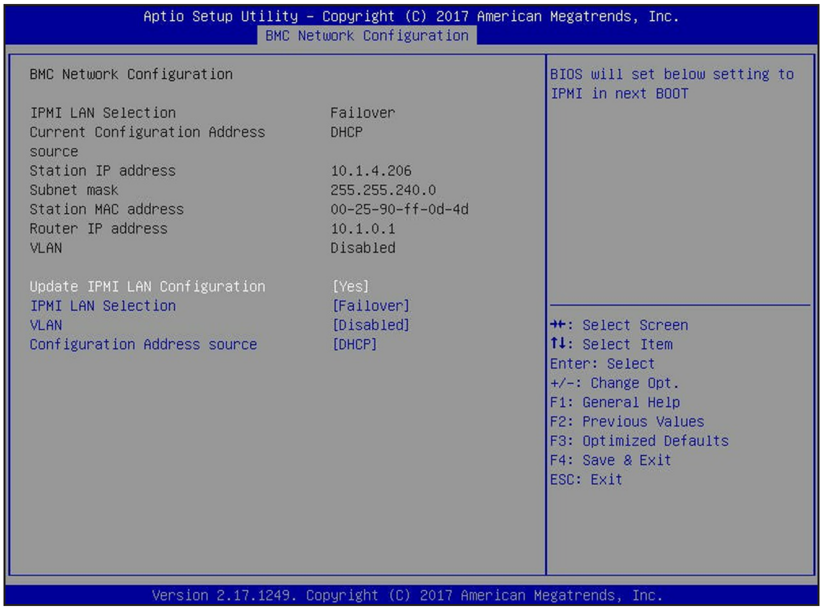
6. Using the keyboard, navigate to the **IPMI** tab and then select **BMC Network Configuration**. The current settings of the BMC configuration display.



```
        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 339 The BMC Configuration screen.

7. Using the keyboard, 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 340 Current IPMI settings.

8. If desired, select **IPMI LAN Selection**. Change the configured setting as needed.

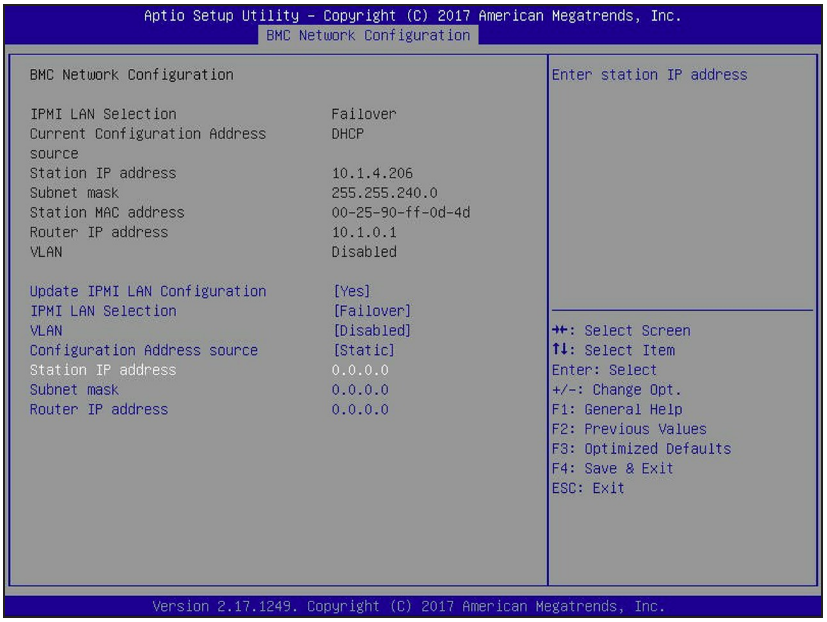
- **Dedicated** - Always uses the dedicated IPMI port for IPMI traffic.
- **Shared** - Always uses the LAN1 port for IPMI traffic.
- **Failover** - On gateway startup, detect if the dedicated IPMI port is connected. If not, the gateway uses the LAN1 port for IPMI traffic.

9. If desired, select **VLAN** to enable or disable VLAN as needed.

10. To change the IPMI address settings, select **Configuration Address source**. The current address source information displays.

11. Select **Static** or **DHCP** addressing.

- If you select **DHCP**, skip to Step 13.
- 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 341 Enter Static IP information.

12. Configure the **Station IP address**, **Subnet mask**, and **Router IP address** with the desired address values.

Note: Only IPv4 addresses are valid.

13. Press **F4** to exit the BIOS and save the entered settings. The BlackPearl gateway reboots.

APPENDIX B - SPECIFICATIONS

This appendix provides detailed specifications for the BlackPearl gateway, 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.

