Spectra T50*e* Library

User Guide

SPECTRALOGIC.COM

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

Attack Hardened, BlackPearl, BlueScale, RioBroker, Spectra, SpectraGuard, Spectra Logic, Spectra Vail, StorCycle, TeraPack, TFinity, and TranScale are registered trademarks of Spectra Logic Corporation. All rights reserved worldwide. All other trademarks and registered trademarks are the property of their respective owners.

Part Number

90970015 Revision U

Revision History

Revision	Date	Description
N	December 2015	Updated for LTO-7 support.
O	August 2017	Updated for 12.7.03 features.
P	December 2017	Updated for LTO-8 support.
Q	April 2018	Updated for 12.7.07.02 features.
R	August 2018	Updated for 12.7.07.02 features.
S	February 2022	Updated for 12.7.07.04 features.
T	January 2023	Network connectivity updates.
U	October 2023	Updated environmental specifications.

Notes:

- To make sure you have the most current version of this guide check the Spectra Logic Technical Support portal at support.spectralogic.com/documentation/user-guides/.
- To make sure you have the release notes for the most current version of the BlueScale software, check the Spectra Logic Technical Support portal at support.spectralogic.com/documentation/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. 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.

Contacting Spectra Logic

To Obtain General Information

Spectra Logic Website: **www.spectralogic.com**

United States Headquarters

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

European Office

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/documentation**

Contents

About This Guide

This guide describes how to configure, use, maintain, and troubleshoot the Spectra® T50e library (also referred to as the library). It also provides specifications for the library.

Intended Audience

This guide is intended for anyone who uses the Spectra T50e library. The information in this guide assumes a familiarity with performing data backup using tape media. It also assumes familiarity with Fibre Channel, Serial Attached SCSI (SAS), SCSI, and Ethernet connectivity and a knowledge of technical tasks such as installing computer expansion cards, installing drivers, and configuring software.

Product Status

The Spectra Logic® Technical Support portal provides information about which products are currently supported and which are considered discontinued. To view information about discontinued products, log on to the portal (see Accessing the Technical Support Portal on page 472), open the Knowledge Base, and search using the term “discontinuance”.

Related Information

This section contains information about this document and other documents related to the T50e library.

BlueScale User Interface Screens

The BlueScale® interface changes as new features are added or other modifications are made between BlueScale software revisions. Therefore, the screens on your library may differ from those shown in this document.

Additional Publications

For additional information about the Spectra T50e library and its tape drives, refer to the publications listed in this section.

Spectra T50e Library

This guide and the following documents related to the T50e library are available as PDF files on the Spectra Logic website at: support.spectralogic.com/documentations/user-guides.

- The *Spectra T50e Quick Start Guide* provides instructions for installing the library and performing the initial power-on and configuration.
- The *Spectra T50e Rack-mount Kit Installation Guide* provides information about installing the T200 or T380 library in a standard 19-inch, four-post rack.
- The *Spectra T50e Preparing for Shipment Guide* provides information on preparing the library for safe shipment.
- The *Spectra Tape Libraries SCSI Developer Guide* provides information about the SCSI and Fibre Channel commands used in the library.
- The *Spectra Tape Libraries Warnings* document provides all of the warnings found in Spectra tape libraries documentation, in English and 27 other languages.

The following document is available after logging into your Support portal account at: support.spectralogic.com.

- The *Spectra T50e Library Release Notes and Documentation Updates* provide the most up-to-date information about the library, drives, and media.

LTO Ultrium Tape Drives

The following documents provide information that is applicable to all IBM LTO tape drives.

- *IBM Tape Device Drivers Installation and User's Guide*

  Note: This guide also provides information about using the IBM Tape Diagnostic Tool (ITDT) to troubleshoot drive problems.

- *IBM TotalStorage LTO Ultrium Tape Drive: SCSI Reference* (LTO-1 through LTO-4)
- *IBM TotalStorage LTO Ultrium Tape Drive: SCSI Reference* (LTO-5 and higher)

For drive-specific information, search for the product name (for example, LTO 5) on the documentation page on the IBM website. You can also search the IBM Support Portal at ibm.com/mysupport/s/?language=en_US.

Spectra SKLM Server

For additional information that can assist you during the installation and configuration of your server, see the following websites:

- *IBM Security Key Lifecycle Manager welcome page*

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 library, the tape drives, 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.

CHAPTER 1

Library Overview

The Spectra T50e library provides unattended data storage, archiving, backup, and retrieval for environments ranging from small workgroups to multi-server networks.

This chapter provides an overview of the library's features and components. It also provides a functional overview of key features of the BlueScale software and the library hardware.

LIBRARY FEATURES

This section provides an overview of the library's BlueScale user interface and its features. It also provides a detailed description of the library's front panel, interior, and back panel components.

BlueScale Software

The BlueScale software controls all of the resources associated with the library. It provides the user interface used to set configuration options, view information and metrics for the library and drives, manage cartridges, monitor library operations, and troubleshoot and maintain the library and its drives. The BlueScale software also controls the operation of the robotics and drives.

You can access the BlueScale software using either of the following methods:

- The BlueScale operator panel interface—via the touch screen on the library's front panel.
- The BlueScale web interface—via the embedded web server using a standard web browser.

The BlueScale software also controls the operation of the robotics and drives. As part of this function, the information about the location and status of each element in the library, as well as the raw media inventory is stored in non-volatile memory.

In addition to its user interface and control functions, the BlueScale software generates and maintains the Media Lifecycle Management (MLM) database, system logs, and other information related to the current system status. It also handles email operations such as sending the configuration backup file and AutoSupport logs to preconfigured recipients.

See Chapter 3 – Introducing the BlueScale User Interface, beginning on page 71, for detailed information about the features and controls provided by the BlueScale user interface.

Important

Many of the features described in this user guide require your library to be running the most current version of the BlueScale software. Spectra Logic recommends that you keep your library's BlueScale software and component firmware up-to-date at all times. If you are using a previously released BlueScale package, upgrading to the current release is strongly recommended. See Updating the BlueScale Software and Library Firmware on page 421 for detailed information.

The sections on the following pages provide an overview of the management features provided by BlueScale software (listed in alphabetical order).

Auto Configuration Save

The Auto Configuration Save feature automatically generates a weekly backup file and stores the file on the memory card in the LCM. The backup file contains the library configuration and the MLM and DLM databases, as well as the encryption configuration and any BlueScale encryption keys. A backup file is also automatically generated and saved whenever a partition is created or modified. See Back Up the Library Configuration Automatically on page 117 for detailed information about using this feature.

If desired, the library can automatically email the configuration backup file each time it is created. This external copy of the configuration backup file ensures that you can recover your MLM and DLM databases and the library configuration in the event of a disaster. See Email Auto Configuration Save on page 111 for instructions on how to configure email for this feature.

Auto Drive Clean

Auto Drive Clean uses cleaning cartridges stored in a dedicated cleaning partition to provide library-based cleaning of LTO drives without user intervention. The cleaning partition can be shared by multiple storage partitions and is used by the library to automatically clean a drive whenever it indicates that cleaning is needed. Automated drive cleaning results in fewer failed tape read/write operations and is the preferred method for cleaning drives. See Chapter 6 – Configuring and Managing Partitions, beginning on page 159 for detailed information about configuring cleaning partitions.

AutoInstall

A specially prepared USB device is shipped with the library. This USB device contains the current version of the library's BlueScale software and the activation keys for the options you purchased with the library. It is used to automatically update the BlueScale software to and load the activation keys into the library.

The automated installation process begins when you insert the USB device into the library's LCM before you power-on the library for the first time during installation. The user interface provides feedback to track the progress during the process. See Perform the AutoInstall on page 62 for more information on the AutoInstall process.

AutoSupport

AutoSupport configures the library to automatically contact library users with system messages whenever specific events occur. It can also be used to open or update a support ticket and send it to a specified email recipient or to Spectra Logic Technical Support. See Chapter 11 – Configuring and Using AutoSupport, beginning on page 334 for detailed information.

Diagnostic Tools

Diagnostic tools, such as trace collection tools, and utilities are available through the BlueScale interface. Selecting utility displays additional information, including whether or not it can be run while the library is operating.

Important In general, the library advanced utilities are only for use under the direction of Spectra Logic Technical Support.

Drive Lifecycle Management

BlueScale Drive Lifecycle Management (DLM) helps you identify drives that are experiencing high error rates or other problems. DLM is automatically enabled when Media Lifecycle Management (MLM) is enabled. See Chapter 9 – Using Drive Lifecycle Management, beginning on page 279 for detailed information.

Encryption Key Management

The Spectra T50e library can encrypt data and manage encryption keys, using either BlueScale key management or the Spectra SKLM key management system.

Spectra SKLM is a stand-alone, centralized key manager, while BlueScale encryption key management is tightly integrated into the BlueScale environment. Encryption is performed through encryption-enabled drives.

See Chapter 10 – Encryption and Key Management, beginning on page 289 for detailed information about encryption.

EnergyAudit Reporting

The BlueScale EnergyAudit feature lets you display and record the estimated power consumption by the library. See Monitoring Your Library on page 142 for more information about energy reports.

Global Spare

The BlueScale Global Spare feature provides a way to remotely substitute an available Fibre Channel LTO-4 or later generation drive in the library for a failed drive of the same type. The feature lets you configure an installed drive as a designated spare for other drives in the library. This drive can then be substituted for a failed drive in any partition that is configured to use the Global Spare drive. When a drive fails, you simply log into the library, select the Global Spare option for the failed drive, and continue normal operations. You can then physically replace the failed drive at your convenience.

See Assign a Global Spare Drive on page 179 for instructions on how to configure a Global Spare drive and Using a Global Spare Drive on page 409 for more information.

Hardware Health Monitoring

BlueScale Hardware Health Monitoring (HHM) provides basic information about power-on hours and robotic moves.

Media Lifecycle Management

BlueScale Media Lifecycle Management (MLM) helps you manage your data cartridges by giving you tools to pro-actively detect potential media errors well before they happen. See Chapter 6 – Configuring and Managing Partitions, beginning on page 159 and Chapter 8 – Configuring and Using Media Lifecycle Management, beginning on page 233 for detailed information about configuring and using the MLM features.

Remote Failure Recovery Management

Failure recovery can be managed remotely by using the BlueScale web interface to reset a drive or reboot the library.

Remote Support

The remote support feature uses a remote web access application, WebEx®, to facilitate remote problem diagnosis. Remote support preserves your organization's site and data security, giving Spectra Logic Technical Support limited access to your library. With WebEx, Technical Support can "drive" the library, taking enough control to gather the data required to speed understanding of the problem. See Remote Support Icon on page 82 for more information.

Shared Library Services (SLS) Partitioning

The library uses Shared Library Services (SLS) virtualization technology to partition the library into a maximum of four virtual libraries. SLS partitioning is an option you can add to the library by purchasing an activation key from Spectra Logic. See Chapter 6 – Configuring and Managing Partitions, beginning on page 159 for information about how partitions function in the library and detailed instructions for configuring and using partitions.

Library Component Overview

The following sections show the locations of and briefly describe the library's major front panel, internal, and rear panel components.

Front Panel Components

Figure 1 shows the library front panel components.

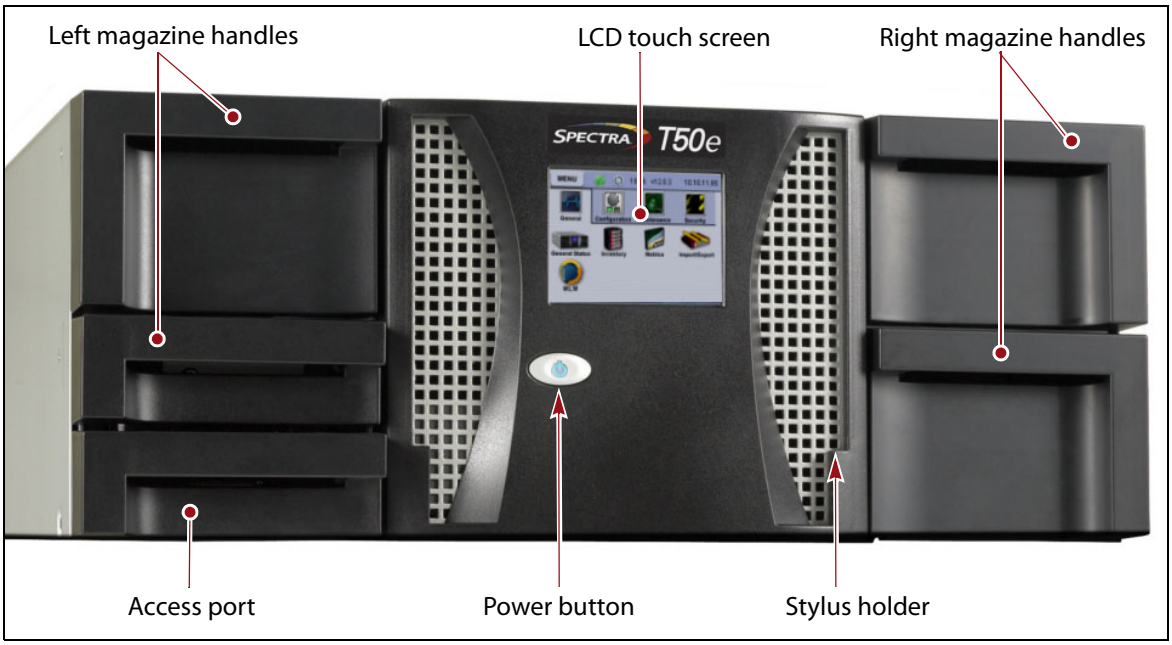
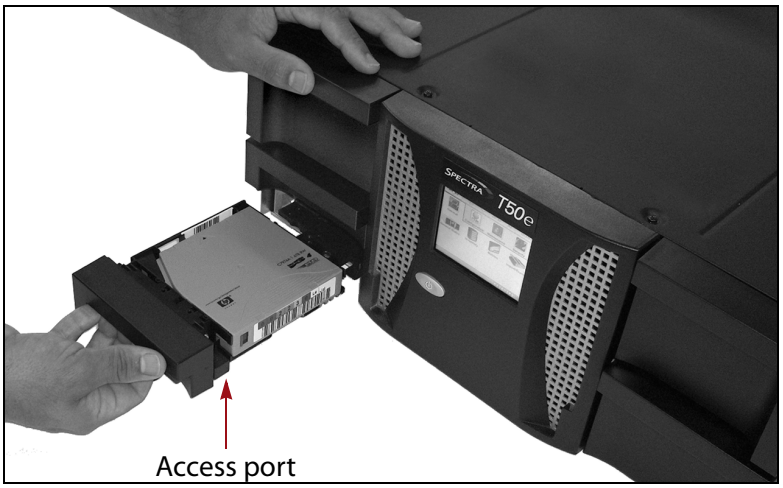


Figure 1 Library front panel components.

Component	Description
LCD Touch Screen and Stylus (not shown)	The library's touch screen provides access to the BlueScale user interface through the Library Control Module (LCM). A stylus for making selections and typing entries on the touch screen can be conveniently stored near the screen. See Touch Screen Operator Panel on page 31 for detailed information. See Chapter 3 – Introducing the BlueScale User Interface, beginning on page 71 for detailed information about the BlueScale user interface.
Power Button	The power button provides on/off control of the library. See Controlling the Library Power on page 140 for usage information.
Magazine Handles	The magazine handles let you slide individual magazines into and out of the library. The magazines must be unlocked through the user interface before they can be removed. See Interior Components for information about the magazines.

Component	Description
Access Port	The bottom front of the lower left magazine is the access port, which contains the Entry/Exit (E/E) slot used for importing or exporting a single cartridge.  **Figure 2** Location of the access port. ▪ **Importing** — You can use the access port to import a single cartridge into the library. When the BlueScale software opens the access port, the E/E slot is exposed to let you insert a cartridge. When you close the access port, the slot slides back into the magazine where it can be accessed by the robotics. ▪ **Exporting** — When exporting cartridges from the library, the robotics moves the requested cartridge to the E/E slot. You then use the BlueScale user interface to open the access port and remove the cartridge. See Chapter 7 – Using Cartridges in the Library, beginning on page 197 for information about using the access port.

Interior Components

Figure 3 shows the interior components of the library.

Note: The interior components of the library are shown for reference only. They are not accessible during normal operation.

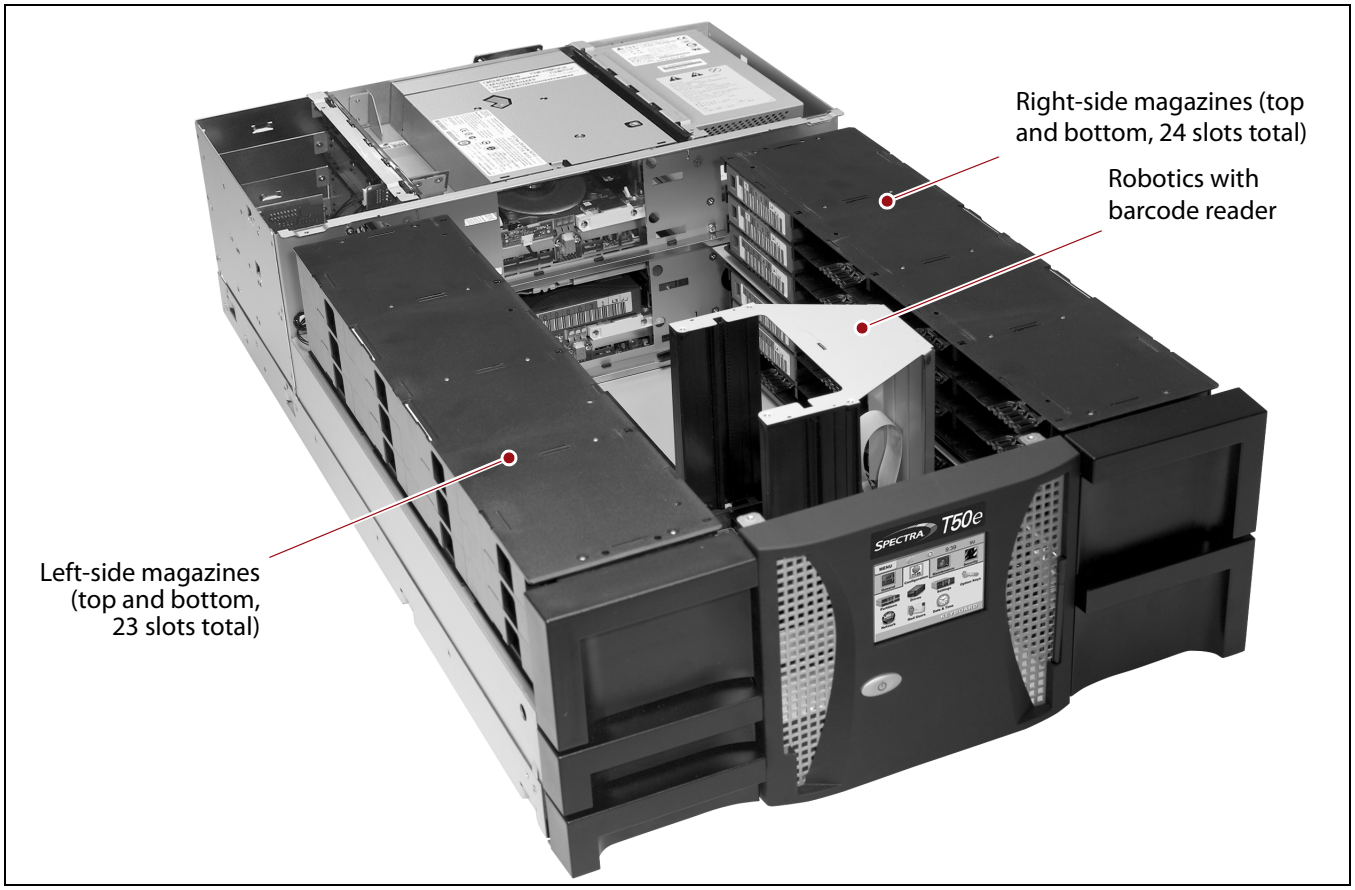


Figure 3 Library interior components.

Component	Description
Magazines	The magazines provide the storage slots for the cartridges inside the library. Magazines along each side of the library contain slots for storing cartridges. The two magazines on the right side of the library and the top left magazine each contain twelve slots. The lower left magazine has eleven slots, leaving space for the one-slot access port at the front of the library. The default library configuration has 10 slots licensed. You must purchase an activation key to license the additional slots (see Capacity-On-Demand (CoD) on page 496).
Robotics	The robotics perform all cartridge moves within the library.
Barcode reader	The integrated barcode reader mounted on the robotics reads the barcode labels on individual cartridges. The library uses the barcode label information to maintain an inventory of the cartridges currently stored inside the library.

Rear Panel Components

Figure 4 shows the rear panel components of the library.

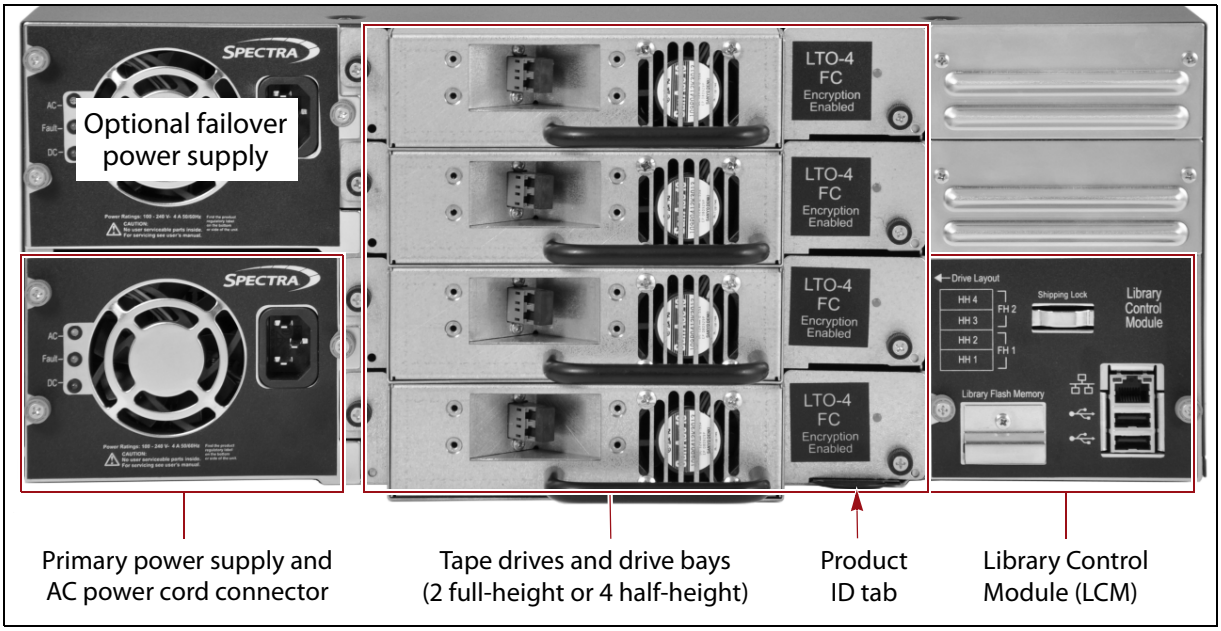
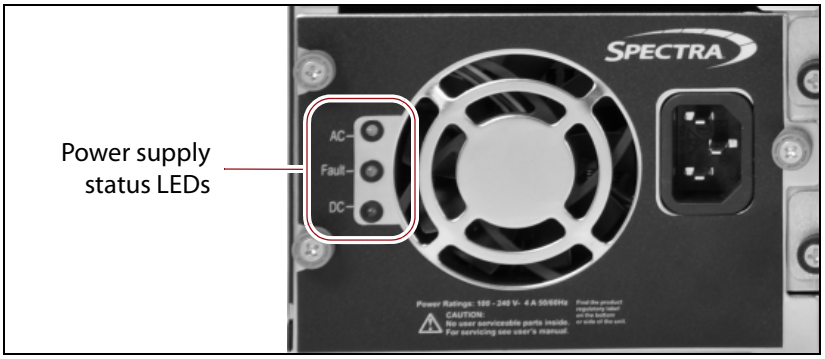


Figure 4 Library rear components (four half-height FC tape drives and redundant power supplies shown).

Component	Description
Power Supplies and AC Connectors	The library includes a primary power supply to convert the AC input to provide the 5 VDC and 12 VDC power used by the robotics and drives. It also provides power to the LCD operator panel.  **Figure 5** The 5/12 VDC power supply LEDs. Each AC power supply includes an AC power cord connector for connecting the library to an AC power source and three status LEDs. ▪ **AC—Blue:** The AC power is on and functioning normally. ▪ **Fault—Orange:** The power supply has a fault condition (normally off). ▪ **DC—Green:** The DC power is on and functioning normally A second, optional power supply provides N+1 redundancy and failover protection. To learn more, see Redundant Power Supplies on page 36. **Note:** When only one power supply is installed, the second bay has a cover installed to maintain proper air circulation through the library.

Component	Description
Tape Drives and Drive Bays	The library accommodates one or two full-height LTO tape drives or from one to four half-height LTO tape drives for data backup. You can also install one full-height drive and two half-height drives. To learn more, see LTO Tape Drives on page 32. **Note:** Any drive bays that do not have drives installed have covers installed to maintain proper air circulation throughout the library.
Product ID	The product ID tab slides outward from the bottom of the library and shows the library serial number.
Library Control Module (LCM)	The LCM is a dedicated on-board computer module that runs the BlueScale software that controls all aspects of library operation. To learn more, see Library Control Module (LCM) on page 35.
Expansion Slots (not shown)	Optionally, up to three half-height drive bays can be replaced with capacity expansion slots if they are not used for tape drives (see Installing Capacity Expansion Slots (Optional) on page 60).
Rack-mount Hardware (not shown)	The library is designed to mount in a standard 4-post, 19-inch rack using just 4 units (4U) of rack space. Alternatively, the library can be placed on a level tabletop or other level horizontal surface. See Install the Library in a Rack on page 45 for important information.

Touch Screen Operator Panel

The touch screen operator panel on the front of the library provides local access to the BlueScale user interface. You can select options and enter information by simply touching the appropriate location on the screen. The touch screen includes a soft keyboard that you can use to enter alphanumeric characters into text fields. Read Chapter 3 – Introducing the BlueScale User Interface, beginning on page 71 for detailed information about the BlueScale user interface.

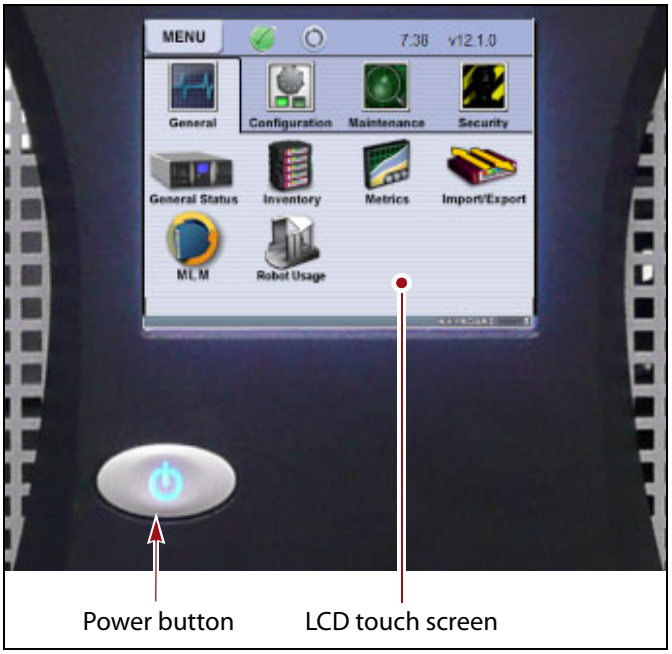


Figure 6 The library operator panel displaying the BlueScale user interface.

Component	Description
LCD touch screen	The 3.4-inch color LCD touch screen lets you monitor library operations and select configuration options using the BlueScale user interface.
Power Button	The power button provides front panel on/off control of the library.

LTO Tape Drives

The library accommodates up to two full-height tape drives or up to four half-height tape drives. It supports IBM LTO-3 and later generation Ultrium tape drives.

The drives are installed in drive bays located at the back of the library (see Figure 4 on page 29) and are easily accessible. Thumb screws on the drive sled face plate secure the drive in its bay.

- See Installing the Tape Drives on page 52 for information about installing or replacing tape drives.
- See LTO Tape Drive Specifications on page 508 for information about the transfer rates and storage capacities of LTO tape drives.

Drive Sled

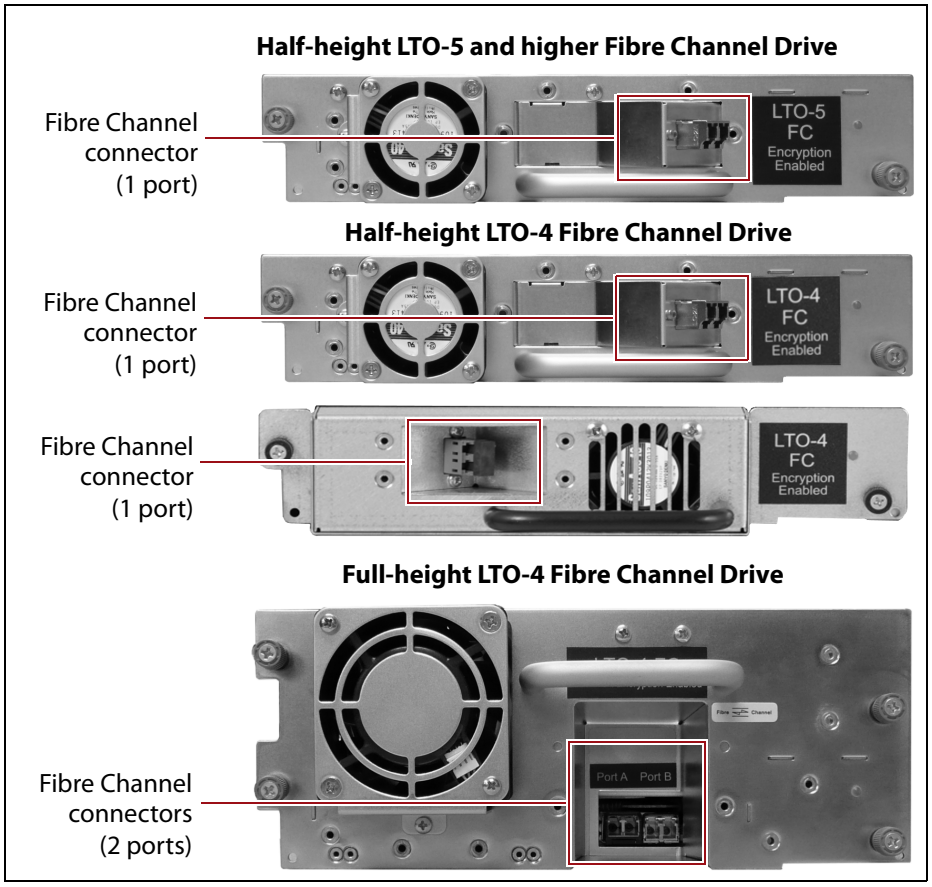
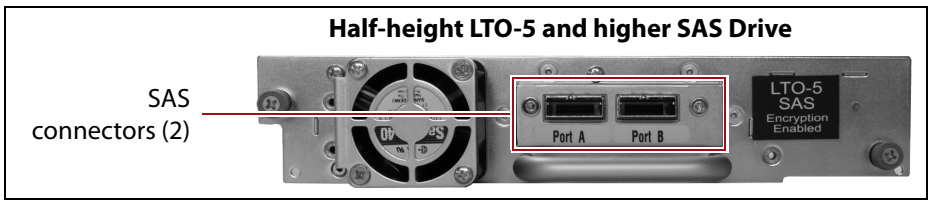
Each drive is mounted in a drive sled which provides the electrical and logical connections to the library, as well as the connections to the host interface used to access each drive. The drives are hot-swappable to provide uninterrupted operation.

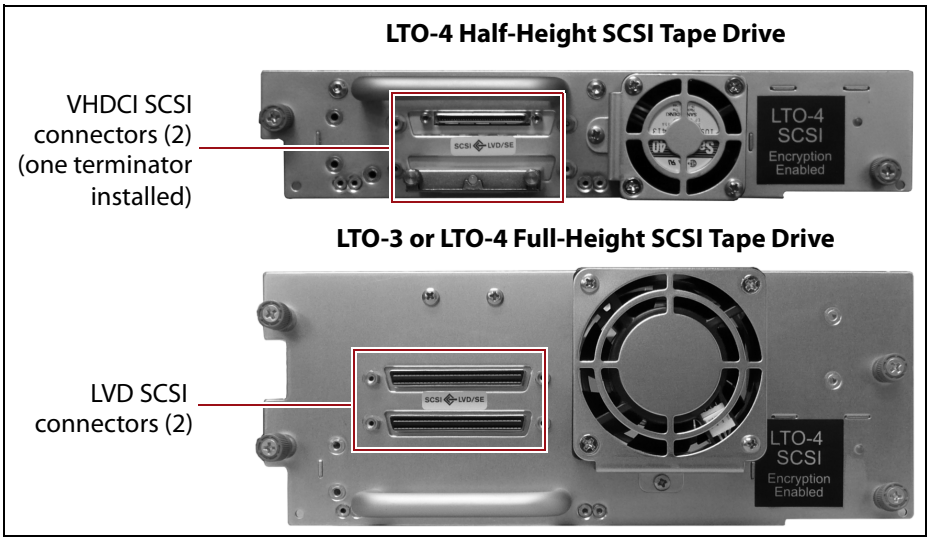
The Drive Control Module (DCM) in the sled assigns an identifier to the drive based on its location in the library (see BlueScale Drive Identifiers on page 154). This identifier is used by the library to identify the drives in the BlueScale interface.

Drive Interface Ports

The method used to connect the library's drives to the network depends on the type of network and the drive interface. The drive sleds have either a Fibre Channel, Serial Attached SCSI (SAS), or LVD SCSI interface.

The following table describes the ports on each type of drive interface.

Interface	Description and Location
Fibre Channel	The Fibre Channel drives use fiber optic multi-mode LC SFPs to provide connectivity for the drive. ▪ Each half-height LTO-4 and later generation Fibre Channel drive is equipped with one fiber optic multi-mode LC SFP. ▪ Each full-height LTO-4 Fibre Channel drive is equipped with two fiber optic multi-mode LC SFPs. The two ports let you connect two separate fiber optic cables to each drive. Only one connection can be active at any time. See Drive Connectivity Failover on page 37 for additional information. **Note:** The position of the single fiber optic multi-mode LC SFP changed in newer half-height LTO-4 Fibre Channel drives. It is now in the same position as for the LTO-5 and later generation drives.  **Figure 7** Fibre Channel tape drive interface connectors.
Serial Attached SCSI (SAS)	Each SAS drive sled has two, unshielded, dual-port SFF-8088 serial connectors that provide the Serial Attached SCSI (SAS) connectivity for the drive.  **Figure 8** SAS tape drive interface connectors.

Interface	Description and Location
SCSI	Each SCSI drive sled has two LVD SCSI connectors. One connector is cabled directly to the host SCSI HBA. The remaining connector always has an LVD SCSI terminator installed. **Important:** Spectra Logic does not support daisy-chaining LTO-4 SCSI drives. LTO-3 SCSI drives can be daisy-chained, but must be limited to two drives on a single SCSI bus. Daisy-chaining other devices on the same SCSI bus as a drive is not supported. ▪ Half-height SCSI drives have two female 68-pin VHDCI Ultra-4 LVD SCSI connectors. ▪ Full-height SCSI drives have two female 68-pin Micro-D Ultra-3 LVD SCSI connectors. ▪ Each drive sled has one LVD SCSI terminator installed on the bottom connector.  **Figure 9** SCSI tape drive interface connectors.

Library Control Module (LCM)

The library uses a dedicated on-board computer module called the Library Control Module (LCM) to run the BlueScale software that controls and manages all aspects of the library operation.

Figure 10 shows the external components on the LCM.

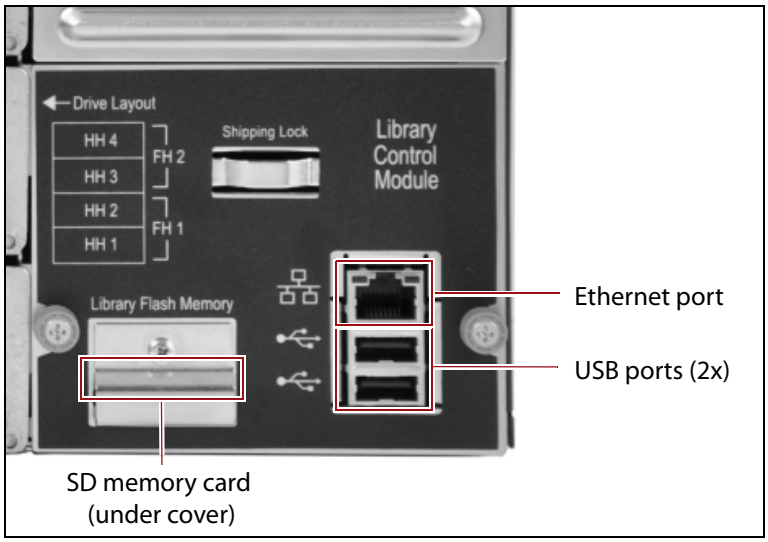


Figure 10 Library Control Module (LCM) components.

The following table describes the components shown in Figure 10.

Component	Description
Ethernet Port	The Ethernet port is used to connect the library to an Ethernet network, providing access to the library through the BlueScale web interface. The library also uses the Ethernet port to send automatic email alerts using Simple Mail Transfer Protocol (SMTP). See Interface Cable Requirements on page 506 for Ethernet cable requirements.
USB Ports (2)	The USB ports on the LCM can be used to connect a USB device for transferring BlueScale encryption keys, saving configurations, and uploading BlueScale packages. You can also connect a USB keyboard to the USB ports and use them when interacting with the BlueScale user interface. This connection provides access to all of the options available from the library's front panel touch screen. See Universal Serial Bus (USB) Support on page 507 for USB device requirements.
Memory Card	The memory card in the module stores the library's operating system, the BlueScale software, and the library configuration information, which includes activation keys, system settings, and partition settings. It also stores the MLM and DLM databases and information related to the current system status. **Note:** One extra memory card is shipped with new libraries for error recovery.

HIGH-AVAILABILITY FEATURES

The following sections describe the high-availability features of the library. These features help keep the library operating even in the event of a component failure or a network connection failure.

Global Spare Drives

The BlueScale Global Spare feature provides a way to remotely substitute an available Fibre Channel LTO-4 or later generation drive in the library for a failed drive of the same type. The feature lets you configure an installed drive as a designated spare for other drives in the library. This drive can then be substituted for a failed drive in any partition that is configured to use the Global Spare drive. When a drive fails, you simply log into the BlueScale web interface from any location, select the Global Spare option for the failed drive, and continue normal operations. You can then physically replace the failed drive at your convenience. See Assign a Global Spare Drive on page 179 and Using a Global Spare Drive on page 409 for more information.

Redundant Power Supplies

The library requires one 5/12 VDC power supply in order to operate. Installing a second power supply, which includes an additional AC power input, provides N+1 redundancy and failover protection. The power supply modules needed for the N+1 power redundancy configuration are an option that you can purchase separately or when you order the library (see Power Supplies on page 497).

If a redundant power supply is used, the AC power connectors for each power supply module should be connected to independent AC branch circuits, which allows for failover in the event of a power failure in one of the circuits.

Drive Connectivity Failover

The full-height LTO-4 Fibre Channel drives are equipped with two Fibre Channel ports. The two Fibre Channel ports cannot be used simultaneously to provide redundant data paths between the hosts and the drive. However, they can be used to provide failover capability in the event that communication to the port currently in use is interrupted. This failover can be accomplished in one of the following ways:

- Manually disconnect the fiber optic cable from the failed port and connect it to the other port. You may need to reconfigure your host software to recognize the alternate port.
- Connect each port on the drive to a separate Fibre Channel HBA in the host. You can also use a dual-port Fibre Channel HBA. Configure one HBA (or HBA port) as the primary connection and the other HBA (or HBA port) as the failover connection. Install failover software on the host computer to control the transfer of I/O from one HBA to the other in case of a failure. You may also need to configure your storage management software to correctly recognize both ports. Refer to your failover software, HBA, and storage management software documentation for instructions.
- Connect each port on the drive to a separate Fibre Channel HBA in the host. You can also use a dual-port Fibre Channel HBA. Configure one HBA (or HBA port) as the primary connection and the other HBA (or HBA port) as the failover connection. Install failover software on the host computer to control the transfer of I/O from one HBA to the other in case of a failure. You may also need to configure your storage management software to correctly recognize both ports. Refer to your failover software, HBA, and storage management software documentation for instructions.

  Note: Tape drives sold by Spectra Logic do not support MPIO.

CHAPTER 2

Installing the Library

This chapter describes how to install the T50e library and log into the user interface for the first time.

PREPARING FOR THE INSTALLATION

Before beginning the installation, complete the requirements described in the following sections.

Prepare the Location

Before unpacking and installing the library, confirm that the location meets the following requirements:

Requirement	Description
Acclimation	▪ Library — If the temperature in the room where the library is to be installed varies by 30° F (15° C), from the location where the library was stored, allow the library to acclimate to the new temperature for a minimum of 12 hours after unpacking and before installing the library. ▪ Media — It is important to acclimate media to the ambient environment for 24 hours before loading it into the library.
ESD	Ensure that the work area is free from conditions that could cause electrostatic discharge (ESD). Discharge static electricity from your body by touching a known grounded surface, such as a computer's metal chassis.
Location	Ensure that the installation location is properly prepared with network connections ready for use, adequate clearance for ventilation, minimal dust and debris, and proximity to an appropriate AC power source. ⚠ **CAUTION:** The maximum ambient temperature of the library is 95° F (35° C). Make sure that you select a location where the air vents at the front of the library and the fans at the back of the library are not blocked. The library requires unobstructed airflow to stay properly cooled.
Rack-mounted installation	If you plan to rack-mount the library, make sure that an appropriate rack is assembled. ▪ The library is designed to fit in a standard 19-inch, 4-post rack that is at least 43 inches (110 cm) deep. Two-post racks are not supported. ▪ Allow an additional 6 inches (15 cm) at the back for cable clearance and 12 inches (30 cm) at the front for the access port. ▪ For accessibility, mount the library in the middle of the rack (near eye level, if possible). ⚠ **CAUTION:** The rack must be located on a level, hard-surfaced floor such as cement or tile. Do not place the rack on a carpeted floor or anywhere else that poses risk for static discharge that could damage your library and its drives.
Tabletop installation	If you plan to place the library on a tabletop or desk, make sure that the surface is level and sturdy enough to support the fully loaded library (up to 60 lb or 27 kg).

Prepare the Hosts

Use the following guidelines to prepare the host computer(s) that connect to the library.

Note: Compatibility information is available at www.spectralogic.com/compatibility.

Requirement	Description

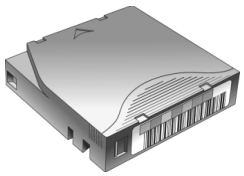
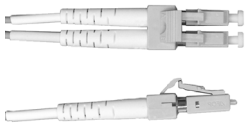
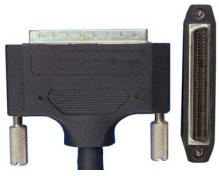
Connections to the library and drives	Install a suitably rated Fibre Channel switch and/or a host bus adapter (HBA) in each host computer.
	▪ **Fibre Channel (FC)**
	  ▪ LTO-7 Fibre Channel drives attempt to connect at 8 Gb/s, but auto-negotiate down to 4 Gb/s, or 2 Gb/s, depending on host requirements.
	  ▪ LTO-5 and LTO-6 Fibre Channel drives attempt to connect at 8 Gb/s, but auto-negotiate down to 4 Gb/s, 2 Gb/s, or 1 Gb/s, depending on host requirements.
	  ▪ LTO-4 Fibre Channel drives attempt to connect at 4 Gb/s, but auto-negotiate down to 2 Gb/s or 1 Gb/s, depending on host requirements.
	▪ **SAS** — LTO-5 and higher SAS drives attempt to connect at 6 Gb/s, but auto-negotiate down to 3 Gb/s depending on host requirements.
	▪ **SCSI** — LTO SCSI drives support connecting to either an Ultra160 or an Ultra320 LVD SCSI HBA. For optimum performance, use an Ultra320 LVD SCSI HBA. Do not connect any disk devices to the same HBA port used for the library; disk and tape drives must be on a different HBA or different ports on the same HBA.
	Important: Daisy chaining LTO-4 SCSI drives is not supported (see Connection Guidelines on page 58 for information about daisy-chaining LTO-3 SCSI drives).

Host	**SCSI drives only.** When connecting SCSI drives to the host, Spectra Logic recommends that you power off the host computer(s) until the library is installed and the initial configuration is complete.
LUN support	Make sure that multiple LUN support is enabled on the host operating system and HBAs. One drive in each partition is used to provide the control path to the library's robotics. The motion commands from the host are routed to the robotics through LUN 1 of one of the drives in the partition. The drive reports the robotics as "SPECTRA PYTHON" on LUN 1. LUN 0 is the drive itself. **Notes:** ▪ Do not use an LVD SCSI HBA that does not support multiple LUNs. ▪ Do not use a SCSI RAID controller unless the RAID support is disabled.
Drivers and software	Make sure that any necessary device drivers and the storage management software are compatible with the library and the drive(s). See Updating Drive Device Drivers on page 462 for information about device drivers. **Note:** The storage management software can be installed on the host computer before or after the library is installed. However, if the software is installed first, you may need to reconfigure it for use with the library after library installation is complete.

Gather the Accessories

Make sure you have the accessories listed in the following table.

Note: You need to acquire the interface cables that were not included with the library. You can purchase cables from Spectra Logic at the same time you purchase the library. See Interface Specifications on page 504 for detailed information about the required cables.

Accessory	Description	
Cartridges	Use only data cartridges and cleaning cartridges designed specifically for LTO Ultrium tape drives. See: ▪ LTO Cartridge Specifications on page 512 ▪ Spectra Certified Media on page 493	
Drive interface cables and accessories	**Fiber Optic Cables** (Fibre Channel drives only) ▪ One multimode optical cable with multi-mode, fixed, optical LC connector for each drive. ▪ If the drive has two Fibre Channel ports, a second fiber optic cable is required in order to configure fail-over. However, only one port at a time can be active. ▪ If your Host Bus Adapter or Fibre Channel switch has an SC interface, you need an LC-to-SC Optical cable.	
	SAS Cables (SAS drives only)—One SFF-8088 SAS cable rated for 6 Gb/s that does not exceed 13 feet (4 m) for each drive.	
	SCSI Cables (SCSI drives only) ▪ One cable that does not exceed 39 feet (12 m) for each drive ▪ Full-height SCSI drives have high-density (HD), wide (68-pin), LVD SCSI connectors. ▪ Half-height SCSI drives have VHDCI connectors.	 68-pin LVD  VHDCI

UNPACKING THE LIBRARY

The library and its components are shipped in cardboard boxes. The only tool you need to unpack the library is a pair of scissors or a box cutter.

Prepare the Unpacking Location

Set the boxes in a location that gives you adequate clearance around and above them so that you can safely unpack the library. After removing the library from its packaging, move it to a work space where you have access to all four sides.

WARNING The library is heavy (see product specifications for details). Use extreme caution and proper equipment when moving the library. Do not install components in the library until it is secured in the rack.

Unpack the Library

Save all of the original packing materials in case you need to ship or move the library later.

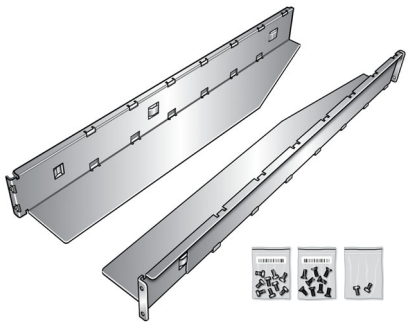
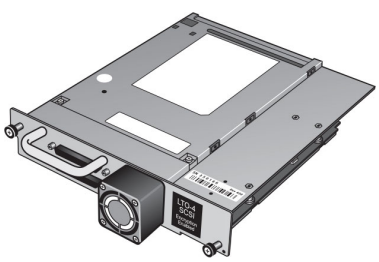
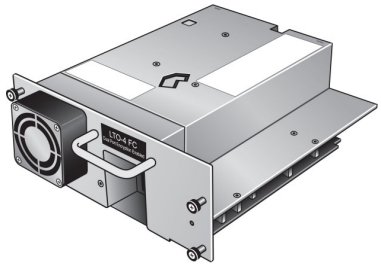
Note: Make sure that you have a work space area prepared before you remove the library from its shipping box.

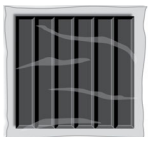
1. Open the library shipping box.
2. Remove the rack mounting rails, the accessories, and the documentation packet, and set them aside.
3. Remove the protective foam and the plastic cover from the library.
4. Lift the library out of the box and move it to the location where it is to be installed. Make sure that you have access to all sides of the library.

Inventory the Components

Unpack and identify the components that shipped with the library using the following table for reference. You typically are not provided all of the components listed in the table. The contents you receive depend on which options were purchased.

Note: Drives and media are shipped separate from the library.

Component	Description
Rack-mount kit	 One rack-mount kit is supplied, which includes all the components required to mount the library in a standard 19-inch, 4-post rack.
Drives	The library supports both full-height and half-height LTO drives. The drives are shipped separately and installed as part of the initial installation process.   For information about the drives supported in the library, see LTO Tape Drives on page 32.
SFPs (Fibre Channel drives only)	Each Fibre Channel drive is shipped with a multi-mode SFP installed in each port. If the drive has two ports, only one port can be active at any time. 
SCSI bus terminator (SCSI drives only)	Each SCSI drive is shipped with one terminator. ▪ Full-height SCSI drives use an active wide HD68 multi-mode,Ultra320 LVD/SE terminator. ▪ Half-height SCSI drives use an active VHCDI Ultra320 LVD/SE terminator. **Note:** Terminators are not included with replacement drives.  HD68 terminator  VHCDI terminator

Component	Description	
Ethernet cable	One CAT-5 data-grade cable is included with the library to connect the LCM to a 10/100BaseT Ethernet network for remote access to the BlueScale user interface through a standard web browser on a remote computer. This connection is also used for sending email notifications from the library.	
Power cord	One standard 110-120 VAC power cord is included for each power supply module you purchased. See Power Cord Specifications on page 501 for the requirements.	
Stylus	A stylus, used to navigate through the user interface, is included with the library.	
USB device	One USB device is shipped with the library. Additional USB devices are available for purchase from Spectra Logic. **Note:** The USB device you receive may look different from the one shown. Keep the USB device near the library to use for backing up and restoring the library configuration and for firmware upgrades. Not all USB devices are compatible with the library, so keep this USB device available.	
Rubber feet	Six rubber feet for the bottom of the chassis can be installed for tabletop installation. Do NOT install the feet if you plan to install the library in a rack.	

INSTALLING THE LIBRARY

The library installation procedure depends on whether you are mounting the library in a rack or placing it on a table.

Task	Described beginning on...
Install the Library in a Rack	page 45
Install the Library on a Flat Surface	page 49
Remove the Shipping Lock	page 51

Install the Library in a Rack

The library is designed to fit into a standard 19-inch, 4-post rack using just 4U of rack space. Do not install the drives or cartridges until *after* the library is installed in the rack.

WARNING

The library is heavy (see product specifications for details). Use extreme caution and proper equipment when moving the library. Do not install components in the library until it is secured in the rack.

WARNING

The library must be installed in the rack that is delivered with the library, or if none is included, in a standard 19-inch (48-cm), four-post rack. A two-post rack cannot support the weight of the library. Ensure your floor has adequate structural integrity, and follow the rack manufacturer's instructions when installing and securing the rack.

Caution

The maximum ambient temperature of the library is 95° F (35° C). Ensure that you select a location where the air vents at the front of the library and the fans at the back of the library are not blocked. The library requires unobstructed airflow to stay properly cooled.

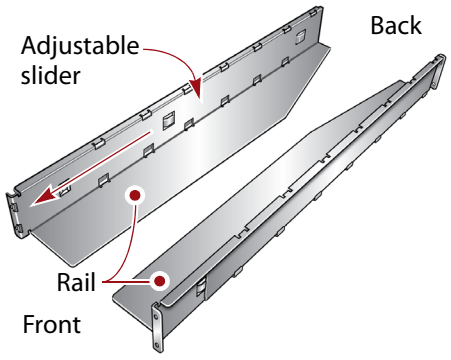
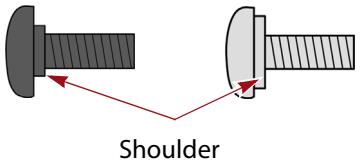
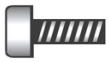
Gather Tools and Supplies

Obtain the following tools and equipment:

- #2 Phillips screwdriver, magnetic recommended
- Level (recommended)

Identify the Rack-mount Kit Components

Unpack the rack-mount kit and identify the components listed in the following table.

Component		Use
Rail assemblies Qty = 2		Support the chassis in the rack. Each rail is pre-assembled and consists of the following components: ▪ Adjustable slider ▪ Rails (2)
M6 screws Qty = 16 (8 each)		Attach the rail assemblies to the rack. Size used depends on rack type. ▪ M6 x 8mm (small shoulder) ▪ M6 x 8mm (large shoulder) Use the screws with the larger shoulder for racks with square holes.
M5 x 12 screws Qty = 2		Secure the library mounting brackets to the rack.

Install the Rails in the Rack

Caution Make sure that the rails and the library are level from front to back and from side to side. If the library is not level when you begin using it, robotic errors could result.

Caution Make sure that nothing in the rack will press down on the top of the T50e once installed.

Note: If possible, position the rails in the rack midway up the rack so you have easy access to the library front panel.

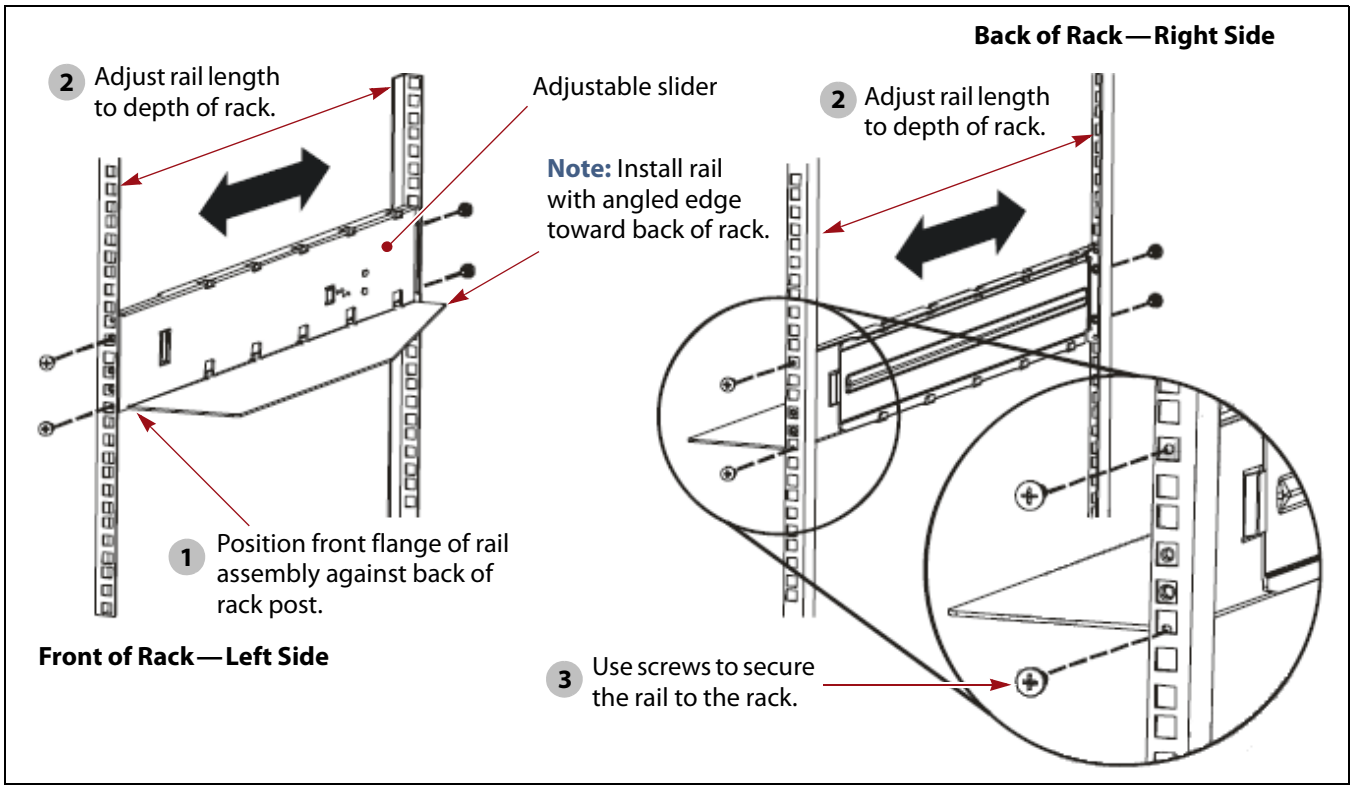


Figure 11 Install the rails in the rack.

1. Position the left-side rail assembly in the rack so that the front flange is behind the front screw holes in the rack post (Figure 11, 1).

   Note: Make sure that the front and back of the rail are attached to the rack at the same height on the front and back posts. Otherwise the library is not level when installed in the rack.

   Using a level simplifies making sure that the rail is level from front to back.

2. Using the slider, adjust the length of the rail assembly as necessary to fit the depth of the rack (Figure 11, 2).

3. Using a #2 Phillips screwdriver, install four M6 screws—two in the front and two in the rear—to secure the rail to the rack (Figure 11, 3). Tighten the screws securely.

   Notes:
   - Two sets of M6 screws are provided. The type you use depends on the type of rack you have. Use the screws with the larger shoulder for racks with square holes.
   - To simplify the installation, have a second person support the rail while you install the screws.
   - Leave the middle hole in each rail empty. You use this hole when attaching the library's mounting brackets to the rack.

4. Repeat Step 1 on page 47 through Step 3 on this page to install the right-side rail.

   Note: Make sure you install the right-side rail at the same level as the left-side rail so that the shelf formed by the rails is level from right to left and front to back in the rack. Otherwise, the library is not level when it is installed in the rack.

   Using a level simplifies making sure that the rails are level from left to right.

Place the Library in the Rack

Important Do not install the rubber feet if you are installing the library in a rack, as they are meant for a tabletop installation only! See Install the Library on a Flat Surface on page 49 for a description of the rubber feet.

1. Lift the library onto the shelf formed by the rails.

   Note: If you are not be able to access the top of the library after it is installed in the rack, you must remove the shipping lock before placing the library in the rack (see Remove the Shipping Lock on page 51).

Caution Do not remove the shipping lock from the library until after you complete the rack installation. If access constraints require you to remove the lock, keep the library as level as possible as you lift it into the rack. Tipping the library without the shipping lock in place may result in severe damage to the robotics.

2. Slide the library completely into the rack so that the mounting brackets are against the posts.

3. Using a #2 Phillips screwdriver, install one M5 screw in each mounting bracket to secure the library to the rack, as shown here.

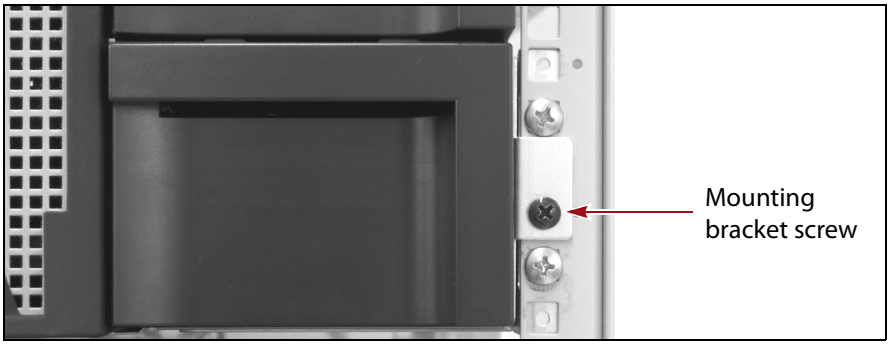


Figure 12 Attach the library to the rack.

4. Skip to Remove the Shipping Lock on page 51 to complete the installation.

Install the Library on a Flat Surface

Caution Do not remove the shipping lock from the library until after you position the library on the tabletop surface where it operates.

Caution When using the library on a tabletop surface, keep the following requirements in mind:

- The library must be installed on a level surface. If the library is not level when you begin using it, the robotics may experience errors.
- Do NOT stack any items on top of the library as it restricts the movement of the robotics.

Caution The maximum ambient temperature of the library is 95° F (35° C). Ensure that you select a location where the air vents at the front of the library and the fans at the back of the library are not blocked. The library requires unobstructed airflow to stay properly cooled.

Use the following steps to prepare the library for use on a tabletop surface.

1. If desired, remove the mounting brackets installed at the front of the library and the guide rollers installed on the two sides of the library using a T10 Torx driver. Set the brackets and guide rollers aside. They must be reinstalled if you decide to rack-mount the library at a later date.

Important Removing the brackets and roller guides is optional. If you select to remove them, make sure that you:

- Reinstall the ***black*** screws you remove from the brackets; they secure the cover to the chassis.
- *Do not* reinstall the ***silver*** screws after you remove the guide rollers.

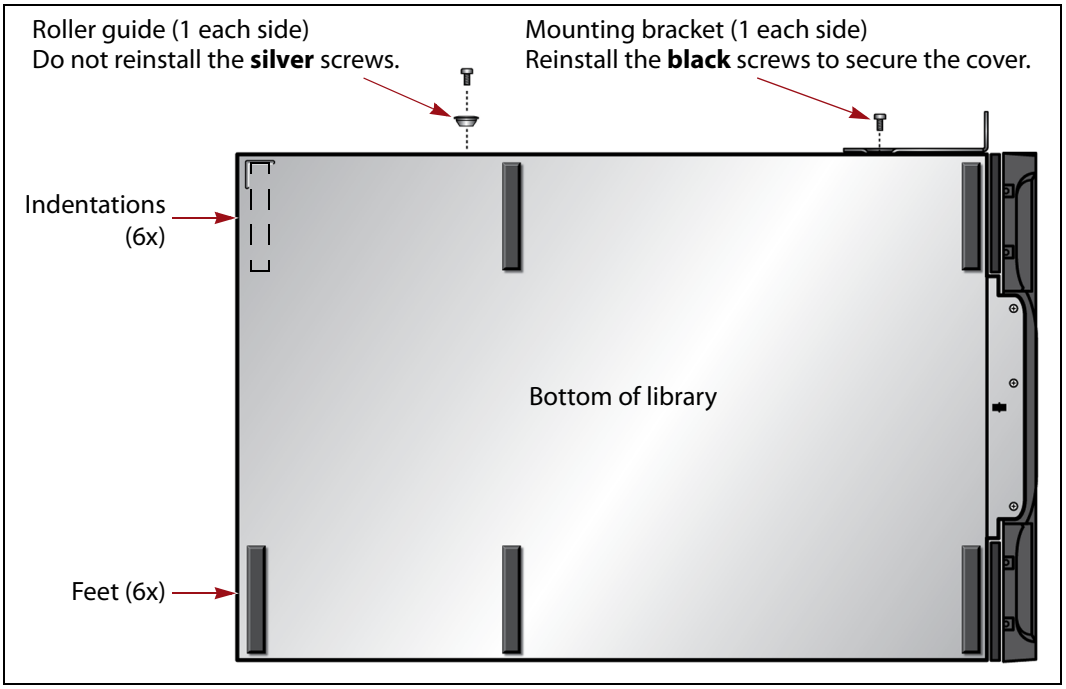


Figure 13 Install the rubber feet when using the library on a tabletop or desktop.

2. Carefully tip the library onto its side to access the bottom of the chassis.

Caution Make sure that the shipping lock is in place before you tip the library. Tipping the library without the shipping lock in place results in severe damage to the robotics.

3. Install the rubber feet on the bottom of the library as shown in Figure 13. Remove the paper backing on the feet and attach them to the locations indicated by the indentations on the bottom of the chassis.

Caution The feet distribute the weight of the cartridge magazines. Operating the library without the feet while it is on a flat surface may cause problems with magazines latching.

4. Place the library on a solid, level surface in a location with good airflow from the front of the library to the back.

Important Make sure that all six feet are firmly in contact with the surface and that the top of the library is level.

Remove the Shipping Lock

The shipping lock, which prevents the robotics from moving during shipment and installation, must be removed before the library is powered on. The shipping lock is located in the top center of the library and is held in place with a small label.

Caution Failure to remove the shipping lock before powering on the library can cause damage to the library.

Important Unless you are not able to access the top of the library when it is installed in a rack, do not remove the shipping lock until after you complete the installation.

1. Remove the tape label holding the lock in place, then remove the lock.
2. Replace the label over the opening.
3. Slide the lock into the storage slot on the back of the library.

   Note: You need to reinstall the shipping lock if you move or ship the library.

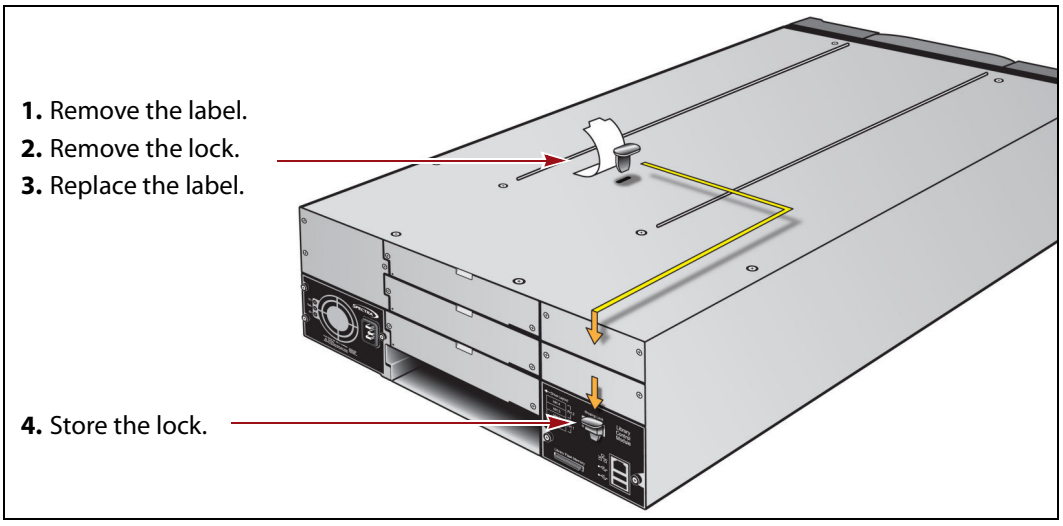


Figure 14 The shipping lock must be removed before powering on the library.

4. You are now ready to install the drives.

INSTALLING THE TAPE DRIVES

The library accommodates up to two full-height drives or up to four half-height drives. Each drive is mounted in a drive sled that provides the electrical and logical connections to the library. There are three types of drive sleds: Fibre Channel, SAS, and SCSI.

Important Although the library supports mixing Fibre Channel, SAS, and SCSI drive *interface types*, as well as half-height and full-height drives, each drive interface type must be in its own partition. You can mix full-height and half-height drives in the same partition *if* they are the same interface type (both Fibre Channel, for example). See Chapter 6 – Configuring and Managing Partitions, beginning on page 159 for instructions on creating partitions.

Important Do not attempt to install drives purchased from other vendors in the T50e library. The drives used in the library are specifically configured for use in the library. Use only drives you purchase from Spectra Logic.

Important Some operating environments require you to install device drivers before the application software can correctly communicate with the drives.

Important Full-height SCSI LTO-3 and half-height SCSI LTO-4 drives are no longer available for purchase with new libraries. They can still be purchased as replacements or upgrades to existing libraries.

Prepare for Installation

Ensure that the environment is free of conditions that could cause electrostatic discharge (ESD) If possible, use an antistatic mat and a grounded static protection wristband during installation. If a mat and wristband are not available, touch a known grounded surface, such as a computer's metal chassis.

Gather tools and supplies You need the following tools and supplies to install a drive:

- One or more drives, each in a Spectra Logic drive sled
- A #2 Phillips screwdriver
- Interface cables appropriate for the drive interface (see Drive interface cables and accessories on page 41)

Determine where to install each drive Depending on whether you purchased full-height or half-height drives, there are two or four drive bays, respectively.

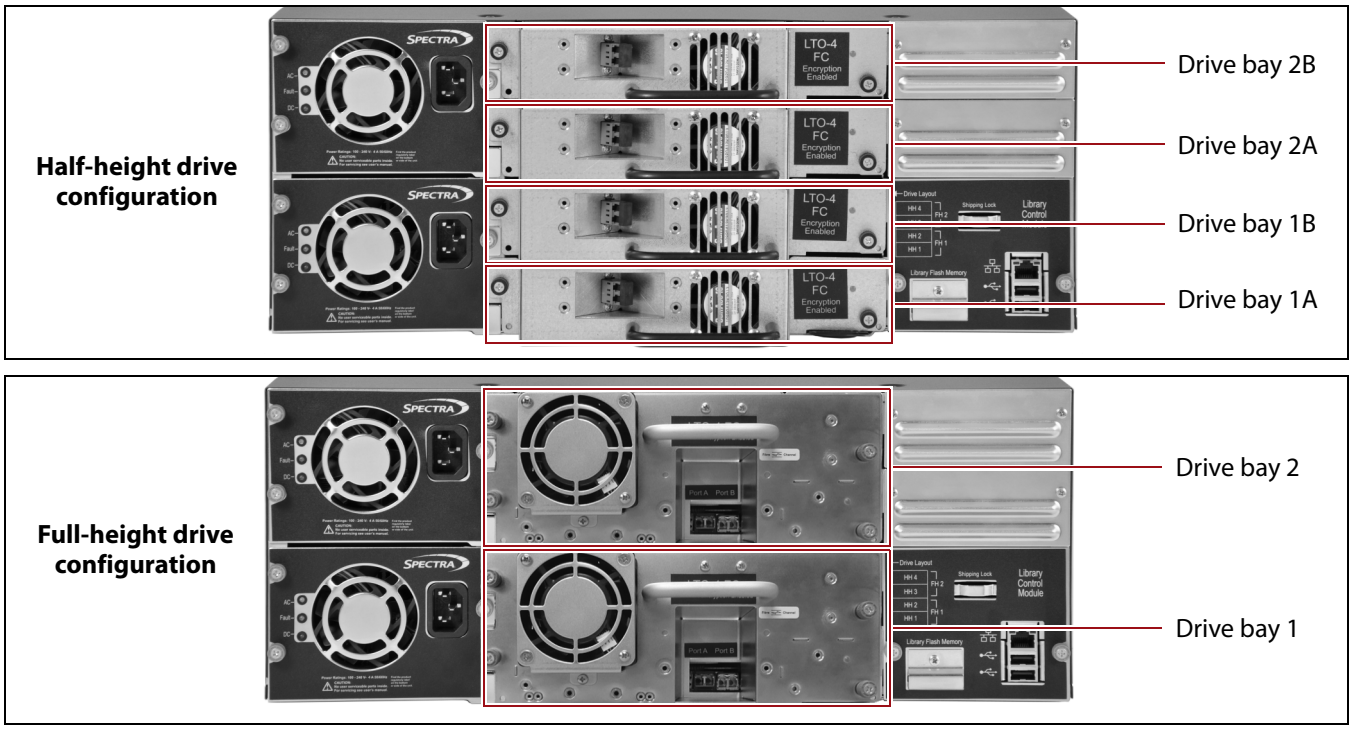


Figure 15 Drive bay locations for half-height and full-height drives.

- Install the drives from bottom to top, beginning with the bottom-most bay (drive bay 1 or 1A).
- If you are installing both half-height and full-height drives, install the full-height drives in the lowest possible drive bay. For example, you can install one full-height drive in drive bay 1 (occupying the bottom two half-height slots), and two half-height drives in drive bays 2B and 2A.
- Any unused drive bays must have covers installed.

Install the Tape Drives

1. Loosen the captive screws securing the drive bay cover using a #2 Phillips screwdriver. Set the cover aside for future use.

   Note: The library ships with the bottom drive bay uncovered, ready for a half-height drive to be installed. You must remove one cover for each half-height drive, and two covers for each full-height drive that you plan to install.

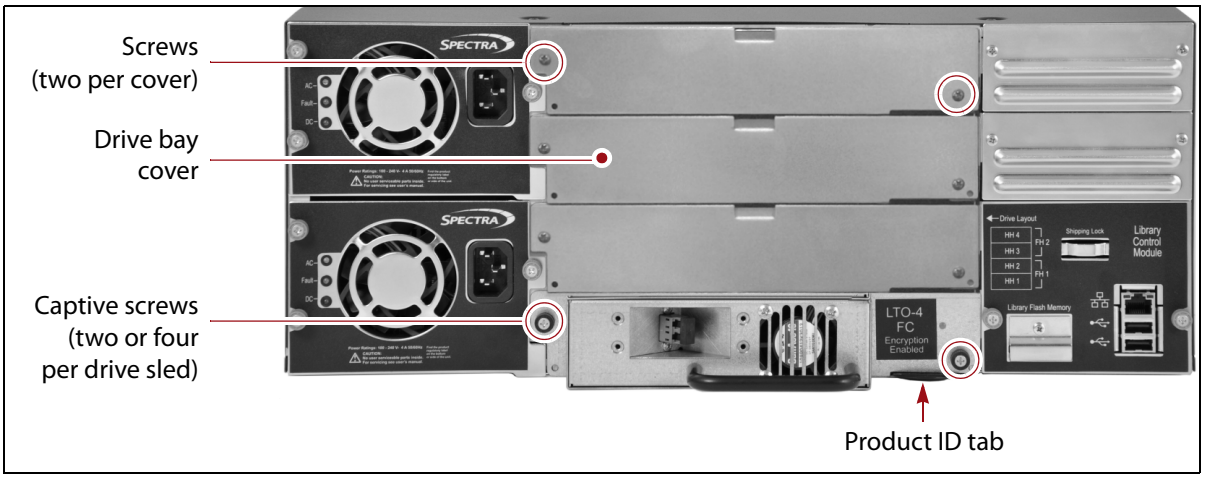


Figure 16 Loosen the captive screws securing the drive bay cover to the library.

2. Remove the drive from its protective packaging.

Caution The full-height drive assembly weighs approximately 7 lb (3 kg); the half-height drive weighs approximately 5 lb (2 kg). Be careful not to drop the drive.

3. When installing a drive in the bottom-most drive bay, slide the product ID tab out from the bottom edge of the drive bay. Push the tab back in after the drive is installed.

   Note: You do not need to slide the product ID tab out when installing the other drives.

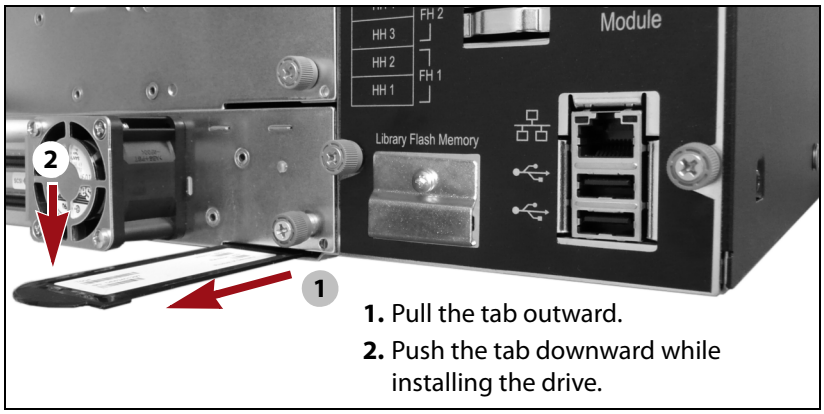


Figure 17 Slide the product ID tab out while installing the drive in the bottom most drive bay.

4. While supporting the drive sled with both hands, align the guides on the sides of the drive sled with the rails on each side of the open drive bay and then carefully slide the drive sled into the open bay. Gently push the drive straight in until it is seated in the back of the library.

Important When you install the drive in the bottom-most drive bay, push the product ID tab down slightly to prevent damage while you install the drive. Be careful not to snag the tab as you slide the drive into place.

Important If the drive is not correctly aligned with the rails on each side of the open drive bay, it does not slide all of the way into the drive bay and does not mate with the connector inside the bay. The library cannot communicate with drives that are not correctly installed.

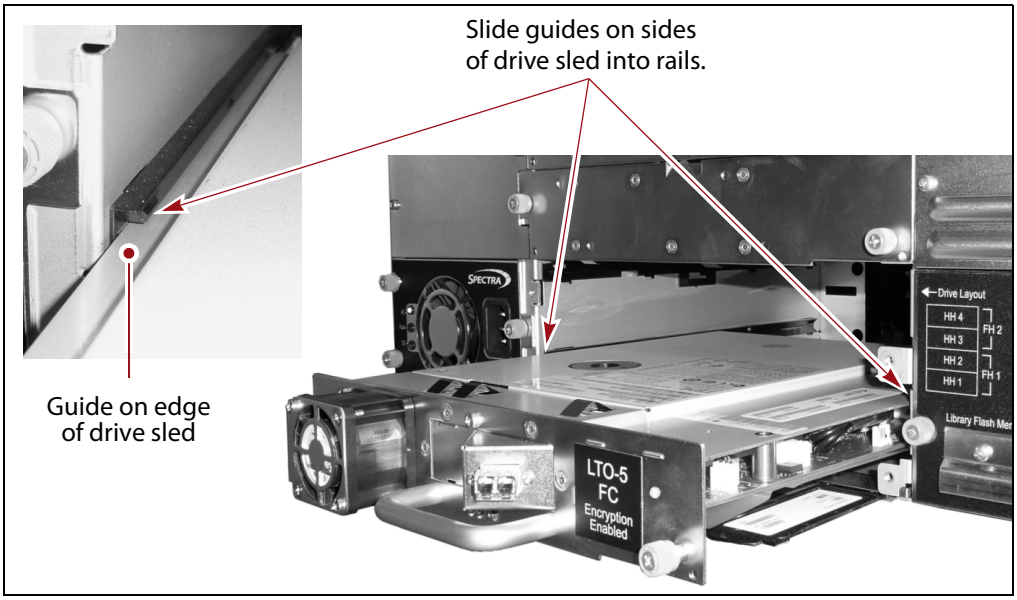


Figure 18 Align the guides on the drive sled with the corresponding rails in the drive bay and slide the drive straight into the drive bay.

5. Using your fingers or a #2 Phillips screwdriver, tighten the captive screws (see Figure 16 on page 54) to secure the drive sled to the chassis.

   Note: The half-height drive has two captive screws and the full-height drive has four captive screws.

6. Repeat Step 1 on page 54 through Step 5 on this page for each additional drive.

Connect the Tape Drives to the Host

Note: The Fibre Channel, SAS, and SCSI drive interfaces all use the SCSI command protocol to control the robotics and drives. The difference lies in how the commands are communicated from the host to the library.

Connecting Fibre Channel Drives

In a Fibre Channel environment, you can connect the drives to a Fibre Channel hub or switch in an arbitrated loop or a switched fabric; you can also connect them directly to a Fibre Channel HBA in the host.

Notes:
- It is not necessary to power off the host computer when connecting Fibre Channel drives.
- For information about the drive World Wide Names (WWN) while in the library, see Drive World Wide Names on page 156.

1. Remove the protective plug from the optical connector on the drive sled.
2. Remove the protective plugs from the fiber optic cable connectors.

Important Do not touch the tips of the connectors after removing the protective plugs. Doing so can contaminate the fiber optic cable and cause communication issues for the drive.

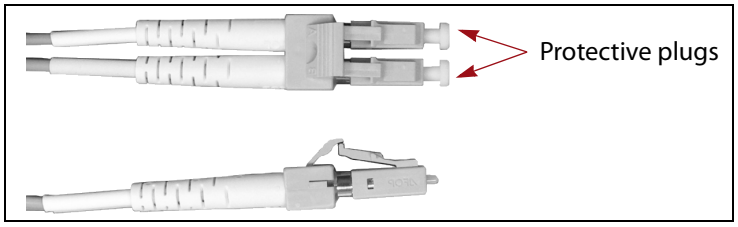


Figure 19 The connectors on an LC fiber optic cable.

3. Insert the connector on the fiber optic cable into one of the ports on the drive until it snaps into place.

Notes:
- The connector on the cable only fits one way. Do not force it.
- Full-height LTO-4 Fibre Channel drives have dual connectors (labeled Port A and Port B). Half-height LTO-4 and later generation drives only have one Fibre Channel connector. See Drive Interface Ports on page 32 for the location of the ports.
- For drives that have two Fibre Channel connectors, only one connector is active at any time. The two Fibre Channel ports cannot be used simultaneously to provide redundant data paths between the hosts and the drive. However, they can be used to provide failover capability in the event that communication to the port currently in use is interrupted (see Drive Connectivity Failover on page 37).

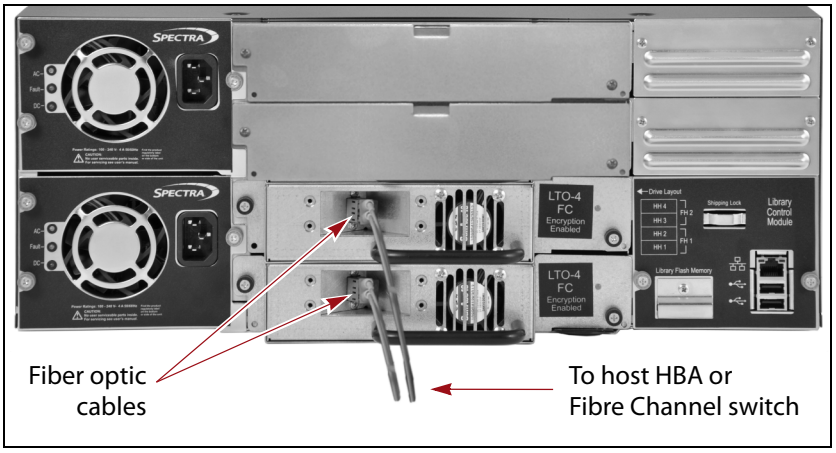


Figure 20 Connect the fiber optic cable to the drive (half-height LTO-4 drives shown).

4. Connect the free end of the cable to an active Fibre Channel switch or hub through which the hosts can access the drive or to the Fibre Channel HBA in the host.
5. Repeat Step 1 on page 56 through Step 4 on this page for each Fibre Channel drive.

Important

After the library is powered on and the Fibre Channel arbitrated loop is initialized, avoid disconnecting the drives in the library from the loop. If you need to disconnect the library from the loop, use the utility provided with your switch or hub to bypass the affected ports before breaking the connection. The bypass sets the port to a non-participating state on the loop. When you reconnect the library, use the utility to return the port to a participating state.

Connecting SAS or SCSI Drives

In a SAS or SCSI environment, each drive is connected directly to individual SAS or SCSI ports on an HBA in the host. You can also connect the SAS drives to a SAS expander to connect the drives to multiple hosts.

Connection Guidelines

The following table provides guidelines to keep in mind as you plan your connections to either SAS or SCSI drives.

Interface	Connection Guidelines
SAS	▪ **Do not exceed bus length restrictions.** The maximum allowable length of a SAS bus is 13 feet (4 m). ▪ **HBA type.** Use a standard 6 Gb/second SAS HBA. ▪ **RAID controllers.** Do not use a SAS RAID controller with the library or drives.

SCSI	▪ **Do not exceed SCSI bus length restrictions.** The maximum allowable length of an LVD SCSI bus is 39 feet (12 m).
	▪ **RAID controllers.** Do not use a SCSI RAID controller with the library or drives.
	▪ **Daisy-chaining LTO-4 drives. Spectra Logic does not support daisy-chaining multiple LTO-4 SCSI drives.**
	▪ **Daisy-chaining LTO-3 drives.**
	  ▪ A maximum of two LTO-3 SCSI drives can be daisy-chained on a single SCSI bus.
	  ▪ When daisy-chaining LTO-3 drives, use a cable length that does not require making tight bends in the cable; the minimum length is 12 inches.
	  ▪ Keep in mind that each daisy-chained drive increases the total length of the SCSI bus.
	  ▪ Connecting multiple devices on a single SCSI bus can impact the performance of all devices on the bus. The data transmission rate to any drive on the bus is limited to the maximum transfer rate of the SCSI bus.
	  ▪ Spectra Logic does not recommend, and does not support, daisy-chaining other SCSI devices on the same SCSI bus as the drives in the library.
	  Note: Although a maximum of 15 devices can be connected to a single wide LVD SCSI bus, attaching more than two devices to a single SCSI bus can have a negative impact on the performance of all devices on the bus.
	▪ **Make sure the SCSI bus is properly terminated.**
	  ▪ If you are connecting each drive to a separate host SCSI HBA, you must install a terminator on one of the SCSI connectors on each drive.
	  ▪ If you are daisy-chaining two LTO-3 drives, install the terminator on the unused SCSI connector.
	Important: Both ends of the SCSI bus must be terminated. If you are daisy-chaining two LTO-3 drives, make sure that a terminator is installed on the unused SCSI connector on one of the drives.

Connect the SCSI or SAS Cables and the SCSI Terminator

Use the following steps to connect the SAS or SCSI cables and the SCSI terminator.

1. Shut down the host computer(s).

   Note: If you are following these instructions to replace a drive in a library that is already installed, also shut down and power off the library (see Power Off the Library on page 141).

2. Connect cables to the drives, as appropriate for your desired configuration. See Drive Interface Ports on page 32 for the location of the ports.

   Note: For SAS drives, the two SAS ports cannot be used simultaneously to provide redundant data paths between the hosts and the drive. However, they can be used to provide failover capability in the event that communication to the port currently in use is interrupted (see Drive Connectivity Failover on page 37).

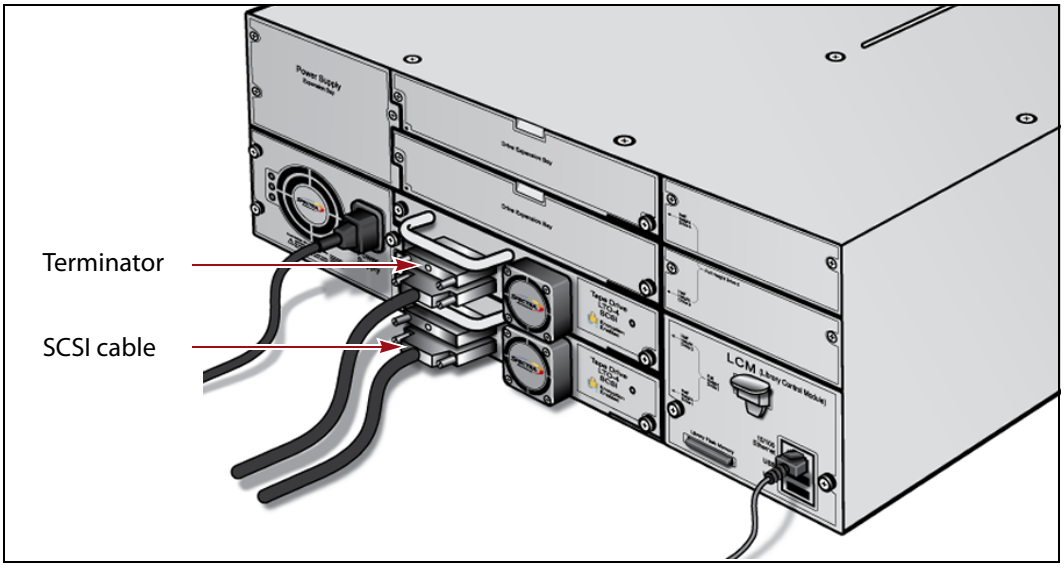


Figure 21 Connect the cables and, for SCSI drives only, install the SCSI terminators (SCSI drives shown).

3. For SCSI drives, connect the provided Ultra 3 Wide Active SCSI terminator to the unused SCSI connector on the drive.

   Note: If you daisy-chained two LTO-3 drives in the library, connect the terminator to the unused SCSI connector on the last drive in the chain.

4. Connect the other end of the cable.

   - **SCSI**—Connect the other end of the SCSI cable to the LVD SCSI HBA in the host computer.
   - **SAS**—Connect the other end of the SAS cable to a standard 6 Gb/second SAS (HBA) in the host computer or to a SAS expander.

5. Repeat Step 1 through Step 4 for any additional drives in the library.

INSTALLING CAPACITY EXPANSION SLOTS (OPTIONAL)

Note: Capacity expansion slots are no longer sold.

The library uses optional capacity expansion slots to increase the number of cartridge slots in the library from 47 up to a maximum of 50 slots. Each capacity expansion slots holds a single cartridge and occupies one half-height drive bay, which reduces the number of drives that can be installed. For example, for the 50-slot configuration, three cartridge capacity expansion slots replace half-height drive bays 1B, 2A, and 2B.

The following table shows the maximum number of half-height or full-height drives and cartridge slots that can be installed in the library.

Drive Form-Factor	Number of Drives	Maximum Number of Slots	Required Capacity Expansion Slots
Half-height	1	50	3
	2	49	2
	3	48	1
	4	47	0
Full-height	1	49	2
	2	47	0

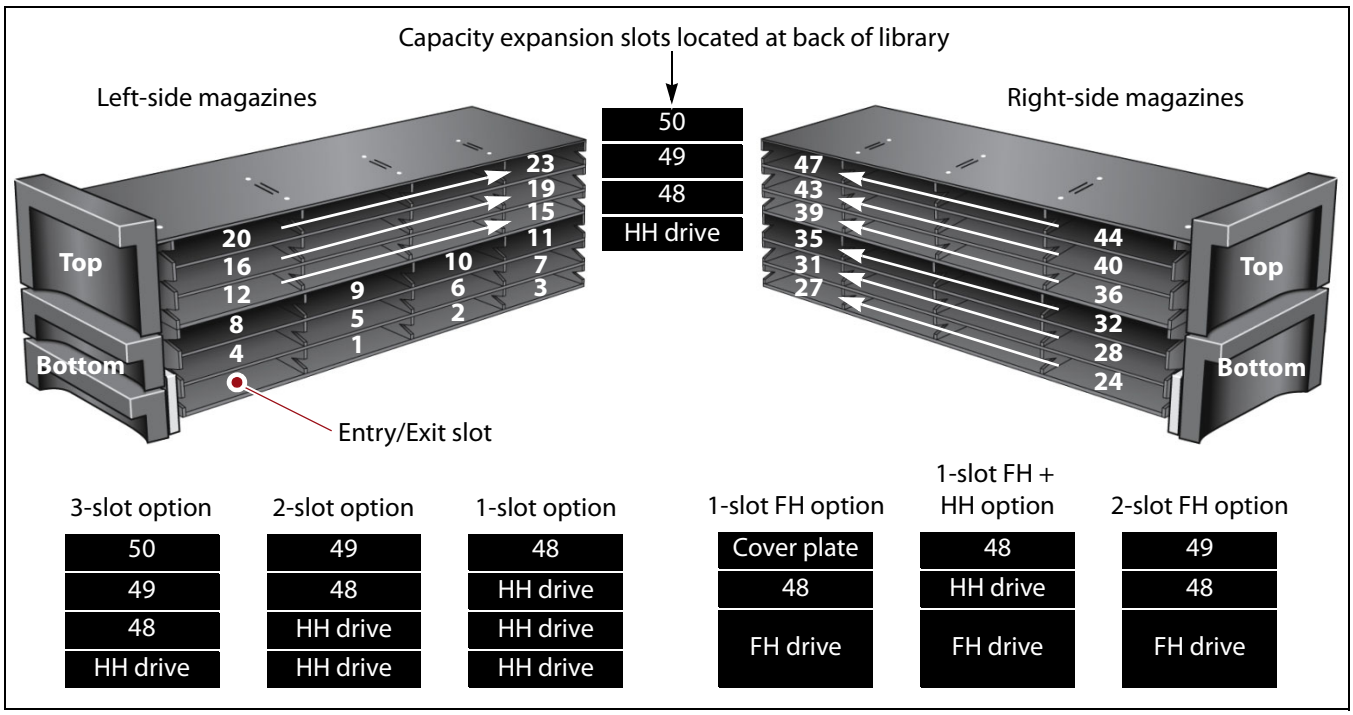


Figure 22 Capacity expansion slot numbering.

Use the following steps to install a capacity expansion slot in the library.

Note: The capacity expansion slots can be installed at any time. If you are replacing a previously installed half-height drive, first remove the drive as described in Removing a Drive from the Library on page 469.

1. Access the back of the library.
2. Using a #2 Phillips screwdriver, remove one of the drive bay cover plates. Set the cover and screws aside for future use.

   Note: Use the first available location going from bottom to top to add expansion slots. Do not leave empty drive bays between the drives and the capacity expansion slot. See Figure 22.

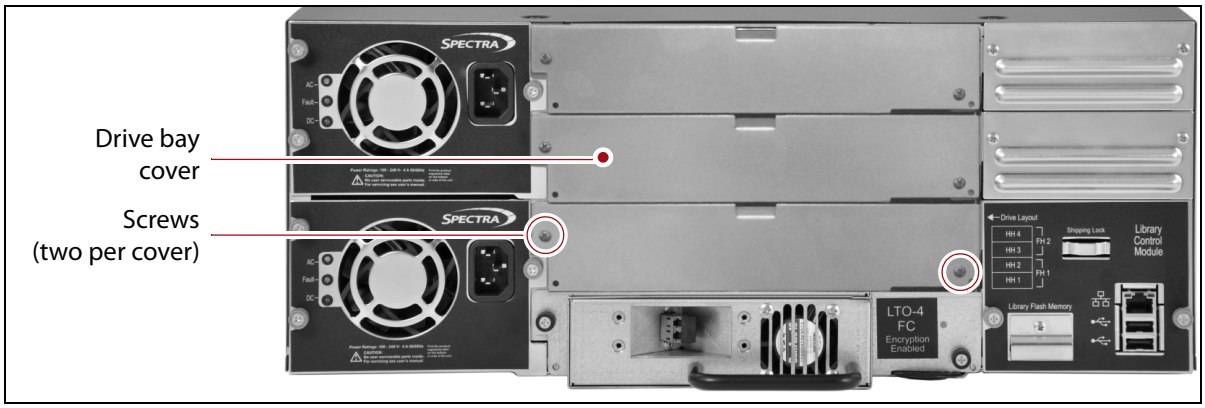


Figure 23 Remove the cover from the drive bay where you want to install the capacity expansion slot.

3. Slide the expansion slot into the library and, using your fingers or a #2 Phillips screwdriver, tighten the captive screws to secure it to the chassis.

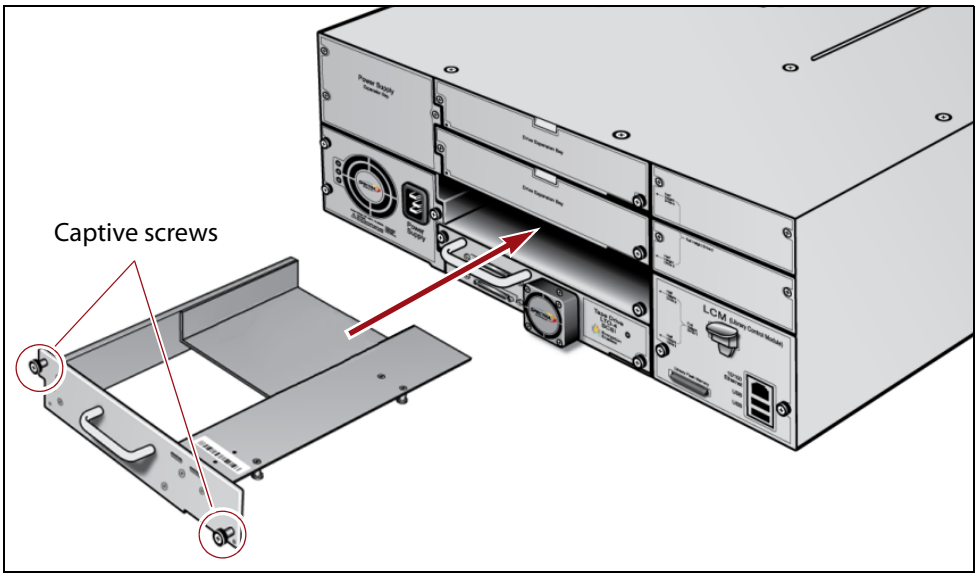


Figure 24 Slide the capacity expansion slot into the empty drive bay.

PERFORM THE AUTOINSTALL

The specially prepared Spectra USB device that came in your document kit (see Inventory the Components on page 43) contains the most current version of the BlueScale software for the library, as well as the activation keys for the options that you purchased with the library. It is used to automatically update the BlueScale software to and load the activation keys into the library.

Notes:

- If this is the *initial* installation, that is, if you have not already installed the library, follow the steps in this section to update the BlueScale software and install the activation keys for the options that you purchased.
- If you need to enter option keys *after* the AutoInstall setup — see Enter Activation Keys on page 115 for instructions.
- After completing this initial AutoInstall process, see Updating the BlueScale Software and Library Firmware on page 421 for instructions for subsequent updates to the library's BlueScale software.

Use the following steps to automatically update the BlueScale software and load the activation keys into the library.

1. Plug the Spectra USB device into one of the USB ports on the back of the library.

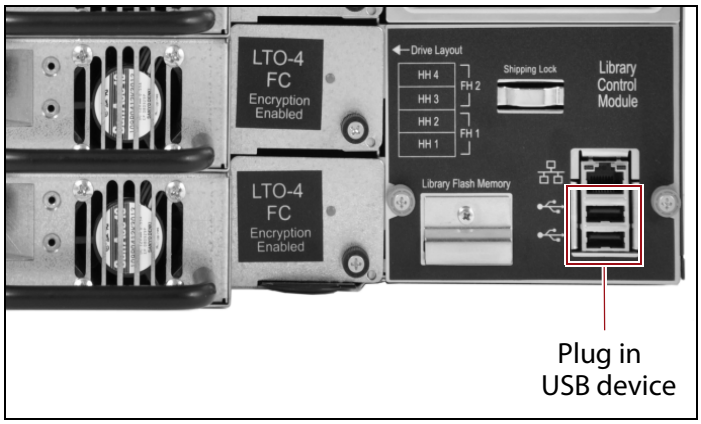


Figure 25 Plug in the Spectra Logic USB device to perform the AutoInstall.

2. Plug an AC power cord into the AC connector on the power supply module. Make sure that the cord is fully seated in the connector. If your library has two power supplies, connect the redundant power supply as well.

Important For redundant AC power configurations, connect each input to a separate branch circuit, which allows for failover in the event of a power failure in one of the circuits (see Power Specifications on page 501 for additional requirements).

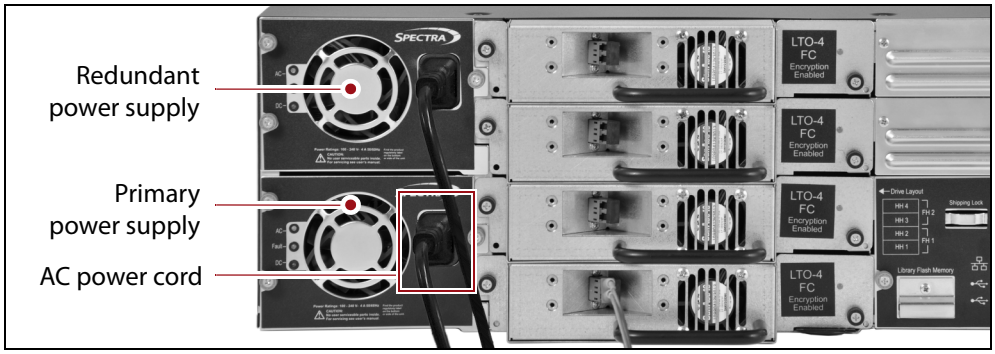


Figure 26 Connect the AC power cords (redundant power supply shown).

3. Connect the free end of each power cord into a properly grounded AC power outlet.
4. For each power supply, confirm that the AC and DC power supply status LEDs (see Figure 5 on page 29) illuminate blue and green, respectively, and that the Fault LED is not illuminated.
5. Press and hold the front panel power button for two to three seconds until the button's LED illuminates.

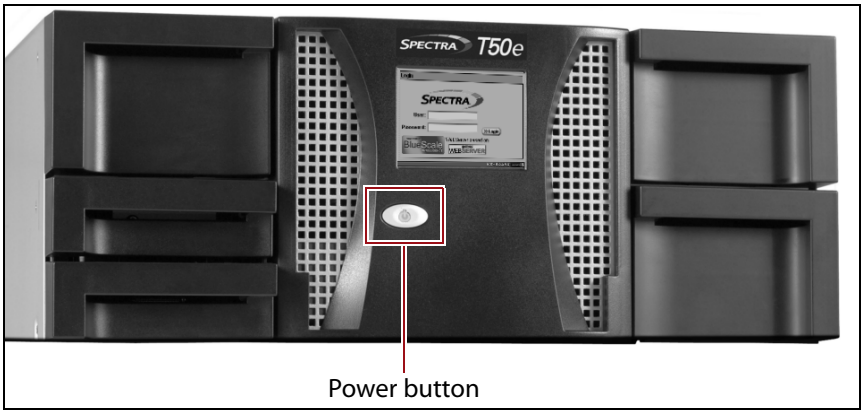


Figure 27 Press and hold the front panel power button.

6. Wait while the library performs its power-on sequence, which typically takes from six to nine minutes.
7. If this is the first time you power-on the library, the touch screen calibration utility runs. Use the stylus to calibrate the touch screen following the instructions provided on the screen.

   The calibration step only occurs during the initial power-on. You can also manually start the calibration process (see Calibrating the Touch Screen on page 438).

8. Wait while the AutoInstall process completes. During the AutoInstall process, the library automatically updates the BlueScale software and reboots.
9. After the reboot, wait while the library completes its power-on sequence, which takes six to nine minutes, depending on the library configuration. After the library completes its power-on sequence, the Library Initialization screen displays.

   This screen lists the required initialization steps and current status of the library's major components (Robotics, RCM, and LCM). Text boxes provide descriptions about the currently active tasks.

   Note: If your library has a static IP address, you can access the library using the remote library controller (RLC) as soon as the Library Initialization screen displays.

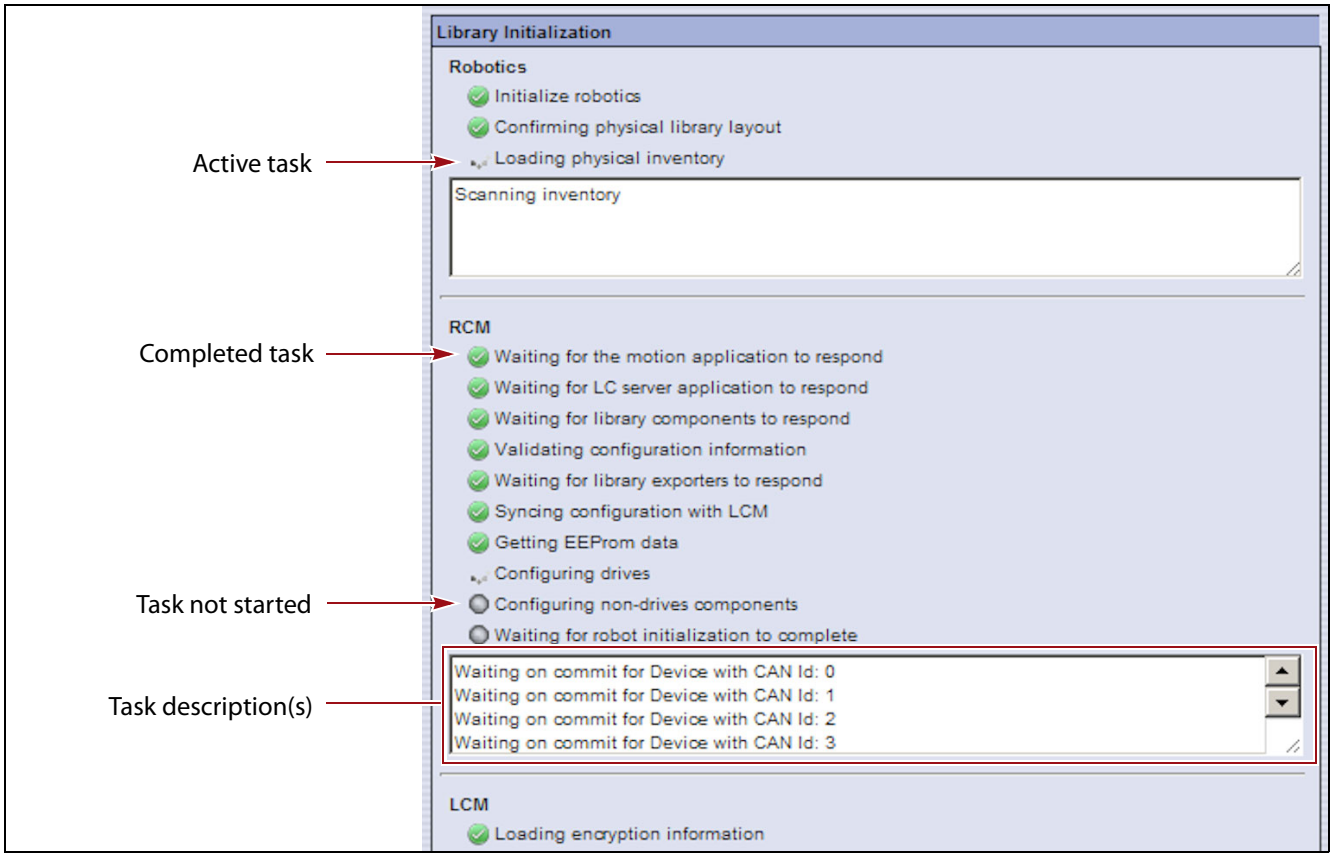


Figure 28 The Library Initialization screen.

10. After the library completes its initialization sequence and the Login screen displays, remove the Spectra USB device from the library.

Important Do not remove the USB device until the Login screen appears, but do not leave the USB device in the library after the installation.

Note: If the library cannot complete the initialization process, it generates system messages and enters maintenance mode. Contact Spectra Logic technical support for assistance.

LOG INTO THE USER INTERFACE

After the power-on sequence completes, the Login screen displays.

Note: If the soft keyboard is not displayed, touch the keyboard icon in the lower right-hand side of the Login screen to display it.

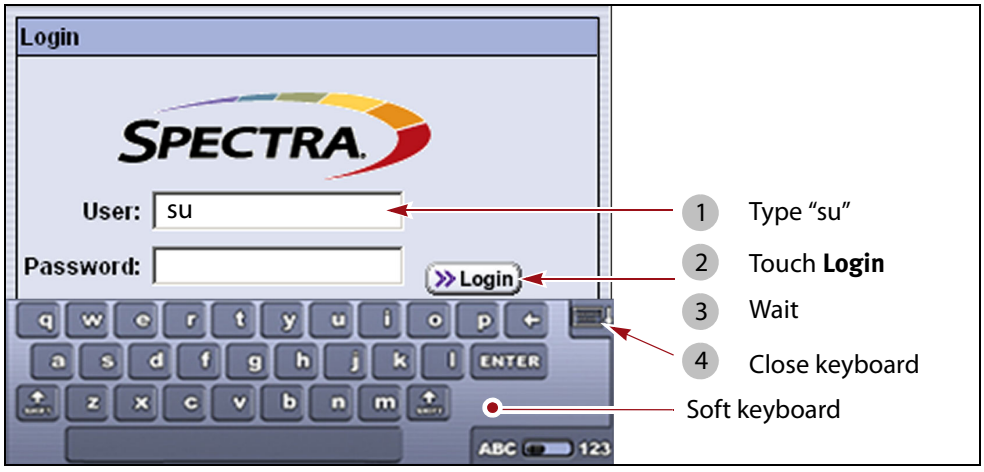


Figure 29 Use the soft keyboard to log into the library.

1. Using the stylus, touch the **User** text box and use the soft keyboard to type **su**.
2. Leave the password field empty, and touch **Login**.

   Note: If this is not the initial login, and you previously established passwords, enter the superuser password before touching **Login**.
3. Wait for the initialization process to complete.
4. Close the keyboard by touching its icon with the stylus.
5. Access the General menu screen. Read Chapter 3 – Introducing the BlueScale User Interface, beginning on page 71 to learn about using the library’s BlueScale user interface.

Review Messages, if shown If there are any alerts, the Messages screen displays. Touch the **MENU** button to continue to the General menu screen. After you complete the initial configuration of the library, you can return to the Messages screen and respond to the messages as necessary (see Check and Respond to Messages on page 143).

Note: The messages screen always displays at the initial installation and when you power cycle the library after adding, removing, or replacing a components (for example, a drive).

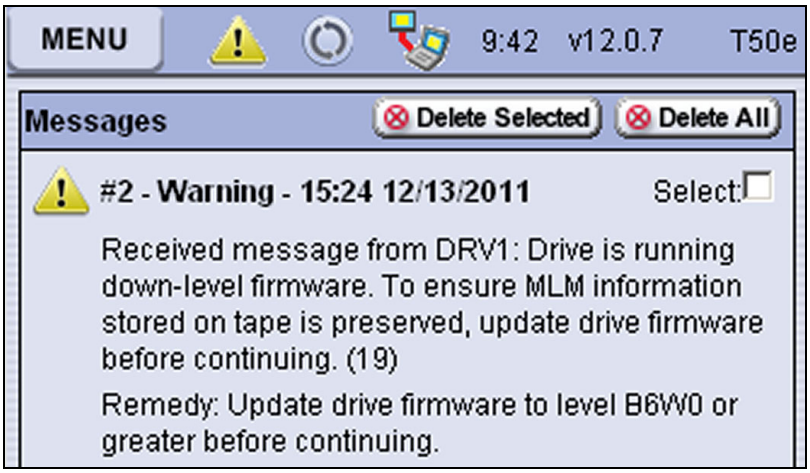


Figure 30 Review the system messages on the Messages screen.

Review the General Status If the library initializes and finds no alerts to report, an General Status overview screen showing the status of the library's components displays. The icons on the page indicate the overall status of the major system components. Touch the **MENU** button to view the General menu screen.

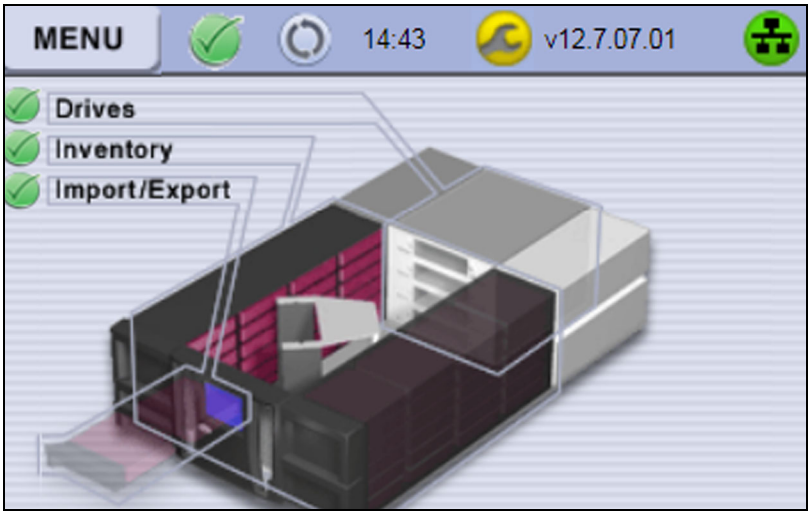


Figure 31 Review the General Status screen.

CONFIRM THE CURRENT BLUESCALE SOFTWARE VERSION

After you log into the library and the General Status screen displays, confirm that your library is using the most current BlueScale software version.

Note: Figures in this section show the Spectra TFinity library. When performing these steps, make sure you select T50e.

1. Locate the BlueScale software version shown on the status bar at the top of the touch screen.

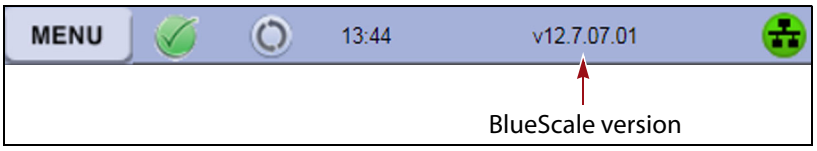


Figure 32 Locate the BlueScale software version on the status bar.

2. Log into your user account on the Technical Support portal at support.spectralogic.com.

   Note: See Accessing the Technical Support Portal on page 472 for information about creating an account and accessing the Technical Support portal.

3. Select **Downloads** ⋯⁘ **Product Software**.

4. On the Product Software page, locate your library type in the **Spectra Product** column. The currently released BlueScale version is listed in the **Current Version** column.

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	BlueScale12.7.00.07-20170906F.hpz	N/A	*Please contact Support for this update*	TFinity Library Release Notes and Documentation Updates
T950	BlueScale12.7.02-20170623F.2lpz	BlueScale12.7.02-20170623F.2lps	72,977/8	T950 Library Release Notes and Documentation Updates
T200/380/680	BlueScale12.6.45.3-20151121F.2boz	N/A	42,540	Spectra T200, T380, & T680 Release Notes and Documentation Updates
T120	BlueScale12.7.03-20170726F.2spz	BlueScale12.7.03-20170726F.2sps	48,929	T120 Library Release Notes and Documentation Updates
T50e	BlueScale12.7.03-20170726F.52z	BlueScale12.7.03-20170726F.52s	18,711	T50e Library Release Notes and Documentation Updates

Figure 33 The Product Software screen.

5. Compare the Current Version available for the library to the version installed on the library.

6. If a more current version of the BlueScale software is available, download and install it. See Updating the BlueScale Software and Library Firmware on page 421 for detailed instructions.

Notes:
- Download the BlueScale software update to a USB device connected to the computer you are using to access the Technical Support portal. Because the library is not yet configured with Ethernet access, you must perform this initial update from the USB device.
- If you are updating a library running BlueScale12.7.03 or later, select a package ending with the letter "s", which indicates a digitally signed package. If you are updating a library running a BlueScale version prior to 12.7.03, select a package ending with the letter "z", which indicates an unsigned zip package.
- If you have any questions or concerns about updating the BlueScale software, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

Complete the Initial Configuration Steps

To prepare the library for use, complete the initial configuration steps described in the following sections.

Create the Initial Partition

Before the hosts that plan to use the library can connect to it, you must create one or more partitions.

Important To ensure that the hosts are able to detect the library and its drives, make sure that you have at least one storage partition configured before you power on the hosts following installation.

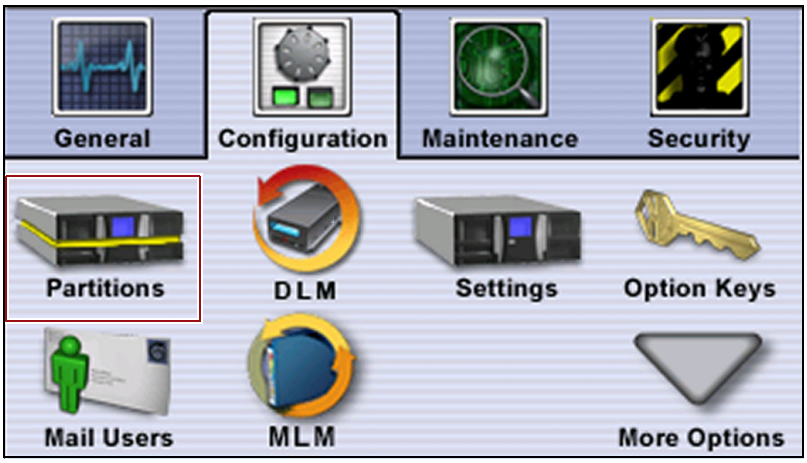


Figure 34 Click **Partitions** on the Configuration tab to begin configuring partitions.

When you select **Configuration ⋯⁘ Partitions** for the first time, you must select how you want to create the initial partition. You can have the library automatically create a single partition using all available slots and drives or you can create partitions manually. Your answer depends on whether you want to use the entire library as a single partition or whether you want to use multiple partitions. Read Chapter 6 – Configuring and Managing Partitions, beginning on page 159 for detailed instructions.

Connect the Ethernet Cable

If you want to manage and monitor the library remotely using a web browser, connect a Category 5 (10/100BaseT) data-grade Ethernet cable to the Ethernet port on the library's LCM. Connect the other end of the cable to an active Ethernet network that is accessible to the computer you plan to use for managing the library.

Note: You can also use this Ethernet connection to download BlueScale software updates directly to the library from the Spectra Logic package server.

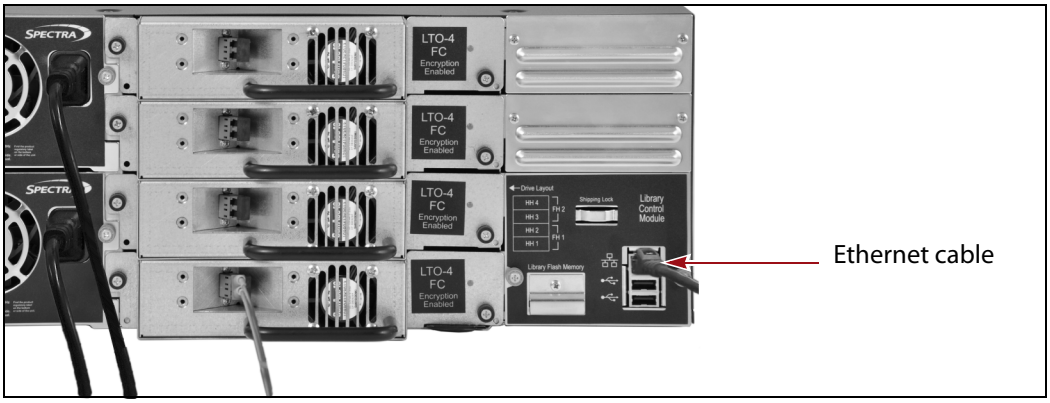


Figure 35 Connect an Ethernet cable to the LCM.

This Ethernet connection is also required for the library to automatically email notifications to users and AutoSupport tickets to Spectra Logic Technical Support.

Power On the Host and Test the Connections

After you connect all of the cables, powered on the library, and configured at least one partition you are ready to power on your host system and confirm that it can communicate with the library.

Connect to the Library Using your storage management software, connect to the library and its drives. Refer to you software documentation for instructions.

Download Device Drivers, if needed As part of preparing your host to communicate with the library and drives, you may need to install drive device drivers. Go to support.spectralogic.com to download device drivers for the drives. See Updating Drive Device Drivers on page 462 for detailed instructions.

Notes:

- You only need to download the Windows® 2008 Medium Changer Driver if you are using Removable Storage Manager (RSM) or Data Protection Manager (DPM) storage management software. If you are not using one of these software packages, you do not need to download or install this device driver. Other storage management software packages provide the necessary drivers, if needed.
- Do not download and install the drivers until after you create the partition, power on the host, and confirm that it can access the library.

Perform a Test Backup Using your storage management software, back up a small amount of data to each of the drives in the library to confirm that the host is able to communicate with the drives.

CHAPTER 3

Introducing the BlueScale User Interface

The BlueScale user interface is used for configuring, monitoring, and maintaining the T50e library. The user interface displays on the touch screen on the front of the library. It can also be displayed remotely through a standard web browser using the Remote Library Controller (RLC).

This chapter describes the library's BlueScale user interface and how it is used.

OVERVIEW OF THE BLUESCALE USER INTERFACE

The BlueScale user interface lets you set configuration options, view library and drive information and metrics, manage media, monitor library operations, and perform maintenance operations.

Note: Unless otherwise specified, references to the user interface screens in this *User Guide* apply to both the library touch screen and the web browser screens presented through the remote connection.

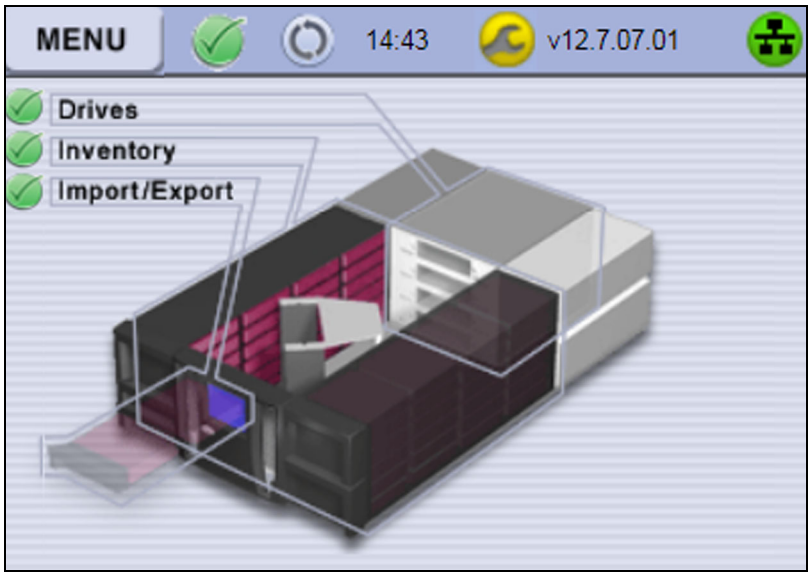


Figure 36 The General Status screen after login.

Access Options

The BlueScale user interface is accessed using either the touch screen on the library operator panel or through the BlueScale web interface.

Operator Panel Touch Screen Interface

The touch screen on the library's operator panel is the library's local BlueScale user interface. You select options and enter information by simply touching the appropriate location on the screen with a stylus or your finger. The touch screen interface includes a soft keyboard that you can use to enter alphanumeric characters into text fields. This soft keyboard can be accessed from the keyboard icon that displays whenever text input is required.

BlueScale Web Interface

The BlueScale web interface lets you use a standard web browser to access the library through the Remote Library Controller (RLC). Simply enter the library's IP address into a browser running on a computer that can access the Ethernet network to which the library is connected.

Important

- When accessing the library remotely through a web browser, do not use the **Enter** key on your keyboard when making selections in the BlueScale user interface. Various web browsers handle the **Enter** key differently, causing inconsistent behavior in the BlueScale interface.
- Always use your mouse to make selections and click the buttons in BlueScale screens instead of using your keyboard.
- Do not use the browser's "back" button to return to a previously viewed BlueScale screen. Always use the BlueScale menus and buttons on the screen to navigate the BlueScale web interface.
- Always use the Refresh Display ( ) button on the Status bar to refresh the screen. Using a keyboard command (for example, **F5**) to refresh the browser when connected to the BlueScale web interface causes unpredictable results.

The BlueScale web interface provides access to the same features and functions that are available through the touch screen, excluding functions that involve physical interaction with the library (for example, using the access port to import or export a cartridge).

When using the web interface, keep the following requirements in mind:

Number of Sessions The BlueScale web interface supports up to eight simultaneous connections to the library. If you attempt to establish more than eight simultaneous web interface connections, the existing connection with the longest idle time is terminated.

Supported Browsers Remote access to the library through the web interface is only supported using the following web browsers:

- Microsoft®Internet Explorer®
- Mozilla® Firefox®
- Google® Chrome™
- Apple® Safari®

Additional browsers are not fully tested with the BlueScale web interface. Using an unsupported browser can result in the BlueScale web interface not displaying or operating as expected.

User Interface Features

The following sections describe the common features that appear in the BlueScale user interface screens.

General Status Screen

When you first log into the library, the General Status screen displays. Icons on this screen indicate the current status for the major library components. Moving the cursor over the name of the component highlights the component in the system graphic.

Notes:
- You can also display the General Status screen by selecting the **General Status** option on the General menu screen.
- A similar pre-login General Status screen displays if there is no interaction with the operator panel within 30 seconds after the Login screen displays. See Pre-Login General Status on page 86 for detailed information.

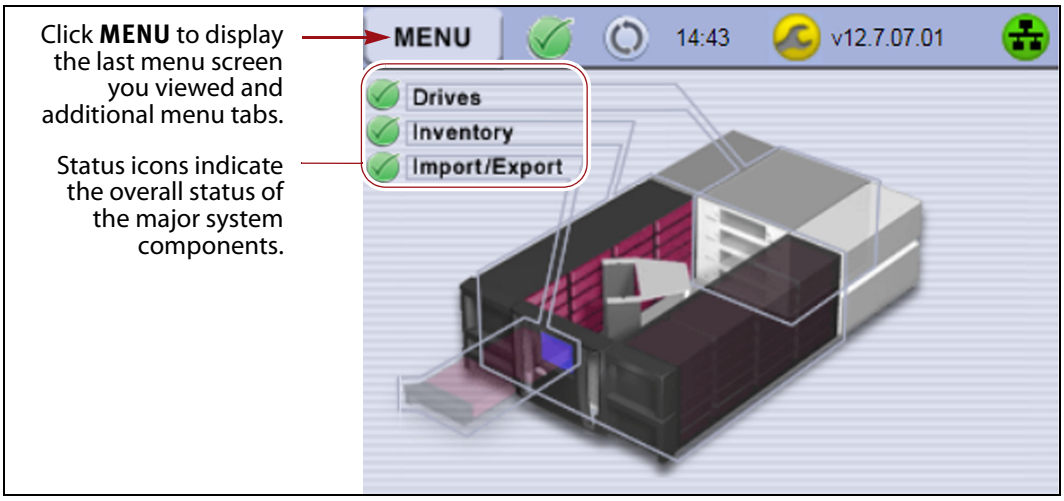


Figure 37 The General Status screen of the user interface.

Do one of the following to access the options provided through the BlueScale user interface.

- Click the **MENU** to display the last menu screen you viewed along with tabs for additional menus (see Figure 38 on page 75). If you just logged into the library, the General menu screen displays.
- Click **Drives** to display the Drives screen, which is also accessed from the **Drives** option on the Configuration menu (see Configuration on page 77).
- Click **Inventory** to display the Inventory screen, which is also accessed from the **Inventory** option on the General menu (see General on page 76).

- Click **Import/Export** to display the Import/Export screen, which is also accessed from the **Import/Export** option on the General menu (see General on page 76).

  Note: Clicking **Import/Export** does not display the Import/Export screen when you are accessing the library using the BlueScale web interface. The Import/Export screen is only available when you are accessing the library using the operator panel.

Using the Menus

The options in the BlueScale user interface are divided into four menus. When you click the icon for one of the menus, its associated options display below it. When you are viewing a screen for one of the BlueScale options, clicking **MENU** displays the last menu screen you viewed. From there you can navigate to other menus to select additional options.

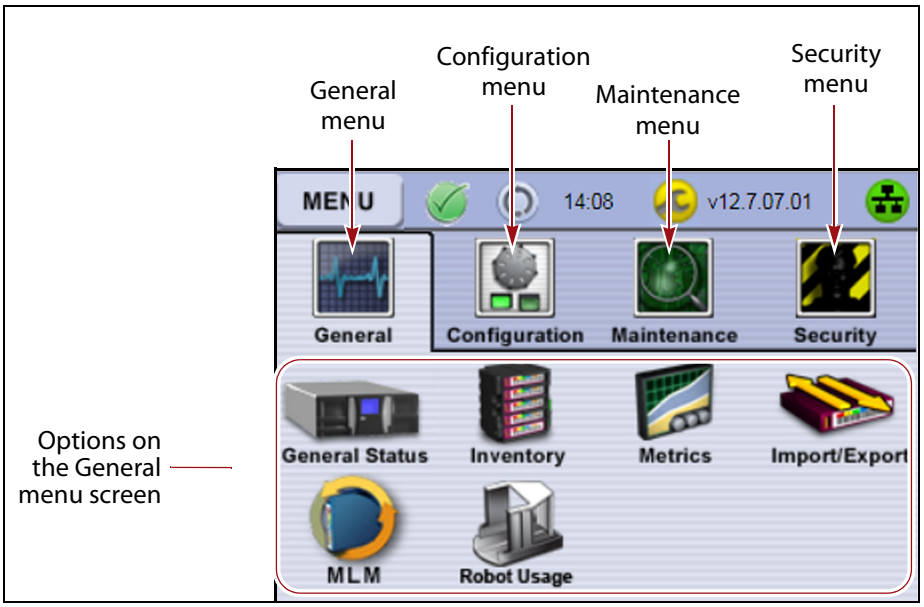
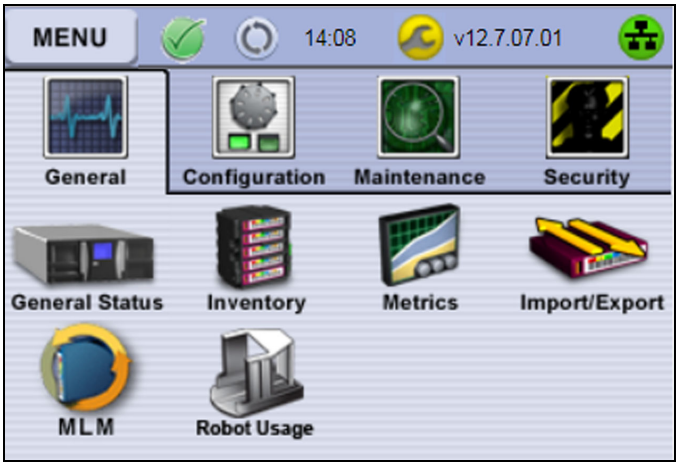


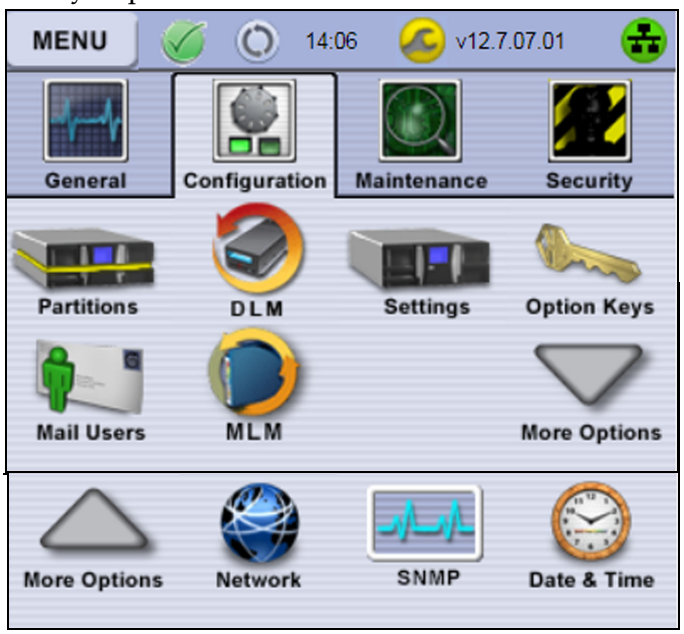
Figure 38 Options on the General menu screen.

Menu Option Overview

The following table provides an overview of the options available under each menu item. Figure 43 on page 80 shows the sequence of the screens under each option.

Menu	Available Options
General	The General menu provides access to the most frequently used library screens and controls.  **Figure 39** The General menu. ▪ **General Status** — Displays the current status for the major library components. See General Status Screen on page 74 for to learn about using the options available on the General Status screen. ▪ **Inventory** — Displays the Inventory screen, which shows the library's media inventory information. Use the controls on the Inventory screen to locate individual cartridges and move cartridges from one location in the library to another. See Using the Cartridge Inventory on page 223 to learn about using the options available from this screen. ▪ **Metrics** — Displays screens that show the metrics for power consumption and storage density for the media types currently in the library. See Use Performance Metrics on page 145 for information about viewing the metrics available for the library. ▪ **Import/Export** — Displays the Import/Export screen, which provides controls for importing, exporting, and exchanging cartridges. See Understanding Cartridge Import and Export on page 198 to learn about using the options available from this screen. **Note:** The **Import/Export** option is not available when accessing the library remotely using the BlueScale web interface. ▪ **MLM (Media Lifecycle Management)** — Displays the Media Lifecycle Management Report screen, which provides controls for generating media lifecycle reports. See Using MLM Reporting on page 262 to learn about using the options available from this screen. ▪ **Robot Usage** — Displays the Robot Utilization screen, which shows the metric that measures the percentage of time the robotics is being used while the library is powered on. See View Robot Utilization Information on page 147 to view this metric.

Menu	Available Options
Configuration	The Configuration menu provides controls for configuring all aspects of the library's operation:



Configuration main screen

Configuration More Options screen

Figure 40 The Configuration menu.

- **Partitions** — Displays the Partitions screen, which lists the partitions currently configured on the library and lets you define new partitions. You can also modify or delete existing partitions. See Chapter 6 – Configuring and Managing Partitions, beginning on page 159, to learn about configuring and using both storage and cleaning partitions in your library.
- **Drives** or **DLM** — Displays the Drives screen, which lists all of the drives installed in the library. Depending on the library configuration, the screen offers options for performing different types of operations on each drive.

  If Media Lifecycle Management (MLM) is enabled, the **Drives** icon in the Configuration menu changes to **DLM**, indicating that Drive Lifecycle Management is enabled. See View Robot Utilization Information on page 147 and Chapter 9 – Using Drive Lifecycle Management, beginning on page 279, to learn about using the options available from the Drives screen.

Note: Enabling MLM automatically enables DLM.

- **Settings, Option Keys, Mail Users, Network, SNMP** and **Date & Time** — Displays controls for enabling purchased library options and configuring the library's system-wide operating parameters. See Chapter 4 – Configuring the Library, beginning on page 93, to learn about using these options.
- **Media Lifecycle Management** — Displays the Media Lifecycle Management Setting screen, which provides controls for enabling MLM and configuring global settings for MLM. See Chapter 8 – Configuring and Using Media Lifecycle Management, beginning on page 233, to learn about using the options available from the Media Lifecycle Management Setting screen.

Menu	Available Options
Maintenance	The Maintenance menu provides access to maintenance and troubleshooting options for the library and drives.

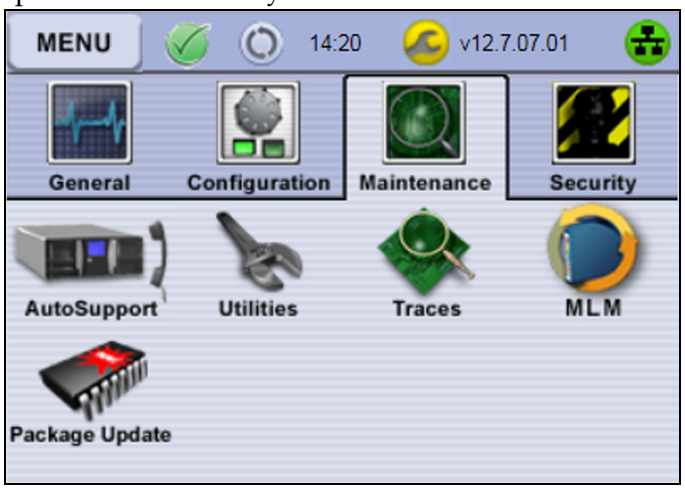


Figure 41 The Maintenance menu.

- **AutoSupport** — Displays the AutoSupport screen, which provides controls for creating and maintaining AutoSupport profiles, opening and updating support tickets, and configuring AutoSupport features. See Chapter 11 – Configuring and Using AutoSupport, beginning on page 334, for detailed information about configuring and using AutoSupport.
- **Utilities** and **Traces** — Displays the Basic Utilities screen and the LCM Traces screen, respectively. These options provide tools used during maintenance and troubleshooting procedures. See Chapter 12 – Library Troubleshooting, beginning on page 352, and Chapter 14 – Maintaining the Library, beginning on page 418, to learn about using the options available from the Utilities screen.
- **MLM** — Displays the Media Lifecycle Management Tools screen, which provides access to controls for using MLM features. See Chapter 8 – Configuring and Using Media Lifecycle Management, beginning on page 233, to learn about configuring MLM and using the options available from the Media Lifecycle Management Tools screen.
- **Package Update** — Displays the Package Update screen, which shows the version of the BlueScale software the library is using and provides controls for updating the BlueScale software and the firmware for individual library components, managing update packages, and configuring and managing package servers. See Configure a Package Server on page 132 and Updating the BlueScale Software and Library Firmware on page 421, to learn about using the options available from the Package Update screen.

Menu	Available Options
Security	The Security menu provides access to options for managing users and for configuring and using the encryption feature for your library. It also indicates the user currently logged into the library and that user's group.

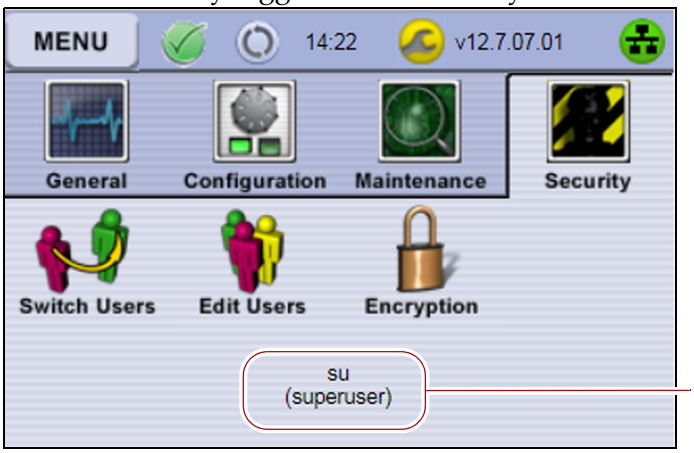
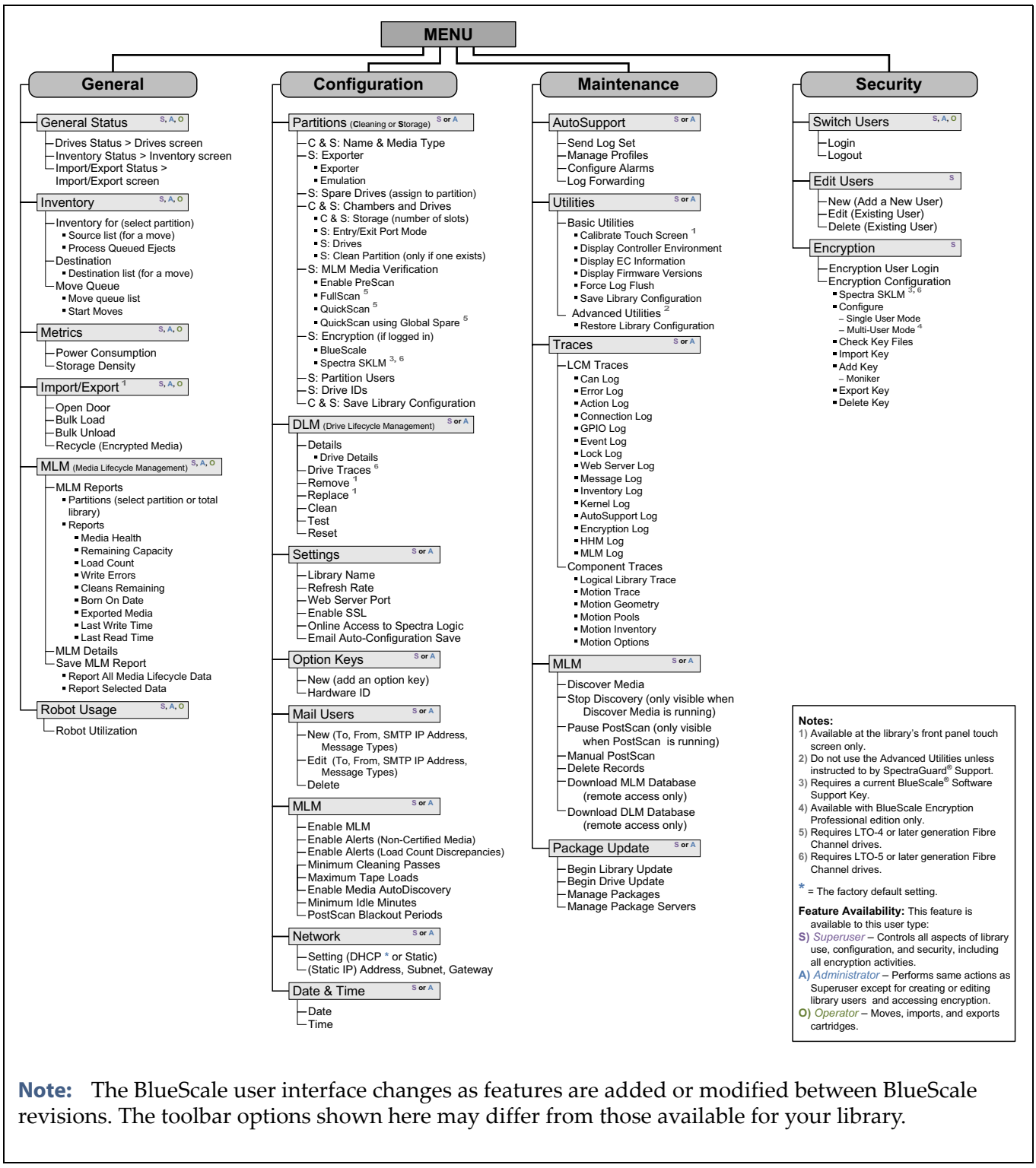


Figure 42 The Security menu.

- **Switch Users** — Displays the Login screen, which logs the current user out of the library and lets a different user log in. See Log Off or Switch Users on page 90 for information about using this option.
- **Edit Users** — Displays the Edit Users screen, which provides tools for adding, editing, and deleting users. See Configuring Library Users on page 94, to learn about using the options available on the Edit Users screen.
- **Encryption** — Displays the Encryption Login screen. You must log into the encryption feature before you can enable and configure either Spectra SKLM or BlueScale Encryption key management options. See Chapter 10 – Encryption and Key Management, beginning on page 289, for information about configuring and using encryption and key management with the library.

Map of Options Available from the BlueScale Menu



Note: The BlueScale user interface changes as features are added or modified between BlueScale revisions. The toolbar options shown here may differ from those available for your library.

Figure 43 Map of the options available from the BlueScale menu.

Status Bar

The status bar is located at the top of each screen. The information and icons displayed on the status bar depend on the status of the system and whether you are using the touch screen operator panel or the BlueScale web interface.

Note: A remote access icon can also appear on the status bar when you access the library remotely (see Remote Support Icon on page 82).

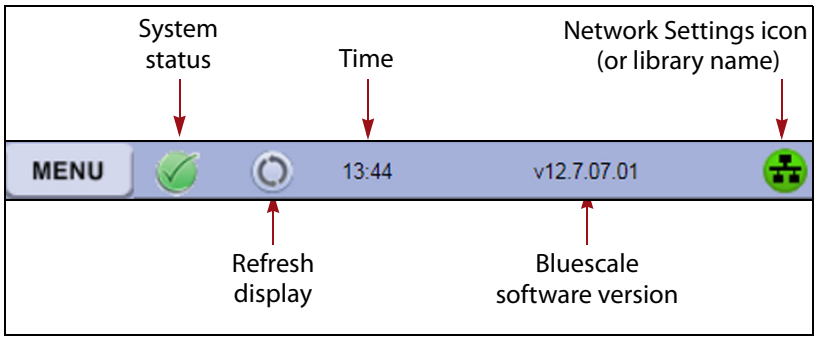


Figure 44 Information on the status bar.

MENU After you log in, the user interface displays a **MENU** button on the top left side of most screens. Clicking **MENU** displays the last menu screen you viewed; from there you can navigate through the user interface options. See Using the Menus on page 75 for a description of the available options.

Note: The **MENU** button also acts as a "back" button in most screens. It returns you to the top level menu in the given menu structure. For example, clicking **MENU** while you are viewing the Date & Time screen returns you to the **Configuration** menu screen.

System Status Icon The status icon on the status bar indicates the severity of the most current system message. Click the status icon to view system messages (see Check and Respond to Messages on page 143 for information about these messages).

The BlueScale user interface uses status icons indicate the status of library components. The following icons appear on the status bar and next to the major system components shown on the General Status screen (see Figure 37 on page 74). They also appear in other screens.

Icon	Meaning
	All system components are functioning correctly.
	An informational message about a system component is available. Check messages to determine the component.
	A system component requires attention. Check messages to determine the component.
	A system component experienced an error condition. Check messages to determine the component.

Refresh Display Button Refreshes (updates) the information currently displayed on the user interface. If you set a long interval for the refresh rate or disabled the automatic screen refresh by setting the refresh rate to zero (see Refresh Rate on page 110), you can refresh the screen manually by clicking the refresh display button.

Important

Do not use keyboard commands (for example, **F5**) to refresh the browser when connected to the BlueScale web interface. These keyboard commands can cause unpredictable results.

Remote Support Icon Provides you with online access to the support section of the Spectra Logic website where you can search the knowledge base, access the product documentation, and download BlueScale update packages and drivers. If you need additional assistance, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

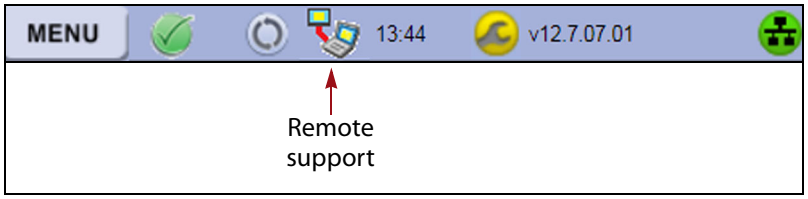


Figure 45 The Remote Support icon on the status bar.

The remote support icon is also used to activate secure remote access capabilities using Cisco WebEx technology. This remote access helps Spectra Logic Technical Support provide faster resolution of support calls. This capability is only enabled on an as-needed basis during a support call.

Notes:
- The remote support icon is only visible when you are accessing the library through the BlueScale web interface.
- When Spectra Logic Technical Support needs to launch a WebEx session to access your library, a link via email is sent.

Auto Download Icon If one or more package servers are configured to auto download firmware packages (See Configure a Package Server on page 132) and a new package was downloaded, the Auto Download icon (a wrench in a yellow circle) displays to indicate that an update package is ready for installation. Click the icon to navigate to the Package Update screen. See Updating the BlueScale Software and Library Firmware on page 421 for information on installing the update.

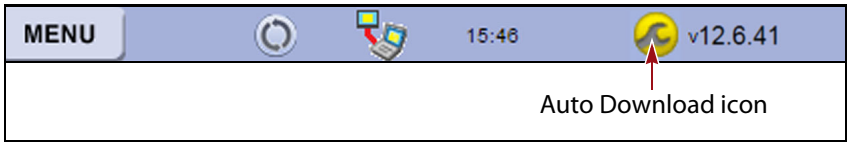


Figure 46 The Auto Download icon in the BlueScale status bar.

Last Refresh Time and Date Shows the last time that the screen was refreshed. The screen can be set to refresh at designated intervals (see Refresh Rate on page 110). The displayed information can always be refreshed manually by selecting the refresh display button.

BlueScale Software Version Shows the version of the BlueScale software currently being used by the library.

IP Address or Library Name Depending on how you are accessing the library, the status bar shows:

- The library's current IP address when you access the library using the touch screen.
- The library's name, if set, when you are accessing the library using the BlueScale web interface through a web browser connection.

  Note: If you are using the BlueScale web interface and you have not set the library name, the right-hand side of the status bar is blank.

If you need to view or set the library's IP address or name, see Configure Network Settings on page 98 and Library Name on page 110, respectively.

Progress Bar

When the library is busy processing a command, a horizontal progress bar displays above the status bar. Do not use the touch screen (or the BlueScale web interface) until the progress bar disappears.

Library Management

The library management features in the BlueScale user interface provide maximum configurability and ease of use for the library. To take full advantage of the library's versatility, read the following overview of the library's management features.

Automatic Email Alerts

Simple Mail Transfer Protocol (SMTP) allows users to receive library status information via email. When library messages are generated through the LCM, the library automatically sends email notifications to selected users. Information included in the notification consists of the message number, severity, details, remedy, and the time it was generated. Message types are Information, Error, Warning, and Fatal (see Check and Respond to Messages on page 143). You can select the types of messages sent as email alerts to each library user (see Configure Mail Users on page 107).

AutoSupport

AutoSupport helps manage problems you may experience with the library. It guides you through the process of sending email regarding library problems — along with library logs and configuration information — directly to internal support personnel or Spectra Logic Technical Support. See Chapter 11 – Configuring and Using AutoSupport, beginning on page 334 for detailed information.

User Security

Library users are assigned to one of three groups, each with its own set of pre-defined library privileges (also known as permissions). These privileges determine the type of operations a user can perform on the library and are the primary means for configuring library security. See Configuring Library Users on page 94 for detailed information about user groups and security.

Note: The encryption feature requires an additional, separate password to access the encryption features. See Passwords and Other Identifiers on page 305 for information about the encryption user.

USING THE BLUESCALE USER INTERFACE

The library's BlueScale user interface lets you set configuration options, view library and drive information and metrics, manage media, and monitor library operations.

Note: Unless otherwise specified, references to the user interface screens apply to both the touch screen on the library operator panel and the screens presented through the BlueScale web interface.

Log Into the User Interface

Overview Before you can manage or configure the library, you must log into the BlueScale user interface. After the library completes its initial power-on processes, the Login screen displays on the library operator panel. This Login screen also displays when you access the library remotely using the BlueScale web interface (RLC), as well as when you switch users.

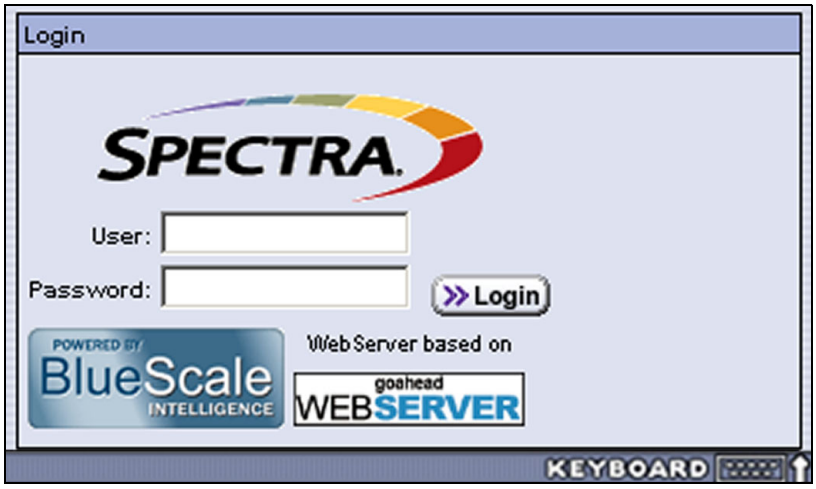


Figure 47 The BlueScale Login screen.

Pre-Login General Status If there is no interaction with the operator panel within 30 seconds after the Login screen displays, the Login screen is replaced by the pre-login General Status screen. This General Status screen provides at-a-glance status for the library and its components without requiring you to log into the library. You can view the status of the entire library or a specific partition.

Note: The pre-login General Status screen does not display when you access the library remotely through the BlueScale web interface.

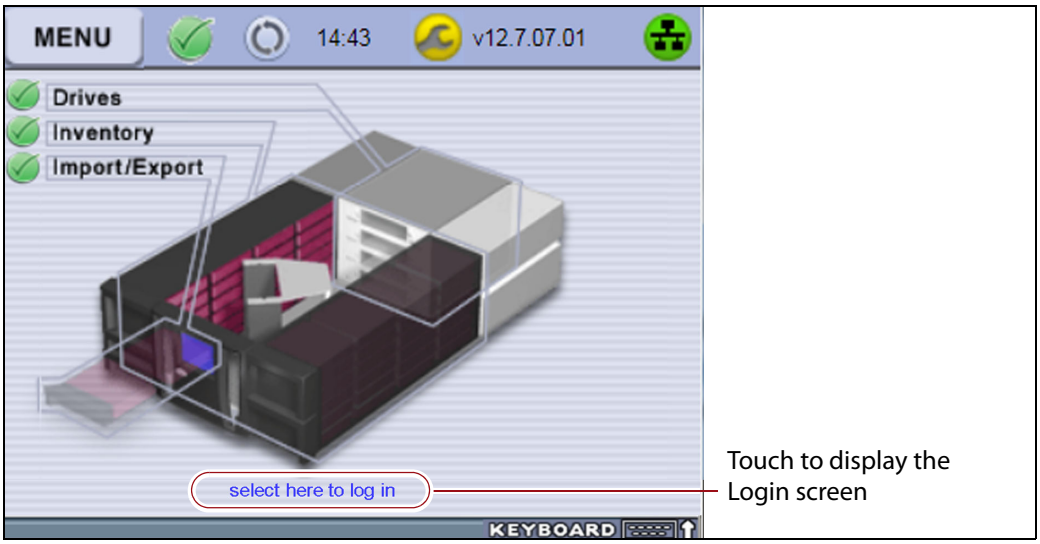


Figure 48 Click anywhere on the pre-login General Status screen to display the Login screen.

Log In Use the following steps to log into the library:

1. Connect to the library. The method depends on how you are accessing the library.

   Using the front panel touch screen or a direct connection to the LCM

   - If the Login screen is displayed, skip to Step 2 on page 88.
   - If the pre-login General Status screen is displayed, touch or click **select here to login** at the bottom of the screen to display the Login screen and then skip to Step 2 on page 88.

   Note: If the soft keyboard is open and covering the bottom of the pre-login General Status screen, touch the keyboard icon to close the soft keyboard or use the scroll bar on the right side of the screen to scroll down to the bottom of the screen.

Connecting to the library remotely using the BlueScale web interface

Enter the IP address of the T50e in the address bar of a web browser on a computer on an active network that has access to the library. The steps you use depend on whether SSL is enabled or not.

Note: The T50E uses TLS 1.0 and does not have functionality for higher versions of TLS.

If SSL is...	Use the following steps...
Not enabled (the default setting)	**1.** Enter the IPv4 or IPv6 address configured for the library in the format: **`http://[library IP address]`** (see Configure Network Settings on page 98). **2.** The BlueScale Login screen displays (see Figure 49 on page 88). Proceed to Step 2 on page 88.
Enabled	**1.** Enter the IPv4 or IPv6 address configured for the library in the format **`https://[library IP address]`** See Enable SSL on page 111 for information about enabling SSL. **Important:** When using SSL, you must prefix the IP address with https:// instead of just entering the IP address. **Important:** The T50E uses TLS 1.0 and does not have functionality for higher versions of TLS. **2.** If you receive a warning about the website's security certificate, choose to ignore or resolve the warning. **Notes:** ▪ The security warning only appears if you have not resolved the security certificate warning, either by storing a valid security certificate on the library (see Install a Security Certificate and Authentication Key on page 123) or by creating a security exception for the library on the browser (method depends on the browser you are using). ▪ If you do not resolve the warning, you will receive the warning about the security certificate each time you access the BlueScale web interface. **3.** The BlueScale Login screen displays (see Figure 49 on page 88). Proceed to Step 2 on page 88.

2. Click 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.

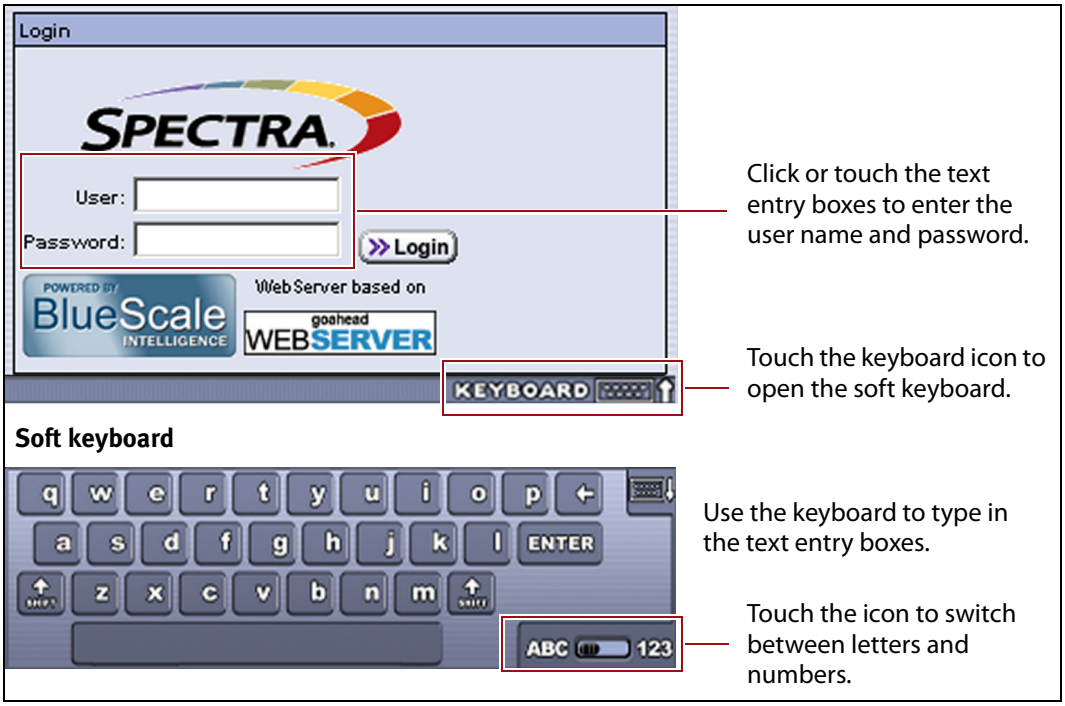


Figure 49 Log into the library using the Login screen.

3. Type your user name (**su** is the default user name for a superuser).

   See Understanding User Groups and Security on page 94 for information about the three types of user groups and the options and controls accessible to each user group.

4. Type your password in the **Password** text box. If you log in as one of the default users, there is no password (unless you configured one).

   Note: By default, passwords are not required to log into the library. If you want to password-protect access to the library, set passwords for each user as described in Configuring Library Users on page 94.

5. Click **Login**. The library's General Status screen displays.

   Note: If you powered-on or reset the library, there may be a delay after you click **Login** while the library completes its initialization. When the initialization is complete, the General Status screen displays.

   - When there are messages to report at login, the BlueScale user interface displays the Messages screen first. Read the messages and take action as necessary.

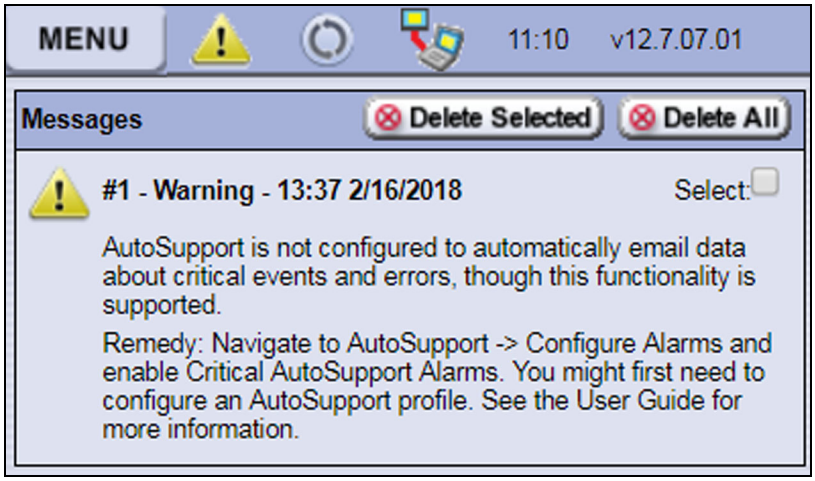


Figure 50 The Messages screen.

   - If there are no messages to report, the General Status screen displays.

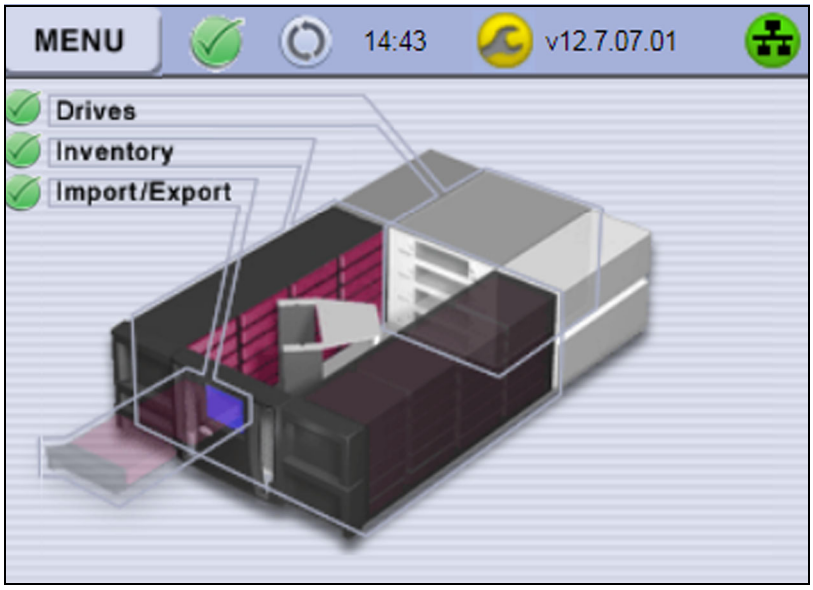


Figure 51 The General Status screen.

6. Click **MENU** to display the General menu.

7. If you want to configure encryption settings or keys, select **Security** ⋯⁘ **Encryption** to log into the encryption feature. See Chapter 10 – Encryption and Key Management, beginning on page 289 for detailed information about configuring and using either Spectra SKLM or BlueScale Encryption key management.

Log Off or Switch Users

1. If a screen other than the Login screen is displayed, click **MENU** and then select the **Security** menu to display the Security options.

Figure 52 Select **Switch Users** on the Security menu to log out.

2. Click **Switch Users** to log the current user out and redisplay the Login screen.
3. If desired, log in again using the same or a different user name and password.

Enter Information on Screens

Entering information on a user interface screen requires using one of the following methods.

BlueScale Web Interface

The BlueScale web interface lets you use your computer keyboard to enter information into the user interface and a mouse to navigate through the user interface screens (see BlueScale Web Interface on page 73). Using the web interface is the most convenient way to enter large amounts of information when you are configuring the library.

Important

- When accessing the library remotely through a web browser, do not use the **Enter** key on your keyboard when making selections in the BlueScale user interface. Various web browsers handle the **Enter** key differently, causing inconsistent behavior in the BlueScale interface. Also do not use any of the keyboard function keys.
- Always use your mouse to make selections and click the buttons in BlueScale screens instead of using your keyboard. Only use the keyboard for typing information into text fields.
- Do not use the browser's "back" button to return to a previously viewed BlueScale screen. Always use the BlueScale toolbar and buttons on the screen to navigate the BlueScale web interface.
- Using a keyboard command (for example, **F5**) to refresh the browser when connected to the BlueScale web interface causes unpredictable results.

Note: Functions that require physical interaction with the library (for example, importing or exporting cartridges) are not available when using the BlueScale web interface.

Soft Keyboard

When using the touch screen on the operator panel, select the keyboard icon in the lower right corner of any screen to activate the on-screen keyboard. When the keyboard is extended, an icon in the lower right corner lets you select between alphabetic or numeric characters. Use a stylus or your finger to select fields and enter alphanumeric information using the keyboard. Touching the keyboard icon again closes the soft keyboard.

External Keyboard and Mouse

If you cannot use the BlueScale web interface, you can connect an external USB keyboard to one of the USB ports on the LCM (see Figure 10 on page 35) when you need to enter large amounts of information. The user interface options available when you use an external keyboard are the same as when you use the library's touch screen operator panel.

Important Not all characters on a USA-type keyboard are supported in the BlueScale user interface. If a character does not appear on the soft keyboard, then its use is not supported.

Notes:

- Make sure that the keyboard cable is long enough to reach the front of the library so that you can view the front panel while typing.
- If using a non-USA type keyboard, you must find the equivalent for some characters like the back slash or forward slash.
- You can connect a USB mouse to one of the USB ports on the LCM and use it for making selections on the user interface.

Feedback Required Screens

When the BlueScale software needs you to make a selection or perform an action it displays a Feedback Required screen. If you do not respond to the Feedback Required screen within 10 minutes, the request times out and the action fails.

CHAPTER 4

Configuring the Library

This chapter describes the procedures for configuring the library's system settings, including the users, the network connections, and optional features.

CONFIGURING LIBRARY USERS

Overview Every library user is assigned to a group, each with its own set of pre-defined library privileges (also known as permissions). These privileges determine the type of operations a user can perform on the library. These privileges are the primary means for configuring library security.

User Privilege Requirements Only a user with superuser privileges can add, modify, or delete users.

Understanding User Groups and Security

Before you begin, read this section to understand the three types of user groups and what types of privileges each has. By default, passwords are not set for any of the three default users.

Note: If encryption is enabled, there is an additional, separate password to access the encryption features. See Passwords and Other Identifiers on page 305 for information about the encryption user.

The following table describes the three user groups and the privileges of each. By default, passwords are not required for any of the three default users.

User Group Type	Description	Default User Name
Superuser	Controls all aspects of the library's configuration and operation, including defining other library users and assigning them to a user-privilege group. **Notes:** ▪ The library requires a minimum of one superuser. You cannot delete the last member of the Superuser group. ▪ Only a user with superuser privileges can add, modify, or delete users. ▪ Only a user with superuser privileges can access and configure encryption features.	**su**
Administrator	Configures and uses the library. With the exception of creating or modifying library users and accessing the Encryption features, users in the Administrator group have the same privileges as users in the Superuser group.	**administrator**
Operator	Performs day-to-day operations. Users assigned to the Operator group move, import, and export media, but cannot gain access to more sensitive library operations such as Configuration, Diagnostics, and Security.	**operator**

Add a New User

Use the following steps to add a new library user and assign that user to a user group.

1. Log into the library as a user with superuser privileges (see Log Into the User Interface on page 85).
2. If necessary, click **MENU** to display the Menu screen.
3. Click **Security** ···⁘ **Edit Users**. The Edit Users screen displays.

Figure 53 Click **New** on the Edit Users screen to add a new user.

4. Click **New** to display the New User screen.

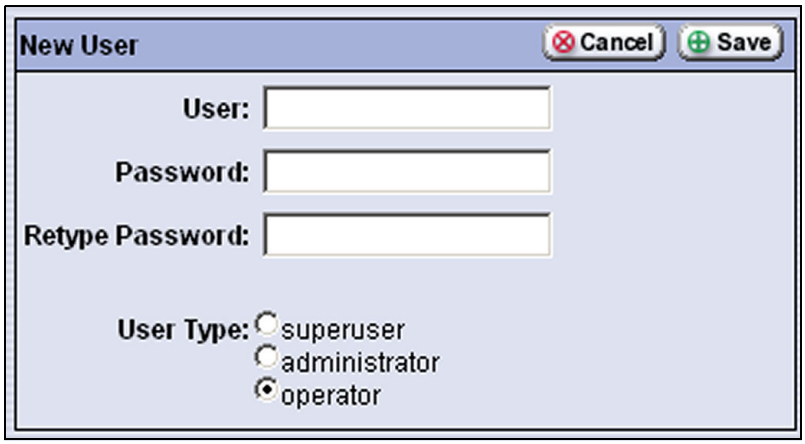


Figure 54 Enter the information for the new user.

5. Complete the information on the New User screen.

   Note: User names and passwords can contain any combination of the numbers 0-9, lower and upper case alphabetic characters (a-z and A-Z), and the at symbol (@), dash (-), underscore (_), period (.), forward slash (/), and space characters. There is no limit to the length but that we recommend lengths of less than 2048 characters.

For this field...	Enter...
User	The name for the user.
Password **Retype Password**	A password for the user; retype the password to confirm. **Notes:** ▪ For security, the text in the **Password** and **Retype Password** fields is shown as asterisks (*). ▪ Though highly recommended, passwords are not required for any of the three user types.
User Type	Select the group to which the user belongs. **Note:** See Understanding User Groups and Security on page 94 for descriptions of the user groups and privileges associated with each.

6. Click **Save**. The new user name and group assignment is added to the list of users on the Edit Users screen.
7. Repeat Step 4 through Step 6 for each additional library user.

Modify an Existing User

Important If you set the passwords for the default users (su, operator, administrator), make sure that you keep a record of the new passwords. If the default superuser is the only user configured and you do not know the password, you are not able to access the library or reset any forgotten passwords.

Use the following steps to change the settings for an existing user.

1. Log into the library as a user with superuser privileges.
2. If necessary, click **MENU** to display the Menu screen.
3. Click **Security** ···⁘ **Edit Users**. The Edit Users screen displays with a list of library user names (see Figure 53 on page 95).
4. Find the user's name, then click **Edit** next to the name.
5. Change the user's name, password, group, or any combination of these.
6. Click **Save** to save your changes.

Delete an Existing User

Use the following steps to delete an existing user.

Important If you delete the default users, make sure that you keep a record of at least one superuser name and password.

Note: The library requires there to be a minimum of one user assigned to the superuser group. You cannot delete the last member of the superuser group.

1. Log into the library as a user with superuser privileges.
2. If necessary, click **MENU** to display the Menu screen.
3. Click **Security ⋯ Edit Users**. The Edit Users screen displays with a list of library user names (see Figure 53 on page 95).
4. Locate the name of the user you want to delete, then click **Delete** next to that user's name.

   When the screen refreshes, the user list on the Edit Users screen no longer includes the user name you just deleted.

CONFIGURING THE GLOBAL SYSTEM SETTINGS

This section describes how to modify the library's global configuration settings. All of the global system settings are accessed through the Configuration menu.

Access the Configuration Menu

1. Log into the library as a user with superuser or administrator privileges.
2. If necessary, click **MENU** to display the Menu screen.

3. Click **Configuration** to display the Configuration menu.

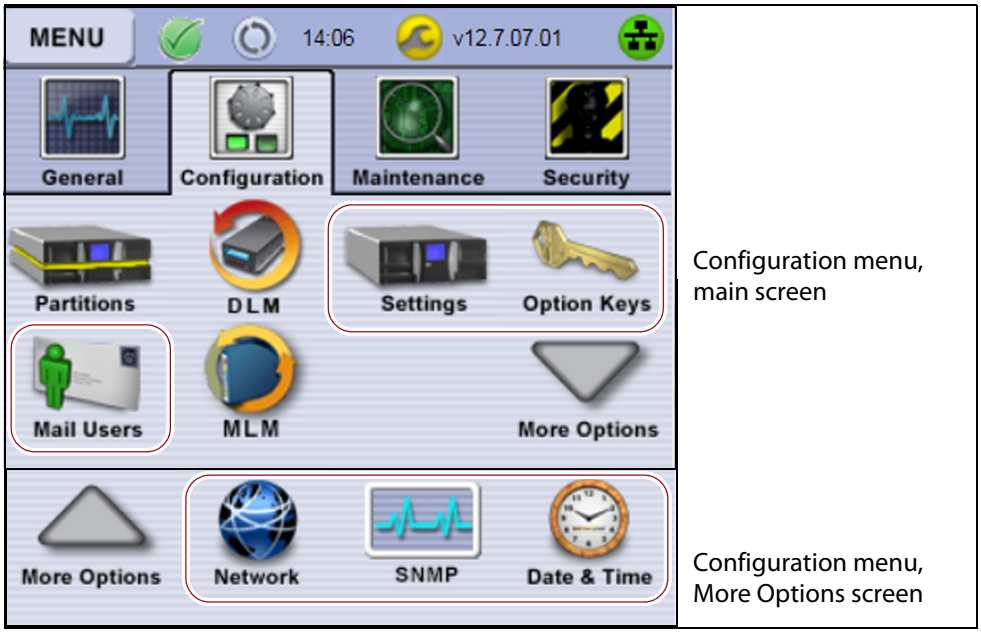


Figure 55 The configuration options on the Configuration menu.

Configure Network Settings

Spectra Logic highly recommends that you connect the library to an Ethernet network and configure it for network access as described in this section. Network access lets you perform the following operations:

- Access the BlueScale web interface for remote management of the library using a standard web browser.
- Open support incidents or send ASLs (AutoSupport Logs) to Spectra Logic Technical Support for troubleshooting directly from the library.
- Automatically email system messages or reports to configured mail users.
- Automatically send a notification to a specified mail recipient when certain critical events occur.
- Download the latest BlueScale update package from Spectra Logic's Support portal directly to the library.

These functions are not available if you do not connect the library to an Ethernet network.

The Network Settings icon displays in the upper right corner of the touch screen operator panel (see Figure 55 on page 98).

Note: If you are accessing the library remotely through the BlueScale web interface, the library name, if configured, displays instead of the Network Settings icon. If the library name is not configured, the upper right corner of the screen is blank.

Using DHCP Addressing By default, the IP address for the Ethernet port on the LCM is set automatically using the Dynamic Host Configuration Protocol (DHCP).

Notes:
- If you select DHCP addressing, the LCM must be connected to an Ethernet network that has a DHCP server to obtain an IP address.
- Do not select DHCP addressing if your network does not have a DHCP server.

Using Static IP Addressing If your network does not use DHCP, or if you want the library to use a fixed IP address, you can configure a static (fixed) IP address as described in this section. Using a static IP address ensures that the IP address for the library remains constant and is highly recommended, especially if you plan to manage the library remotely using the BlueScale web interface.

Prepare the Library

Important If you want to change the network settings of the library, make sure that the library is connected to the network *before you power on the library*.

Before configuring the network settings, make sure that you address the following requirements:

- The library is connected to an active link on the Ethernet network.
- A unique IP address is available on the network if you plan to use a static IP address. This address cannot be in use by another device.
- The DHCP server is configured on the network if you plan to use DHCP addressing.

Set the IP Addressing

Use the following steps to configure the library for Ethernet network access.

1. Log into the library as a user with superuser or administrator privileges.
2. If necessary, click **MENU** to display the Menu screen.
3. Click **Configuration** to display the Configuration menu.
4. On the Configuration menu, click **More Options** (down arrow) to display additional configuration options.
5. Click **Network**. The Network screen displays. This screen changes depending on whether the library is configured to use DHCP or Static IP addressing.

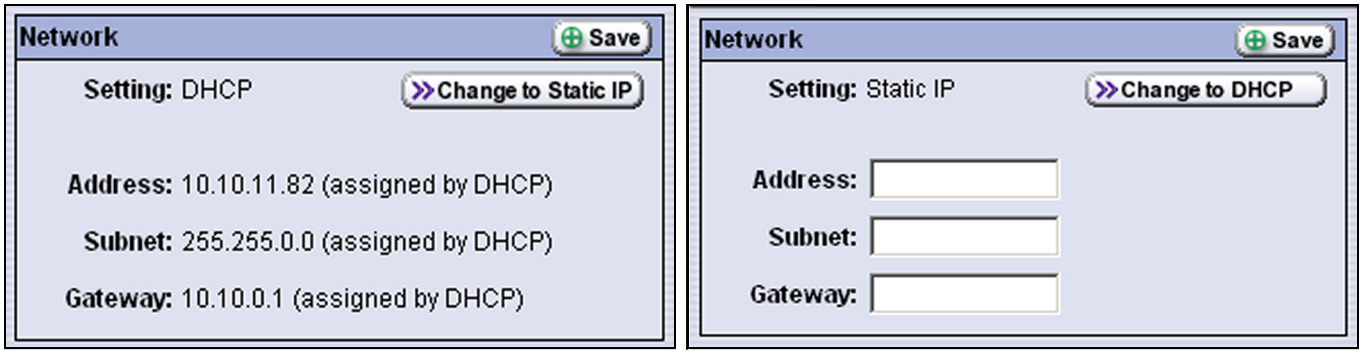


Figure 56 The Network screen for BlueScale 12.7.03 and earlier.

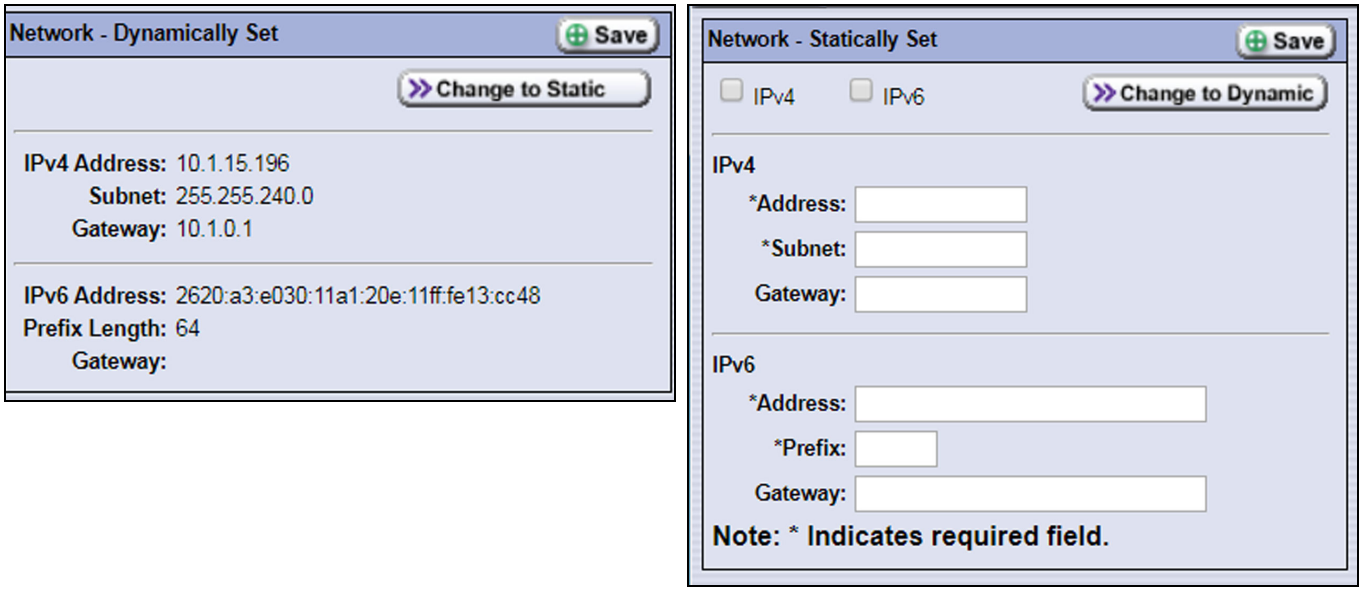


Figure 57 The Network screen for BlueScale 12.7.07 and later.

6. Decide which type of addressing you want the library to use.
   - **DHCP** (default setting)—The library is issued an IP address by the DHCP server.
   - **Static** (highly recommended)—The library uses a fixed IP address. If you select static addressing, enter the following information.

     Note: When entering IP addresses, do not include http: or https:

For BlueScale12.7.03 or earlier:

For this field...	Enter...
Address	A valid IPv4 address.
Subnet	The subnet mask. The subnet mask must be a valid IPv4 address.
Gateway	A valid network gateway IPv4 address. Enter 0.0.0.0 for the Gateway if your network does not use a gateway.

For BlueScale12.7.07 or later:

For this field...	Enter...
If the IPv4 check box is selected: (if the IPv4 check box is not selected, the IPv4 address defaults to 127.0.0.1 and is effectively disabled)	
Address	A valid IPv4 address.
Subnet	The subnet mask. The subnet mask must be a valid IPv4 address.
Gateway	A valid network gateway IPv4 address. Leave the field blank if the network does not use a gateway.
If the IPv6 check box is selected:	
Address	A valid IPv6 address. The library compresses the IPv6 address when saved.
Prefix	Enter an integer between 1 and 128 to indicate the portion of the IPv6 address that indicates a group of IP addresses on the same network.
Gateway	A valid network gateway IPv6 address. Leave the field blank if the network does not use a gateway.

7. Click **Save** to change the IP addressing.

   Note: The library's IP address changes as soon as you click **Save**. As a result, if you are connected to the library through the BlueScale web interface the connection to the library is lost. Reconnect to the library using the new IP address.

Enable and Configure SNMP

Overview Simple Network Management Protocol (SNMP) is a protocol for monitoring the health and welfare of your library by using integrated alerts.

Note: Spectra Logic libraries use SNMPv2c.

Network-Based Library Management If you are using a network-based library monitor/management application other than the library's BlueScale user interface, you may need to configure the library's SNMP settings in the application.

Configure SNMP Use the following steps to enable and configure SNMP.

1. Log into the library as a user with superuser or administrator privileges.
2. If necessary, click **MENU** to display the Menu screen.
3. Click **Configuration** to display the Configuration menu.
4. On the Configuration menu, click **More Options** (down arrow) to display additional configuration options.
5. Click **SNMP**. The SNMP Settings screen displays.

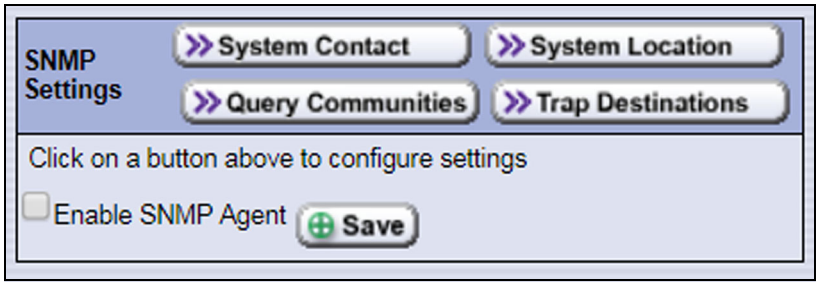


Figure 58 The SNMP Settings screen.

6. Click **System Contact**. The Edit System Contact screen displays.

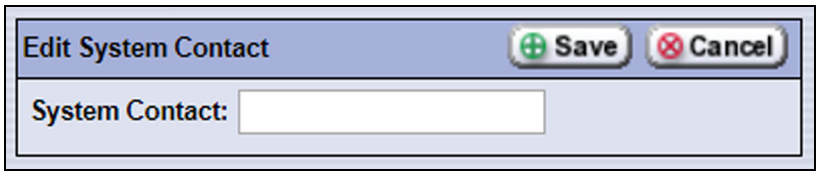


Figure 59 The Edit System Contact screen.

7. In the **System Contact** field, enter the value for the sysContact object and then click **Save**. The SNMP Settings screen redisplays.

8. Click **System Location**. The Edit System Location screen displays.

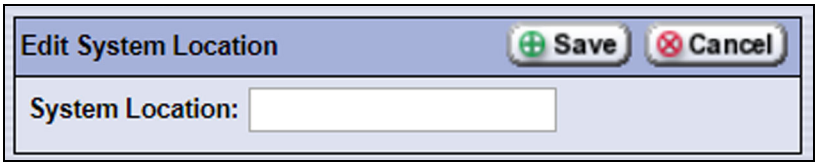


Figure 60 The Edit System Location screen.

9. In the **System Location** field, enter the value for the sysLocation object and then click **Save**. The SNMP Settings screen redisplays.
10. Click **Query Communities**. The Valid Query Communities screen displays listing all SNMP communities to which the library currently belongs. The library only responds to SNMP queries from members of these communities.

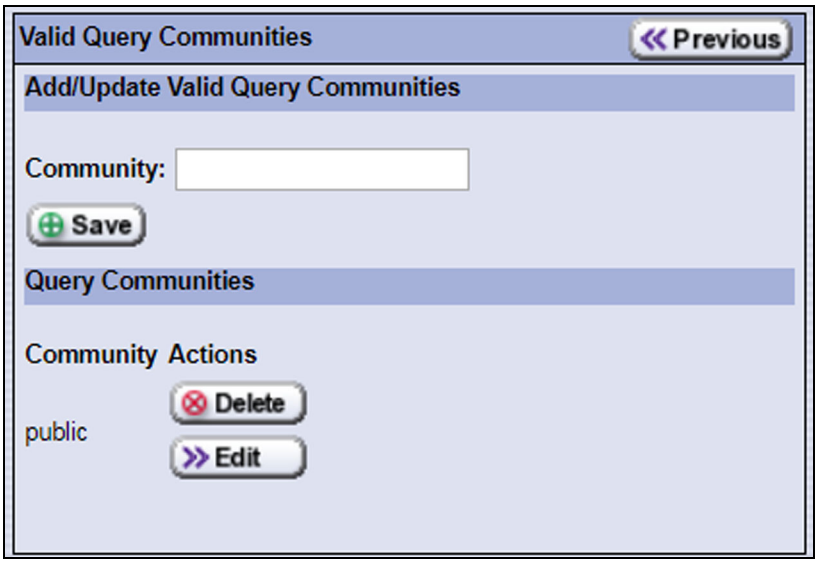


Figure 61 The Valid Query Communities screen.

Make changes to the query communities as needed:

Action	Instructions
Add	Enter a community name in the Community field and click **Save**. **Important:** Community strings are case sensitive. If the library is configured to include the community called "OurCommunity," it answers to queries from OurCommunity but not from a community called "ourcommunity."
Delete	Click **Delete** next to a community name to remove it.
Edit	Click **Edit** next to a community name to display the name in the Add/Update Valid Query Communities pane. Make any required changes and click **Save**.

11. When all desired community strings are configured, click **Previous** to return to the SNMP Settings screen.

12. Click **Trap Destinations**. The Trap Destinations screen displays listing all trap destinations to which the library sends SNMP traps.

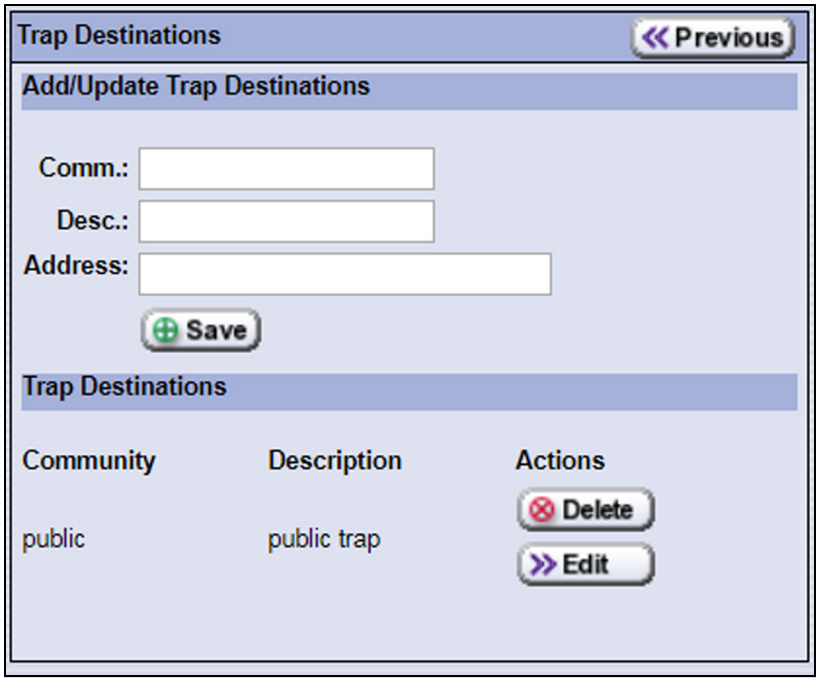


Figure 62 The Trap Destinations screen.

Make changes to the trap destinations as needed:

Action	Instructions
Add	Enter the Community, Description, and IPv4 or IPv6 Address in the appropriate fields and click **Save**. **Notes:** ▪ Only one community at a time may contain IPv6 addresses. ▪ The library compresses the IPv6 address when saved.
Delete	Click **Delete** next to a trap destination to remove it.
Edit	Click **Edit** next to a trap destination to display the name the configuration information in the Add/Update Trap Destination pane. Make any required changes and click **Save**.

13. When all desired trap destinations are configured, click **Previous** to return to the SNMP Settings screen.

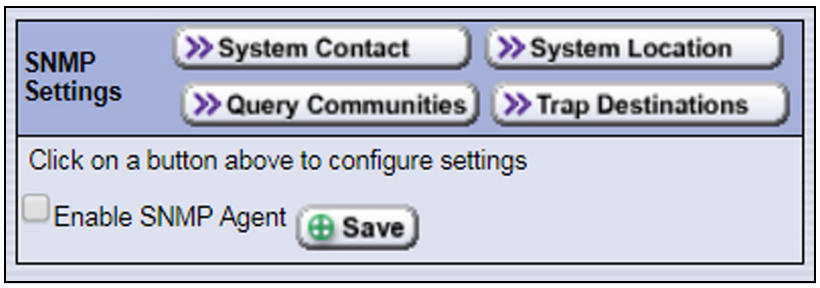


Figure 63 The SNMP Settings screen.

14. Select **Enable SNMP Agent** and click **Save**.

    The agent returns information contained in the library's Management Information Base (MIB) to the workstation used to manage the network. The MIB defines what information is available from the library over the network. The MIB file is available for download from the **Downloads** ⋯ **Tools** page of the support portal.

15. Click **MENU** to return to the Configuration menu.

Set the Date and Time

Use the following steps to configure the library's system clock.

Note: The time shown on the status bar does not continually update. It is updated based on the refresh rate you set for the web server (see Configure the Library Web Server Settings on page 110).

1. Log into the library as a user with superuser or administrator privileges.
2. If necessary, click **MENU** to display the Menu screen.
3. Click **Configuration** to display the Configuration menu.
4. On the Configuration menu, click **More Options** (down arrow) to display additional configuration options.
5. Click **Date & Time**. The Date & Time screen displays showing the method currently selected for setting the date and time.

   Note: The values in the Date & Time counters do not wrap. For example, to change the month from December to January, click and hold the **–** button to decrement the month.

Figure 64 Set the date and time for the library.

6. Use the **+** and **–** buttons to set the month, day, year, hour, and minute to display.

   Note: Instead of clicking the **+** or **–** button multiple times, you can click and hold the button to advance through the available values.
7. Click **Save**.
8. Click **MENU** to return to the Configuration menu.

Configure Mail Users

Mail users are the preconfigured recipients of email notifications generated by the library. The library can automatically send email notifications to selected mail users whenever a specified message type is generated. Email notifications can also be sent on demand when traces are run, reports are generated, or the library's configuration data is backed up. The email includes attachments containing any system messages, traces, or diagnostic results associated with the notification. The library can also send AutoSupport messages to selected mail users.

Important

You must edit the **autosupport@spectralogic.com** mail user to configure the SMTP server if you want to open an AutoSupport ticket directly from the library (see Chapter 11 – Configuring and Using AutoSupport, beginning on page 334). This mail user is also used to send the ASL and HHM files that the library generates to Spectra Logic Technical Support when troubleshooting a problem.

Note: You must configure the library's IP address as described in Configure Network Settings on page 98 before you can configure mail recipients.

1. Log into the library as a user with superuser or administrator privileges.
2. If necessary, click **MENU** to display the Menu screen.
3. Click **Configuration** to display the Configuration menu.
4. Click **Mail Users**. The Mail Users screen displays.

Note: If you do no configure any mail users, this screen only shows the default mail recipient for Spectra Logic autosupport.

Figure 65 Use the Mail Users screen to configure mail recipients.

5. Do one of the following:
   - Click **New** to add a mail user.
   - Click **Edit** to modify an existing mail recipient.
   - Click **Delete** to remove an existing mail recipient. Click **Yes** on the Confirmation screen.
   - Click **Test** to send a test message to the Mail User.
6. Enter or update the information for the mail user.
   - For a new mail user, enter their information on the New Mail User screen.
   - For an existing mail user, update their information on the Edit Mail User screen.

     Note: A previously entered IPv6 address displays compressed.

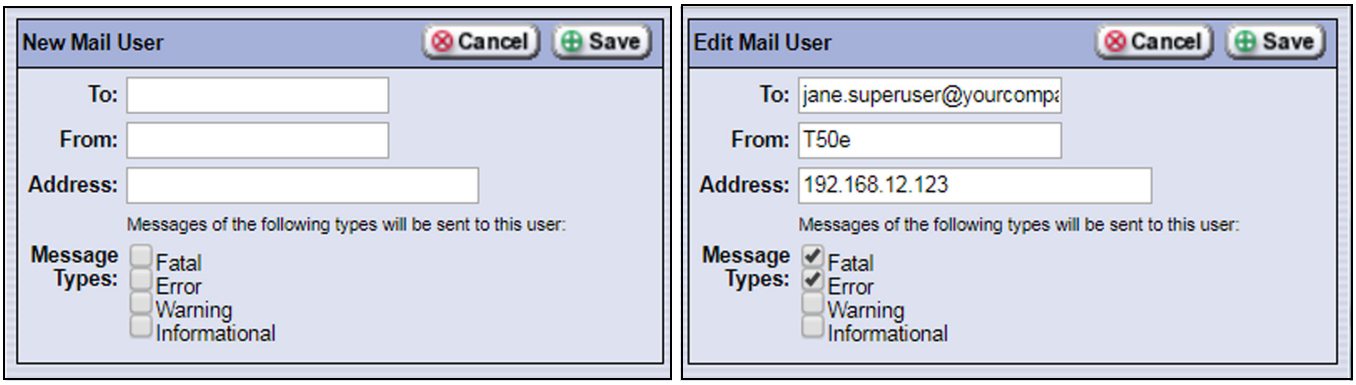


Figure 66 Enter or modify the information for the mail user.

For this field...	Do the following...
To	Enter the email address of the recipient. Be sure to use the full email address using the standard email format, including the @ symbol. **Important:** The email address cannot contain spaces or other non-alphanumeric characters (for example, an ampersand, &). To include multiple addresses, leave a space between each address.
From	Enter an alphanumeric string to uniquely identify the library (for example, the name or location of the library). **Important:** The string cannot contain spaces or most non-alphanumeric characters (for example, the & or the % symbols).
Address	Enter the IPv4 or IPv6 address of your SMTP server in the **SMTP IP Address** field. **Note:** The library compresses the IPv6 address when saved.