Note: For specifications that differ for the BlackPearl 1.0 chassis, see BlackPearl 1.0 Chassis Overview & Specifications.

Data Storage Specifications **556**

System Specification **560**

Size and Weight **563**

Environmental Specifications **568**

Heat Generation 571

Power Requirements **571**

Input Power Requirements 571

Power Cord Specifications 573

Interface Specifications **577**

System Interface Connectors 578

Expansion Node and Tape Drive Interface Connectors 580

Network Interface Cables 581

Networking Naming Conventions 582

Universal Serial Bus (USB) Support 583

DATA STORAGE SPECIFICATIONS

The following tables show the data storage specifications for the BlackPearl gateways.

Notes:

- 1 TB is defined as 1,000,000,000,000 bytes.
- 1 GB is defined as 1,000,000,000 bytes.

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

Drive Purpose	Drive Type
	• 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 gateways.

Gen2 X Series BlackPearl Gateway

Parameter	Specifications
CPU	One 64-core CPU
System disk drives	Two 480 GB NVMe
Memory	256 GB (8 x 32 GB DIMMs)
Interface connections	• One integrated 1 GigE Ethernet ports [a] • One standard two-port 100 GigE Ethernet card • (Optional) Four-port SAS card [b] • (Optional) Four-port Fibre Channel card [c]

Gen2 V Series BlackPearl Gateway

Parameter	Specifications
CPU	One 16-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 [d] • (Optional) One dual-port 25 Gigabit Ethernet NIC • (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.

[d] One port is available for data transfers, one port is dedicated to the BlackPearl user interface for gateway management.

Gen2 S Series BlackPearl Gateway

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 [a] • (Optional) One dual-port 25 Gigabit Ethernet NIC • (Optional) four-port SAS card [b] • (Optional) four-port Fibre Channel card [c]

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]

[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.

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.

Gen2 X Series BlackPearl Gateway

Parameter	Gen2 X Series BlackPearl Gateway	Shipping Container [a]
Dimensions		
• Height (2U)	3.5 in. (8.9 cm)	TBD
• Width	19 in. (48.3 cm)	
• Depth	29 in. (73.7 cm) [b]	
Maximum Weight Including rail kit [c]	60 lb (27.2 kg)	TBD

Gen2 V Series BlackPearl Gateway

Parameter	Gen2 V Series BlackPearl Gateway	Shipping Container [a]
Dimensions		
• Height (2U)	3.5 in. (8.9 cm)	11.5 in. (29.2 cm)
• Width	19 in. (48.3 cm)	23.7 in. (60.2 cm)
• Depth	33 in. (83.8 cm) [b]	45 in. (114.3 cm)
Weight [c]		
• Empty chassis	72 lb (32.7 kg)	TBD
• Additional for each HDD	1.8 lb (0.8 kg)	
• Additional for each SSD	0.8 lb (0.4 kg)	

[a] Includes chassis, drives, box, and packaging.

[b] Includes the front bezel.

[c] Weights are approximate.

Gen2 S Series BlackPearl Gateway

Parameter	Gen2 V Series BlackPearl Gateway	Shipping Container [a]
Dimensions		
• Height (2U)	7 in. (17.8 cm)	15.9 in. (40.4 cm)
• Width	19 in. (48.3 cm)	23.7 in. (60.2 cm)
• Depth	37.5 in. (95.3 cm) [b]	46.9 in. (119.1 cm)
Weight [c]		
• Empty chassis	99 lb (44.9 kg)	TBD
• Additional for each HDD	1.8 lb (0.8 kg)	
• Additional for each SSD	0.8 lb (0.4 kg)	

Gen1 V Series 2U BlackPearl Gateway

Parameter	Gen1 V Series 2U BlackPearl Gateway	Shipping Container [a]
Dimensions		
• Height (2U)	3.5 in. (8.9 cm)	13.25 in. (33.7 cm)
• 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)

[a] Includes chassis, drives, box, and packaging.

[b] Includes the front bezel.

[c] Weights are approximate.

Gen1 S Series 4U BlackPearl Gateway and 44-Bay Expansion Node

Parameter	Gen1 S Series 4U BlackPearl 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		
• 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]	44.1 in. (112 cm)
	38.5 in. (97.8 cm) [d]	
Weight [e]		
• Empty chassis	TBD	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)	
	21 lb (9.5 kg)	

[a] Includes chassis, drives, box, and packaging.

[b] Includes the front bezel.

[c] Weights are approximate.

[d] Includes optional cable management arm.

[e] Weights are approximate.

Parameter	77-bay Expansion Node	Shipping Container
• Additional for rack mounting kit • Fully loaded chassis with rack mounting kit	TBD	242 lb (110 kg) [a]

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) [b]
• 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 chassis and packaging.

[b] 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

The tables below show the temperature, humidity, and altitude requirements for each chassis.

Gen2 X Series BlackPearl 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)	

Gen2 S Series and Gen2 V Series BlackPearl 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)

[a] When moving the BlackPearl 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 gateway or expansion node in its original packaging. The packaging protects the BlackPearl 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.

Gen1 S Series and Gen1 V Series BlackPearl Gateways, and 44-Bay Expansion Nodes

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 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 gateway or expansion node in its original packaging. The packaging protects the BlackPearl 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
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 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 gateway, result in data loss, or both.

Input Power Requirements

The following tables provide the input power requirements for each gateway or expansion node.

Gen2 X Series BlackPearl Gateway

Parameter	Requirements
Input Voltage	200–240 VAC, 40 A peak, 1600 watts maximum
Input Frequency	50–60 Hz

Gen2 V Series BlackPearl Gateway

Parameter	Requirements
Input Voltage	100-120 VAC, 40 A peak, 800 watts maximum 200–240 VAC, 20 A peak, 800 watts maximum
Input Frequency	50–60 Hz

Gen2 S Series BlackPearl Gateway

Parameter	Requirements
Input Voltage	200–240 VAC, 40 A peak, 1600 watts maximum
Input Frequency	50–60 Hz

Gen1 V Series 2U BlackPearl Gateway

Parameter	Requirements
Input Voltage	100–240 VAC, 11–4.5 A, 920 watts maximum
Input Frequency	50–60 Hz

Gen1 S Series 4U BlackPearl 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 gateways are part of the unit and are not intended for use with any other equipment.

IMPORTANT Confirm the PDU used with the BlackPearl gateway has enough amperage for the power supply in each chassis included in your installation.

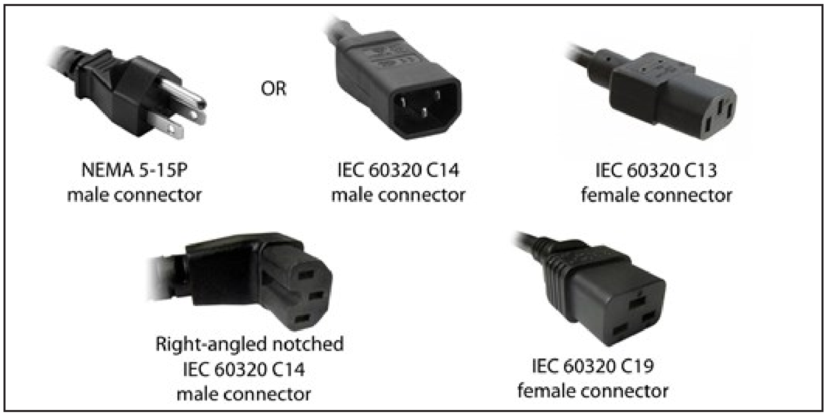
Cables provided by Spectra Logic are between 6 ft (1.8m) to 6.5 ft (2m) in length. If you need to use a longer cord, make sure it conforms to the specifications listed below.

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, 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, 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, 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

INTERFACE SPECIFICATIONS

This section provides information about the interfaces used to connect a BlackPearl gateway to expansion nodes, tape drives, and host systems.

Note: For “Interface Specifications” for the BlackPearl 1.0 chassis, see BlackPearl 1.0 Chassis Overview & Specifications.

System Interface Connectors

Gen2 X Series BlackPearl 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.
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 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 (25 GigE) (Optional)	Two SFP28 optical modules with a duplex LC connector per optional 25 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.

Interface Type	Number of Ports and Connector Type
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 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.
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.
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 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.

Interface Type	Number of Ports and Connector Type
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 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 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 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 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 gateway. Either port can be used for the connection.

Network Interface Cables

The type of cables required to connect the BlackPearl 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.
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.

Interface Type	Cable Requirements
	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 Nearline 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

We:

Spectra Logic Corporation
6101 Lookout Road
Boulder, CO 80301 USA

declare under sole responsibility that the

BlackPearl Converged Storage System

to which this declaration relates, meets the essential health and safety requirements and is in conformity with the EU Directives listed below using the relevant section of the EU standards and other normative documents listed in the following table.