For this field...	Do the following...
Message Types	Select the type(s) of messages that the mail user should receive by selecting one or more of the message types listed. ▪ **Fatal** — An error occurred that prevents the library from continuing operation. Immediate attention is required. ▪ **Error** — An error occurred that impacts the operation of the library. Determine the cause of the error and remedy as soon as possible. ▪ **Warning** — The library detected conditions that may impact operation. Determine the cause of the problem and remedy as soon as possible. ▪ **Informational** — Activities that generate system messages occurred. **Notes:** ▪ Selecting a message type automatically sends all messages of that type to the recipient as they are generated by the library. ▪ If no message type is selected, the library does not automatically send an email to the mail user. However, messages can still be sent to the mail user on an individual basis when traces or diagnostics are run. ▪ Do not select message types for the autosupport@spectralogic.com mail recipient. This mail recipient is only used to receive AutoSupport ticket requests or ASL and HHM files that are generated by the library.

7. Click **Save**. The Mail Users screen redisplays (see Figure 65 on page 107).
8. If desired, select **Test** next to the newly added mail recipient to send a test email.
9. Repeat Step 5 on page 108 through Step 7 on this page to configure or modify additional email recipients.
10. Click **MENU** to return to the Configuration menu.

Configure the Library Web Server Settings

Use the following steps to configure the library name, refresh rate, web server port, and automatic configuration save settings.

1. Access the Configuration menu (see Access the Configuration Menu on page 97).

   Note: If the secondary Configuration menu is displayed, click **More Options** (up arrow) to display the main Configuration menu.

2. On the Configuration menu, click **Settings** to display the Settings screen.

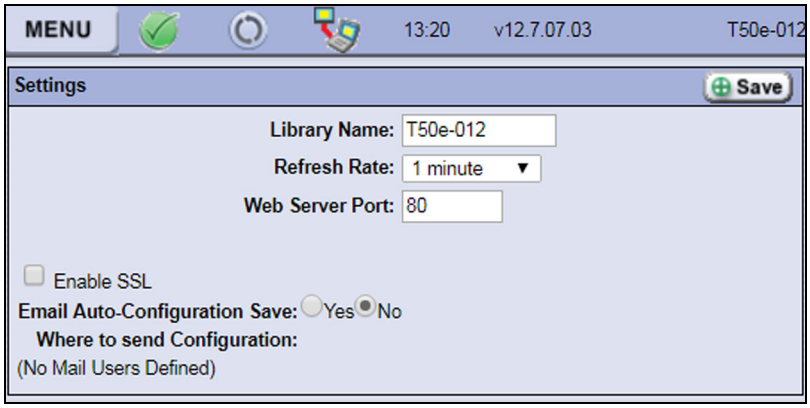


Figure 67 Set the configuration information.

3. Change the settings on this screen as required for your environment.

For this setting...	Do the following to change....	Default
Library Name	Set the name used to identify the library in messages it sends to mail recipients. Use a name that helps identify the library to a remote user.	blank (no name set)
Refresh Rate	Use the **Refresh Rate** drop-down list to set how frequently the information on the BlueScale user interface screens is refreshed. **Notes:** ▪ You can manually refresh the displayed information at any time by selecting the refresh button located at the left end of the status bar (see Status Bar on page 81). ▪ If you want to disable automatic refreshing of the display, set the refresh rate to **never**. ▪ If you use something other than the default refresh rate or disable automatic refreshing, you must reset the refresh rate every time you log into the library.	1 minute

For this setting...	Do the following to change....	Default
Web Server Port	Enter a port number from 0 to 65,535 for the dedicated Ethernet port used to access the library's embedded web server. The default port number is 80, which is appropriate for most installations and is strongly recommended. If you use a port number other than 80, the port number must be explicitly entered into the web browser when accessing the library remotely. **Important:** Do not set the web server port to 443. Using this port number causes the front panel display to become unstable. **Notes:** ▪ The Web Server Port field does not display if SSL is enabled. ▪ If you change the web server port, you must enter a colon (:) after the library's IP address and then the new port number when accessing the library through the BlueScale web interface (for example, 192.165.10.11**:90**).	80
Enable SSL	Select the **Enable SSL** check box to enable Secure Socket Layer (SSL) access to the BlueScale web interface. **Important:** Enabling SSL configures the BlueScale web interface to use a secure Internet connection. You must prefix the IP address with **https://** instead of just entering the IP address when accessing the BlueScale web interface. **Important:** The T50E uses TLS 1.0 and does not have functionality for higher versions of TLS.	Cleared (Disabled)
Email Auto Configuration Save	Enable or disable sending the Auto Configuration Save file to a previously configured mail recipient. See Back Up the Library Configuration Automatically on page 117 for information about the Auto Configuration Save file. **Important:** To use this automatic email option, you must first configure the person to whom you want the backup file sent as a mail user (see Configure Mail Users on page 107). **Note:** The Auto Configuration Save file is always generated, regardless of whether you select to email it.	No (Disabled)
Where to send Configuration	If you enabled emailing the Auto Configuration Save file, select the recipient that you want to automatically receive the Auto Configuration Save file each time it is generated. To configure mail users, see Configure Mail Users on page 107. **Note:** If you do not configure one or more mail users, you cannot make selections for this option.	Blank (No mail users configured —OR— No mail user selected)

4. Click **Save**.

   Note: If you enabled SSL, click **OK** in response to the notification about resetting the web server. Wait for the web server to reset (approximately 2 to 3 minutes), and then log back into the library using **https://**.

5. Click **MENU** to return to the Configuration menu screen.

6. If you changed the web port number, reset the library to enable the new setting (see Resetting the Library on page 372). Make sure that there are no backups running before you reset the library.

ENABLING BLUESCALE SOFTWARE SUPPORT, OPTIONS, AND UPGRADES

Overview Activation keys are required to enable the BlueScale Software Support license and any library options and upgrades you purchase. These activation keys are tied to the library Hardware ID (serial number).

Requirements for updating the library BlueScale software A valid BlueScale Software Support key is required in order to update the library's BlueScale software and component firmware. When you renew or extend your service contract, you receive an activation key that must be entered into the library to enable continued BlueScale updates.

Important

Your initial library purchase includes a BlueScale Software Support key that is valid for the duration of the warranty period, or for the duration of any uplifted or extended service contract you purchased with the library, whichever is longer.

When you renew or extend your service contract, you must obtain a new BlueScale Software Support key (see Purchase the Option on page 114) and enter the new key into the library to allow continued access to BlueScale upgrades. If you have questions about your service agreement, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

Standard and upgraded options for the library The default library configuration includes a basic set of options that lets you start using the library immediately. These options do not require activation keys to enable them. When you purchase upgraded options or additional Capacity on Demand (CoD), you receive an activation key that must be entered into the library to enable the options. See Library Support and Upgrades on page 495 for information about the available upgrade options.

Purchase Additional Options or Features

This section describes how to obtain activation keys for new options *after* the initial installation and enter them into the library. See Renewing the BlueScale Software Support Key on page 419 if you need to renew or extend your service contract, which includes the BlueScale Software Support key.

Important The BlueScale Software Support key and all option activation keys are tied to the library serial number. If you have multiple libraries, you need separate activation keys for each library.

Determine the Hardware ID

The library Hardware ID is required for renewing or extending your service contract, which includes the BlueScale Software Support key, and for purchasing additional Capacity on Demand (CoD) or other upgrade options.

1. Access the Configuration menu (see Access the Configuration Menu on page 97).

   Note: If the secondary Configuration menu is displayed, click **More Options** (up arrow) to display the main Configuration menu.

2. On the Configuration menu, click **Option Keys** to display the Option Keys screen. The Hardware ID appears near the top of this screen.

   Note: The Hardware ID is a ten-character alphanumeric string. If the Hardware ID shown on the Option Keys screen is a seven-digit number, contact Technical Support for assistance in obtaining the Hardware ID you should use for your portal account and when purchasing activation keys. See Contacting Spectra Logic on page 7.

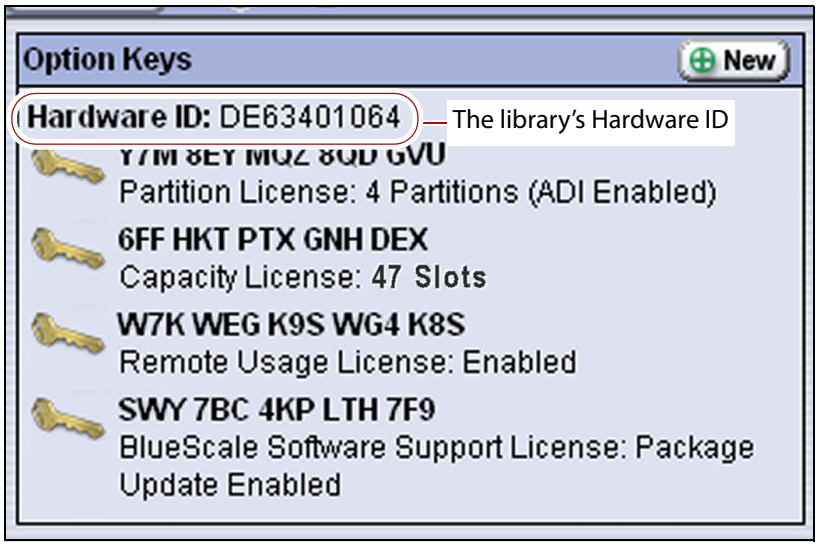


Figure 68 Locate the library's Hardware ID.

3. Make a record of the library's Hardware ID; it is needed when renewing your BlueScale Software Support contract or purchasing options for the library.

   Note: The library's hardware serial number is printed on the Product ID tab that slides out from the bottom of the library. The Hardware ID and the hardware serial number are typically the same, but not always. If the two are different, use the Hardware ID shown on the Option Keys screen.

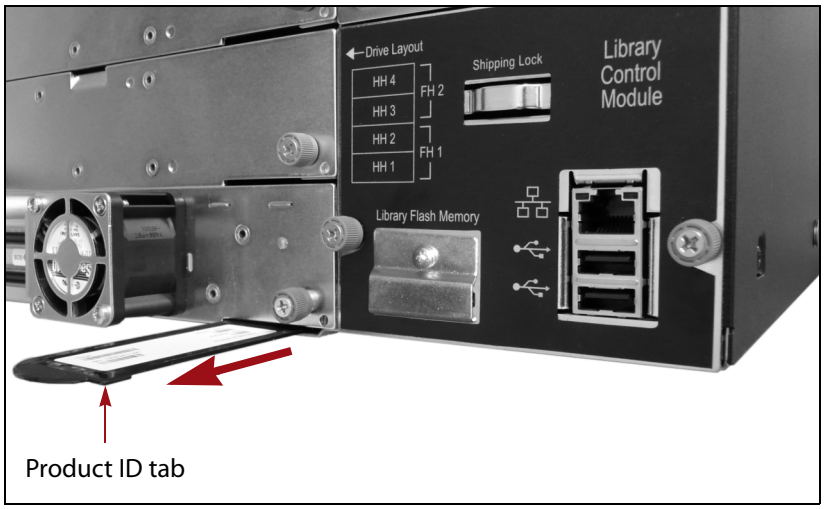


Figure 69 Slide the product ID tab out from the bottom of the library to view the library's serial number.

Purchase the Option

1. Contact your Spectra Logic sales representative to order the desired options (see Contacting Spectra Logic on page 7).

Important If you have multiple libraries, you need separate activation keys for each one.

2. When your order is processed, the Spectra Logic Customer Care team contacts you with instructions for generating the activation key for the option you purchased.

Enter Activation Keys

Notes:
- The activation keys for the initial BlueScale Software Support license, the initial licensed slot capacity, and any additional options you purchased with the library were automatically entered into the library during the initial installation process (see Perform the AutoInstall on page 62).
- If you purchase options after the initial library installation, you are provided an activation key for each option as described in Purchase Additional Options or Features on page 113.

Use the following steps to enter a new BlueScale Software Support key or the activation key for a new option into the library.

1. Have on hand the activation key for the BlueScale Software Support license or other option that you need to enter into the library (see Purchase the Option on page 114).
2. Access the Configuration menu (see Access the Configuration Menu on page 97).

   Note: If the secondary Configuration menu is displayed, click **More Options** (up arrow) to display the main Configuration menu.
3. On the Configuration menu, click **Option Keys** to display the Option Keys screen (see Figure 68 on page 113).
4. Click **New** to display the New Option Key screen.

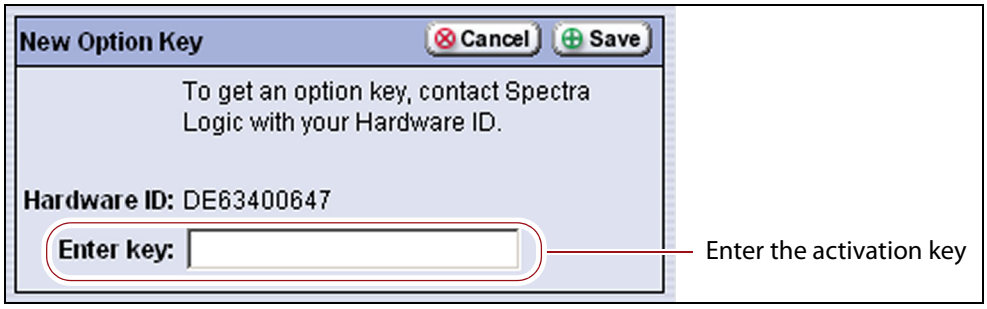


Figure 70 Enter the activation key in the New Option Key screen.

5. Enter the activation key for the option you want to enable in the **Enter key** field.

Notes:
- The activation keys are not case-sensitive.
- Enter Information on Screens on page 91 provides instructions for entering information into the screens.
- If you receive activation keys by email, use the BlueScale web interface (RLC) to access the library. You can then copy each key from the email and paste into the New Option Key screen instead of typing it.

6. Click **Save**.

   The Option Keys screen displays with the new option key and its description included in the list of keys. You can view this list at any time to determine what options are currently enabled.

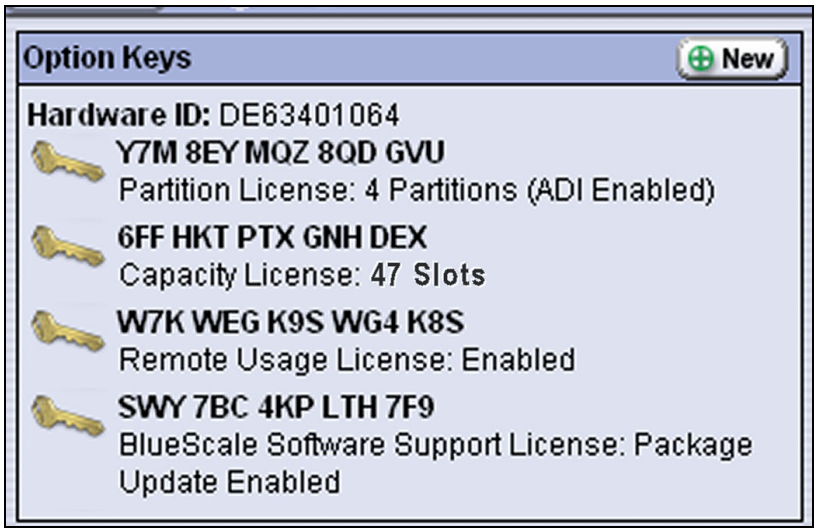


Figure 71 List of option keys stored in the library.

Note: Keep a copy of all activation keys that you receive. You must re-enter them if the library is ever reset to factory defaults, which could be required by Spectra Logic Technical Support for certain troubleshooting procedures.

BACKING UP THE LIBRARY CONFIGURATION

Overview Having a current backup of the library's metadata is an essential component of any disaster recovery plan. This metadata includes the library configuration, the option activation keys, the MLM and DLM databases, and any BlueScale encryption keys stored in the library. This backup is also extremely useful if problems require you to replace the LCM or the memory card in the LCM. After the replacement procedure is complete, you can use the saved configuration to restore the library's settings, including the partitions, instead of having to manually re-enter all of the information.

Important Backing up the library configuration also backs up any BlueScale encryption keys that are stored in the library at the time the file is created.

Important The backup configuration can only be used to restore the library that generated the backup. The configuration is tied to the Hardware ID of the library and cannot be transferred to another library.

In the event that you need to restore the library configuration, you can use either the automatically saved configuration backup file from the LCM or the emailed copy (see Restoring the Library Configuration on page 374).

See Back Up and Protect the Library Metadata on page 485 for additional information about backing up the library's configuration information, the MLM database, the DLM database, and any BlueScale encryption keys (the library metadata).

Options The library provides two methods for backing up the configuration:

- **Automatic** — See Back Up the Library Configuration Automatically on page 117
- **Manual**— See Back Up the Library Configuration Manually on page 118

Back Up the Library Configuration Automatically

Auto Configuration Save Process The library generates an Auto Configuration Save backup file once a week and every time you create or modify a partition. This backup file contains the current library configuration, the MLM and DLM databases, and any BlueScale encryption keys stored in the library. The backup file is saved to a time-stamped zip file on the memory card in the LCM. The zip file is named `<date-time>cfg.zip`, where `<date-time>` is the time stamp for when the backup file was created.

Notes:
- The Auto Configuration Save backup file is generated at the same time each week based on the first time the file was generated.
- The library does not generate an Auto Configuration Save backup file when you make configuration changes other than creating or modifying a partition.

Auto Configuration Save Email Process As an extra security measure, you can configure the library to automatically email the time-stamped zip file to a previously configured email recipient each time the backup file is created. Saving an external copy of the automatically generated configuration backup file ensures that you can recover the library configuration, the MLM and DLM databases, and any BlueScale encryption keys stored in the library in the event of a disaster.

When the recipient receives the email, they should verify the backup as described in Verify the Configuration Backup on page 121 and Verify the Database Backup File on page 274.

Important To use this automatic email option, you must first configure the person to whom you want the backup file sent as a mail recipient (see Configure Mail Users on page 107) and then enable emailing the Auto Configuration Save file and select the recipient (see Email Auto Configuration Save on page 111).

Note: The library does not generate an Auto Configuration Save backup file when you make configuration changes other than creating or modifying a partition.

For detailed information about using the automatically generated configuration backup file to restore the library, see Restore From an Auto Configuration Save File on page 375.

Back Up the Library Configuration Manually

Overview Whenever you make a configuration change to the library that does not result in the library automatically generating a configuration backup file (for example, you entered activation keys after the creation date of the most current automatically generated backup file), you can manually back up the library configuration as described in this section.

Notes:

- The Save Library Configuration utility described in this section does not back up the MLM database or the DLM database.

  To back up the MLM and DLM databases, use the Save MLM Database utility, as described in Back Up the MLM and DLM Databases on page 270. After you create the backup, be sure to verify it as described in Verify the Database Backup File on page 274.

- Backing up the library configuration also backs up any BlueScale encryption keys that are stored in the library at the time the file is created.

User Privilege Requirements Only a user with superuser or administrator privileges can create a manual backup of the library configuration. See Understanding User Groups and Security on page 94 for information about the three types of user groups and what types of privileges each has.

Generate the Configuration Backup File

1. Log into the library as a user with superuser or administrator privileges.
2. If you want to save the configuration to a USB device, connect the device to a USB port on the LCM and allow time for the device to mount before continuing (see Figure 25 on page 62).

Important The option to save the file to USB is only available if you connect a USB device to the library's USB port before you access the utilities.

3. If necessary, click **MENU** to display the Menu screen.
4. Click **Maintenance** to display the Maintenance menu.

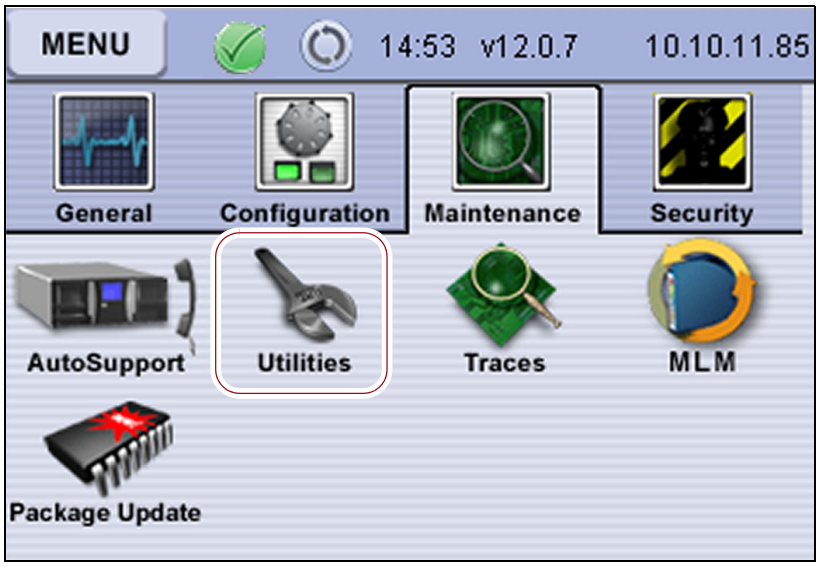


Figure 72 Click **Utilities** on the Maintenance menu.

5. Click **Utilities**. The Basic Utilities screen displays.

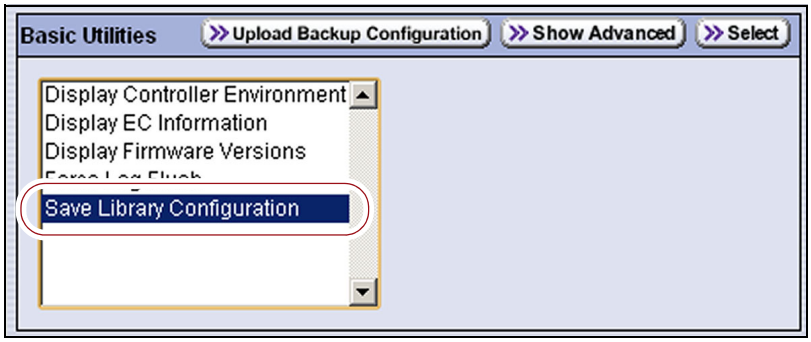


Figure 73 Select **Save Library Configuration** on the Basic Utilities screen.

6. Scroll through the list of utilities and select **Save Library Configuration**.

7. Click **Select**. The screen refreshes to show the details for the utility.

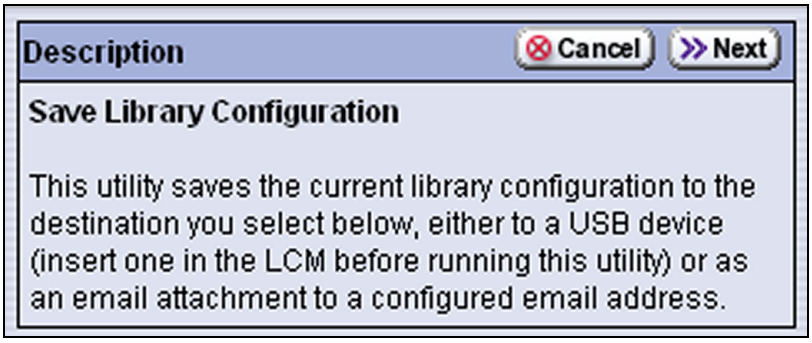


Figure 74 Read about the Save Library Configuration utility.

8. Click **Next** and select whether to save the configuration backup file to USB or to email it to a previously configured mail user.

Figure 75 Select the destination for the configuration backup file.

Select...	To...
USB	Save the library configuration file to the USB device connected to a USB port on the LCM. The backup file is stored in a folder called `SavedConfigs\<date-time>`, where `<date-time>` is the time stamp for when the backup was created. The folder contains multiple configuration files with the format `cnnnnnn.cfg`, where each `n` is a number between 0 and 9. **Note:** The **USB** option is only available if you connect a USB device to the library's USB port before you access the utilities.
[mail recipient]	Send the library configuration file as a zip file attached to an email addressed to a previously configured mail user (see Configure Mail Users on page 107). **Note:** Do not send the file to autosupport@spectralogic.com unless Spectra Logic Technical Support specifically requested the file for troubleshooting.

9. Click **Next** to select where to send the utility results system message.

   Note: The Destinations screen specifies where to send the utility results system message. It does not affect where the actual configuration backup file is sent.

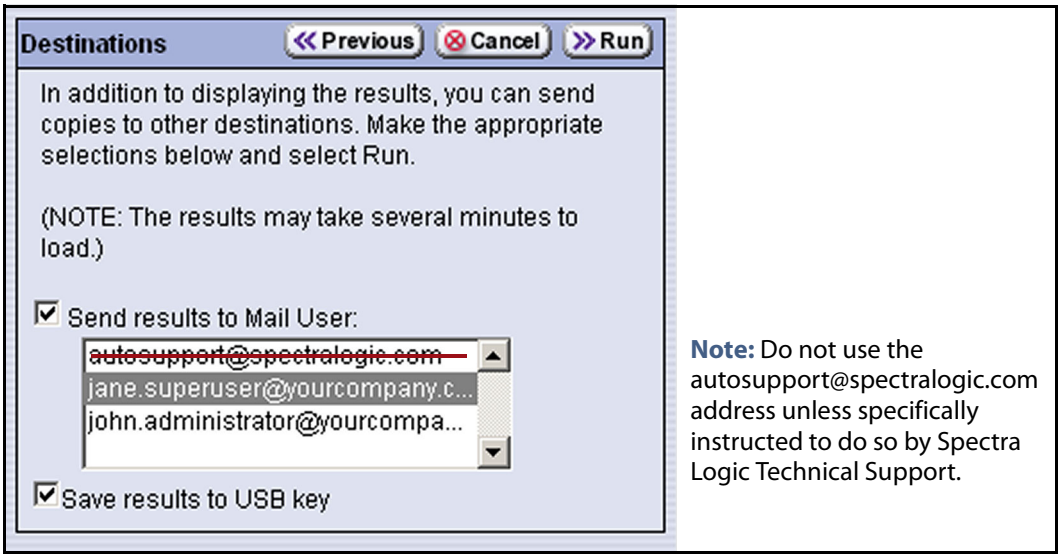


Figure 76 Select additional destinations for the utility results file.

10. Click **Run**.

    After a brief delay, the Utility Results screen redisplays, showing that the configuration file was sent to the selected destination.

11. Confirm that the backup was successful, as described in Verify the Configuration Backup.

Verify the Configuration Backup

After creating a backup of your library configuration, use one of the methods described in the following sections to verify that the backup was successful as soon as possible after you create it.

When Saved to a USB Device

1. Plug the USB device into a USB port on an available computer.
2. Examine the list of files on the USB device and locate the `\SavedConfigs` folder.
3. Open the `\SavedConfigs` folder and verify that a folder corresponding to the date and time you created the backup is present.

4. Open the <*date-time*> folder and confirm that it contains several configuration files named using the format `cnnnnnn.cfg`, where *n* is a number between 0 and 9. Make sure that all of the files are more than 0 bytes in size.

   - If the configuration files are present and all are more than 0 bytes in size, the backup was successful. Store the USB device in a safe location.

     Note: You can zip the files in the folder and email the zip file to others or make additional copies of the folder for safekeeping.

   - If the configuration files are not present, or if any of the files are zero (0) bytes in size, then the configuration backup was not successful. Repeat the entire backup (Back Up the Library Configuration Manually on page 118) using a different USB device.

When Sent as an Email Attachment

1. Open the email and confirm that it contains a zip file attachment named <*date-time*>`cfg.zip`, where <*date-time*> is the time stamp for when the zip file was created.
2. Open the zip file and confirm that it contains several configuration files named using the format `cnnnnnn.cfg`, where *n* is a number between 0 and 9. Make sure that all of the files are more than 0 bytes in size.

   - If the configuration files are present and are more than 0 bytes in size, the backup was successful. Save the email attachment to a safe location from which you can copy it to a USB device, if needed.
   - If the email attachment does not contain the configuration files or if one or more of the files are 0 bytes in size, repeat the backup process (Back Up the Library Configuration Manually on page 118) to send the email again.

Read Back Up and Protect the Library Metadata on page 485 for additional information about backing up the library's configuration information, the MLM and DLM databases, and any BlueScale encryption keys.

CONFIGURING OPTIONAL LIBRARY SETTINGS

This section describes optional configuration settings that you may select to use for your library and operating environment. If you make changes to these settings, be sure to manually back up the library configuration when you are finished (see Back Up the Library Configuration Manually on page 118).

Install a Security Certificate and Authentication Key

If you enabled SSL (see Enable SSL on page 111), use the following steps to obtain and install a security certificate and private key.

1. Obtain a security certificate and private key using one of the following methods:

Important The ssl.crt and ssl.key files can only contain ONE certification or key. The BlueScale software does not support multiple keys (chaining keys) in the key or certificate files. If there are multiple keys in the files, they are all considered invalid.

Important When generating a self signed certificate using openssl, use the -x509 command line option. Loading a file without this option may cause the LCM to hang.

Important When generating a self signed certificate or a certificate signing request using openssl, use the -nodes command line option to prevent the key from being encrypted.

- **Create a Self-Signed Certificate**

  For example, to create a self-signed certificate and authentication key using **openssl**, use the following command.

  ```
  openssl req -x509 -nodes -days 365
  -newkey rsa:2048 -keyout ssl.key -out ssl.crt
  ```

  The `openssl req` command is a certificate request and certificate generating utility. The following parameters are used in the example:

  - `-x509` - This option outputs a self signed certificate instead of a certificate request.
  - `-nodes` - This option specifies that the private key not be encrypted.
  - `-days` *`n`* - When the `-x509` option is also used, this option specifies the number of days (*`n`*) that the certificate is valid.
  - `-newkey rsa:`*`nbits`* - Generates an RSA key *`nbits`* in size. The Library supports RSA keys in bits of 512, 768, 1024 and 2048.
  - `-keyout` *`filename`* - This option specifies the private key file name.
  - `-out` *`filename`* - This option specifies the certificate file name.

After entering the command, you are prompted to provide the following information. Sample responses are shown.

- Country Name (2 letter code) [AU]: **US**
- State or Province Name (full name) [Some-State]: **Colorado**
- Locality Name (eg, city) []: **Boulder**
- Organization Name (eg, company) [Internet Widgits Pty Ltd]: **Spectra Logic**
- Organizational Unit Name (eg, section) []: **DVT Test**
- Common Name (e.g. server FQDN or YOUR name) []: **T950@company.com**
- Email Address []: **support@company.com**

- **Request a Certificate Using a Certificate Signing Request**

  Request a security certificate and the authentication key from your signing authority and process the key for use in with the BlueScale software.

  a. Request a certificate from www.verisign.com, www.instantssl.com, www.letsencrypt.org or another SSL certificate vendor to obtain the certificate. For example, to generate a certificate signing request using **openssl**, use the following command:

  ```
  openssl req -newkey rsa:2048 -nodes
  -subj "/C=US/ST=Colorado/L=Boulder/O=Spectra/
  CN=DVT-T950" -out ssl.csr -keyout ssl.key
  ```

  The `openssl req` command is a certificate request and certificate generating utility. The following parameters are used in the example:

  - `-newkey rsa:`*nbits* - Generates a new certificate signing request and a new RSA private key *nbits* in size. The Library supports RSA keys in bits of 512, 768, 1024 and 2048.
  - `-nodes` - This option specifies that the private key not be encrypted.
  - `-subj "`*arg*`"` - This option provides the answers to many of the prompts shown in the example above.
  - `-keyout` *filename* - This option specifies the private key file name.
  - `-out` *filename* - This option specifies the certificate signing request file name.

  b. Send the certificate signing request to the signing authority. A certificate named ssl.crt and a key named ssl.key will be returned.

2. The BlueScale web server must use an RSA private key and cannot use a key with a passphrase. If the private key does not include `BEGIN RSA PRIVATE KEY` in the header or uses a passphrase, rename the key to `original_ssl.key` and issue the following command.

   ```
   openssl rsa -in original_ssl.key -out ssl.key
   ```

   If the key has a passphrase, issuing this command prompts you for the passphrase.

3. Save the security certificate file (`ssl.crt`) and the private key (`ssl.key`) in the root folder of a USB device.

   Note: The security certificate file must be named `ssl.crt` and the private key must be named `ssl.key`.

4. Connect the USB device to a port on the LCM (see Figure 4 on page 29) and wait for the device to mount.

5. Log into the library as a user with superuser or administrative privileges (see Log Into the User Interface on page 85).

6. From the toolbar menu, select **Maintenance ⋯⁘ Utilities ⋯⁘ Show Advanced**. The Advanced Utilities Confirmation screen displays.

7. Click **Yes**. The screen refreshes to show a list of the advanced utilities.

8. Scroll through the list of advanced utilities and select the **Load SSL Certificate and Key from USB** utility.

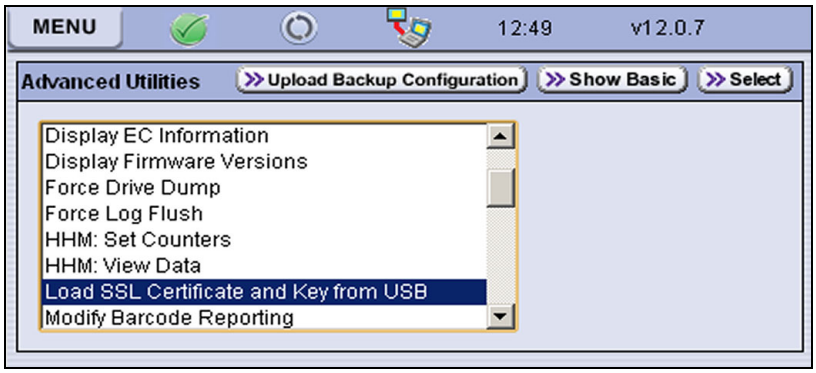


Figure 77 Use the **Load SSL Certificate and Key from USB** utility to load the security certificate onto the library.

9. Click **Select** o display the Description screen.

10. Read the description of the utility and then click **Next**.

11. Select whether you want to email the utility results file to a preconfigured mail recipient or save it to a USB device.

    Notes:
    - The results file just indicates whether the utility completed successfully. It does not contain the SSL key.
    - Do not send the file to autosupport@spectralogic.com.

12. Click **Run** to copy the security certificate and authentication key to the library web server.

Notes:
- The SSL keys are not stored as part of the library configuration. If you replace the SD card, you will have to reload these keys.
- To change or update the SSL keys, you must first manually delete the old keys from the LCM. Contact Spectra Logic Technical Support for assistance (see Contacting Spectra Logic on page 7).

Configure Barcode Reporting

Overview The Spectra Logic tape libraries support barcode data strings consisting of a start character; from 1 to 16 characters, including alphanumeric characters and an optional checksum character; and the stop character. Quiet zones precede and follow the start and stop characters.

By default, the library:

- Expects barcode labels with checksums (that is, it treats the right-most character as a checksum character).
- Does not use the checksum character to validate the barcode.
- Reports up to 16 characters but does not report the checksum character.

Notes:
- BlueScale12.3.1 increases the number of barcode digits the T50e can recognize to 16 characters. Prior to BlueScale12.3.1, the library can recognize 8 characters, plus one checksum character.
- With the exception of the checksum, the barcode labels typically show the human-readable character that each barcode character represents. The checksum character is not considered human-readable.
- If you change the barcode options for a partition, the library will report a tape mismatch error when tape cartridges previously discovered by MLM are loaded into a drive.

Barcode Reporting Mismatch Errors Unexpected behavior can occur if the library's barcode reporting configuration does not match the type of barcode labels that are being used **and** what the storage management software expects. The following table shows the reasons for most commonly occurring mismatch errors.

The library is configured to...	But the barcode labels...
Expect a checksum character,	Do not have a checksum character. **Note:** In this case, the barcode reported by the library is "missing" the right-most character. This is because the library treats the last character in the barcode as an unreported checksum character, when it is actually part of the barcode.
Use barcode labels that do not include a checksum,	Include a checksum character. **Note:** In this case, the library treats the checksum character as part of the barcode and therefore reports a seemingly random "garbage" character as the last character of the barcode.
Use barcode labels that include a checksum and perform checksum verification,	Do not have a checksum character. **Note:** In this case, the library reports a verification error on every barcode label because the character it is using to perform the checksum verification is not a checksum character.

Factors Affecting Barcode Reporting If your environment has any of the following:

- Labels without a checksum character
- A requirement to validate the barcode using the checksum
- Storage management software with specific barcode requirements

then you may need to modify the default settings used by the library.

Important

- Proceed with caution when changing the library's default barcode reporting settings. Any changes that you make affect every partition in the library. Before making changes, make sure that the changes do not adversely affect others using the library.
- If you modify the barcode reporting settings, you should do so before using any cartridges in the library. If you change the barcode reporting settings after the cartridges are used by the storage management software, the software may no longer recognize those cartridges. In general, it is best to leave the library set to its defaults and make any reporting modifications on the software side if that is an option.
- If you change the barcode options, the library will report a tape mismatch error when tape cartridges previously discovered by MLM are loaded into a drive.
- Never mix cartridges that use a checksum in the barcode with cartridges that do not use a checksum in the barcode in the library.

User Privilege Requirements Only a user with superuser or administrator privileges can modify barcode reporting. See Understanding User Groups and Security on page 94 for information about the three types of user groups and what types of privileges each has.

Change How the Library Reports Barcodes

Note: If you are unsure whether your labels include a checksum character, see Determine the Barcode Label Type on page 131.

If necessary, you can change the library's default barcode reporting configuration to disable the use of checksum characters, enable or disable the verification of the checksum character, or modify what portion of the actual barcode is reported to the host.

Important

After the utility completes, the LCM reboots. After the library completes its initialization, it rescans the barcode labels of all media in the library. This rescan takes approximately 18 seconds per cartridge.

1. Log into the library as a user with superuser or administrator privileges.
2. If necessary, click **MENU** to display the Menu screen.
3. Click **Maintenance** to display the Maintenance menu (see Figure 72 on page 119).
4. Click **Utilities**. The Basic Utilities screen displays.

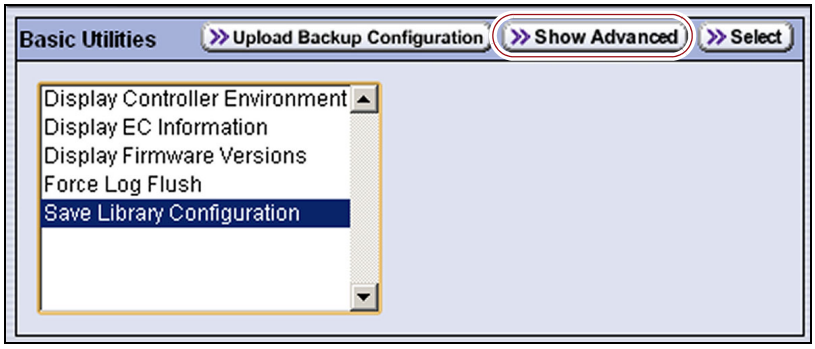


Figure 78 Click **Show Advanced** on the Basic Utilities screen.

5. Click **Show Advanced**. The Confirmation screen displays.

6. Click **Yes** to acknowledge the warning about using the advanced utilities. The Advanced Utilities screen displays a list of the advanced utilities.

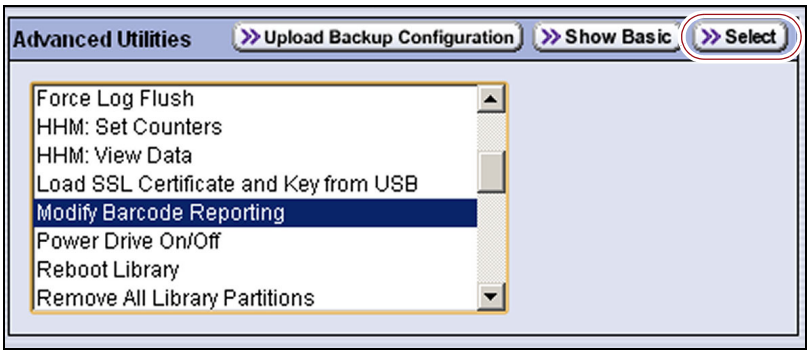


Figure 79 Select the **Modify Barcode Reporting** utility and click **Select**.

7. Select the **Modify Barcode Reporting** utility and click **Select**.
8. Read the information about the utility and then click **Next**. The Entry 1 of 3 screen displays.

Figure 80 Select the desired checksum behavior.

9. Select how barcode checksums are handled as required for your environment.

Select...	If...
Non-check-summed barcodes	Your labels do not include a checksum.
Check-summed barcodes	Your labels include a checksum **and** you want the barcode verified against the checksum when it is read. Verification is not generally required, but adds extra confirmation that the barcode label was read correctly by the barcode reader.
Ignore check-sum barcodes	Your labels include a checksum character but you do not want the barcode verified against the checksum when it is read. This is the default setting.

10. Click **Next**. The Entry 2 of 3 screen displays.

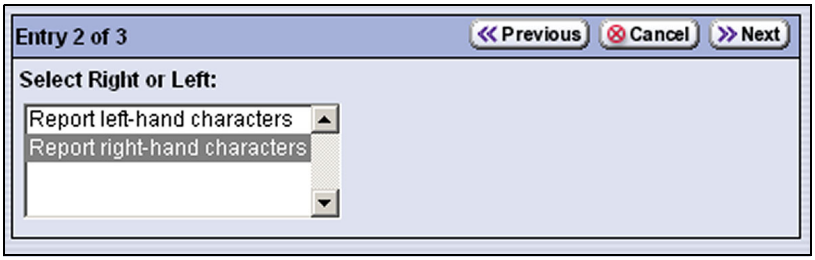


Figure 81 Change the reporting direction for the barcodes.

11. Change the reporting direction as required for your environment.

Select....	If...
Report left-hand characters	You want the library to report only the left-most characters in the barcode.
Report right-hand characters	You want the library to report only the right-most *x* human-readable characters in the barcode.

12. Click **Next**. The Entry 3 of 3 screen displays.

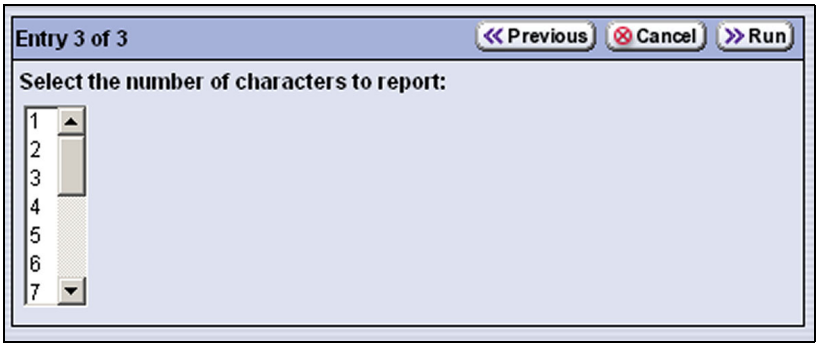


Figure 82 Select the number of barcode characters to be reported.

13. Scroll and click on the number of human-readable barcode characters you want the library to report. If your labels include a checksum, the number you enter includes the checksum character. The default number of characters is 16.

Important

Be careful when specifying the number of characters to report. You may end up with duplicate barcodes reported. For example:

- If you select to report the four left-most characters 123456L2 and 1234ABL3 are both reported as 1234.
- If you select to report the four right-most characters, 123456L2 and ABCD56L2 are both reported as 56L2.

14. Click **Run**.

When the utility completes, the LCM reboots. After the library completes its initialization, it rescans the barcode labels of all media in the library. This rescan takes approximately 18 seconds per cartridge.

Determine the Barcode Label Type

A checksum character is an "invisible" character—readable by the barcode reader, but not shown in the human-readable text on the label. Its function is similar to a parity check.

See Barcode Label Specifications for Half-Inch Media on page 514 for information about the required physical characteristics of barcode labels.

If you have...	The barcode labels...
Spectra Certified data cartridges with standard barcode labels,	Have a barcode with eight human-readable characters followed by a checksum character that is not human-readable. The last two human-readable characters indicate the media type (for example, L4 is LTO-4 media and L5 is LTO-5 media).
Spectra Certified data cartridges with custom barcode labels,	Are customized to your specifications. Custom labels can have up to 16 characters including an optional checksum character. **Important:** The T50e barcode reader supports a maximum of 15 human-readable characters plus a checksum character or a maximum of 16 human-readable characters if no checksum character is present.
Barcode-labeled cartridges that you did not purchase from Spectra Logic, —OR— Cartridges purchased from one vendor and barcode labels purchased from a different vendor,	Must consistently either include or not include a checksum. When ordering labels, make sure that you always specify the same type of barcodes (always include or always do not include a checksum). **Important:** Never use cartridges that use a checksum in the barcode and cartridges that do not use a checksum in the barcode in the library.

Use the following steps to determine if the barcode labels on your cartridges include a checksum character.

Important

After the utility completes, the LCM reboots. After the library completes its initialization, it rescans the barcode labels of all media in the library. This rescan takes approximately 18 seconds per cartridge.

1. Log into the library as a user with superuser or administrator privileges.
2. Run the **Modify Barcode Reporting** utility (see Change How the Library Reports Barcodes on page 128).

3. Make sure that the options for the utility are set as follows:

For...	Make sure it is set to...
Select checksum behavior	Ignore check-sum barcodes
Select Right or Left	Report right-hand characters
Select the number of characters to report:	16

4. Examine each barcode label you want to test and make a note of the human-readable text on each.
5. Import the cartridges into the library, then view the partition inventory, either on the BlueScale Inventory screen (see View the Cartridge Inventory for a Partition on page 224) or through your storage management software.
   - If the reported barcode exactly matches the human-readable text you recorded, then the barcode includes a checksum character.
   - If the reported barcode is missing the right-most character, then the barcode does not include a checksum character.
6. See Change How the Library Reports Barcodes on page 128 to configure the barcode reporting to match your barcodes.

Configure a Package Server

Overview Configuring a package server is optional. A local package server can be used to store BlueScale packages downloaded from Spectra Logic for updating the BlueScale software or library component firmware. Update packages can also be downloaded directly from the Spectra Logic website to the memory card in the library's LCM or to a USB device.

Note: For additional information about BlueScale packages and how to use them, see Updating the BlueScale Software and Library Firmware on page 421.

User Privilege Requirements Only a user with superuser or administrator privileges can configure a package server.

Configure a Package Server

Use the following steps to configure, modify, or delete a local package server.

1. Identify the server or servers you want to use for storing BlueScale packages. Make sure that these servers can access the Internet and that they are on the same network as the libraries you want to update.

   Note: Both Microsoft's Internet Information Services (IIS) and the Unix-based Apache server work as package servers.

2. Log into the library as a user with superuser or administrator privileges.
3. If necessary, click **MENU** to display the Menu screen.
4. Select **Maintenance** ⋯⁘ **Package Update**. The Package Update screen displays.

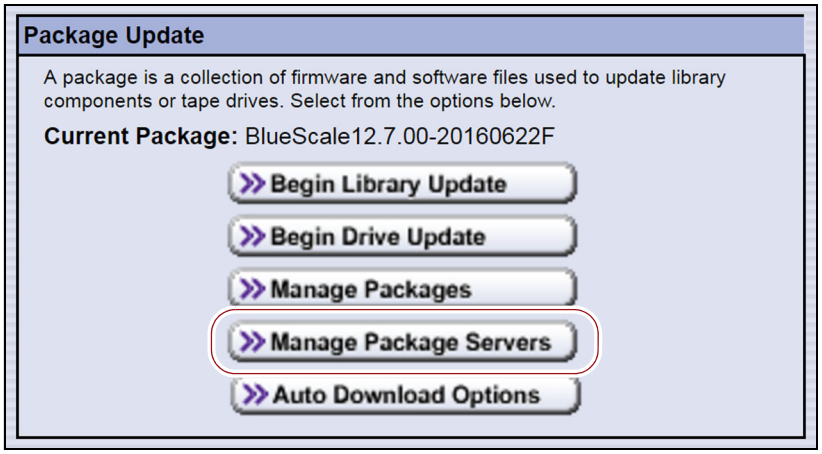


Figure 83 The Package Update screen.

5. Click **Manage Package Servers**. The Manage Package Servers screen displays, and provides the server name and configuration settings for each currently configured package server:
   - **Server name**—Name assigned to the server when it was added.
   - **IP Address**—The IP address of the package server.
   - **Directory**—The directory where BlueScale packages are stored.
   - **Auto Download** —Indicates whether Auto Download is configured. If configured (See Add a package server on page 134), the library checks the package server once a week for a library update package newer than what the library is currently running. If a new package is available, the library downloads it, generates a system message, and displays an icon on the status bar to indicate the update is available (see Auto Download Icon on page 83). If you want to delay the notification about a new package, see Modify Auto Download Options on page 135.

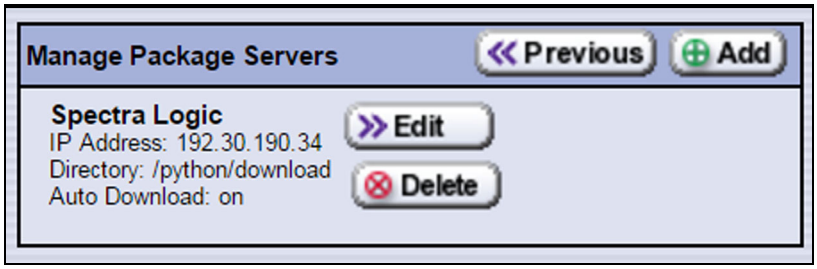
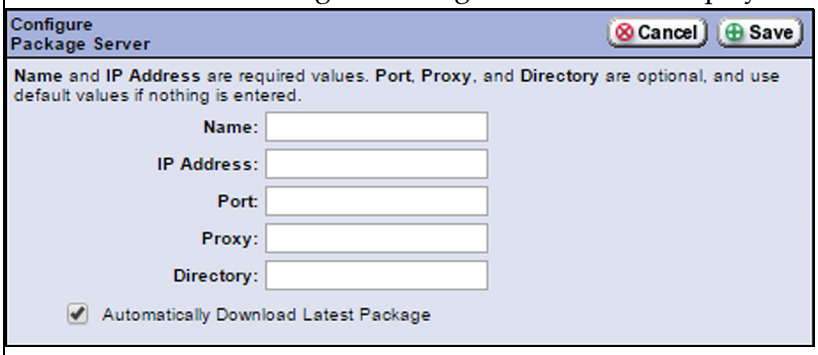


Figure 84 The Manage Package Servers screen.

6. Click the correct button to add, delete, or edit a package server.

Task	Procedure
Add a package server	**1.** Click **Add**. The Configure Package Server screen displays.  **Figure 85** The Configure Package Server screen. **2.** Fill in the requested information: ▪ **Required — Name** and **IP Address**. If no **Proxy** is set, the **IP Address** can be an IPv4 or an IPv6 address. If a **Proxy** is set, the **IP Address** must use IPv4. ▪ **Optional — Port**, **Proxy**, and **Directory** fields use default values if nothing is entered. The **Proxy**, if set, must use IPv4. **3.** Select or clear **Automatically Download Latest Package**. ▪ If selected, the library checks the package server once a week for a library update package newer than what the library is currently running. If a new package is available, the library downloads it, generates a system message, and displays an icon on the status bar to indicate the update availability. ▪ If cleared, you must check for updates manually. **4.** Click **Save**. The screen refreshes and lists the new server in the Package Servers portion of the screen. **Note:** The library compresses the IPv6 address when saved.
Edit a package server	**1.** Click **Edit** next to the server's name and details. The Configure Package Server screen displays. **2.** Edit the server information as necessary. **3.** Click **Save**. **Note:** The library compresses the IPv6 address when saved.
Delete a package server	Click **Delete** next to that server's name and details. **Important:** There is no confirmation requested when you delete a package server. After you click **Delete**, the server is immediately removed from the list of available package servers. **Important:** If you delete a package server from the library configuration, you can no longer access the firmware package files stored on that package server from the library. However, the firmware packages are not deleted.

Modify Auto Download Options

Overview When auto download is enabled for a package server (see Add a package server on page 134) you can configure when the library sends notification of a new downloaded package update.

> **Note:** For additional information about BlueScale packages and how to use them, see Updating the BlueScale Software and Library Firmware on page 421.

User Privilege Requirements Only a user with superuser or administrator privileges can configure auto download options.

Configure Auto Download Options Use the following steps to configure or modify auto download options.

1. Log into the library as a user with superuser or administrator privileges.
2. If necessary, click **MENU** to display the Menu screen.
3. Select **Maintenance** ···⁘ **Package Update**. The Package Update screen displays.

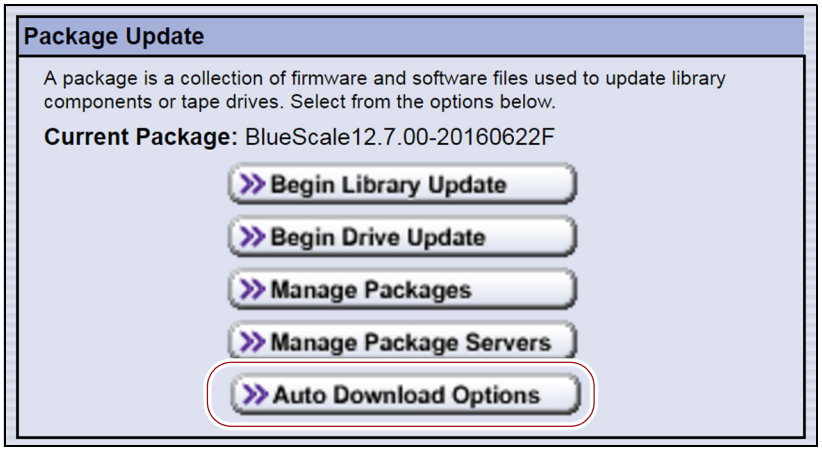


Figure 86 The Package Update screen.

4. Click **Auto Download Options**. The Auto Download Options screen displays showing the current auto download setting.

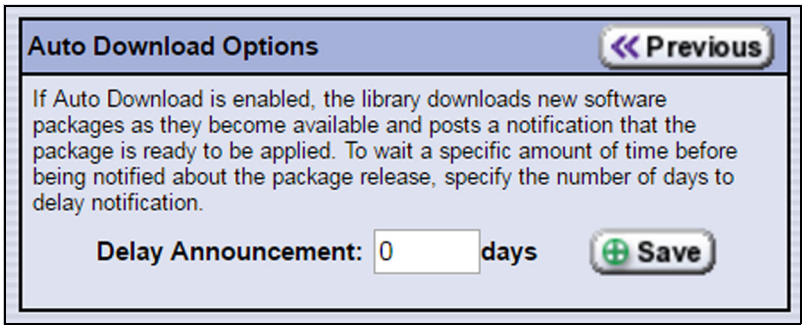


Figure 87 The Auto Download Options screen.

5. If you want to delay the notification about a new package, enter the number of days to delay in the **Delay Announcement** field.
6. Click **Save** to save the new settings.

Configure Emulation

Overview The library identifies itself as "SPECTRA PYTHON" in response to a SCSI Inquiry command. If your storage management software or operating system does not specifically support one of the Spectra Logic libraries that identifies itself as "SPECTRA PYTHON," you can configure one or more partitions to emulate another type of library. Because most storage management software is certified for one or more of these libraries, using the emulation mode may allow these applications to support the library.

Caution Using emulation is not the preferred method of operation and should only be used when recommended by Spectra Logic Technical Support.

Important StorNext® versions 4.1.2 and later provide native support for Spectra tape libraries. However, if you are using an earlier version of StorNext, you must configure one or more storage partitions to emulate a Sun StorageTek L700 library. Configuring a partition to emulate the STK L700 library results in the following changes to the SCSI data it reports:

- The **INQUIRY** command returns STK L700 as the product identification.
- The **READ ELEMENT STATUS** command reports the element addresses (the element addresses for the robotics, drives, and magazine slots) using the format defined for the Sun StorageTek L700 library.

Notes:
- Configuring emulation changes how the library identifies itself to the operating system or storage management software.
- The following instructions describe an advanced partition configuration option that is used only in the context of creating or editing a partition. The screens for configuring emulation are only accessible after you complete the initial configuration steps for the partition (see Define the Partition Name and Media Type on page 177).

User Privilege Requirements Only a user with superuser or administrator privileges can configure emulation. See Understanding User Groups and Security on page 94 for information about the three types of user groups and what types of privileges each has.

Configuration Procedure Use the following steps to configure a partition to emulate another type of library.

1. Log in as a user with superuser or administrator privileges.
2. Access the partition wizard to create or modify the partition to be used with emulation (see Accessing the Partition Wizard on page 169).
3. On the Partitions screen, click **New** to create a new partition or **Edit** to modify an existing partition. The Name & Media Type screen displays.

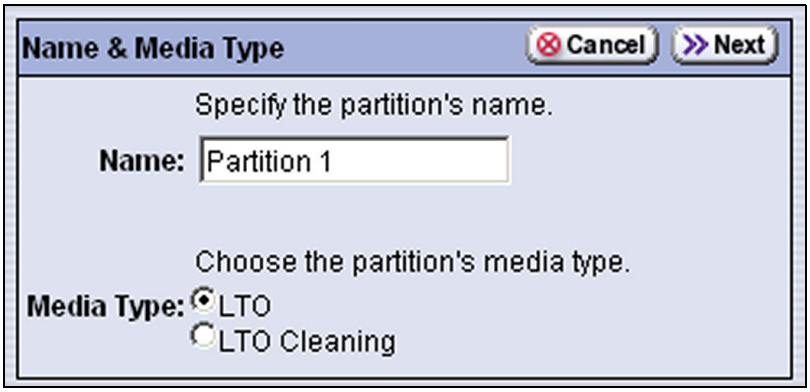


Figure 88 Click **Next** to advance to the Exporter screen.

4. Click **Next** on the Name & Media Type screen. The Exporter screen displays.

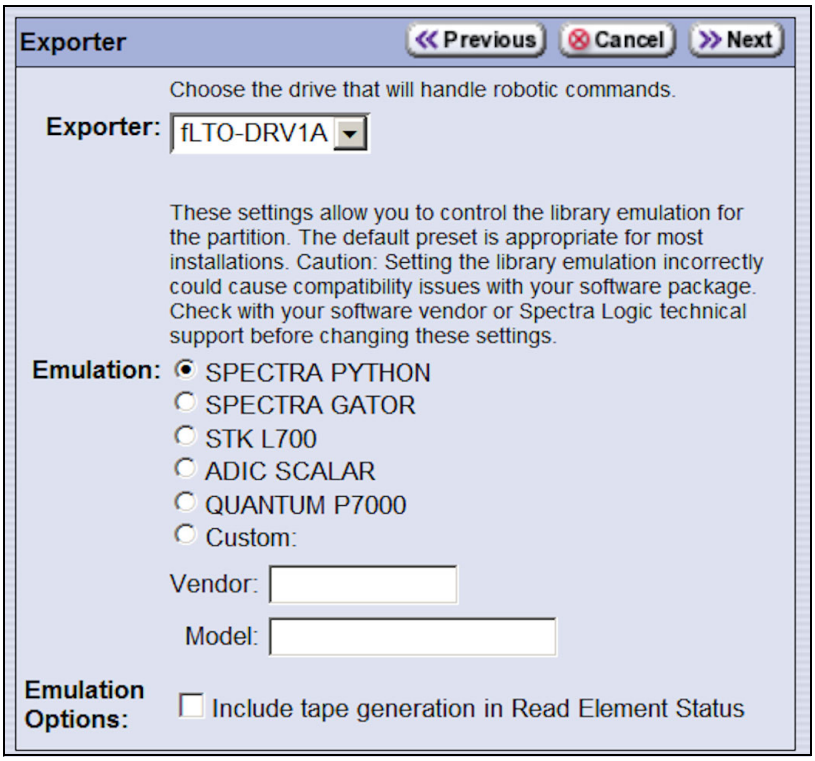


Figure 89 Specifying the emulation type.

5. Select the type of library you want the library to emulate. You can either:

   - Select a preconfigured emulation from the **Emulation** list.

   —OR—

   - Create a custom emulation, enter the **Vendor** and **Model** for the library to be emulated. These fields are used in the string that the library returns in response to a SCSI Inquiry command.

   Note: The default setting is SPECTRA PYTHON.

6. If you want the SCSI Read Element Status command response to include Media Domain, Media Type, Drive Domain, and Drive Type, select **Include tape generation in Read Element Status**. See the *Spectra Tape Libraries SCSI Developer Guide* for more information.

7. Click **Next**. The Spare Drives screen displays the drives that are available for use as Global Spares.

   The Spare Drives screen is the beginning of a series of configuration screens. The sequence of steps and screens matches those described in Creating a Storage Partition on page 174.

CHAPTER 5

Operating the Library

This chapter describes procedures for the day-to-day operation of your library.

Note: For additional instructions on how to perform operations related to specific features, see:

- Chapter 7 – Using Cartridges in the Library, beginning on page 197
- Chapter 8 – Configuring and Using Media Lifecycle Management, beginning on page 233
- Chapter 9 – Using Drive Lifecycle Management, beginning on page 279

CONTROLLING THE LIBRARY POWER

The library power is controlled using the front panel power button.

Power On the Library

1. Make sure that one or both of the library's power cables are plugged into AC outlets. Make sure that the cord is fully seated in the connector.

Important For redundant AC power configurations, connect each input to a separate branch circuit, which allows for failover in the event of a power failure in one of the circuits (see Power Specifications on page 501 for additional requirements).

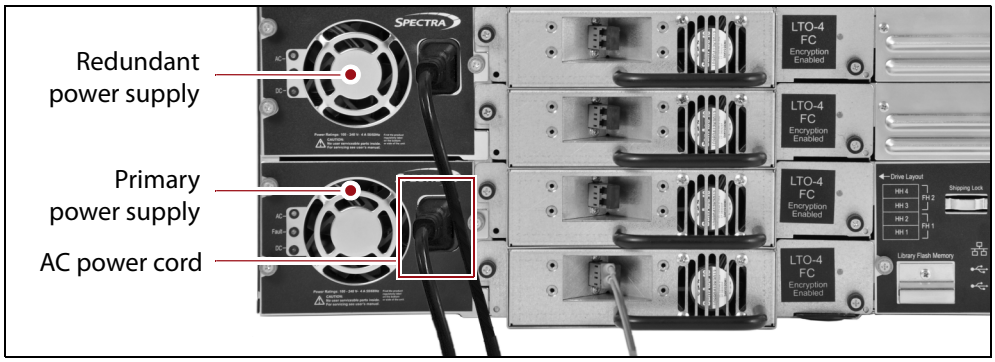


Figure 90 Connect the AC power cords (redundant power supply shown).

2. Press and hold the front panel power button for two to three seconds until the button's LED illuminates.

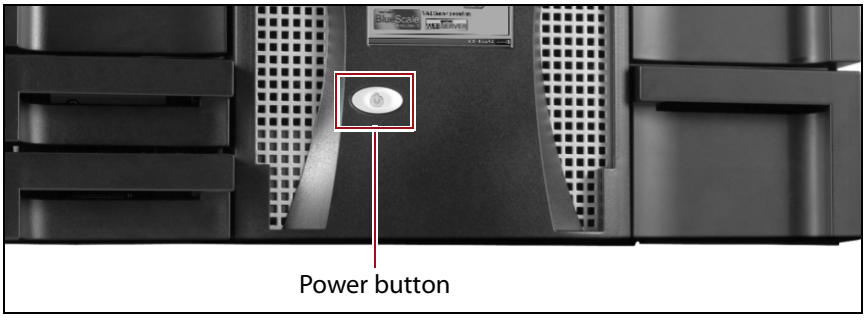


Figure 91 Press and hold the front panel power button.

3. Wait while the library completes its power-on sequence, which takes six to nine minutes, depending on the library configuration. After the library completes its power-on sequence, the Library Initialization screen displays (see Figure 28 on page 64). This screen lists the required initialization steps and current status of the library's major components (Robotics, RCM, and LCM). Text boxes provide descriptions about the currently active tasks.

   Note: If your library has a static IP address, you can access the library using the remote library controller (RLC) as soon as the Library Initialization screen displays.

4. After initialization is complete, the Login screen displays and you can log into the library (see Log Into the User Interface on page 85).

   Note: If the library cannot complete the initialization process, it generates system messages and enters maintenance mode. Contact Spectra Logic technical support for assistance.

Power Off the Library

Before powering off the library, use the following steps to prepare for shut-down.

Note: If you need to reset the library instead of powering it off, see Resetting the Library on page 372

1. Use your storage management software to stop any backups running to the library.
2. Pause PostScan if it is running (see Pause the PostScan Process on page 261). Any tapes currently being scanned are returned to their storage locations.
3. Press and hold the front panel power button for approximately one second. The power-off sequence takes approximately two minutes, which allows the BlueScale software and components to shut down gracefully.
   - **If the system is stable at power off**, a message displays indicating that the power button was pressed.
   - **If the system is unstable at power off** (that is, if you power off the library when it is in an error state), the power off time takes approximately one minute and shows no indication that it is powering off. Wait for the sequence to complete.

     If the library does not power off after two minutes, press and hold the front panel power button for ten seconds to invoke the *emergency power off* process. This process powers off the library immediately without a graceful shutdown of the BlueScale software and library components.

   Note: If you intend to leave the library powered down for an extended length of time, disconnect the AC power cords from the library.

MONITORING YOUR LIBRARY

Overview The BlueScale user interface provides a number of tools for monitoring the health and performance of the library, its components, and its media.

- The quickest way to obtain important information is to check the status icons on the General Status screen (see Figure 37 on page 74). They provide at-a-glance information about the status of major system components.
- The system status icon on the status bar indicates the highest severity level for the unread system messages. See System Status Icon on page 82 for a description of what each icon means.
- The following table lists where to find additional information about the health and performance of the library, its components, and its media.

Check...	To monitor...	For details, see...
System Messages	Events that resulted in system messages about the library and its operation.	Check and Respond to Messages on page 143.
Performance Metrics	The power consumption and storage density statistics for your library.	▪ View Power Consumption Statistics on page 145. ▪ View Storage Density Statistics on page 146.
Robot Utilization Information	The percentage of time the robotics is being used while the library is powered on.	View Robot Utilization Information on page 147.
Drive Status	The operational status, firmware level, and cleaning status of the drives.	View Drive Status Information on page 148.
Media Lifecycle Management (MLM)	The usage and health of MLM-enabled media in the library. **Note:** MLM also provides limited health information about media that is not MLM-enabled.	Chapter 8 – Configuring and Using Media Lifecycle Management, beginning on page 233.
Drive Lifecycle Management (DLM)	The usage and health of the LTO drives in the library.	Chapter 9 – Using Drive Lifecycle Management, beginning on page 279.

Check and Respond to Messages

Overview Check the library's system messages regularly. These messages provide important information about the library, its operation, and any library problems. Reviewing the messages is also the first step in troubleshooting.

Note: When you configure mail users, you can specify which types of system messages the library automatically emails to each mail user. See Configure Mail Users on page 107 for detailed instructions.

User Privilege Requirements All users can view system messages and view performance metrics.

Use the following steps to view BlueScale system messages through either the operator panel or a web browser.

1. Log into the library.
2. Select the system status icon on the status bar. The Messages screen displays.

   Note: See Status Bar on page 81 for the location and description of the system status icons.

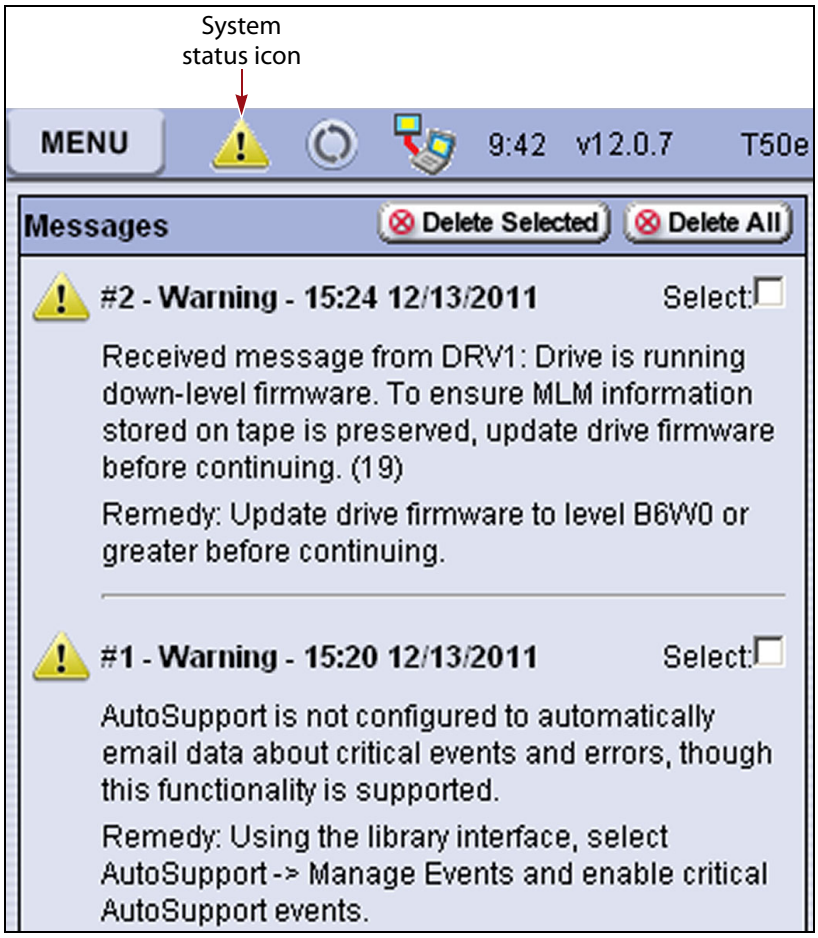


Figure 92 The Messages screen.

The following table describes the severity ranking for messages.

Icon	Message Severity	Description	Response
	**Informational**	The library is working as intended. An event occurred that generated information about an operation or a system component that may require attention to keep the library running at 100%. **Example:** The utility completed successfully.	▪ If the event was expected, no action is required. ▪ If the event was unexpected, determine the cause of the event and take remedial steps.
	**Warning**	The library operation is impaired and requires user intervention. **Example:** QuickScan did not complete, and there is a tape stuck in a drive as a result.	Determine the cause of the error and take remedial steps.
	**Error** or **Fatal Error**	The library experienced an event that prevents it from continuing operations. **Example:** The robot is not responding.	Examine any additional information in the message and take the required remedial steps.

3. Read the message(s), and follow any recommended steps.

   Note: Some error messages are followed by a series of errors that provide additional information. To understand the sequence of events, scroll up through the previous messages to locate the first error message in the series, then read the entire series of messages for clarification.

   If you need assistance, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

4. When you are finished reading the messages and completed the appropriate actions, you can select and delete individual messages or you can delete all of the messages.

Use Performance Metrics

The library includes the following metrics for monitoring the performance of your library.

- View Power Consumption Statistics, on this page
- View Storage Density Statistics on page 146

User Privilege Requirements All users can view performance metrics.

Access the Metrics Screen

1. Log into the library.
2. Click **MENU**, then click **General** to display the General menu (see Figure 38 on page 75).
3. Click **Metrics** to display the Metrics screen. The Metrics screen showing the last metric you viewed displays.

View Power Consumption Statistics

The BlueScale EnergyAudit feature provides information about the library's power consumption.

1. Access the Metrics screen.
2. Select which power consumption metric you want to view from the **Metric** drop-down menu:
   - Power Consumption (kWh)
   - Power Consumption (kWh/Ft^2)
   - Power Consumption (kWh/Ft^3)
   - Power Consumption (kWh/TB)
3. Click **Go**. A screen showing the selected metric displays.

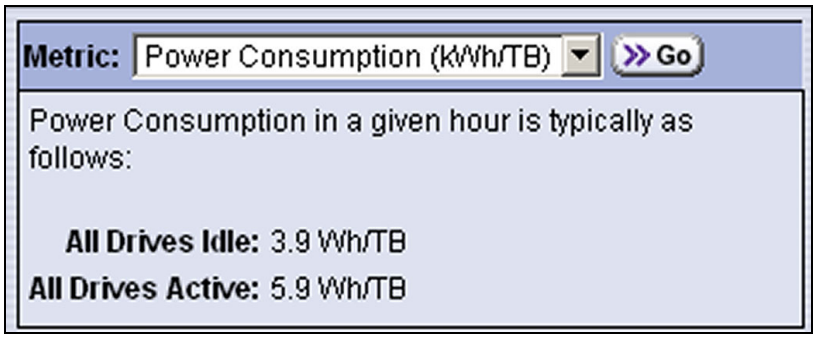


Figure 93 The Metrics screen showing power consumption.

View Storage Density Statistics

The Storage Density metrics let you monitor the amount of data your library is capable of storing based on the number and type of data cartridges currently stored in the library.

Use the following steps to view the storage density data for the library.

1. Access the Metrics screen (see Access the Metrics Screen on page 145.
2. Select **Storage Density** from the **Metric** drop-down menu.
3. Use the drop-down lists to select the **Media Type** and the **Unit** of measure for the density values.
4. Click **Go**. The Metrics screen refreshes to show the storage density metrics.

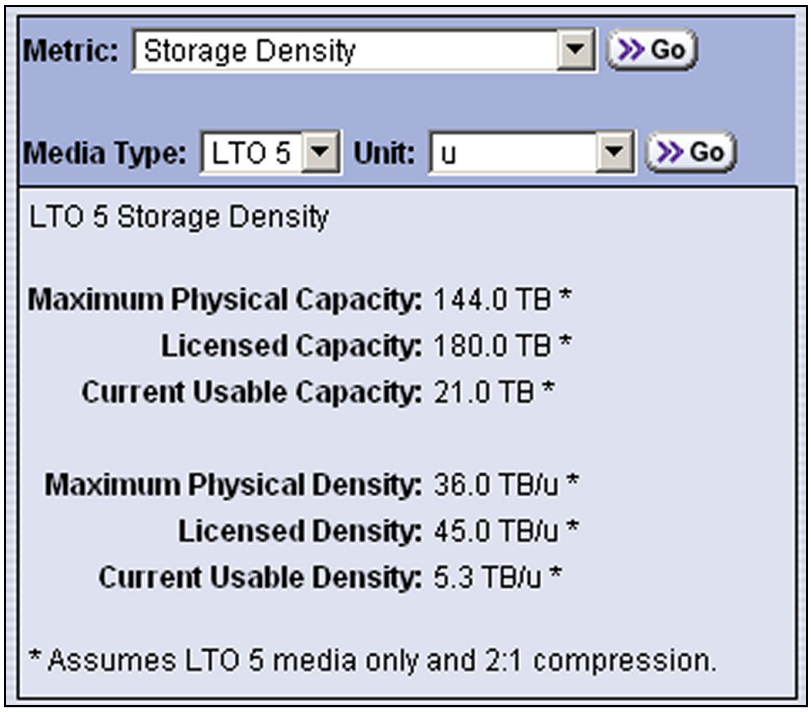


Figure 94 The Metrics screen showing storage density.

View Robot Utilization Information

The Robot Utilization by Hour metric lets you monitor the percentage of each hour that the library's robotics are actively operating over the last 24 hours. The data is updated every hour while the library is powered on.

- The Robot Utilization by Hour metric can include up to 24 data points, one for each hour that data was collected over a 24-hour period. The first time period begins one full hour after the library is powered on. Data collected during the first partial hour following power-on is discarded as invalid data.
- The data is stored in volatile memory and is not retained when the library is powered off.

Use the following steps to view the robot utilization information.

1. Select **Menu** ⋯⁘ **General** to display the General menu (see Figure 38 on page 75.
2. Click **Robot Usage** to display the Robot Utilization Screen.

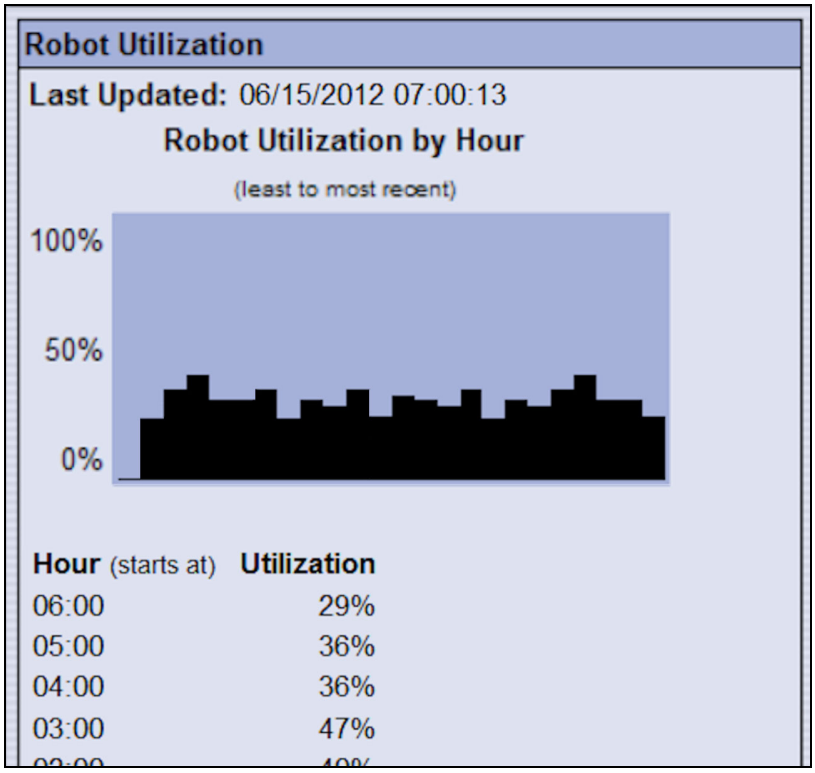


Figure 95 The Robot Utilization screen

View Drive Status Information

Overview The drive status icon on the General Status screen indicates the overall status of the library's drives (see Figure 37 on page 74). If the status icon indicates that a drive is experiencing a problem, view the Drive and Drive Details screens for detailed information about a specific drive.

The Drive Details screen includes the drive firmware version and manufacturer's serial number, as well as more detailed status information. From the Drive Details screen you can access the Drive Lifecycle Management (DLM) report for the drive. See Chapter 9 – Using Drive Lifecycle Management, beginning on page 279 for detailed information about DLM.

Use the information on the Drive Details screen and the DLM report to troubleshoot drive problems (see Troubleshooting Drives on page 390). If the drive is in an error state, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

User Privilege Requirements Only a user with superuser or administrator privileges can access the Drive and Drive Details screens. See Understanding User Groups and Security on page 94 for information about the three types of user groups and what types of privileges each has.

View the Drive Status Information Use the following steps to view information about the individual drives in the library.

> **Note:** You can also access the Drives screen by clicking Drives on the General Status screen.

1. Log into the library as a user with administrator or superuser privileges.
2. Access the Configuration menu (see Access the Configuration Menu on page 97).

3. Click **DLM** (or **Drives** if DLM is not enabled) to display the Drives screen. This screen lists all of the drives in the library, along with basic information about each drive and the available operations for each drive.

   Note: The operations available for each drive depend how you are accessing the BlueScale user interface and whether or not:

   - DLM is enabled
   - The drive is configured in a partition
   - Auto Drive Clean is enabled for the partition

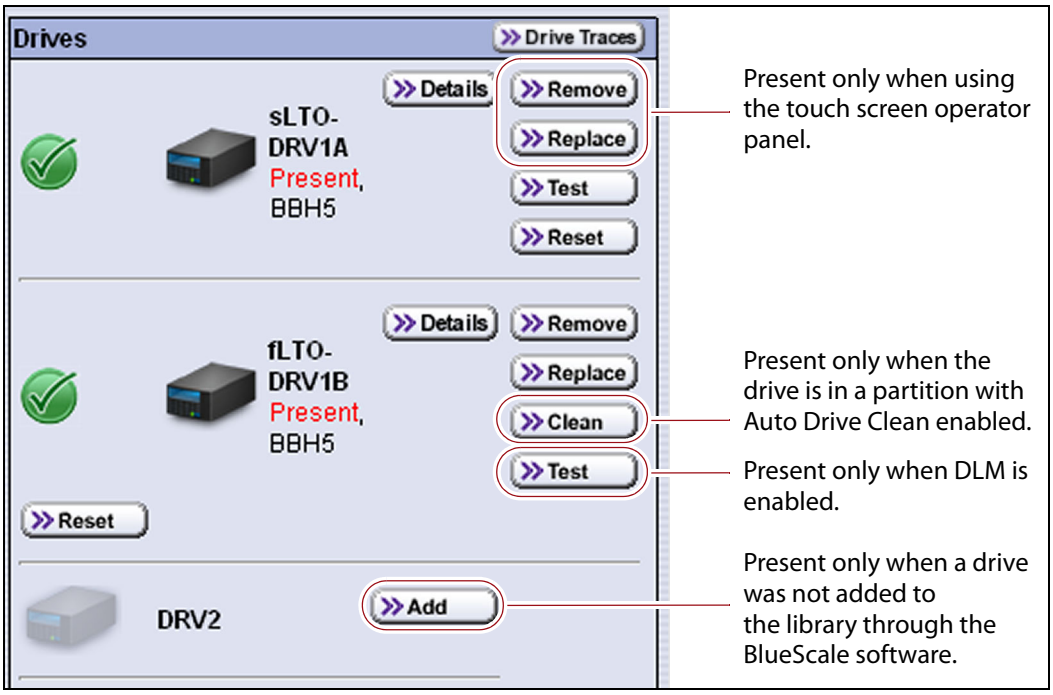


Figure 96 The Drives screen (when accessed from the operator panel).

4. Click **Details** next to the drive for which you want to view detailed information. The Drive Details screen displays.

Notes:
- The information on the Drive Details screen depends on the drive interface type and whether the drive is configured in a partition.
- The information on the Drive Details screen is a snapshot of the information at the time you clicked **Details**. Click **Previous** and then click **Details** again to refresh the information.

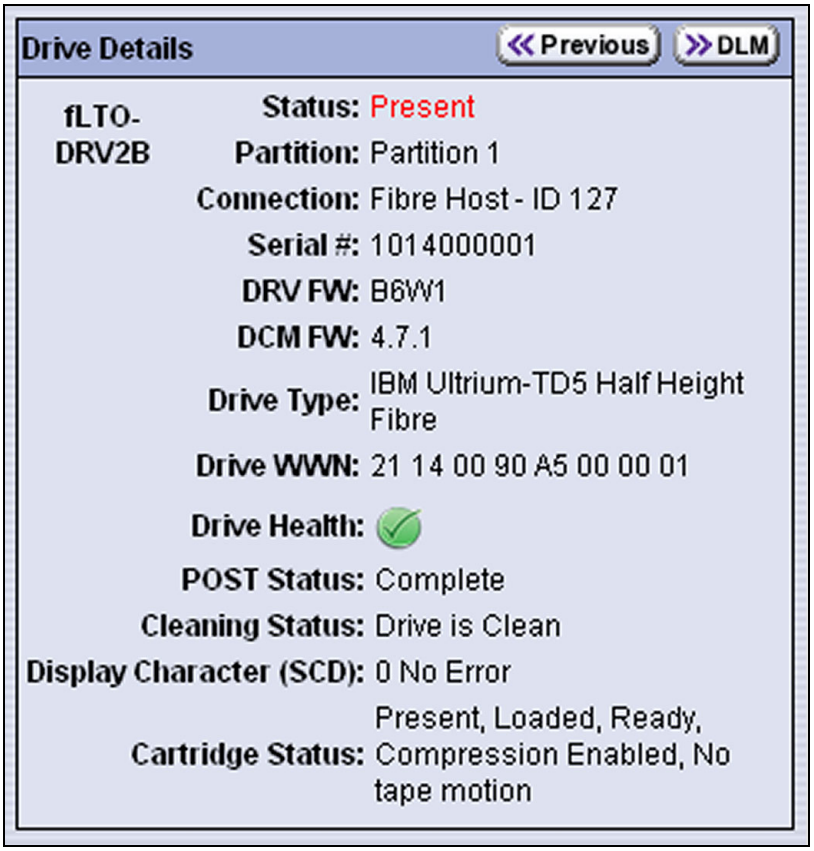


Figure 97 The Drive Details screen (Fibre Channel shown).

This field...	Shows...
<*interface*>LTO–DRV<*bay*>	The drive identifier assigned by the BlueScale software. See BlueScale Drive Identifiers on page 154 for detailed information.
Status	Whether or not a drive that was added to the library through the BlueScale software is present, missing, or impaired.
Partition	The name of the partition to which the drive is assigned or **None** if the drive is not assigned to a partition.
Connection	▪ The Host Fibre Channel ID for a Fibre Channel drive. ▪ The SCSI ID for a SCSI drive. **Note:** This field is not present for SAS drives.

This field...	Shows...
Serial #	The location-based serial number assigned to the drive while it is in the library. This serial number makes it possible to replace one drive with another without having to reconfigure the storage management software that accesses the drive. See Drive Serial Numbers on page 157 for additional information.
Drive FW	The firmware version being used by the drive.
DCM FW	The firmware version being used by the drive sled that houses the drive.
Drive Type	The description of the drive, which includes the manufacturer name, the drive type, and the form-factor.
Drive WWN	▪ The WWN for a Fibre Channel drive. See Drive World Wide Names on page 156 for detailed information about the WWNs for drives. ▪ The SAS port identifier for a SAS drive. **Note:** This field is not present for SCSI drives.
Drive Health	The icon corresponding to the drive's current health (see Using the Drive Health Icons on page 282).
POST Status	The results of the drive's Power-On Self-Test (POST).
Cleaning Status	Whether or not the drive needs cleaning (for example, Drive is Clean, Drive Cleaning Required).
Display Character (SCD)	The code displayed on the drive's single-character display (SCD) and its meaning. See Interpreting the SCD Codes on page 394 for detailed information.
Cartridge Status	Whether the drive contains a cartridge and if it does, whether the cartridge is loaded into the tape path and ready for use. This status also indicates whether the drive is configured to compress data as it is written and whether the drive is currently moving tape. **Note:** A status of "No tape motion" indicates either that the drive is empty or, if the drive contains a cartridge, that the tape is not moving.

5. If DLM is enabled, click **DLM** on the Drive Details screen to access the DLM report for the drive (see Viewing and Saving a Detailed Drive Health Report on page 284).

   Note: The **DLM** button is not present if DLM is not enabled.

USING A USB DEVICE

You can plug a USB device into a USB port on the LCM and use it for the following purposes:

- Backing up or restoring the library configuration
- Backing up or restoring the MLM and DLM databases
- Importing or exporting BlueScale encryption keys
- Gathering log files
- Uploading BlueScale software updates to the library.

Important After connecting a USB device, allow time for the device to mount before continuing.

Important Do not leave a USB device plugged into the LCM indefinitely, unless specifically directed to do so by Spectra Logic Technical Support.

One Spectra USB device is shipped with the library, but most types of USB devices work.

Important The library only recognizes FAT-formatted, not NTFS-formatted, USB devices.

If you are unable to access a USB device from the library, remove it and use a different one.

Guidelines for Using a USB Device

When using a USB device, keep the following guidelines in mind:

It is...	To continue backups while...
Safe	Exporting or importing a BlueScale encryption key to or from a USB device.
	Saving library configurations and other information to a USB device.
	Capturing traces and saving the trace results data to a USB device.
Not Safe	Restoring a saved library configuration or the MLM database from a USB device.
	Updating the library BlueScale software using an update package previously copied to the library.

Connect a USB Device to the Library

To use a USB device, plug it into either of the USB ports on the LCM and allow time for the device to mount.

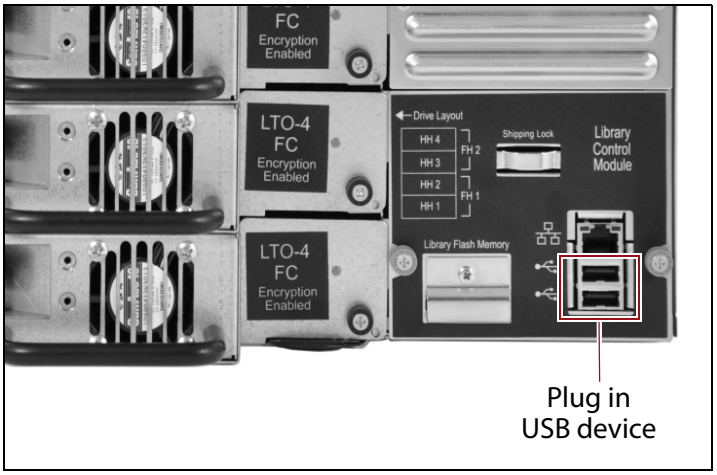


Figure 98 Plug the USB device into the LCM.

Notes:

- Not all USB devices are compatible with the library. If you are unable to access a USB device from the library, remove it and use a different one. If the library stops responding after you insert an incompatible USB device, reset it as described in Resetting the Library on page 372.
- Plug the USB device into the LCM *before* beginning a procedure that reads or writes data, to allow time for device recognition. For many utilities, the option to read from or write data to a USB device is not available if a USB device was not plugged into the LCM before you select the utility.

IDENTIFYING DRIVES AND PARTITIONS IN THE LIBRARY

The following sections describe methods for identifying the partitions and drives in the library, both through the BlueScale user interface and from the host software and SAN management tools.

Identify the Drives in the Library

The library assigns unique, location-based BlueScale identifiers and serial numbers to each drive in the library. The BlueScale identifiers appear on the Drives and Drive Details screens as well as in system messages. In addition, each Fibre Channel or SAS drive is assigned a location-based World Wide Name (WWN). For Fibre Channel drives, the WWN can be used to identify the drives on the host Fibre Channel arbitrated loop or fabric.

BlueScale Drive Identifiers

The firmware in the drive sled that houses each drive assigns an identifier to the drive based on its location in the library. This identifier is shown in the BlueScale user interface. Because the identifier is location-based, it remains constant even if the physical drive is replaced by a new drive. The new drive assumes the location-based identifier, making drive replacement completely transparent to the storage management software.

Figure 99 shows the relationship between the drive locations and the drive identifiers for both half-height and full-height drives.

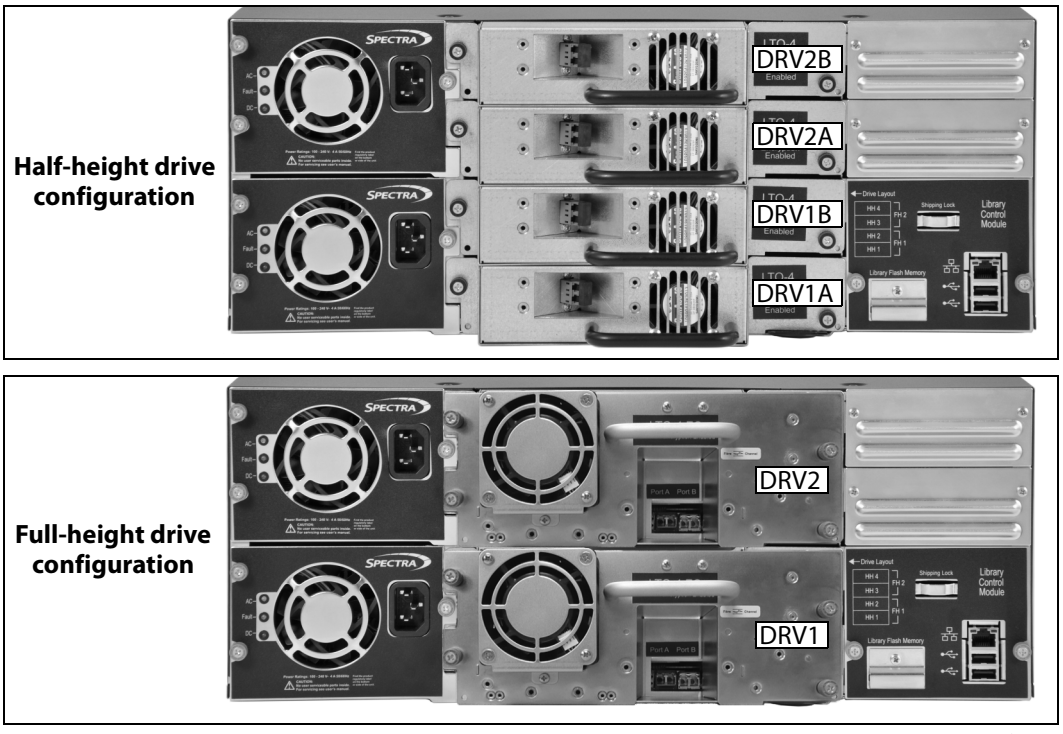


Figure 99 The relationship between the drive locations and the drive identifiers in the BlueScale user interface.

The drive identifier is shown as **<*interface*>LTO–DRV<*bay*>**, where:

- **<*interface*>LTO** indicates the type of interface used by the LTO tape drive.
  - **fLTO**—Fibre Channel LTO
  - **sLTO**—SAS LTO
  - **LTO**—SCSI LTO
- **DRV<*bay*>** is the number of the drive bay. The drive bays are numbered from bottom to top, with drive bay 1 (DRV1 or DVR1A) being the bottom-most (see Figure 99 on page 154).

For example, Figure 100 shows the drive identifier for a half-height SAS LTO drive installed in the top half-height drive bay as **sLTO-DRV2B** on the Drives screen. The descriptor indicates that the drive is present and that it is powered off.

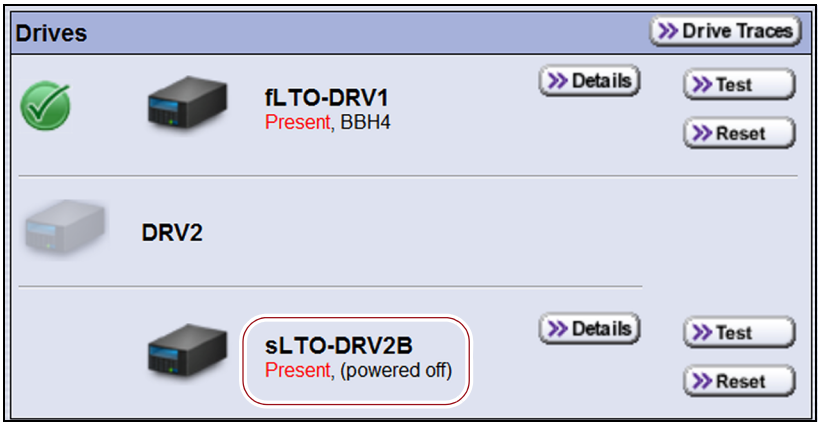


Figure 100 The Drives screen showing the component identifier for a drive (remote access).

Drive World Wide Names

As part of providing network connectivity, the drive sled firmware assigns a location-based World Wide Name (WWN) for the Fibre Channel or SAS tape drive it houses. This WWN is displayed on the Drive Details screen and can be used by the host software to address the drive. Because this WWN is location-based, it remains constant even if a drive is replaced by a different one of the same type. The new drive assumes the location-based BlueScale identifier and WWN.

Notes:

- The fourth digit in the WWN indicates the drive bay where the drive is installed.
- The WWN for Fibre Channel drives is actually the WWPN for Port A on the drive sled. If the drive sled has two ports, the WWPN for port B is the same as the one for port A except that the second digit from the left is **2** instead of **1**.
- The WWN for SAS drives is actually the SCSI port identifier for Port A on the drive sled. Like the Fibre Channel WWN, this identifier is assigned by the device manufacturer and is typically world-wide unique. SAS devices use these port identifiers to address communications to each other.

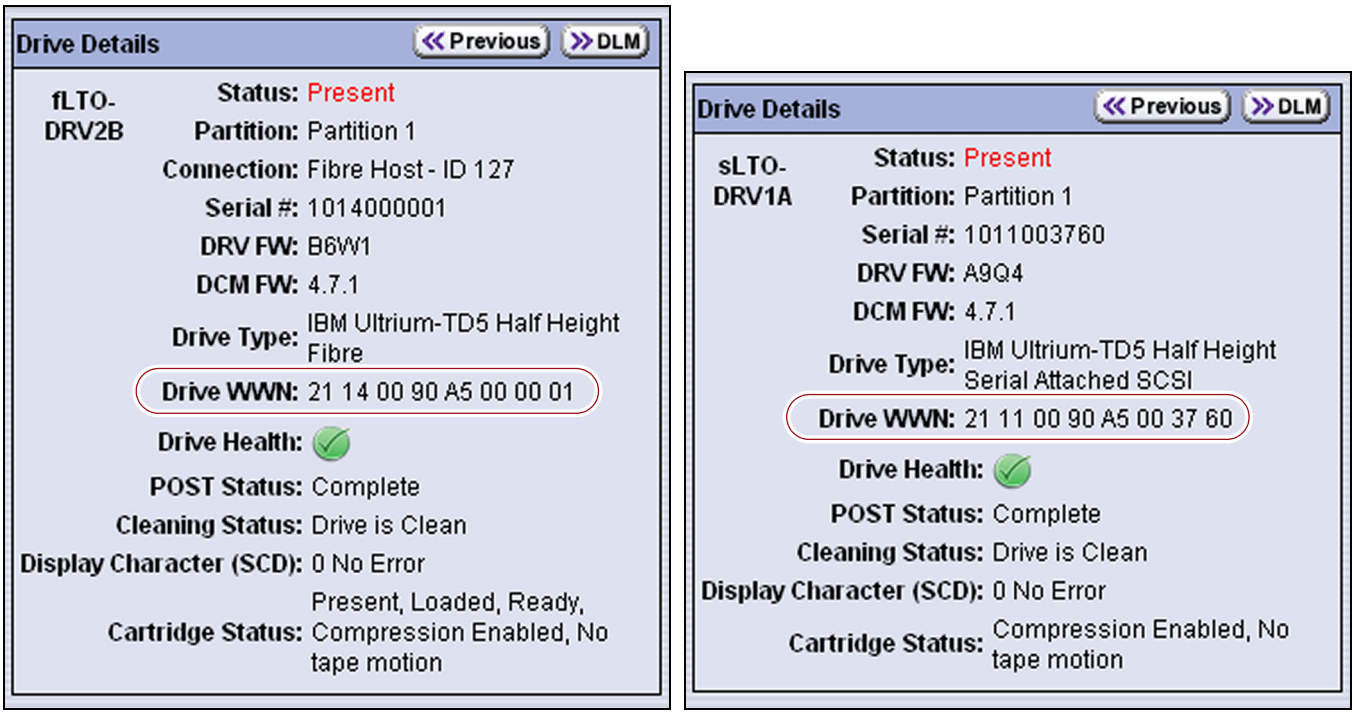


Figure 101 The WWN assigned to a Fibre Channel drive (left) or a SAS tape drive (right).

Drive Serial Numbers

The firmware in the drive sled that houses each drive also assigns a serial number to the drive based on its location in the library. This serial number is especially useful for identifying SCSI tape drives, which do not have a WWN.

The fourth digit from the left in the assigned serial number indicates the drive's location, as shown in Figure 102.

- For half-height drives, the drive bays are numbered from 1 through 4, with drive bay 1 being the bottom-most location.
- For full-height drives, the drive bays are numbered 1 and 3, with drive bay 1 being the bottom-most location.

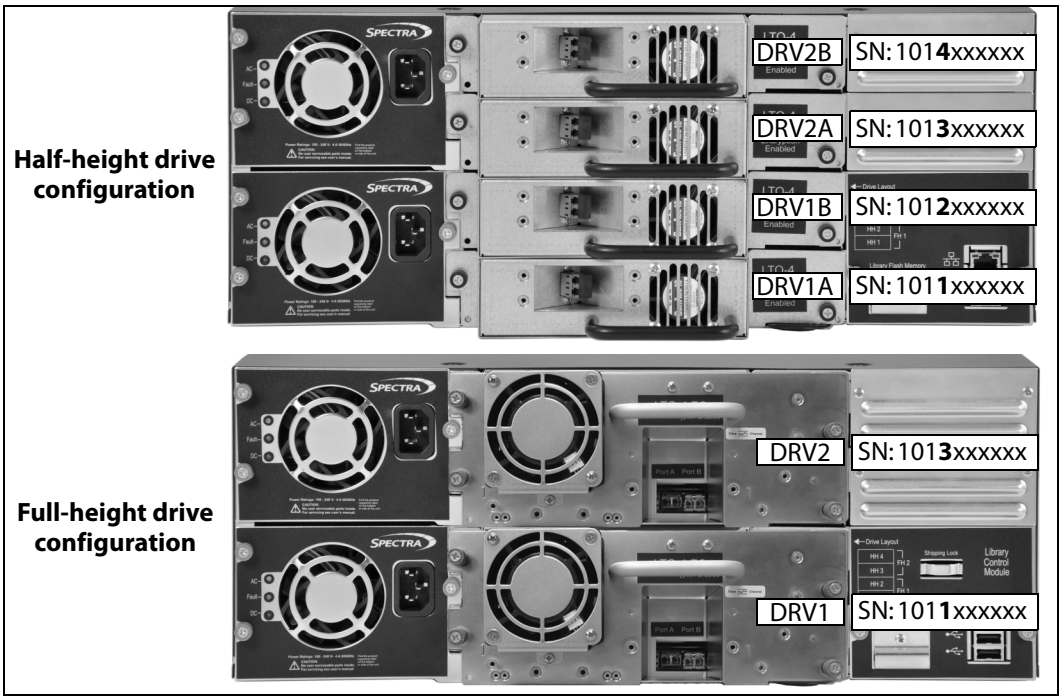


Figure 102 The relationship between the drive bays and the drive serial number.

The serial number also appears on the Drive details screen. For example, in Figure 103 the drive serial number for LTO-DRV1B on the Drive Details screen indicates that the drive is installed in drive bay 2.

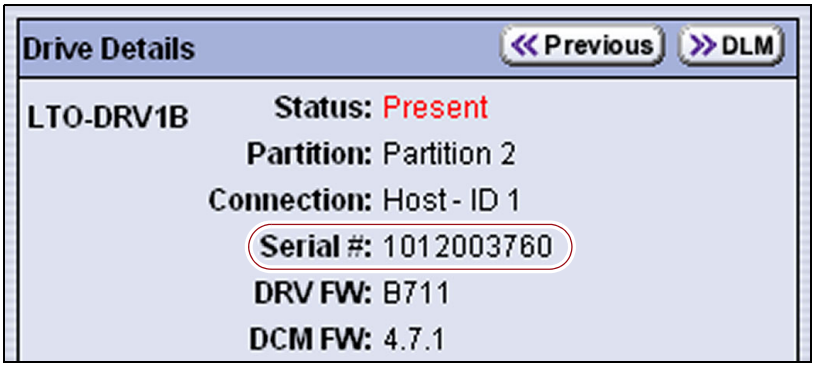


Figure 103 The serial number assigned to a drive.

Identify Fibre Channel-Based Partitions

When monitoring connections to multiple libraries through a Fibre Channel switch, knowing the WWN for a storage partition is useful for identifying a particular library.

Each Fibre Channel-based partition in the library is identified by the WWN shown on the Partitions screen. The partition WWN is actually the World Wide Port Name (WWPN) for Port A of the Fibre Channel drive that provides the robotic control path for the partition (the exporting drive). As a result, the partition has a direct relationship to the WWN of the exporting drive. For example, compare the WWN for Partition 1 with the WWN for drive fLTO-DRV2B in Figure 104.

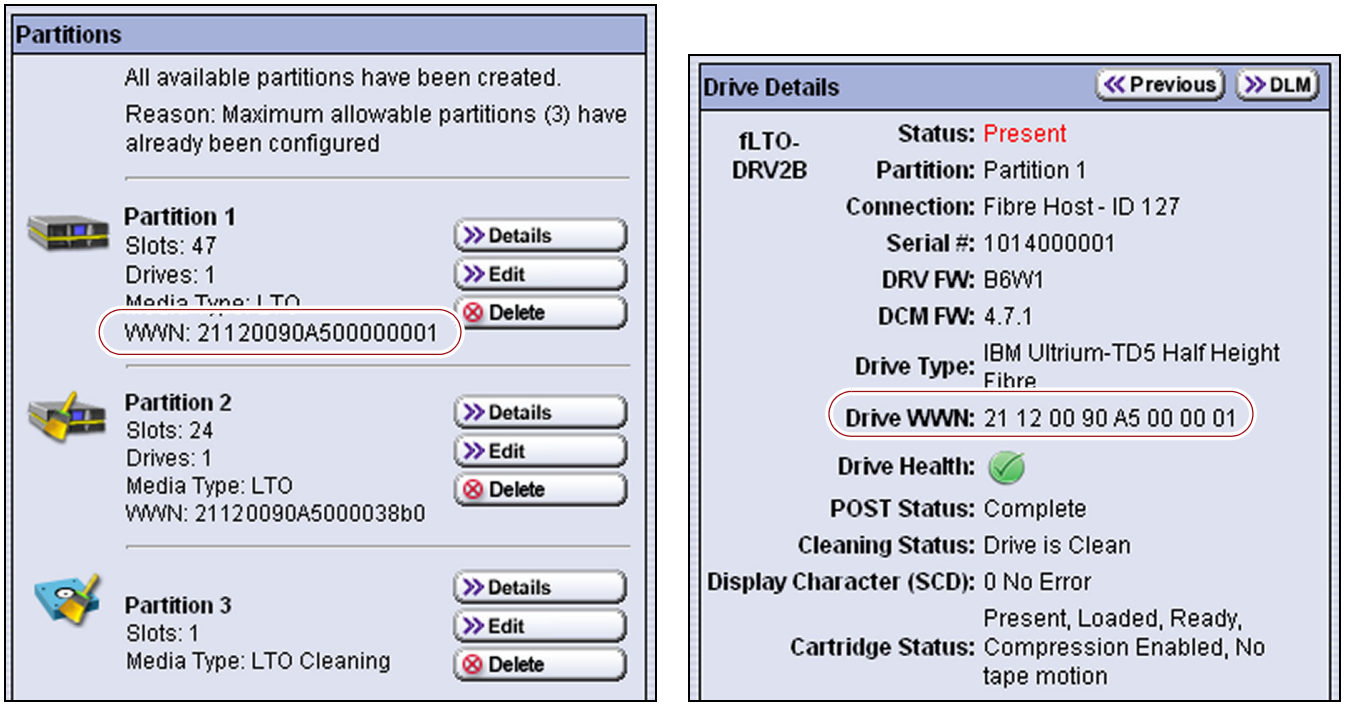


Figure 104 Compare the WWN assigned to Partition 1 (shown on the Partitions screen) with the WWN for drive fLTO-DRV2B, which is the exporting drive for Partition 1 (shown on the Drive Details screen).

Partition WWNs have the following characteristics:

- When seen from the Fibre Channel switch, each storage partition defined in the library appears as an independent library connected to the Fibre Channel arbitrated loop or fabric.
- When seen from the Fibre Channel switch, the second digit of a partition's WWN indicates which tape drive port is connected to the switch. If the second digit from the left in the WWN is **1**, the connection is through Port A; a **2** indicates a connection through Port B. Only the WWN for Port A is shown on the Partitions screen.
- Because they do not have any drives associated with them, cleaning partitions do not have WWNs.
- SAS-based partitions are also assigned WWNs. The WWN is based on the SCSI port identifier for Port A.

CHAPTER 6

Configuring and Managing Partitions

This chapter describes how to use the BlueScale partition wizard to configure and manage partitions in the library.

PARTITION OVERVIEW

The library uses Shared Library Services (SLS) virtualization technology to logically divide the library into one or more storage partitions, up to a maximum of four storage partitions (one for each installed tape drive). Each storage partition looks like a separate physical library to the rest of the backup environment.

By default, the library lets you create a single storage partition. If you need additional storage partitions, you must purchase an SLS activation key to enable creating the additional partitions. Refer to Enabling BlueScale Software Support, Options, and Upgrades on page 112 for information about purchasing and entering activation keys.

When multiple partitions are configured, each partition:

- Has exclusive access to the drives and slots assigned to it.
- Can control the robotics to move cartridges within the partition.
- Shares access to the Entry/Exit slot.

In addition to storage partitions, the library also supports creating a cleaning partition for use when the Auto Drive Clean feature is enabled. The cleaning partition does not count against the number of licensed storage partitions.

The following sections provide information that is useful as you configure the partitions in your library.

Storage Partitions

Functional Overview A storage partition is used to store the data cartridges that are used with the library and your storage management software. The library requires, at a minimum, one storage partition to be configured before you can use the library. Each storage partition must have a minimum of one slot and at least one drive assigned to it. The slots assigned to storage partitions count against the licensed capacity of the library.

Important Unless it is configured as a Global Spare, a drive can only be assigned to one storage partition at a time; it cannot be shared by multiple partitions.

The robotic control path for each storage partition is provided by one of the drives assigned to the partition. This drive is referred to as the exporting drive. The SCSI motion commands used to control the robotics are sent from the host to logical unit number 1 (LUN 1) of the exporting drive. The exporting drive passes the commands to the robotics. SCSI commands to control the operation of the drive itself are sent from the host to LUN 0 of the drive.

Advantages of Multiple Partitions In some environments, using multiple storage partitions is crucial to data center efficiency and growth. For example, multiple partitions are extremely useful in the following situations:

Situation	Advantage of Using Multiple Partitions
Multiple Storage Management Software Applications	If groups within your company use different storage management software applications, each software application requires its own dedicated library. Instead of maintaining multiple physical libraries — one per storage management software application — you can use a single library with multiple partitions; each partition appears to the software as a dedicated library.
Multiple Databases	If your company uses multiple databases, partitioning the library preserves the backup processes associated with each type of database.
Shared Resources	If each department in the company must keep their data segregated, creating multiple partitions supplies this segregation and ensures the integrity of each data set. Each partition can only access the drives and cartridge slots assigned to it. Data from one partition cannot become intermixed with the data stored on the cartridges in another partition.
Multiple Drive Generations	If your data center uses multiple generations of LTO drives, Spectra Logic strongly recommends configuring separate partitions for each generation to ensure read/write compatibility between the drives and cartridges.
Multiple Drive Interfaces	If you have drives with different interface types (for example, Fibre Channel and SAS) installed in the library, the drives using each interface must be in separate partitions.
Encryption	If you want to encrypt some, but not all of your backup data, you can create an encryption partition and a non-encryption partition to segregate the two types of data.

Entry/Exit Operation Modes

The library supports two modes of operation for the Entry/Exit slot: Standard mode and Queued Ejects mode. The mode used by the library is set on the Slots and Drives screen for the first storage partition you configure (see Allocate Slots and Drives on page 180). The mode you select affects the number of partitions that can be configured and determines how the E/E slot operates during export or exchange operations.

Notes:
- The Entry/Exit mode only applies to storage partitions. Importing, exporting, or exchanging cleaning cartridges in cleaning partitions is always done manually using the library operator panel.
- For additional information about the Entry/Exit modes, log on to the portal (see Accessing the Technical Support Portal on page 472), open the Knowledge Base, and search for KBA-01770, *How do Shared IE and Queued Ejects function on the T120?*. The information applies to the T50e as well.

If you select...	Then...
Standard Mode	The entire library must be configured as a single storage partition. From the perspective of the storage management software, the E/E slot is accessible at all times. When the storage management software ejects a cartridge, the cartridge is physically moved to the E/E slot. You must then use the **Open Door** option on the Import/Export screen to open the access port so that you can remove or exchange the cartridge. **Notes:** ▪ Using Standard mode is recommended when the library is configured with a single storage partition. Standard mode is not an option when the library is configured with multiple partitions, including a cleaning partition. ▪ When you configure a storage partition to use Standard mode, the BlueScale software prevents you from configuring any additional partitions. You must reconfigure the partition to use Queued Eject mode before you can configure another storage partition. Similarly, if an existing storage partition uses the Queued Eject mode, you cannot select Standard mode for another storage partition. ▪ If you have only one storage partition and you plan to eject multiple cartridges at a time, using Queued Ejects mode may simplify the process. You can use your storage management software to eject as many cartridges as desired and then remove or exchange the cartridges when it is convenient.

If you select...	Then...
Queued Ejects Mode	The library can be configured with two or more storage partitions. Queued Ejects mode can also be used if there is only one storage partition. Queued Ejects mode allows multiple storage partitions to share the single E/E slot. When operating in Queued Ejects mode, the BlueScale software coordinates access to the E/E slot to ensure that it is always clear which partition "owns" the cartridge in the E/E slot at any given time. The BlueScale software treats all eject operations initiated by the storage management software as logical moves to the E/E slot. The move is reported as successful, but the ejected cartridge is left in its original slot; the slot is marked as inaccessible to the storage management software. Leaving the ejected cartridges in their original slots allows the storage management software to eject more cartridges than the single physical E/E slot can accommodate. When you are ready to physically remove cartridges from the library, you must use the BlueScale user interface from the library's operator panel to select a partition and then use the "Process Queued Ejects" option. During the export process all of the cartridges that were logically ejected by the storage management software are moved one by one to the E/E slot, and the access port opened, so that the cartridges can be removed from the library. After the cartridges are exported, the slots they occupied are once again accessible to the storage management software.

Global Spare Drives

The Global Spare option lets you remotely substitute a working Fibre Channel drive for a failed one using a spare drive in the library. Having a Global Spare drive in the library lets you continue your backup operations and replace the failed drive the next time you are physically present at the library. See Assign a Global Spare Drive on page 179 for instructions on how to assign a Global Spare to a partition; see Using a Global Spare Drive on page 409 for instructions on how to use the Global Spare drive in place of a failed drive.

Configuration Requirements for a Global Spare Drive Before you can configure a partition to use the Global Spare option, the following requirements must be met:

- The partition must use Fibre Channel or SAS LTO drives. The Global Spare feature is not available for SCSI LTO drives.
- In addition to the drives assigned to the partition for use by the host software, the library must have available at least one drive of the same technology generation and interface type as the drives the Global Spare would replace. For example, you cannot use an LTO-4 drive as a spare for an LTO-5 drive nor can you use a SAS LTO-5 drive as a spare for a Fibre Channel LTO-5 drive.
- A Global Spare drive can be shared by multiple partitions. However, the drive can only be used by one partition at a time.
- If a drive of the required type is already installed in the library, you can configure a drive as a Global Spare as part of the initial partition creation process. If you do not currently have a drive that can be used as a Global Spare installed in the library, but install one later, you can edit the partition to configure Global Spares.
- The type of drive you select as the Global Spare determines the type of drives that you can assign to the partition.
- When selecting the drive to be the Global Spare, the library prevents you from selecting drives that cannot be used as Global Spares.
- A Fibre Channel drive that is configured as a Global Spare must be connected to the same Fibre Channel arbitrated loop or fabric as the drives it would replace. If is are not connected to the same Fibre Channel arbitrated loop or fabric, it is not accessible to the application software. You may need to reconfigure your switch to access the Global Spare drive.

  Similarly, a SAS Global Spare drive must be connected to the same host or SAS expander as the drives it would replace.

Global Spare Requirements for Using PostScan If you plan to use one of the MLM PostScan options that requires a Global Spare drive (see Enable and Configure MLM PreScan and PostScan on page 182), you must configure at least one Global Spare drive for the partition.

Keep in mind that when the PostScan process starts, it "owns" the Global Spare drive it is using until all of the cartridges in the PostScan queue are processed (unless you pause the PostScan operation as described in Pause the PostScan Process on page 261). If a Global Spare drive is being used for PostScan it is not available for use as a spare.

Note: See Using PostScan on page 254 for information about the PostScan feature.

Cleaning Partitions and Auto Drive Clean

Cleaning Partition Overview A cleaning partition provides permanent storage for cleaning cartridges inside the library. This special-purpose partition is only used when Auto Drive Clean is enabled for one or more storage partitions and can be shared by multiple storage partitions. The cleaning partition does not have any drives associated with it.

Configuring a cleaning partition does not require an SLS activation key; nor does a cleaning partition count against the four partition maximum for the library. If fewer than the physically present cartridge storage slots are licensed with a Capacity On Demand (CoD) key, the cleaning partition uses any cartridge slots that are not licensed. The slots assigned to the cleaning partition do not count against the licensed capacity. If all of the physically present slots are licensed, the cleaning partition can use any slots that are not already assigned to another partition.

Auto Drive Clean Functional Overview Auto Drive Clean uses the cleaning cartridges stored in the cleaning partition to provide automatic, library-based cleaning of LTO drives without user intervention. Automated drive cleaning results in fewer failed tape read/write operations and is the preferred method for cleaning drives. See Cleaning Cartridge Tracking on page 237 for information about how Media Lifecycle Management (MLM) manages the cleaning cartridges in the cleaning partition.

Note: Drive cleaning operations that are initiated by the storage management software cannot use the cleaning cartridges stored in a cleaning partition; the cartridges are not accessible to the storage management software.

When the drive is unloaded in response to a host request and the data cartridge is moved to its storage location, the library queries the drive to determine if it needs cleaning. If cleaning is required, the library delays notifying the host that the SCSI move command for the unloaded data cartridge is complete while it performs an automatic drive cleaning.

During the delay, the library retrieves a cleaning cartridge from the cleaning partition and inserts it into the drive. When the cleaning is complete, the library returns the cleaning cartridge to the cleaning partition and then notifies the host that the SCSI move command for the unloaded data cartridge is complete.

Automatic cleaning of drives does not occur more than once in any 12 hour period. If the next data cartridge load/unload cycle occurs within this 12 hour waiting period, a cleaning is not attempted unless the previous cleaning attempt failed due to an expired cleaning cartridge. When a cleaning fails, the cleaning is reattempted the next time the host unloads a data cartridge from the drive if the cleaning partition contains a good cleaning cartridge. If you want to clean the drive immediately after you receive the notification that a cleaning failed, you can initiate a manual cleaning (see Manually Cleaning a Drive on page 446).

Configuration Requirements for a Cleaning Partition and Auto Drive Clean

When configuring a cleaning partition, keep the following requirements in mind:

- The Auto Drive Clean feature requires a cleaning partition to be associated with the storage partitions that contain the drives you want to clean. The cleaning partition is created separately and then assigned to one or more storage partitions.
- Configuring a cleaning partition and assigning it to one or more storage partitions automatically enables the Auto Drive Clean feature for those storage partitions (see Creating a Cleaning Partition on page 170 and Allocate Slots and Drives on page 180).
- When a Global Spare drive is associated with a storage partition that has Auto Drive Clean enabled, the drive is cleaned automatically. If a cleaning partition is not associated with the storage partition, the Global Spare drive must be cleaned manually (see Manually Cleaning a Drive on page 446).
- The option to perform a manual cleaning operation using a cleaning cartridge stored in a cleaning partition is only available for drives that are in storage partitions associated with a cleaning partition.
- The cleaning cartridges in the cleaning partition are inaccessible to the storage management software running on the host.
- If you do not configure a cleaning partition and associate it with the storage partitions, you must either use your storage management software to perform the cleaning or use the BlueScale user interface to import a cleaning cartridge into the storage partition and move it to the drive that needs cleaning (see Manually Cleaning a Drive on page 446).
- If your storage management software supports automated drive cleaning and you plan to use this method to clean the drives instead of the library's Auto Drive Clean feature, you can store a cleaning cartridge in the storage partition. The storage management software can then access the cleaning cartridge when needed.

Important

If you store cleaning cartridges in the storage partition, make sure that they are identified as required by your storage management software to prevent the software from attempting to use the cartridges for writing or reading data.

PREPARING TO CONFIGURE PARTITIONS

As you prepare to configure partitions in the library, keep the following requirements in mind. These requirements apply to both cleaning and storage partitions and are in addition to those described in Storage Partitions on page 160 and Cleaning Partition Overview on page 165.

User Privilege Requirements Only users with superuser or administrator privileges can create or modify partitions. See Understanding User Groups and Security on page 94 for information about the three types of user groups and what types of privileges each has.

Slot Availability When you create a storage partition, the library automatically makes all of the licensed cartridge slots that are not already assigned to another partition available for use in the new partition. If all of the slots in your library are already licensed and assigned to existing partitions, you must modify one or more partitions to make slots available for creating a new partition (see Modifying an Existing Partition on page 191).

Background Operations You cannot create, modify, or delete a partition if the library is actively running a PreScan or PostScan operation or if the library is performing certain other background processes (for example, Media Auto Discovery).

> **Note:** See MLM PreScan and PostScan on page 240 to learn how the MLM PreScan and PostScan features interact with the storage partitions.

If you do not want to wait for a Media Auto Discovery, PreScan, or PostScan operation to complete, you can stop the Media Auto Discovery or PreScan operation or pause the PostScan operation. For other background operations, wait for the process to complete.

- Click **Stop Discovery** on the Media Lifecycle Management Tools screen to stop a Media Auto Discovery or PreScan operation (see Initiate Media Discovery Manually on page 250).
- Click **Pause PostScan** on the Media Lifecycle Management Tools screen to pause PostScan for one hour (see Pause the PostScan Process on page 261).

Creation Order You can configure storage partitions either before or after you configure cleaning partitions. However, if you know that you want to use Auto Drive Clean with a storage partition, it is easier to configure the cleaning partition before you configure the storage partition.

If you select to create the storage partitions before the cleaning partition, you must modify the storage partition to assign the cleaning partition to it (thereby enabling Auto Drive Clean for the partition).

Plan the Configuration Before you begin configuring partitions, decide how you want to configure each of the partition settings listed in the following table.

Partition: Setting	Description
Cleaning partition: Number of slots	If you plan to use the Auto Drive Clean feature, decide how many slots you want to assign to the cleaning partition. A cleaning partition can be shared by multiple storage partitions.
Storage partition: Exporter	When a storage partition contains multiple drives, decide which drive is the exporter for the partition. The exporter receives the robotic control commands from the host and relays them to the robotics.
Storage partition: Global Spares	Decide whether you want to use the Global Spare feature and if so, which drive to designate as a Global Spare. See Assign a Global Spare Drive on page 179 for detailed information about the requirements for using Global Spares. **Important:** If you plan to use one of the PostScan options that uses a Global Spare, a Global Spare drive must be assigned to the storage partition.
Storage partition: Number of slots	Decide how many slots you want to assign to each storage partition.
Storage partition: Drive Assignments	Decide which drives to assign to each partition. Only drives that are already installed in the library are available. Each storage partition must have at least one drive associated with it.
Storage partition: PreScan and PostScan	Decide whether or not you want the library to scan the cartridges in the partition for media errors. See Using PreScan on page 252 and Using PostScan on page 254 for detailed information about the PreScan and PostScan features.
Encryption Mode	Decide whether or not to encrypt data in the partition and what type of encryption and encryption key management to use. The Encryption screen does not display unless you are logged into the library as an encryption user and either create one or more BlueScale encryption keys or configure a Spectra SKLM server. See Chapter 10 – Encryption and Key Management, beginning on page 289 for details.
Storage partition: Users	Decide which users are allowed to access the partition. See Configuring Library Users on page 94 for information about the user groups and the privileges each has. **Note:** Members of the superuser and administrator groups can access all partitions.
Fibre Channel Storage Partition: Drive Addressing Mode and Loop ID	If the partition uses Fibre Channel drives, decide what addressing mode to use for each Fibre Channel drive. If you select soft addressing, each Fibre Channel port is identified by an address assigned to the drive when it connects to the Fibre Channel arbitrated loop, fabric, or SAN. If you select hard addressing, the drive uses the fixed Loop ID you set.
SCSI Storage partition: Drive SCSI IDs	If a partition uses SCSI drives, decide what SCSI ID to use for each drive. Each SCSI ID must be unique for the SCSI bus to which the drive is connected. Valid SCSI IDs on a wide SCSI bus are 0 – 15.

ACCESSING THE PARTITION WIZARD

The BlueScale Partition wizard is used to perform all partition configuration operations. Use the following steps to access the wizard whenever you need to create or modify a partition.

1. Log into the library as a user with superuser or administrator privileges. If you want to configure encryption in the partition, log in as an encryption user (see Chapter 10 – Encryption and Key Management, beginning on page 289 for more details).
2. The General Status screen displays. Click **MENU** to display the menu screen that was last viewed.
3. Click **Configuration** to display the Configuration menu.

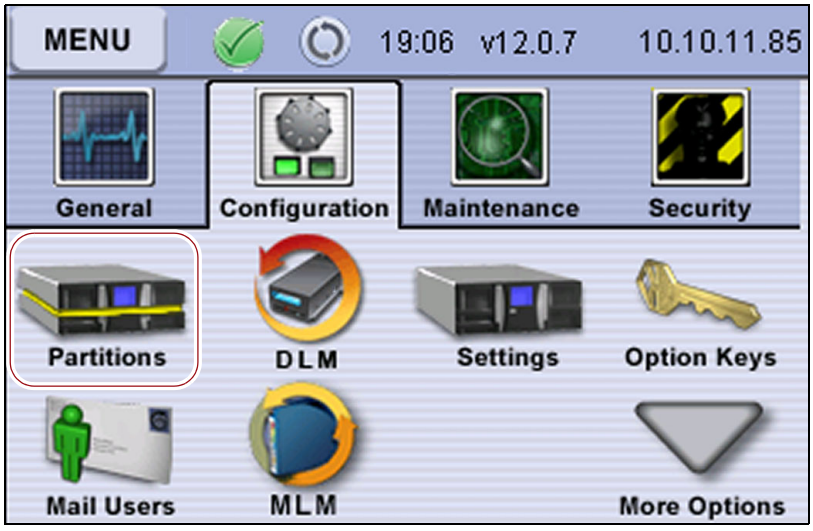


Figure 105 Click **Partitions** on the Configuration menu.

4. Click **Partitions** on the Configuration menu. The Partitions screen displays.

Figure 106 The Partitions screen with existing partitions.

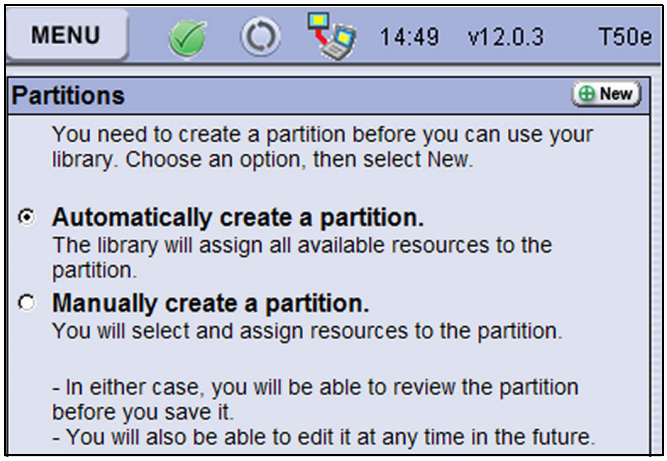


Figure 107 The Partitions screen with no existing partitions.

5. Click **New** or **Edit** to launch the partition wizard.

CREATING A CLEANING PARTITION

If you know that you want to use Auto Drive Clean with a storage partition, it is easier to configure the cleaning partition before you configure the storage partitions. If you select to create the storage partitions before you create the cleaning partition, Auto Drive Clean is not enabled until you modify the storage partitions to assign a cleaning partition to them.

Notes:
- If you want to configure the storage partitions first, skip to Creating a Storage Partition on page 174.
- If the existing storage partitions use all of the slots in the library, modify a storage partition to make slots available for use in the cleaning partition (see Modifying an Existing Partition on page 191).

Use the following steps to create a cleaning partition.

1. Access the BlueScale Partition wizard (see Accessing the Partition Wizard on page 169).
2. From the Partitions screen, the next step depends on whether any partitions, including a cleaning partition, are already configured.
   - If the library does not currently have any partitions configured, the Partitions screen displays two options for creating a partition. Select **Manually create a partition**, then click **New**.

Important Do not select the **Automatically create a partition** option. Doing so configures all of the available slots in the library as a storage partition. You then need to modify the storage partition to make slots available for a cleaning partition.

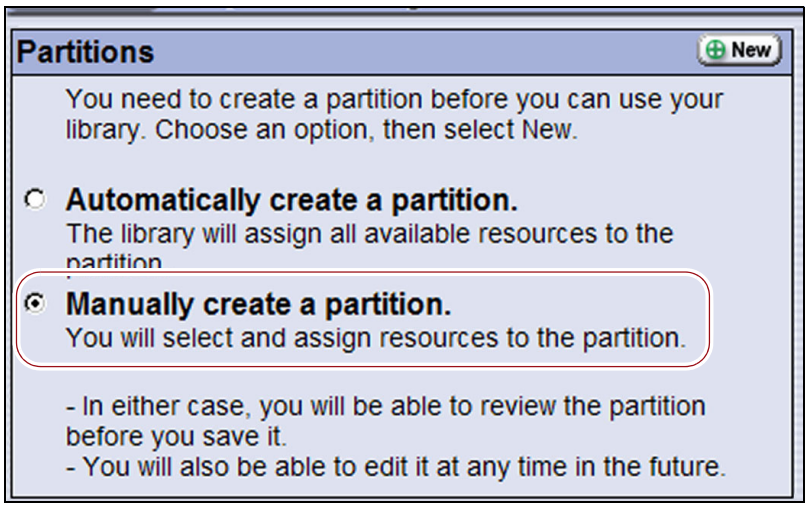


Figure 108 Select **Manually create a partition** to create a cleaning partition.

- If one or more partitions are already created, the existing partitions are listed in alphabetical order on the Partitions screen. Click **New** to create a new partition.

Note: If the **New** button is NOT displayed, then all slots in the library are allocated or the existing partition is configured for Standard Entry/Exit mode. You need to edit an existing partition to free up slots or change the Entry/Exit mode before you can create a cleaning partition.

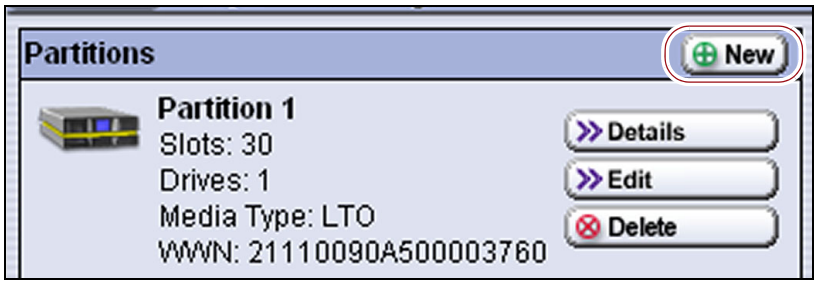


Figure 109 Click **New** on the Partitions screen to begin creating the cleaning partition.

3. On the Name & Media Type screen, enter a name for the partition and select **LTO Cleaning** as the media type.

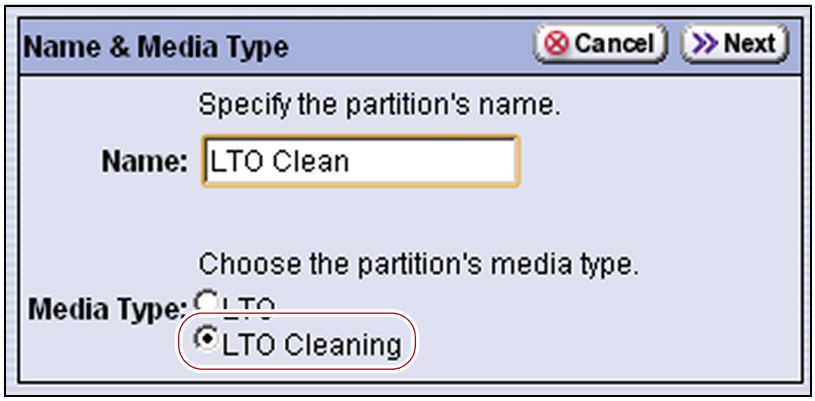


Figure 110 Enter a name for the partition and select **LTO Cleaning** to create a cleaning partition.

For this field...	Do the following...
Name	Enter a unique, descriptive name to identify the partition as a cleaning partition. Names can be any length and can include @ - _ /. and the space character. Partition names over 32 characters cause a scroll bar to display on some screens and are not recommended. **Note:** The default name for a cleaning partition is "Cleaning *n*", where *n* is a number. The partition names list alphabetically in many of the BlueScale screens. If you want the cleaning partitions to be listed after the storage partitions, precede the name with a "z" or "_".
Media Type	Select **LTO Cleaning** to create a cleaning partition.

4. Click **Next**. The Chambers screen displays.

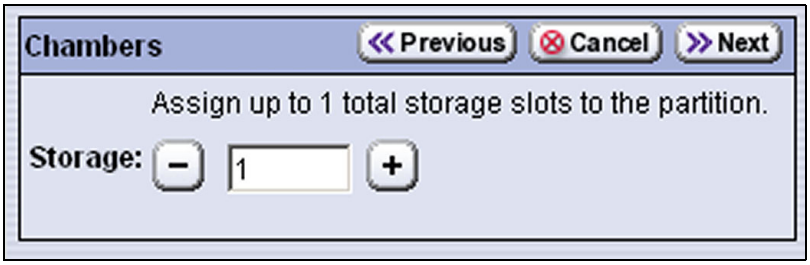


Figure 111 Set the number of slots for the cleaning partition.

5. Click **–** and **+** as required to set the number of storage slots assigned to the cleaning partition.

   Note: A minimum of one slot must be assigned to the partition.

6. Click **Next**. The Save Library Configuration screen displays.

   Note: If you want to save the configuration to a USB device, connect the drive to the USB port on the LCM (see Connect a USB Device to the Library on page 153) and allow time for the device to mount before continuing.

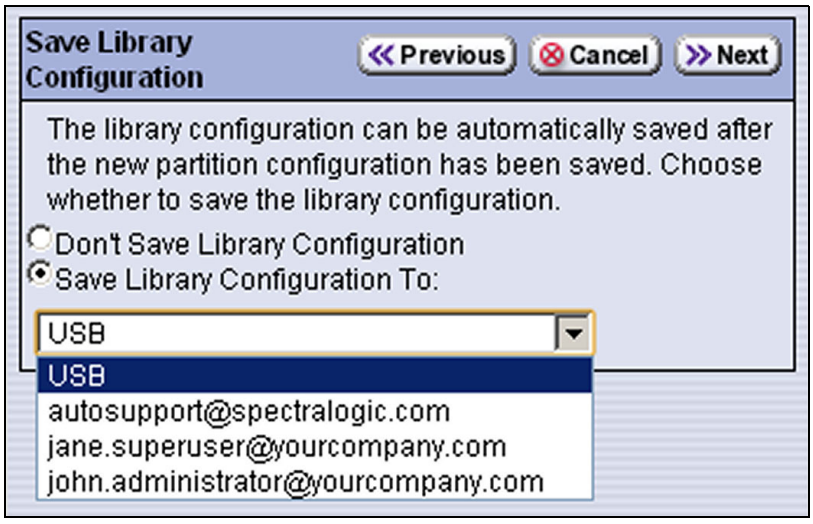


Figure 112 Select whether to save the updated library configuration.

7. Select whether you want to save the current library configuration.

   - **Don't Save Library Configuration** — A backup of the changed library configuration is not saved.
   - **Save Library Configuration To** (highly recommended)—Saves a backup of the library configuration to the selected destination. Using this option is highly recommended to ensure that you can easily restore the library configuration, if necessary.

Select whether to save the library configuration file to USB or to email it to an already-configured mail recipient (see Configure Mail Users on page 107).

Note: Do not select autosupport@spectralogic.com as a recipient. Spectra Logic does not save emailed configuration files unless they are specifically requested for troubleshooting.

8. Click **Next**. The Summary screen displays.

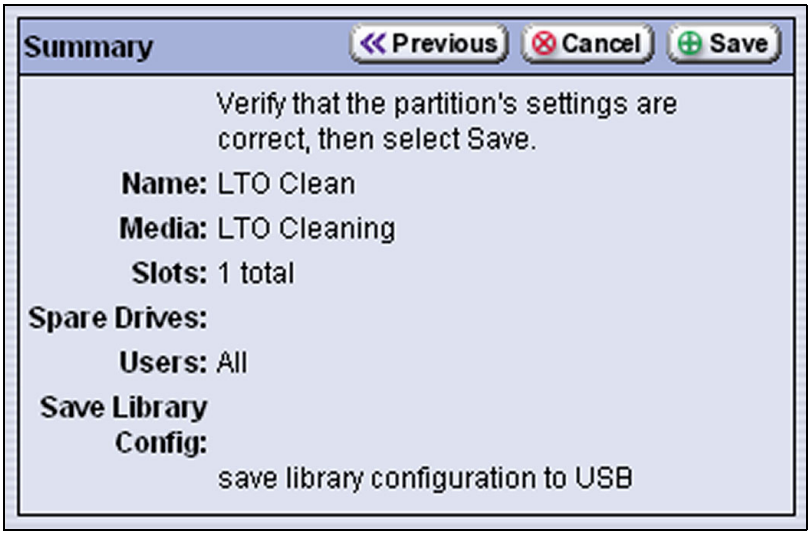


Figure 113 Review the settings for the cleaning partition.

9. Review the information on the screen and confirm that all settings are correct for this partition's configuration.
   - If the configuration information is correct, proceed to Step 10.
   - If the configuration information is not correct, either:
     - Click **Previous** to move backward through the configuration screens until you reach the settings that need correcting. Make any necessary corrections, then click **Next** to move forward through the screens and return to the Summary screen.

       Note: If the screen requiring the correction is toward the beginning of the configuration process, it may be easier to click **Cancel** and repeat the entire configuration process.

       As you move backward through the configuration screens, the values are reset to their default values. After you reach the desired screen and make the necessary changes, advance through the screens and re-enter the necessary information.

     - Click **Cancel** to configure the partition again from the beginning.

10. Click **Save**. The library requires several minutes to store the configuration information, after which the Partitions screen redisplays with the partition you just created added to the list of partitions.

Figure 114 The Partition screen showing the new cleaning partition.

Notes:
- When you save the partition, the library automatically generates a configuration backup file and saves it to the memory card in the LCM. This backup file contains the library configuration, the MLM and DLM databases, and any BlueScale encryption keys that are currently stored in the library.
- If you configured the email option for the automatically generated backup file, the library sends an email with the backup file attached to the specified recipient (see Email Auto Configuration Save on page 111).

CREATING A STORAGE PARTITION

The following sections describe using the BlueScale Partition wizard to create a new storage partition.

Prepare the Library

Before you begin creating a storage partition, make sure that you complete the following:

- Install the drives to be assigned to the storage partition, including any drive that you plan to use as a Global Spare (see Installing the Tape Drives on page 52).
- Enter the CoD activation key for any additional slot capacity you plan to use (see Enter Activation Keys on page 115).
- If you want to configure the partition to use encryption, log into the encryption feature (see Log Into the Encryption Feature on page 291).

Important Components not configured in a partition may not display in the BlueScale interface for a few minutes after library initialization.

Define the Initial Storage Partition Settings

If you did not yet create any partitions on the library, you can choose to either have the BlueScale partition wizard automatically create a single storage partition that uses all of the licensed slots and installed drives or you can use the wizard to manually create storage partitions to your own specifications.

Important The drives you plan to use in the partition must be installed in the library before you start configuring the partition.

Important Components not configured in a partition may not display in the BlueScale interface for a few minutes after library initialization.

Automatically Create a Partition

Use the following steps to have the BlueScale partition wizard automatically create a single storage partition that uses all the slots that are licensed by the CoD activation key, all installed drives, and Standard mode for the Entry/Exit mode.

1. Log in as a user with superuser or administrator privileges.
2. On the General Status screen, click **MENU** to display the menu screen that was last viewed.
3. Click **Configuration** to display the Configuration menu.
4. Click **Partitions** on the Configuration menu. The Partitions screen displays.

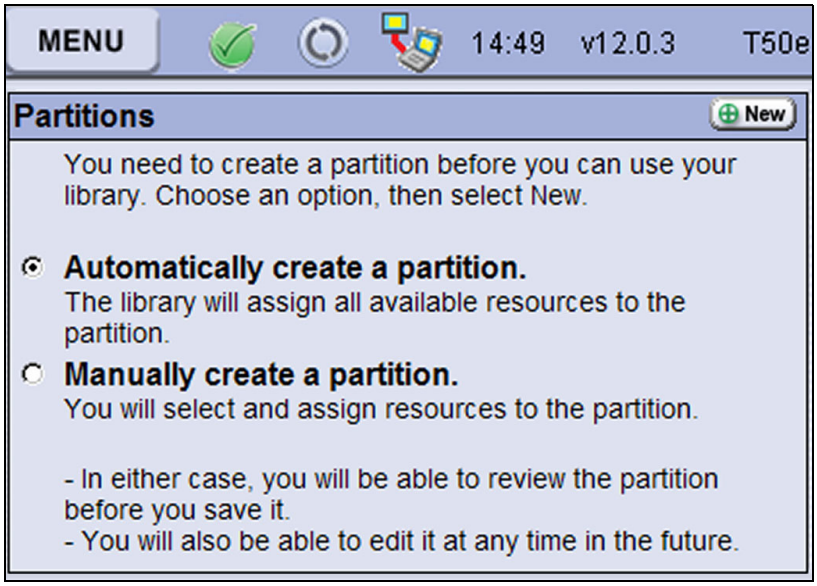


Figure 115 The Partitions screen with no existing partitions.

5. Select **Automatically create a partition** and click **New**.

Notes:
- This option is only available if all of the drives in the library are of the same type (Fibre Channel or SAS) and there are currently no partitions, including cleaning partitions.
- If you want to use Auto Drive Clean with the partition and the library does not contain unlicensed chambers, you need to modify the partition after it is created to remove some of the chambers assigned to it so that you can create a cleaning partition.
- If you want to use the Global Spare option with the partition, you need to modify the partition after it is created to unassign one or more of the drives that were automatically assigned to the partition, and then reassign those drives as Global Spares.
- If you want to use encryption with the partition, you need to modify the partition after it is created to enable encryption (see the *Spectra Tape Libraries Encryption User Guide*).

Manually Create a Partition

Use the following steps to create a storage partition using the partition wizard.

1. Log in as a user with superuser or administrator privileges. If you want to configure encryption in the partition, you must also log in as an encryption user (see the *Spectra Tape Libraries Encryption User Guide* for more details).
2. On the General Status screen, click **MENU** to display the menu screen that was last viewed.
3. Click **Configuration** to display the Configuration menu.
4. Click **Partitions** on the Configuration menu. The Partitions screen displays.

Figure 116 The Partitions screen with existing partitions.

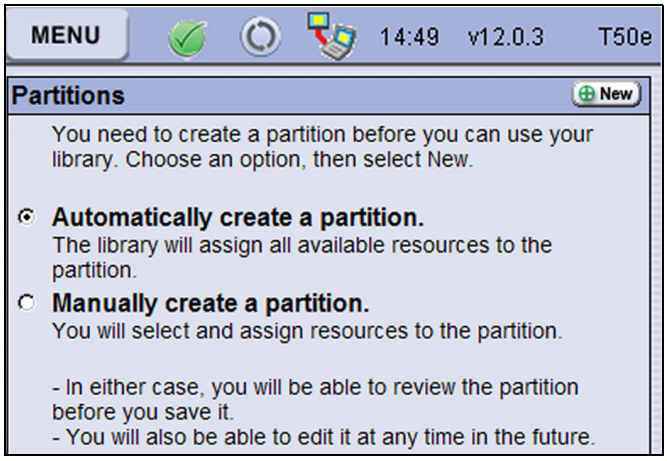


Figure 117 The Partitions screen with no existing partitions.

5. Select **Manually create a partition**, if necessary, and click **New**. The Name and Media Type screen displays.

   Note: If the **New** button is NOT displayed, then all slots in the library are allocated, the existing partition is configured for Standard Entry/Exit mode, or the maximum number of partitions already exist. You need to edit an existing partition to free up slots or change the Entry/Exit mode before you can create a storage partition.

Define the Partition Name and Media Type

After choosing the method for creating the partition, click **New** to display On the Name and Media Type screen, enter a name for the storage partition and select the media type, and then click **Next**.

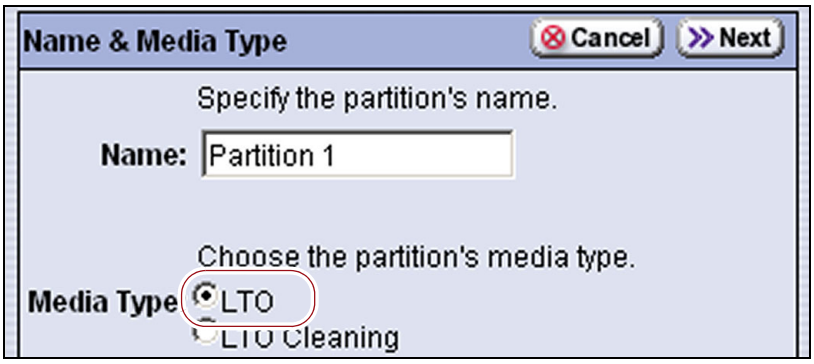


Figure 118 Enter a name for the partition and select the media type.

For this field...	Do the following...
Name	Enter a unique, descriptive name to identify the partition. Names can be any length and can include @ - _ /. and the space character. Partition names over 32 characters cause a scroll bar to display on some screens and are not recommended. The default name for a storage partition is "Partition *n*", where *n* is a number. **Note:** In many of the BlueScale screens, the partitions are listed alphabetically. Keep this in mind when naming your partitions.
Media Type	Select **LTO** to create a storage partition that uses LTO drives and media.

Select the Exporter for the Partition

One drive in the partition is designated as the "exporter" for the partition. This drive provides the control path for the robotic motion commands sent from the host to the robotics.

Note: You can use any drive you plan to include in the partition as the exporter.

1. From the Name and Media Type screen, click **Next**. The Exporter screen displays a list of the drives currently installed in the library.

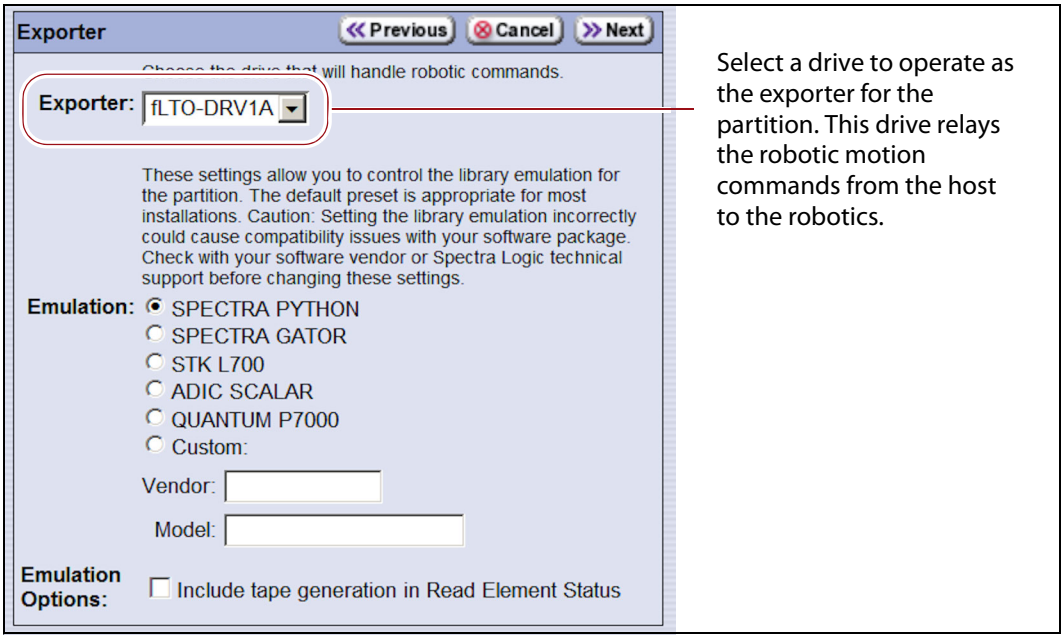


Figure 119 Select the exporting drive.

2. Select the drive that provides the control path for the robotics.
3. If you need to configure the partition to emulate a different type of library, see Configure Emulation on page 136.

Assign a Global Spare Drive

Use the following steps to configure one or more Global Spare drives for the partition. See Global Spare Drives on page 163 for information about configuring Global Spares.

1. From the Exporter screen, click **Next**. The Spare Drives screen lists the drives that are available for use as Global Spares.

   If you do not want to configure spare drives or if the screen indicates that no drives are available for use as a spare, click **Next** again and skip to Allocate Slots and Drives on page 180.

2. Select one of the available drives to be designated as a spare. The check boxes for drives that cannot be used as spares are grayed out.

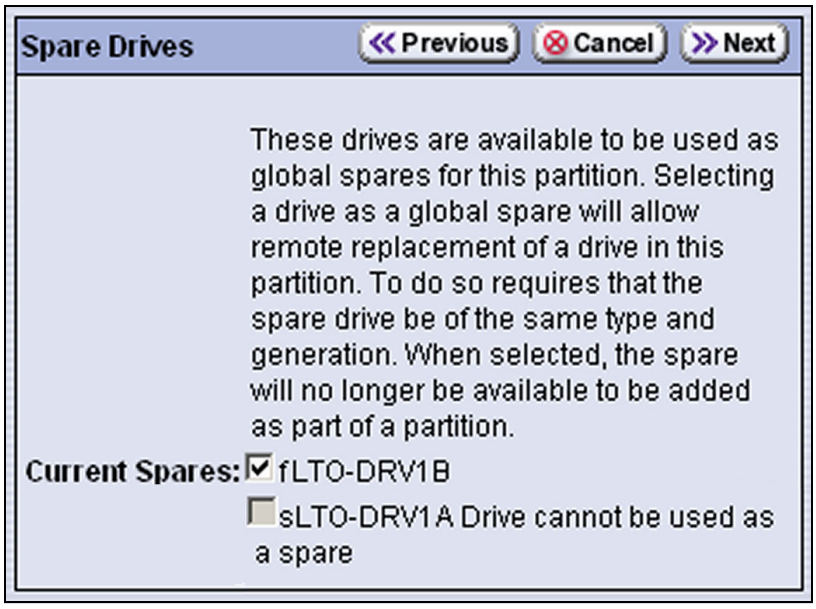


Figure 120 Select the drive you want to use as a Global Spare.

Allocate Slots and Drives

1. From the Spare Drives screen, click **Next**. The Chambers & Drives screen displays.

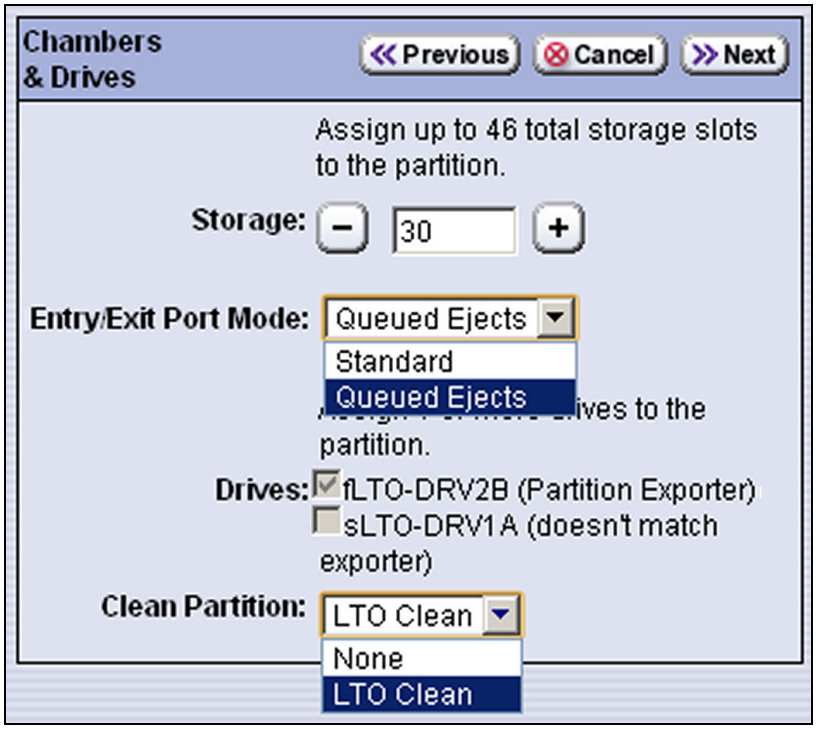


Figure 121 Set the options in the Chambers & Drives screen.

2. Set the following options.

For this option...	Do the following...
Storage	Click **–** and **+** as required to set the number of storage slots to assign to the partition. **Notes:** ▪ A storage partition must have a minimum of one slot. ▪ Slots assigned to the cleaning partition are separate from the slots assigned to a storage partition. ▪ If all of the slots in the library are licensed with a CoD option key and you want to use a cleaning partition but did not yet created it, subtract the number of slots you want to use for the cleaning partition from the total number of slots available to be assigned to the storage partition. ▪ If you did not license all of the slots in the library, the slots that are not licensed are available for use in a cleaning partition.

For this option...	Do the following...
Entry/Exit Port Mode	Select the operational mode for the access port. See Entry/Exit Operation Modes on page 162 for detailed information about how the two modes operate. ▪ **Standard** — Use this option if you are configuring the entire library as a single storage partition and do not plan to use a cleaning partition. ▪ **Queued Ejects** — Use this option if you are configuring multiple partitions, including a cleaning partition. If you already configured one or more partitions, Queued Ejects is the only available option.
Drives	Select the drives to be dedicated to this partition. The check boxes for any installed drives that cannot be used in the partition are grayed out. **Important:** If you plan to use MLM to monitor media health, Spectra Logic strongly recommends that you configure LTO-4 and later generation drives in separate partitions and that you do not routinely share LTO-4 media between LTO-4 and later generation drives. This ensures the accuracy of the LTO-4 media health data (see Media Health Score on page 235 for more information). ▪ You can only select drives with the same interface type as the exporting drive for the partition. You cannot use drives with different interface types in the same partition. ▪ Only drives that are not already assigned to a partition or configured as a Global Spare are listed. ▪ If you enabled Global Spares (see Assign a Global Spare Drive on page 179), you can only select drives of the same generation and interface type as the Global Spare drive assigned to the partition. ▪ If you plan to mix multiple generations of cartridges in the same partition, make sure that the drives in the partition are compatible with every generation (see LTO Read/Write Compatibility on page 513 for compatibility information).
Cleaning Partition	Select the name of the cleaning partition to be used for the drives in the storage partition. Associating a cleaning partition with the storage partition enables the Auto Drive Clean feature for the partition. If you do not want to enable Auto Drive Clean, click **None**. **Note:** The option to select a cleaning partition is only available if you previously configured a cleaning partition that uses the same type of media as the storage partition (see Creating a Cleaning Partition on page 170). If you create a cleaning partition later, edit the storage partition to associate the cleaning partition with it.

Enable and Configure MLM PreScan and PostScan

When MLM is enabled, you can configure the partition to use the MLM PreScan and PostScan features.

Notes:
- MLM is enabled by default. If you want to use PreScan and PostScan but do not see the MLM Media Verification screen, check to see if MLM is disabled (see Enabling MLM and Configuring Global Settings on page 242).
- The available features depend on the drive type used in the partition. See Using PreScan on page 252 and Using PostScan on page 254 for information about these features.

Drive Type	PreScan	PostScan			Drive Firmware Required
		FullScan	QuickScan	QuickScan with Global Spares	
LTO-3, SCSI	**available**	unavailable	unavailable	unavailable	93G0 or later
LTO-3, Fibre Channel	**available**	unavailable	unavailable	unavailable	93G0 or later
LTO-4, Fibre Channel	**available**	**available**	**available**	**available**	97F9 or later
LTO-5, Fibre Channel	**available**	**available**	**available**	**available**	B170 or later
LTO-5, SAS	**available**	unavailable	**available**	unavailable	B170 or later
LTO-6, Fibre Channel	**available**	**available**	**available**	**available**	C9T4 or later
LTO-6, SAS	**available**	unavailable	**available**	unavailable	C9T4 or later
LTO-7, Fibre Channel	**available**	**available**	**available**	**available**	FA11 or later
LTO-7, SAS	**available**	unavailable	**available**	unavailable	FA11 or later
LTO-8, Fibre Channel	**available**	**available**	**available**	**available**	HB83 or later
LTO-8, SAS	**available**	unavailable	**available**	unavailable	HB83 or later
LTO-9, Fibre Channel	**available**	**available**	**available**	**available**	NCA1 or later
LTO-9, SAS	**available**	unavailable	**available**	unavailable	NCA1 or later

Use the following steps to configure the PreScan and PostScan features used in the partition.

1. From the Chambers and Drives screen, click **Next**. The MLM Media Verification screen displays.

   Note: If you do not want to use the PreScan and PostScan features, click **Next** again and skip to Configure Encryption on page 185.

2. Enable and configure the PreScan and PostScan options for the partition.

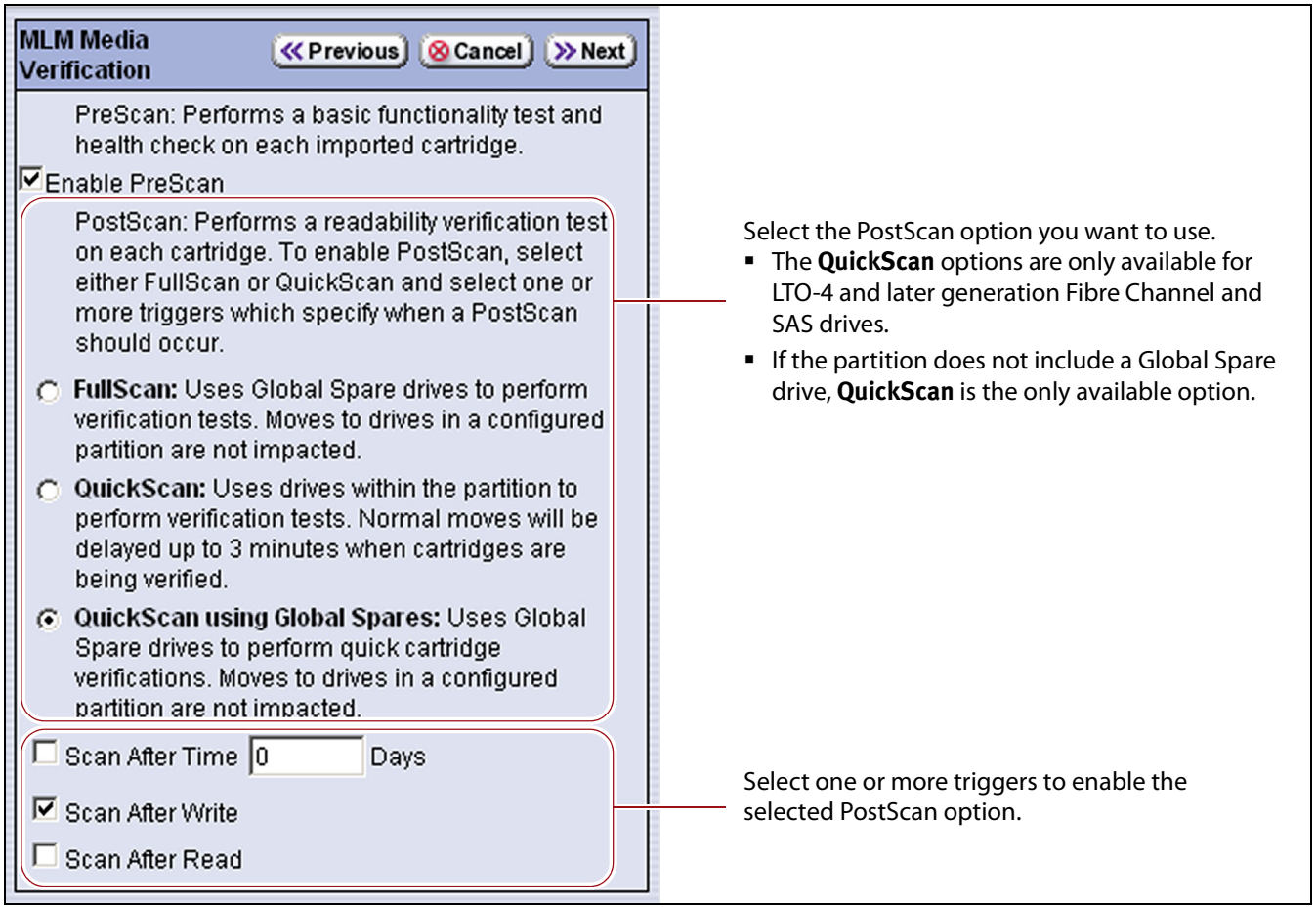


Figure 122 Enable PreScan and select the PostScan option and triggers.

Important To enable PostScan for the partition you must select one of the PostScan options (FullScan, Quick Scan, or QuickScan using Global Spares) and one or more of the Scan triggers.

Notes:
- The available PostScan options depend on whether the partition uses LTO-4 and later generation drives and whether or not a Global Spare drive is assigned to the partition.
- The automatic PostScan operation configured on this screen only verifies MLM-enabled LTO cartridges. If your partition uses LTO cartridges that are not MLM-enabled, you must add them to the PostScan queue manually (see Schedule a Manual PostScan on page 258).

Select this option...	To...	Default
Enable PreScan	Enable the PreScan feature. When enabled, PreScan replaces the more basic Media Auto Discovery process. See Using PreScan on page 252 for information about this option.	Cleared (Disabled)

Select this option...	To...	Default
FullScan	Use the FullScan feature. When enabled by selecting one or more PostScan triggers, FullScan uses a Global Spare drive assigned to the partition to verify all of the data on each cartridge. See Using PostScan on page 254 for information about this option. **Notes:** ▪ FullScan is not available unless a Global Spare drive is configured for the partition. ▪ FullScan is only available if the partition uses Fibre Channel or SAS LTO-4 and later generation drives. It is not available for SCSI LTO drives.	Not selected and no Scan triggers selected (PostScan Disabled)
QuickScan	Use the QuickScan feature. When enabled by selecting one or more PostScan triggers, QuickScan uses one of the drives in the partition to verify the data on a single wrap, from the beginning of the tape (BOT) to the end of the wrap or the end of recorded data (EOD), whichever comes first. See Using PostScan on page 254 for information about this option. **Note:** QuickScan is only available if the partition uses LTO-4 or later generation drives.	Not selected and no Scan triggers selected (PostScan Disabled)
QuickScan using Global Spares	Use the QuickScan using Global Spares feature. When enabled by selecting one or more PostScan triggers, QuickScan uses a Global Spare drive assigned to the partition to verify the data on a single wrap, from the beginning of the tape (BOT) to the end of the wrap or the end of recorded data (EOD), whichever comes first. See Using PostScan on page 254 for information about this option. **Notes:** ▪ QuickScan using Global Spares is not available if a Global Spare drive is not configured for the partition. ▪ QuickScan using Global Spares is only available if the partition uses LTO-4 or later generation drives.	Not selected and no Scan triggers selected (PostScan Disabled)
Scan Triggers	Enable the selected PostScan option and configure one or more triggers. ▪ **Scan After Time** — Add the cartridges in the partition to the automatic PostScan queue after the specified number of days pass since the last scan. Enter the number of days in the **Days** field. ▪ **Scan After Write** — Add a cartridge to the automatic PostScan queue each time data is written to it. ▪ **Scan After Read** — Add a cartridge to the automatic PostScan queue each time data is read from it. **Note:** Selecting any of these triggers automatically enables the selected PostScan option.	All cleared (PostScan Disabled)

Configure Encryption

Note: If you do not want to enable encryption for the partition you are configuring, click **Next** and proceed to Specify the Partition Users on page 186.

Requirements If the storage partition is using an LTO-4 or later generation tape drive and you create a BlueScale encryption key, you can enable BlueScale Encryption key management for the partition and assign an encryption key to it.

If the storage partition is using an LTO-5 or later generation tape drive and you configured a Spectra SKLM server, you can enable Spectra SKLM Encryption key management for the partition.

Important To use Spectra SKLM Encryption key management, LTO-5 drives must be updated to firmware version C7RC, or later. All LTO-6 or later generation drive firmware supported for use with the library can be used with Spectra SKLM encryption.

The Encryption screen does not display unless you are logged into the library as an encryption user and either created an encryption key or configured a Spectra SKLM server.

Notes:
- If you are not logged into the encryption feature, or did not either create an encryption key or configure a Spectra SKLM server, proceed to Specify the Partition Users on page 186. You can modify the partition to use encryption later, as described in this section.
- See Chapter 10 – Encryption and Key Management, beginning on page 289 for detailed configuration instructions.
- You can only use one type of encryption in a partition.
- Spectra SKLM key management is not compatible with BlueScale Encryption key management, because they cannot share encryption keys. Data encrypted using Spectra SKLM key management cannot be decrypted using BlueScale Encryption key management, and vice versa.

Use the following steps to configure encryption in the partition:

1. From the MLM Media Verification screen, click **Next**. The Encryption screen displays.

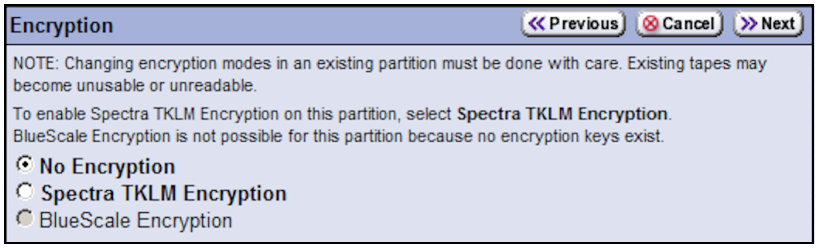


Figure 123 If desired, enable encryption for the partition.

2. Select the type of encryption you would like to enable:

Type	Configures the partition to...
No Encryption	Turn off encryption. None of the data in the partition is encrypted. This is the default setting.
Spectra SKLM Encryption	Turn on Spectra SKLM Encryption key management for drive-based encryption using direct-attached LTO-5 and later generation drives. **Note:** If PostScan was enabled on the MLM Media Verification screen, Spectra SKLM Encryption cannot be selected, and is grayed out.
BlueScale Encryption	Turn on BlueScale drive-based encryption using direct-attached LTO-4 and later generation drives. All key management tasks are performed through the BlueScale user interface. **Note:** If you have BlueScale Encryption Professional edition and multiple encryption keys configured on the library, select the primary key for the partition. This key is used when encrypting and decrypting data. Then, Select none, one, or multiple additional keys to be associated with the partition for decrypting data. A maximum of eight decryption keys can be assigned to one partition.

Specify the Partition Users

1. From the MLM Media Verification screen or the Encryption screen, click **Next**. The Partition Users screen displays.

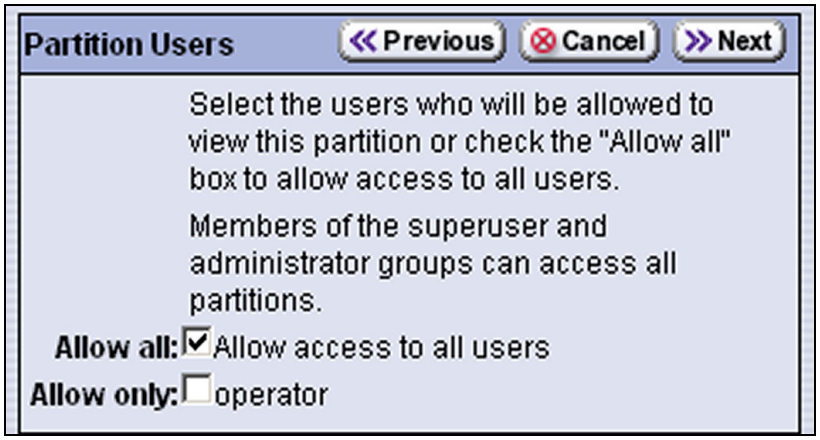


Figure 124 Select which users access the partition.

2. Select the users who are allowed access to this partition. Only users who are already configured can be selected (see Configuring Library Users on page 94).

   Note: All of the users who are configured with operator privileges are listed under **Allow only**. Select one or more of these users to enable partition-based security for operators. Superusers and administrators always have full access to all partitions.

Assign Drive IDs

You must assign a *unique* ID to each Fibre Channel or SCSI drive used in the partition.

Note: SAS tape drives do not have IDs. If the partition uses SAS drives, the Drive IDs screen does not display. Skip to Confirm and Save the Partition Settings on page 188.

1. From the Partition Users screen, click **Next**. The Drive IDs screen displays. The method for setting the Drive ID depends on the interface type used by the drive.
   - **Fibre Channel drives**—Select **Soft addressing** or **Hard addressing**.

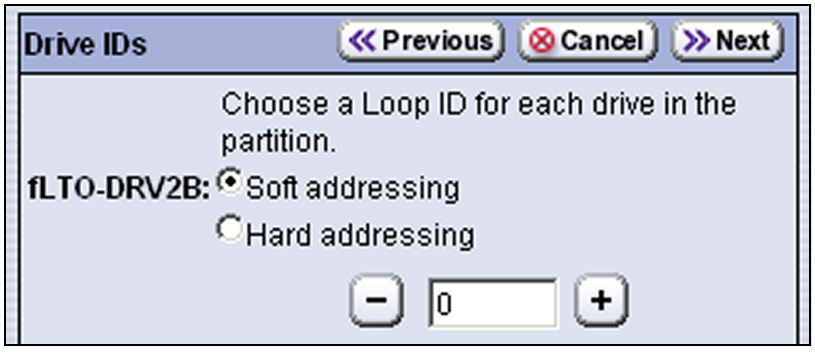


Figure 125 Set the Loop ID mode for a Fibre Channel drive.

   - **Soft addressing** (recommended) is the default setting. The drive is assigned a soft address when it connects to the Fibre Channel arbitrated loop or fabric.
   - If you select **Hard addressing**, click **+** and **–** as required to select a unique loop ID for each tape drive. If the address you select is assigned to another device on the Fibre Channel arbitrated loop or fabric, the host may not be able to connect to the drive.
   - **SCSI drives**—Click **+** and **–** as required to select a unique SCSI ID for the drive.

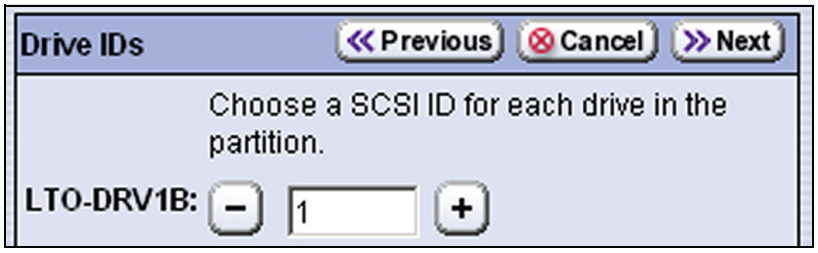


Figure 126 Set the SCSI ID for a SCSI drive.

Each device on the SCSI bus must have a unique SCSI ID. Valid SCSI IDs are from 0 to 15 on a wide SCSI bus.

Important Make sure that the SCSI IDs you specify are not assigned to other devices on the same SCSI bus. Assigning the same SCSI ID to multiple devices on the same SCSI bus causes communication problems on the bus.

Confirm and Save the Partition Settings

After you finish configuring the storage partition, confirm and save the settings to complete the creation process.

Note: If you want to save the configuration to a USB device, connect the device to the USB port on the LCM (see Connect a USB Device to the Library on page 153) and allow time for the device to mount before continuing.

1. From the Partition Users or Drive IDs screen, click **Next**. The Save Library Configuration screen displays.

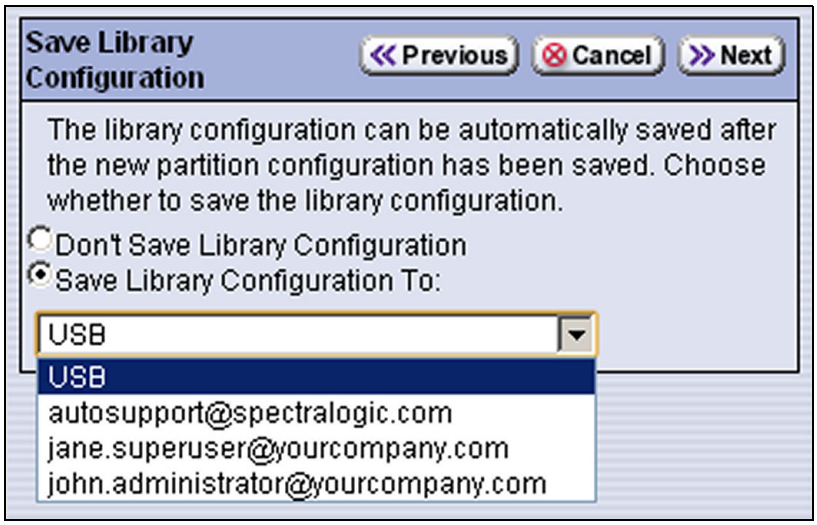


Figure 127 The Save Library Configuration Screen.

2. Select whether you want to save the current library configuration.
   - **Don't Save Library Configuration** — A backup of the changed library configuration is not saved.
   - **Save Library Configuration To** (highly recommended)—Saves a backup of the library configuration to the selected destination. Using this option is highly recommended to ensure that you can easily restore the library configuration, if necessary.

     Select whether to save the library configuration file to USB or to email it to an already-configured mail recipient (see Configure Mail Users on page 107).

   Note: Do not use the default autosupport@spectralogic.com email recipient. Spectra Logic does not save emailed configuration files unless they are specifically requested for troubleshooting.

3. Click **Next**. The Summary screen displays.

   Note: Depending on the options you chose, the Summary screen on your library may be different from the one shown in Figure 128.

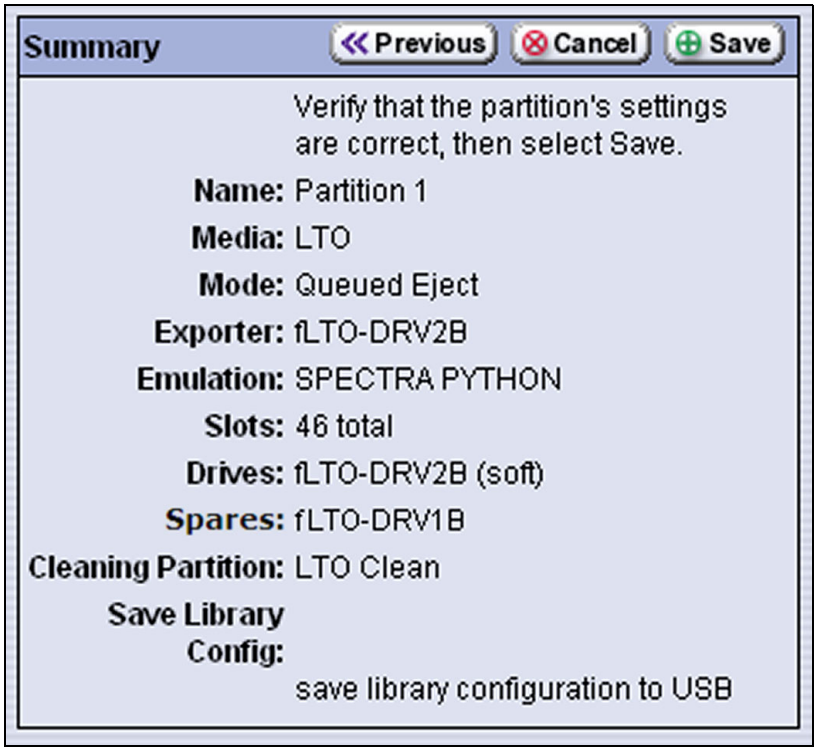


Figure 128 Confirm the settings for the partition.

4. Review the information on the Summary screen to confirm that all settings are correct for this partition's configuration.
   - If the configuration information is correct, proceed to Step 5.
   - If the configuration information is not correct, do one of the following:
     - Click **Cancel** to configure the partition again from the beginning.
     - Click **Previous** to move backward through the configuration screens until you reach the settings that need correcting.

       As you move backward through the configuration screens, the values are reset to their default values. After you reach the desired screen and make the necessary changes, advance through the screens and re-enter the necessary information until you again reach the Summary screen.

   Note: If the screen requiring the correction is toward the beginning of the configuration process, it may be easiest to click **Cancel** and repeat the entire configuration process.

5. Click **Save**. The library requires several minutes to store the configuration information, after which the Partitions screen redisplays with the partition you just created added to the list of partitions.

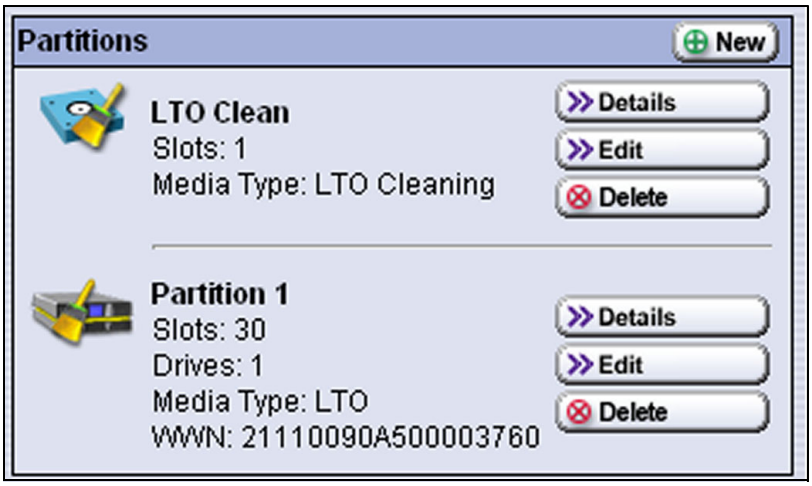


Figure 129 The Partitions screen showing a cleaning partition and a storage partition.

Notes:
- When you save the partition, the library automatically generates a configuration backup file and saves it to the memory card in the LCM. This backup file contains the library configuration, the MLM and DLM databases, and any BlueScale encryption keys that are currently stored in the library.
- If you configured the email option for the automatically generated backup file, the library sends an email with the backup file attached to the specified recipient (see Email Auto Configuration Save on page 111).

6. To configure another storage partition, repeat the entire configuration process, beginning with Creating a Storage Partition on page 174.

MODIFYING AN EXISTING PARTITION

Overview This section describes how to edit or modify an existing partition. You might want to modify an existing partition for any of the following reasons:

- **Assign a Cleaning Partition**—If you created a cleaning partition and now want to assign it to the storage partition, you need to modify the Chambers and Drives screen for the storage partition to add the cleaning partition.
- **Assign a Global Spare Drive**—If you want to designate one of the installed drives as a Global Spare, you need to modify the Spare Drives screen to assign the drive to the partition.
- **Create a New Cleaning or Storage Partition**—If you previously created one or more partitions that use all of the available slots in the library, and now want to create and use a new partition, you need to reduce the number of slots assigned to an existing partition to provide the slots needed for the new partition. If you want to create a storage partition, you may also need to install additional drives or reassign drives that were previously assigned to other partitions.
- **Rename a Partition**—If you want to rename the partition, change the name on the Name & Media Type screen.
- **Disable PreScan or Change the PostScan Settings**—If you want to change the settings that you chose (to take advantage of a new Global Spare drive, for example), you need to select a different setting in the MLM Media Verification screen.
- **Enable or Disable Encryption**—If you need to modify encryption settings for the partition, you need to log in as an encryption user and make the necessary changes.

Preparation Before making changes to an existing partition, review the information at the beginning of this chapter to be sure that you address any requirements (see Preparing to Configure Partitions on page 167). In addition, address the following recommendations and requirements:

- Spectra Logic strongly recommends backing up the library configuration, either to a USB device or as an attachment to an email sent to a previously configured mail recipient, before you make changes.
- When reducing the number of slots assigned to a partition, physically export any cartridges in those slots, as described in Exporting or Exchanging Cartridges on page 214, *before* you remove slots from the partition.

Important By default, the library deletes empty slots from a partition first. If all of the slots are full, the library is forced to delete populated slots. When this happens, the deleted slots are no longer accessible through the BlueScale interface or the storage management software. You must add the slots to a new or an existing partition to access them.

Auto Configuration Save When you make a change to a partition, the library generates an auto-configuration file and saves it to the memory card in the LCM. If you configured the email option for the Auto Configuration Save file, an email containing the updated library configuration, as well as the MLM and DLM databases and any BlueScale encryption keys stored on the library, are sent to the specified recipient (see Email Auto Configuration Save on page 111).

Note: Do not use the default autosupport@spectralogic.com email recipient. Spectra Logic does not save emailed configuration files unless they are specifically requested for troubleshooting.

Use the following steps to modify an existing partition.

1. Discontinue any backups to the partition you want to modify.
2. Log into the library as a user with superuser or administrator privileges.
3. Select **Maintenance** ⋯⁘ **MLM** to display the Media Lifecycle Management Tools screen. If Media Auto Discovery, PreScan, or PostScan is running (as indicated by the presence of a **Stop Discovery** or **Pause PostScan** button, respectively), do the following:
   - Click **Stop Discovery** to temporarily stop Media Auto Discovery or PreScan (see Figure 163 on page 252).
   - Click **Pause PostScan** to pause the PostScan for one hour (see Figure 168 on page 261).
4. If you configured the partition to use encryption or if you want to enable encryption in a partition that did not previously use it, log into the encryption feature (see Configuring BlueScale Key Management on page 310).
5. Select **Configuration** ⋯⁘ **Partitions** to display the Partitions screen.

Figure 130 Click **Edit** for the partition you want to modify.

6. Click **Edit** for the partition you want to modify. The Name & Media Type screen for the partition displays.

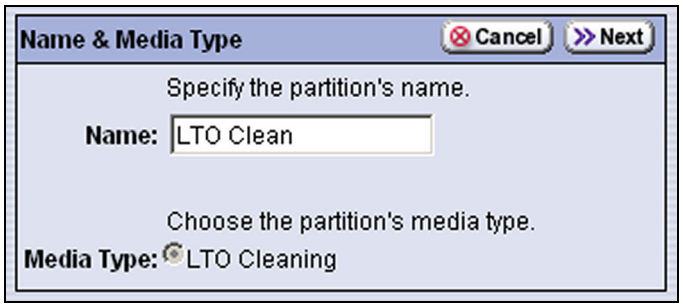


Figure 131 The Name and Media Type screen for a cleaning partition.

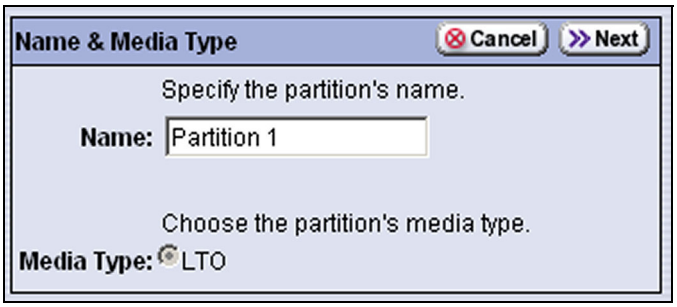


Figure 132 The Name and Media Type screen for a storage partition.

7. The Name & Media Type screen is the beginning of a series of configuration screens. Depending on the type of partition you are modifying, follow the instructions for creating the partition to modify the partition.
   - To modify a cleaning partition, see Creating a Cleaning Partition on page 170,

     —OR—
   - To modify a storage partition, see Creating a Storage Partition on page 174.

   Notes:
   - You cannot change the media type selected for the partition.
   - If you logged into the encryption feature, you can modify the encryption settings for the partition (see Configure Encryption on page 185).

DELETING A PARTITION

Overview When you delete a partition, the drives and slots previously assigned to that partition can be reassigned to an existing partition or used to create a new partition.

Preparation Before deleting an existing partition, make sure you address the following:

- Spectra Logic strongly recommends backing up the library configuration, either to a USB device or as an attachment to an email sent to a previously configured mail recipient, before you delete a partition.
- Make sure that none of the drives in the partition contains a cartridge. If necessary, unload the cartridges from the drives using your storage management software.

- If you plan to delete a storage partition, use your storage management software to eject all of the cartridges from the storage partition to ensure that you do not inadvertently mix cartridges from one storage partition with those from another. After the cartridges are ejected, export them from the library as described in Exporting or Exchanging Cartridges on page 214.

Important After the partition is deleted, any cartridges in the slots that were assigned to the partition are not accessible until the slots are assigned to another partition.

- If you plan to delete a storage partition and it is configured to use Global Spares, edit the partition and deselect all of the drives that are designated as Global Spares for the partition (see Assign a Global Spare Drive on page 179).
- If you plan to delete a storage partition and it is configured to use BlueScale encryption, make sure that you export the BlueScale encryption key for any cartridges that were in the partition (see Exporting and Protecting Encryption Keys on page 314). The encryption key is required if you import the cartridges into another partition in order to access the data on the cartridges at a later date.
- If you plan to delete a cleaning partition, edit any storage partitions that use the cleaning partition to disassociate the cleaning partition from the storage partition (see Allocate Slots and Drives on page 180).

Auto Configuration Save When you delete a partition, the library automatically generates a configuration backup file and saves it to the memory card in the LCM. If you configured the email option for the Auto Configuration Save file, an email with the backup file as an attachment is sent to the specified recipient (see Email Auto Configuration Save on page 111).

Note: Do not use the default autosupport@spectralogic.com email recipient. Spectra Logic does not save emailed configuration files unless they are specifically requested for troubleshooting.

Delete a Partition Use the following steps to delete an existing partition.

1. Log in as a user with superuser or administrator privileges.
2. If you want to save the updated library configuration to a USB device, connect it to a USB port on the LCM (see Connect a USB Device to the Library on page 153) and allow time for the device to mount before continuing.

3. Select **Maintenance ···⁘ MLM** to display the Media Lifecycle Management Tools screen. If Media Auto Discovery, PreScan, or PostScan is running (as indicated by the presence of a **Stop Discovery** or **Pause PostScan** button, respectively), do the following:
   - Click **Stop Discovery** to temporarily stop Media Auto Discovery or PreScan (see Figure 163 on page 252).
   - Click **Pause PostScan** to pause the PostScan for one hour (see Figure 168 on page 261).
4. If you configured the partition to use BlueScale encryption, log into the encryption feature (see Configuring BlueScale Key Management on page 310).
5. Select **Configuration ···⁘ Partitions** to display the Partitions screen.

Figure 133 Click **Delete** for the partition you want to remove.

6. Click **Delete** for the partition you want to delete. A Confirmation screen displays.

7. Select whether you want to save the current library configuration.
   - **Don't Save Library Configuration** — A backup of the changed library configuration is not saved.
   - **Save Library Configuration To** (highly recommended) — Saves a backup file of the changed library configuration to either a USB device connected to the LCM or as an attachment to an email sent to a previously configured recipient (see Configure Mail Users on page 107). Using this option is highly recommended to ensure that you can easily restore the library configuration if necessary.
8. Click **Yes** to confirm that you want to delete the partition or click **No** to return to the Partitions screen without deleting the partition.

   After you click **Yes**, the library updates the configuration. When complete, the Partitions screen displays. The deleted partition is no longer listed.

CHAPTER 7

Using Cartridges in the Library

This chapter describes importing, exporting, and moving cartridges in the library. See Chapter 8 – Configuring and Using Media Lifecycle Management, beginning on page 233 for information about using MLM to manage the cartridges in the library.

UNDERSTANDING CARTRIDGE IMPORT AND EXPORT

Importing cartridges into the library and exporting cartridges from the library are the primary interactions you have with the physical library. You load cartridges into the library for your initial setup, and both load and unload cartridges for normal day-to-day backup operations.

Operation Variables

Using the BlueScale Web Interface The import and export options are not available when you access the library using a remote connection to the BlueScale web interface (RLC). Import and export operations are always performed from the local BlueScale user interface on the library operator panel.

Important You must be physically present at the library to import or export cartridges.

Imports Importing cartridges into the library cannot be controlled by the storage management software. All cartridges imported are controlled using the BlueScale user interface from the library's operator panel. Cartridges are imported either one at a time using the access port or as a group using the bulk load process.

After you finish importing the cartridges, you must then synchronize the library's inventory with the inventory maintained by the storage management software, since those cartridges were moved into the library outside of the storage management software's control.

Exports and the Entry/Exit Mode Cartridge exports are typically initiated by the storage management software ejecting the cartridges from the library. The export process is completed by physically removing the cartridges from the library under the control of the BlueScale software.

The library supports two Entry/Exit operation modes when a data cartridge is ejected from the library by the storage management software: Standard mode and Queued Ejects mode. The mode used is determined by the partition configuration and affects when cartridges ejected by the storage management software are moved to the E/E slot. See Entry/Exit Operation Modes on page 162 for an explanation of the how the Entry/Exit modes function.

In addition to exports performed under control of the storage management software, you can export cartridges using the BlueScale user interface from the library's operator panel. You can export single cartridges one at a time using the access port or you can export multiple cartridges in one operation using the bulk unload process.

Note: You can also exchange cartridges instead of removing them.

Cartridge Inventory Maintained by the Library The slots in the library are scanned during library initialization to determine the current cartridge inventory. The inventory is stored in volatile memory and is maintained as long as the library is powered on. The cartridge inventory is actively updated as cartridges are moved within the library and when cartridges are imported into and exported from the library. However, the inventory maintained by the storage management software may not be automatically updated when the physical inventory changes. Check with your storage management software vendor for proper import/export operations.

Requirements and Restrictions

User Privilege Requirements Any user with operator privileges who is assigned to the partition and all users with superuser or administrator privileges can perform import, export, or exchange operations. See Specify the Partition Users on page 186 for information about assigning users to a partition.

Background Operations You cannot import, export, or exchange cartridges if the library is actively running a background operation such as Media Auto Discovery, PreScan, or PostScan.

If you do not want to wait for a PreScan or PostScan operation to complete, you can stop the PreScan operation or pause the PostScan operation. For background operations other than PreScan or PostScan, you must wait for the process to complete.

- Click **Stop Discovery** on the Media Lifecycle Management Tools screen to stop the PreScan operation (see Stop the Discovery Process on page 252).
- Click **Pause PostScan** on the Media Lifecycle Management Tools screen to pause the PostScan operation for one hour (see Pause the PostScan Process on page 261).

Preparing Cartridges for Use

This section provides guidelines for using data and cleaning cartridges in the library and instructions for preparing the cartridges for use before you import them into the library.

Cartridge Guidelines and Requirements

When preparing cartridges for use, keep the following guidelines and requirements in mind:

Spectra Certified Media For best performance, use Spectra Certified Media (both data and cleaning cartridges). Spectra certification guarantees both media compatibility and the cartridge itself over its lifetime. Using Spectra Certified Media also lets you take full advantage of the library's Media Lifecycle Management (MLM) features. See Chapter 8 – Configuring and Using Media Lifecycle Management, beginning on page 233 for detailed information about using MLM to monitor the health of data and cleaning cartridges.

Multiple Tape Technology Generations When using multiple tape technology generations, Spectra Logic strongly recommends configuring separate partitions for each generation. It is especially important to keep LTO-4 drives and data cartridges separated from LTO-5 and later generation drives and data cartridges. This ensures the accuracy of the LTO-4 media health data (see MLM Health Reports on page 235 for more information).

Barcode Labels To ensure that the library can properly maintain its media inventory, make sure that all cartridges have unique barcode labels. For your convenience, all Spectra Certified Media is available pre-labeled with sequential barcode labels. Optional custom barcode sequences can be ordered, if desired. See Media and Accessories on page 494 for information about purchasing barcode labels.

- **Data cartridges**—The library automatically notifies you whenever you attempt to import unlabeled cartridges or cartridges whose labels indicate that the LTO generation is not supported by the partition.
- **Cleaning cartridges**—If you plan to use a cleaning partition and the Auto Drive Clean feature, the cleaning cartridges must be identified with "CLN" at the beginning of the barcode sequence on their labels. This requirement applies to both standard and custom barcode labels. The library does not import cartridges into a cleaning partition if they not identified with "CLN" at the beginning of the barcode sequence on their labels.

  If you plan to store cleaning cartridges in a storage partition, label the cartridges as required by your storage management software to prevent the software from attempting to read data from or write data to a cleaning cartridge.

Write Protection Before loading data cartridges into the library, make sure that the write-protect switch is properly set. For normal backup operations, the write-protect switch is set to the write-enabled or unlocked position. The write-protect switch is typically set to the write-protect or locked position when the cartridge is removed from the library for storage and during data restore operations.

Support for LTFS for LTO-5 Data Cartridges LTO-5 and later generation drives support a tape format called Linear Tape File System (LTFS).

LTFS uses an area in the LTO-5 cartridge MAM (Medium Auxiliary Memory) that was previously used for MLM data. When running BlueScale12.0.3 or later, the library moves the MLM data to a protected area of the MAM the first time an LTO-5 data cartridge is loaded into an LTO-5 drive using firmware version B6W1 or later.

If you plan to reformat your LTO-5 data cartridges to use LTFS, do the following to ensure that the MLM data is moved to its new location **before** you reformat the cartridges.

1. Make sure that the library is using BlueScale12.0.3 or later and your LTO-5 drives are using firmware version B6W1 or later.
2. After meeting these requirements, load and then unload each cartridge into the updated LTO-5 drives to move the MLM data. This load/unload process automatically moves the MLM data to the new location on the cartridge MAM.

Important

The library must be using BlueScale12.0.3 or later and the LTO-5 drives must be using firmware version B6W1 or later in order to move the MLM data to the new location on the cartridge MAM.

If you reformat LTO-5 data cartridges to use LTFS in a library using an earlier version of the BlueScale software or if you reformat the cartridges before you load and unloaded them from a drive to move the MLM data, the MLM data for the cartridge is lost. The cartridges are subsequently treated as non-MLM-enabled.