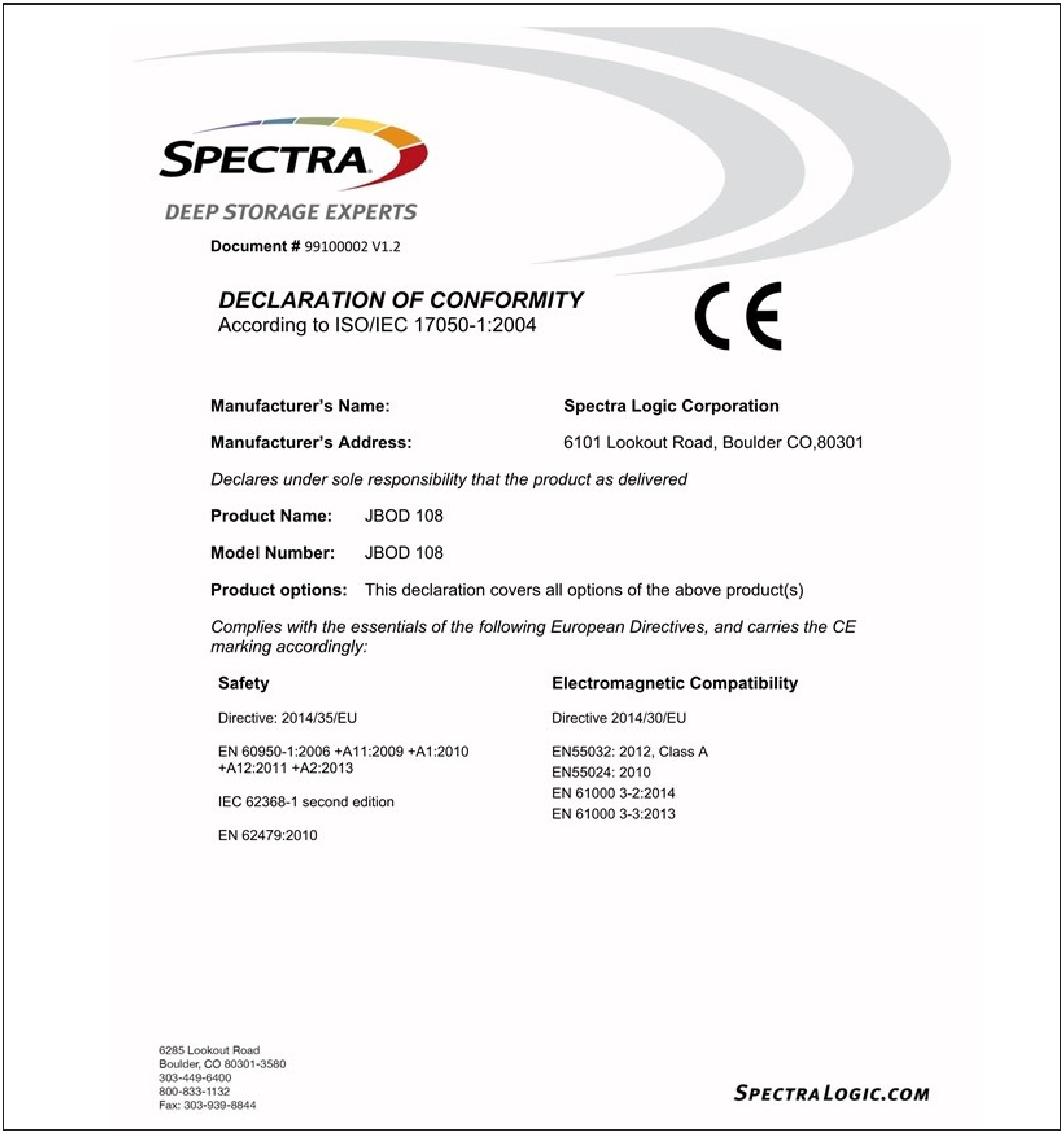
Nicole Gallego

Nicole Gallego

Senior Director of Manufacturing and Quality Operations

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

Directive	Compliance
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.