Important

When an LTO-5 drive is running a firmware version earlier than B6W1, it can only access the MLM data at the old MAM location. The BlueScale software does not attempt to move the MLM data; it continues to use the old location for the MLM data. If the cartridge is reformatted to use LTFS without moving the data to the new location, the MLM data for the cartridge is lost.

Important

If the BlueScale software already moved the MLM data, the cartridge appears to be non-MLM enabled when loaded into a drive that is using down-level firmware. The MLM data is not updated.

To ensure full MLM tracking of your LTO-5 data cartridges, make sure that the library is using BlueScale12.0.3 or later and that all LTO-5 drives are using firmware version B6W1 or later.

Prepare the Cartridges for Use

Use the following steps to prepare the individual cartridges to be loaded into the library.

1. If your cartridges are unlabeled, prepare and affix a barcode label to each cartridge. Position each label in the indented area on the cartridge, as illustrated in Figure 134. See Barcode Label Specifications for Half-Inch Media on page 514 for detailed information about barcode labels.

Caution Do not place labels on any surface of the cartridge except the area shown in Figure 134. A label can become dislodged and damage the drive.

Important Before importing cartridges into the library, allow them to acclimate to the ambient temperature and humidity for 24 hours.

Important When used in a cleaning partition, all cleaning cartridges must be identified with "CLN" at the beginning of the barcode sequence on their labels. This requirement applies to both standard and custom barcode labels.

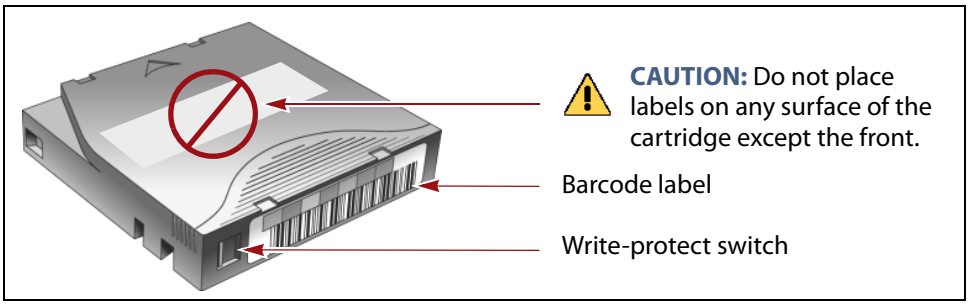


Figure 134 Attach barcode labels to cartridges and check write-protect switch setting.

2. Depending on whether you plan to write data to a cartridge or restore data from a cartridge, make sure the write-protect switch on the cartridge is set for the desired operation.

   Note: Cleaning cartridges do not have a write-protect switch.

If the switch...	The cartridge is...
Does not cover the opening	Write-enabled. Data can be written to, read from, or erased from the tape.
Covers the opening	Write-protected. Data can be read from the tape. Data cannot be written to or erased from the tape.

LTO-7 Type M Media

When the library loads an unused LTO-7 tape cartridge with a barcode label ending with "M8" into an LTO-8 tape drive using firmware HB82 or later, the drive attempts to initialize the tape for LTO-7 type M density, increasing the density from 6 TB to 9 TB. Once initialized, the tape can no longer be written to, or read by, an LTO-7 drive.

To use the LTO-7 type M feature, make sure that your tape library uses the default barcode reporting configuration or a configuration that reports the last two characters, not including the checksum. See Configure Barcode Reporting on page 126 for details of the default barcode reporting configuration and instructions for changing the barcode configuration.

If the tape drive determines that the tape cartridge does not meet the unused criteria, the LTO-7 type M initialization fails and the tape retains LTO-7 density. If the library or your storage management software reports an LTO-7 type M initialization failure, Spectra Logic recommends replacing the barcode on the tape with an L7 barcode.

Note: M8 tapes cannot be read by or written to by LTO-9 drives.

LTO-9 New Media Optimization

With its increased density, LTO-9 media require a one-time initialization process to optimize data placement for each new cartridge before it is used for writing data. The media optimization process takes place automatically on the first load of a new LTO-9 cartridge in an LTO-9 tape drive. The process typically takes between 40 and 60 minutes, but can take up to 2 hours. All Spectra Certified LTO-9 media is initialized before it ships and does not need to go through this optimization process.

Important After the LTO-9 new media initialization starts on a non-Spectra Certified tape, using the front panel to move the tape from the drive aborts the initialization process, requiring the drive to go through mid-tape recovery. The next time the tape is moved to a drive, the initialization process starts over.

Important All Spectra Certified LTO-9 media is initialized before it ships and does not need to go through the optimization process.

IMPORTING CARTRIDGES

This section describes how to import cartridges into the library.

Import Overview

When importing cartridges into the library, keep in mind the information in the following sections.

Import Requirements

Partitions You must have one or more partitions defined before you can import cartridges into the library. Chapter 6 – Configuring and Managing Partitions, beginning on page 159 provides detailed instructions for creating partitions.

Make sure that the partition has sufficient empty slots available to accommodate the cartridges you plan to import. The partition's Import/Export screen shows the number of empty slots available (see Figure 140 on page 212). If there are no empty slots available in the partition, export one or more cartridges from the partition (see Exporting or Exchanging Cartridges on page 214).

Capacity Expansion Slots If you are using the capacity expansion slots, you must import cartridges into those slots as described in Import Individual Cartridges on page 212. You cannot bulk-load these slots.

Cartridge Labeling Make sure that each data and cleaning cartridge is labeled with a unique barcode (see Prepare the Cartridges for Use on page 202).

Cleaning Partition When importing cleaning cartridges into a cleaning partition, keep the following in mind:

- The cleaning cartridges in a cleaning partition can only be used for drives in a storage partition that is configured to use that cleaning partition. Associating a cleaning partition with the drives in a storage partition automatically enables the Auto Drive Clean feature for that partition (see Allocate Slots and Drives on page 180).
- The cleaning cartridges in the cleaning partition are inaccessible to the application software running on the host. Make sure that you disable any software-based drive cleaning to prevent repeated requests to import a cleaning cartridge.
- If your storage management software supports automated drive cleaning and you plan to use this method to clean the drives instead of the library's Auto Drive Clean feature, refer to your software documentation for instructions. You must import the properly labeled cleaning cartridges into the storage partition.

Auto Discovery Media Auto Discovery and PreScan are background operations that use the drives in a partition to discover newly imported LTO cartridges and add them to the MLM database. The discovery process cannot begin while the hosts are actively loading cartridges into or unloading cartridges from the drives. If you import cartridges during this time, the library posts a failure message stating that no drives are available to perform the discovery process.

Either wait until the library is idle before beginning the import or manually start the discovery process for imported cartridges when the library is idle. See Initiate Media Discovery Manually on page 250 for instructions.

Additional Requirements and Restrictions See Understanding Cartridge Import and Export on page 198 for additional requirements and restrictions when importing cartridges.

Import Options

The method you use to import cartridges depends on whether you are importing individual cartridges into the library as part of day-to-day operations or you are loading cartridges into the library for the first time following installation.

Bulk Load (Initial Loading of Cartridges) Spectra Logic recommends that you only use the Bulk Load option when you are loading cartridges into the library as part of the initial installation process.

- When you first install your library and load cartridges for use, you may prefer to use the Bulk Load option to save time.
- Using the Bulk Load option has an associated risk of inventory corruption if you previously imported cartridges, defined your partitions, and are using the library with MLM enabled.

See Import Multiple Cartridges Using Bulk Load on page 206 for a detailed description of how to load cartridges into the library using this option.

Single Cartridge Import (Day-to-Day Operations) For normal day-to-day operation, individual cartridges are imported manually using the access port. You can import as many cartridges as needed using this option. See Import Individual Cartridges on page 212.

Import Multiple Cartridges Using Bulk Load

Spectra Logic recommends that you only use the Bulk Load option when you are loading data cartridges into a single-partition library as part of the initial installation process.

If you select to use the Bulk Load option when the library is configured with multiple partitions, make a list of the barcode label information for each cartridge before beginning the Bulk Load. After completing the Bulk Load operation, use the Inventory screen to check the cartridge barcodes for each partition. You may need to export and reimport cartridges that end up in the wrong partition.

Caution

If you use the Bulk Load option when you have multiple partitions configured in the library, cartridges may end up in the wrong partition since you may not know which physical slots are assigned to each partition. Importing cartridges into the wrong partition and then writing data to the them risks mixing data sets that you intended to keep separate.

As an additional consideration, keep in mind that cartridges added using Bulk Load are not automatically added to the MLM database. They must be discovered, either manually or as part of the normal load/unload process, before they can be tracked by MLM. See Add Cartridges to the MLM Database on page 247 for information about the discovery process.

1. Prepare the cartridges as described in Preparing Cartridges for Use on page 199.
2. From the operator panel, log into the library as a user with the appropriate privileges (see User Privilege Requirements on page 199).

3. Click **MENU**, then select **General** ⋯⁘ **Import/Export**. The Import/Export screen displays showing information for the last partition that was viewed on either the Import/Export screen or the Inventory screen.
4. Select the partition you want to use from the drop-down list, then click **Go**. The Import/Export screen refreshes to show the current status of the slots assigned to the selected partition.

   Note: If the library only has one partition configured, the Import/Export screen shows that partition and does not include a drop-down list.

Figure 135 Select the partition and then click **Bulk Load**.

Note: If there are no empty slots in the partition, the **Bulk Load** button is not present.

5. Click **Bulk Load**. The library automatically releases the locks on the two magazines on the left side of the library and then displays the following feedback message.

Important Do not respond to the feedback message until **after** you load the cartridges into the magazines and push them back into place.

Note: If all of the slots in the left-side magazines are full, push the magazines back into place and click **Continue** to unlock the right-side magazines. The process for loading the cartridges into the right-side magazines is the same as for the left-side magazines (see Step 7 on page 211).

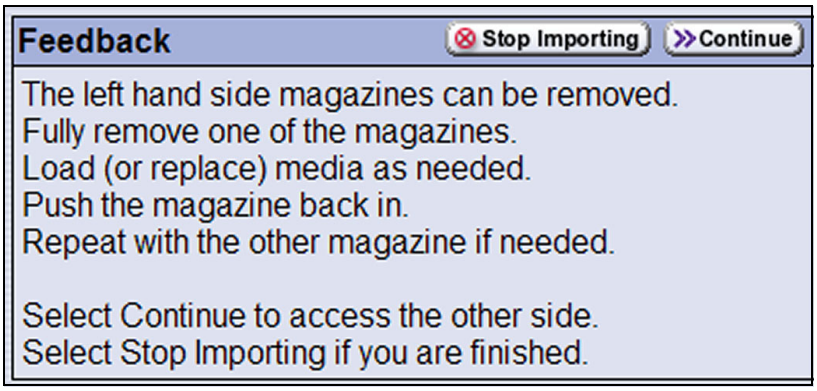


Figure 136 Do not click **Continue** until **after** you load the magazines on the left side of the library.

6. Load the cartridges into the left-side magazines.

Important You must load the cartridges, reinsert the magazines, and press the feedback button on the front screen within ten minutes after you click **Bulk Load**.

a. Remove one or both of the left-side magazines by grasping the handle and pulling straight out from the library.

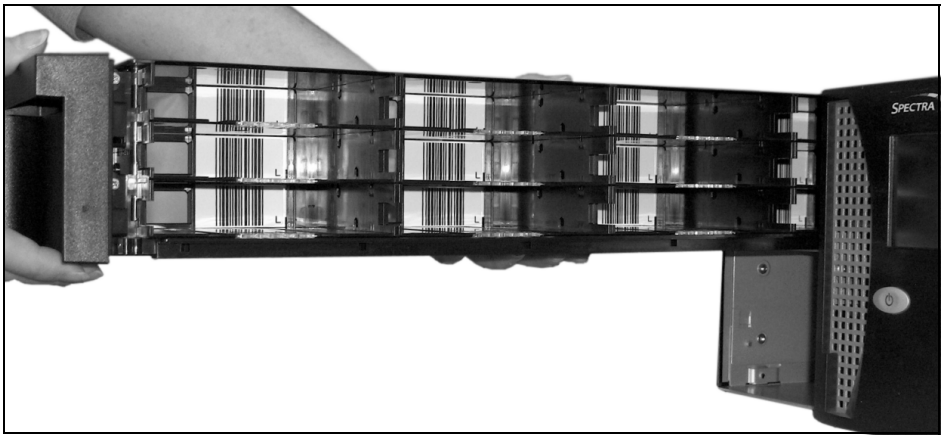
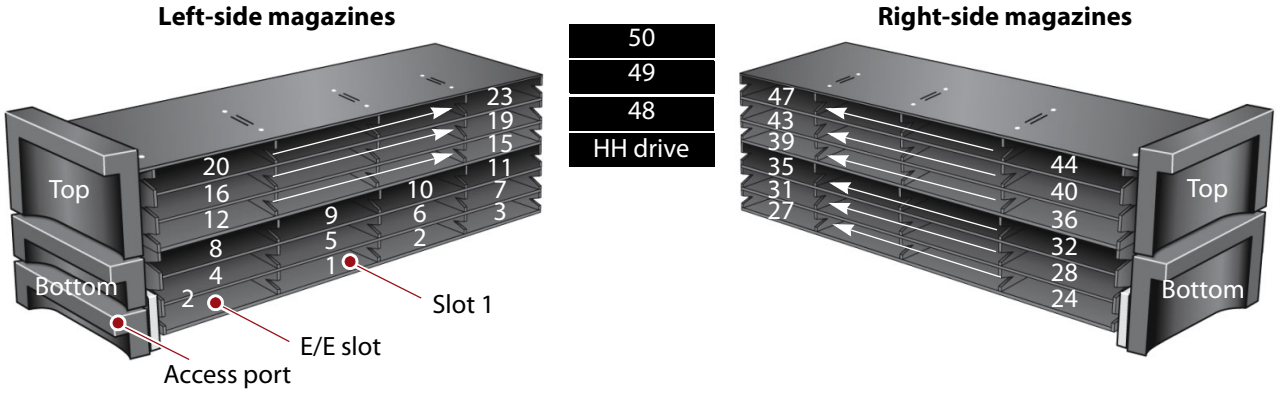


Figure 137 Remove the magazines from the library.

b. Insert the cartridges smooth-side up and with the barcode labels facing out. Push the cartridge into the slot until the latch on the slot engages the ridges on the cartridge.

Important The slots are keyed to only accept correctly oriented cartridges. Do not force the cartridges into the slots.



Important:

- Load the cartridges beginning at slot 1, and continuing sequentially.
- Do not insert a cartridge in the E/E slot.
- Make sure that you reinsert the magazines in their original locations to prevent the access port from becoming unusable.
- Capacity expansion slots, if present, must be loaded individually using the access port.

Figure 138 Load cartridges into the magazines.

Load the cartridges into the magazines sequentially based on your capacity license, as follows:

- Bottom left magazine: Slots 1 through 11
- Top left magazine: Slots 12 through 23

Note: When loading cartridges into the magazines, the slots you use depends on your capacity license. Do not insert cartridges in slots outside the locations licensed by your CoD capacity license; they are not accessible by the library or your storage management software. Figure 138 on page 209 shows the slot numbering.

For example, if your capacity license enables 10 slots, only insert cartridges in slots 1 through 10. Do not insert cartridges in the other slots.

c. Carefully reinsert the magazines back into their original locations in the library.

Caution A fully loaded magazine weighs several pounds. Use both hands when lifting the magazine and sliding it into the library.

Important Make sure that you reinsert the magazines back into their original locations to prevent the access port from becoming unusable.

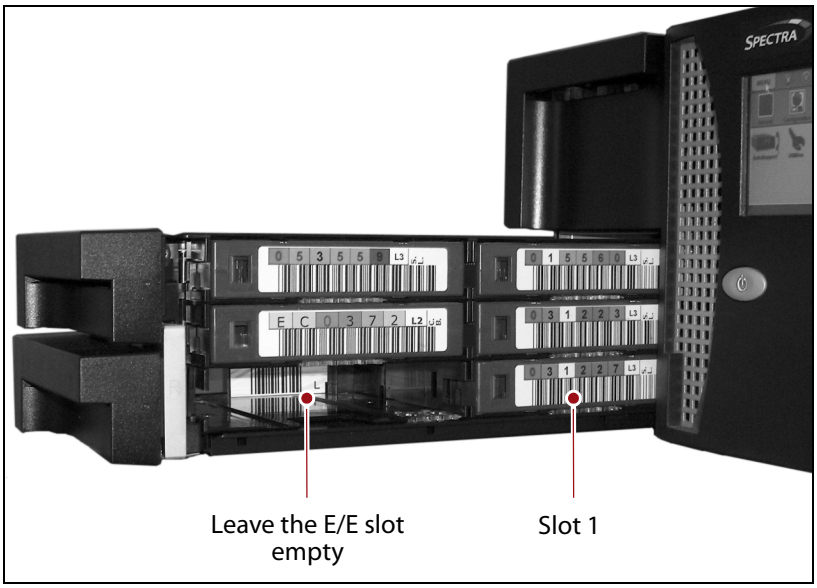


Figure 139 Slide the filled magazines into the library.

7. Return to the operator panel and select the appropriate option on the Feedback Required screen.

Important You must load the cartridges, reinsert the magazines, and press the feedback button on the front screen within ten minutes after you click **Bulk Load**. If you wait more than 10 minutes to respond, the library times out and displays a message about the timeout on the operator panel. Repeat the Bulk Load process.

Select...	If...
Continue	Your capacity license allows for more than 23 slots. Load cartridges into the magazines on the right-hand side of the library using the following steps: **1.** Remove one or both of the right-side magazines and insert the cartridges smooth-side up and with the barcode labels facing out (see Step 6 on page 208). Load the cartridges into the magazines sequentially based on your capacity license, as follows: ▪ Bottom right magazine: Slots 24 through 35 ▪ Top right magazine: Slots 36 through 47 **2.** Carefully reinsert the magazines back into their original locations in the library. **3.** Return to the operator panel and click **Stop Importing** on the Feedback Required screen. The library locks all of the magazines and performs an inventory of the magazines that were unlocked.
Stop Importing	You do not have any more cartridges to load. The library locks all of the magazines and performs an inventory of the magazines that were unlocked.

8. Use your storage management software to update the cartridge inventory it maintains (see Updating the Software Media Inventory on page 232).

Important After bulk loading cartridges, you must use your storage management software to update the inventory it maintains in order for the software to use the cartridges.

Import Individual Cartridges

For normal day-to-day operation, import individual cartridges using the access port.

Note: The following steps describe importing a cartridge beginning from the Import/Export screen. This method requires you to open the access port and insert the cartridge as described in this section and then go to the Inventory screen to create a move queue to move the cartridge from the E/E slot to a slot in the partition.

A more straightforward method is to start with the Inventory screen and create a move queue that moves one or more cartridges from the access port to specific slots in the partition (see Move Cartridges Within a Partition on page 226).

1. Prepare the cartridges as described in Preparing Cartridges for Use on page 199.
2. From the operator panel, log into the library as a user with the appropriate privileges (see User Privilege Requirements on page 199).
3. Click **MENU**, then select **General** ⋯⁘ **Import/Export**. The Import/Export screen displays showing information for the last partition that was viewed on either the Import/Export screen or the Inventory screen.
4. Select the partition you want to use from the drop-down list, then click **Go**. The Import/Export screen refreshes to show the current status of the slots assigned to the selected partition.

   Note: If the library only has one partition configured, the Import/Export screen shows that partition and does not include a drop-down list.

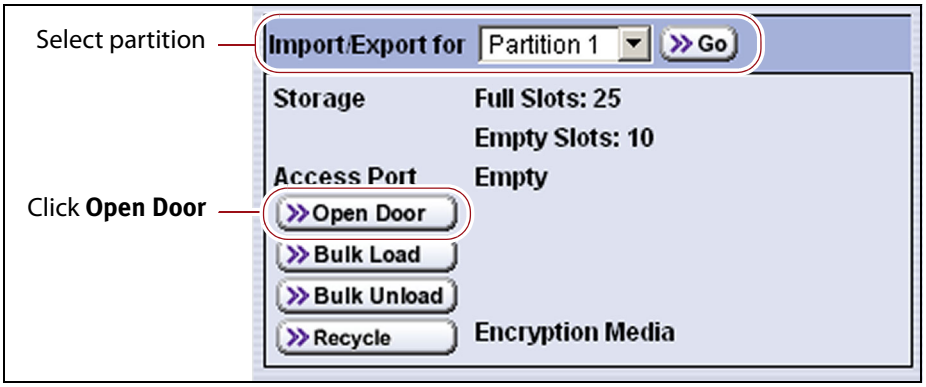


Figure 140 Select the partition and then click **Open Door** to open the access port.

5. Click **Open Door**. A progress screen displays describing the process.

6. When the access port opens, insert the cartridge into the E/E slot, smooth side up and with the barcode label facing out. Push the cartridge into the slot until the latch on the slot engages the ridges on the cartridge.

Important The slot is keyed to only accept a correctly oriented cartridge. Do not force the cartridge into the slot.

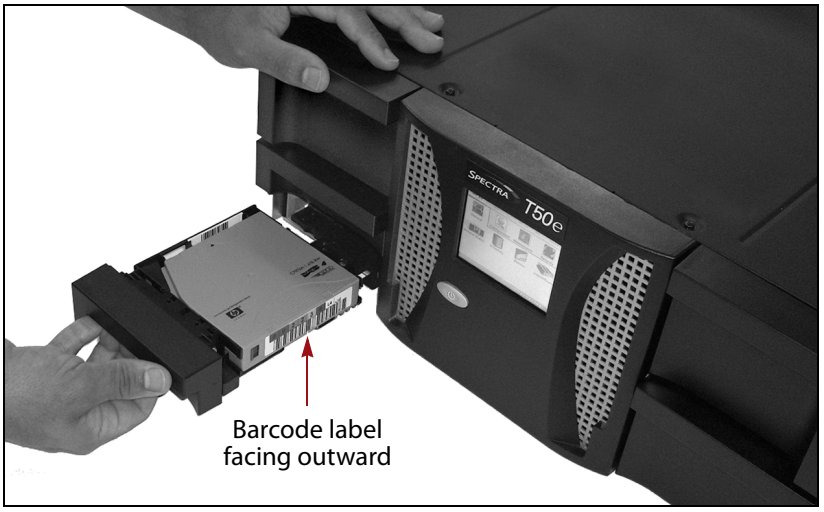


Figure 141 Insert the cartridge into the E/E slot.

7. Wait for a message prompting you to close the access port.
8. Gently push the access port closed.

Important Do not use force to push the access port closed, and do not close the door before you are prompted to do so.

The library scans the cartridge barcode label and updates its cartridge inventory to indicate that the imported cartridge is in the E/E slot.

9. Click **MENU**, then select **General** ···⁘ **Inventory**. The Inventory screen displays showing the imported cartridge in the EE slot.

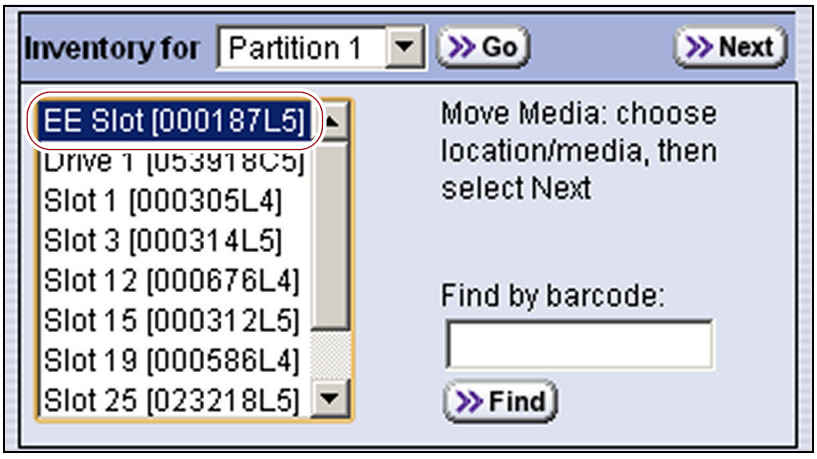


Figure 142 Select the cartridge in the EE slot.

10. Select the cartridge in the EE slot and create a move queue to move the cartridge to the desired slot in the partition (see Move Cartridges Within a Partition on page 226).
11. Use your storage management software to update the library inventory it maintains (see Updating the Software Media Inventory on page 232).

Important After importing cartridges you must use your storage management software to update the inventory it maintains in order for the software to use the cartridges.

EXPORTING OR EXCHANGING CARTRIDGES

This section provides instructions for exporting or exchanging cartridges in a partition.

Note: If you want to export or exchange a specific cartridge, see Export or Exchange Cartridges Individually on page 217.

Overview of the Export and Exchange Processes

During normal operations, data cartridges are typically ejected from the library using your storage management software and then removed from the library using the access port. This process ensures that the data cartridge inventory maintained by the storage management software is accurate.

Process Queued Ejects versus Individual Ejection The method used for exporting or exchanging cartridges depends on the Entry/Exit mode used by the library (see Entry/Exit Operation Modes on page 162 for detailed information about how the two modes operate) and whether the storage management software has queued cartridges to be ejected.

- If the library uses Queued Ejects mode and the storage management software has queued cartridges for ejection, use Export or Exchange Cartridges Using Queued Ejects on page 215.
- If the library uses Standard eject mode or you will manually move cartridges to the E/E slot for ejection, use Export or Exchange Cartridges Individually on page 217.

Export Process The *export* process physically removes cartridges from the library. The exported cartridges are not replaced by new cartridges.

Exchange Process The *exchange* process operates the same way as the export process, except that you replace the cartridge in the E/E slot with another one. Exchanging cartridges is especially useful when there are no open slots in the partition and you need to temporarily import a cleaning cartridge into a storage partition to clean a drive when you are not using the Auto Drive Clean feature.

Prepare to Export or Exchange Cartridges

Requirements See Understanding Cartridge Import and Export on page 198 for information about requirements and restrictions when exporting or exchanging cartridges.

Preparation If you are exchanging cartridges, prepare the cartridges as described in Preparing Cartridges for Use on page 199.

Export or Exchange Cartridges Using Queued Ejects

Important When the library is configured to use Queued Ejects mode, you **must** use the access port to export or exchange cartridges. Do not use the Bulk Unload option unless you are removing all of the cartridges from the library. When looking at the magazines you cannot tell which cartridges are queued for removal unless you examine the barcode label on each cartridge and compare it to a list of barcodes for the cartridges you want to remove.

1. Use your storage management software to eject cartridges from the library. You can eject as many cartridges as desired.

   Note: If you have multiple partitions configured, you must eject the cartridges from each partition separately.

   The eject process removes the cartridges from the cartridge inventory maintained by the storage management software. The library makes the cartridges inaccessible to the software; from the software's perspective the cartridges were removed from the library. However, the cartridges remain in the library until you export or exchange them using the BlueScale user interface.

2. From the operator panel, log into the library as a user with the appropriate privileges (see User Privilege Requirements on page 199).

3. Click **MENU**, then select **General ···⁘ Inventory**. The Inventory screen displays showing the information for the last partition that was viewed on either the Import/Export screen or the Inventory screen.

4. Select the partition you want to use from the drop-down list, then click **Go**. The Inventory screen refreshes to show the cartridge inventory for the selected partition.

   Notes:
   - If the library only has one partition configured, the Inventory screen shows that partition and does not include a drop-down list.
   - The cartridges that were ejected by the storage management software are indicated by an asterisk in the Inventory screen, as shown in Figure 143.

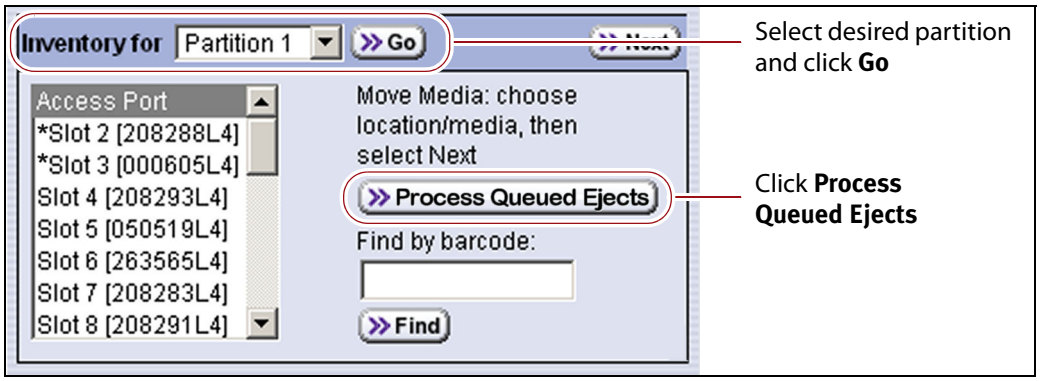


Figure 143 Select the partition and then click **Process Queued Ejects** to begin exporting the ejected cartridges from the library.

5. Click **Process Queued Ejects**.

   The library creates a move queue containing the cartridges to be exported, moves the first cartridge to the E/E slot, and opens the access port.

6. Insert a finger through the opening in the back of the access port and carefully push the cartridge out of the E/E slot.

Caution Be careful not to drop or jar the cartridge when you remove it. Mishandling cartridges can result in failures when you attempt to use the cartridge.

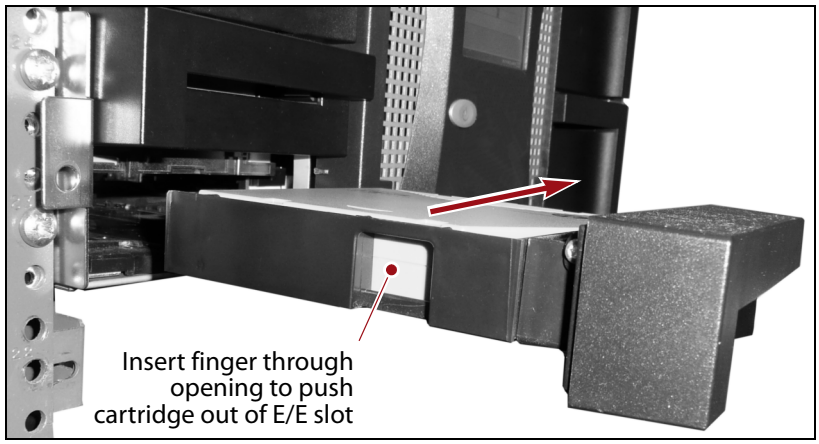


Figure 144 Remove the cartridge from the E/E slot.

7. If you are exchanging a different cartridge for the one you removed, insert the new cartridge in the E/E slot (see Figure 141 on page 213). Push the cartridge into the slot until the latch on the slot engages the ridges on the side of the cartridge.

Important The slot is keyed to only accept a correctly oriented cartridge. Do not force the cartridge into the slot.

8. Wait for a message prompting you to close the access port.
9. Gently push the access port closed.

Important Do not close the door before you are prompted to do so. Do not use force to push the access port closed.

   - If you exchanged cartridges, the library moves the new cartridge to the slot previously occupied by the cartridge you removed.
   - The library then moves the next queued cartridge to the E/E slot and opens the access port.

10. Repeat Step 6 through Step 9 as the library moves each of the queued cartridges to the access port. The process continues until all queued cartridges are exported from the library.

Export or Exchange Cartridges Individually

Cartridges can be exported or exchanged individually, using the BlueScale user interface, after they are moved to the E/E slot either manually or by the storage management software. If the library uses Standard eject mode, when the storage management software ejects a cartridge, the library immediately moves the cartridge to the E/E slot and reports that the eject is complete.

1. Use your storage management software to eject the desired cartridge from the library or manually move a cartridge to the E/E slot (see Move Cartridges Within a Partition on page 226 for instructions).
2. Click **MENU**, then select **General ⋯⁘ Import/Export**. The Import/Export screen displays showing information for the last partition that was viewed on either the Import/Export screen or the Inventory screen.

3. Select the partition you want to use from the drop-down list, then click **Go**. The Import/Export screen refreshes to show the current status of the slots assigned to the selected partition.

   Note: If the library only has one partition configured, the Import/Export screen shows that partition and does not include a drop-down list.

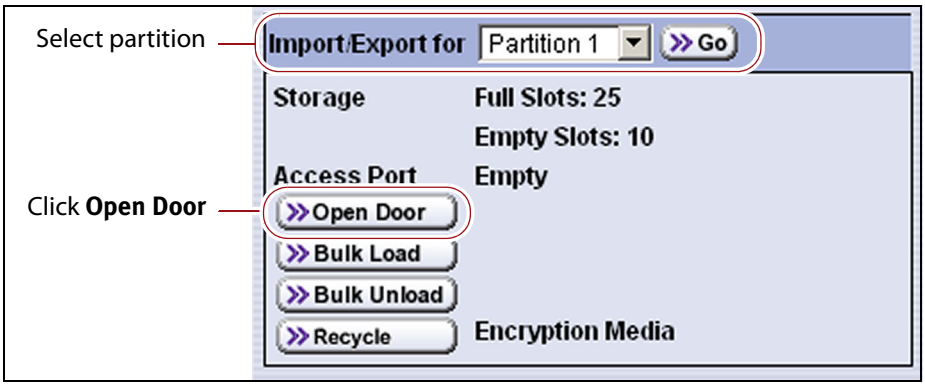


Figure 145 Select the partition and then click **Open Door** to open the access port.

4. Click **Open Door**. A progress screen displays describing the process.
5. Insert a finger through the opening in the back of the access port and carefully push the cartridge out of the E/E slot.

Caution Be careful not to drop or jar the cartridge when you remove it. Mishandling cartridges can result in failures when you attempt to use the cartridge.

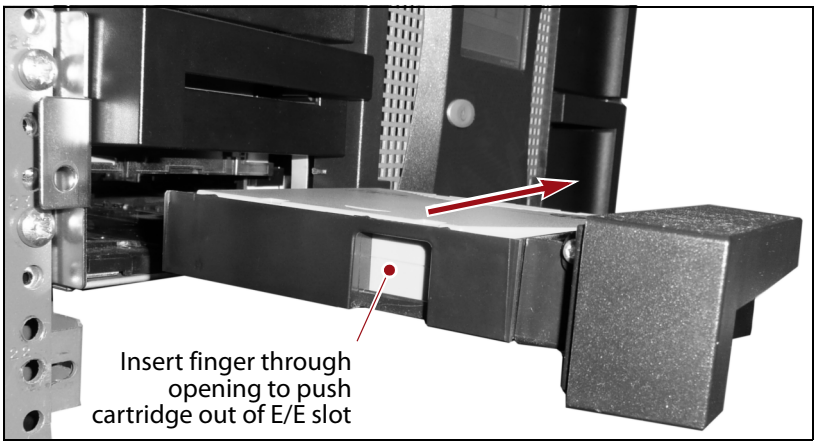


Figure 146 Remove the cartridge from the E/E slot.

6. If you are exchanging a different cartridge for the one you removed, insert the new cartridge in the E/E slot (see Figure 141 on page 213). Push the cartridge into the slot until the latch on the slot engages the ridges on the side of the cartridge.

Important The slot is keyed to only accept a correctly oriented cartridge. Do not force the cartridge into the slot.

7. Wait for a message prompting you to close the access port.
8. Gently push the access port closed. If you exchanged cartridges, the library moves the new cartridge to the slot previously occupied by the cartridge you removed.

Important Do not use force to push the access port closed, and do not close the port before you are prompted to do so.

9. Repeat Step 1 through Step 8 if you need to exchange or export additional cartridges.
10. If the exported tape was manually moved to the E/E port, update your storage management software's inventory as described in Updating the Software Media Inventory on page 232.

Export Cartridges Using Bulk Unload

This section describes how to remove cartridges from the library using the Bulk Unload option. If you are exporting or exchanging cartridges from a partition as part of day-to-day operations, follow the instructions in one of the following sections:

- If the library is configured to use Queued Ejects mode, see Export or Exchange Cartridges Using Queued Ejects on page 215.
- If the library is configured to use Standard mode, seeExport or Exchange Cartridges Individually on page 217.

Important Spectra Logic recommends **only** using the Bulk Unload option when removing all of the cartridges from the library. Cartridges removed from the library using Bulk Unload are not removed from the cartridge inventory maintained by the storage management software. After completing the Bulk Unload, update the inventory maintained by the storage management software (see Updating the Software Media Inventory on page 232).

Important Exporting cartridges using Bulk Unload does not update the MLM database to show that the cartridges are exported. If you are permanently removing the cartridges from the library, you can delete the records from the MLM database, if desired (see Delete MLM Records From the Database on page 275).

Use the following steps to remove all of the cartridges from the library using Bulk Unload.

1. From the operator panel, log into the library as a user with the appropriate privileges (see User Privilege Requirements on page 199).
2. Click **MENU**, then select **General ⋯⁘ Import/Export**. The Import/Export screen displays showing information for the last partition that was viewed on either the Import/Export screen or the Inventory screen.

3. Select the partition you want to use from the drop-down list, then click **Go**. The Import/Export screen refreshes to show the current status of the slots assigned to the selected partition.

   Note: If the library only has one partition configured, the Import/Export screen shows that partition and does not include a drop-down list.

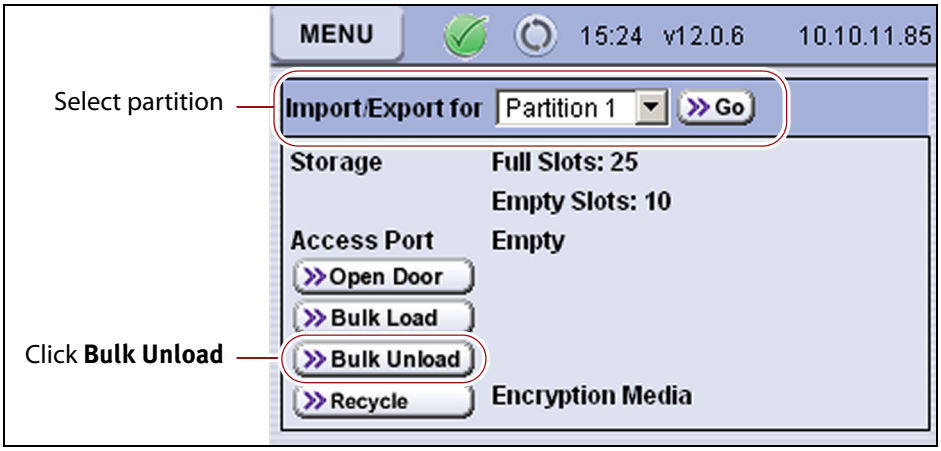


Figure 147 Select the partition and then click **Bulk Unload**.

4. Click **Bulk Unload**. The following feedback message displays.

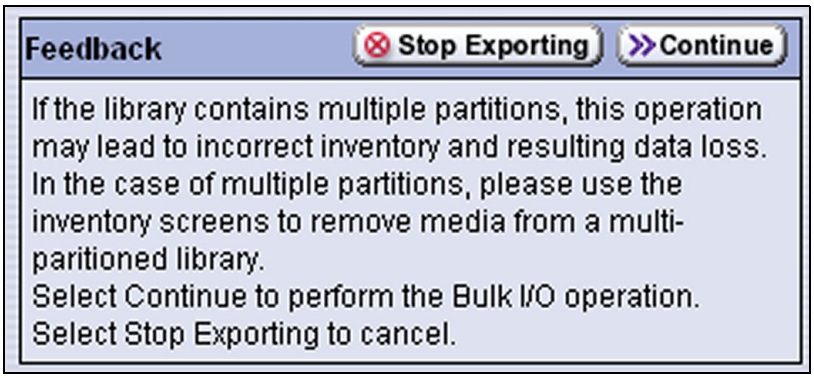


Figure 148 Click **Continue** in response to the Feedback required message.

5. Click **Continue** to unlock the magazines.

6. The library automatically releases the locks on the two magazines on the left side of the library and then displays the following feedback message.

Important Do not respond to the feedback message until **after** you remove the cartridges from the magazines and push the magazines back into place.

Figure 149 Do not click **Continue** until **after** you unload the magazines on the left side of the library.

7. Remove the cartridges from the magazines.

Caution A fully loaded magazine weighs several pounds. Use both hands when lifting a magazine and sliding it out of the library.

Important You must remove the cartridges, reinsert the magazines, and press the feedback button on the front screen within ten minutes after you click **Bulk Unload**. If you wait more than 10 minutes to respond, the library times out and displays a message about the timeout on the operator panel. Repeat the Bulk Unload process.

   a. Remove one or both of the left-side magazines by grasping the handle and pulling the magazine straight out from the library.

b. Insert a finger through the openings in the back of the magazine and carefully push the cartridges out of the slots.

Caution Be careful not to drop or jar the cartridges when you remove them. Mishandling cartridges can result in failures when you attempt to use the cartridge.

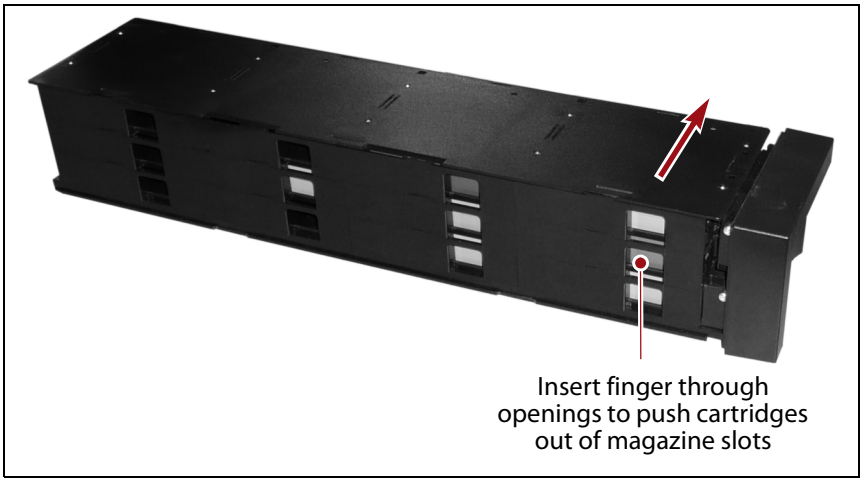


Figure 150 Remove the cartridges from the slots in the magazine.

c. Carefully reinsert the magazines back into their original locations in the library.

Important Make sure that you reinsert the magazines back into their original locations to prevent the access port from becoming unusable.

8. Return to the operator panel and select the appropriate option on the Feedback Required screen.

Important If you wait more than 10 minutes to respond, the library times out and displays a message about the timeout on the operator panel. Repeat the Bulk Unload process.

Select...	If...
Continue	You need to remove cartridges from the magazines on the right-hand side of the library. **1.** Remove one or both of the right-side magazines and remove the cartridges. **2.** Carefully reinsert the magazines back into their original locations in the library. **3.** Return to the operator panel and click **Stop Exporting** on the Feedback Required screen. The library locks all of the magazines and performs an inventory of the magazines that were unlocked.
Stop Exporting	If you do not have any more cartridges to remove. The library locks all of the magazines and performs an inventory of the magazines that were unlocked.

9. Use your storage management software to update the cartridge inventory it maintains (see Updating the Software Media Inventory on page 232).

Important After using Bulk Unload to remove cartridges from the library you must use your storage management software to update the inventory it maintains in order to prevent the software from attempting to use the cartridges.

Understanding the Cartridge Inventory

The library's cartridge inventory is viewed using the Inventory screen on the BlueScale user interface. The inventory is a record of all the cartridges stored in each library partition and their current locations (in a specific slot or in a drive). As cartridges are imported into a partition, the barcode reader on the robotics reads the barcode labels on the individual cartridges. The library uses this barcode information to maintain its physical inventory, which is stored in the library's volatile memory.

Note: Because it is stored in volatile memory, the cartridge inventory is lost when the library is powered off. The library reestablishes the inventory each time it is powered on by scanning all of the slots for cartridges and recording the barcode label information for each cartridge it detects.

Using the Cartridge Inventory

Overview The Inventory screen, which lists all of the cartridges currently stored in the selected partition, is accessed from the General menu. You use the Inventory screen to interact with the cartridge inventory in the following ways:

If you want to...	The Inventory screen lets you...	See...
View information about the cartridges in a partition,	▪ View the barcode label information and locations for cartridges located in a storage partition. ▪ View the barcode label information and locations for cartridges located in a cleaning partition. ▪ Identify expired cleaning cartridges. An * (asterisk) appears next to the slot number if the cleaning cartridge is expired.	View the Cartridge Inventory for a Partition on page 224
Locate a specific cartridge in the partition,	Search for a cartridge in a partition using its barcode label information.	Locate a Specific Cartridge on page 225

If you want to...	The Inventory screen lets you...	See...
Move a cartridge from one location to another within a partition,	Create a move queue to: ▪ Move a cartridge that was imported using the access port, from the E/E slot to an empty slot in the partition. ▪ Move one or more specific cartridges from their current locations to different locations. ▪ Move a specific cartridge to the E/E slot so that it can be removed from the library. ▪ Move a cleaning cartridge stored in a storage partition to a drive as part of a manual cleaning operation when the Auto Drive Clean feature is not configured for the partition. ▪ Move an expired cleaning cartridge to the E/E slot so that it can be exchanged for a new one.	Move Cartridges Within a Partition on page 226

User Privilege Requirements Any user with operator privileges who is assigned to the partition and all users with superuser or administrator privileges can access and use the Inventory screen. See Specify the Partition Users on page 186 for information about assigning users to a partition.

View the Cartridge Inventory for a Partition

Note: You can also view the cartridge inventory for a partition using the Media Lifecycle Management Report screen (see Using MLM Reporting on page 262).

1. From the operator panel, log into the library as a user with the appropriate privileges (see User Privilege Requirements, above).
2. Click **MENU**, then select **General ⋯⁘ Inventory**. The Inventory screen displays, showing the information for the last partition that was viewed on either the Import/Export screen or the Inventory screen.

3. Select the partition for which you want to view the inventory from the **Partition** drop-down list, then click **Go**. The screen refreshes to show the cartridge inventory for the selected partition.

Notes:
- If the library only has one partition configured, the Inventory screen shows that partition and does not include a drop-down list.
- The access port only appears in the cartridge inventory when you are accessing the Inventory screen from the operator panel.
- With the exception of the access port, only those slots that contain a cartridge are listed.

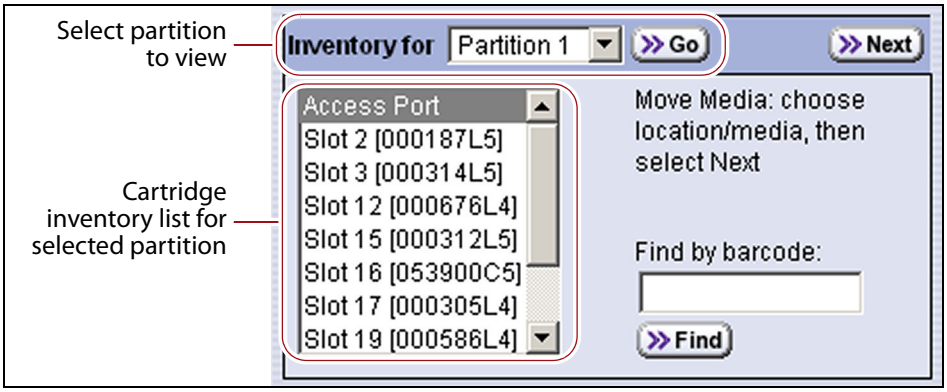


Figure 151 Use the Inventory screen to view the cartridge inventory for a partition.

Locate a Specific Cartridge

The Inventory screen provides two different methods for locating a specific cartridge in the library.

1. From the operator panel, log into the library as a user with the appropriate privileges (see User Privilege Requirements on page 224).
2. Display the cartridge inventory for the desired partition (see View the Cartridge Inventory for a Partition on page 224).

3. Locate the desired cartridge using one of the following methods.

To locate by...	Do the following...
Viewing the cartridge inventory list,	1. Scroll through the list until you find the slot number or barcode for the desired cartridge. 2. Click the barcode to select the cartridge. **Important:** Only the slots below the top one displayed in the list are searched. Scroll to the top of the source list before clicking **Find**. The search starts at the second visible slot.
Searching for a specific barcode,	1. Enter the barcode label information for the cartridge you want to locate in the **Find by Barcode** field. 2. Click **Find**. The cartridge inventory list refreshes to show the requested cartridge highlighted at the top of the list. 3. Click the barcode to select the cartridge. **Important:** Only the slots below the top one displayed in the list are searched. Scroll to the top of the source list before clicking **Find**. The search starts at the second visible slot.

Move Cartridges Within a Partition

Overview During normal operations, you typically use your storage management software to move cartridges from one location to another within the library. However, you may occasionally need to use the library's BlueScale interface to move an individual cartridge from one location to another inside the library without using the your storage management software (for example, to move a cleaning cartridge stored in the storage partition to a drive if you are not using the Auto Drive Clean option). These types of moves are performed using a move queue that is configured through the Inventory screen.

Important You cannot use the Inventory screen to move a cleaning cartridge in a cleaning partition to a drive in a storage partition. Instead, use the **Clean** button on the Drives screen (see Manually Cleaning a Drive on page 446).

Move queue A move queue is a list of one or more source/destination pairs, with each pair representing a single move operation. All moves performed using the Inventory screen require creating a move queue that specifies the source and destination for each cartridge move.

Note: The maximum number of moves that can be configured in a single move queue is 100 source/destination pairs.

Using the Access Port as the move source or destination Moving a cartridge to or from the access port opens the access port as part of the move. Each move requires you to physically close the access port to complete the move and begin processing the next move. For this reason, the **Access Port** option is only available as the source or destination for a move when you are using the library operator panel; it is not available when using remote access through the BlueScale web interface.

Because the access port opens as a part of any move that includes the access port, a move queue that uses the access port is especially useful for importing or exporting cartridges.

Note: All moves that use the access port must be in the same direction (either from a source location to the access port or from the access port to a destination location). The direction of the first move in the queue dictates the direction for subsequent moves. Imports and exports cannot be performed in the same move queue.

- **Importing cartridges**—You can import one or more cartridges into a partition by creating a move queue that moves each cartridge from the access port to a specific slot in the partition. This type of move queue is an alternative to using the Import/Export screen as described in Import Individual Cartridges on page 212.
- **Exporting or exchanging cartridges**—You can export individual cartridges from a partition using a move queue that moves each cartridge from its slot in the partition to the access port so that you can remove the cartridge or exchange it for a different one. This type of move queue is especially useful when you need to exchange an expired cleaning cartridge for a new one.

Using the EE slot as the move source or destination Moving a cartridge to or from the E/E slot does not open the access port. The next move in the queue is processed as soon as the move to the E/E slot completes. For this reason, the **EE slot** option is available as a move source or destination from both the operator panel and the BlueScale web interface.

Important

If you configure a move queue to include a move to the E/E slot, neither the EE slot nor the access port is available as a destination for subsequent moves in that queue. When a cartridge is moved to the E/E slot, you must use the **Open Door** button on the Import/Export screen to open the access port and then remove the cartridge.

Moving a cartridge to the E/E slot is especially useful if you want to use one of the cartridges in the partition as the scratch cartridge required by the DLM Drive Health Verification wizard (see Using DLM to Test an LTO Drive on page 414). Moving a cartridge to the E/E slot also makes it possible to transfer a data cartridge from one storage partition to another without opening the access port. However, the move from the E/E slot to a slot in a different partition must be performed using a separate move queue.

Create a Move Queue

1. From the operator panel, log into the library as a user with the appropriate privileges (see User Privilege Requirements, above).
2. Display the cartridge inventory for the desired partition (see View the Cartridge Inventory for a Partition on page 224).
3. Select the source for the move.

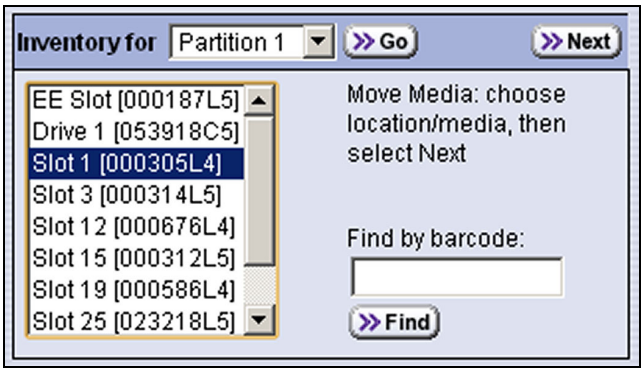


Figure 152 Select the cartridge you want to move.

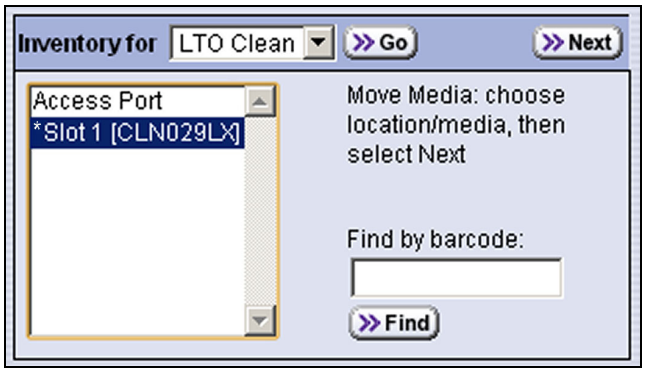


Figure 153 Select the expired cleaning cartridge to exchange.

- To move a cartridge from one location to another, locate and select the cartridge you want to move (see Locate a Specific Cartridge on page 225).
- To import a cartridge using the access port, select **Access Port** as the source.

Notes:
- The **Access Port** is only included on the inventory list when you access the user interface from the front panel.
- If the E/E slot contains a cartridge, **EE Slot** and the barcode label of the cartridge it contains appear on the inventory list instead of **Access Port**.
- If one of the partition's drives contains a cartridge, that drive is included in the list.
- Cleaning cartridges have an * (asterisk) next to the slot number if the cartridge is expired.
- If a move queue is already defined, the Inventory screen includes a **View Move Queue** button which immediately displays the Move Queue screen without needing to go through the process of configuring a move queue (see Figure 155 on page 230).

4. Click **Next**. The Destination screen displays a list of available locations in the partition. Only locations that do not already contain a cartridge are listed.

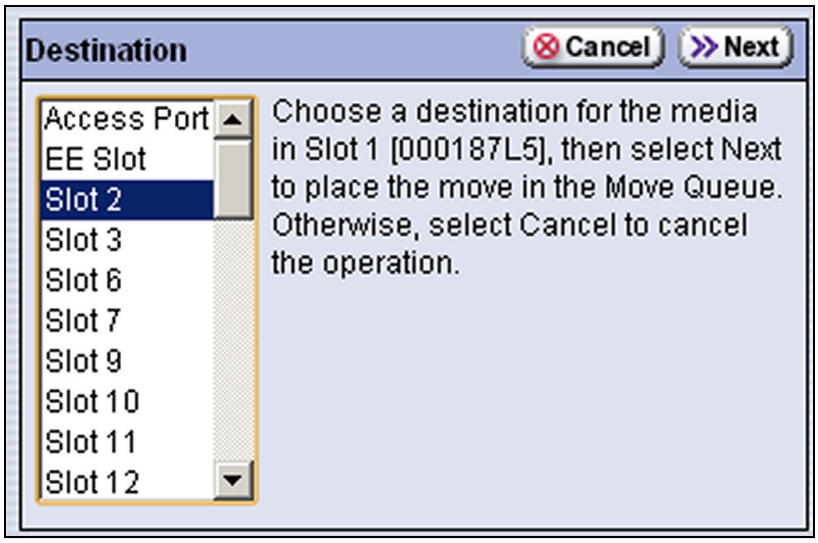


Figure 154 Select the destination for the cartridge you want to move.

5. Select the location to which you want to move the cartridge.

Notes:

- Select **Access Port** as the destination if you want to export or exchange a cartridge.
- For a storage partition, if the E/E slot is empty, both the **Access Port** and the **EE Slot** are listed as potential destinations. The end result of the move depends on which one you select.
  - If you select **Access Port**, the access port opens after the cartridge is moved to the E/E slot. You must remove (or exchange) the cartridge in the E/E slot and close the port before the next move can be processed.
  - If you select **EE Slot**, the cartridge is moved to the E/E slot but the access port does not open. The next move in the queue is processed as soon as the move is complete. The cartridge is left in the E/E slot.
- For a cleaning partition, if the E/E slot is empty the **Access Port** is listed as a potential destination. The **EE slot** is not available as a move destination in a cleaning partition.
- If one or more of the drives in the partition are empty, those drives are included in the list of available destinations.

6. Click **Next**. The Move Queue screen displays. The move you just defined is listed on the left side of the screen.

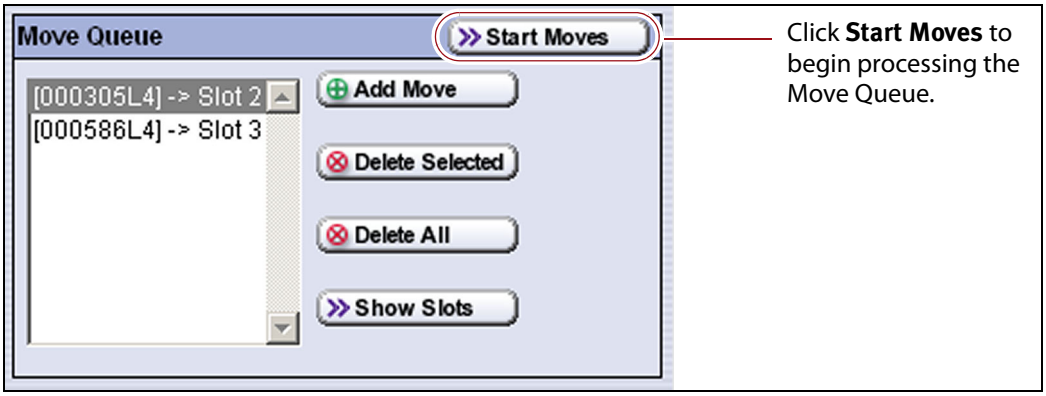


Figure 155 Click **Start Moves** to begin processing the move queue.

7. To add another move, click **Add Move** and repeat Step 3 on page 228 through Step 6 on this page for each additional cartridge you want to move.

   After you finish creating the move queue, you are ready for the library to perform the requested moves.

   Note: If you want to remove one or more of the moves in the queue:

   - Select the move and click **Delete Selected** to remove it from the Move Queue list.
   - Click **Delete All** to remove all of the defined moves from the Move Queue list.

8. Click **Start Moves** on the Inventory screen to begin processing the moves in the order that they are listed in the queue.

   A progress screen tracks the progress of the move operations. When all of the moves in the queue are processed, the library displays a Move Status screen showing the result of each move.

Important If the move destination is the access port, do not close the access port until a Feedback Required screen notifies you that the port can be closed.

   Note: If you selected **Access Port** as the destination for a move, the access port opens after the cartridge is moved to the E/E slot. A Feedback Required screen displays instructing you to remove the cartridge and close the port.

   If you want to exchange the cartridge for a different one, remove the cartridge and replace it with the new one.

   After you close the access port, the library moves the cartridge to the location originally occupied by the cartridge you removed.

9. When all of the moves in the queue are complete, a status screen displays showing the results of the moves. Click **Finish** to return to the Inventory screen.

10. Use your storage management software to update the inventory it maintains (see Updating the Software Media Inventory on page 232).

Complete Any Move to the E/E Slot

If one of the moves had a destination of **EE slot**, complete one of the following actions when all of the moves in the queue are complete.

Remove the cartridge from the E/E slot

1. From the library operator panel, click **MENU**, then select **General** ⋯ **Import/Export**. The Import/Export screen displays showing the information for the last partition that was viewed on either the Import/Export screen or the Inventory screen.

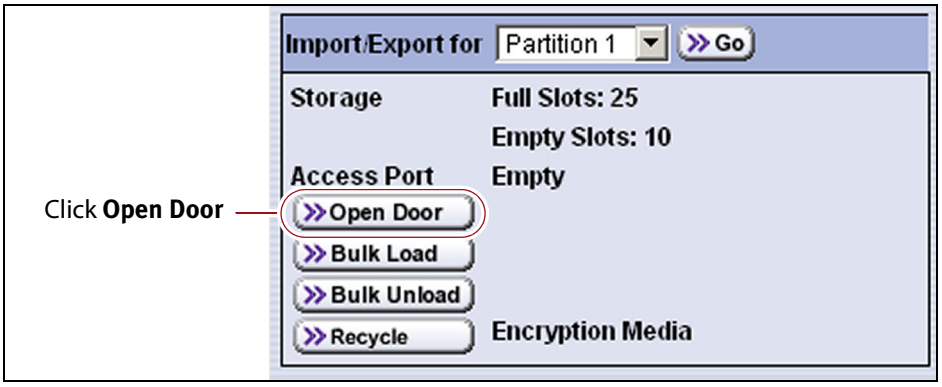


Figure 156 Click **Open Door** to open the access port and remove the cartridge.

2. Click **Open Door** to open the access port.
3. Remove the cartridge from the E/E slot.

Move the cartridge to another partition

Repeat Step 2 on page 228 through Step 9 on this page to create and process a move queue that moves the cartridge from the E/E slot to a different storage partition.

UPDATING THE SOFTWARE MEDIA INVENTORY

As you import, export, or exchange cartridges, the library reads the barcode labels on the individual cartridges and automatically updates the physical inventory that it maintains. This process does not automatically update the media inventory maintained and used by the storage management software.

The storage management software maintains its own media inventory, which it uses when performing backup/restore operations and for media management. To avoid errors when the storage management software requests a specific cartridge, be sure to use your storage management software to update its media inventory whenever you import cartridges into or export/exchange cartridges from a storage partition as described in this chapter. Refer to your software documentation for more information.

CHAPTER 8

Configuring and Using Media Lifecycle Management

This chapter describes how to use BlueScale Media Lifecycle Management to monitor and report on the health of the cartridges in your library. See MLM Best Practices on page 481 for information about using Media Lifecycle Management (MLM) effectively in your environment and ensuring that your MLM data is protected.

MEDIA LIFECYCLE MANAGEMENT OVERVIEW

This section describes the major features of BlueScale Media Lifecycle Management (MLM). The remainder of the chapter provides detailed information about configuring and using MLM.

Important Before you can use Media Lifecycle Management, you must enable it as described in Enabling MLM and Configuring Global Settings on page 242.

Note: MLM is only supported for LTO-4 and later generation drives and compatible media.

Overview BlueScale Media Lifecycle Management (MLM) helps you manage your tape media (cartridges) by giving you tools to proactively detect potential media errors well before they happen. When used in combination with Spectra Certified MLM-enabled media, MLM lets you manage, track, and report all facets of tape usage from creation to retirement. When used with media that is not MLM-enabled, MLM tracks and reports the general health of the media.

Spectra Certified MLM-Enabled Media

Media Lifecycle Management starts with packaged, barcode labeled, Spectra Certified MLM-enabled media (LTO-3 and later generation data cartridges and LTO cleaning cartridges). Before shipment, Spectra Logic writes baseline data to the MAM (Medium Auxiliary Memory) embedded in each cartridge. Throughout its life, the cartridge MAM continually collects data to support MLM tracking and reporting. See Spectra Certified Media on page 493 for additional information.

Media Tracking and Reporting

Overview MLM uses the information from the cartridge's MAM to maintain a database of vital information about each MLM-enabled cartridge in the library, including the drives into which it was loaded and any errors it encountered. The statistical and diagnostic information in the MLM database helps you proactively manage your tape media throughout its life. Using the information in the database, MLM can generate a variety of reports that let you monitor important health information about every MLM-enabled data cartridge and cleaning cartridge in your library. If desired, you can save the reports to a USB device or email them to a previously configured mail user. You can also download the MLM database as a comma separated value (CSV) file.

Notes:
- The MLM database also includes limited information about cartridges that are not MLM-enabled.
- The cartridge inventory is separate from the MLM database and only shows cartridges currently stored in the library. The cartridge inventory does not differentiate between MLM-enabled cartridges and those that are not MLM-enabled.

Discovery Requirement Until an LTO cartridge is discovered, either through the automatic media discovery process or when it is loaded into and then unloaded from a drive for the first time, it is not included in the MLM database.

Media Health Score The initial load/unload during discovery establishes an initial media health score for each cartridge and adds this information to the MLM database. This initial health score may not accurately reflect the actual health of the media. The health score stabilizes and becomes more accurate after the first four loads/unloads as current usage statistics are updated and used in the tape's health scoring.

MLM Health Reports MLM reports let you review important health information about every MLM-enabled data tape and cleaning tape in your library. You can generate comprehensive health reports for the MLM-enabled media in the whole library or in an individual partition. You can also generate more detailed reports with information about compression ratios, load counts, write errors, remaining capacity, encryption status, and more.

The MLM reports help you identify tapes with high error rates or other problems (for example, a dropped leader pin) that pose a risk to protecting your data. These tapes can then be removed before they cause data corruption or other problems. See Generate MLM Reports on page 262 for detailed information about the types of reports you can generate.

MLM Database Management After a cartridge is added to the MLM database, its MLM data remains in the database even if the cartridge is exported from the library. If the cartridge is later reimported, the MLM database is updated to reflect any new information obtained from the cartridge MAM. When a cartridge is permanently removed from service, it can be manually deleted from the database.

The MLM database is restricted to a maximum of 100 records. Each record corresponds to a cartridge with a unique barcode label. When a new cartridge, beyond the 100 already in the database, is imported into the library, the record for the least recently exported cartridge is automatically deleted from the database. The Export Date tracked by MLM determines which record is deleted. The library does not notify you when it reaches the maximum number of records.

To ensure that you have a complete record of all the cartridges that are used in the library, regularly generate and export a Media Health report for the entire library (see Using MLM Reporting on page 262). When a cartridge is retired or permanently exported from the library, its record can be deleted from the MLM database. Records can be deleted individually or as a group (see Delete MLM Records From the Database on page 275).

If desired, the information in the MLM database can be exported to a comma separated value (CSV) file, which can then be imported into Microsoft Excel® or other software applications that support this file type (see Download the MLM Database for Analysis and Archiving on page 277).

Data Cartridge Tracking

A primary function of MLM is to track the health and usage of the data cartridges that are currently in, or were previously in, the library.

Functional Overview Each time a Spectra Certified MLM-enabled data cartridge is loaded into a drive, MLM records over 30 data points about the cartridge. These data points include health information, the cartridge age, how many times it was loaded and into which drives, and how many errors it accumulates. It also records when the cartridge is exported from the library and by whom. Each MLM-enabled data cartridge has a unique identifier that allows each cartridge to be tracked throughout its life, even if its barcode label is damaged or removed.

Important

LTO-5 and later generation drives support a tape format called Linear Tape File System (LTFS).

LTFS uses an area in the cartridge MAM that was previously used for LTO-5 cartridge MLM data. Starting with BlueScale12.0.3, the library's BlueScale software automatically moves the MLM data to a protected area of the MAM the first time an LTO-5 data cartridge is loaded into and then unloaded from an LTO-5 drive running firmware version B6W1 or later. See Support for LTFS for LTO-5 Data Cartridges on page 201 for detailed information about how support for LTFS impacts MLM.

Remaining Capacity Calculations In addition to media health, the library uses information in the MLM database to estimate the Remaining Capacity report for the cartridges in the selected partition. If the partition contains a mix of MLM and non-MLM-enabled data cartridges, the report only shows the estimated capacity on the MLM-enabled cartridges.

Note: Until a data cartridge is loaded into, threaded, and then unloaded from a drive for the first time, its remaining capacity is not included in the Remaining Capacity report.

Cleaning Cartridge Tracking

Functional Overview The library tracks expired cleaning cartridges in the cartridge inventory and does not attempt to use an expired cleaning cartridge. You can identify expired cartridges by examining the Inventory screen. Expired cleaning cartridges are identified by an "x" next to the slot number.

When you enable MLM and use Spectra Certified MLM-enabled LTO cleaning cartridges, MLM tracks and reports usage information for the cleaning cartridges. This information, which includes the number of cleans remaining and the cartridge health (good, near expiration, or expired), is stored in the MLM database.

When a cartridge is nearing the end of its useful life, MLM notifies you so that you can have another on hand to replace it. This early notification helps prevent failed cleanings resulting from using an expired cleaning cartridge. See Enabling MLM and Configuring Global Settings on page 242 for information about setting the threshold for generating the notification.

Expired MLM-Enabled Cleaning Cartridges Each time an MLM-enabled cleaning cartridge is used in a drive, the drive decrements the number of cleans remaining on the cartridge. When the cartridge is unloaded from the drive, MLM reads the number of cleans remaining from the cartridge MAM. When the number of cleans remaining reaches zero, the library flags the cartridge as expired and does not attempt to use the cartridge again. Because the library does not need to load a cleaning cartridge into a drive to determine that it is expired, cleaning failures due to an expired cartridge are eliminated (assuming the cleaning partition contains a good cleaning cartridge). Information about an expired cleaning cartridge remains in the MLM database even after the cartridge is exported from the library.

Expired Non-MLM Cleaning Cartridges When MLM is not enabled or if the cleaning cartridges are not MLM-enabled, the library must load the cleaning cartridge into a drive to determine whether it is expired. When an expired cleaning cartridge is loaded into a drive, it is immediately ejected; the cleaning fails. The library flags the cleaning tape as expired in the cartridge inventory and generates system messages to notify you of the expired cleaning tape and the failed drive cleaning. The library does not attempt to use the expired cartridge for subsequent cleanings.

The library does not store any information about non-MLM cleaning cartridges in the MLM database. The library retains the information about an expired cleaning cartridge for as long as it remains in the library or until the library is power-cycled. If an expired non-MLM cartridge is exported and then reimported into the library, the cartridge must be loaded into a drive in order to identify it as expired.

Media Discovery

Overview Importing a cartridge into a partition does not add it to the MLM database. The cartridge must be discovered by loading it into and then unloading it from a drive in order to add it to the MLM database. After discovery, the cartridge is tracked by MLM and included in MLM reports.

Automatic Discovery The Media Auto Discovery feature is a background process that loads MLM-enabled cartridges into an LTO-4 or later generation drive, records the MLM information to the cartridge MAM, adds the cartridge to the MLM database, and returns the cartridge to its original location. The process is performed by the library independently from the storage management software. Media Auto Discovery must be enabled on the library, as described in Enabling MLM and Configuring Global Settings on page 242, before it can be used.

Notes:
- If you do not want to use automatic media discovery, you can wait until the library loads and then unloads each cartridge from an MLM-capable drive for the first time during normal operation. When the cartridge is unloaded from the drive, the library discovers it and records the MLM data to the cartridge MAM and enters the data into the MLM database.
- After you enable Media Auto Discovery, importing a cartridge into a partition triggers the discovery process in that partition.

When Media Auto Discovery is enabled, MLM provides two options for proactively discovering media in a partition:

- **Media Auto Discovery**—The default process that collects information from the cartridge MAM and adds it to the MLM database. The Media Auto Discovery process only operates on newly imported cartridges that are not already in the MLM database.

  Note: Media Auto Discovery loads and reads the MAM in the tape, but does not thread the tape. The drive only reports the maximum and remaining capacity for the tape after the tape is threaded. Therefore, these statistics report as "0" until a drive reads from, or writes to, the tape.

- **PreScan**—An optional process that replaces Media Auto Discovery. If the PreScan feature is enabled in a partition, the PreScan process runs instead of the Media Auto Discovery process and operates on all of the media in the partition, regardless of whether it is already in the MLM database or not.

In addition to adding information collected from the cartridge MAM to the MLM database, PreScan performs a basic functionality test and health check on each imported cartridge using available LTO-4 or later generation drives in the partition (see Using PreScan on page 252 for more information).

Discovery Process When automatic media discovery is enabled, the discovery process can either be manually initiated by you or set to run automatically so that the library discovers the cartridges and adds their information to the MLM database shortly after a cartridge is imported into the library. The discovery process is independent of any storage management software.

The discovery process depends on whether the library is using Media Auto Discovery or PreScan. With Media Auto Discovery the library reads the barcode label on each new cartridge in the partition; with PreScan the library reads the barcode label on every cartridge in the partition. If a barcode is not already in the MLM database, the library loads the cartridge into a drive and performs either a PreScan or the basic Media Auto Discovery.

- If the cartridge is MLM-enabled, the library collects the available MLM information from the cartridge's MAM, including the born-on date. If the cartridge was used previously, the library also collects media health and encryption status from the MAM. The library updates the MLM database to include the collected information and the name of the partition where it currently resides. Any updated MLM information is also written to the MAM in the cartridge.
- If the cartridge is not MLM-enabled, the library collects the cartridge barcode label information, the cartridge health information, and the name of the partition where the cartridge currently resides. It then adds this information to the MLM database.

When the discovery process is complete, the drive unloads the cartridge and the library returns the cartridge to its original location. Each subsequent load/unload updates the MLM database and the cartridge MAM, providing ongoing tracking and reporting for the cartridge.

Manual Discovery If Media Auto Discovery is not enabled or if you enabled MLM when the library already contained cartridges, you can start the media discovery process manually to add the cartridges to the MLM database (see Initiate Media Discovery Manually on page 250).

Limitations Automatic media discovery cannot begin while the library is actively loading cartridges into drives. If you import cartridges during this time, the library posts a failure message stating that no drives are available for media discovery.

To avoid this failure, either wait until the library is idle before importing media or start the manual discovery process for the imported media when the library is idle. See Initiate Media Discovery Manually on page 250 for instructions.

MLM PreScan and PostScan

Overview MLM PreScan and PostScan are configurable background processes that use an LTO-4 or later generation drive to provide two levels of verification for LTO data cartridges. See Using PreScan on page 252 and Using PostScan on page 254 for detailed information about configuring and using PreScan and PostScan.

Note: PostScan and Spectra SKLM encryption key management cannot be configured for use in the same partition.

Enable and Configure PreScan and PostScan Both PreScan and PostScan are enabled and configured as part of the partition creation process, as described in Enable and Configure MLM PreScan and PostScan on page 182. During configuration you set the scanning frequency and select the types of scan you want to use.

Using PreScan and PostScan Refer to the following sections for detailed information about using the PreScan and PostScan features:

For information about...	See this section...
Usage requirements for PreScan.	Using PreScan on page 252
Usage requirements for PostScan and detailed information about how the QuickScan and FullScan options in the PostScan feature operate. This section also provides instructions for manually adding a tape to the PostScan queue and pausing the currently running PostScan process.	Using PostScan on page 254

PreScan and PostScan System Messages Both PreScan and PostScan generate system messages as possible error conditions are detected (for example, a broken leader or a media error). The messages indicate that the error condition was detected by the PreScan or PostScan process and not during normal operation.

Interaction with Move Requests If a host requests a move while a cartridge is being scanned using one of the partition drives (PreScan or QuickScan), the move is delayed until the scan completes and the cartridge is returned to its slot.

Background Operations To protect you against making changes that could negatively impact the library's operation, the BlueScale software automatically prevents you from performing certain operations while the library is performing background operations, including Media Auto Discovery, PreScan, or PostScan.

- You cannot import or export cartridges while the library is running a Media Auto Discovery or PreScan operation, nor can you use the BlueScale user interface to move cartridges from one location to another in the library. If you cannot wait for the operation to complete, you can stop Media Auto Discovery or PreScan and then manually start it at another time (Stop the Discovery Process on page 252).

- You cannot perform any of the following operations while either a FullScan or a QuickScan that uses Global Spare drives is running in a partition.
  - Import cartridges into or export cartridges from the library
  - Use the BlueScale user interface to move a cartridge from one location to another
  - Use the Global Spare drive being used by PostScan to replace a malfunctioning drive in the partition
  - Change the library configuration settings
  - Create or modify partitions
  - Update the BlueScale software or drive firmware

  If you need to perform any of these operations or if you need to reset the library, you can pause the PostScan process for one hour (see Pause the PostScan Process on page 261). The library returns any cartridges currently being scanned to their original locations. After an hour passes, the library checks the prerequisites for starting PostScan (see Prerequisites for Starting a PostScan Operation on page 254) and when met, restarts the PostScan operation on the tape that was being verified at the time of the interruption.

Additional MLM Features

In addition to the features described in the previous sections, MLM provides the following features (listed in alphabetical order):

Database Management Management tools let you manually delete one or more tape records from the MLM database when the tape is retired or permanently exported from the library.

Media Alert The Media Alert feature generates a system message when a tape's health is identified as poor (red) during five consecutive loads. This message is only generated once per tape. A separate system message is generated whenever a cartridge experiences a hard error.

Tracking Non-MLM-Enabled Media MLM tracks the basic health information for LTO data cartridges that are not MLM-enabled. This basic health information is based on tape log data retrieved from an MLM-capable LTO drive (LTO-4 or later) when the cartridge is ejected. The data pertinent to media health is stored in the MLM database and used to determine the media health status (Usable or Impaired) included in Media Lifecycle Management reports.

ENABLING MLM AND CONFIGURING GLOBAL SETTINGS

Overview This section describes enabling MLM on the library and configuring the global MLM features. The global features are optional and operate for every partition that is configured to use PreScan and PostScan (see Enable and Configure MLM PreScan and PostScan on page 182).

Notes:
- MLM is enabled by default. If you do not want to use MLM, you must disable it.
- Disabling MLM also disables DLM.

Important Before disabling (or re-enabling) Media Lifecycle Management, make sure that none of the drives in the library contain a cartridge. Use your application software to unload cartridges from the drives and return them to the slots in the library.

User Privilege Requirements Only a user with superuser or administrator privileges can enable MLM and configure the global MLM features.

Enable MLM and Configure Settings

Use the following steps to enable MLM and Media Auto Discovery and configure the global settings for MLM. These settings affect all partitions in the library.

Note: Enabling MLM automatically enables Drive Lifecycle Management (DLM) as well. See Chapter 9 – Using Drive Lifecycle Management, beginning on page 279 for information about DLM.

1. Log into the library as a user with superuser or administrator privileges.

2. Click **MENU**, then select **Configuration ⋯⁘ MLM**. The MLM Settings screen displays.

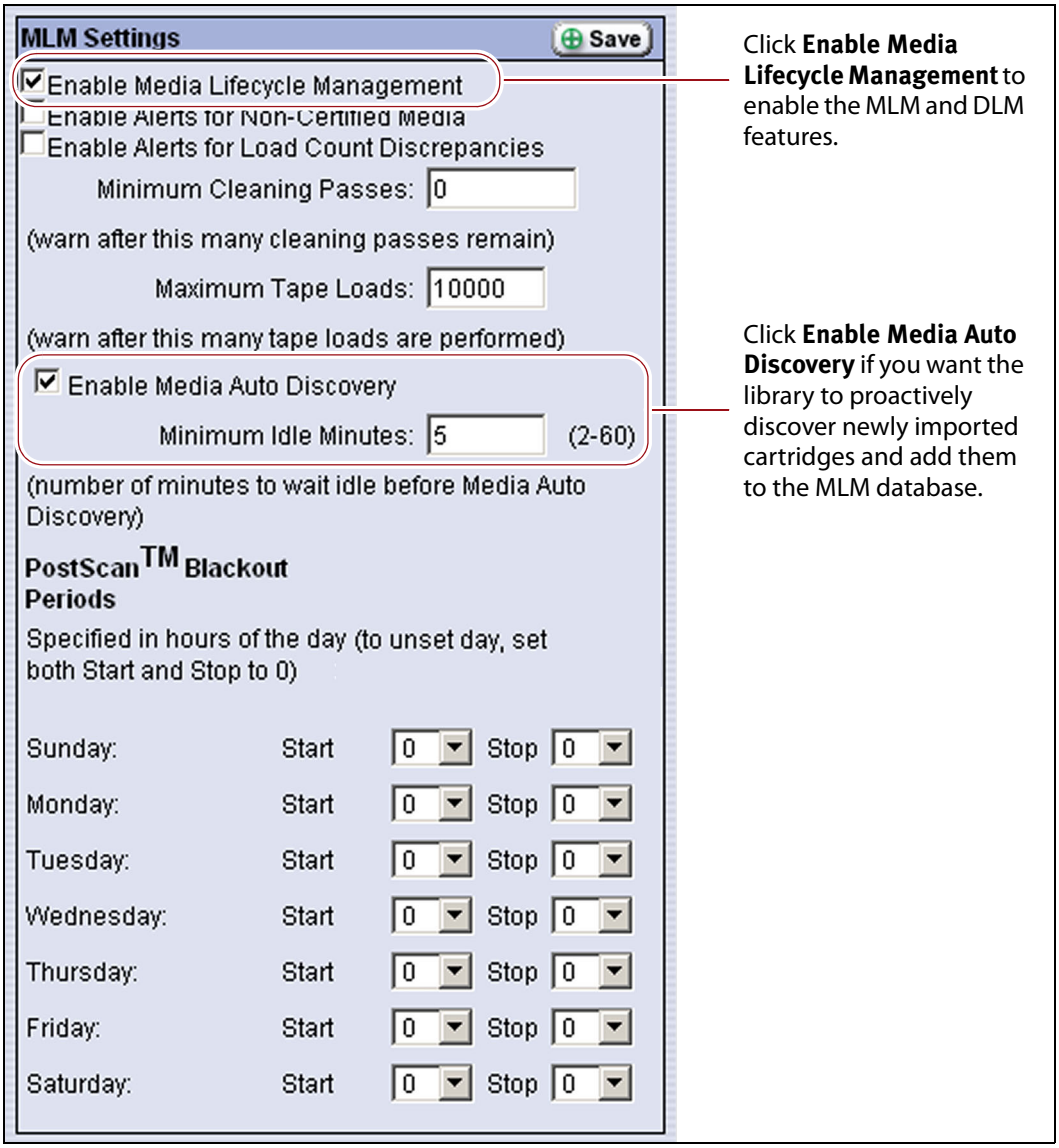


Figure 157 Use the MLM Settings screen to enable MLM and configure the global configuration settings.

3. Select the MLM features you want to use.

Select this option...	To...	Default Setting
Enable Media Lifecycle Management	Enable the Media Lifecycle Management (MLM) features in the library. MLM is enabled by default. Enabling Media Lifecycle Management also enables Drive Lifecycle Management (DLM), which is described in Chapter 9 – Using Drive Lifecycle Management, beginning on page 279.	Selected (Enabled)
Enable Alerts for Non-Certified Media	Configure MLM to generate an alert message when a cartridge that is not MLM-enabled is loaded into a drive. **Note:** Enabling this alert is only recommended if all of the cartridges typically used in the library are MLM-enabled.	Cleared (Disabled)
Enable Alerts for Load Count Discrepancies	Configure MLM to generate an alert message when the load count for a cartridge stored in the MLM database differs from the load count stored on that cartridge's MAM.	Cleared (Disabled)
Minimum Cleaning Passes	Set the threshold for the minimum number of cleaning passes remaining on a cleaning cartridge. When a cleaning cartridge reaches this threshold, a warning message is generated showing that the cleaning cartridge is nearly expired. The warning message is generated every time the cleaning tape is used while the number of cleanings remaining is at or below the threshold value. **Note:** When the number of cleans remaining on the cartridge reaches zero, the library flags the cartridge as expired.	Zero (0)
Maximum Tape Loads	Set the number of times a data cartridge can be loaded into a drive before a load count warning message is generated. When the number of loads reaches the specified threshold, a warning message is generated. Subsequent loads do not generate additional messages. Generate a Load Count Media Lifecycle Report to determine the current usage status of the cartridges in your library (see Using MLM Reporting on page 262 for detailed information). **Note:** If you began using MLM-enabled data cartridges before you enabled MLM, some of your data cartridges may already exceeded the thresholds you set.	10,000 loads

Select this option...	To...	Default Setting
Enable Media Auto Discovery	Enable the Media Auto Discovery feature. Media Auto Discovery must be enabled before the library proactively discovers newly imported LTO cartridges and adds them to the MLM database. If you enable PreScan for the partition, the Media Auto Discovery process is replaced by the more in depth PreScan process for that partition (see Enable and Configure MLM PreScan and PostScan on page 182). **Requirements** ▪ Media Lifecycle Management must be enabled. ▪ All cartridges must have barcode labels. **Notes:** ▪ The Media Auto Discovery process identifies MLM-enabled cartridges as well as those that are not MLM-enabled. ▪ The Media Auto Discovery process may be affected by your storage management software. In addition, software that polls the drives on a regular basis is affected by the discovery process. If you encounter interactions with your storage management software, you can select to either stop the storage management software from accessing the library before starting the discovery process or you can select not to use Media Auto Discovery. ▪ If you do not enable Media Auto Discovery, you can start the discovery process for a specific partition manually. See Initiate Media Discovery Manually on page 250 for instructions. —OR— You can let the library discover cartridges and add them to the MLM database the first time they are loaded and unloaded from an MLM-enabled drive during normal operations.	Cleared (Disabled)
Minimum Idle Minutes	Set the number of minutes that the library needs to be idle before the Media Auto Discovery or PreScan process begins.	5 minutes
PostScan Blackout Periods	Configure time periods during which the automatic PostScan process does not operate. See Configure PostScan Blackout Periods on page 246 for detailed information.	Zero (0) (Disabled)

4. Click **Save** to enable the selected MLM features.

Configure PostScan Blackout Periods

If desired, you can configure blackout periods during which PostScan process does not operate. Configuring blackout periods ensures that during the blackout period, all cartridges in the partition are immediately available and the Global Spare drive is available if needed.

Important

When configuring blackout periods, keep the following information in mind:

- The blackout periods you configure apply to all of the partitions in the library.
- If PostScan is actively verifying a tape at the time the blackout period starts, it completes the current scan. No additional tapes are scanned until the blackout period expires.

1. Access the MLM Settings screen (see Enable MLM and Configure Settings on page 242).
2. In the PostScan Blackout Periods section, use the **Start** and **Stop** drop-down lists to set the start and end times for the blackout period for each day of the week.

   Notes:
   - Times are based on a 24-hour clock, where 0 is midnight.
   - To disable the blackout period for a specific day, set both **Start** and **Stop** to 0.
   - By default, the blackout periods are all set to 0 (disabled). The PostScan process runs whenever there are tapes in the PostScan queue and a Global Spare drive is available.
   - Configuring a blackout period to begin at 23 hours and end at 0 is not supported.

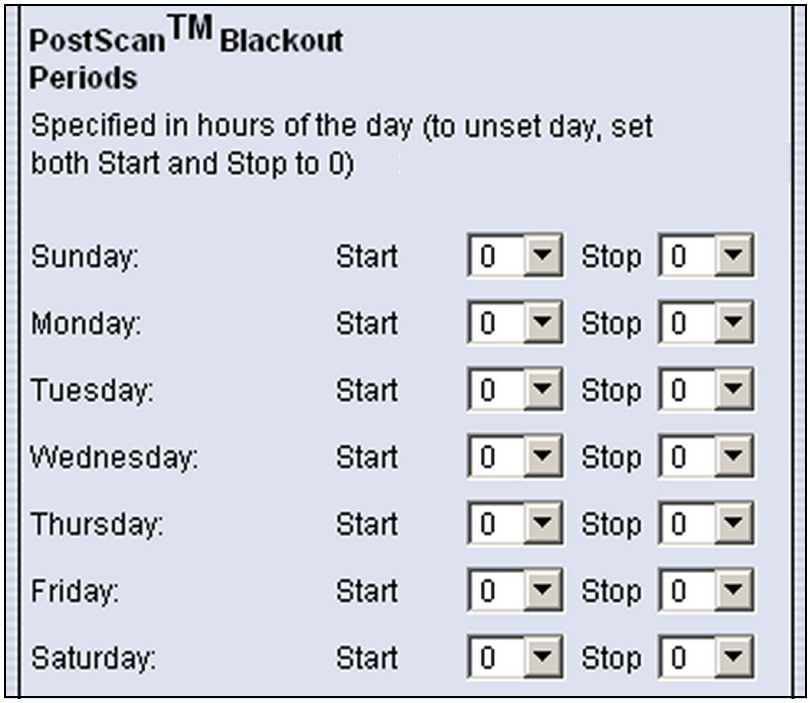


Figure 158 Select the desired blackout periods for PostScan.

3. Click **Save**.
4. The blackout periods you set take effect when you enable PostScan for individual partitions by configuring one or more PostScan triggers (see Enable and Configure MLM PreScan and PostScan on page 182).

USING MEDIA LIFECYCLE MANAGEMENT

Overview After you enable MLM and configure the global settings (see Enabling MLM and Configuring Global Settings on page 242), you are ready to begin using MLM to track and monitor the LTO cartridges in the library.

Note: If you want to use the PreScan and PostScan options, you must enable and configure these options for each partition (see Enable and Configure MLM PreScan and PostScan on page 182).

User Privilege Requirements See Specify the Partition Users on page 186 for information about assigning users to a partition.

- Only a user with superuser or administrator privileges can manually start and stop media discovery (using either Media Auto Discovery or PreScan), manually start and pause PostScan operations, and manage the MLM and DLM databases.
- Any user with operator privileges who is assigned to the partition and all users with superuser or administrator privileges can generate and save MLM reports.

Add Cartridges to the MLM Database

The cartridges used in the library are not added to the MLM database until they are discovered. The process you use to discover cartridges and add them to the MLM database depends on when you loaded the cartridges into the library.

Important If a cartridge is write-protected when it is inserted into a drive, the library cannot update the MLM information on the cartridge's MAM.

Important The discovery process cannot begin while the library is actively loading cartridges into drives. If you import cartridges during this time, the library posts a failure message stating that no drives are available. Either wait until the library is idle before importing cartridges or start the discovery process for the imported cartridges manually when the library is idle.

Note: If you import cartridges into the library with MLM disabled, those cartridges are not automatically discovered and added to the MLM database. After you enable MLM, you must use the manual discovery process to add the cartridges to the MLM database (see Initiate Media Discovery Manually on page 250.

The following table provides information about different possible scenarios for adding cartridges to the MLM database.

If you...	Do this to add the cartridges to the MLM database...
Recently purchased your library and are importing cartridges into the library for the first time,	**1.** Make sure that MLM is enabled (see Enabling MLM and Configuring Global Settings on page 242). **2.** If desired, enable PreScan (see Using PreScan on page 252). **3.** Import media into the partitions to trigger the automatic discovery process. **Important:** Discovery cannot begin while the hosts are actively loading cartridges into and unloading cartridges from drives. If you import cartridges during this time, the library posts a failure message stating that no drives are available. Either wait until the library is idle before importing cartridges or manually start the discovery process when the library is idle.
Have an existing library that does not have the most current version of BlueScale installed and: ▪ You began using MLM-enabled Spectra Certified LTO media when it became available but before BlueScale10.4 introduced the MLM functionality in the fall of 2008, —OR— ▪ You began using a mixture of MLM-enabled and non-MLM-enabled Spectra Certified LTO media before the MLM functionality was introduced in BlueScale10.4,	**1.** Update the library to the most current BlueScale version. See Updating the BlueScale Software and Library Firmware on page 421 for instructions. **2.** Enable MLM for the library (see Enabling MLM and Configuring Global Settings on page 242). **3.** If desired, enable PreScan (see Using PreScan on page 252). **4.** Discover the cartridges in the library using one of the following methods: ▪ Import new cartridges into the partition to trigger the automatic discovery process. If you do not have PreScan enabled, the discovery process only checks cartridges that are not already in the MLM database. If PreScan is enabled, all of the cartridges in the partition are processed, regardless of whether or not they are already in the MLM database. **Important:** Discovery cannot begin while the hosts are actively loading cartridges into and unloading cartridges from drives. If you import cartridges during this time, the library posts a failure message stating that no drives are available. Either wait until the library is idle before importing cartridges or manually start the discovery process when the library is idle. ▪ If you do not want to wait until you import new cartridges to have the cartridges already in the library added to the MLM database, manually start the discovery process (see Initiate Media Discovery Manually on page 250). ▪ Use your storage management software to load each cartridge into an LTO-4 or later generation drive and then unload it. ▪ Let the library update the MLM database as part of normal operation. The information for each cartridge is added to the MLM database the first time the cartridge is loaded into and then unloaded from an LTO-4 or later generation drive. **5.** When the initial discovery process is complete, disable the alert about non-MLM-enabled media, if desired.

If you...	Do this to add the cartridges to the MLM database...
Have an existing library with the most current version of BlueScale installed. Cartridges are already imported into the library, but you just recently enabled MLM,	**1.** If you want to detect any non-MLM-enabled cartridges being imported, temporarily enable the alert on the MLM Settings screen (see Enable Alerts for Non-Certified Media on page 244). The alert is disabled by default. **2.** If desired, enable PreScan (see Using PreScan on page 252). **3.** Discover the cartridges in the library using one of the following methods: ▪ Import new cartridges into the partition to trigger the automatic discovery process. If you do not have PreScan enabled, the discovery process only checks cartridges that are not already in the MLM database. If PreScan is enabled, all of the cartridges in the partition are processed, regardless of whether or not they are already in the MLM database. ▪ If you do not want to wait until you import new cartridges to have the cartridges already in the library added to the MLM database, manually start the discovery process (see Initiate Media Discovery Manually on page 250). ▪ Use your storage management software to load each cartridge into an LTO-4 or later generation drive and then unload it. ▪ Let the library update the MLM database as part of normal operation. The information for each cartridge is added to the MLM database the first time the cartridge is loaded into and then unloaded from an LTO-4 or later generation drive. **4.** When the initial discovery process is complete, disable the alert about non-MLM-enabled media, if desired. **5.** To routinely verify the readability of the cartridges, configure PostScan for each partition in the library (see Using PostScan on page 254).

Initiate Media Discovery Manually

The manual discovery process is useful if you did not enable Media Auto Discovery but still want to take advantage of the MLM features or if you enabled MLM when the library already contained cartridges.

Note: Spectra Logic highly recommends that you perform the manual Media Auto Discovery process when your storage management software is not accessing the library and the library is idle.

1. Make sure that Media Lifecycle Management is enabled before you start the discovery process (see Enabling MLM and Configuring Global Settings on page 242).
2. Click **MENU**, then select **Maintenance ⋯ MLM**. The Media Lifecycle Management Tools screen displays.
3. Click **Discover Media** to start the manual discovery process.

   Note: If all of the media in the library was previously discovered, the **Discover Media** button is grayed out. You do not need to perform a manual media discovery.

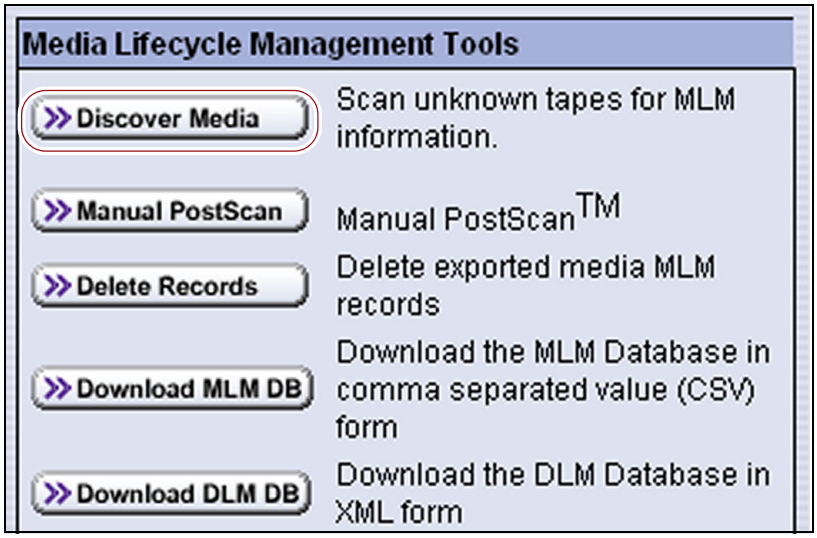


Figure 159 Click **Discover Media** to begin configuring the manual media discovery process.

4. Select the partition containing the cartridges you want to add to the MLM database, then click **Next**.

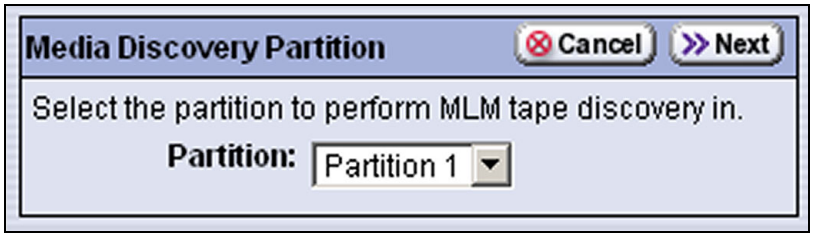


Figure 160 Select the partition containing the cartridges you want to add to the MLM database.