SPECTRA

DEEP STORAGE EXPERTS

Document # 99100002 V1.2

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

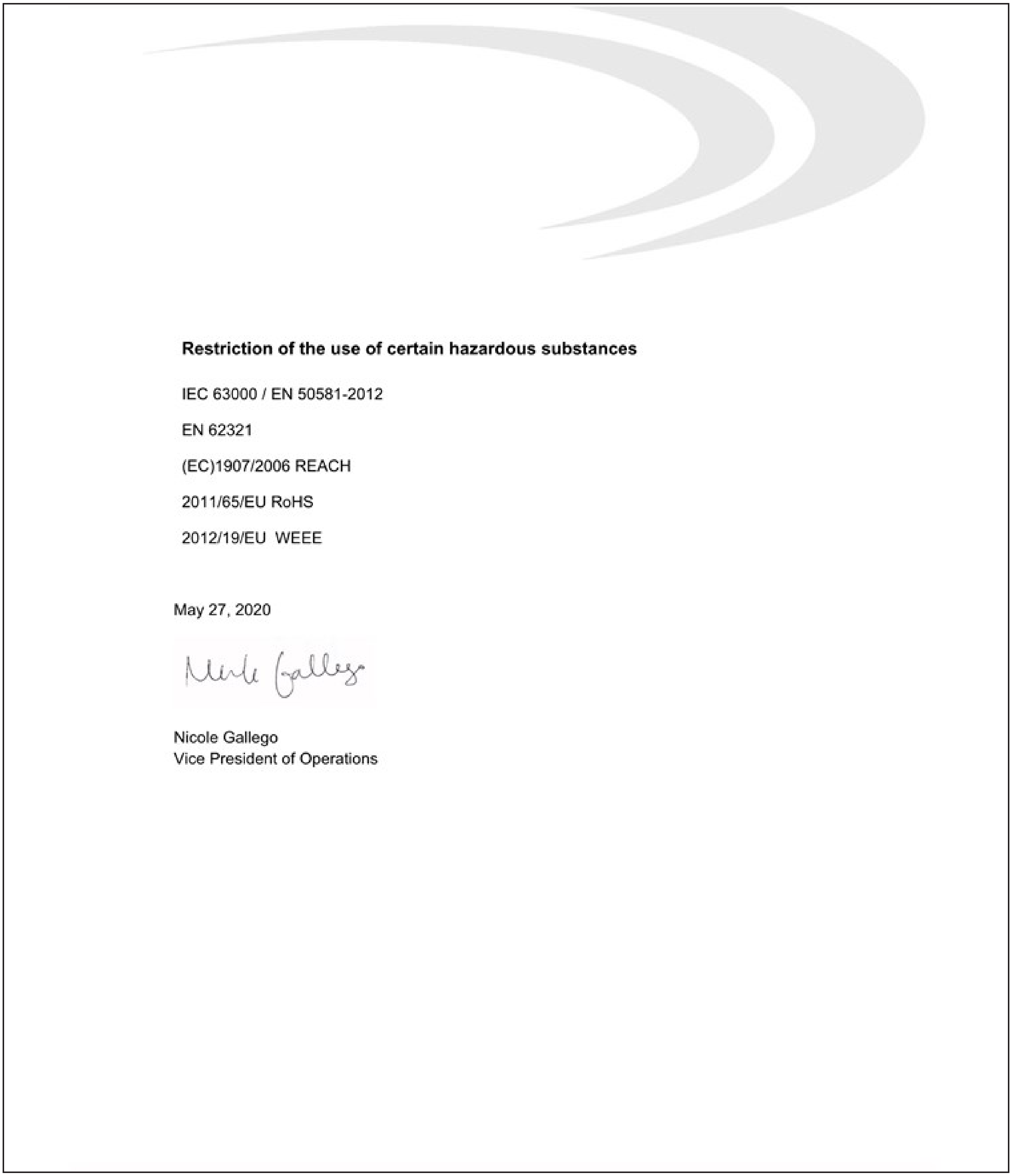
Product Name:	JBOD 108
Model Number:	JBOD 108
Product options:	This declaration covers all options of the above product(s)

Complies with the essentials of the following European Directives, and carries the CE marking accordingly:

Safety	**Electromagnetic Compatibility**
Directive: 2014/35/EU	Directive 2014/30/EU
EN 60950-1:2006 +A11:2009 +A1:2010 +A12:2011 +A2:2013	EN55032: 2012, Class A EN55024: 2010 EN 61000 3-2:2014 EN 61000 3-3:2013
IEC 62368-1 second edition	
EN 62479:2010	

6285 Lookout Road
Boulder, CO 80301-3580
303-449-6400
800-833-1132
Fax: 303-939-8844

SPECTRALOGIC.COM



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

May 27, 2020

Nicole Gallego

Nicole Gallego
Vice President of Operations

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 system 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

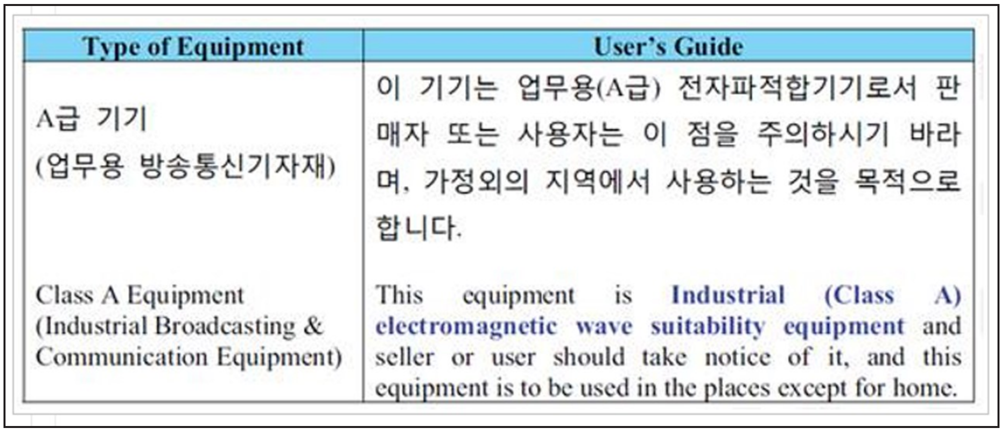
The CE marking is affixed on this device according to Article 10 of the EU Directive 90/336/EEC.