5. Click **OK** on the Start Media Discovery screen to begin the discovery process.

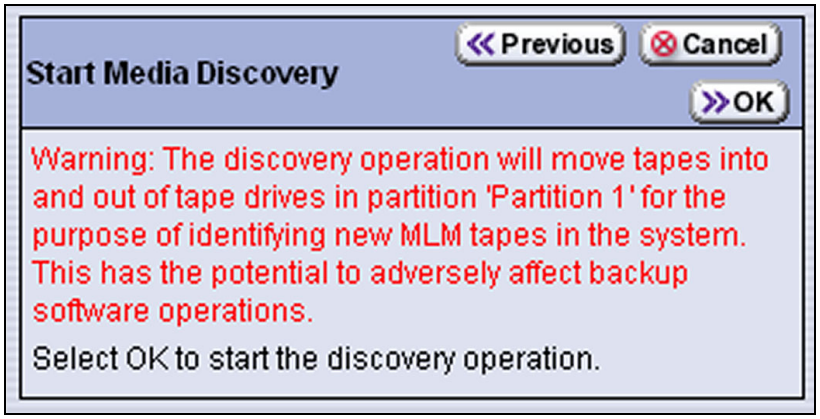


Figure 161 Click **OK** on the Start Media Discovery screen to start the discovery process.

6. When the Media Discovery Start Results screen displays, click **OK** to confirm that the process started and return to the Media Lifecycle Management Tools screen.

   The discovery process continues in the background while the library continues to operate.

   Note: See Background Operations on page 240 for information about operations that cannot be performed while the discovery process is running.

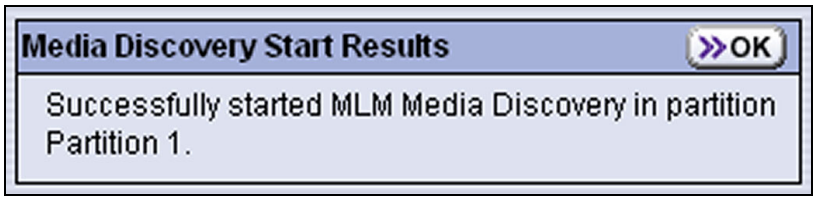


Figure 162 The Media Discovery Start Results screen displays when the discovery process starts.

Stop the Discovery Process

If for some reason you need to interrupt the discovery process before it is complete, click **Stop Discovery** on the Media Lifecycle Management Tools screen. The library completes any Media Auto Discovery or PreScan operations that are in progress and returns the cartridges to their slots.

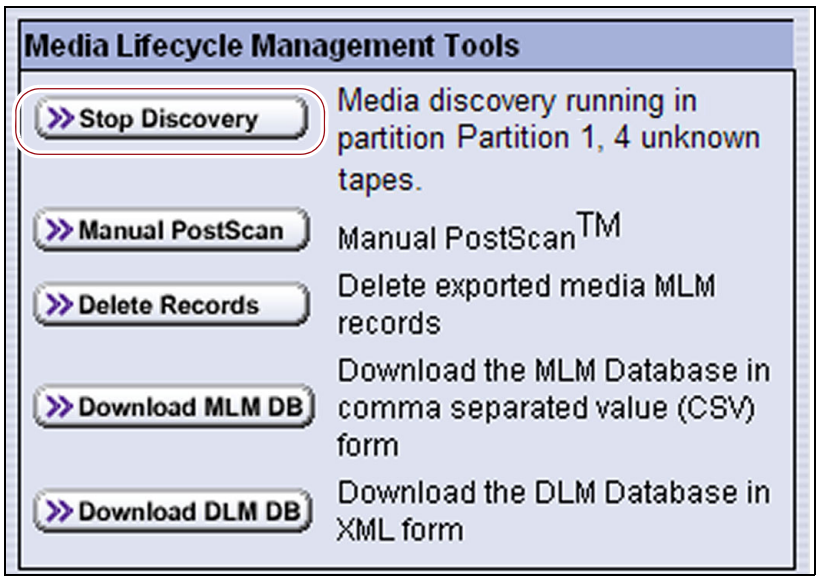


Figure 163 Click **Stop Discovery** to stop the discovery process.

To resume the discovery process, repeat the steps in Initiate Media Discovery Manually on page 250 or wait until you import additional cartridges into the partition to trigger the discovery process automatically.

Using PreScan

Overview The MLM PreScan feature is a background process that replaces the default Media Auto Discovery process in partitions where it is enabled; unlike Media Auto Discovery, it does not operate globally. PreScan is enabled when you configure the partition (see Enable and Configure MLM PreScan and PostScan on page 182).

PreScan provides verification of data cartridges by performing a basic functionality test and health check on each imported cartridge using available LTO-4 or later generation drives in the partition. As a part of the PreScan process, any cartridges that are not already in the MLM database are added to the MLM database.

During the PreScan process, the library automatically inserts each cartridge into an available LTO-4 or later generation drive assigned to the partition. The drive loads the cartridge and checks it to determine whether it has any of the following characteristics:

- Non-MLM-enabled
- Broken or dislodged leader
- Red media health
- Write protected
- Encrypted tape with a moniker not currently stored in the library

When the PreScan process is complete, the library stores the tape health information for the cartridge in the MLM database. It also writes the MLM data to the cartridge MAM. When the drive ejects the cartridge, the library returns it to its original slot.

Requirements for Use In order to use PreScan, make sure that the library, drives, and data cartridges meet the following requirements:

Consideration	Requirement
Drive Firmware	▪ LTO-4: requires 97F9 or later firmware. ▪ LTO-5: requires B171 or later firmware. ▪ LTO-6 and later: supported with any firmware.
Updating MLM Data on MAM	Updating the cartridge MAM requires the cartridge to be write-enabled. **Important:** If a cartridge is write-protected when it is inserted into a drive, the information about the cartridge is added to the MLM database, but the library cannot update the MLM information on the cartridge's MAM.
Drive Availability	The media discovery process loads the cartridges in the partition into the drives assigned to that partition. While in use for PreScan, host moves to the drives being used are delayed until the PreScan operation completes. Spectra Logic highly recommends that you perform the manual media discovery process when your storage management software is not accessing the library and the library is idle.
Auto Drive Clean Restrictions	Auto Drive Clean operations do not start while PreScan is running on any partition that is associated with the cleaning partition. If a drive requires cleaning, wait until the PreScan operation is complete and then manually clean the drive.
Cleaning Partitions	The PreScan feature cannot be enabled for a cleaning partition and does not affect the operation of cleaning cartridges.

USING POSTSCAN

This section provides detailed information about how PostScan operates, as well as prerequisites for using PostScan and performing manual PostScan operations.

PostScan is enabled and configured for each individual partition. PostScan does not operate until the PostScan option is selected and one or more triggers are specified for the partition are reached (see Enable and Configure MLM PreScan and PostScan on page 182).

> **Note:** PostScan and Spectra SKLM encryption key management cannot be configured for use in the same partition.

Operational Overview PostScan, which has three operation options—FullScan, QuickScan, and QuickScan using a Global Spare, performs a read verification test on each LTO cartridge in the partition to check the data integrity and identify media errors that can impact the library's ability to restore data. The FullScan and QuickScan using a Global Spare options use an LTO-4 or later generation Global Spare drive assigned to the partition; the QuickScan option uses an LTO-4 or later generation drive assigned to the partition.

All three PostScan options operate as a background process performed by the library independent of the storage management software normally used to read and write data to the tape. You can configure a partition to run PostScan automatically (see Enable and Configure MLM PreScan and PostScan on page 182) or you can start the PostScan process manually. For automatic scans you can set the scanning frequency and select the PostScan option to use.

Using FullScan on tapes that are written using variable-length block sizes is not recommended.

Prerequisites for Starting a PostScan Operation When an MLM-enabled cartridge meets the PostScan trigger criteria configured for the partition, the cartridge is added to the PostScan queue. The queue is processed in a first-in-first-out (FIFO) basis.

> **Note:** The automatic PostScan triggers only apply to MLM-enabled LTO cartridges. LTO cartridges that are not MLM-enabled must be manually added to the PostScan queue (see Schedule a Manual PostScan on page 258).

Before beginning the PostScan process, the library verifies that the following prerequisites are met:

- The system is idle for the period of time specified for the partition (see Enable and Configure MLM PreScan and PostScan on page 182).
- The library is not currently in a PostScan blackout period (see Configure PostScan Blackout Periods on page 246).

- If either **Full Scan** or **QuickScan with Spare Drives** is enabled, an LTO-4 or later generation Global Spare drive assigned to the partition must be available.

  —OR—

  If **QuickScan** is enabled, an LTO-4 or later generation drive in the same partition as the cartridge that met the PostScan trigger criteria is available.

PostScan Cartridge Processing If the PostScan prerequisites are met, the library inserts the first cartridge in the PostScan queue into an available drive. The cartridges in the PostScan queue are processed on a First In, First Out (FIFO) basis. Depending on the PostScan option selected for the partition, the drive loads the cartridge and begins one of the following operations to check for media errors.

Notes:
- PostScan reads the data on the tape but does not process this data into a usable form. It simply verifies that it can read the data from the tape.
- See Enable and Configure MLM PreScan and PostScan on page 182 for additional information about the differences between the FullScan and QuickScan processes.

This PostScan option...	Uses...
FullScan	A Global Spare drive assigned to the partition. FullScan verifies all of the data on the tape, from the beginning of the tape (BOT) to the end of the recorded data (EOD) or the physical end of the tape, whichever comes first. **Notes:** ▪ If the partition uses LTO-4 drives, FullScan is the only available option. ▪ A Global Spare drive must be assigned to the partition. ▪ The cartridge does not appear on the BlueScale inventory screens while it is being scanned. If the cartridge is requested by the storage management software it is immediately ejected from the drive that is performing the verification and moved to the location requested by the storage management software. A system message is posted to indicate that the FullScan operation was interrupted. The cartridge is returned to the top of the PostScan queue and is the first one processed after it is returned to its slot. ▪ The Global Spare drive cannot be activated while FullScan is running. You must first pause the PostScan process (see Pause the PostScan Process on page 261). The library immediately aborts the FullScan currently in progress and returns the cartridge to its original location. You can then activate the Global Spare drive (see Using a Global Spare Drive on page 409). The aborted FullScan process resumes when the Global Spare drive is again available. ▪ The time to complete a FullScan depends on the type and amount of data on the tape and whether it was written using fixed- or variable-length blocks. ▪ Using FullScan on tapes that are written using variable-length block sizes is not recommended.

This PostScan option...	Uses...
QuickScan	One of the LTO-4 or later generation drives in the partition. QuickScan verifies all of the data on a single wrap, from the beginning of the tape (BOT) to the end of the wrap or the end of recorded data (EOD), whichever comes first. **Notes:** ▪ If a Global Spare drive is not assigned to the partition, a QuickScan using one of the partition's drives is the only option available. ▪ If possible, the library avoids using the drive from which the cartridge was most recently unloaded to perform the QuickScan. ▪ A QuickScan using a partition's drive is limited to three minutes. If the QuickScan exceeds this time limit, the operation is aborted and the cartridge is returned to its slot. The library posts a message stating that the QuickScan failed. Use FullScan to verify the cartridge. ▪ While QuickScan is running, all other moves in the partition are delayed until the scan is complete.
QuickScan using a Global Spare	An LTO-4 or later generation Global Spare drive. QuickScan verifies all of the data on a single wrap, from the beginning of the tape (BOT) to the end of the wrap or the end of recorded data (EOD), whichever comes first. **Notes:** ▪ The cartridge does not appear on the BlueScale Inventory screen while it is being scanned. If the cartridge is requested by the storage management software it is immediately ejected from the drive that is performing the verification and moved to the location requested by the storage management software. A system message is posted to indicate that the QuickScan operation was interrupted. The cartridge is returned to the top of the PostScan queue and is the first one processed after it is returned to its slot. ▪ The Global Spare drive cannot be activated while a QuickScan using Global Spares is running. You must first pause the PostScan process (see Pause the PostScan Process on page 261). The library immediately aborts the QuickScan currently in progress and returns the cartridge to its original location. You can then activate the Global Spare drive (see Using a Global Spare Drive on page 409). The aborted QuickScan process resumes when the Global Spare drive is again available. ▪ A QuickScan using a Global Spare drive is limited to ten minutes. If the QuickScan exceeds this time limit, the operation is aborted and the cartridge is returned to its slot. The library posts a message stating that the QuickScan failed. Use FullScan to verify the cartridge.

Updating the MLM Database When the PostScan process on a cartridge is complete, the library writes the scan date and a pass/fail test result to the cartridge MAM and updates the MLM database with the scan date, the pass/fail test result, and when (or if) the next scan should occur. The drive then unloads the cartridge and the library returns it to its original slot. The library posts a system message showing that the cartridge was scanned. If the QuickScan option was used, the library reports that the unload move for the backup operation that preceded the QuickScan operation is complete.

Global Spare Drive Cleaning If either the FullScan or QuickScan using a Global Spare option was used, the library checks to see if the drive requires cleaning after the cartridge is unloaded from the Global Spare drive. If cleaning is required and a cleaning partition is associated with the storage partition to which the Global Spare is assigned, the drive is cleaned before the next cartridge is processed.

Note: If a cleaning partition is not present, periodically check the Drive Details screen for each drive to determine whether cleaning is required. If cleaning is required, follow the instructions in Manually Cleaning a Drive on page 446.

Meet Requirements for Configuring and Using PostScan

As you configure PostScan and prepare to use it, keep the following information in mind:

Consideration	Description
Drive Firmware	▪ LTO-4: requires 97F9 or later firmware. ▪ LTO-5: requires B171 or later firmware. ▪ LTO-6 and later: supported with any firmware.
Updating MLM Data on MAM	Updating the cartridge MAM requires the cartridge to be write-enabled. **Important:** If a cartridge is write-protected when it is inserted into a drive, the information about the cartridge is added to the MLM database, but the library cannot update the MLM information on the cartridge's MAM.
Drive Support for PostScan	LTO-4 or later generations: Both FullScan and QuickScan are available when using LTO-4 or later generation drives. **Note:** While a drive is in use for QuickScan operations, it is unavailable to the storage management software.
Background Operations	To protect you from making changes that could negatively impact the library's operation, the BlueScale software automatically prevents you from performing certain operations while either a FullScan or a QuickScan that uses Global Spare drives is running. However, you can pause the FullScan or a QuickScan operation if you cannot wait for it to complete. See Background Operations on page 240 for detailed information.
Storage Management Software Configuration	When using automatic PostScan to check your cartridges, configure your storage management software to allow at least 15 minutes for a requested move to complete. If a cartridge is in the process of being scanned when it is requested for a backup or restore operation, it must be unloaded from the Global Spare and moved to another drive before the move request is reported as complete.
Global Spare Drives	Both FullScan and QuickScan using Global Spare require a Global Spare drive. Although a Global Spare drive can be shared by multiple partitions, assigning a separate Global Spare drive to each partition is recommended. Each partition can then perform PostScan whenever the prerequisites are met, without waiting for PostScan in another partition to complete.

Consideration	Description
Blackout Periods	Because the storage management software can potentially request a tape that is currently undergoing verification, you can configure blackout periods during which the PostScan operation is suspended. Configuring blackout periods ensures that PostScan does not operate during your normal backup window. The blackout periods apply to all of the storage partitions in the library. See Configure PostScan Blackout Periods on page 246 for instructions.
Cleaning Partitions	The PostScan feature cannot be enabled for a cleaning partition and does not affect cleaning tapes.

Enable PostScan

PostScan is enabled by selecting one of the PostScan options and one or more scan triggers when you configure a partition (see Enable and Configure MLM PreScan and PostScan on page 182). The available PostScan options depend on which generation of drives are in the partition and whether or not a Global Spare drive is assigned to the partition.

Important PostScan is enabled and configured for each individual partition. PostScan does not operate until the PostScan option is selected and one or more triggers are specified for the partition are reached.

Schedule a Manual PostScan

The automatic PostScan triggers only add MLM-enabled LTO data cartridges to the PostScan queue. However, cartridges can also be added to the PostScan queue manually. This is especially useful if your library contains LTO cartridges that are not MLM-enabled. You can also use the manual PostScan process to verify a suspect MLM-enabled cartridge even if it was previously scanned.

Cartridges that are manually added to the PostScan queue are processed before cartridges that were added as a result of the trigger criteria for the partition. They are processed using the PostScan option that was specified for the partition.

Use the following steps to manually start the PostScan process.

1. Click **MENU**, then select **Maintenance ⋯⁘ MLM**. The Media Lifecycle Management Tools screen displays.

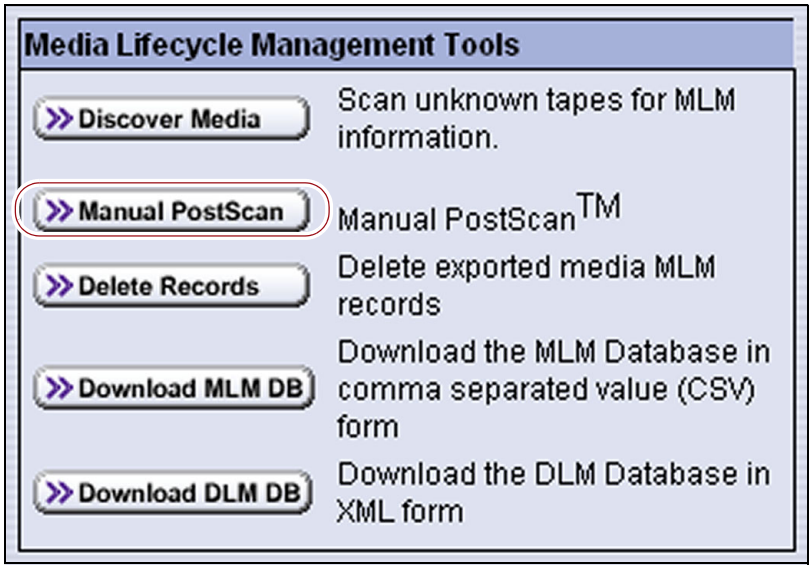


Figure 164 Click **Manual PostScan** on the Media Lifecycle Tools screen.

2. Click **Manual PostScan**. The Select Partition screen displays.

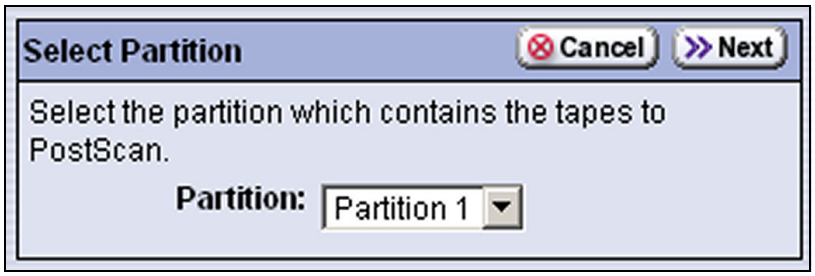


Figure 165 Select the partition containing the cartridges to add to the PostScan queue.

3. Select the desired partition from the **Partition** drop-down list.

4. Click **Next**. The Select Tapes screen displays.

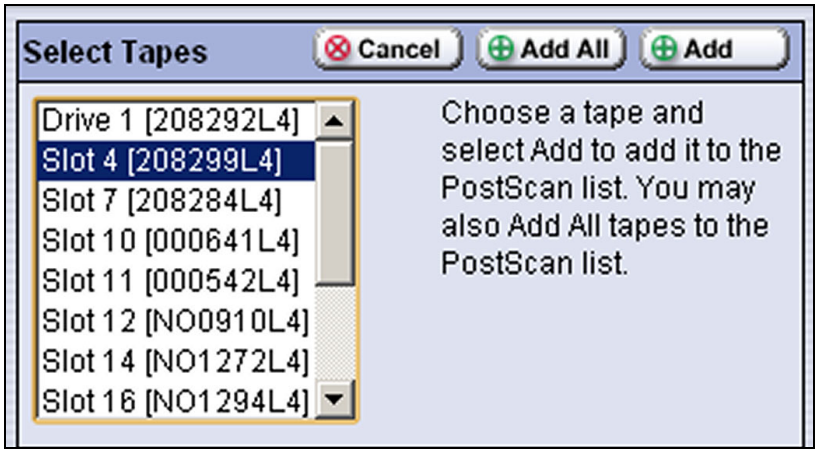


Figure 166 Select the cartridges to be added to the PostScan queue.

5. Select the cartridge that you want to check for media errors.
6. Click **Add** to add the selected cartridge or click **Add All** to add all of the cartridges listed to the PostScan queue. The Tapes to PostScan screen displays.

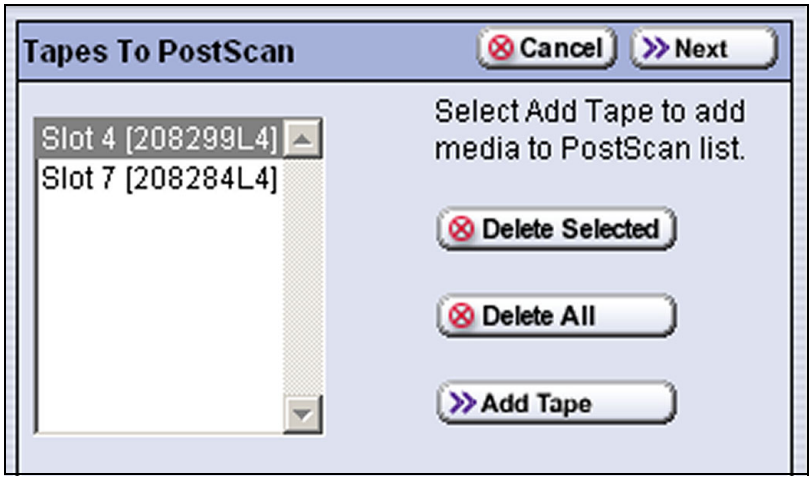


Figure 167 The Tapes To PostScan shows the cartridges currently in the PostScan queue.

7. If you want to add additional cartridges to the list of cartridges to be scanned, click **Add Tape** and repeat Step 4 though Step 6.

   Note: If you want to remove one or more cartridges from the list of cartridges scheduled to be scanned:

   - Select the cartridge and click **Delete** to remove it from the list.
   - Click **Delete All** to remove all of the cartridges from the list.

8. Click **Next** to queue the selected tapes for the PostScan process. The PostScan process begins when all of the prerequisites are met (see Prerequisites for Starting a PostScan Operation on page 254).
9. Click **Finish** to return to the Media Lifecycle Management Tools screen.

Pause the PostScan Process

If you need to perform any of the operations listed in Background Operations on page 240 or if you need to reset the library, you can pause the PostScan process. The library returns any cartridges currently being scanned to their original locations.

Important Pausing PostScan affects all partitions that are configured to use PostScan.

Use the following steps if you need to temporarily pause the PostScan process.

1. Click **MENU**, then select **Maintenance ⋯⁝ MLM.** The Media Lifecycle Management Tools screen displays.

   Note: The **Pause PostScan** button is only present if the PostScan process is running.

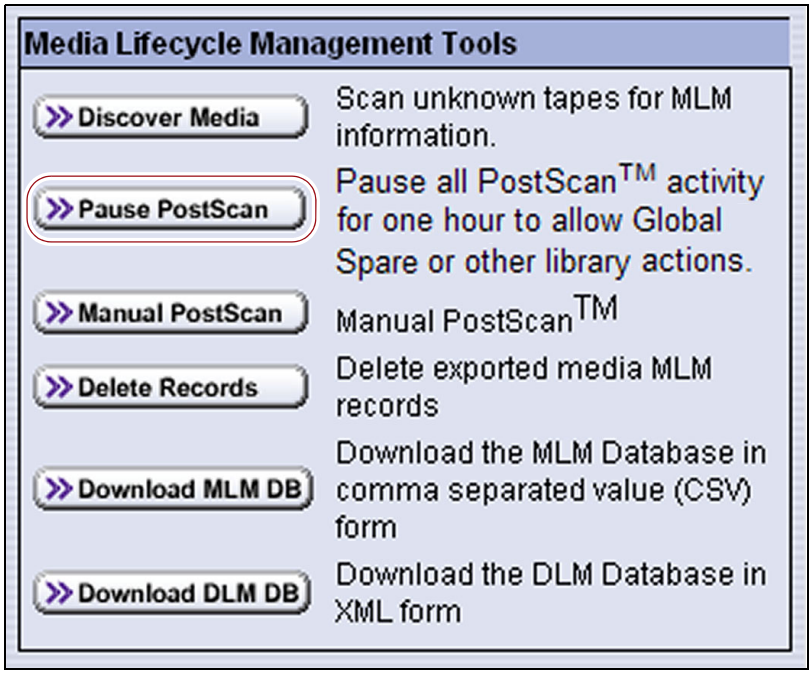


Figure 168 Click **Pause PostScan** on the Media Lifecycle Management Tools screen.

2. Click **Pause PostScan** to pause the PostScan operation for one hour so that you can use the Global Spare or perform other library operations.

   After an hour passes, the library restarts the PostScan operation on the tape that was being verified at the time of the interruption, provided the PostScan prerequisites are met (see Prerequisites for Starting a PostScan Operation on page 254).

USING MLM REPORTING

After the LTO cartridges in your library are added to the MLM database, you are ready to make use of this powerful tool to manage, track, and report all facets of tape usage from creation to retirement.

Generate MLM Reports

1. Log into the library.
2. Click **MENU**, then select **General** ⋯ **MLM**. The MLM Reports screen displays.
3. Select either **Total Library** or a specific partition from the **Partition** drop-down list, and then click **Go**.

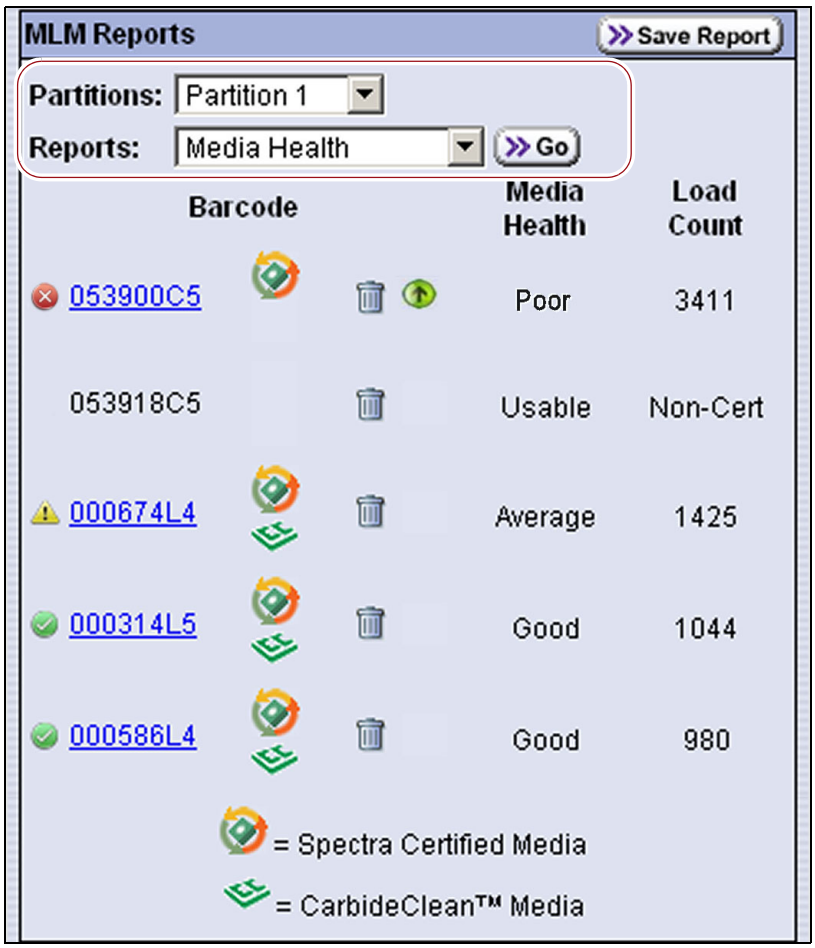


Figure 169 Select the partition and the type of report you want to display.

4. Select the type of report you want from the **Report** drop-down list.

Notes:
- Many of the MLM reports are not available for non-MLM-enabled cartridges.
- Information about MLM-enabled cleaning cartridges only appears in the Exported Media, Cleans Remaining, and Born on Date reports.

This report...	Shows...
Media Health	▪ The barcode label information, the overall health (media health), and the load count (the number of times the cartridge was loaded into a drive) for each MLM-enabled cartridge in the selected location. ▪ The barcode label information for each non-MLM-enabled cartridge and whether the cartridge appears to be usable or impaired.
Remaining Capacity	The remaining capacity and maximum capacity for each MLM-enabled data cartridge. The capacity reflects the native capacity of the cartridge, not the compressed capacity. **Notes:** ▪ Until a data cartridge is loaded into, threaded, and then unloaded from a drive for the first time, its remaining capacity and maximum capacity report as "0". ▪ The remaining capacity and maximum capacity for a cartridge are displayed as GB or TB. ▪ This report does not include information about non-MLM-enabled cartridges.
Load Count	The load count for each MLM-enabled data cartridge in the selected location and the born on date (the date on which Spectra Logic enabled the cartridge to support MLM tracking and reporting). **Note:** This report is not available for non-MLM-enabled cartridges.
Write Errors	The number of soft errors and the load count for each MLM-enabled data cartridge. **Note:** This report is not available for non-MLM-enabled cartridges.
Cleans Remaining	The number of cleanings remaining and the born on date for each MLM-enabled cleaning cartridges. **Note:** This report is not available for non-MLM-enabled cartridges.
Born on Date	The date that the MLM-enabled cartridge (both data and cleaning) was created and certified by Spectra Logic and the load count for each cartridge. **Note:** This report is not available for non-MLM-enabled cartridges.
Exported Media	A list of all the MLM-enabled cartridges (both data and cleaning) that were exported from the library, sorted by the export time (oldest first). The report also shows the user name of the person who exported the media. **Note:** This report is not available for non-MLM-enabled cartridges.
Last Write Time **Last Read TIme**	Shows the time and date for the most recent write and read operations for each MLM-enabled data cartridge. **Note:** This report is not available for non-MLM-enabled cartridges.

5. Click **Go**. The MLM Reports screen refreshes to display the selected report with a list of the barcode labels for all media in the selected location. A media health icon indicates the overall health of each MLM-enabled cartridge as of the last time it was loaded into a drive.

   Note: Health icons are not used with LTO media that is not MLM-enabled.

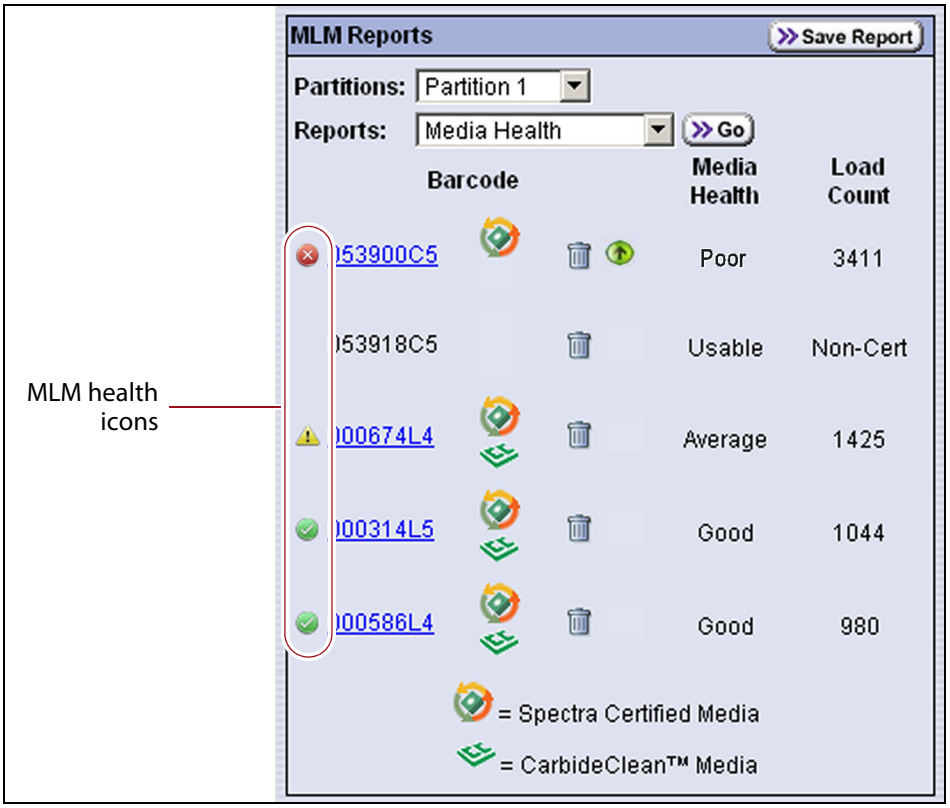


Figure 170 Use the health icons on the MLM Reports screen to quickly assess media health.

The following table describes the meaning of each media health icon. Select the barcode next to the icon to view detailed information about that specific cartridge.

Icon	Health score	Meaning
	100 – 80	The media health is **Good**. ▪ **Data cartridge:** The media is in good condition and operating properly. The cartridge can be used for writing data and reading previously written data. ▪ **Cleaning cartridge:** More than ten cleaning cycles remain on the cartridge.
	79 – 50	The media health is **Average.** ▪ **Data cartridge:** When the Health graph on the Details screen for the cartridge falls below a health score of 80, the media health icon changes from green to yellow (generally due to normal aging). For maximum reliability, only use the cartridge for restores. ▪ **Cleaning cartridge:** The cleaning cartridge is near expiration. From one to ten cleaning cycles remain.
	49 – 0	The media health is **Poor**. ▪ **Data cartridge:** When the Health graph on the Details screen for the cartridge falls below a health score of 50, the media health icon changes to red. The combination of media errors, tape age, and usage indicates that the media reached the end of its useful life for reliable data backups and restores and should be retired. If you are experiencing an unexpected number of cartridges with poor media health, you may want to investigate further: ▪ Review the media health data for each cartridge to see if it has a high error rate. A high error rate can indicate either that the media health is poor and the cartridge should be retired or that the cartridge was written to by a drive that is having trouble. ▪ If multiple cartridges with high error rates are written to by the same drive, the drive may be the source of the errors. Clean the drive or, if necessary, replace it. **Notes:** ▪ If the source of the high error rate is a drive, the media health icon for the affected cartridges should return to either green or yellow after approximately three load/read or write/unload cycles in a known good drive. ▪ If your cartridge has a high error rate that cannot be attributed to a faulty drive, environmental factors, or the end of the cartridge's normal working life contact Spectra Logic Technical Support for troubleshooting assistance (see Contacting Spectra Logic on page 7). ▪ **Cleaning cartridge:** The cleaning cartridge is expired. No more cleaning cycles remain. Replace the cleaning cartridge.
		The media health is **Unknown.** The status of the media cannot be determined.

6. If you want to view detailed information about a specific cartridge, scroll through the list of cartridges on the MLM Reports screen to locate the barcode of the desired cartridge.

7. Click the cartridge barcode to view detailed information about the cartridge. The Details screen for the selected cartridge displays.

   Notes:
   - The health score for a cartridge is based on the MLM-tracked history of the cartridge. The health indicated by the Health graph on the Details screen may fluctuate until the cartridge is loaded six times.
   - Environmental Statistics — For LTO-9 media or LTO-8 media used in an LTO-9 drive, environmental information for the time the tape was in the drive displays.

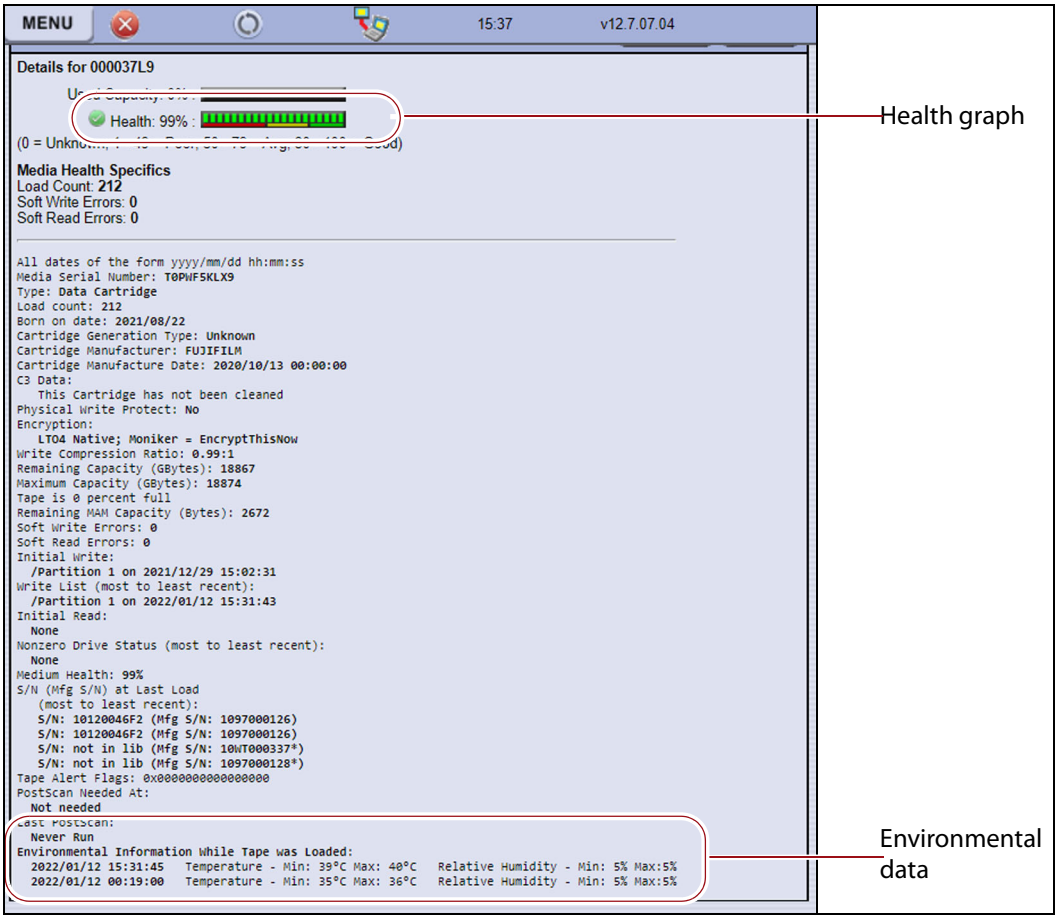


Figure 171 The detailed MLM report for the selected media.

8. Click **Previous** to return to the main MLM Reports screen (Figure 170 on page 264).

Save an MLM Report

You can select to save a copy of the MLM report, which is a comma-separated text file (*.rpt), to a USB device, email the saved report to previously configured mail user, or both. If desired, you can zip the file before saving it.

Note: You can also download the MLM database as a comma separated value (CSV) file (see Download the MLM Database for Analysis and Archiving on page 277).

1. Generate the desired report as described in Generate MLM Reports on page 262.
2. If you want to save the MLM report to a USB device, connect the device to the LCM's USB port and allow time for the device to mount before continuing.

   Note: The option to save the report to USB is only available if you plug a USB device into the LCM's USB port before you click **Save Report** on the MLM Reports screen.

3. Click **Save Report** on the MLM Reports screen to display the Save MLM Report screen.

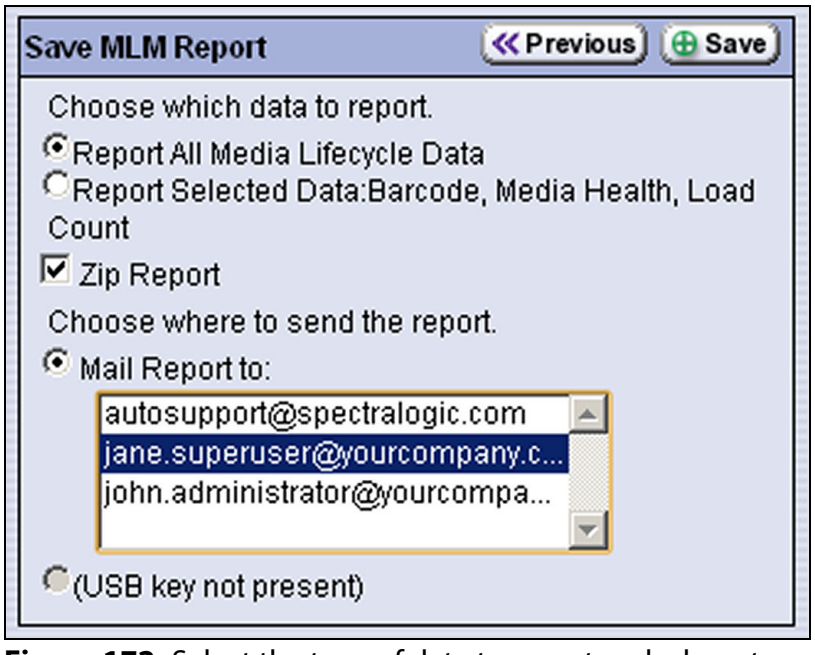


Figure 172 Select the type of data to report and where to save the report.

4. Select the data to include in the saved report and how you want the report saved.

   Note: If you want to email the report, the intended recipient must be a previously configured mail user (see Configure Mail Users on page 107).

This option...	Saves...
Report All Media Lifecycle Data	A report containing all of the available detailed MLM data for MLM-enabled media in the selected location (a specific partition or the total library). **Note:** Depending on the number of cartridges in the selected location, this report can be quite large.
Report Selected Data	Only the fields displayed in the report that you selected on the MLM Reports screen (Figure 170 on page 264). **Note:** The headings in the saved report reflect the fields displayed in the report you selected in the MLM Reports screen.
Zip Report	The report as a zip file which is compatible with standard file compression software. Zipping the report is especially useful when emailing the Report All Media Lifecycle Data report. **Note:** If you unzip the report using the standard format used by most file-zipping applications, the application creates the following directory structure: *\hard disk\lc\reports.
Mail Report to	The report and attaches it to an email sent to a previously configured mail user. Use the drop-down list to select the recipient for the report file. **Note:** Do not use the default autosupport@spectralogic.com email user. Spectra Logic does not save emailed MLM report files unless they are specifically requested for troubleshooting.
Save to USB	The report to the USB device. **Note:** The USB option is only available if you plugged a USB Device in to the LCM's USB port before you selected **Save Report** on the MLM Reports screen.

5. Click **Save** to send the report to the selected destination. Click **Previous** to return to the MLM Reports screen without sending the report.

Override a Poor Cartridge Health Report

Under certain circumstances you may need to override the health of an MLM-enabled cartridge that is reported as poor (a red health icon appears next to the cartridge barcode). When the cartridge health is poor, a green arrow button appears, that can be used to override the reported health.

During the override process, the library progressively eliminates any recent hard errors from the tape health calculation. If the health is still red, all hard errors are eliminated from the tape health calculation. The library continues to use this adjusted tape health until the cartridge health returns to either Good or Average as part of normal health monitoring.

Important Do not reset the cartridge health unless you believe that the reported poor health is due to drive problems and not the cartridge or you are specifically directed to do so by Spectra Logic Technical Support.

Use the following steps to reset the health of a single cartridge.

1. Display the MLM Reports screen as described in Generate MLM Reports on page 262.
2. Locate the barcode of the cartridge for which you need to reset the health (see Step 7 on page 266).
3. Click the green arrow button for the cartridge. The library adjusts parameters used to calculate the tape health until the reported health is Average.

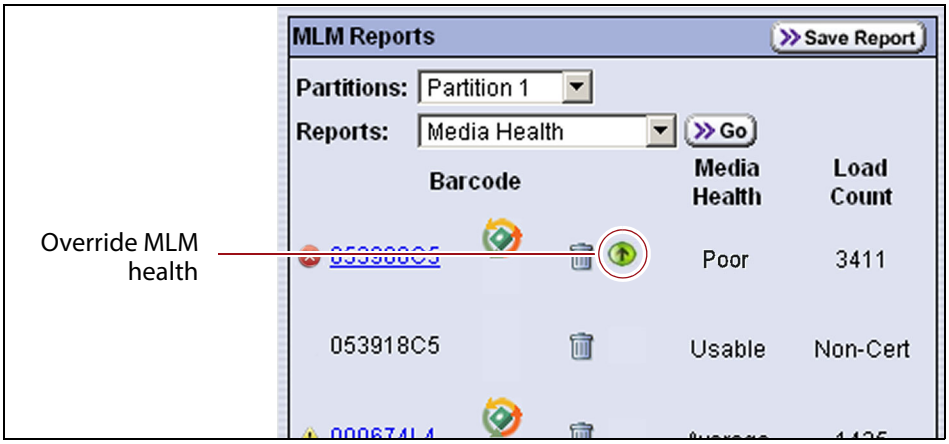


Figure 173 Select the green override button to reset the reported health for an MLM-enabled LTO cartridge.

4. Attempt to resolve the issues that were causing the media health to be reported as poor.

MANAGING THE MLM DATABASE

The MLM database contains the usage and media health history, as well as the PostScan verification data, for all of the MLM-enabled cartridges in your library. It also contains the Drive Lifecycle Management data for all of the drives in your library (see Monitoring Drive Health Using DLM on page 280).

Deciding when and how often you back up the MLM database depends on many factors, including how often tapes are loaded into a drive.

- If all of the tapes are loaded into drives frequently, the MLM database can be rebuilt relatively quickly. The database can be backed up less frequently.
- If many of the tapes remain in the library without being loaded into a drive for a long period of time, or if tapes are exported and stay outside of the library for a long period of time, rebuilding the MLM database can take a long time. Back up the MLM database more frequently.

Back Up the MLM and DLM Databases

Based on your environment, determine how frequently backups are needed, then use the following steps to create a backup. You can choose to save the backup to a USB device or send it as an email attachment to a previously configured mail recipient.

1. Use your storage management software to stop all backup or restore operations on the library.

Important Backing up the MLM and DLM databases requires the library to be idle.

2. Log into the library as a user with superuser or administrator privileges.
3. If you want to save the backup of the MLM and DLM databases to a USB device, connect the USB device to the LCM and allow time for the device to mount; otherwise, skip to the next step.

4. Click **MENU**, then select **Maintenance** to display the Maintenance menu.

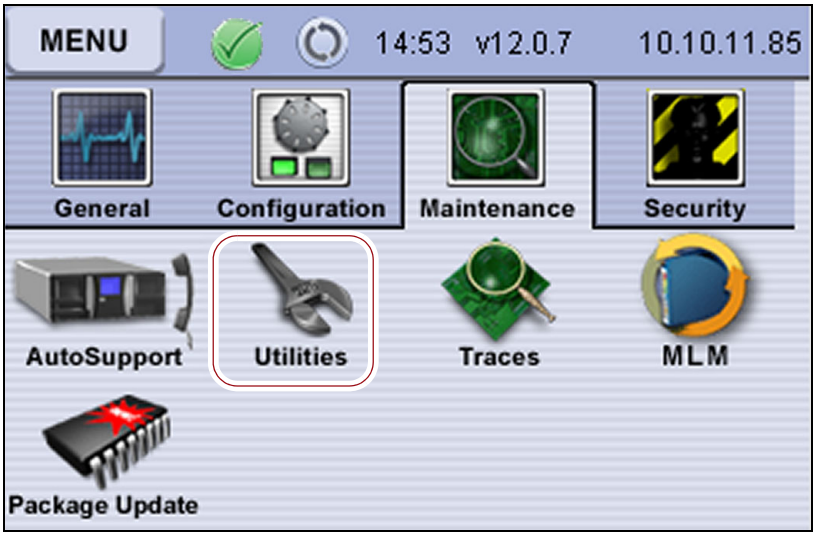


Figure 174 Click **Utilities** on the Maintenance menu.

5. Click **Utilities**. The Basic Utilities screen displays.

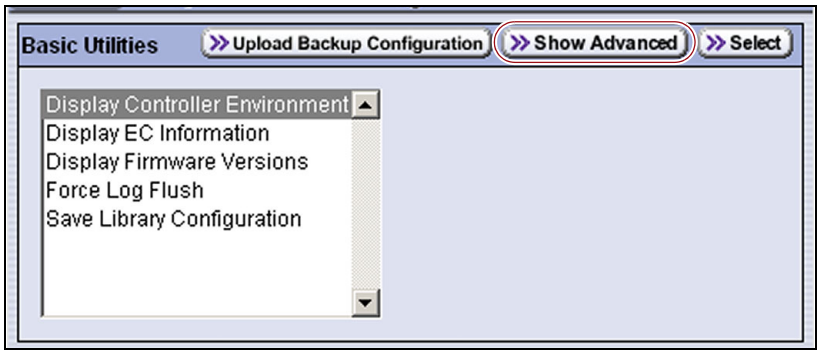


Figure 175 Click **Show Advanced** on the Basic Utilities screen.

6. Click **Show Advanced**. The Confirmation screen displays.
7. Click **Yes** to acknowledge the warning about using the advanced utilities. The Advanced Utilities screen displays.

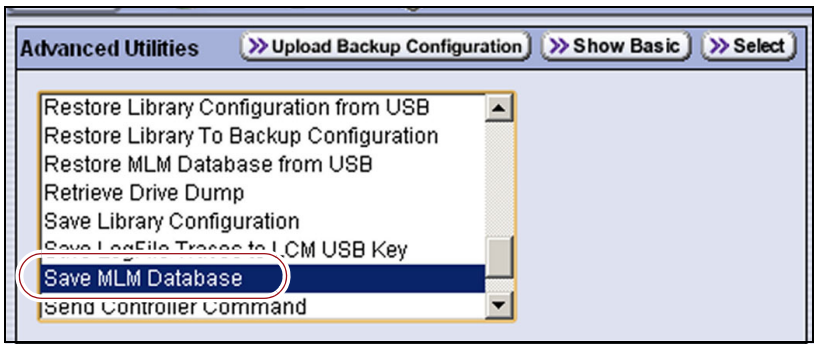


Figure 176 Select **Save MLM Database**.

8. Scroll down and select **Save MLM Database**, then click **Select**. The screen refreshes to show the details for the utility.

9. Click **Next** and select the destination for the saved file and whether to compress the file.

   a. Use the **Select the destination** scroll list to select where you want to save the database file.

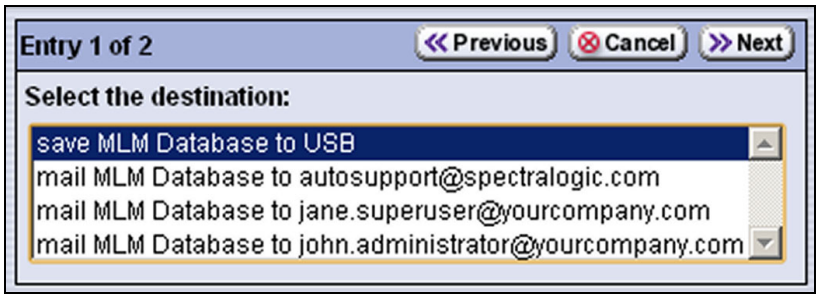


Figure 177 Select destination for the saved report.

Select this option...	To...
Save MLM Database to USB	Backup the MLM database to a USB device.
Mail MLM Database to...	Send the MLM database file as an email attachment to the specified mail recipient. **Notes:** ▪ Do not select autosupport@spectralogic.com as a recipient. Spectra Logic does not save emailed files unless they are specifically requested for troubleshooting. ▪ Only previously configured mail users are listed. To send the email to someone who is not listed, exit the utility, configure that person as an mail user (see Configure Mail Users on page 107), and then run the utility again.

   b. Click **Next** and select whether you want to compress the file to make it smaller.

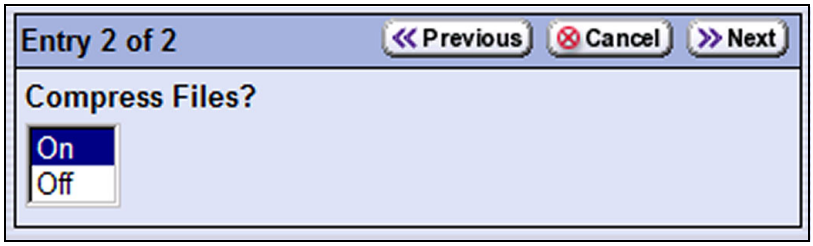


Figure 178 Select whether to compress the report.

10. Click **Next**. If you want to save the system message showing the result of the utility, select the destination.

    Note: This screen only relates to the system messages indicating that the utility completed successfully (or failed). They do not relate to the MLM database file itself.

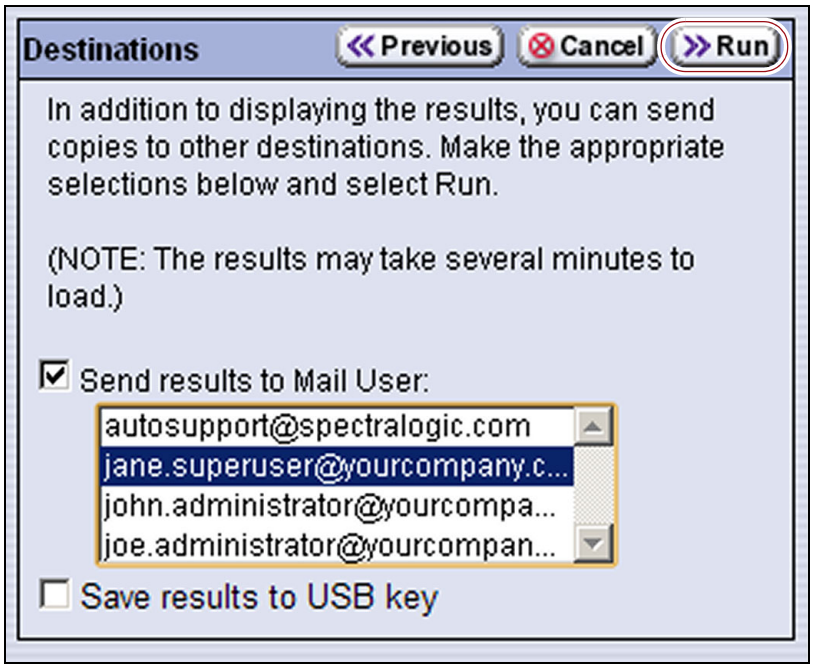


Figure 179 Click **Run** to save the MLM database to the specified destination.

Selecting this option...	Saves the results system message...
Send results to Mail User	As an attachment to an email sent to the specified mail recipient. Use the drop-down list to select the recipient for the report file. Only previously configured mail users are listed. To send the email to someone who is not listed, exit the utility, configure that person as an mail user (see Configure Mail Users on page 107), and then run the utility again. **Note:** Do not select autosupport@spectralogic.com as a recipient unless Spectra Logic Technical Support specifically asks you to send the results to them. Spectra Logic does not save emailed files unless they are specifically requested for troubleshooting.
Save results to USB key	To a USB device connected to the USB port on the LCM. **Note:** This option is only available if you inserted a USB device in Step 3 on page 270.

11. Click **Run**.

    After a brief delay, the Utility Results screen displays, showing that the database file was either saved or sent.

Verify the Database Backup File

After backing up the MLM database, use one of the procedures in the following table to confirm that the backup file was generated.

If the backup was...	Follow these steps...
Saved to a USB device	**1.** Plug the USB device into a PC that is not connected to the library. **2.** Examine the list of files on the USB device and locate the SavedMLMDB folder. **3.** Open the folder to verify that it contains one of the following files, where `<date-time>` is the time stamp for when the backup was created: ▪ `cminfo_<date-time>.zdt` (if you chose to compress the file in Step 9 on page 272) —OR— ▪ `cminfo_<date-time>.dat` (if you chose not to compress the file) **4.** Make sure that the file is more than 0 bytes in size. **5.** If a file with the correct filename format is present and is more than 0 bytes in size, the database backup was successful and the file is usable. Store the USB device in a safe location. **6.** If the MLM database file is not present or if it is 0 bytes in size, repeat the backup process (Back Up the MLM and DLM Databases on page 270) using a different USB device.
Sent as an email attachment	**1.** Open the email attachment and verify that: ▪ The attachment contains a zip file called `cminfo_<date-time>.zdt` —AND— ▪ The file is more than 0 bytes in size. **2.** If the zip file is present and is more than 0 bytes in size, the backup was successful and is usable. Save the email attachment to a safe location from which you can copy it to a USB device, if needed. **3.** If the zip file is not present or if it is 0 bytes in size, repeat the backup process (Back Up the MLM and DLM Databases on page 270) to generate the email again.

Delete MLM Records From the Database

The MLM database is limited to a maximum of 100 records. When this maximum is reached, the record for the least recently exported cartridge, as determined by the Export Date tracked by MLM, is automatically deleted. The library does not notify you when it reaches the maximum number of records.

When a tape is retired or permanently exported from the library, you can manually delete its record from the MLM database. Records can be deleted individually or as a group.

Delete an Individual Record

If you only need to delete one or two cartridges from the MLM database, you can use the MLM Reports screen to delete individual records.

1. Log into the library as a user with superuser or administrator privileges.
2. Display the MLM Reports screen as described in Generate MLM Reports on page 262.
3. Locate the barcode of the cartridge you want to remove from the MLM database (see Step 7 on page 266).

   Note: An asterisk (*) next to the barcode indicates that the cartridge was exported from the library.
4. Click the trash can icon next to the barcode to delete the record.

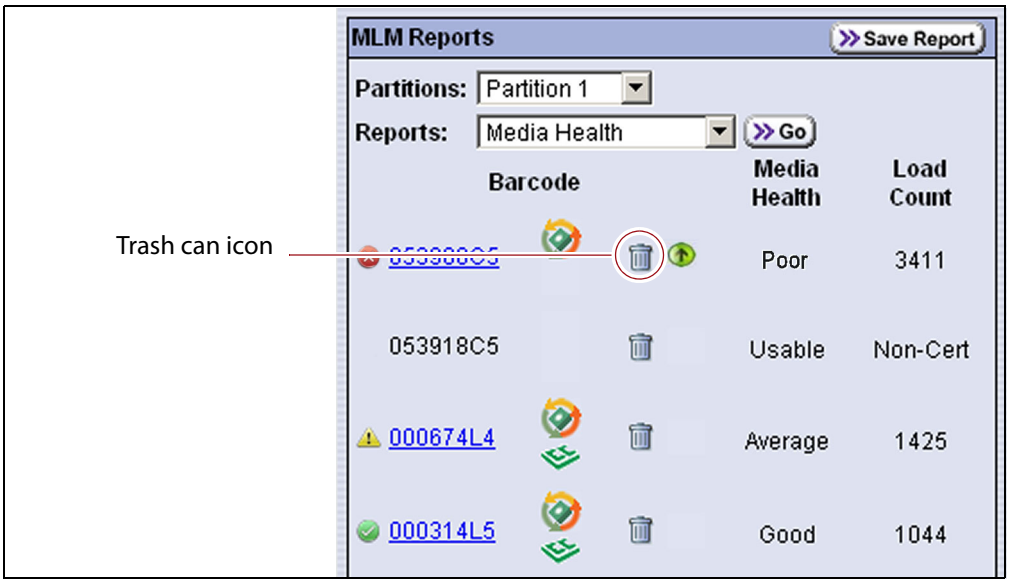


Figure 180 Click the trash can icon to delete an individual record from the MLM database.

5. Respond to the confirmation message to delete the record.

Delete Multiple Records

1. Log into the library as a user with superuser or administrator privileges.
2. Click **MENU**, then select **Maintenance ⋯⁘ MLM.** The Media Lifecycle Management Tools screen displays.

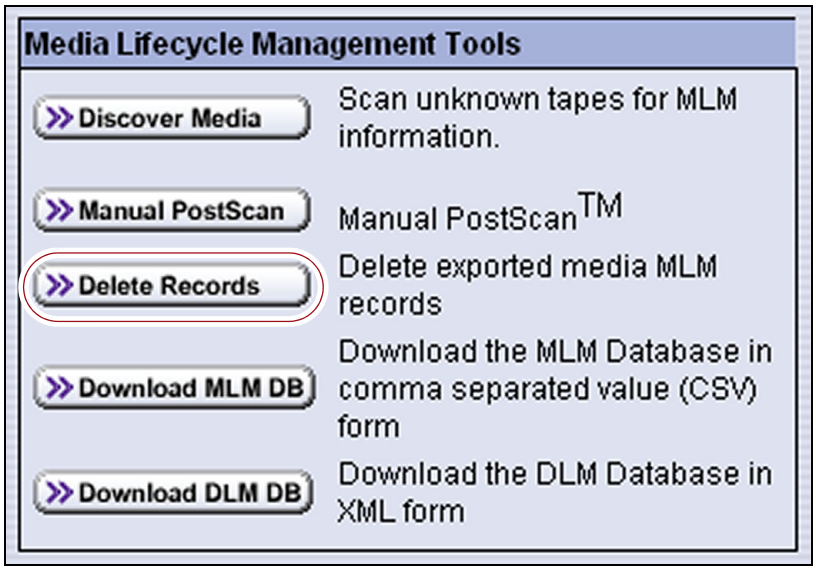


Figure 181 Click **Delete Records** to begin removing records from the MLM database.

3. Click **Delete Records**. The Delete MLM Records screen displays a list of the cartridges that were exported from the library.

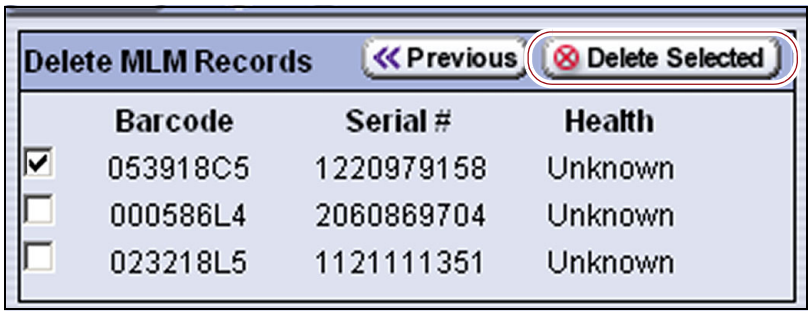


Figure 182 Select the cartridges to remove from the MLM database.

4. Select the cartridge records you want to delete from the MLM database.
5. Click **Delete Selected** to remove the selected records from the MLM database.

   Note: If you reimport a cartridge that was deleted from the MLM database, it must be rediscovered before it is once again included in the MLM database and MLM reports.

Download the MLM Database for Analysis and Archiving

If desired, you can download the MLM database as a comma separated value (CSV) file for analysis and archiving. You can then open the file in any software application that supports this type of file (for example, spreadsheet software) and view the information it contains.

Important The MLM information contained in the CSV file cannot be used to restore the MLM database. Always maintain a current backup of the MLM database as described in Back Up the MLM and DLM Databases on page 270.

Note: The **Download MLM DB** button is only available when you access the library using the BlueScale web interface (RLC). It is not available from the operator panel.

1. Log into the library as a user with superuser or administrator privileges.
2. Click **MENU**, then select **Maintenance** ⋯ **MLM**. The Media Lifecycle Management Tools screen displays.

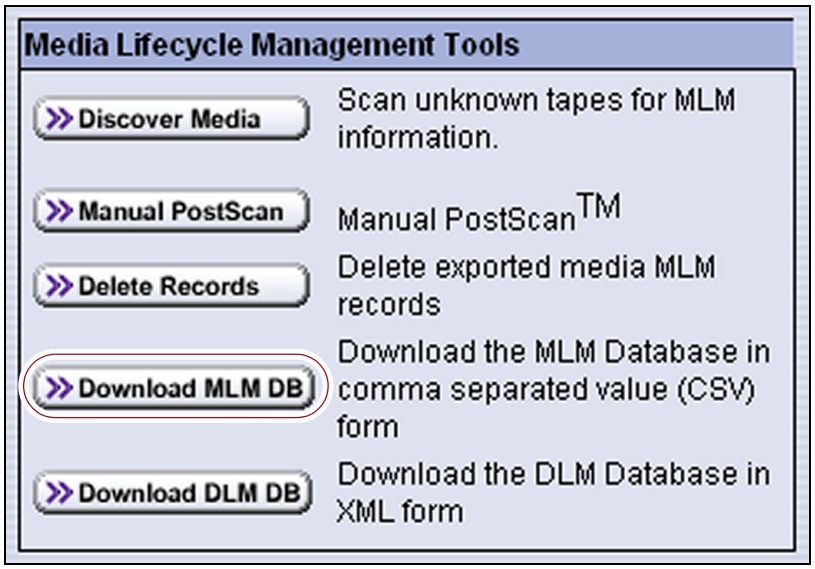
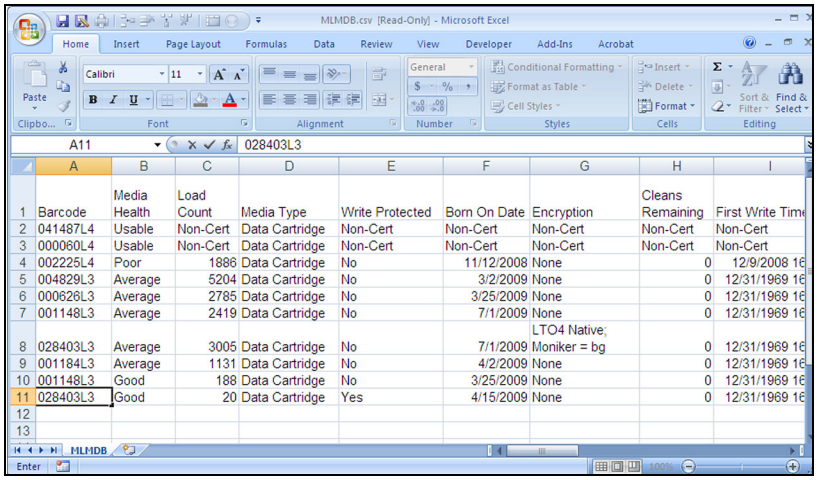


Figure 183 Click **Download MLM DB** to export the MLM database.

3. Click **Download MLM DB**.
4. To view the information stored in the MLM database, open the CSV file using a software program that supports this file type.



	A	B	C	D	E	F	G	H	I
1	Barcode	Media Health	Load Count	Media Type	Write Protected	Born On Date	Encryption	Cleans Remaining	First Write Time
2	041487L4	Usable	Non-Cert	Data Cartridge	Non-Cert	Non-Cert	Non-Cert	Non-Cert	Non-Cert
3	000060L4	Usable	Non-Cert	Data Cartridge	Non-Cert	Non-Cert	Non-Cert	Non-Cert	Non-Cert
4	002225L4	Poor	1886	Data Cartridge	No	11/12/2008	None	0	12/9/2008 16
5	004829L3	Average	5204	Data Cartridge	No	3/2/2009	None	0	12/31/1969 16
6	000626L3	Average	2785	Data Cartridge	No	3/25/2009	None	0	12/31/1969 16
7	001148L3	Average	2419	Data Cartridge	No	7/1/2009	None	0	12/31/1969 16
8	028403L3	Average	3005	Data Cartridge	No	7/1/2009	LTO4 Native; Moniker = bg	0	12/31/1969 16
9	001184L3	Average	1131	Data Cartridge	No	4/2/2009	None	0	12/31/1969 16
10	001148L3	Good	188	Data Cartridge	No	3/25/2009	None	0	12/31/1969 16
11	028403L3	Good	20	Data Cartridge	Yes	4/15/2009	None	0	12/31/1969 16
12									
13									

Figure 184 An example of the downloaded MLM database file (opened in Microsoft Excel).

CHAPTER 9

Using Drive Lifecycle Management

This chapter describes how to use BlueScale Drive Lifecycle Management to proactively monitor the health of the LTO drives in your library.

BLUESCALE DRIVE LIFECYCLE MANAGEMENT

Overview BlueScale Drive Lifecycle Management works in conjunction with MLM to help you identify drives that experience a high number of errors or other problems during operation.

Each time a cartridge is unloaded from a drive, the library collects the media health data from the drive. This data includes read/write errors, tape alerts, and flags generated during the time the most current cartridge was loaded in the drive. It also includes the current value for the drive's single character display (SCD) and any errors detected at the time the cartridge is unloaded. All of this data, plus the MLM data for the 50 most recently loaded cartridges, is stored in the DLM database. This data is used to generate an overall drive health status for the library, as well as health reports for each individual drive.

Enabling DLM BlueScale Drive Lifecycle Management (DLM) is automatically enabled when Media Lifecycle Management (MLM) is enabled and cannot be used without MLM. See Chapter 8 – Configuring and Using Media Lifecycle Management, beginning on page 233 for detailed information about enabling and using MLM.

Drive Health Reports A health icon next to each drive indicates the overall health of the drive. Detailed reports provide information about the cartridges that were loaded into the drive and any errors reported. The DLM database containing the health information for every drive in the library is backed up whenever the MLM database is backed up. The reports can also be saved and exported as XML files.

Drive Testing If a drive is experiencing problems, the DLM drive test wizard lets you test the basic functionality of the drive. This test, when used in conjunction with other DLM data and MLM data, can help you determine whether a drive or the media is the source of the errors you are investigating.

User Privilege Requirements Only a user with superuser or administrator privileges can access and use the DLM features. See Understanding User Groups and Security on page 94 for information about the three types of user groups and what types of privileges each has.

MONITORING DRIVE HEALTH USING DLM

When DLM is enabled, the Drives icon in the Configuration menu changes to the DLM icon.

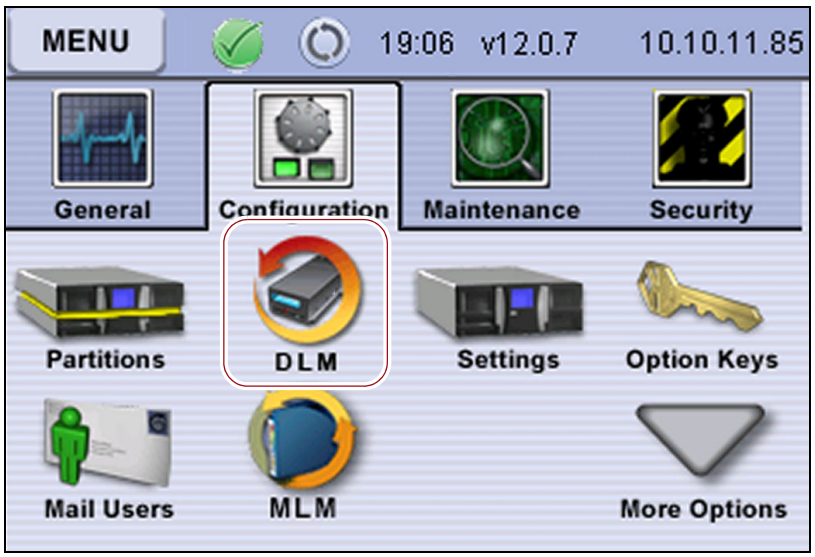


Figure 185 Enabling DLM changes the Drive icon to a DLM icon in the Configuration menu.

Selecting DLM from the Configuration menu displays the Drives screen, which uses health icons to provide at-a-glance information about the health of each drive in the library. From the Drives screen you can access detailed drive health reports for each drive in the library, as well as drive management tools.

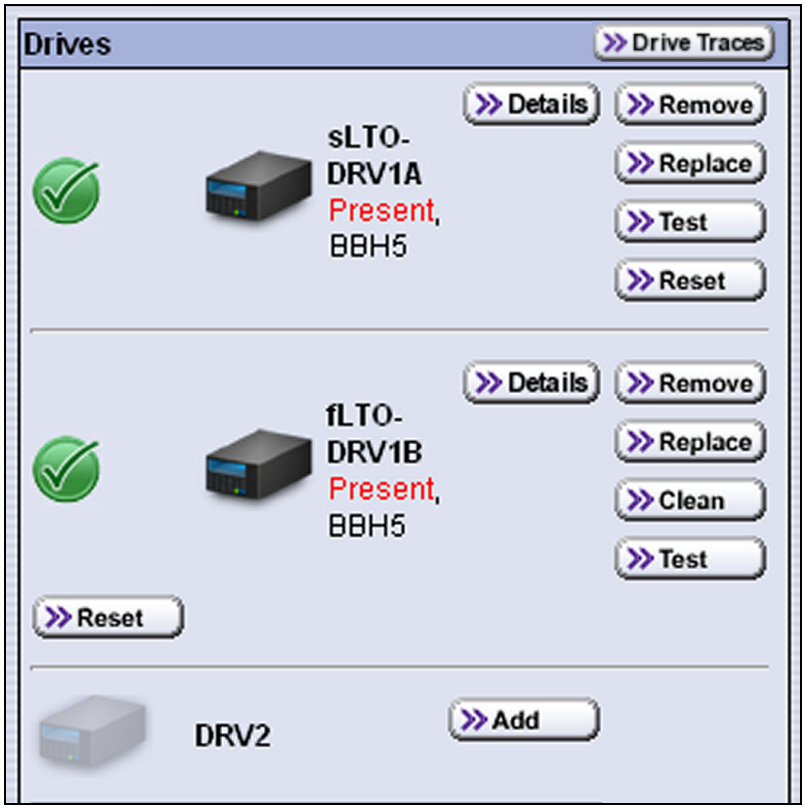


Figure 186 Use the health icons on the Drives screen for at-a-glance monitoring of drive health.

Each button on the Drives screen lets you perform additional operations.

This button...	Lets you...
Drive Traces	Collect drive traces for LTO-5 and later generation drives (see Use the Drive Traces Button on page 402).
Update All DLM Data	Refresh the DLM data for all of the drives in the library. **Note:** The **Update All DLM Data** button only displayed if Drive Lifecycle Monitoring is enabled (see Enabling MLM and Configuring Global Settings on page 242).
Remove **Replace** **Add**	Remove or replace a drive that is already in the library. If a DBA has an empty drive bay, the **Add** button powers on a newly installed drive and initializes it in the library (see Adding or Replacing a Drive on page 463). **Notes:** ▪ These buttons only display on the front panel. ▪ The **Add** button only displays if a DBA location does not contain a drive.

This button...	Lets you...
Clean	Clean the drive using a cleaning tape in an associated cleaning partition. See Manually Cleaning a Drive on page 446. **Note:** The **Clean** button only displays if the partition to which the drive is assigned has an associated cleaning partition.
Detail	View detailed information about the selected drive (see Viewing and Saving a Detailed Drive Health Report on page 284).
Test	Use the DLM Drive Test wizard to test a drive (see Using DLM to Test an LTO Drive on page 414).
Reset	Reset the drive, which power cycles the drive, runs the internal drive diagnostics, and reinitializes it in the library (see Resetting a Drive on page 408).

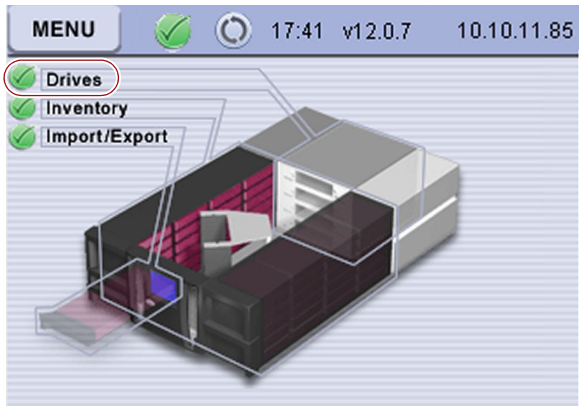
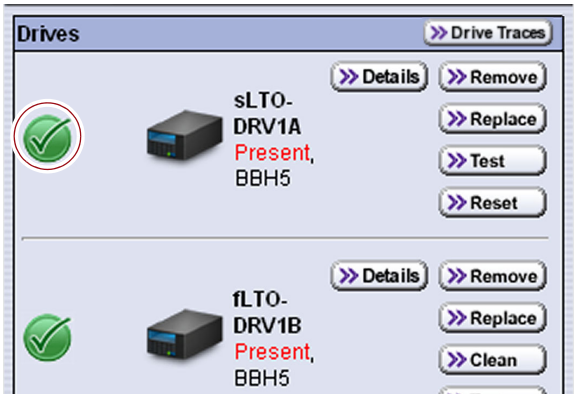
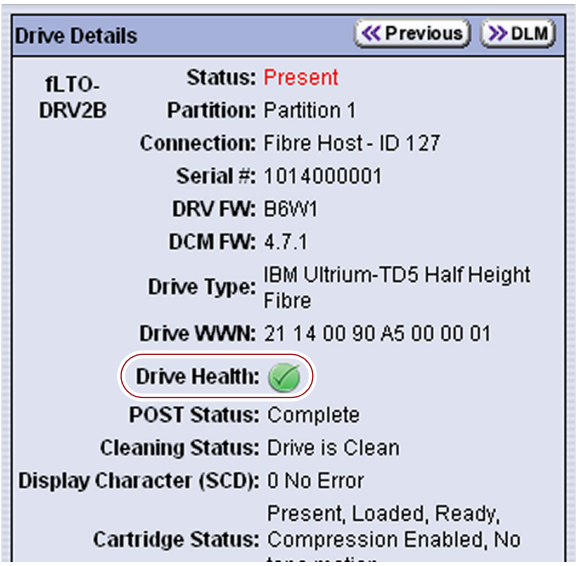
Using the Drive Health Icons

The drive health icons provide at-a-glance health status for the drives in the library. The drive health icon state is based on data collected for the drive when the last cartridge was loaded in the drive. This data consists of the code presented on the drive's SCD, as well as tape alerts, and errors detected at the time the tape is unloaded. See Interpreting the SCD Codes on page 394 for detailed information about the SCD codes for LTO drives. The following table describes the drive health status icons.

Note: Not all SCD codes have an associated DLM icon.

Icon	Meaning
	The drive health is **Good**. The drive is operating normally.
	The drive requires **Attention**. Use the SCD code information on the Drive Details screen to determine the type of action required.
	The drive health is **Poor**. The drive experienced an unrecoverable error or problem. Use the SCD code information on the Drive Details screen to determine the type of action required.
	The drive health is **Unknown.** The status of the drive cannot be determined.

The drive health icons appear on the following screens, as well as in the drive health reports (see Viewing and Saving a Detailed Drive Health Report on page 284).

The health icon on this screen...	Indicates...
General Status 	The overall drive health for the library. **Note:** The Drives health icon on the General Status screen reflects the lowest health score for any of the drives in the library.
Drives 	The overall health of each individual drive in the library.
Drive Details 	The health of the selected drive.

Viewing and Saving a Detailed Drive Health Report

1. Log into the library as a user with superuser or administrator privileges.
2. Click **MENU**, then select **Configuration** ···⁘ **DLM** to display the Drives screen.

Figure 187 Select **Details** to view detailed information about a drive.

3. Click **Details** next to the drive for which you want to view more information. The Drive Details screen displays.

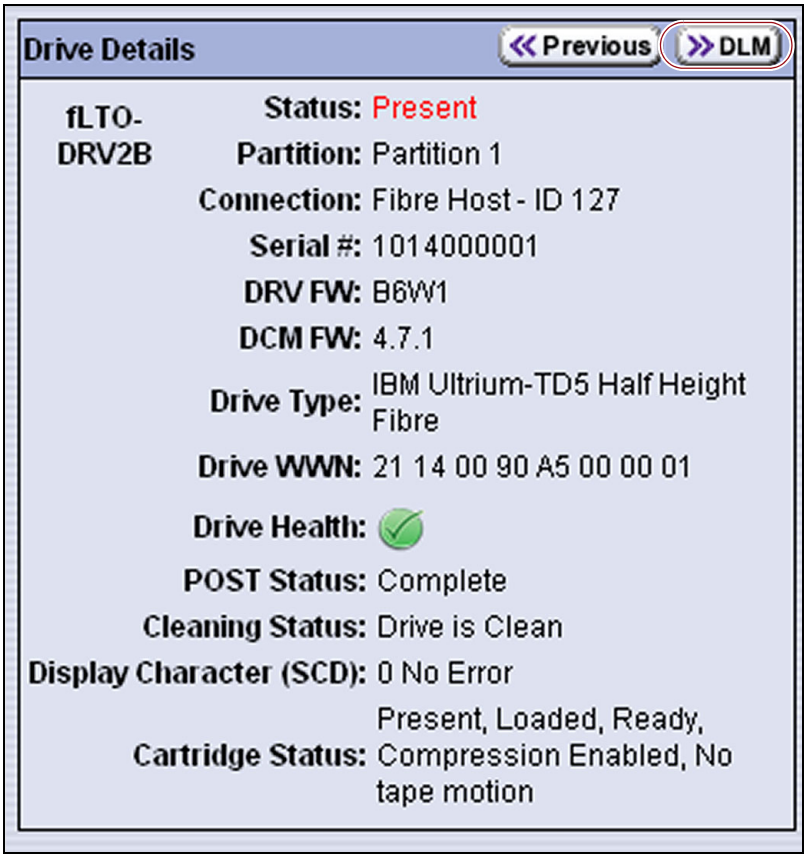
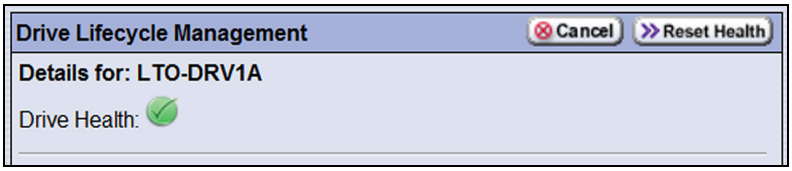
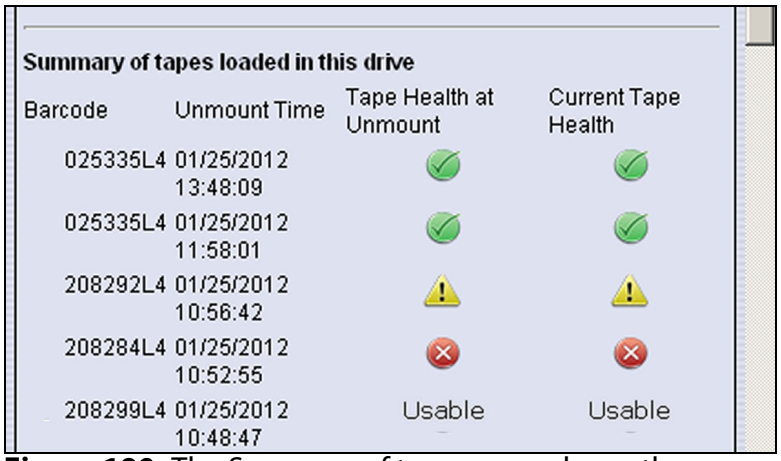


Figure 188 The Drive Details screen shows detailed information about the selected drive.

4. Click **DLM** on the Drive Details screen to view a detailed Drive Lifecycle Management report.

   Note: The **DLM** button on the Drive Details screen is not present if MLM and DLM are not enabled (see Enable and Configure MLM PreScan and PostScan on page 182).

   The Drive Lifecycle Management screen is divided into four panes, which are described in the following table.

This pane...	Shows...
Drive health overview	The drive identifier and any status information. The drive health icon indicates the drive's overall health at the time the screen was displayed.  **Figure 189** Check the drive health icon for the overall health of the drive.
Summary of tapes	The barcode label information and health information for the last 10 cartridges loaded into the drive. The health icon indicates the cartridge health at the time the cartridge was unloaded from the drive (Tape Health at Unmount) and the current health status stored in the MLM database (Current Tape Health). Refer to the table on page 265 of Chapter 8 – Configuring and Using Media Lifecycle Management, beginning on page 233 for descriptions of the icons related to media health. **Note:** Depending on the drive's history, this pane may not have any entries.  **Figure 190** The Summary of tapes pane shows the cartridge barcode label and health information.

This pane...	Shows...
History of tapes	Detailed information about the last 50 cartridges loaded into the drive as well as any Tape Alerts and SCD codes posted by the drive while the tape was loaded in the drive.  **Figure 191** The History of tapes pane shows detailed information about each of the individual tapes. **Notes:** ▪ Depending on the drive's history drive, this pane may not have any entries. ▪ Refer to the tape drive documentation for information about Tape Alerts (see LTO Ultrium Tape Drives on page 19).

5. To save the information on the Drive Lifecycle Management screen, use the Save MLM Database utility as described in Back Up the MLM and DLM Databases on page 270.
6. If you corrected a condition that changed the drive's health to yellow or red, click **Reset Health** to reset the drive health to Good (Green). Click **Continue** to complete the reset health process.

   Notes:
   - If the condition was not truly corrected, the next tape load sets the drive health back to the previous indication.
   - Resetting the drive health deletes the drive's Summary of Tapes and History of Tapes data.

DOWNLOADING THE DLM DATABASE

If desired, you can open and save the DLM database as an XML file. This file contains the same information that appears on the Drive Lifecycle Management screen (see Step 4 on page 285).

Important The DLM database information in the XML file cannot be used to restore the DLM database. The information required to restore the DLM database is backed up with the MLM database. See Back Up the MLM and DLM Databases on page 270 for information about backing up the MLM database.

Note: **Download DLM DB** is only available when you access the library using the BlueScale web interface (RLC). It is not available from the operator panel.

1. Log into the BlueScale web interface (RLC) as a user with superuser or administrator privileges.
2. Click **MENU**, then select **Maintenance ⋯⁘ MLM.** The Media Lifecycle Management Tools screen displays.

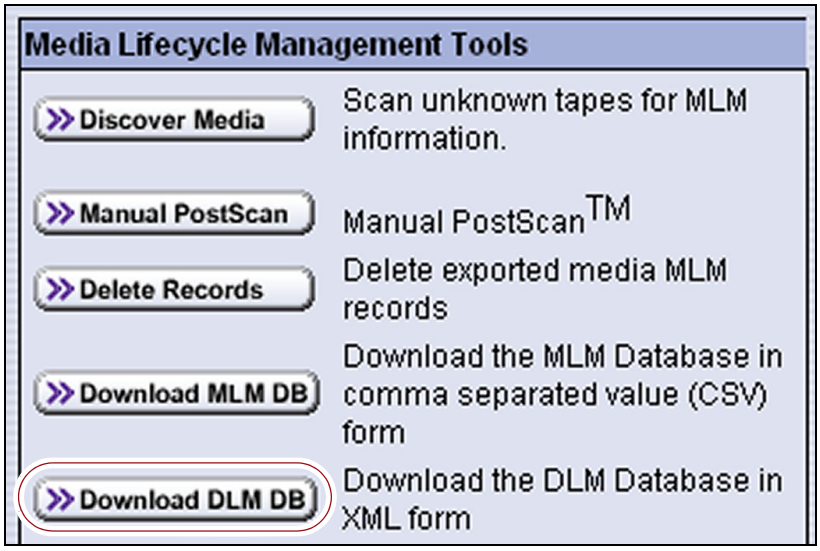


Figure 192 Click **Download DLM DB** to export the DLM database as an XML file.

3. Click **Download DLM DB**. The XML file opens in the application associated with that file type on the computer accessing the library's BlueScale web interface.

   Note: Typically, the application associated with XML files is a web browser. Depending on the browser, the file may open in a new browser window (or browser tab).

Figure 193 The DLM database XML file opened in a web browser.

4. Use the **Save as...** option in the application that opened the XML file to save it to a known location on your computer.
5. You can open the saved XML file using Microsoft Excel 2007 or later, or use another program that supports the XML file format.

CHAPTER 10

Encryption and Key Management

This chapter describes configuring and using encryption and key management on a Spectra T50e library.

ENCRYPTION AND KEY MANAGEMENT OVERVIEW

The Spectra T50e library can encrypt data and manage encryption keys, using either the Spectra SKLM key management system or BlueScale Encryption key management. Spectra SKLM is a stand-alone, centralized key manager, while BlueScale Encryption key management is integrated within, and specific to, the library.

The following table shows the encryption features and functionality provided by BlueScale key management and Spectra SKLM key management.

Feature	Spectra SKLM	BlueScale
Library Integrated Server		✓
Stand-alone Server	✓	
Supports T50e, T120, T200, T380, T680, T950, TFinity	✓	✓
Multi-vendor Support (dual vendor shops)	✓	
Graphical User Interface	✓	✓
Command Line Interface	✓	✓
LTO-4 Drive Support		✓
LTO-5 - LTO-9 Drive Support	✓	✓
Multi-library/ Multi-site Support	✓	
AES-256 Bit Encryption	✓	✓
Secure Initialization Mode		✓
Maximum Number of Encryption Keys	1,000,000+	30
Key per Tape	✓	
M-of-N Key Shares		✓
Symmetric Shares	✓	✓
Asymmetric Shares	✓	
Role-based Access Control	✓	✓
Key Grouping	✓	
Device Grouping	✓	
Key Group Policies	✓	
Key Rotation Policies	✓	
Key Lifecyle Status	✓	
Audit Verified Key Deletion	✓	
Certificates of Authority	✓	
Audit Trail	✓	
FIPS Certification	✓	
IKEv2-SCSI Compliance	✓	
Configuration, Policies, & Keystore Backup	✓	
LDAP Support	✓	
MLM PostScan Media Verification		✓

ACCESSING THE ENCRYPTION FEATURE

Use the following sections to access the encryption feature to configure the library to use either Spectra SKLM or BlueScale Encryption key management.

Log Into the Encryption Feature

User Privilege Requirements. Only users with superuser privileges can access and use the encryption feature on the library.

1. Log into the library as a user with superuser privileges, then click **MENU** ···⁘ **Security** to display the Security menu.

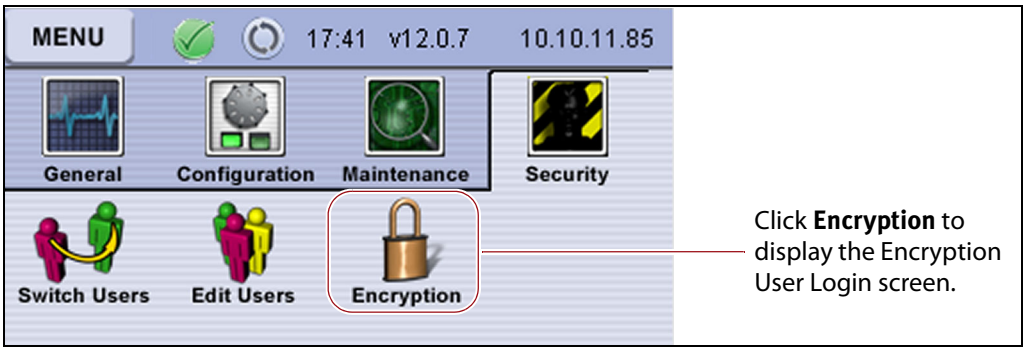


Figure 194 Click **Encryption** to display the Encryption User Login screen.

2. Click **Encryption**. The Encryption User Login screen displays.

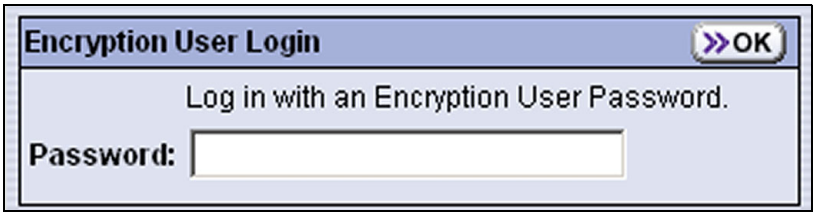


Figure 195 Enter the encryption password to log into the encryption feature.

3. Enter the encryption password (if one is set) and then click **OK**. The Encryption Configuration screen displays the moniker for any BlueScale encryption keys currently stored in the library.

Notes:
- The default encryption password is blank.
- If you are configuring encryption for the first time or you are using Spectra SKLM key management, no encryption key monikers display.
- If you are using BlueScale Professional Edition, up to 30 encryption keys can be stored in the library.

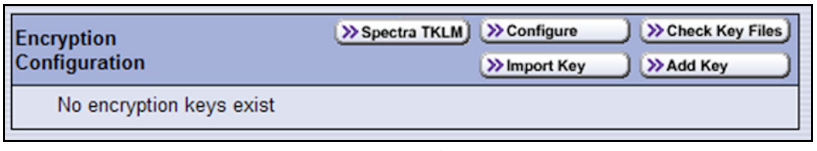


Figure 196 The Encryption Configuration screen.

Configure the User Mode (BlueScale Professional Only)

If you are configuring Spectra SKLM or BlueScale Encryption Standard Edition, the User Mode option does not apply. Proceed to Configure the Secure Initialization Mode (BlueScale Only) on page 293.

If you are configuring the BlueScale Encryption Professional Edition, use the following steps to set the encryption user mode.

1. From the Encryption Configuration screen, click **Configure.** The Encryption Users screen displays.

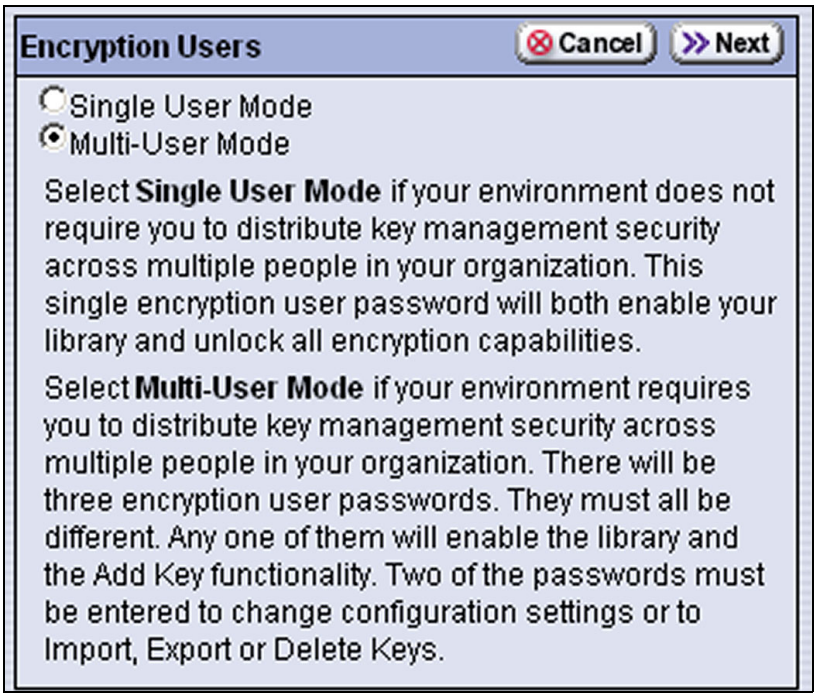


Figure 197 Select **Single User Mode** or **Multi-User Mode**.

2. Select either **Single User Mode** or **Multi-User Mode**.

With this mode...	Accessing encryption requires...
Single User Mode	Only one encryption password can be configured and only one is required to access all encryption features.
Multi-User Mode	Three unique encryption passwords to be configured. After you set up the three passwords, they are used as follows: ▪ Enter any one of the three to permit a library using Secure Initialization mode to initialize encryption when the library is starting up and to otherwise access most encryption features, excluding export and import encryption key features. ▪ Enter any two of the three passwords, when prompted, to access export and import encryption key features.

Configure the Secure Initialization Mode (BlueScale Only)

If you are configuring Spectra SKLM, the Secure Initialization mode option does not apply. Continue with Configure the Password on page 294.

If you are configuring BlueScale Encryption key management, use the following steps to set the Secure Initialization mode.

1. From the Encryption Configuration screen in Standard Edition, click **Configure** or from the Encryption Users screen in Professional Edition, click **Next** to display the Encryption Settings screen.

Figure 198 Select the desired initialization behavior (BlueScale Standard Edition or Professional Edition Single User mode).

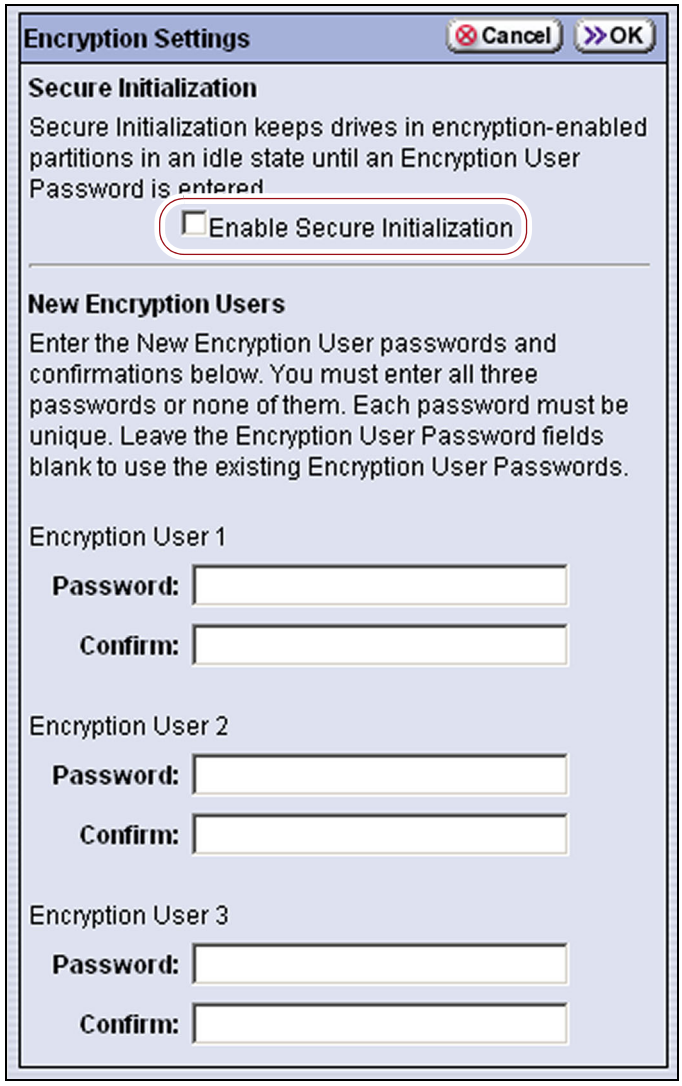


Figure 199 Select the desired initialization behavior (BlueScale Professional Edition Multi-User mode).