Note: To meet CE certification requirements, you must be running the BlackPearl Nearline 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.

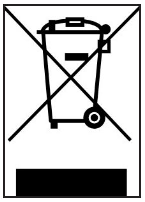
Safety Standards and Compliance

The Spectra BlackPearl Nearline 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.

RoHS
COMPLIANT

Recycling Your System

For information on recycling your Spectra gateway, check the Spectra Logic website at: *spectralogic.com/environment*.

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 *conflictminerals@spectralogic.com*.

APPENDIX D - OPEN SOURCE CODE ACKNOWLEDGMENTS & PACKAGE LIST

This appendix contains the licenses and notices for open source software used in the BlackPearl Nearline 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 9).

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

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

bash-5.1.16

black_pearl-3.0_4

bluestorm_backend-2.0.2959489_7

bluestorm_frontend-2.1.2959489

bluestorm_gui-2.0.2961416_6

bluestorm_mgmt-2.0.2961416

bluestorm_tests-2.0.2886232_1

bluestorm_workers-2.0.2959489_6

boost-libs-1.72.0_7

brotli-1.0.9,1

c-ares-1.18.1

ca_root_nss-3.77

cdbcmd-0.0.1774343,1

compat10x-amd64-10.4.1004000.20181014

compat11x-amd64-11.2.1102000.20181014

ctags-5.8

curl-7.84.0

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

expat-2.4.8

fieldmod-2.0.0.2867631

fio-3.30

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

glib-2.70.4_5,2

gmp-6.2.1

gnome_subr-1.0

gnupg-2.3.3_3

gnutls-3.7.7

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

java-zoneinfo-2021.e

javavmwrapper-2.7.9

ksh93-93.u_1,2

kyua-0.13_6,3

libarchive-3.6.0,1

libassuan-2.5.5

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

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

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-1.20.2_9,2

node16-16.16.0

npth-1.6

openjdk8-8.322.06.1

openldap24-client-2.4.59_4

p4-2016.1.1492381_3

pam_google_authenticator-1.09,1

pcre-8.45_1

pdksh-5.2.14p2_6

perl5-5.32.1_1

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-14.3

postgresql14-contrib-14.3

postgresql14-server-14.3_1

python38-3.8.13

readline-8.1.2

redis-7.0.4

rrdtool-1.7.2_6

ruby-3.0.4,1

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-3.0.0.2959489

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-0.1.0.2933665

rubygem-devstat_stat-0.0.1.1280468

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-1.0.7.2961849

rubygem-freebsd_mps-1.1.1.1325934

rubygem-freebsd_ses-1.3.2.2915144

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-1.0.1.2943746

rubygem-libifconfig-0.1.0.2959489_1

rubygem-libxml-ruby-3.2.2_1

rubygem-live_record-0.2.1.1686790

rubygem-liveresource-2.1.2.2910675

rubygem-loofah-2.16.0

rubygem-lsiexp-1.2.4.2923542

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-1.5.2.2267479

rubygem-passenger-nginx-6.0.12_2

rubygem-pg-1.3.5

rubygem-pkg-config-1.4.7

rubygem-pmbus-1.1.2.1718448

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-2.2.3,3

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-redis-actionpack-rails61-5.3.0

rubygem-redis-activesupport-rails61-5.3.0

rubygem-redis-rack-2.1.4

rubygem-redis-rails-rails61-5.0.2

rubygem-redis-store-1.9.1

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-0.0.2.2714935

rubygem-snmp-1.2.0

rubygem-spectra_acl-1.2.1.2959489_2

rubygem-spectra_cli-1.0.2.2959488

rubygem-spectra_platform-1.3.1.2934439

rubygem-spectra_support-5.0.0.2916870

rubygem-spectra_view-2.3.0.2961416_10

rubygem-spectra_workers-5.0.0.2959488

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-0.1.3.1325934,1

rubygem-stringio-3.0.1

rubygem-sys-uname-1.2.2

rubygem-tape_backend-0.1.2882562

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-0.0.12.2934187

samba413-4.13.17_2

sedutil-1.12.2934263

sg3_utils-1.45

smartmontools-7.3

smp_utils-0.99

source-highlight-3.1.9_1

spectra_ltfs-2.5.0.0.2923343