2. Select or clear the **Enable Secure Initialization** check box to configure the desired initialization mode.

Initialization Mode	Description
Standard mode	The partitions configured to use encryption are accessible to the hosts as soon as the library completes its initialization. Data can be backed up to partitions that support encryption without entering an encryption password. To use Standard Mode, make sure that the **Enable Secure Initialization** check box is *cleared*. Standard mode is the default setting.
Secure Initialization mode	The partitions configured to use BlueScale Encryption key management are not accessible to the hosts until the encryption password is entered through the Encryption User Login screen. Until that time, any backup or restore operations using partitions that use encryption cannot run. To initialize the encryption partitions and make them available for use, each time the library is initialized, a user with superuser privileges must first log into the library and then log into the encryption feature using the encryption password. To enable Secure Initialization mode, make sure that the **Enable Secure Initialization** check box is *selected*. Secure Initialization mode becomes active after the library is power-cycled.

Configure the Password

1. If you want to change the current encryption user password(s), enter the new password(s) in the **New Encryption Users Password** field(s) using any combination of the numbers **0-9**, lower and upper case alphabetic characters (**a-z** and **A-Z**), and the at symbol (**@**), dash (**–**), underscore (_), and period (**.**) characters.

Caution

The BlueScale encryption user password is separate from the password used to log into the library. Make sure you keep a record of this password. If you lose this password, you are not able to configure the encryption settings.

If you are using BlueScale key management, you are not able to import/export encryption keys that were already assigned and used with encrypted data.

Notes:
- The encryption user password is separate from both the BlueScale login password and the encryption key password you define when you export a BlueScale encryption key (see Export an Encryption Key on page 316).
- Security is greatly enhanced when the user who knows the encryption password is different from the user who performs day-to-day operations such as importing or exporting cartridges.
- If BlueScale Professional edition Multi-User mode was selected, you must enter three unique encryption passwords.

2. Retype the password(s) in the **Confirm** field, then click **OK**. The Encryption Configuration screen displays.

SPECTRA SKLM KEY MANAGEMENT

Spectra Tivoli Key Lifecycle Manager (Spectra SKLM) is a centralized key management system that allows you to manage the lifecycle of the encryption keys and security certificates for your library. Spectra SKLM provides role-based access control, based on user privileges, for tasks that range from creating and assigning encryption keys to the backup and restoration of data.

Spectra SKLM is installed on an external server, which is connected to the library by Ethernet. All administrative activities are performed on the server, including configuration; administration of groups, users, and roles; and management of keys, key groups, and devices. Encryption is performed at the drive level, through encryption-enabled LTO-5 and later generation tape drives.

After Spectra SKLM key management is enabled, the drives in an encryption-enabled partition request a key from the Spectra SKLM server. The server sends the encryption key to the drive, and the drive uses the key to automatically encrypt data as it is backed up.

Before you configure your library to implement Spectra SKLM key management, there are three required components:

- **Spectra SKLM Encryption-capable Drives** Spectra SKLM key management is only compatible with LTO-5 and later generation tape drives.
- **Spectra SKLM Option Key** Purchase and install the Spectra SKLM option key to activate Spectra SKLM key management. For more information on how to install the option key on your library, see Enter Activation Keys on page 115.

Spectra SKLM Server Install and configure Spectra SKLM on your server. Spectra SKLM is available for either Linux or Windows. For additional information that can assist you during the installation and configuration of your server, see the following websites:

  - *IBM Tivoli Key Lifecycle Manager Information Center*
  - *Tivoli Key Lifecycle Manager Installation and Configuration Guide*

- Spectra SKLM key management is not compatible with BlueScale Encryption key management, because they cannot share encryption keys. Data encrypted using Spectra SKLM key management cannot be decrypted using BlueScale Encryption key management, and vice versa.

Configuring Spectra SKLM Key Management

Use the following steps to configure the library to use Spectra SKLM key management.

User Privilege Requirements Only users with superuser privileges can configure the encryption features.

Caution The encryption password is separate from the password used to log into the library. Make sure you keep a record of this password. If you lose this password, you are not able to access the library encryption configuration screen.

Configure the Spectra SKLM Server

1. Access the encryption feature (see Log Into the Encryption Feature on page 291).
2. On the Encryption Configuration screen, click **Spectra SKLM.** The Spectra SKLM Server Status screen displays.

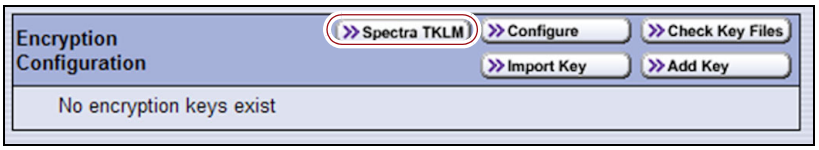


Figure 200 Access the Spectra SKLM Server Status screen.

3. The Spectra SKLM Server Status screen displays a list of previously configured Spectra SKLM servers (if any). Up to four Spectra SKLM servers are supported; each is listed by its IP address.

   Note: When read or write processes begin, a green check mark appears in the Status column next to servers the library can access. A red **X** in the Status column indicates the library is currently unable to connect to that server.

   On the Spectra SKLM Server Status screen, click **Edit** to add or modify Spectra SKLM servers.

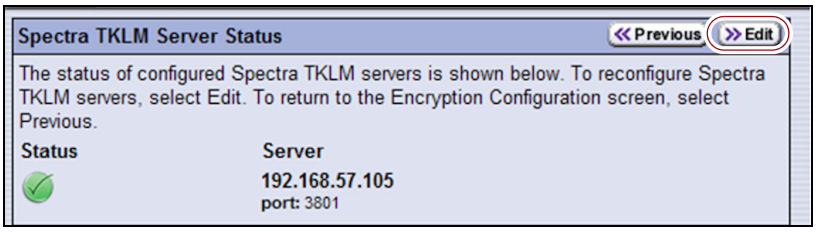


Figure 201 Click **Edit** to add or modify a server.

4. The Spectra SKLM Server Configuration screen displays an editable list of configured Spectra SKLM servers (if any). Enter the appropriate information for the server you want to configure.

   a. Enter the IPv4 or IPv6 address of the server.

   Notes:
   - A previously entered IPv6 address displays compressed.
   - If a server is no longer needed, delete its IP address.

   b. If desired, modify the port. The default port setting is 3801.

   Note: If you are setting up Spectra SKLM on a Windows server, you must add a Windows firewall rule to allow connections to this port. Otherwise, the library is not able to access the server.

   Click **Update** to accept the changes, and display the Spectra SKLM Update Result screen or click **Cancel** to return to the Spectra SKLM Server Status screen without saving the changes.

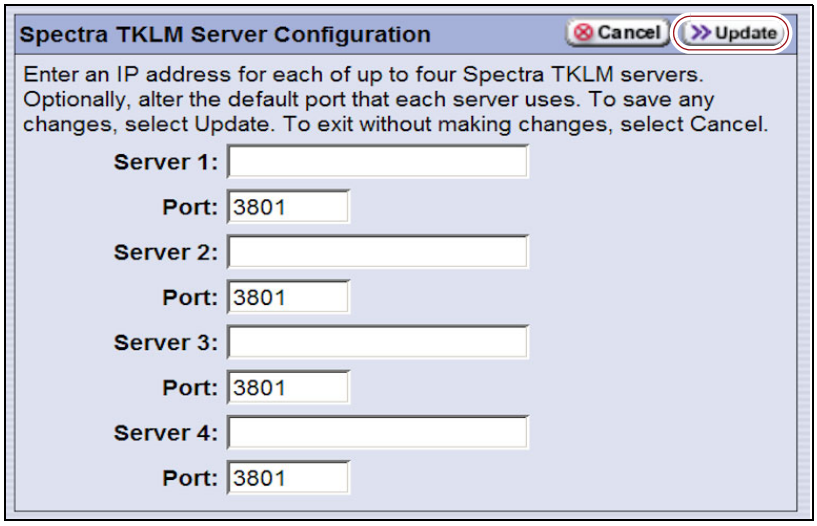


Figure 202 Click **Update** to save the changes.

5. If you selected **Update**, the library attempts to connect to the server and the Spectra SKLM Update Result screen displays the success or failure of the Spectra SKLM server configuration.

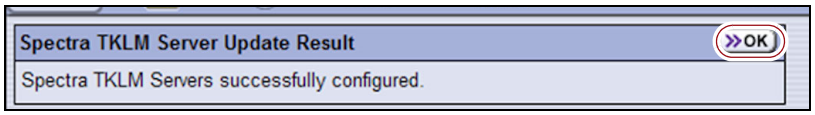


Figure 203 The SKLM Server Update Result screen.

6. Click **OK** to return to the Spectra SKLM Server Status screen.

   Note: Newly added servers are added to the list of servers on the Spectra SKLM Server Status screen. If the library could not connect to the server or verify it as a Spectra SKLM server, it does not appear on the list.

Configuring a Partition to Use a Spectra SKLM Server

Overview After configuring a Spectra SKLM server, you can enable Spectra SKLM for one or more partitions.

Important To use Spectra SKLM Encryption key management, LTO-5 drives must be updated to firmware version C7RC, or later. All LTO-6 or later generation drive firmware supported for use with the library can be used with Spectra SKLM encryption.

Notes:
- The Encryption screen in the partition wizard lets you enable the encryption features for the partition. It only displays if you are logged in as an encryption user and already configured a Spectra SKLM server or a BlueScale encryption key. (See Configure the Spectra SKLM Server on page 296 or Configuring BlueScale Key Management on page 310 for more information.)
- Spectra SKLM key management is not compatible with BlueScale Encryption key management, because they cannot share encryption keys. Data encrypted using Spectra SKLM key management cannot be decrypted using BlueScale Encryption key management, and vice versa.
- Spectra SKLM key management is only compatible with LTO-5 and later generation tape drives.

Use the following steps to assign a Spectra SKLM server to the partition and encrypt all data sent to the partition:

1. Access the encryption feature (see Log Into the Encryption Feature on page 291).

   Note: If you are not already logged in as an encryption user, you must enter the encryption password before you create or edit a partition using the BlueScale partition wizard. If you are not logged in, the Encryption screen does not display.

2. Click **Menu,** then select **Configuration** ···⁘ **Partitions**. The Shared Library Services screen displays.
3. Click **New** to create a partition, or click **Edit** to modify the settings for an existing partition (see Creating a Storage Partition on page 174).
4. Navigate through the partition wizard by clicking **Next** until you reach the Encryption screen.

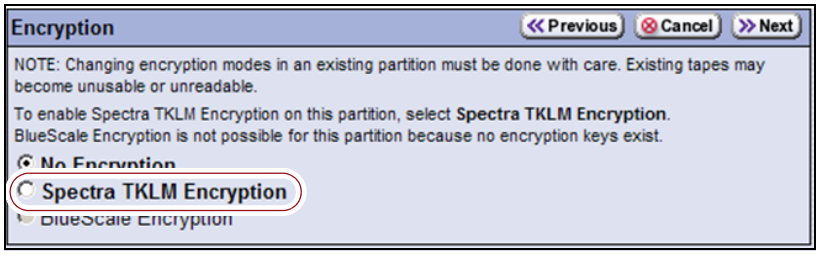


Figure 204 The Encryption screen.

5. Choose the type of encryption to use.

Encryption Option	Description
No Encryption	Turns off encryption. None of the data in the partition is encrypted.
Spectra SKLM Encryption	Turns on Spectra SKLM Encryption key management for drive-based encryption using direct-attached LTO-5 and later generation drives. **Note:** If PostScan was enabled on the MLM Media Verification screen, Spectra SKLM Encryption cannot be selected, and is grayed out.
BlueScale Encryption	Enables the library partition to use Spectra BlueScale key management. See Configuring BlueScale Key Management on page 310 for more information.

6. Navigate through the remaining partition configuration screens by clicking **Next**.
7. When you reach the Save Partition screen, click **Save**.

Disabling Encryption in a Partition

Use the following steps to disable encryption in a partition.

Note: If you are not already logged in as an encryption user, you must enter the encryption password before you create or edit a partition using the BlueScale partition wizard. If you are not logged in, the Encryption screen does not display.

1. Access the Partitions screen (see Accessing the Partition Wizard on page 169).
2. Select the partition for which you want to disable encryption. Click **Edit**.
3. Click **Next** to navigate through the partition wizard screens until you reach the Encryption screen (see Figure 204 on page 298).
4. Select **No Encryption**.
5. Click **Next** to move to the next partition configuration screen. Navigate through the remaining partition configuration screens by clicking **Next**.
6. When you reach the Summary screen, click **Save**.

BLUESCALE KEY MANAGEMENT

BlueScale key management is tightly integrated into your Spectra T50e library. Encryption is handled through encryption-enabled LTO-4 and later generation drives. BlueScale Encryption key management is provided through the library's user interface.

Understanding the Components

The BlueScale Encryption key management system has two major components which together let you easily implement the strongest encryption available, as recognized by the United States Federal Government: AES encryption using a 256-bit key.

- **The BlueScale Key Management software** The key management feature is accessed through the library's user interface, either using the operator panel or a remote connection through the BlueScale web interface. Optionally, you can secure the web browser using SSL. Spectra BlueScale key management is available in Standard and Professional Editions to meet your site security requirements (see Standard Edition vs. Professional Edition).
- **The encryption chip in the LTO-4 and later generation drives** Using hardware encryption makes encryption extremely fast and places no burden on your network. Encryption-enabled LTO-4 and later generation drives perform the encryption as the data is written to tape. After encryption is enabled, data is automatically encrypted as it is backed up.

Encryption and LTO-3 LTO-3 and earlier generation drives do not support drive-based encryption and cannot be used in a partition configured to use drive-based encryption.

LTO-4 and later commonality The encryption-enabled LTO-4 and later generation drives use the same encryption algorithm, ensuring that data encrypted by an LTO-4 drive can be read by an encryption-enabled LTO-5 drive.

Notes:
- You can only use one type of encryption in a partition.
- BlueScale Encryption key management is not compatible with Spectra SKLM key management, because they cannot share encryption keys.

Standard Edition vs. Professional Edition

To determine a BlueScale Encryption key management strategy appropriate for your site and your data, decide on the security level appropriate for your site, and the amount and kinds of data to encrypt. See Best Practices on page 302 for things to consider when determining your encryption requirements and processes. After you decide on the appropriate security level and whether data sets need to be isolated, you can decide which edition of BlueScale Encryption meets your needs.

BlueScale Encryption Standard Edition Standard Edition is included as a standard feature on the library. It is suitable for sites with a primary goal of securing data while it is transported to a remote location and stored there for long-term archival. See Low Security Site on page 307 for an example of setting up encryption using BlueScale Encryption Standard Edition.

BlueScale Encryption Professional Edition Professional Edition provides additional choices for defining the level of security you implement in your data center. It is suitable for sites that want the added security of multi-password access to the encryption configuration controls and for importing and exporting encryption keys, and the added flexibility of storing up to 30 encryption keys on the library. See Medium Security Site on page 308 and High Security Site on page 309 for examples of setting up encryption using BlueScale Encryption Professional Edition.

The following table shows the major differences between the Standard and Professional Editions.

Feature	Standard Edition	Professional Edition
Availability	Included as a standard feature on the library.	Requires a purchased option key to activate.
Encryption Login Passwords	Single encryption password accesses all encryption features.	Choice of using one or three passwords to access all encryption features. Using the three-password option requires the following: ▪ Three unique encryption passwords must be configured. ▪ Any one of the three passwords must be entered to enable encryption when the library is in Secure Initialization mode. ▪ Any one of the three passwords must be entered to access encryption key management and configuration options, excluding key import and export. ▪ Two of the three passwords must be entered to import and export keys.

Feature	Standard Edition	Professional Edition
Keys (Data Set Isolation)	▪ Single encryption key stored on the library at a time. ▪ The same key is used for all partitions configured to use encryption.	▪ Up to 30 encryption keys stored on the library. ▪ Separate encryption keys can be assigned to each storage partition to isolate data sets.
Key Export and Import	A single password is used when exporting and importing the encryption key. The encryption key is exported in a single file.	Choice of using one or M-of-N shares with multiple passwords to export and import keys. With the M-of-N shares option, a single file of encrypted key data is split into multiple parts, or shares (N), and some specified subset (M) is required to import the file containing the key data.
Compression	Drive-based compression only.	
Compatibility between Software Editions	Data encrypted using either software edition can be decrypted by a library running the other edition.	

Best Practices

To effectively use key management and to ensure data security, create an encryption strategy and back it up with the appropriate staff and custom strategies based on your security requirements.

People

Identify the key people who are responsible for managing the encryption of data written to tape.

Superuser One or more people who have superuser privileges on the library. Only a superuser can access and configure the encryption features. See Understanding User Groups and Security on page 94 for information about the three types of user groups and what types of privileges each has.

Encryption Password Holder One or more superusers who have the library's encryption password(s).

When determining the number of superusers and encryption password holders, balance the needs for security and availability for the encrypted data. It may be wise to have more than a single user familiar with passwords, depending on the size of your organization, so that if one person is not available, another can take over.

Processes

Consider the following when establishing your encryption procedures:

Startup Security

- Develop procedures for tracking user names and passwords. Make sure only the authorized users know the encryption passwords, and that the passwords themselves are secure. Refer to Passwords and Other Identifiers on page 305 for more information on setting up passwords.
- Optionally, identify a primary and secondary encryption team, so that you have redundancy in your encryption strategy. Although that means the information required to decrypt data is spread across more people, it also means that restoration of encrypted data may be much easier, and you may ultimately have more data protection given the extra layer of coverage; for example, if a user leaves, you are not in a position to lose data.
- Determine the level of security to use at startup. Both editions of BlueScale Encryption permit a standard mode and a secure initialization mode. In standard mode, data is encrypted and restored as soon as the library is started with no further action required. In secure initialization mode, the partitions configured to use encryption are not accessible for backup or restore operations until a user with superuser privileges logs into the library and entered the encryption password. (Spectra SKLM does not use the secure initialization mode.)

Data to Encrypt

- Decide whether to encrypt all data or a subset. If all of the site's data is to be encrypted on backup, then a single partition could be sufficient. If, however, you are backing up some data without encryption, create a partition dedicated to encrypted data, and another for non-encrypted data.
- Determine whether the encrypted data can be grouped together or if it must be isolated into sets. If sets of encrypted data need to be isolated from each other, create several encrypted storage partitions, each using a different encryption key. For example, your site may store financial data as one set and consumer identity information as a separate set.

BlueScale Encryption Key Protection

BlueScale Encryption uses AES-256 encryption, which is a symmetric, private key encryption method. BlueScale Encryption identifies each key by the moniker (nickname) used to generate the key; the key itself is never displayed. In addition, keys are encrypted before they are exported and the file containing the key is password-protected.

Best practices dictate that you make copies of the key immediately following the key's creation. To ensure security, make sure that you track each copy of an encryption key.

- Decide on the number of copies to make of each key and keep a record of each copy's location. Consider storing multiple copies of keys, that you then track carefully, storing the copies in separate places and away from the data encrypted using those keys.

Caution

As a matter of best practice, Spectra Logic recommends exporting encryption keys to a USB device instead of using email.

Although emailing encryption keys is supported by the library, using email presents security issues, including the following:

- Copies of encryption keys may be left on the email servers used for sending and receiving email and are thus subject to compromise.
- The difficulty in verifying where all the copies of emailed encryption keys may be located can make security audits more challenging.

- Establish a key rotation plan that specifies how often to create and use new keys. The rotation plan may be a simple schedule such as changing keys once every six months, and destroying the keys only after the last set of data encrypted using that key is overwritten or destroyed.

  BlueScale Encryption Standard Edition stores one key on the library at a time; you must delete the key currently on the library before you can create or import another key. Professional Edition permits multiple keys per library, with one key per encryption-enabled partition.
- Establish a procedure for tracking monikers. Make sure you track the information required to access and identify keys, along with the location of stored data that uses each encryption key. Make sure this information is not stored with the encrypted data. Keep it on a system or in an archive that is not available on a network. For additional security, encrypt this information as well.
- Before you delete a key from the library, make sure that at least one copy was exported and stored securely. It is important to make sure that at least one copy of each key is secure and readable (that is, uncorrupted), to ensure you can restore your data.

  Keeping a copy of an exported key is essential; after a key is deleted from the library, it is not recoverable. Once the key is gone, the data is inaccessible; for legal and practical purposes the data is typically considered to be deleted.

Process Testing and Exception Handling

- Run drills to confirm that your data is being encrypted properly, that keys are stored properly, and that you can recover your data. Make sure that these drills are included with your overall organizational security strategy.

- Create procedures to handle encrypted data that is, or may be, compromised. Make sure you can identify the data associated with any compromised key or keys. You may want to take all compromised data and decrypt it and then re-encrypt it and store it in an alternate location to minimize the potential for unauthorized access. You also need to investigate the incident involving compromised data and take appropriate actions if identity-related data was exposed.

Special Considerations When Using BlueScale Encryption Professional Edition

- Drive-based encryption only allows one encryption key per cartridge, regardless of the number of keys stored on the library.
- To simplify data restoration in case of disaster recovery and to achieve business continuity goals, make sure that critically important data is stored on a separate, well-identified cartridge and that only one key is used for encrypting all the data on the cartridge.
- You may want to take advantage of the M-of-N shares option. This option lets you split an exported encryption key into multiple files, or shares, each stored on a separate USB device or emailed to separate mail recipients. Some specified subset of the shares is required to import the encryption key into the library. Splitting an exported key into multiple shares further protects data from unauthorized access.

  For example, if you choose the 2-of-3 shares option, the exported encryption key is split into three shares (M). In order to import the encryption key into the library, two of the shares (N), each on a separate USB device, must be present.

Passwords and Other Identifiers

BlueScale Encryption requires you to supply passwords and monikers (key names) when configuring and using the encryption feature. Your site may want to consider implementing specific rules that govern how these are created.

Superuser Login/Encryption Passwords BlueScale Encryption requires a separate password from the one used to log into the library in order to access the library's encryption features. This password must be entered after a user with superuser privileges logs into the library.

If you are using Professional Edition, you have the option to set three separate encryption passwords. If you select to use this option, two of the three encryption passwords must be entered in order to import BlueScale encryption keys into the library or export them from the library.

The following passwords are required with both editions of BlueScale Encryption:

- **Superuser Password**—Only a user logged into the library with superuser privileges can access the Encryption User Login screen.
- **Encryption Password**—Lets you access encryption features. This password must be entered after the superuser login.

Password(s) for Key Import and Export Passwords are also used to encrypt keys for export and when importing previously exported keys. Your site may consider whether to create different rules for these passwords, such as requiring that these passwords are longer than the encryption access password(s), and therefore more secure. Optionally, in Professional Edition, you can require two different passwords in order to import and export keys.

Monikers A moniker is an alphanumeric identifier that is tied to the never-revealed true key value, which is a 256-bit encryption key. The library uses monikers to generate unique encryption keys. The library displays the moniker, not the encryption key itself, whenever it references the encryption key. The actual value of an encryption key is **never** displayed. The moniker helps to protect data encrypted using the key by eliminating the need to display or type the actual key value.

Your site may want to create rules governing naming conventions for key monikers to ensure that each key is unique.

Recommended Make a habit of using a single case (all upper or all lower) for monikers. After the encryption key is created and exported, the library ignores the case used in the moniker.

For example, the library interprets Spectra1, spectra1, and SPECTRA1 as the same moniker when importing a key. However, the key generated by each variation is unique.

Important If you create two monikers that are identical except for case, you may not be able to retrieve your data after importing a key that was created using a different variation of the moniker.

Password and Moniker Standards Create standards to govern passwords and moniker names based on your site's security requirements. For example, if your site requires a high level of security for access to encryption partitions, your passwords and monikers may need to incorporate some combination of the following requirements:

- Use a minimum number of characters.
- Use both alphabetic characters and numeric characters.
- Use both uppercase and lowercase letters for passwords.
- Do not use words found in a dictionary.
- Change the passwords at regularly scheduled intervals.

Site Security Examples

The following sections provide examples of different security scenarios.

Low Security Site

The following table describes the security considerations and the suggested encryption configuration for a small company with 75 employees.

Security Consideration	Strategy
Security goals	Protecting company from legal liability associated with unauthorized access to data stored on tape, both onsite and offsite, including transport to the offsite location.
Encryption principals	IT administrator, company president, corporate legal counsel.
Data to encrypt	Financial and consumer identity data.
Level of security to implement	BlueScale Standard Edition: single key per library is sufficient. Standard initialization mode: encryption partitions enabled at start-up.
Data sets requiring isolation	None. A single partition for encrypted data is sufficient.
Key escrow method	Staff at company escrow keys at a site remote from the data storage location.
Copies of each key to store and their locations	Keep three copies of each key: one with the senior IT administrator, one with the company president, one in a corporate safety deposit box.
Key rotation plan	Create a new key every six months.
Tracking key monikers and passwords	On a non-networked computer that supports encryption, create one or more charts or lists with this data, including key monikers, dates used, encryption and superuser passwords, and passwords used to encrypt exported keys. For additional security, you may want to avoid tracking the relationship between monikers and the encrypted cartridges. The library prompts for the required moniker when you restore encrypted data from a cartridge.
Multiple encryption teams (optional)	Configure a separate set of users who are responsible for managing encrypted data. These users may be the same as those identified as the encryption principals.
Decrypt and restore encrypted data	Regularly review data encryption and decryption procedures to make sure that backups and restores are working properly. Run tests to ensure that encrypted data can be decrypted and restored when needed.
Passwords	▪ Require passwords with a minimum of 12 characters, including at least one number and one letter, to access the encryption features. ▪ Require passwords with a minimum of 30 characters, including at least one number and one letter, to export and import encryption keys.

Medium Security Site

The following table describes the security considerations and the suggested encryption configuration for a medium-sized organization with 250 employees.

Security Considerations	Strategy
Security goals	Protecting company from legal liability associated with unauthorized access to data stored on tape onsite and offsite, including transport to the offsite location.
Encryption principals	IT senior staff, chief operating officer.
Data to encrypt	Intellectual property, financial, customer, and inventory data.
Level of security to implement	▪ BlueScale Professional Edition, with multiple keys ▪ Standard initialization mode: encryption partitions enabled at start-up ▪ Multi-user mode, with three encryption passwords
Data sets requiring isolation from other encrypted data	Separate partitions and keys for these data sets: financial data, inventory data, customer data, and intellectual property data. With this requirement, the site must use a minimum of four encryption-enabled partitions, along with partition(s) for non-encrypted data.
Key escrow method	Store key copies with corporate legal counsel and a paid, trusted, third-party escrow service.
Number of copies of each key to store, and locations	Keep three copies of each key: store one with corporate legal counsel, two with the key escrow service.
Key rotation plan	Create a new key every quarter for each partition dedicated to encryption.
Tracking key monikers, exported key passwords, and password to permit access to encryption features	Send to key escrow service an encrypted document that includes the password used to access encryption features, superuser password, and all passwords necessary to import encryption keys. This file cannot be created or stored on a networked computer. Delete the file from the computer after the document or file is transmitted securely to the key escrow service.
Multiple encryption teams (optional)	Three IT administrators, along with the senior IT admin and the COO.
Schedule and run drills	Annual evaluation and review, along with wider corporate security plan.
Passwords	▪ Passwords to access encryption features: minimum of 12 characters, including at least one number and one letter ▪ Password to export and import encryption keys: minimum of 30 characters, including at least one number and one letter

High Security Site

The following table describes the security considerations and the suggested encryption configuration for an enterprise organization.

Security Considerations	Strategy
Security goals	Protecting all stored data.
Encryption principals	IT senior staff, chief operating officer, chief security officer, chief technology officer.
Data to encrypt	All.
Level of security to implement	▪ BlueScale Professional Edition, with multiple keys ▪ Secure Initialization Mode: After the library power is turned on, the encryption user must enter the password to enable partitions dedicated to encryption ▪ Multi-user mode, with three encryption passwords
Data sets requiring isolation	Each data set is separately keyed, as defined by the department generating data.
Key escrow method	Store key copies with two remote corporate legal counsel offices and also with a paid, trusted third-party escrow service.
Copies of each key to store, and the stored key locations	Keep three copies of each key: store one at the main office of corporate legal counsel, two with the key escrow service.
Key rotation plan	Create a new key every month for each partition dedicated to encryption.
Tracking key monikers and passwords	Send to the key escrow service an encrypted file with encryption access passwords and superuser passwords. Send to corporate legal office a list of passwords used to export keys. Files with this data cannot be created or stored on a networked computer; delete file or files from the computer once data is transmitted securely.
Multiple encryption teams (optional)	Senior IT admin, chief operating officer, chief security officer, chief technology officer.
Schedule and run drills	Quarterly evaluation and review, in conjunction with wider corporate security plan.
Passwords	▪ Passwords to access encryption features: minimum of 15 characters, including at least one number and one letter ▪ Password to export and import encryption keys: minimum of 40 characters, including at least one number and one letter

Configuring BlueScale Key Management

The following sections describe the configuration steps for both the Standard and Professional Editions of the encryption feature.

Create an Encryption Key

1. Access the encryption feature (see Log Into the Encryption Feature on page 291).
2. On the Encryption Configuration screen, click **Add Key**. The New Encryption Key screen displays.

Figure 205 Click **Add Key** to begin the key creation process.

3. Enter a name for the encryption key in the **Moniker** field. Make sure that the moniker meets the following requirements:
   - A moniker can be any combination of the numbers **0-9**, lower and upper case alphabetic characters (**a-z** and **A-Z**), and the at symbol (@), dash (–), underscore (_), and period (.) characters. To improve readability, use an underscore to separate words. Do not use any space characters.

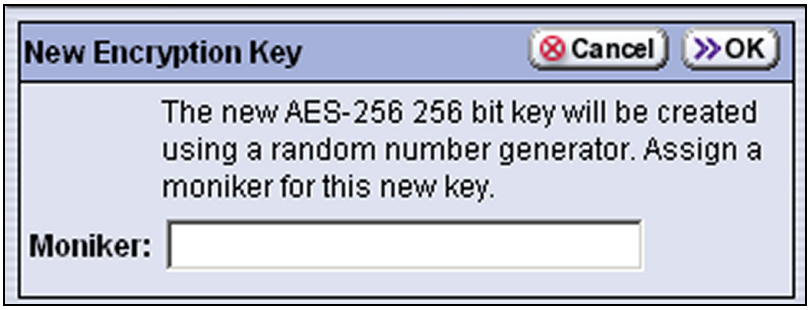


Figure 206 Enter a unique moniker to create a new encryption key.

   - Each moniker must be a unique string of characters that was not used for any other encryption key.

- **Recommended.** Make a habit of using a single case (all upper or all lower) for monikers. After the encryption key is created and exported, the library ignores the case used in the moniker.

  For example, the library interprets Spectra1, spectra1, and SPECTRA1 as the same moniker when importing a key. However, the key generated by each variation is unique.

Important If you create two monikers that are identical except for case, you may not be able to retrieve your data after importing a key that was created using a different variation of the moniker.

4. Click **OK**. The Encryption Configuration screen displays with a confirmation showing the moniker for the newly created encryption key and a message reminding you to create a copy of the key for safekeeping.

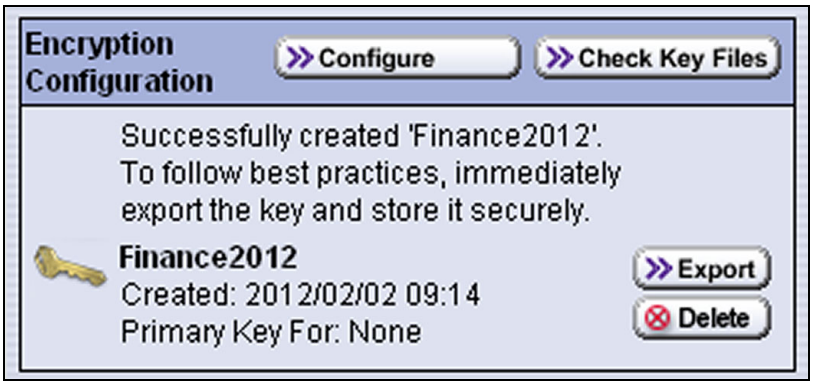


Figure 207 The new encryption key is listed on the Encryption Configuration screen.

   - If the key is not yet assigned to a partition, **None** displays in the **Primary Key For** field.
   - The BlueScale Encryption Standard Edition only supports using one encryption key. The **Import Key** and **Add Key** buttons no longer display after you create a key. If you delete the existing key, they display again. BlueScale Encryption Professional Edition is required if you want to store multiple encryption keys in the library.

5. Export the newly created encryption key and save it to a secure location (see Export an Encryption Key on page 316).

Caution If you lose the encryption key, data encrypted using the key cannot be recovered. For this reason, promptly copying the key and storing it safely (that is, away from the data encrypted using the key) is extremely important to data decryption and recovery. See Exporting and Protecting Encryption Keys on page 314 for additional information.

6. If you have Professional Edition, repeat the steps in this section to create additional encryption keys, if desired.
7. If desired, proceed to Assign the Encryption Key to a Partition.

Assign the Encryption Key to a Partition

Overview After creating an encryption key, you can assign it to one or more partitions. The encryption choices available for a partition depend on the hardware assigned to the partition.

Notes:
- The Encryption screen in the partition wizard lets you enable the encryption features for the partition. It only displays if you are logged in as an encryption user and already created an encryption key as described in Create an Encryption Key on page 310.
- By default, LTO-4 and later generation drives are configured to compress data. If necessary, use your storage management software to modify the drive property settings to turn off compression.
- Spectra SKLM key management is not compatible with BlueScale Encryption key management, because they cannot share encryption keys. Data encrypted using Spectra SKLM key management cannot be decrypted using BlueScale Encryption key management, and vice versa.

Use the following steps to assign a key to a partition and encrypt all data sent to the partition.

1. Access the encryption feature (see Log Into the Encryption Feature on page 291).

   Note: If you are not already logged in as an encryption user, you must enter the encryption password before you create or edit a partition using the BlueScale partition wizard. If you are not logged in, the Encryption screen does not display.

2. Click **MENU**, then select **Configuration** ⋯⁘ **Partitions**.
3. Click **New** to create a partition, or click **Edit** to modify the settings for an existing partition (see Creating a Storage Partition on page 174).
4. Navigate through the partition configuration wizard by clicking **Next** until the Encryption screen displays.

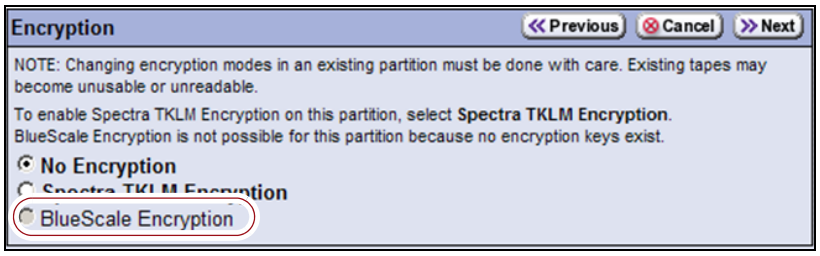


Figure 208 The Encryption screen in the partition wizard.

5. Select the type of encryption to use. Click **Next**.

Encryption Option	Description
No Encryption	Turns off encryption. None of the data in the partition is encrypted.
Spectra SKLM Encryption	Turns on Spectra SKLM Encryption key management for drive-based encryption using direct-attached LTO-5 and later generation drives. **Note:** See Spectra SKLM Key Management on page 295 for more information.
BlueScale Encryption	Enables the library partition to use BlueScale Encryption and key management. All key management tasks are performed through the BlueScale user interface.

6. Click **Enable Encryption**.

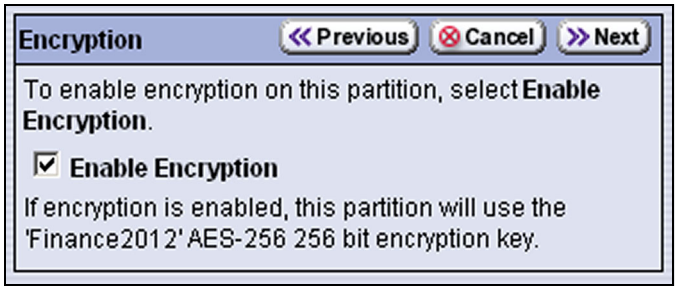


Figure 209 The Encryption screen in the partition wizard with a single key in the library.

Figure 210 The Encryption screen in the partition wizard with multiple keys in the library.

7. If you have BlueScale Encryption Standard Edition or if you have only one key in the library, skip to Step 8.

   If you have BlueScale Professional Edition and there are multiple encryption keys in the library use the following steps to configure encryption and decryption for the partition.

   a. Select the primary key for the partition. This key is used when encrypting and decrypting data. Only one key can be assigned as the primary encryption key.

   b. Select none, one, or multiple additional keys to be associated with this partition. A maximum of eight decryption keys can be assigned to one partition.

   Notes:
   - The additional keys are only used for decrypting data. Having additional keys associated with the partition makes it possible to decrypt data encrypted with those keys even if the primary key for the partition is different.
   - You do not need to reselect the primary key.

8. Click **Next** to move to the next partition configuration screen. Navigate through the remaining partition configuration screens by clicking **Next**.
9. When you reach the Summary screen, click **Save**. All data sent to this partition is encrypted using the key you selected.
10. Access the encryption feature and confirm that the listed keys reflect the assignments you just completed.

Exporting and Protecting Encryption Keys

Ensuring that you have a backup of all keys used in the library and a record of the password for each exported key is essential to ensuring that you can recover encrypted data. For safe-keeping and security, export the encryption key and store it in a safe, secure location so that you can import it back into the library if needed.

Overview

Decrypting encrypted data requires both the encryption key and the encryption key password used to protect the encryption key when it is exported. To ensure that the keys are protected, use the Export Key option described in this section to export encryption keys to a USB device as soon as possible after you create them.

Caution

Data cannot be recovered without the encryption key used to encrypt the data, so protecting encryption keys is extremely important to data decryption and recovery. To decrypt and restore encrypted data, you need the data, the encryption key, and the encryption key password used to protect the exported key and data.

Important

Backup files of the library configuration include any encryption keys that were stored in the library at the time the file was created.

Best Practice

Spectra Logic recommends that you export each encryption key to at least two different USB devices and store them in separate locations. Remember, lost encryption keys cannot be recreated; you should keep them as secure (and as backed up) as your data.

Caution

As a matter of best practice, Spectra Logic recommends exporting encryption keys to a USB device instead of using email.

Although emailing encryption keys is supported by the library, using email presents security issues, including the following:

- Copies of encryption keys may be left on the email servers used for sending and receiving email and are thus subject to compromise.
- The difficulty in verifying where all of the copies of emailed encryption keys may be located can make security audits more challenging.

Key Protection Features of BlueScale Professional

If you are using BlueScale Encryption Standard Edition, continue with Export an Encryption Key on page 316.

Three Passwords to Access Export and import Key Functions If you enabled Multi-User mode when you configured the encryption feature, you must enter two of the three encryption passwords in order to export keys from the library. See Configure the User Mode (BlueScale Professional Only) on page 292) and Configure the Secure Initialization Mode (BlueScale Only) on page 293 for information about enabling Multi-User mode and configuring the library to support multiple encryption passwords.

Export as M-of-N Shares With the Standard Edition, an exported key is encrypted and saved as a password-protected file that is either copied to a USB device or sent as an email attachment to a preconfigured recipient.

The Professional Edition offers an addition safeguard when exporting and importing encryption keys. If desired, you can choose to split an encryption key into multiple files (M-of-N shares) when you export it. During the export process, you select the a total number of shares (N) to split the key into and the subset of those shares (M) required to import the encrypted key file into the library. Depending on your site requirement, you can select one of the following options for your M-of-N shares:

- 2-of-3
- 2-of-4
- 3-of-4
- 2-of-5
- 3-of-5
- 4-of-5

Each of the shares is then copied to a separate USB device or sent to a separate mail recipient. See Step 4 on page 317 for additional information about using the M-of-N shares option when exporting a key.

Requirements for Exporting Keys as M-of-N Shares If you have BlueScale Professional Edition and you want to export the encryption key as M-of-N shares, you must meet the following requirements.

- If you select to export the key to USB, you need a separate USB device for each share. The shares are copied to the USB devices one after the other.
- If you choose to email the key, you must select different, previously configured mail users to receive the shares. Each recipient receives one share as an email attachment.
- Although you can email shares when exporting the key, the only way to import shares of a key is to use USB devices.

For example, if you choose the 2-of-3 option, then the encrypted key, which is further protected by a key-specific password, is split into three shares. Each share is then copied to a separate USB devices or sent as an email attachment.

Export an Encryption Key

Use the following steps to export the current encryption key:

1. Access the encryption feature (see Log Into the Encryption Feature on page 291).
2. From the Encryption Configuration screen, click **Export**.

Figure 211 Click **Export** the begin the key export process.

   - If you selected Multi-User mode for Professional Edition and you did not already enter a second encryption user password, you are prompted to enter another password. Enter one of the encryption user passwords that you did not use during the initial login and then click **Next**. The Export Type screen displays.
   - Otherwise, the Export Type screen immediately displays.
3. If you want to export the encryption key to one or more USB devices, plug a USB device into a USB port on the LCM and allow time for the device to mount before continuing.

4. On the Export Type screen, select the desired export option.

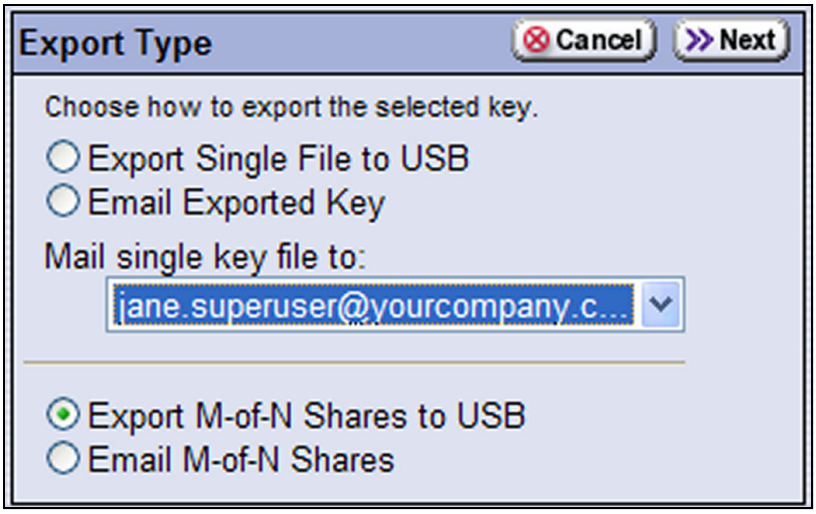


Figure 212 Choose the method for exporting the key.

Caution

As a matter of best practice, Spectra Logic recommends exporting encryption keys to a USB device instead of using email.

Although emailing encryption keys is supported by the library, using email presents security issues, including the following:

- Copies of encryption keys may be left on the email servers used for sending and receiving email and are thus subject to compromise.
- The difficulty in verifying where all the copies of emailed encryption keys may be located can make security audits more challenging.

Note: The options to export M-of-N shares are only available with BlueScale Encryption Professional Edition. See Export as M-of-N Shares on page 315 for detailed information about using these options.

Select....	To...
Export Single File to USB	Save the exported encryption key to the USB device connected to the LCM.
Email Exported Key	Send the encryption key as an email attachment to a previously configured mail recipient (see Configure Mail Users on page 107). Use the **Mail single key file to:** drop-down list to select the desired recipient. **Note:** Do not use the default autosupport@spectralogic.com email recipient. Spectra Logic does not save emailed files unless they are specifically requested for troubleshooting.
Export M-of-N Shares to USB	Divide the exported key into multiple shares, with each share saved to a separate USB device. When you select this option, have on hand a separate USB device for each share (N).
Export M-of-N Shares	Divide the exported key into multiple shares, with each share sent as an email attachment to a separate, previously configured mail recipient (see Configure Mail Users on page 107).

5. Click **Next**.
   - If you are using BlueScale Encryption Standard Edition, the Export Password screen displays. Skip to Step 9 on page 319.
   - If you are using BlueScale Encryption Professional Edition and you chose one of the M-of-N options, the Export M-of-N Shares screen displays.

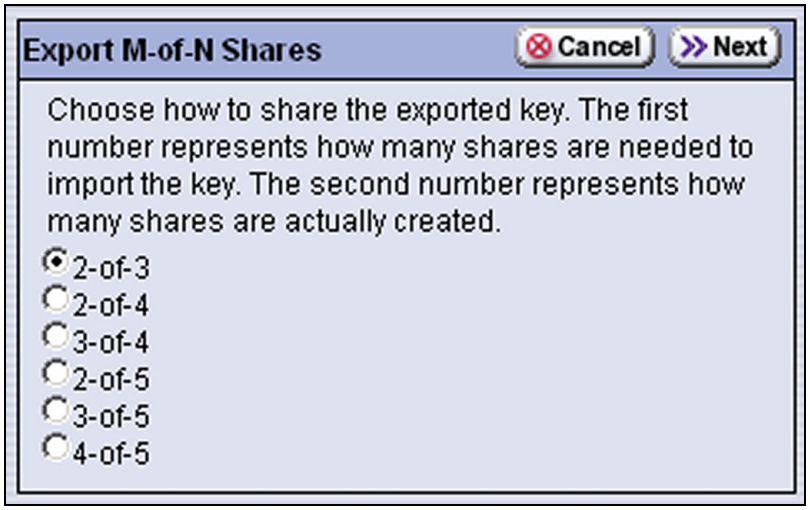


Figure 213 Select the M-of-N option you want to use (Professional Edition).

6. Select the desired M-of-N option, where **M** is the minimum number of shares required to import the encryption key and **N** is the total number of shares to be created.
7. Click **Next**.
   - If you chose to export the shares to USB, the Export Password screen displays. Skip to Step 9 on page 319.
   - If you chose to email the shares, the Export M-of-N Email screen displays.

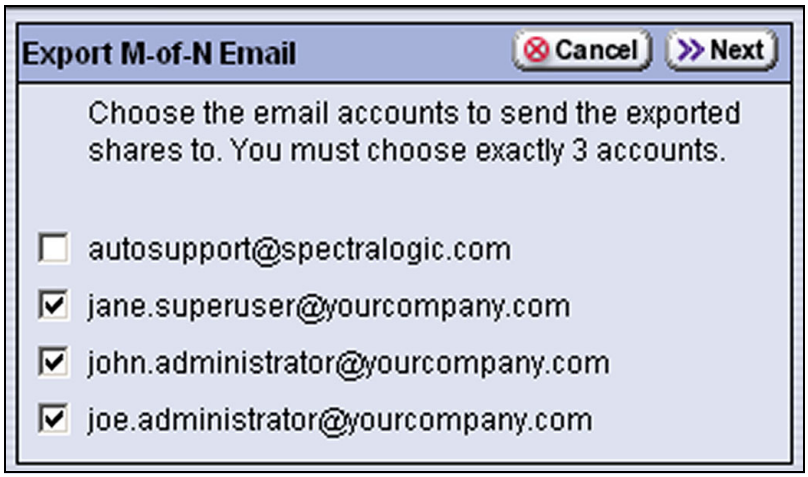


Figure 214 Select the email recipients for each of the shares.

8. Select from the list of email users; you must select the same number of email users as the total number of shares (N) and then click **Next**.

   Note: Do not use the default autosupport@spectralogic.com email recipient. Spectra Logic does not save emailed files unless they are specifically requested for troubleshooting.

9. The Export Password screen displays.

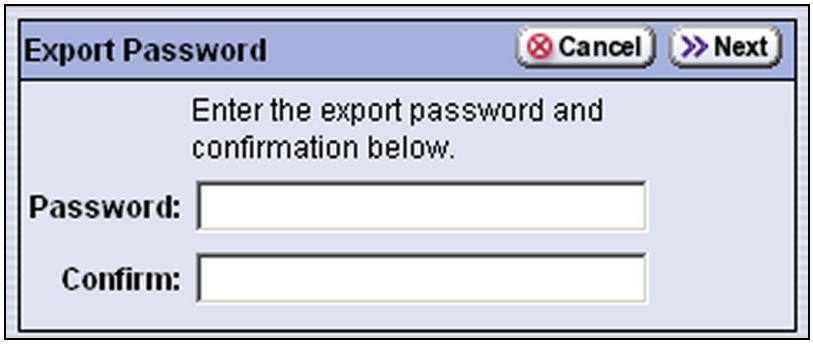


Figure 215 Enter and confirm a password for the exported encryption key.

10. Type and retype an export password using any combination of the numbers **0-9**, lower and upper case alphabetic characters (**a-z** and **A-Z**), and the at symbol (@), dash (–), underscore (_), and period (.) characters. This key is used to encrypt the exported key.

11. Make a record of the encryption key password; you need it in order to import the key back into the library. Without the password, you cannot import the key, and the data encrypted using the key is inaccessible.

Caution

Do not lose the encryption key password. Without it, you cannot reimport an encryption key after it is deleted from the library, and the data encrypted using the key is inaccessible.

12. Click **Next** to export the key to the selected location. If you selected the option to split the key across M-of-N shares on multiple USB devices, remove the USB device from the LCM when you are prompted to do so, insert another USB device, and allow time for the device to mount.

13. Confirm that the encryption key was correctly exported.

    - **If you exported the encryption key to a USB device**—Immediately confirm that the encrypted key copied correctly by clicking **Check Key Files** and following any prompts. If desired, save or print the Check Key Files report for an audit record showing that the USB device was readable, and that the destination key matched the source key. Use the steps in Verify the Exported Encryption Key to provide a second confirmation.

Figure 216 Use **Check Key Files** to confirm successful export.

    If the confirmation indicates the key did not copy correctly, delete all data from the USB device so that no trace of the failed export file remains, then export the key again using a different USB device, beginning with Step 2 on page 316.

    - **If you exported the encryption key using email**—Confirm the receipt of the email with the attachment by contacting the user to whom you sent the encrypted key file. Have them confirm that the email attachment contains a key file as described in Verify the Exported Encryption Key.

Verify the Exported Encryption Key

After exporting an encryption key, verify that the export was successful as soon as possible.

When Saved to a USB Device

1. Plug the USB device into a computer that is not connected to the library.
2. Examine the contents of the USB device to verify that it contains a file called *name*`.bsk` if you exported the key as a single file or *name*`.bss` if you exported the key as a share, where *name* is the moniker you assigned to the key when it was created.

   Make sure that the file is more than 0 bytes in size. If the file meets these requirements, the encryption key was successfully exported and is usable.
3. Store the USB device in a safe location.

4. If you exported the key as M-of-N shares, repeat Step 1 through Step 3 for each additional USB device.
5. If the exported key file is not present or if the file is 0 bytes in size, repeat the export process as described in Export an Encryption Key on page 316 using a different USB device.

When Sent as an Email Attachment

1. Open the email attachment and verify that it contains at least one file called *name*`.bsk` if you exported the key as a single file or *name*`.bss` if you exported the key as a share, where *name* is the moniker you assigned to the key when it was created.

   Make sure that the file is more than 0 bytes in size. If the file meets these requirements, the encryption key was successfully exported and is usable.
2. Save the email attachment to a safe location from which you can copy it to a USB device, if needed.
3. If you exported the key as M-of-N shares, have each share recipient perform Step 1 and Step 2 for each emailed share.
4. If the email attachment does not contain the exported key file or if the file is 0 bytes in size, repeat the export process as described in Export an Encryption Key on page 316.

Protect the Encryption Key

In conformance with your security plan, track the location of each USB device containing the exported key or the name of each person who received the email message with the exported key file attached. Also keep track of the password you used when you exported the key.

Caution Make sure you keep a record of the password created when exporting the key. You must have this password *and* the encrypted file containing the exported key in order to import the encryption key back into the library. Without the key password, you are not able to import the encryption key.

Important Backup files of the library configuration include any encryption keys that were stored in the library at the time the file was created.

The following guidelines outline the essential tasks required to protect encryption keys:

- Save one or more copies of every key using the Key Export option on the Encryption Configuration screen (see Export an Encryption Key on page 316.

Caution

As a matter of best practice, Spectra Logic recommends exporting encryption keys to a USB device instead of using email.

Although emailing encryption keys is supported by the library, doing so presents security issues, including the following:

- Copies of encryption keys may be left on the email servers used for sending and receiving email and are thus subject to compromise.
- The difficulty in verifying where all the copies of emailed encryption keys may be located can make security audits more challenging.

- If you choose to store only a single copy of an encryption key make sure that you keep the copy secure. If something happens to the device where you stored the exported key and the key was deleted from the library, both the key and all data encrypted using the key are unrecoverable.

Caution

To emphasize: If you lose the encryption key or the password for the exported file, your data is **unrecoverable** if the key was deleted from the library. You need to balance the number of copies of the key to store to guarantee access to the encrypted data against the security risk associated with storing multiple keys. Make sure that the key is successfully stored prior to removing a key from the library.

- Store encryption keys offsite in a location other than the site used for media storage. Confirm that the key is stored correctly on the USB device or was received by the intended recipient before deleting the key from your system. If you delete the key, you must import the key back into the library in order to decrypt the data that was encrypted using the key. Importing keys is described in Import the Required Key Into the Library on page 325.

  You may want to make two copies of a key, storing each in a secure location. Keep a record of each key's location so that you can easily find the key when you need to restore or delete data.

- Maintain a list of every password associated with each key and securely store the list. Never keep this list as cleartext (unencrypted text) on a networked computer, or send it through email as cleartext. For added security, encrypt the file containing the list of passwords.

- Track every copy of each key. This tracking is critical in order to meet requirements that may govern data retention and data destruction. Destroying all exported copies of keys associated with encrypted data AND deleting the keys from the library is sufficient to satisfy data destruction requirements, since encrypted data cannot be accessed without the key used to encrypt it.

  Spectra Logic recommends tracking the information listed in the following table for every key that you create. For added security, encrypt the file containing the tracking information.

Key moniker:	
Number of shares (if any):	
Number of key copies:	
Location of each copy:	
Password(s) associated with exported copy of the moniker:	
Location of cartridges containing data that are encrypted using this moniker:	
Moniker creation date:	
Planned expiration date:	

Restoring Encrypted Data

Overview Restoring encrypted data from a cartridge follows the standard data restore processes that you use with your storage management software. The only difference is that the key used to encrypt the data being restored needs to be stored in the library and assigned to the partition in which the encrypted cartridge is loaded. If the key is already stored on the library, the data is automatically decrypted as it is read from tape; if the encryption key is not currently stored on the library, it must be imported before the data can be decrypted. Once the required encryption key is assigned to the partition, standard restore procedures are unchanged.

Three Passwords to Access Import Key Functions If you have BlueScale Professional Edition and you enabled Multi-User mode, two of the three encryption passwords are required to access the import key function. See Configure the User Mode (BlueScale Professional Only) on page 292) and Configure the Secure Initialization Mode (BlueScale Only) on page 293 for information about enabling Multi-User mode and configuring the library to support multiple encryption passwords.

Requirements for Importing Keys Split into M-of-N Shares If you have BlueScale Professional Edition and you exported the encryption key as M-of-N shares, then M shares are required in order to import an encryption key into the library. See Export as M-of-N Shares on page 315 for information about using the M-of-N shares option.

Keys that are split into shares can only be imported from USB devices; they cannot be uploaded through the BlueScale web interface. If the shares were sent as email attachments, each share must be copied to a separate USB device in order to import the key.

For example, if you select the 2-of-3 option and exported the key to USB devices, two of the three USB devices, along with the encryption key password, are needed to import the key.

Use a Key Stored in the Library

If the encryption key used to encrypt the data is currently stored in the library, use the following steps to decrypt and restore data.

> **Note:** If the data was not encrypted using the key currently stored in the library, the library prompts you with the moniker of the key that is required to decrypt the data. You must import the key as described in Import the Required Key Into the Library on page 325 before the data can be restored.

1. If you selected Secure Initialization, access the encryption feature (see Log Into the Encryption Feature on page 291).
2. If necessary, import the cartridges containing the data to be decrypted into the library (see Importing Cartridges on page 203).
3. If the partition containing the cartridges does not currently have the required encryption key assigned to it, modify the partition as described in Assign the Encryption Key to a Partition on page 312.

   > **Note:** If you assigned the required password to the partition as an additional key, you do not need to modify the partition to make the key primary.

4. Use your storage management software to restore the data. The data is automatically decrypted using the stored key.

Import the Required Key Into the Library

If the encryption key required for a specific set of encrypted data was deleted from the library, the library prompts you with the moniker of the key that is required to decrypt the data. Use the key moniker to identify the required encryption key, then import the key into the library as described in this section. After you assign the imported key to the partition containing the encrypted cartridge, the key is available for decrypting data.

Important In addition to the file containing the exported key, you need the password for the key file in order to import the key into the library. Without the key password, you are not able to import the encryption key.

Note: If you are using BlueScale Encryption Standard Edition and there is already an encryption key stored in the library, you must first delete that key as described in Deleting an Encryption Key from the Library on page 329. You can then import another key.

As described in the following sections, you can import the encryption key from a USB device or from a remote computer through the library's BlueScale web interface.

Important You cannot import a key that was exported using M-of-N shares using the BlueScale web interface. You must use multiple USB devices to import the key. If the shares of the encrypted key were distributed as email attachments, the required number of shares (M) must be copied to separate USB devices before the key can be imported and used to decrypt and restore data.

- Import the Key from a USB Device
- Import the Key Using a Remote Connection to the Library on page 327

Import the Key from a USB Device

Use the following steps to import a key stored on a USB device.

Note: If you exported the key as M-of-N shares, you must have the required number shares (M) available on separate USB devices.

1. Access the encryption feature (see Log Into the Encryption Feature on page 291).

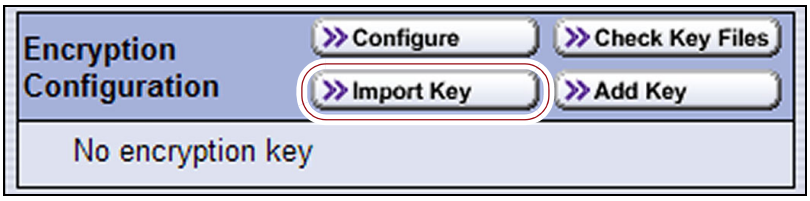


Figure 217 Click **Import Key** to begin the key import process.

2. Plug the USB device containing the exported encryption key you want to import into a USB port on the LCM and allow time for the device to mount.

   Note: If the key was exported as M-of-N shares, plug the USB device containing one of the shares into the LCM.

3. From the Encryption Configuration screen, click **Import Key**.

   - If you selected Multi-User mode for Professional Edition and you did not already enter a second encryption user password, you are prompted to enter another password. Enter one of the encryption user passwords that you did not use during the initial login, then click **Next**. The Encryption Key Files Source screen displays.
   - Otherwise, the Encryption Key Files Source screen displays immediately.

   Note: If you are accessing the library from the operator panel, the Import Key Selection screen displays instead of the Encryption Key Files Source screen.

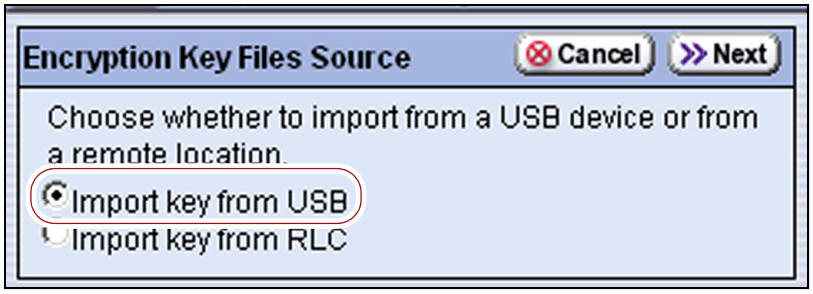


Figure 218 Select **Import key from USB** to retrieve the key file from the USB device.

4. Select **Import key from USB**, and then click **Next**. The Import Key Selection screen displays.

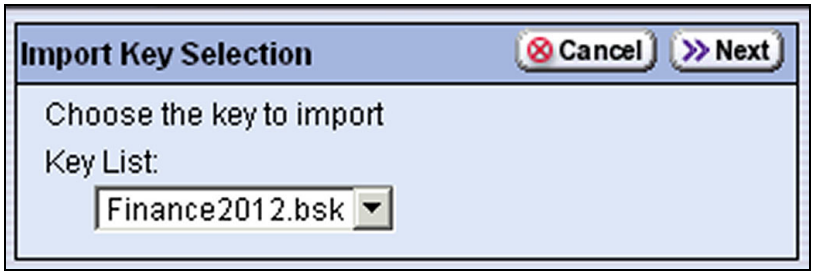


Figure 219 Select the key you want to import.

5. Choose the key to import from the **Key List** drop-down list, then click **Next**. The Import Password screen displays.

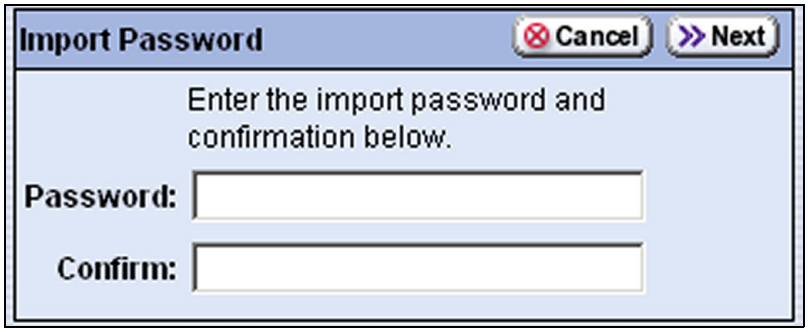


Figure 220 Enter and confirm a password for the importing encryption key.

6. Type and retype the password that was used to encrypt the key file when it was exported (see Export an Encryption Key on page 316). Click **Next**.

   Note: If the key was exported as M-of-N shares, connect each of the required UBS drives, one after the other, when prompted. For each share, type and retype the password that was used to encrypt the key file when it was exported. The password is the same for all of the shares.

7. When the key import is complete, the Encryption Configuration screen displays, showing the moniker of the newly imported key.
8. Assign the imported key to the partition which contains the encrypted cartridge (see Assign the Encryption Key to a Partition on page 312).
9. Use your storage management software to restore the data.

Import the Key Using a Remote Connection to the Library

Use the following steps to import a key from a remote computer using the library's BlueScale web interface (RLC).

Notes:
- The option to import a key from a remote computer is only available if you are accessing the library using the BlueScale web interface.
- The key must be accessible to the computer you are using to access the library's BlueScale web interface.
- Importing a key from a remote computer is not supported for keys that were split into M-of-N shares.

1. Access the encryption feature (see Log Into the Encryption Feature on page 291).

Figure 221 Click **Import Key**.

2. From the Encryption Configuration screen, click **Import Key**.
   - If you have Professional Edition with Multi-User mode enabled and you did not already enter a second encryption user password, you are prompted to enter another password. Enter one of the encryption user passwords that you did not use during the initial login, then click **Next**. The Encryption Key Files Source screen displays.
   - Otherwise, the Encryption Key Files Source screen displays immediately.

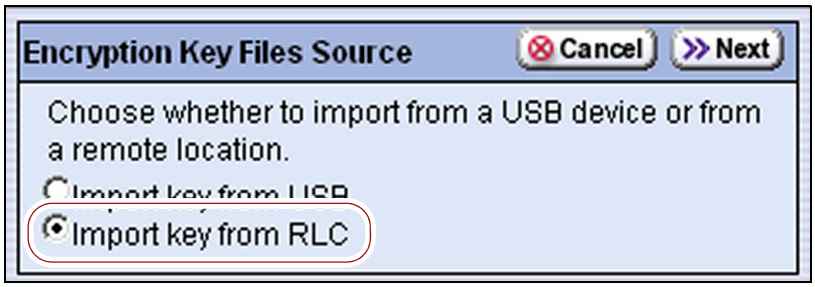


Figure 222 Select **Import key from RLC** to upload the key file from a remote computer.

3. Select **Import key from RLC**, and then click **Next**.

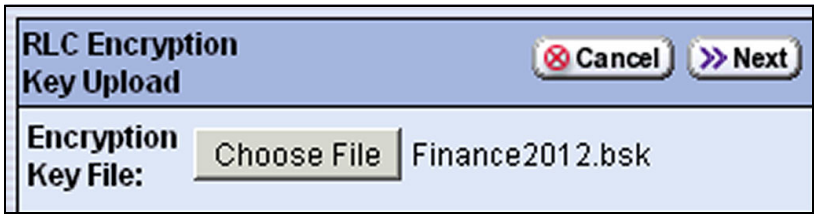


Figure 223 Enter the name of the key file you want to import.

4. Click **Choose File** and use the Open dialog box to navigate to the location where the key is stored.
5. Select the key file, then click **Open**. The RLC Encryption Key Upload redisplays with the filename for the key next to the **Choose File** button.
6. Click **Next**. The Import Password screen displays (see Figure 220 on page 327).
7. Enter the password that was used to encrypt the key file when it was exported (see Export an Encryption Key on page 316).
8. Click **Next**. The Encryption Configuration screen displays, showing the moniker of the newly imported key.
9. If necessary, assign the imported key to the partition in which the cartridge with the encrypted data is stored (see Assign the Encryption Key to a Partition on page 312).
10. Use your storage management software to restore the data.

Deleting an Encryption Key from the Library

Overview BlueScale Encryption Standard Edition only supports storing a single encryption key in the library. You must first delete the key currently stored in the library before you can create a new key and assign it to one or more partitions (see Assign the Encryption Key to a Partition on page 312).

BlueScale Encryption Professional Edition supports storing up to 30 encryption keys in the library. If, in accordance with your key retirement policies, an encryption key is no longer to be used, you can remove the key from the library.

Caution Make sure that you export a copy of the existing key before you delete it. You need a copy of the exported key and its password to import the key back into the library and restore data that was encrypted with the key.

Important Backup files of the library configuration include any encryption keys that were stored in the library at the time the file was created.

Use the following steps to delete a key:

1. Access the encryption feature (see Log Into the Encryption Feature on page 291).
2. Export at least one copy of the key and store it in a safe location (see Export an Encryption Key on page 316).
3. If the encryption key you plan to delete is assigned to a partition, either as the primary key or as a decryption-only key, edit the partition to disable encryption (see Disabling Encryption in a Partition on page 330 or assign a different key (see Assign the Encryption Key to a Partition on page 312).

   Note: If you delete an encryption key that is assigned to a partition you are not able to encrypt or decrypt data in that partition until you reimport the key.

4. From the Encryption Configuration screen, click **Delete** next to the key you want to remove from the library and respond to the confirmation screens to delete the key.

Figure 224 Click **Delete** to remove the key from the library.

5. The Encryption Configuration screen redisplays with a message indicating that the key was successfully deleted. The moniker is no longer listed on the screen.

Figure 225 The Encryption Configuration screen shows that the key was successfully deleted.

Disabling Encryption in a Partition

Use the following steps to disable encryption in a partition:

Note: If you are not already logged in as an encryption user, you must enter the encryption password before you create or edit a partition using the BlueScale partition wizard. If you are not logged in, the Encryption screen does not display.

1. Access the BlueScale partition wizard (see Accessing the Partition Wizard on page 169).
2. Select the partition for which you want to disable encryption. Click **Edit**.
3. Click **Next** to navigate through the partition wizard screens until you reach the Encryption screen (see Figure 208 on page 312).
4. Select **No Encryption**.
5. Click **Next** to move to the next partition configuration screen. Navigate through the remaining partition configuration screens by clicking **Next**.
6. When you reach the Summary screen, click **Save**.

Recycling Media

Overview Encryption-enabled LTO-4 and later generation drives require that all data encrypted and written to a single cartridge use the same encryption key—that is, a single key is associated with all the encrypted data on an individual cartridge. If you want to change the encryption key associated with a cartridge that was encrypted using BlueScale Encryption, you must first recycle the cartridge using the BlueScale Recycle Encryption Media feature. In addition, you must recycle the cartridge before you can re-use it if you lose the encryption key for the cartridge.

Caution After encrypted media is recycled using this process, the data is unrecoverable.

Notes:
- If you plan to use the same key that was used to encrypt the data already on the cartridge, you do not need to recycle the cartridge using the process described in this section.
- Make sure that the storage management software cannot access the drive you plan to use for recycling the encrypted media.
- The recycle media operation can only be performed from the library operator panel. You cannot access the Import/Export screen when using the BlueScale web interface from a remote computer.
- This feature is for cartridges encrypted using BlueScale encryption only, not Spectra SKLM encryption.

User Privilege Requirement Any user with operator privileges who is assigned to the partition and all users with superuser or administrator privileges can recycle encrypted cartridges. See Specify the Partition Users on page 186 for information about assigning users to a partition.

Requirements You cannot run backup or restore operations while the library is recycling encrypted cartridges. If you have a large number of cartridges to process, make sure that you wait until the library is idle.

Important Before beginning the recycle process, use your software to take the library off-line or stop all backup or restore operations to the partition. Attempting to recycle media while the host is issuing commands to the library through the exporting drive may cause the backup or restore operation to fail. In addition, the library may hang and require a restart in order to continue operations.

Use the following steps to recycle one or more encrypted LTO cartridges so that they can be reused with a new encryption key.

1. From the operator panel, log into the library as a user with the appropriate privileges (see User Privilege Requirement).

2. Click **MENU**, then select **General** ⋯⁘ **Import/Export**. The Import/Export screen displays showing the information for the last partition that was viewed on either the Import/Export screen or the Inventory screen.
3. Select the partition that contains the cartridges you want to recycle from the drop-down list, then click **Go**. The Import/Export screen refreshes to show the current status of the slots assigned to the selected partition.

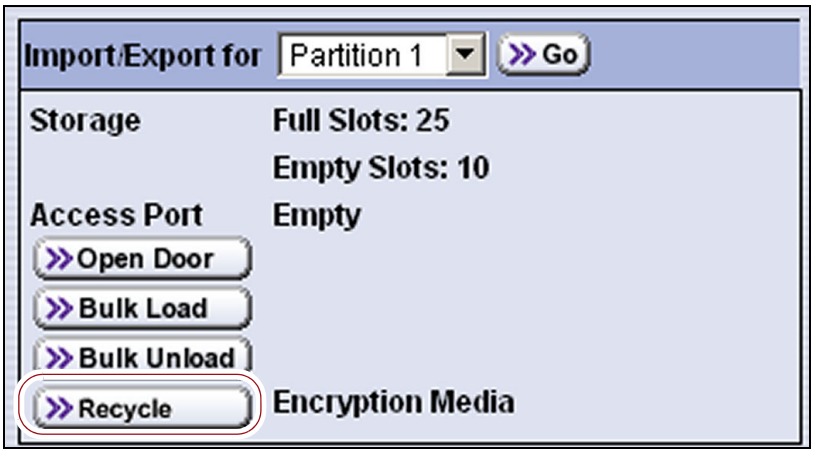


Figure 226 Click Recycle on the Import/Export screen.

Note: If the library only has one partition configured, the Import/Export screen shows that partition and does not include a drop-down list.

4. Click **Recycle**. The Select Tapes screen displays a list of all of the cartridges currently in the partition, both encrypted and unencrypted.

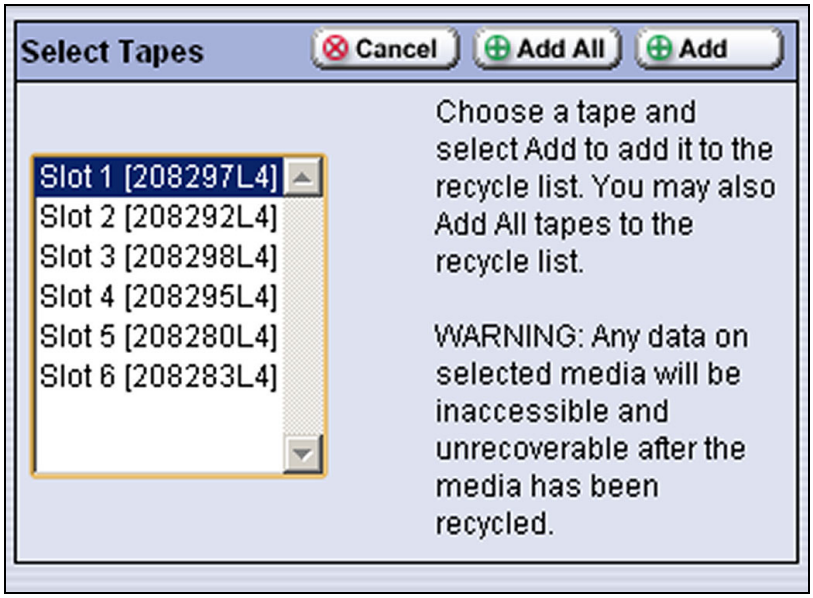


Figure 227 Select the first cartridge to recycle.

5. Select the cartridge that you want to recycle, then click **Add**. If you want to recycle all of the cartridge in the list, click **Add All**. The Tapes to Recycle screen displays with the cartridge you selected shown in the list.

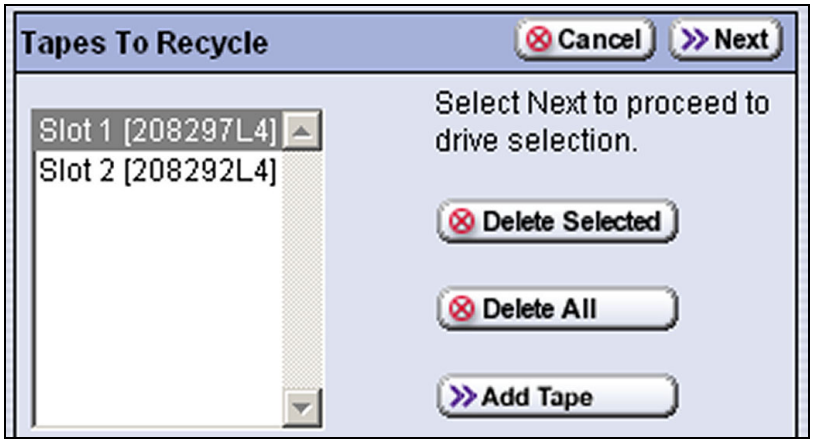


Figure 228 The Tapes to Recycle screen.

6. To select additional individual cartridges for recycling, click **Add Tape** and repeat Step 5.
7. To remove cartridges from the list, select the cartridge in the list on the left side of the Tapes to Recycle screen and click **Delete Selected** or click **Delete All** to remove all of the cartridges from the list.
8. After you select all of the cartridges that you want to recycle, click **Next** on the Tapes to Recycle screen. The Select Drive screen displays.

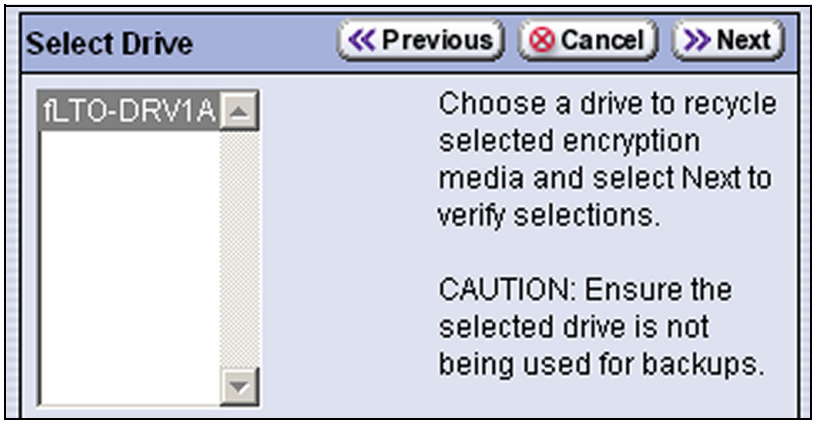


Figure 229 Select the drive to use for recycling the cartridges.

9. Select the drive that you want to use for recycling the cartridges, then click **Next**. The Summary screen displays.
10. Verify your selections, then click **Recycle** to begin the recycling operation.

Note: Once the recycle operation starts, you cannot perform any other library operations until it is complete.

CHAPTER 11

Configuring and Using AutoSupport

This chapter describes how to configure and use AutoSupport with your library. All AutoSupport functionality is included with your library purchase.

AUTOSUPPORT OVERVIEW

AutoSupport configures the library to automatically notify support personnel or others with messages when specific events occur. It can also be used to open or update a support ticket and send it to a specified recipient or to Spectra Logic Technical Support. AutoSupport can be used without configuring the library with email access by saving the AutoSupport Log (ASL) files generated by AutoSupport to a USB device and then manually sending an email containing the stored information to Spectra Logic Technical Support.

Note: ASL information is only for troubleshooting purposes. This log information is separate from the data path and contains no customer data.

Send Log Sets

This feature lets you manually generate a standard ASL file and email it to a pre-configured recipient or save it to a USB device. You can use the Send Log Sets option to open or update a support ticket and send it to a specified recipient or to Spectra Logic Technical Support. The ASL included in the support ticket includes the following types of information:

- Library message logs
- Library Control Module (LCM) logs
- LCM configuration (including the current physical configuration)
- A simplified report of the MLM and DLM databases
- Engineering Change (EC) version data from all components
- BlueScale version
- Contact information for data center staff
- Other library information specified in the AutoSupport user profile

Log Forwarding

This feature configures the library to send monthly ASL files to preconfigured recipients (see Configure Log Set Forwarding on page 344).

Critical Alarms

When you enable critical alarms, the library automatically generates an ASL file whenever any of the events in the following table occurs. If you configured one of your AutoSupport profiles as the AutoSend Profile, the library automatically sends the ASL file to the mail recipients in the AutoSend profile.

Note: If you select autosupport@spectralogic.com as a mail recipient in the AutoSend profile, the library also sends the ASL file and a ticket request to Spectra Logic Technical Support.

For this event...	An AutoSupport ticket request is generated...
Motion Restart	Whenever motion restarts. Each motion restart is treated as a separate event and results in generation and submission of an AutoSupport ticket request.
Drive Failure	When the library detects a drive failure that results in the percentage of failed drives in a partition meeting or exceeding the specified threshold. The following drive problems can generate a drive failure event: ▪ Failure of the drive firmware or hardware ▪ Loss of communication between the library and the drive ▪ Removal of a drive from the library without using the BlueScale Drive Remove or Drive Replace operation. AutoSupport ticket requests are not generated if the drive is removed following a Drive Remove or a Drive Replace operation.
LCM Fails to Initialize	If the LCM fails to properly initialize.

CONFIGURING AUTOSUPPORT

If you have any questions about configuring AutoSupport, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

Note: To simplify entering the information required to configure and use AutoSupport, use the BlueScale web interface or a keyboard attached to the LCM.

Network and Support Contract Requirements Before you configure AutoSupport, Spectra Logic recommends connecting the library to an email gateway. You need to do the following:

- Connect a 10/100BaseT Ethernet cable to the Ethernet connector on the LCM (see Figure 10 on page 35).
- Obtain the library's IP address, subnet, and gateway address (see Configure Network Settings on page 98).
- Obtain the AutoSupport Customer/Contract Number for the library from Spectra Logic.

User Privilege Requirements Only a user with superuser or administrator privileges can configure the AutoSupport features. See Understanding User Groups and Security on page 94 for information about the three types of user groups and what types of privileges each has.

Configure Mail Recipients

If not already completed, configure one or more mail recipients who should receive AutoSupport information (see Configure Mail Users on page 107). At a minimum, configure Spectra Logic Technical Support (**autosupport@spectralogic.com**) as a mail recipient if you want to automatically send AutoSupport ticket requests to Spectra Logic Technical Support. If desired, you can configure additional recipients.

Notes:
- The default autosupport@spectralogic.com mail recipient can be used for any ASL or HHM files that are generated by the library. This includes those generated manually, or automatically in response to critical events or log forwarding.
- Do not configure the autosupport@spectralogic.com mail recipient to receive messages that result from configuration changes or system messages generated by the library.
- AutoSupport can be used without email access by saving the information generated by AutoSupport to a USB device and then manually sending the stored information to Spectra Logic Technical Support.

Configure AutoSupport Profiles

Use the following steps to create or modify a profile for each person assigned to work with Spectra Logic Technical Support to troubleshoot problems with the library or drives.

1. Log into the library as a user with superuser or administrator privileges.
2. Click **MENU**, then select **Maintenance ⋯⁘ AutoSupport**. The AutoSupport screen displays.

   Notes:
   - If you have not yet configured an AutoSupport profile, the **Send Log Set** button is grayed out.
   - If you have not configured a profile for AutoSend, the **Configure Alarms** button is grayed out.

Figure 230 Click **Manage Profiles** to create, modify, or delete an AutoSupport profile.

3. Click **Manage Profiles**. The AutoSupport Profiles screen displays.

Figure 231 Use the AutoSupport Profiles screen to manage profiles.

Create or Modify a Profile

1. From the AutoSupport Profiles screen, click **New** to create a new profile or click **Edit** to modify an existing profile. The Company Info screen displays.

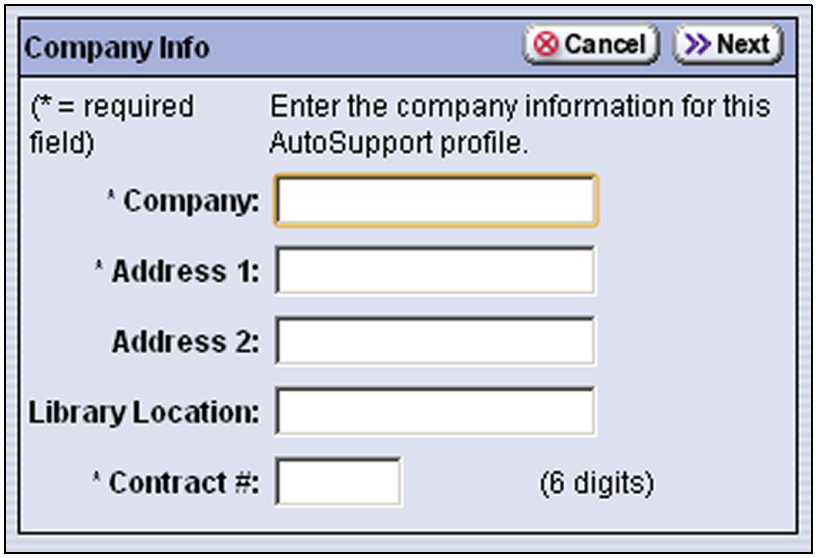


Figure 232 Enter the required information for your company.

- Complete the information in this screen. The information marked with an asterisk (*) is required.

Note: Make sure to fill in *all* of the required fields in each of the following screens. You cannot advance to the next screen if required information is missing.

- The Customer/Contract Number is no longer used. Enter any six alpha-numeric characters.

2. Click **Next**. The Contact Info screen displays. Enter the information for your contact person in the fields provided. This information determines how Spectra Logic contacts this person.

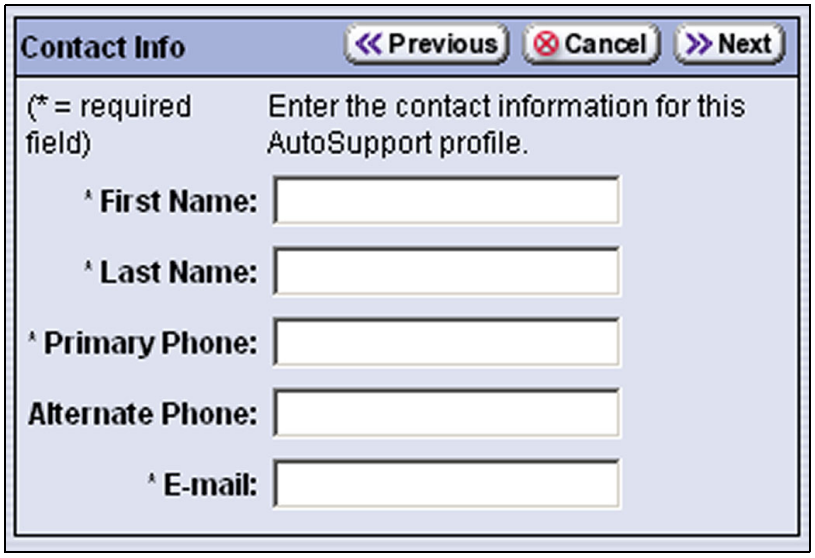


Figure 233 Enter the required information for the contact person.

3. Click **Next**. The System Info screen displays. Enter information about your library's operating environment and storage management software in the fields provided.

Note: Entering this information is optional. However, providing as much information as possible helps the ticket recipients in their assessment of the issue.

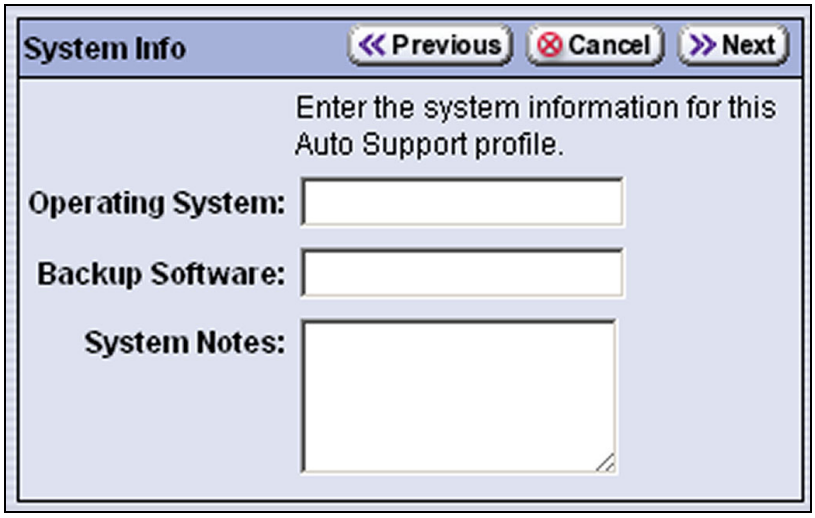


Figure 234 Enter information about your operating environment.

4. Click **Next**. The Mail Users screen displays.

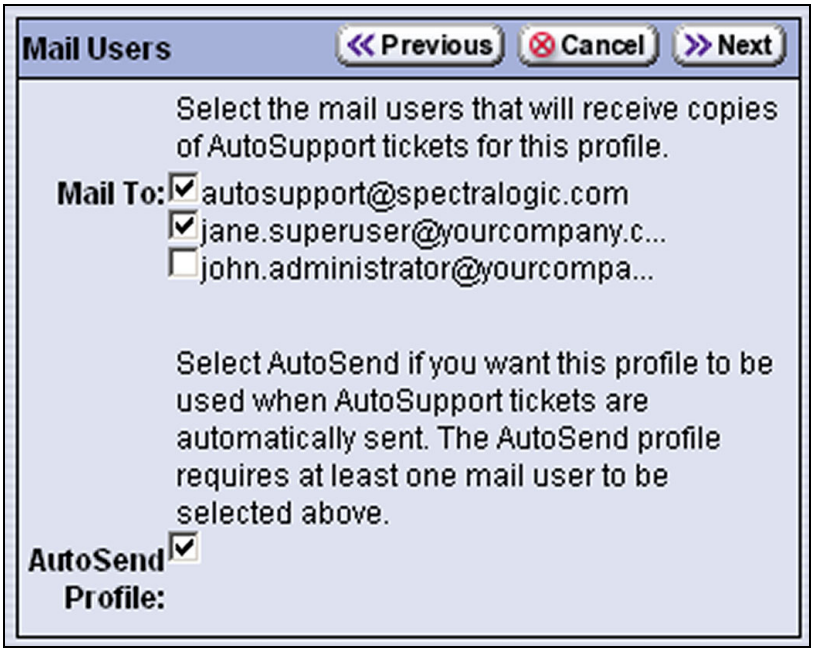


Figure 235 Select the mail users who are associated with the profile.

- Select the mail user(s) whom you want to receive copies of AutoSupport tickets from the **Mail To** choices presented. Only mail recipients that were previously configured are listed (see Configure Mail Users on page 107).

Note: You must select **autosupport@spectralogic.com** as one of the recipients if you want the library to send an AutoSupport ticket request to Spectra Logic Technical Support.

- Use the **AutoSend Profile** check box to configure the current profile as the recipient for critical alarm log sets automatically sent by the library.

Notes:
- Only one profile can be configured as the AutoSend profile. The profile can include multiple mail users as recipients for the AutoSupport tickets and critical alarm log sets.
- Configuring one of the profiles as the AutoSend recipient enables the **Configure Alarms** button on the AutoSupport screen (see Figure 230 on page 337).

5. Click **Next**. The Summary screen displays. Verify that all of the information shown is correct.

   If any information needs to be changed, click **Previous** to display the screen in which the changes need to be made.

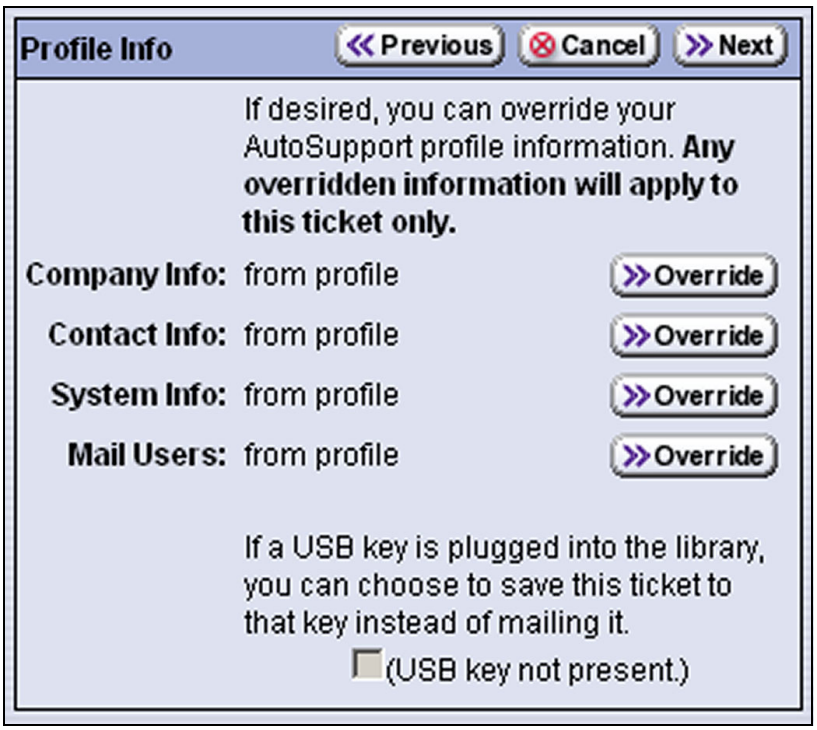


Figure 236 Review the profile information.

6. When all of the information is correct, click **Save**. The AutoSupport screen displays.
7. Repeat Step 1 through Step 6 if you want to create additional profiles.

   Note: When you create multiple profiles, they are listed in the order in which they are created, not in alphanumeric order.

8. If desired, click **Manage Profiles**. AutoSupport Profiles screen displays, listing the newly completed profile.

Figure 237 All of the AutoSupport profiles are listed on the AutoSupport Profiles screen.

Delete an AutoSupport Profile

Use the following steps to delete an existing profile.

1. Log into the library as a user with superuser or administrator privileges.
2. Click **MENU**, then select **Maintenance ···⁘ AutoSupport**. The AutoSupport screen displays (see Figure 230 on page 337).
3. Click **Manage Profiles**. The AutoSupport Profiles screen displays (see Figure 237 on page 341).
4. Click **Delete** next to the contact you want to remove.
5. Click **Yes** on the Confirmation screen. The AutoSupport screen redisplays.

Configure Alarms (Optional)

Use the steps in this section if you want the library to automatically generate an ASL file in the event that any of the critical events listed under Critical Alarms on page 335 occurs.

Note: The **Configure Alarms** button is only available when one of the AutoSupport profiles is configured as the AutoSend recipient (see Step 4 on page 340).

1. Log into the library as a user with superuser or administrator privileges.
2. Click **MENU**, then select **Maintenance ···⁘ AutoSupport**. The AutoSupport screen displays.

   Note: If you have not configured a profile as the AutoSend recipient, the **Configure Alarms** button is grayed out.

Figure 238 Click **Configure Alarms** to configure how AutoSupport handles alarms.

3. Click **Configure Alarms**. The AutoSupport Alarm Handling screen displays.

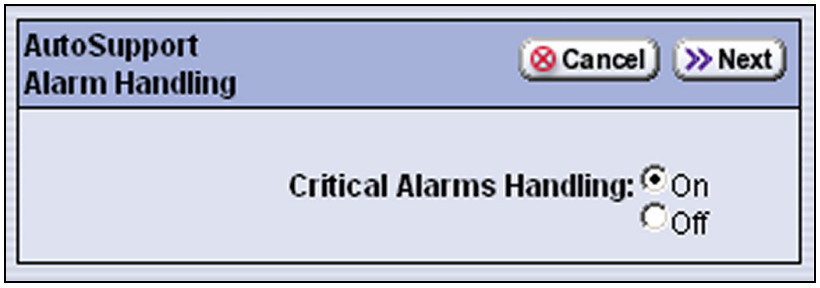


Figure 239 Select **On** for **Critical Alarms Handling** to enable the critical alarm handling.

4. Select **On** to enable **Critical Alarm Handling**. When enabled, the library generates an ASL file whenever one of the critical events listed under Critical Alarms on page 335 occurs. Any ASL file that is generated as a result of a critical event is automatically sent to all of the recipients selected in the AutoSend profile.

   Note: The autosupport@spectralogic.com address must be selected as a mail recipient in the AutoSend profile if you want the library to send critical event ASL files to Spectra Logic Technical Support.

5. Click **Next**. The Critical Alarms: Drive Failures screen displays.

Figure 240 Select the **Failure Threshold** for the drives in any single partition.

6. If desired, change the setting for the **Failure Threshold** for failed drives in the library. This threshold is the only configurable critical event.

   The failure threshold is the percentage of all drives in a partition whose failure causes an AutoSupport ticket request to be generated. You can select 25% or 50%; the default is 50%. The threshold applies to all partitions in the library.

7. Click **Next**. The AutoSupport Alarms Summary screen displays.

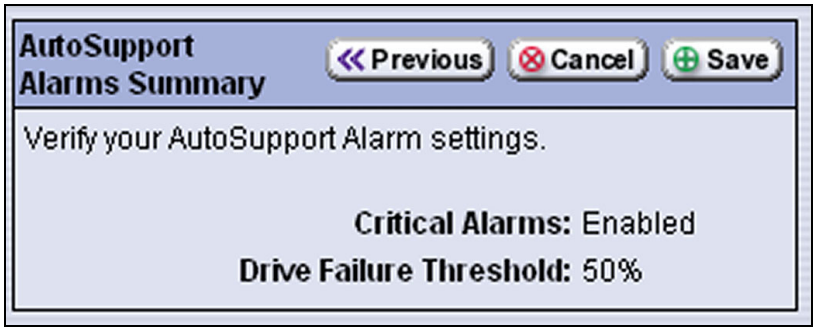


Figure 241 Review the AutoSupport Alarms Summary screen.

8. Click **Save** to save your changes or click **Cancel** to return to the AutoSupport screen without saving your changes.

   After your changes are saved, the AutoSupport screen displays.

Configure Log Set Forwarding

Log forwarding is enabled by default from the factory. This is a monthly log set that is forwarded to Spectra Logic for data collection. No action is taken by Spectra Logic Technical Support for a particular library when the log set is received, but the data is parsed and stored in our database to better understand our field population and how the library is used and how it can be improved.

Note: ASL information is only for troubleshooting purposes. This log information is separate from the data path and contains no customer data.

1. Log into the library as a user with superuser or administrator privileges.
2. Click **MENU**, then select **Maintenance** ···⁘ **AutoSupport**. The AutoSupport screen displays.

Figure 242 Click **Log Forwarding** to configure log set forwarding.