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

tdb-1.4.3,1

tevent-0.10.2_1

tidy-html5-5.8.0_2

tmux-3.2a

tomcat-native-1.2.24_1

tomcat85-8.5.82

vail-2.0.0.5302_1

verde_hotpair-3.0.2959489

vim-8.2.4669

yarn-1.22.18

zip-3.0_1

zsh-5.8.1

zstd-1.5.2

Index

A

Activation keys

entering manually 338

importing automatically 68

Active Directory, join 226

Amazon S3 data replication rule

about 166

add to data policy 166

delete 192

edit 190

Amazon S3 target

about 143

create 143

Apache, open source acknowledgement 597

autosupport

about 454

configure mail recipient 455

enter contact information 454

B

bezel, removing 486

BlackPearl

components 35, 44, 53

features 29

monitoring 414

overview 28

power 69

serial number 544

size and weight 563

specifications 560

updating 474

BlackPearl data replication rule

about 165

add to data policy 165

delete 192

edit 189

BlackPearl software

current available version 477

BlackPearl target

about 139

create 139

BlackPearl user interface

about 60

current version 475

exit 450

log in 74

menus 60

overview 60

status icons 64

supported browsers 61, 65

bucket

about 171

configure 179

create 171

delete 182

edit 180

bulk TAP, using

correct orientation for magazines 390

door operation 388, 391

export magazines 403

import magazines 388

C

cartridges, exporting or exchanging

export from storage or cleaning partition 399

CE Marking 590

center TAP, using

exporting magazines 401

certificates

configure 334

CIFS

configure service 234

create new share 226

edit share 267

remove sharing 268

set permissions 229

cleaning cartridges, using

export from cleaning partition 399

cleaning cartridges, using with MLM

Cleans Remaining report 503

cleaning partitions, using

export maintenance magazines 399

Cleans Remaining, MLM report 503

component OK icon 64

components

front view 40, 49

rear panel 44, 53

configuring

bucket 179

certificates 334

CIFS service 234

DNS 287

email 288

Ethernet ports 281

mail recipients 455

NAS replication 239

NAS storage pools 213

NAS volumes 217

network connections 280

NFI 235

NFI volume policy 221

NFS service 237

NTP 290

S3 service 292

services 234, 239, 292, 310

shares 226

SMTP 288

snapshots 257

user 323, 329

Conflict Mineral Policy 595

contact information, enter 454

contacting Spectra Logic 9

contacting, Technical Support 544

corporate headquarters, Spectra Logic 9

D

data drive

install new 487

remove 486

data integrity verification

disk pools 465

tape media 467

data persistence rule

about 163

add to data policy 163

delete 197

edit 195

data policy

about 159

create 159

delete 194

edit 193

disk partition

about 130, 137

create 130, 137

delete 205

edit 204

DNS, configure 287

documentation

typographical conventions 25

door, bulk TAP, operating 388, 391

drive, install new 481

DS3

clients 91

online forum 27

E

eccentricity pool

export magazines 399

email

configuring 288

send test 457

Spectra Logic offices 9

error condition icon 64

Ethernet ports, configure 281

EU Declaration of Conformity 585

export or exchange

magazines 399

F

fax numbers, Spectra Logic 9

FCC Notice 591

Free BSD

open source acknowledgement 598

front view 40, 49

H

hardware

monitor status 421

I

icons

component OK 64

error condition 64

information 64

unknown state 64

warning 64

Import/Export TeraPack Magazines screen

using 382

using to export magazines 400

information icon 64

J

Java

open source acknowledgement 599

L

LEDs

data drives 55

library, using

export magazines 399

logging in 380, 398

license agreement, software 3

M

magazines

export 399

inserting into bulk TAP 390

magazines, using

inserting into TAP 384-385

mail recipients

add 455

configure 455

mailing address, Spectra Logic 9

maintenance magazines

export from cleaning partition 399

maintenance, replace component 489

management port, use 281

MIB file, download 301

Microsoft Azure data replication rule

about 168

add to data policy 168

delete 192

edit 191

Microsoft Azure target

about 147

create 147

MLM reports

Cleans Remaining 503

N

NAS replication

cancel replication in progress 271

configure 239

configure schedule 243

configure volumes 241

delete 274

disable 272

edit configuration 273

manual 270

restore files from a replication target 271

NAS storage pools

about 212

create new 213

delete 251

expand 249
options 134, 136, 215
protection levels 134, 136, 216
requirements 213

NAS volumes
about 212
configure 217
create new CIFS share 226
create new NFS share 231
create snapshot 257
delete 256
delete snapshot 262
edit 253
edit share 267
move 252
options 218, 221
remove sharing 268
restore file from snapshot 265
restore snapshot 264
scheduled snapshots 259
snapshot restore 264
snapshots 257

nearline disk pool
import 206

network
cables 581
configure 280
configure DNS 287

NFI
configure 221, 235
edit service 235, 276
restore files 278

NFS
configure service 237
create new share 231
edit share 267
remove sharing 268

Nginx, open source acknowledgement 607

NTP
configuring 290

O

online disk pool
create 134
delete 207
import 206

open source acknowledgement
Apache 597
Free BSD 598
Java 599
Nginx 607
Ruby 608
Ruby on rails 609
ZFS 610

P

partitions, using
export magazines 399

performance metrics 438

phone numbers, Spectra Logic offices 9

pools, see NAS storage pools, nearline disk pools, or online disk pools 212

portal

accessing for technical support 470-471

power

power off 451

power on 69

reboot 451

requirements 571

R

rear panel 44, 53

rear view 42, 51, 57

recycling 594

regulatory

CE Marking 590

Conflict Mineral Policy 595

EU Declaration of Conformity 585

FCC Notice 591

RoHS 593

Safety Standards and Compliance 593

WEEE Directive 593

replication

configure target system 241

replication, see NAS replication 273

reports, MLM

Cleans Remaining 503

RoHS 593

Ruby on rails, open source acknowledgement 609

Ruby, open source acknowledgement 608

S

S3 group

create 329

S3 service

configure 292

Safety Standards and Compliance 593

sales, contacting 9

serial number

where to find 544

services

CIFS 234

configuring 234, 239, 292, 310

NFI 235

NFS 237

status 423

shares

about 212

configure 226

create new CIFS 226

create new NFS 231

delete 268

edit 267

manage 267

SMTP

configure 288

snapshots

about 257

configure 257

create new 257

daily, create 244, 260

delete 262

hourly, create 243, 259

restore 264

retrieve single file 265

scheduled, about 259

weekly, create 245, 261

SNMP service

configure 296, 300

software

license agreement 3

software version

check current available version 477

specifications

data storage 556

environmental 568

power 571

power cords 573

size and weight 563

system 560

Spectra Logic

contacting 9

status lights 416

storage domain

about 150

create 150

delete 187

edit 186

storage domain member

about 156

adding 156

delete 185

edit 183-185

storage partitions, using

export magazines 399

storage pool

export magazines 399

storage pools, see NAS storage pools, nearline disk pools, or online disk pools, 212

support

contacting 544

support portal

accessing 470

support ticket

opening 545

sending 545

system messages 420

system name

edit 291

T

TAP

correct orientation for a magazine 384-385

tape partition

about 138

create 138

technical support

accessing the Technical Support portal 470-471

contacting 9

touch screen interface

logging in 380, 398

typographical conventions 25

U

unknown state icon 64

updates

download 478

USB, support 583

user

configure 323, 329

delete 326

edit 323

types 323, 329

user interface

logging in 380, 398

users

logging in 380, 398

V

Visual Status Beacon, lights 415

volumes, see NAS volumes 212

W

warning icon 64

web interface

logging in 380, 398

website

Spectra Logic 9

WEEE Directive 593

WORM tape media, not supported 96, 138, 343

Z

ZFS, open source acknowledgement 610