3. Click **Log Forwarding**. The Log Forwarding screen displays.

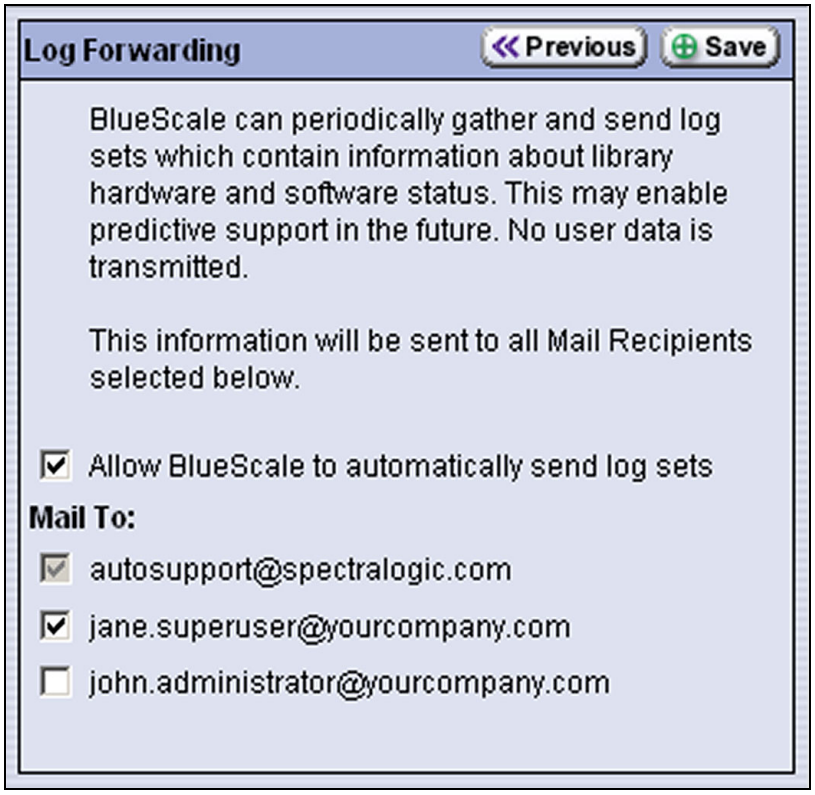


Figure 243 Select the mail recipients who you want to receive the automatically generated ASL files.

4. Select the forwarding options you want to use.
   - **Allow BlueScale to automatically send log sets** is selected by default. Clear the check box if you do not want the library to submit the monthly log sets when they are generated.
   - The **autosupport@spectralogic.com** mail recipient is selected by default. All ASL files generated by the library are automatically sent to Spectra Logic Technical Support.
   - Select any additional mail recipient(s) from the **Mail To** choices presented. Only mail recipients that were previously configured are listed (see Configure Mail Users on page 107).
5. Click **Save**.

   After your changes are saved, the Log Forwarding screen redisplays with a confirmation message.
6. Click **Previous** to return to the AutoSupport screen.

USING AUTOSUPPORT TO CREATE OR UPDATE A TICKET

User Privilege Requirements Only a user with superuser or administrator privileges can open and modify support tickets using AutoSupport. See Understanding User Groups and Security on page 94 for information about the three types of user groups and what types of privileges each has.

Use the following steps to open a new ticket with Spectra Logic Technical Support or to update a previously submitted AutoSupport ticket.

Notes:
- If *autosupport@spectralogic.com* is included in the **Mail To:** field for the autosupport profile used to submit a ticket, then Spectra Logic immediately sends a confirmation email to the email address listed in the autosupport profile used to submit the ticket, and a support person contacts the person submitting the ticket during normal service contract hours.
- If it is during your service contract hours and the problems requires immediate attention, call Spectra Logic Technical Support after submitting the AutoSupport ticket (see Contacting Spectra Logic on page 7).
- Go to Spectra Logic's website at: support.spectralogic.com/services-and-contracts/support-offerings/ for information about the warranty and service options for your library.

1. Log into the library as a user with superuser or administrator privileges.
2. From the toolbar menu, select **Maintenance ⋯⁘ AutoSupport**. The AutoSupport screen displays.

Figure 244 Click **Send Log Set** on the AutoSupport screen.

3. If you want to save the AutoSupport ticket information to a USB device, insert the device into the LCM's USB port (see Figure 10 on page 35) and allow time for the device to mount.

   Note: The option to save the ticket to USB is only available if you plug a USB device in to the LCM's USB port before you click **Send Log Set**.

4. Click **Send Log Set**. The Select Profile screen displays.

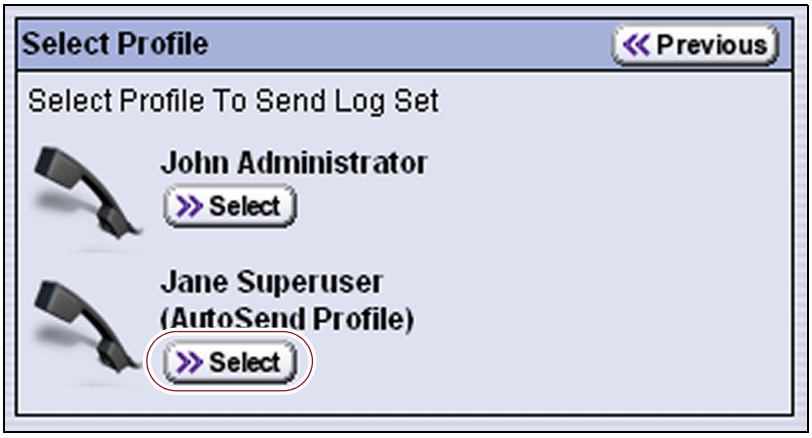


Figure 245 Click **Select** under the profile you want to use for sending the AutoSupport ticket.

5. Click **Select** next to the profile for the main contact person for the issue. The Open Ticket screen displays.

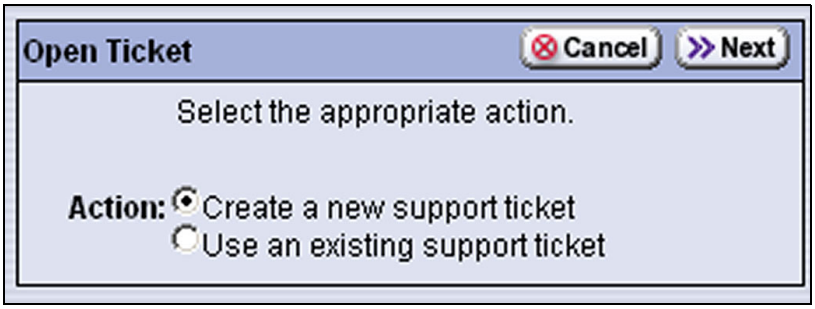


Figure 246 Select the type of ticket you want to open.

- If this is a new ticket, select **Create a new support ticket**. This option is selected by default.
- If you are sending additional information about an existing support ticket, select **Use an existing support ticket**. Updating a ticket is particularly useful for mailing new logs to Technical Support.

Notes:
- You must have the reference number for the existing ticket—which you receive when you open the ticket—and the information you are sending must be related to the specific issue reported in *that* ticket.
- If you have a new issue with your library, open a new ticket to address that issue separately.

6. Click **Next**. The Description screen displays.

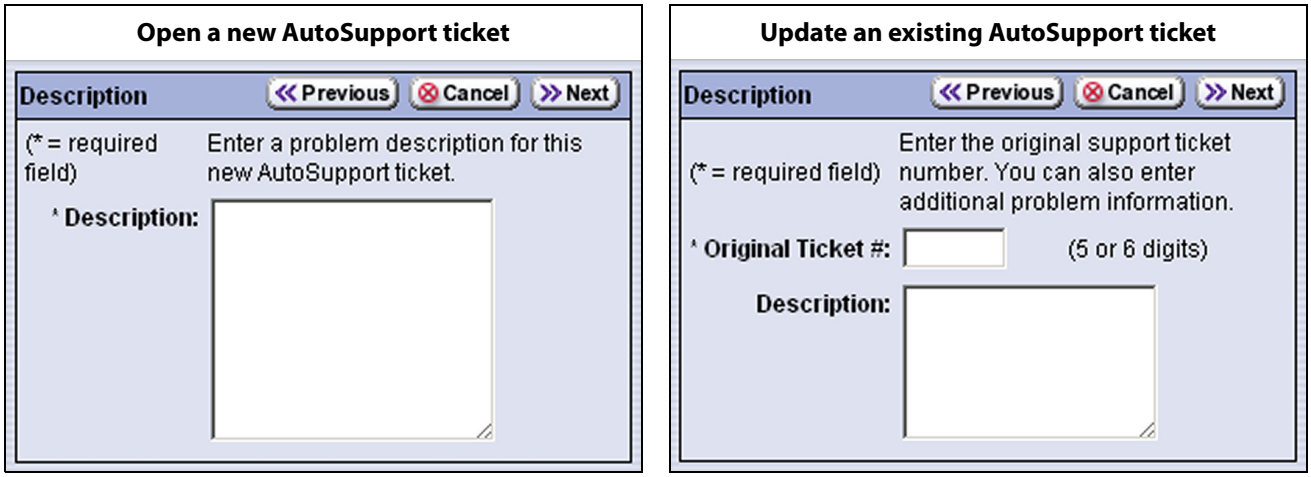


Figure 247 Enter or update the information about the issue.

- Type a detailed description of the issue in the **Description** field, including what happened just before the failure occurred.

Note: Supplying a detailed problem description helps support personnel to address the issue more quickly and efficiently.

- If you are sending additional information about an existing support ticket, enter the ticket number in the **Original Ticket #** field.

7. Click **Next**. The Profile Info screen displays.

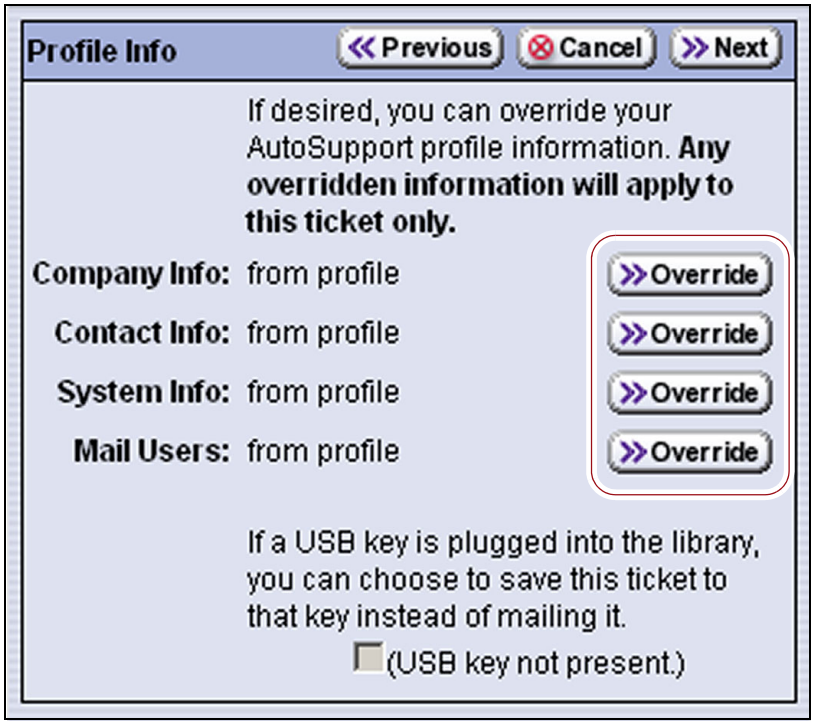


Figure 248 Use **Override** to temporarily change the profile information.

8. Review the information on the Profile Info screen.

   - If you do not need to make any changes to the contact person's information for this support ticket, proceed to Step 9 on page 350.
   - If you need to *temporarily* change the contact person's information for this ticket, click **Override** next to the information you need to update. The screen associated with the information displays. See Configure AutoSupport Profiles on page 337 for information about each of the profile screens.

     Make any necessary changes in the Profile Summary screen, then click **Override**. The Profile screen redisplays.
   - If the library is not connected to a network with an SMTP server, select the check box at the bottom of the screen to save the ticket information to a USB device *instead* of emailing it from the library.

   Notes:
   - The USB option is only available if you plugged a USB device into a USB port on the LCM before you clicked **Send Log Set** to begin the ticket process.
   - After saving the ticket information to the USB device, you can upload it to the Technical Support portal (see Accessing the Technical Support Portal on page 472).

9. Click **Next**. The Summary screen displays.

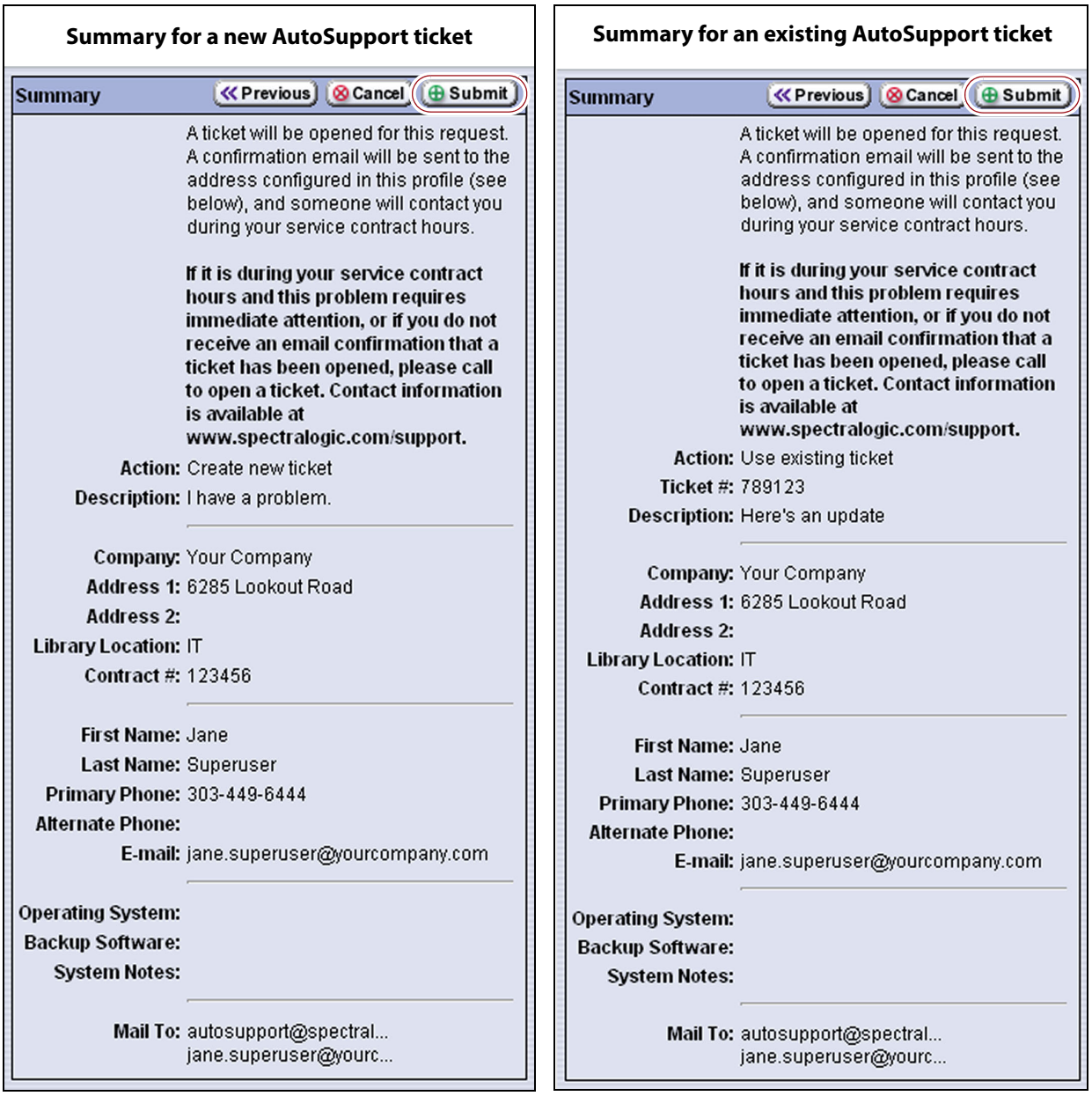


Figure 249 Review the ticket summary then click **Submit**.

10. Verify that all information is correct.

- If all of the information is correct, click **Submit**. A progress screen indicates that the ticket request (with log information) is being sent. When completed, the AutoSupport Profiles screen displays.

  When Spectra Logic receives the request, a ticket is opened and an email response is sent to the user with a ticket number.

- If you need to make changes, do the following:

  a. Click **Previous** to return to the screen for the information that needs to be changed.

  b. Modify the problem description as required.

  c. Select **Next** until you reach the Summary screen.

  d. If all of the information is correct, click **Submit**.

CHAPTER 12

Library Troubleshooting

This chapter describes troubleshooting steps you can take, as appropriate, to help resolve problems you might encounter while operating the library. Try these troubleshooting procedures *before* you open a support ticket with Spectra Logic Technical Support. If you are unable to resolve the problem yourself, open a support ticket (see Opening a Support Ticket on page 474).

Note: The library must be under warranty or have a valid service contract in order to qualify for support (see Service Contract Extension on page 495 to learn about service contracts).

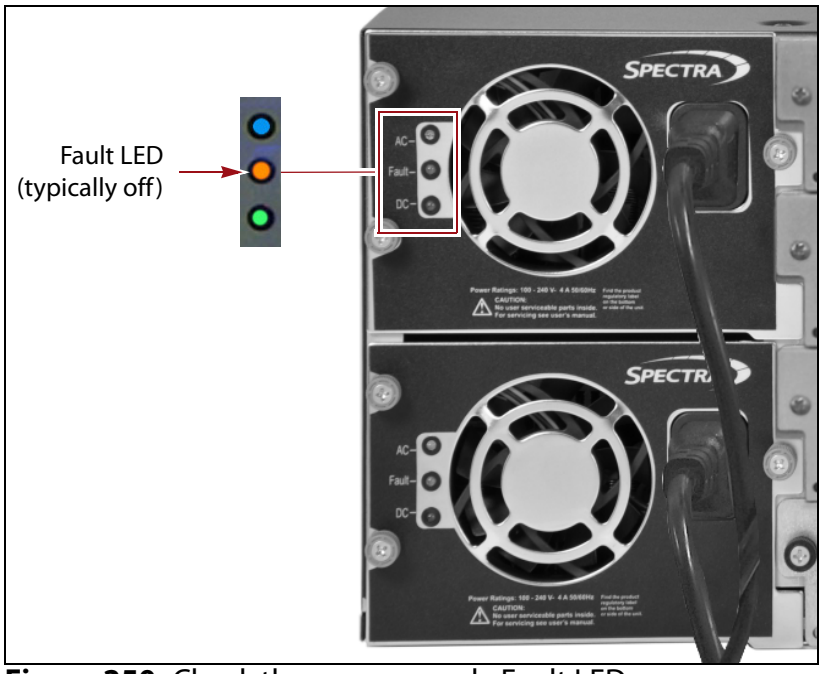
GETTING HELP WITH LIBRARY ISSUES

If you have a problem with your library, use the information in this section to obtain help with resolving the problem.

Check...	To...
Error Sense Codes	Look up the definition of an error sense code referenced in a system message using the *Spectra Tape Libraries SCSI Developer Guide*.
Library BlueScale Version	Confirm that your library is at the latest released version of the BlueScale software (see Check the Library BlueScale Software Version on page 423). Some problems with library components may be fixed by updating the component firmware if the library is using a downlevel version of BlueScale software.
System Messages	Review any System Messages that were posted by the library (see Check and Respond to Messages on page 143) and take any action described in the message(s).
Technical Support Portal	Find information about the most current version of BlueScale software and additional service and support tools. You can access the Technical Support portal at support.spectralogic.com. **Note:** Accessing many of the tools available on the Technical Support portal requires creating a user account. See Accessing the Technical Support Portal on page 472 for instructions. ▪ Check the options under the **Documentation** and **Knowledge Base** menus for additional troubleshooting information. ▪ Check the **Service & Contracts** menu to view information about the warranty and service options available for your library as well as the Spectra Certified Media warranty.

TROUBLESHOOTING LIBRARY HARDWARE ISSUES

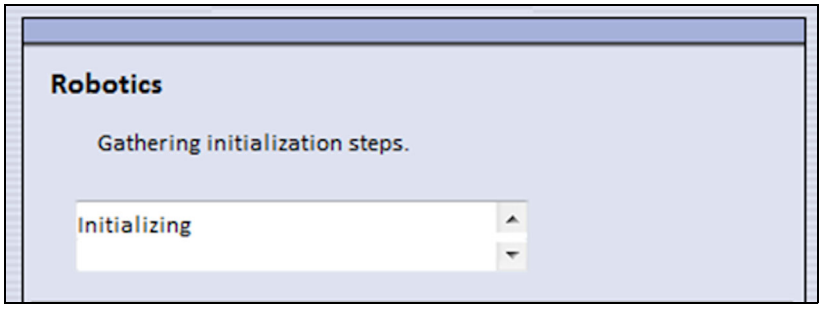
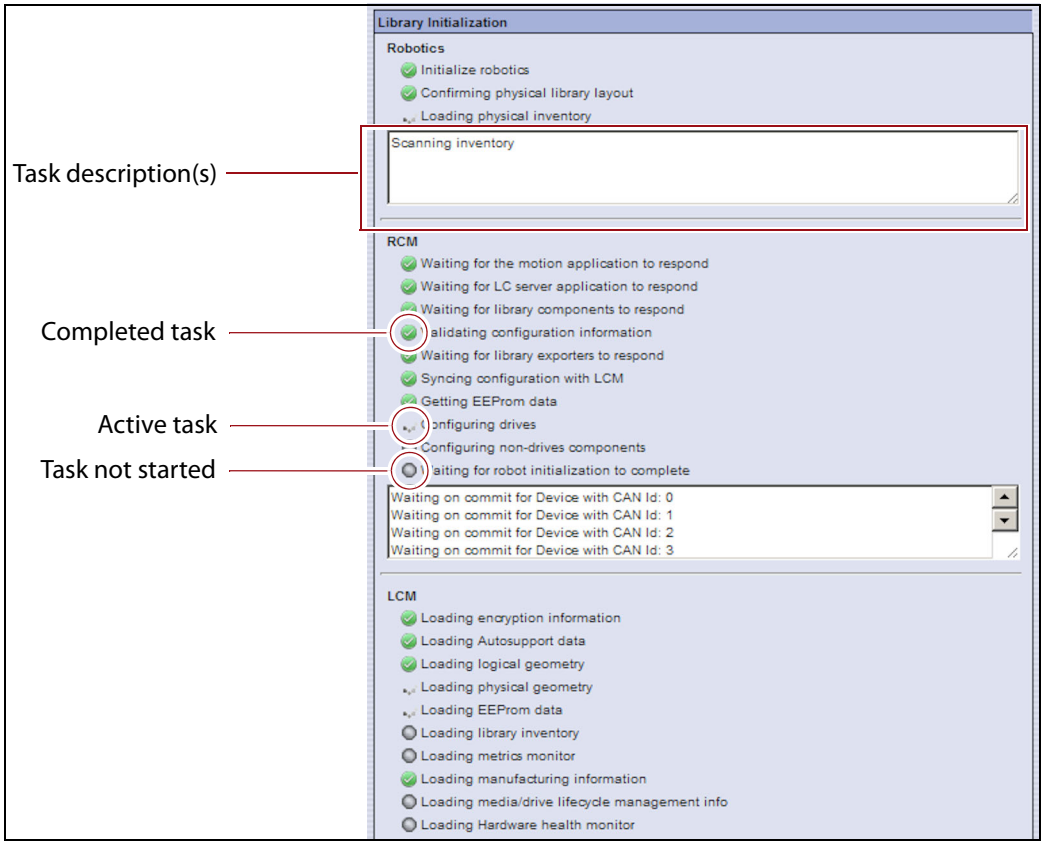
This section provides information about potential hardware issues that you may experience during the initial installation and when you make configuration changes.

Issue	Resolution
Power Supplies	If you have a redundant power supply installed, periodically check the Fault LED on each power supply to ensure that the power supplies are functioning properly.  **Figure 250** Check the power supply Fault LED.
Host Bus Adapter Compatibility	Make sure that the Fibre Channel, SAS, or SCSI HBA you are using to connect the library to the host is supported by Spectra Logic. Refer to the *Spectra T50e Library Release Notes and Documentation Updates* for current information about the supported HBAs.
SAS Connectivity	Keep these requirements in mind as you plan your SAS connections: ▪ Do not exceed bus length restrictions. The maximum allowable length of a SAS bus is 13 feet (4 meters). ▪ LTO-5 and higher SAS drives cannot be daisy-chained. ▪ Use a standard 6 GB SAS HBA.

Issue	Resolution
SCSI Connectivity	Keep these guidelines in mind as you plan your SCSI connections: ▪ **Do not exceed SCSI bus length restrictions**. The maximum allowable length of an LVD SCSI bus is 39 feet (12 meters). **LTO-3:** ▪ A maximum of two LTO-3 SCSI tape drives can be daisy-chained on a single SCSI bus. ▪ When daisy-chaining LTO-3 tape drives, use a cable length of at least 12 inches and that does not require making tight bends in the cable. **LTO-4:** Spectra Logic does not support daisy-chaining LTO-4 drives. ▪ **General:** ▪ Keep in mind that each daisy-chained LTO-3 drive increases the total length of the SCSI bus. ▪ Connecting multiple devices on a single SCSI bus can impact the performance of all devices on the bus. The data transmission rate to any drive on the bus is limited to the maximum transfer rate of the SCSI bus. ▪ Spectra Logic does not recommend, and does not support, daisy-chaining other SCSI devices on the same SCSI bus as the drives in the library. **Note:** Although a maximum of 15 devices can be connected to a single wide LVD SCSI bus, attaching more than two devices to a single SCSI bus can potentially have a negative impact on the performance of all devices on the bus.
SCSI Bus Termination	If the SCSI bus is not properly terminated you may experience one or more of the following failure symptoms: ▪ Read/Write failures ▪ Bus hangs ▪ Connectivity issues—tape drive is not seen on bus or drops off bus ▪ Command failures—commands to a tape drive may fail while commands to other devices on the bus may work properly If you experience sporadic errors and are using SCSI drives in the library, make sure that the SCSI bus connected to each tape drive is properly terminated at both ends. ▪ **LTO-3:** If a LTO-3 tape drive in the library terminates the SCSI bus, either as the last drive in a daisy chain or as the only drive connected to the bus, install a wide Ultra 3 Active SCSI terminator on the tape drive's second SCSI connector. ▪ **LTO-4:** Install a wide Ultra 3 Active SCSI terminator on the tape drive's second SCSI connector (do not daisy-chain LTO-4 SCSI tape drives).

TROUBLESHOOTING LIBRARY INITIALIZATION ISSUES

This section provides information about potential library initialization issues that you may experience.

Issue	Resolution
Library hangs while gathering initialization tasks	The library gathers tasks at the beginning of the library initialization process, and displays this as its first task on the Library Initialization screen. If the library is unable to gather the required initialization tasks within a few minutes of powering on, contact Spectra Logic technical support for assistance. 
Library hangs during initialization	If the library cannot complete the initialization process, it generates system messages and enter maintenance mode. Contact Spectra Logic technical support for assistance (see Contacting Spectra Logic on page 7). Do not power off the library. 

TROUBLESHOOTING BLUESCALE USER INTERFACE ISSUES

This section provides information about potential issues that you may experience while using the library's BlueScale user interface, either from the operator panel or through the web interface (RLC).

Issue	Resolution
BlueScale screens exhibit display problems	Occasionally, the BlueScale interface may exhibit display problems (for example, one screen displays on top of another), either on the operator panel user interface or through the web interface. Use the refresh button ( ) on the status bar to refresh the screen. **Important:** If you are accessing the library through the BlueScale web interface, do not use the keyboard to refresh the screen (for example, by pressing **F5**). Doing so may cause unpredictable results.
Cannot access the library using the BlueScale web interface (RLC)	Check the following: ▪ Make sure that the library is connected to the network via an Ethernet cable connected to the LCM. ▪ Make sure that an IP address is configured for the library (see Configure Network Settings on page 98). ▪ Make sure that the web server port is correctly configured for your environment (see Configure the Library Web Server Settings on page 110). ▪ If SSL is enabled for the library, make sure that you enter the IP address using the form: **`https://[`*`library IP address`*`]`**. See Configure the Library Web Server Settings on page 110 for additional information. **Important:** The T50E uses TLS 1.0 and does not have functionality for higher versions of TLS. ▪ If none off the above resolves the issue, reset the library to make sure that the Ethernet port is not hung (see Resetting the Library on page 372).

Cannot change a configuration setting	Before attempting to change configuration settings, do the following:
	▪ **Recommended.** Make sure that all of the drives in the partition are empty.
	▪ Make sure that the host is not communicating with the library.
	▪ Make sure that no background processes are running (for example, Media Auto Discovery, PreScan, or PostScan). If a background process is running, the library displays a message indicating what it is.
	  ▪ If the background process is Media Auto Discovery, PreScan, or PostScan and you cannot wait for the process to complete, you can stop or pause the operation (Stop the Discovery Process on page 252 and Pause the PostScan Process on page 261).
	  ▪ For all other background processes, wait until the process is completed and then try changing the configuration again.

Issue	Resolution

Cannot create a new storage partition	Make sure that you have:
	▪ An active SLS key to support multiple partitions entered in the Option Keys screen (see Enabling BlueScale Software Support, Options, and Upgrades on page 112).
	▪ Unassigned, licensed slots available for use in the new partition. If necessary, modify an existing partition to make slots available (see Modifying an Existing Partition on page 191), or license additional slots with a CoD capacity key (see Capacity-On-Demand (CoD) on page 496).
	▪ No partitions already configured for Standard Entry/Exit mode. You need to edit the existing partition to change the Entry/Exit mode before you can create a cleaning or storage partition.
	▪ One or more drives available for use in the new partition. If necessary, modify an existing partition to make one or more drives available or install additional drives.
	▪ Fewer than four storage partitions configured. The library supports a maximum of four storage partitions when using half-height drives or two partitions when using full-height drives.
	▪ Make sure that no background processes are running (for example, Media Auto Discovery, PreScan, or PostScan). If a background process is running, the library displays a message indicating what it is.
	  ▪ If the background process is Media Auto Discovery, PreScan, or PostScan and you cannot wait for the process to complete, you can stop or pause the operation (Stop the Discovery Process on page 252 and Pause the PostScan Process on page 261).
	  ▪ For all other background processes, wait until the process is completed and then try creating the partition again.

Cannot import or export cartridges.	Make sure that no background processes are running (for example, Media Auto Discovery, PreScan, or PostScan). If a background process is running, the library displays a message indicating what it is. ▪ If the background process is Media Auto Discovery, PreScan, or PostScan and you cannot wait for the process to complete, you can stop or pause the operation (Stop the Discovery Process on page 252 and Pause the PostScan Process on page 261). ▪ For all other background processes, wait until the process is completed and then retry the import or export operation.
Cannot log into the library. **Forgot a user name or password.**	Log into the library as one of the superusers configured for the library. See Configuring Library Users on page 94 for a list of the default user names and passwords. **Note:** The library must always have at least one superuser configured. Make sure that you keep a record of the superuser's username and password if you delete the default superuser (su). If you do not know the username or password, open a support ticket to Spectra Logic Technical Support (see Opening a Support Ticket on page 474) to obtain assistance.

Issue	Resolution

Cannot use a Global Spare drive to replace a malfunctioning drive in the partition.	▪ Make sure that a Global Spare drive is assigned to the partition (see Assign a Global Spare Drive on page 179).
	▪ Make sure that no background processes are running (for example, Media Auto Discovery, PreScan, or PostScan). If a background process is running, the library displays a message indicating what it is.
	  ▪ If the background process is Media Auto Discovery, PreScan, or PostScan and you cannot wait for the process to complete, you can stop or pause the operation (see Stop the Discovery Process on page 252 and Pause the PostScan Process on page 261).
	  ▪ For all other background processes, wait until the process is completed and then try using the Global Spare again.

Operator panel touch screen displays broken graphics or an error message.	▪ Click **Menu** then select the desired menu to refresh the display ▪ If the user interface is unusable, reset the library (see Resetting the Library on page 372).
System message states that the BlueScale Software Support key expired.	A valid BlueScale Software Support key is required before you can update BlueScale software and library firmware. Renew the key as described in Renewing the BlueScale Software Support Key on page 419
Touch screen buttons and text fields are out of alignment.	Recalibrate the touch screen (see Calibrating the Touch Screen on page 438).
USB device does not appear as a "save to" option.	▪ Make sure that you plug the USB device into the LCM and allow time for the device to mount before you select the option that saves data to the USB device. ▪ The library only recognizes FAT-formatted, not NTFS-formatted, USB devices. Try using a different USB device. ▪ If the problem persists, reset the library to make sure that the USB port is not hung (see Resetting the Library on page 372).

TROUBLESHOOTING MLM ISSUES

This section provides information about potential issues that you may experience while using MLM.

Issue	Cause	Resolution
An asterisk (*) appears next to the barcode on the MLM Details screen or an MLM report.	The cartridge was exported from the library.	If you do not intend to reimport the cartridge, you can delete it from the MLM database (see Delete MLM Records From the Database on page 275).
An "x" appears next to a barcode in the Inventory screen.	The cleaning cartridge is expired.	Export the expired cartridge or exchange it for a new one (see Exporting or Exchanging Cartridges on page 214).
The library does not proactively discover new cartridges when they are imported.	The discovery process (Media Auto Discovery or PreScan) cannot begin while the hosts are actively loading cartridges into or unloading cartridges from the drives. If you import cartridges during this time, the library posts a failure message stating that no drives are available to perform the discovery process.	Either wait until the library is idle before beginning an import operation or manually start the discovery process for imported cartridges when the library is idle. See Initiate Media Discovery Manually on page 250 for instructions.
The media health reported by MLM for LTO-4 media changed after it was loaded into an LTO-5 or LTO-6 drive.	The algorithm used to determine MLM media health in LTO-5 and later generation drives differs from the algorithm used for LTO-4 drives. For BlueScale software versions earlier than BlueScale12.0.7, when LTO-4 media is used in both LTO-4 and LTO-5 or LTO-6 drives, the media health reported by MLM is inconsistent between the two drive generations. Beginning with BlueScale12.0.7, after an LTO-4 cartridge is loaded into an LTO-5 or later generation drive, the library adjusts the algorithm used to calculate the media health score whenever the cartridge is subsequently loaded into an LTO-4 drive. This adjustment ensures that the reported media health is consistent, regardless of whether the LTO-4 cartridge is used in an LTO-4 or an LTO-5 or later generation drive.	As a best practice for your LTO-4 media, Spectra Logic recommends that you configure LTO-4 and LTO-5 or later generation drives in separate partitions and that you do not routinely share LTO-4 media between LTO-4 and LTO-5 or later generation drives.

Issue	Cause	Resolution
LTFS-formatted LTO-5 data cartridges are treated as non-MLM cartridges.	LTO-5 drives using firmware version B6W0 or later automatically move the MLM data on the cartridge MAM the first time a cartridge is loaded and then unloaded from the drive. From that point forward, the MLM data is maintained in the new location. ▪ If the cartridge is formatted to LTFS before the MLM data is moved, the MLM data is lost. ▪ If a properly prepared and LTFS-formatted cartridge is loaded into an LTO-5 drive that is not using firmware version B6W1 or later, the drive cannot locate or update the MLM data on the cartridge.	▪ If you plan to reformat your LTO-5 data cartridges to use LTFS, load and then unload each cartridge into an LTO-5 drive that is using firmware version B6W1 or later before you reformat the cartridges. ▪ To ensure full MLM tracking of your LTFS-formatted LTO-5 data cartridges, make sure all LTO-5 drives in the library are updated to firmware version B6W1 or later.

TROUBLESHOOTING ENCRYPTION ISSUES

The information in this section may help resolve encryption-related problems.

Issue	Cause	Resolution
Library can not access the Spectra SKLM server.	The Spectra SKLM server's operating system firewall does not allow the library to access the server.	If you are setting up Spectra SKLM on a Windows server, create a firewall rule on the server to allow the library to access the server. Use the port setting that was assigned to the server during the BlueScale (library) portion of the Spectra SKLM server configuration. The default port setting is 3801. See Configure the Spectra SKLM Server on page 296 to determine your port setting.
System message states that "Load attempted while encryption is enabled, but no moniker or key list was sent to the DCM."	If a cartridge is left in a drive after the library loses power or you reset or power-cycle the library, the drive is not able to receive encryption monikers. This can also occur if a tape is left in a drive while the drive is reset or reseated.	Use the following steps to re-enable the encryption process: **1.** Move the cartridge out of the drive and return it to its storage location (see Move Cartridges Within a Partition on page 226). **2.** Reset the drive (see Resetting a Drive on page 408).

Issue	Cause	Resolution
System message states that a tape drive requires a specific moniker.	The cartridge was encrypted using an encryption key that is not currently available on the library. Or, if you are using BlueScale Professional Edition, the required encryption key is available, but was not selected as one of the partition's decryption keys.	Depending on which BlueScale Encryption edition you are using, use the following steps to enable the cartridge to be read: **BlueScale Standard Edition** **1.** Log into the library as a superuser. **2.** Log into the encryption feature. **3.** Export and then delete the encryption key currently listed on the Encryption Configuration screen (see Deleting an Encryption Key from the Library on page 329). **4.** Import the required encryption key (see Import the Required Key Into the Library on page 325). **5.** Select **Configuration ⋯⁘ Partitions.** **6.** Click **Edit** next to the partition containing the cartridge. **7.** Navigate through the BlueScale partition wizard to the Encryption screen. **8.** Select the encryption key to be associated with the partition. **9.** Click **Next** to proceed to the Summary screen of the Partition Wizard, and click **Save**. **BlueScale Professional Edition** **1.** Log into the library as a superuser. **2.** Log into the encryption feature. **3.** Make sure the encryption key is listed on the Encryption Configuration screen. If it is not listed, add the key to the library (see Import the Required Key Into the Library on page 325). **4.** Select **Configuration ⋯⁘ Partitions.** **5.** Click **Edit** next to the partition containing the cartridge. **6.** Navigate through the BlueScale partition wizard to the Encryption screen. **7.** Select the required encryption key as either the primary encryption key or as a decryption key. **Note:** A maximum of eight decryption keys can be assigned to one partition. **8.** Click **Next** to proceed to the Summary screen of the Partition Wizard, and click **Save**.

Resolving Operational Issues

This section provides information about potential issues you may encounter while operating the library.

Issue	Cause	Resolution
Cartridge left in a tape drive after a library power-cycle or reset.	If the library loses power during backup operations or you reset or power-cycle the library without first unloading all of the drives, cartridges may remain in the drives.	**CAUTION:** When the Unload Drives utility runs, cartridges are unloaded from all drives in the selected partition(s), even if they are active. This could cause backups to fail. Do not use the Unload Drives utility when backup or restore operations are actively running. **1.** Select **Maintenance ⋯⁘ Utilities**. The Utilities screen displays. **2.** Click **Show Advanced**. The Advanced Utilities Confirmation screen displays. **3.** Click **Next**. The Utilities screen refreshes to show the advanced utilities. **4.** Scroll down and select **Unload Drives**. **5.** From the **Select the partition or library** drop-down list, select a partition or **Total Library**. **6.** Click **Run Utility**. **7.** A progress screen displays, all drives assigned to partitions in the library or the selected partition are unloaded, and the cartridges are returned to their original slots or the first available slot if the original slot is not available. When the operation is complete, a Utility Results screen displays. **Note:** This utility does not unload cartridges from Global Spare tape drives being used for PostScan. If there is a cartridge left in a Global Spare tape drive, see Cartridge left in a Global Spare tape drive after a library power-cycle or reset. on page 364

Issue	Cause	Resolution
Cartridge left in a Global Spare tape drive after a library power-cycle or reset.	If the library loses power or if you reset or power-cycle the library while the PostScan process is running, the cartridge being scanned remains in the drive. The library generates a message to notify you that the Global Spare contains a cartridge after it completes its initialization process.	**CAUTION:** Make sure the drive you are sparing is not actively running a backup or restore operation. This could cause backups to fail. Use the following steps to return the cartridge to its storage location: **1.** Examine the partition inventories to determine in which partition the cartridge belongs (see View the Cartridge Inventory for a Partition on page 224). **2.** Substitute the Global Spare tape drive containing the cartridge for another drive in the same partition (see Using a Global Spare Drive on page 409). **3.** Move the cartridge out of the drive and return it to its storage location (see Move Cartridges Within a Partition on page 226). **4.** Return the drive back to Global Spare status (see Undo the Global Spare Drive on page 412).
Element addresses change after installing additional drives.	Installing additional drives into the library, or removing drives from the library, may cause the library to reassign element addresses.	To avoid errors after adding a new drive, make sure that you reconfigure the element addresses your storage management software uses to access drives when you install a new drive (refer to your software documentation for instructions).
Cartridge is left in the robotics following a move.	The library was unable to insert the cartridge into its original slot and no empty slots are available. The library posts a system message and halts.	Contact Spectra Logic technical support for assistance (see Contacting Spectra Logic on page 7).

CAPTURING TRACES

Overview Spectra Logic uses traces to help diagnose problems with the library. You only need to capture traces when instructed to do so by Spectra Logic Technical Support. They indicate what type of trace you need to capture.

Emailing Trace Results If you plan to email trace results directly from the library, make sure that you previously configured the recipients as mail users (see Configure Mail Users on page 107).

If you are connected to the library using a web browser, you can also copy and paste the trace results into a text file and email it to Spectra Logic Technical Support if they request it.

Saving Trace Results to USB If you plan to save trace results to USB, you must connect the USB device to the LCM **before** you select the **Traces** on the Maintenance Tools screen (see Connect a USB Device to the Library on page 153). If a USB device is not connected, the USB option is not available. You can, however, still save trace results to the memory card in the LCM. You can also view the results without saving them.

User Privilege Requirements Only a user with superuser or administrator privileges can capture traces.

1. Log into the library as a user with superuser or administrator privileges.
2. If you want to save the traces to a USB device, connect the USB device to the LCM and allow time for the device to mount; otherwise, skip to the next step.
3. Click **MENU**, then select **Maintenance** ⋯⁘ **Traces**. The Traces screen displays with the trace options that were selected the last time the screen was viewed.

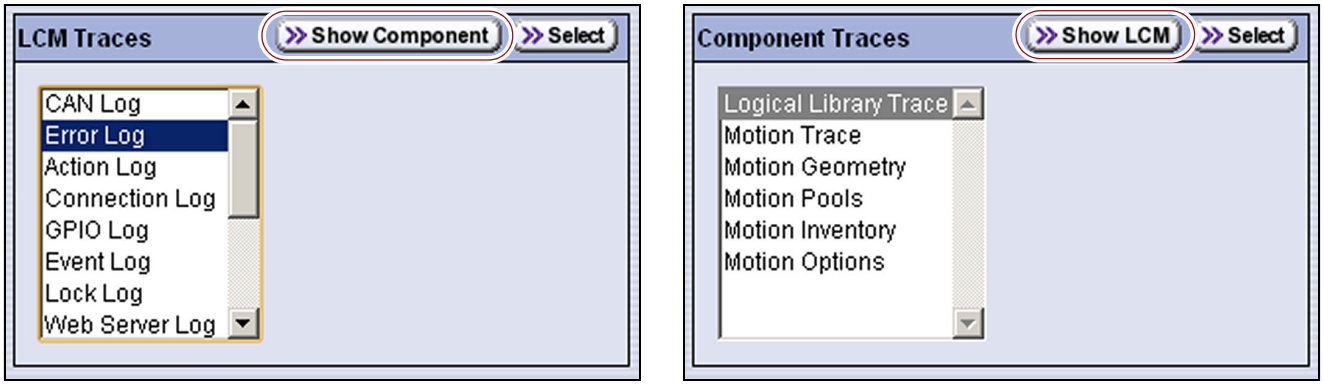


Figure 251 Click **Show Component** or **Show LCM** to select the category of traces to view.

4. Depending on the category of trace you need and which category is currently displayed, click **Show Component** or **Show LCM** to select the category of traces to view.
   - **LCM Traces**—Captures log files relating to a single aspect of operations related to the LCM.
   - **Component Traces**—Captures a trace relating to the logical library or a single aspect of operations related to the robotics.
5. Select the trace you want to capture from the list of traces, then click **Select**. The Error Log screen for the selected trace displays.

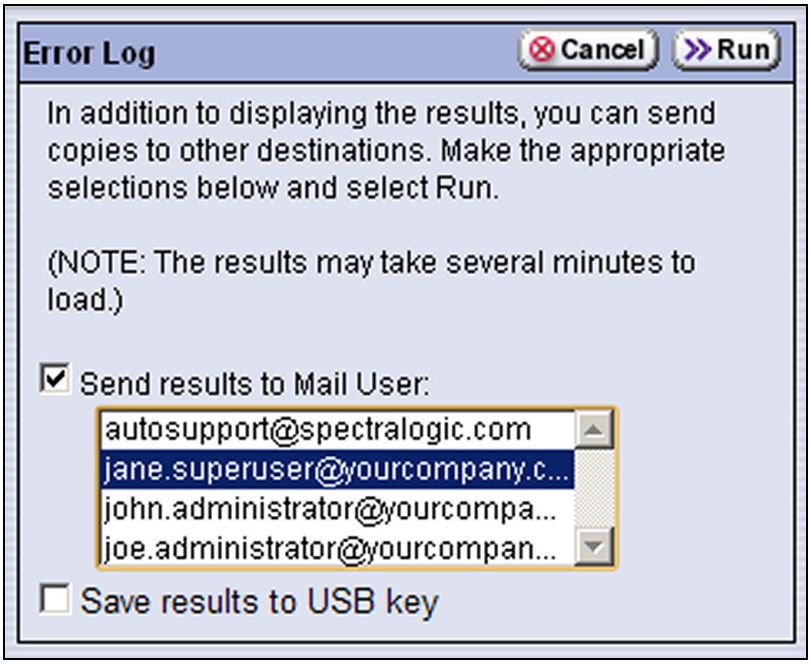


Figure 252 Select the destination for the captured trace (Error Log screen shown).

6. Use the check boxes to select any combination of the options for saving the generated trace.

Option	Description
Send results to Mail User	Sends the trace report to a previously configured mail recipient. Use the drop-down list to select the recipient for the report file. Only previously configured mail recipients are listed. To send the email with the attached trace file to someone who is not listed, exit the utility, configure that person as a mail user (see Configure Mail Users on page 107), and then run the utility again. **Note:** Do not select autosupport@spectralogic.com as a recipient. Spectra Logic does not save emailed traces unless they are specifically requested for troubleshooting.
Save to USB	Saves the report to the USB device. The results can then be viewed from any device that can read from USB. **Note:** This option is only available if you inserted a USB device in Step 2 on page 365.

7. Click **Run**. The library retrieves the requested trace, which may take several minutes, and then displays the results on the Results screen.

   Notes:
   - If you are connected to the library using a web browser, you can drag the bottom right corner of the scroll box containing the trace results to adjust the length and width of the scroll box.
   - If you are connected to the library using a web browser, you can copy and paste the results into a text file and email it to Spectra Logic Technical Support if they request it from you.

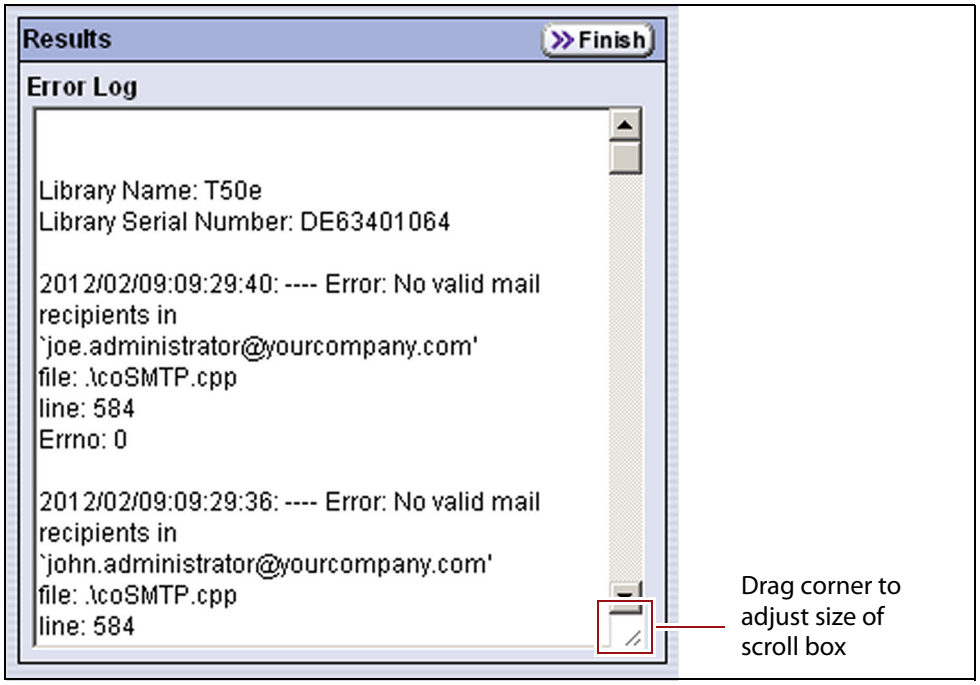


Figure 253 Review the information for the requested trace (Error Log Results shown).

8. If you chose to save the file to a USB device or mail it, a message displays showing the filename for the trace file.
9. Click **Finish** to return to the Traces screen from which you started the collection process.

VIEW HARDWARE HEALTH MONITORING (HHM) DATA

Overview BlueScale Hardware Health Monitoring (HHM) tracks maintenance thresholds for key library components. This section describes using the advanced utility called HHM: View Data to generate a report showing the current status of the HHM counters. This information includes the following:

- Library serial number and name (if configured)
- Robotics moves

Important In addition to the HHM: View Data utility, two additional HHM utilities configure the HHM counters and thresholds for the monitored components. **Do not** change the values for any counters or thresholds unless you are specifically instructed to do so by Spectra Logic Technical Support.

User Privilege Requirements Only a user with superuser or administrator privileges can respond to HHM notifications by creating an AutoSupport ticket and viewing HHM data. See Understanding User Groups and Security on page 94 for information about the three types of user groups and what types of privileges each has.

Use the following steps to view the current HHM data.

1. Log into the library as a user with superuser or administrator privileges.
2. If you want to save the HHM report to a USB device, insert the USB device into a USB port on the LCM and allow time for the device to mount; otherwise, skip to the next step.

   Note: The option to save the HHM report to USB is only available if you connect the USB device to the LCM **before** you select **Show Advanced** (see Figure 98 on page 153).

3. Click **MENU**, then select **Maintenance ···⁘ Utilities**. The Basic Utilities screen displays.

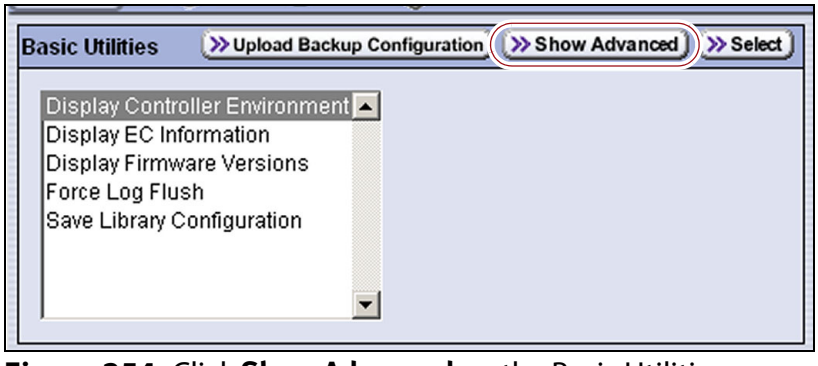


Figure 254 Click **Show Advanced** on the Basic Utilities screen.

4. Click **Show Advanced**. The Advanced Utilities Confirmation screen displays.

5. Click **Yes** to acknowledge the warning about using the advanced utilities. The Advanced Utilities screen shows a list of the advanced utilities.

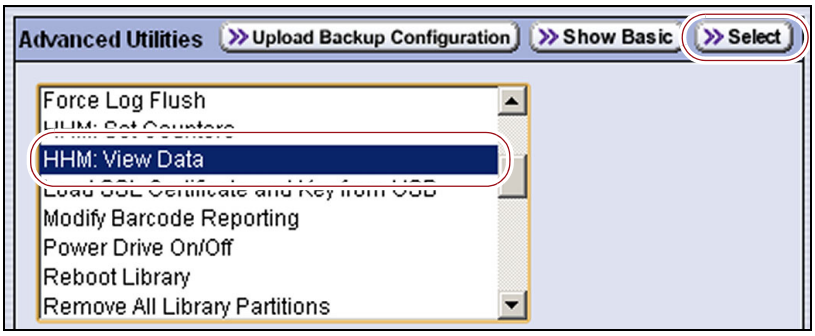


Figure 255 Select the **HHM: View Data** utility.

6. Scroll through the list of advanced utilities and select **HHM: View Data**.
7. Click **Select**. The Description screen shows information about the utility.

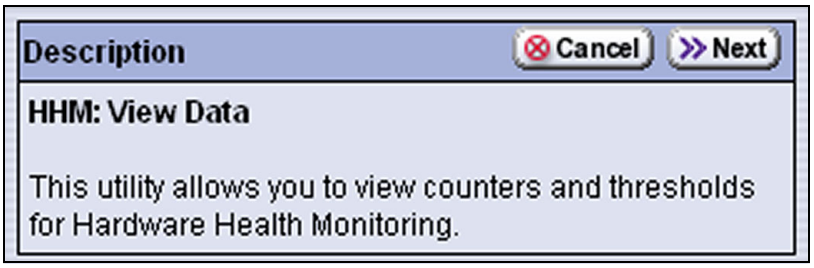


Figure 256 Read the description of the HHM: View Data utility, then click **Next**.

8. Click **Next**. The Destinations screen displays.

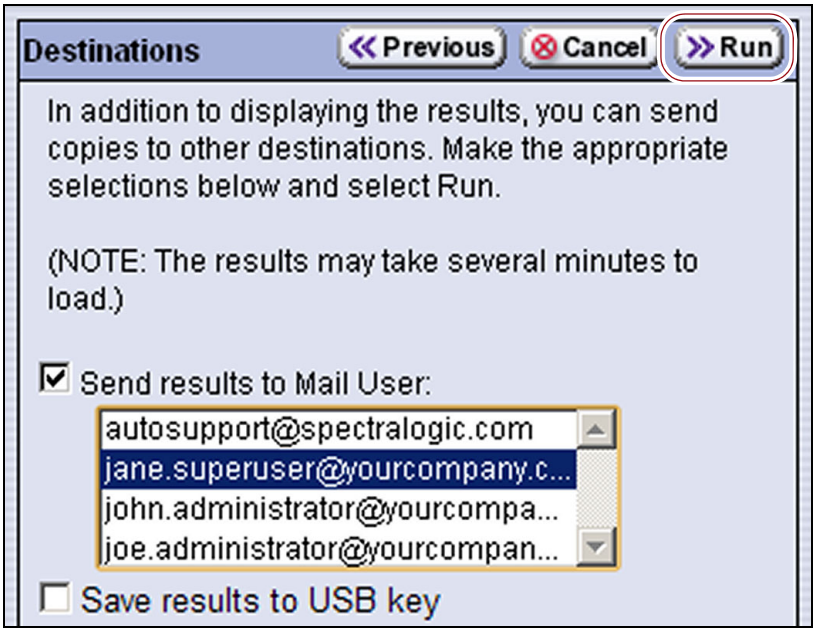


Figure 257 Select the destination for the output of HHM: View Data utility.

9. If you want to save the output from the utility, use the check boxes on the Destinations screen to select the location; otherwise skip to Step 10.

Selecting this option...	Saves the report...
Send results to Mail User	As an attachment to an email sent to the specified mail recipient. Use the scroll list to select the recipient for the report file. Only previously configured mail recipients are listed. To send the email with the attached HHM report to someone who is not listed, exit the utility, configure that person as a mail user (see Configure Mail Users on page 107), and then run the utility again. **Note:** Do not select autosupport@spectralogic.com as a recipient unless Spectra Logic Technical Support specifically instructs you to send the HHM report to them. Spectra Logic does not save emailed HHM report files unless they are specifically requested for troubleshooting.
Save results to USB key	To a USB device connected to the USB port on the LCM. **Note:** This option is only available if you inserted a USB device in Step 4 on page 368.

10. Click **Run**.

After a brief delay, the Results screen displays the current HHM data. Scroll as necessary to view all of the data.

Note: If you are connected to the library using a web browser, you can drag the bottom right corner of the scroll box containing the HHM data to adjust the length and width of the scroll box.

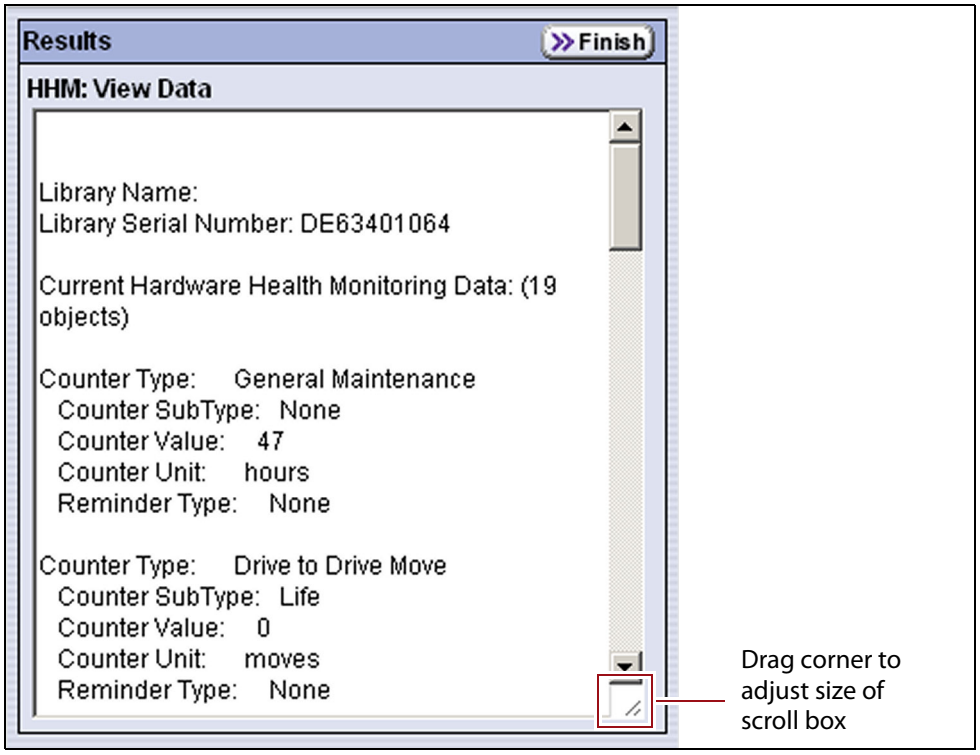


Figure 258 View the output of the HHM: View Data Utility.

11. If you chose to save the file to a USB device, a message displays showing the filename for the results file.

If you are connected to the library using a web browser, you can also copy and paste the information from the Results screen into a text file and email it to Spectra Logic Technical Support if they request it.

12. Click **Finish** to return to the list of advanced utilities.

RESETTING THE LIBRARY

Performing some types of troubleshooting operations or recovering from some error conditions require you to reboot (power-cycle) the library. Power-cycling the library resets all of the components in the library.

Caution

Do not reset the library unless you are specifically instructed to do so. Trace data generated by the library may be lost when you reset the library or a component, making diagnosing problems difficult.

Note: Any drives that are not assigned to a partition generate system messages showing that the drive disappeared and then reappeared whenever the library is power-cycled.

Prepare for the Reset

1. Use your storage management software to stop any backups running to the library.
2. If possible, pause Media Auto Discovery, PreScan, or PostScan if any of these processes is running (Stop the Discovery Process on page 252 and Pause the PostScan Process on page 261).
3. Discontinue all I/O to the library.

Reset Using the Power Button

1. Power off the library (see Power Off the Library on page 141).
2. Wait at least 10 seconds.
3. Power on the library (see Power On the Library on page 140) and wait while the library performs its initialization process.
4. If a cartridge is left in a drive after the reset is complete, see Resolving Operational Issues on page 363 for information about returning the cartridge to its storage location.

Reset Remotely

If you are accessing the library using the BlueScale web interface, use the Reboot Library utility to reset the library.

User Privilege Requirements Only a user with superuser or administrator privileges can reset the library remotely. See Understanding User Groups and Security on page 94 for information about the three types of user groups and what types of privileges each has.

1. Log into the library as a superuser or administrator.
2. Click **MENU**, then select **Maintenance** ···⁘ **Utilities**. The Basic Utilities screen displays.

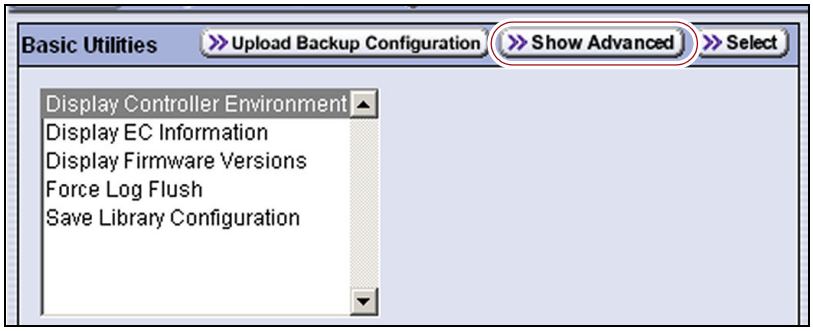


Figure 259 Click **Show Advanced** on the Basic Utilities screen.

3. Click **Show Advanced**. A Confirmation screen displays.
4. Click **Yes** to acknowledge the warning about using the advanced utilities. The Advanced Utilities screen displays a list of the advanced utilities.

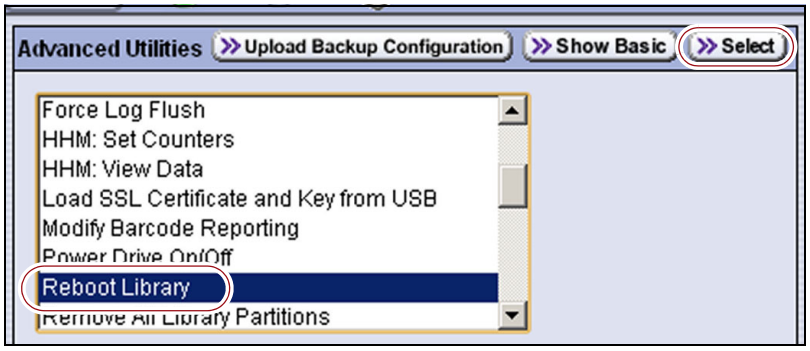


Figure 260 Select **Reboot Library**.

5. Select **Reboot Library**, then click **Select**.
6. The Description screen shows the details for the utility. Click **Run** to start the reboot process.
7. Wait while the library runs the utility.

   During the reboot process, the connection to the BlueScale web interface is lost.
8. Wait approximately ten minutes, then reconnect to the library.

RESTORING THE LIBRARY CONFIGURATION

Overview If you have valid backups of the library's configuration and the MLM database saved on a USB device or sent as an email attachment, you can use the backups to restore the library in the event of a disaster. You can also use these backups to restore the library if problems require you to replace the LCM or the memory card in the LCM. See Backing Up the Library Configuration on page 116 for information about backing up the library configuration.

Notes:

- A library configuration backup file can only be used to restore the library that generated it. The configuration backup file cannot be used to clone the configuration from one library to another.
- All backup files of the library configuration include any BlueScale encryption keys that were stored in the library at the time the file was created.
- The backup of the MLM database also contains the DLM database.

To restore the...	Using the...	See...
Library configuration, the MLM and DLM databases, and the BlueScale encryption keys stored in the library	Auto Configuration Save file,	Restore From an Auto Configuration Save File on page 375.
Library configuration and the BlueScale encryption keys stored in the library	Saved configuration file,	Restore the Library Configuration Using a Saved Configuration on page 381.
MLM and DLM databases	MLM database backup file,	Restore the MLM and DLM Databases on page 384.
BlueScale encryption keys	Exported key file,	Import the Required Key Into the Library on page 325.

User Privilege Requirements Only a user with superuser or administrator privileges can restore the library configuration and the MLM and DLM databases. To restore BlueScale encryption keys, the user must also be logged in as an encryption user. See Understanding User Groups and Security on page 94 and Configuring BlueScale Key Management on page 310 for additional information.

Restore From an Auto Configuration Save File

The advanced utility called "Restore Library Configuration from Auto Save" restores the library configuration, as well as the MLM and DLM databases, using the Auto Configuration Save backup file that the library generates automatically (see Back Up the Library Configuration Automatically on page 117). This utility also restores any BlueScale encryption keys that were stored in the library when the Auto Configuration Save backup file was created.

Important Before restoring your system using the automatically generated backup file, check the time stamp included in the file name to ensure that you have the best available file.

Important The library does not automatically save a backup when you make changes to any of the library configuration settings other than those for partitions. Any changes made since the last backup need to be entered manually.

The library automatically generates a configuration backup file whenever any of the following events occurs:

- When you make a change to a partition, the library immediately generates a configuration backup file and saves it to the memory card in the LCM. If you configured the option to email the backup file, the backup file is sent as an email attachment to the specified recipient (see Email Auto Configuration Save on page 111).
- Changes to any of the library configuration settings other than those for partitions are automatically saved in the configuration backup file that the library creates each week. The timing for this backup is based on the first time the automatic backup file is generated.
- If you cannot restore from the configuration backup file on the LCM and you have manually generated backups of the library configuration and the MLM database that are more current than the available automatically generated configuration backup file that is saved elsewhere, you may want to use those backups instead of the automatically generated configuration backup file (see Restore the Library Configuration Using a Saved Configuration on page 381 and Restore the MLM and DLM Databases on page 384).

Restore the Library

Use the following steps to restore the library configuration, the MLM and DLM databases, and any BlueScale encryption keys using an automatically generated configuration backup file.

Note: If you cannot use the automatically generated configuration backup file stored in the library, locate an Auto Configuration Save file that was saved to a USB device or sent as an email attachment.

Important The library cycles power after restoring the previous configuration.

1. If you plan to restore using the zip file containing the automatically generated configuration backup file that was sent as an email attachment, use the following instructions to copy it to a USB device; otherwise, skip to Step 2.
   a. Create a folder called `\autocfgsave` on a USB device.
   b. Copy the zip file you received in the email to the `\autocfgsave` folder on the USB device.
   c. Connect the USB device to the USB port on the LCM and allow time for the device to mount before continuing.
2. Log into the library as a user with superuser or administrator privileges.
3. Click **MENU**, then select **Maintenance** ···⁘ **Utilities**. The Basic Utilities screen displays.

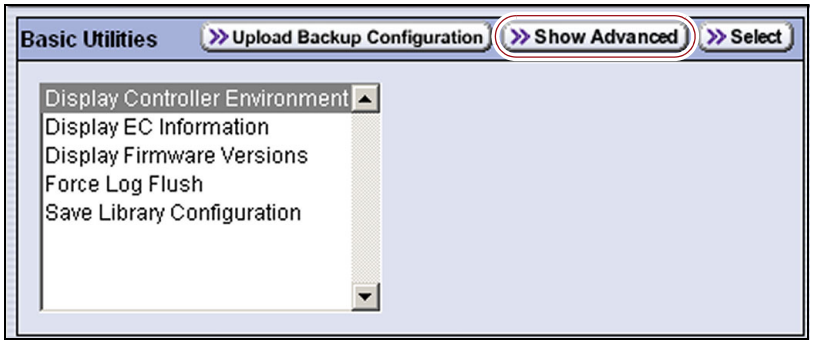


Figure 261 Click **Show Advanced** on the Basic Utilities screen.

4. Click **Show Advanced**. A Confirmation screen displays.

5. Click **Yes** to acknowledge the warning about using the advanced utilities. The Advanced Utilities screen displays a list of the advanced utilities.

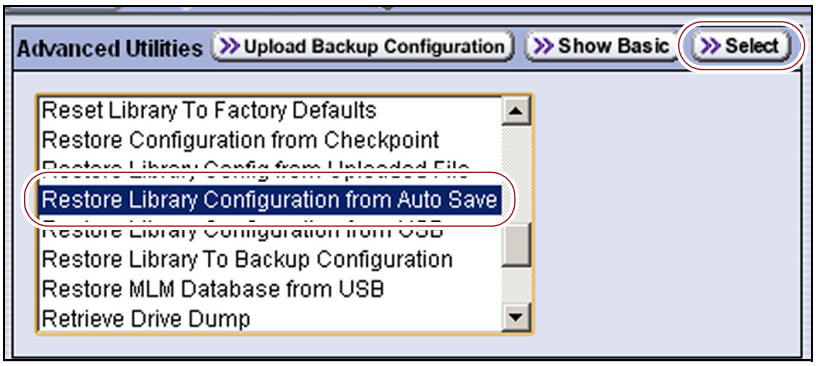


Figure 262 Select **Restore Library Configuration from Auto Save** to use the LCM copy of the configuration file.

6. Scroll through the list of advanced utilities and select **Restore Library Configuration from Auto Save**.
7. Click **Select**. The Description screen show the details for the utility.

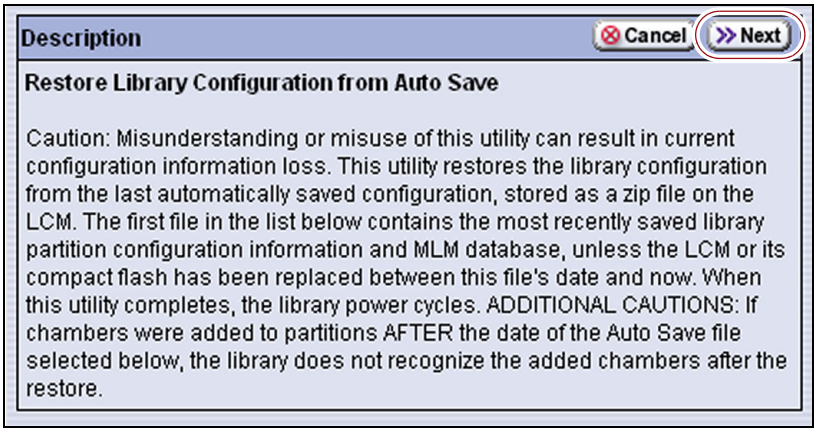


Figure 263 Read the description of the Restore Library Configuration from Auto Save utility, then click **Next**.

8. Click **Next**. Use the **Select a configuration time stamp** drop-down list to select the configuration backup file you want to use. The automatically generated configuration backup files are named `<date-time>cfg.zip`, where `<date-time>` is the time stamp for when the file was created.

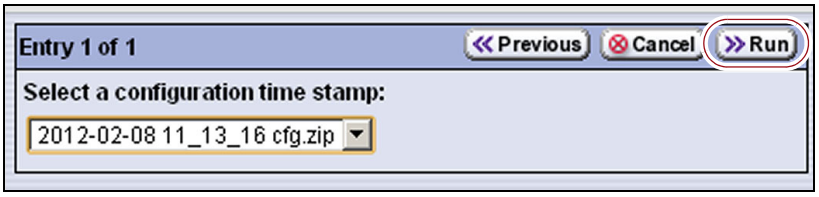


Figure 264 Select the configuration file you want to use, then click **Run**.

Notes:
- If available, the zipped configuration backup file stored on the LCM memory card contains the most recently saved library configuration information, as well as the MLM and DLM databases. Check the time stamp in the filename of the zipped Auto Configuration Save file to determine whether any manually generated backup file you have is more recent.
- Unless you replace the LCM or its memory card, the first file listed is the zipped configuration backup file stored on the LCM memory card.
- If you connected a USB device to the LCM, the configuration backup files are listed after the file on the LCM.

9. Click **Run**.

   After a brief delay, the Utility Results screen appears, showing that the configuration was restored. The library then performs a power- cycle reset.

10. Once the library begins its power-on sequence, remove the USB device if necessary.

Important If you do not remove the USB device, the library power-on sequence fails.

If the library fails to boot, power off the library as described in Power Off the Library on page 141. Once the library is powered off, remove the USB device and power on the library as described in Power On the Library on page 140.

Restore Other Configuration Changes

The library does not immediately generate a configuration backup file when you make changes to any of the library configuration settings other than those for partitions. If you made any changes to the library configuration after the automatically generated configuration backup file you used to restore the library was generated, you need to repeat those changes after completing the restore.

- If you have a manual backup of the library configuration that is more current than the automatically generated configuration backup file you used, you can use it to restore the updated configuration (see Restore the Library Configuration Using a Saved Configuration on page 381).
- If you do not have a manual backup available, you need to restore the following changes manually:
  - If you made configuration changes after the creation date of the automatically generated configuration backup file you used to restore the configuration, you need to use the options in the Configuration menu to repeat those changes after the restore is complete.
  - If you entered activation keys after the creation date of the automatically generated configuration backup file you used to restore the configuration, you need to use the New Option Key screen to re-enter those keys (see Enter Activation Keys on page 115).
  - If you created or imported a BlueScale encryption key after the creation date of the automatically generated configuration backup file you used, you need to import the key into the library before it can be used to encrypt or decrypt data (see Import the Required Key Into the Library on page 325).

Update the Library Inventory

When you restore the configuration, any cartridges that were imported into a partition after the configuration backup file you used was generated are not recognized as belonging to a specific partition. Instead, the library notifies you that it contains cartridges that are not assigned to any partition.

Use the following instructions to update the library inventory to reflect the correct number of slots assigned to the partition.

1. Log in as a user with superuser or administrator privileges.
2. Click **MENU**, then select **Configuration ⋯⁘ Partitions**. The Shared Library Services screen displays.
3. Based on the barcode information on the unassigned cartridges, determine to which partition the cartridges should belong.
4. Click **Edit** for the partition that should contain the cartridges.

5. Click **Next** to advance through the partition wizard screens until you reach the Chambers & Drives screen.

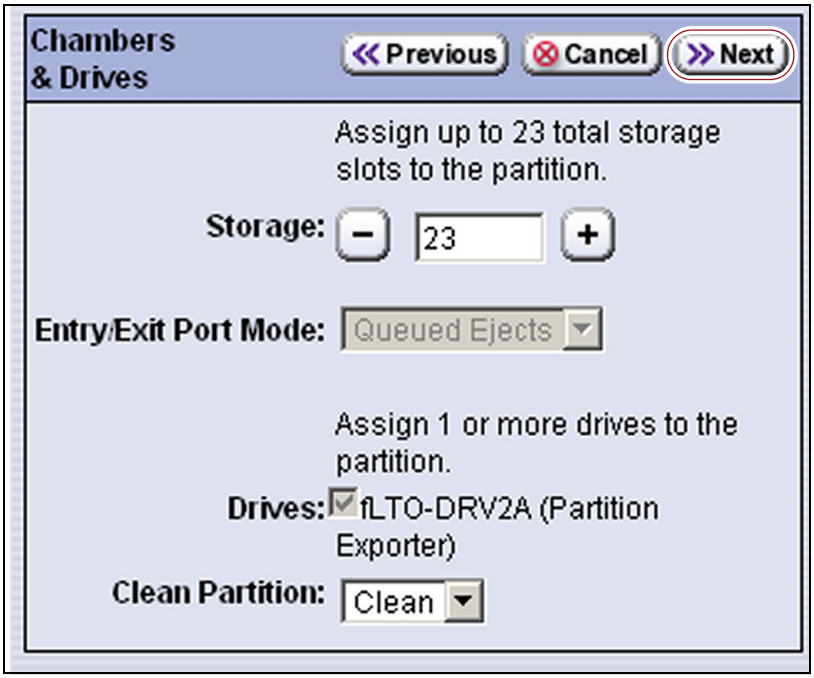


Figure 265 Adjust the number of slots assigned to the partition.

6. Decrease the number of slots assigned to the partition by the number of cartridges the library reported as unassigned.
7. Click **Next** to advance through the remainder of the screens without making any additional changes until you reach the Summary screen.
8. Click **Save**. The Partitions screen redisplays.
9. Repeat Step 2 through Step 7, this time increasing the number of slots assigned to the partition to the original number. The cartridges that were reported as unassigned are assigned to the partition.

Important

If the library has multiple partitions and you imported cartridges into all of the partitions after the configuration backup file you used to restore the library was generated, the cartridges can potentially end up in the wrong partition. Carefully examine the cartridge inventory for each partition. Export any wrongly assigned cartridges and reimport them into the correct partition.

10. Review the information on the screen and confirm that all settings are correct for this partition's configuration.
    - If the configuration information is correct, proceed to Step 11.
    - If the configuration information is not correct:
      - Click **Cancel** and configure the partition again from the beginning.

      —OR—

      - Click **Previous** to move backward through the configuration screens until you reach the settings that need correction. Make any necessary corrections, then click **Next** to move forward through the screens and return to the Save Partition screen.
11. Click **Save**. The library requires several minutes to store the configuration information, after which the Partitions screen redisplays.

    Note: When you make a change to a partition, the library generates an Auto Configuration Save backup file and saves it to the LCM memory card. If you configured the email option for the automatically generated backup file, the library sends an email with the backup file attached to the specified recipient (see Email Auto Configuration Save on page 111).

Restore the Library Configuration Using a Saved Configuration

Use the following steps if you want to restore the library from a configuration backup file that was generated manually, as described in Back Up the Library Configuration Manually on page 118.

Note: The manually-generated configuration backup files do not include the MLM and DLM databases. If you also need to restore the MLM and DLM databases, you must use a separately generated backup of the MLM database (see Restore the MLM and DLM Databases on page 384).

1. If you plan to restore using a configuration backup file that was sent as an email attachment, use the following instructions to copy it to a USB device; otherwise, skip to Step 2.
   a. Create a folder called `\SavedConfigs\<date-time>` folder, where `<date-time>` is the time stamp for the zip file you received in the email.
   b. Copy the zip file you received in the email to the `\SavedConfigs\<date-time>` folder on the USB device.
2. If the configuration backup file you are using to perform the restore is on a USB device, insert the USB device into a USB port on the LCM and allow time for the device to mount; otherwise, skip to the next step.

   Note: The option to restore from USB is only available if you connect the USB device to the LCM **before** you select **Show Advanced** (see Figure 98 on page 153).

3. Log into the library as a user with superuser or administrator privileges.
4. Click **MENU**, then select **Maintenance ···⁘ Utilities**. The Basic Utilities screen displays.

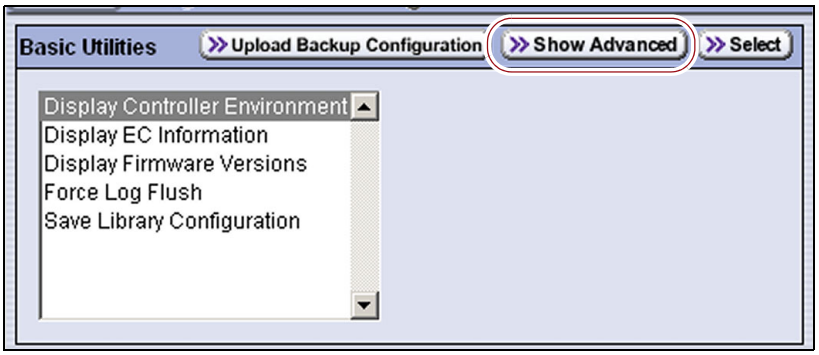


Figure 266 Click **Show Advanced** on the Basic Utilities screen.

5. Click **Show Advanced**. A Confirmation screen displays.
6. Click **Yes** to acknowledge the warning about using the advanced utilities. The Advanced Utilities screen displays a list of the advanced utilities.

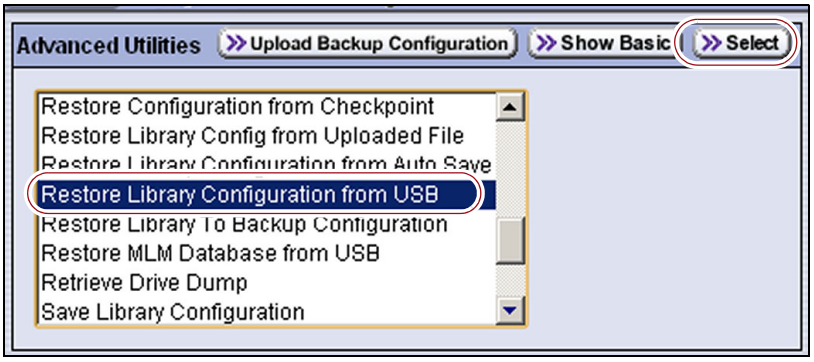
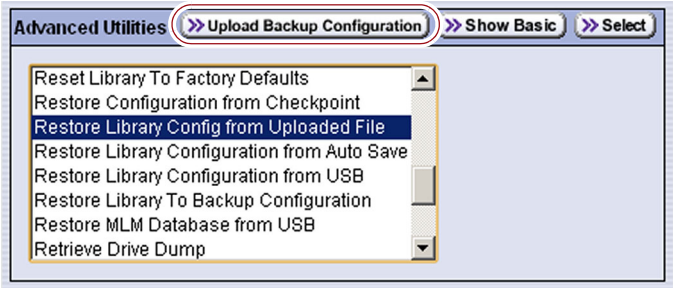


Figure 267 Select the **Restore** utility you want to use.

7. Scroll through the list of advanced utilities and select one of the following, as applicable for your situation.

Use this Restore Option...	To...
Upload Backup Configuration	Upload a configuration backup file to a temporary location in the library from a computer that has network access to the library. **1.** Click **Upload Backup Configuration** at the top of the screen.  **2.** When the upload is complete, you must then run the **Restore Library Configuration from Uploaded File** utility to restore the library configuration. **Notes:** ▪ The **Upload Backup Configuration** button is only available when you access the library through the BlueScale web interface. ▪ This option is always used in conjunction with **Restore Library Configuration from Uploaded File**.
Restore Configuration from Checkpoint	Restore the library configuration from the checkpoint made during the last package upgrade. When this utility completes, the library resets. **Important:** This utility should only be run under the direction of Spectra Logic Technical Support.
Restore Library Configuration from Uploaded File	Complete the restore process after using **Upload Backup Configuration** to upload a saved configuration file from a computer. **Note:** This option is always used in conjunction with **Upload Backup Configuration**, which must be run first.
Restore Library Configuration from USB	Restore a library configuration file previously stored on a USB device. **Note:** The USB device must be plugged into the USB port on the LCM before you continue.
Restore Library To Backup Configuration	Use this option to restore the library configuration to the previous configuration, which was automatically stored on the LCM before either the "Reset Library to Factory Defaults" or "Remove all Library Partitions" utility was run. When the "Restore Library To Backup Configuration" utility completes, the library resets. **Important:** This utility should only be run under the direction of Spectra Logic Technical Support.

8. Click **Select**. The Description screen for the selected utility shows information about the utility.

9. Click **Next**. If you are restoring from a USB device connected to the LCM, use the **Select a restore stamp** drop-down list to select the backup file you want to use. The backup files are named `<date-time>cfg.zip`, where `<date-time>` is the time stamp for when the file was created.
10. Click **Run**.

Important

Before the library is restored using a saved configuration file on the USB device, the current configuration is saved to the USB device with a time stamp indicating when the file was created. The library is then restored using the selected auto saved configuration.

The USB device now contains one additional configuration file.

After a brief delay, the Results screen displays showing that the configuration was restored. The library then performs a power-cycle reset.

11. Once the library begins its power-on sequence, remove the USB device if necessary.

Important

If you do not remove the USB device, the library power-on sequence fails.

If the library fails to boot, power off the library as described in Power Off the Library on page 141. Once the library is powered off, remove the USB device and power on the library as described in Power On the Library on page 140.

12. If you imported cartridges into a partition after you generated the backup configuration file, see Restore Other Configuration Changes on page 378.
13. If necessary, restore the MLM and DLM databases as described in Restore the MLM and DLM Databases on page 384.

Restore the MLM and DLM Databases

Use the following steps to restore the MLM database from a previously saved backup that was created using the Save MLM Database utility (see Back Up the MLM and DLM Databases on page 270).

Caution

The Restore MLM Database from USB utility overwrites the existing MLM and DLM databases with the versions previously saved on the USB device.

Notes:
- Restoring the MLM database also restores the DLM database.
- You can also restore the MLM and DLM databases using an Auto Configuration Save backup file (see Restore From an Auto Configuration Save File on page 375).

1. Use your storage management software to stop all backup or restore operations on the library.

Important

Restoring the MLM and DLM databases requires the library to be idle.

2. If you plan to restore using an MLM database backup file that was sent as an email attachment, use the following instructions to copy the file to a USB device; otherwise, skip to Step 4.

   a. Create a folder called `SavedMLMDB` on a USB device.

   b. Copy the `cminfo_<date-time>.dat` or `cminfo_<date-time>.zdt` file to the `SavedMLMDB` folder on the USB device.

   Note: The file extension depends on whether you chose to compress the database when you backed it up.

3. If the MLM database backup file you are using to perform the restore is on a USB device, insert the USB device into a USB port on the LCM and allow time for the device to mount; otherwise, skip to the next step.

   Note: The option to restore from USB is only available if you connect the USB device to the LCM **before** you select **Show Advanced** (see Figure 98 on page 153).

4. Log into the library as a user with superuser or administrator privileges.

5. Stop any PreScan or PostScan operations that are currently running (see Stop the Discovery Process on page 252 and Pause the PostScan Process on page 261).

6. Click **MENU**, then select **Maintenance** ···⁘ **Utilities**. The Basic Utilities screen displays.

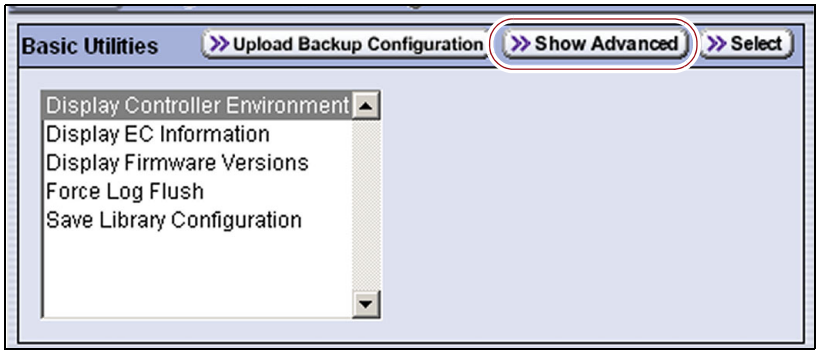


Figure 268 Click **Show Advanced** on the Basic Utilities screen.

7. Click **Show Advanced**. A Confirmation screen displays.

8. Click **Yes** to acknowledge the warning about using the advanced utilities. The Advanced Utilities screen displays a list of the advanced utilities.

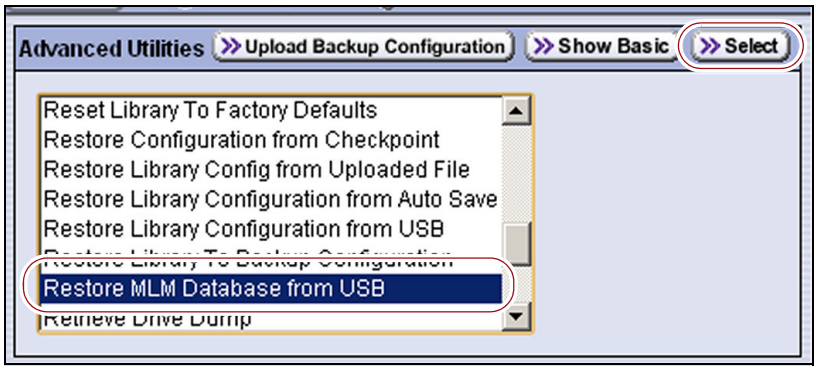


Figure 269 Select the **Restore MLM Database from USB** utility.

9. Scroll through the list of advanced utilities and select **Restore MLM Database from USB**. The screen refreshes to show the details for the utility.

10. Click **Select**. The Description screen show the details for the utility.

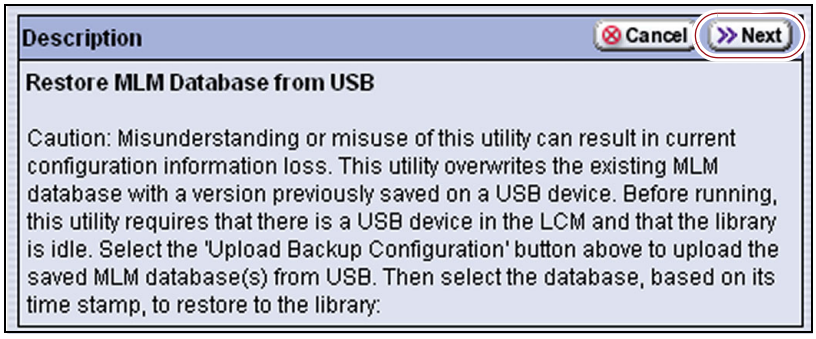


Figure 270 Read the description of the Restore Library Configuration from Auto Save utility, then click **Next**.

11. Click **Next** and use the **Select a restore time stamp** drop-down list to select the `cminfo<date-time>.dat` or `cminfo_<date-time>.zdt` file containing the MLM database backup you want to use for the restore.

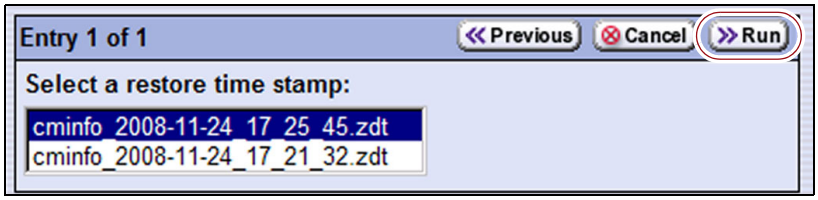


Figure 271 Select the MLM database backup you want to use.

12. Click **Run**.

    After a brief delay, the Results screen displays, showing that the database was restored.

    Note: After an MLM database restore, the **Discover Media** button on the Media Lifecycle Management Tools screen (**Maintenance** ⋯ **MLM**) may be active even if all cartridges have been discovered.

EMERGENCY MAGAZINE REMOVAL

If you need to remove the magazines in an emergency instance (for example, if you cannot use the front panel to instruct the library to unlock the magazines) follow the steps in this section.

Caution Do not perform this procedure if the library is powered on; if the library is powered on, the robotics could attempt to load or unload a cartridge from a slot in the magazine that is unlocked using the emergency magazine removal procedure. You risk damaging the robotics, the magazines, or the library.

Important Do not use this magazine removal procedure unless specifically instructed to do so by Spectra Logic Technical Support.

1. Discontinue operations running on the library.
   a. Use your storage management software to stop any backup or restore operations running to the library.
   b. Use your storage management software to move any cartridges that are currently in drives back to their storage locations.

      If you cannot use your storage management software, move the cartridges as described in Move Cartridges Within a Partition on page 226.
   c. Pause PostScan if it is running (see Pause the PostScan Process on page 261). Any tapes currently being scanned are returned to their storage locations.
2. Press the front panel power button until the button's LED starts to flash. Wait for the power-off sequence to complete, which allows the applications to shut down gracefully.

3. Access the back of the library.

Important Ensure that you can simultaneously reach both the front and the back of the library, or ask a second person to help you with this procedure.

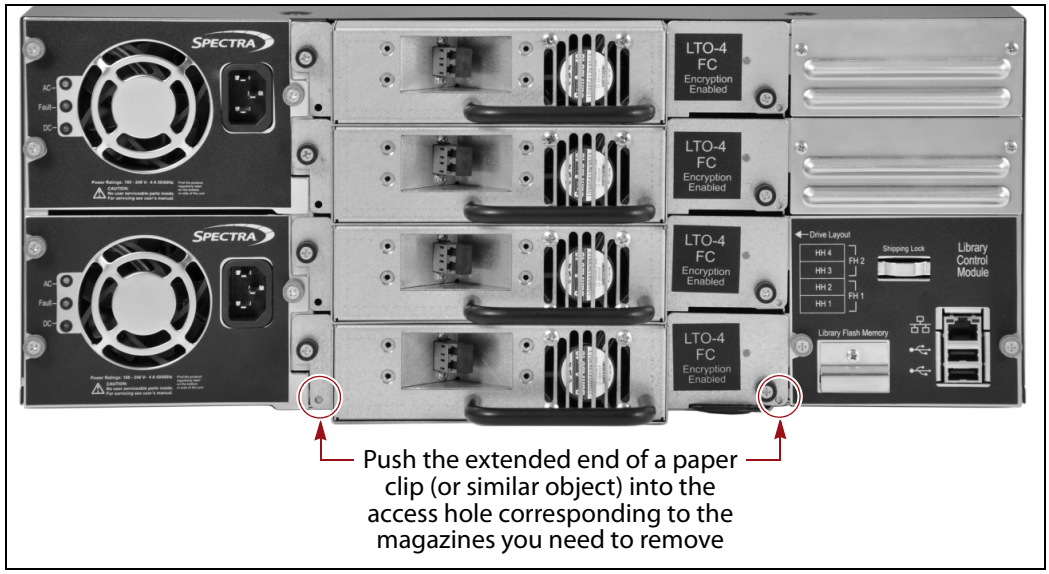


Figure 272 Emergency magazine removal.

4. Insert a straightened paper clip (or similar object) into the magazine release access hole, then depress and hold the lock release button that corresponds to the magazine you need to remove (see Figure 272).

   Note: The lock release button on the right side of the library releases the top and bottom magazines on the right side of the library; the lock release button on the left releases the left-side magazines.

5. While you are depressing the lock release button, carefully slide the magazine straight out of the front of the library.

Caution You must depress the lock release button while removing the magazine.

If you attempt to remove a magazine while the lock release button is not depressed, the internal magazine latch may break. This type of failure cannot be repaired in the field, and requires the library to be returned to Spectra Logic.

Caution A fully loaded magazine weighs several pounds.

CHAPTER 13

Drive Troubleshooting

This chapter describes procedures for dealing with the most common problems encountered with the library's drives. Try these troubleshooting procedures *before* you open a support ticket with Spectra Logic Technical Support. If you are unable to resolve the problem yourself, open a support ticket (see Opening a Support Ticket on page 474). For additional troubleshooting information, refer to the drive documentation (see LTO Ultrium Tape Drives on page 19).

Note: The library must be under warranty or have a valid service contract in order to qualify for support (see Service Contract Extension on page 495 to learn about service contracts).

TROUBLESHOOTING DRIVES

The following sections provide information about troubleshooting drive problems.

Identify the Problem

1. When you encounter problems with drive operation while using the library's BlueScale user interface, begin troubleshooting by checking the following:

Check...	To...
System Messages	Review any System Messages that were posted by the library (see Check and Respond to Messages on page 143) and take any action described in the message(s).
Error codes	Look up the definition of an error sense code referenced in a system message using the *Spectra Tape Libraries SCSI Developer Guide*.
Drive documentation	Find detailed troubleshooting information for the drive. See LTO Ultrium Tape Drives on page 19 for information about obtaining drive documentation.
Technical Support Portal	Find information about the most current version of BlueScale software and additional service and support tools. You can access the Technical Support portal at support.spectralogic.com. **Note:** Accessing many of the tools available on the Technical Support portal requires creating a user account. See Accessing the Technical Support Portal on page 472 for instructions. ▪ Check the options under the **Documentation** and **Knowledge Base** menus for additional troubleshooting information. ▪ Check the **Service & Contracts** menu to view information about the warranty and service options available for your library as well as the Spectra Certified Media warranty.

2. Display the Drive Details screen for the drive you suspect is having problems and review the information about the drive (see View Robot Utilization Information on page 147). Use the following table and the information in Interpret the Detailed Drive Information on page 393 to determine how to proceed.

Detail Field	Description
POST Status	Indicates whether the drive successfully completed its power-on self-tests (POST). When an LTO drive is power-cycled or reset, it automatically runs self-diagnostic tests (POST), which check the drive's memory and sensors, perform motor and servo tests, and test the data channels to ensure that the drive is functioning within normal parameters.
Cleaning Status	Indicates whether the drive requires cleaning (see Cleaning a Drive on page 442).
Display Character	Corresponds to the single-character display (SCD) on the drive. The meaning of the character displayed depends on the LTO drive generation. See Interpreting the SCD Codes, beginning on page 394 for detailed information.
Cartridge Status	Indicates whether a cartridge is currently loaded in the drive, tape motion, and other information related to reading and writing data.

3. If you were successfully operating the storage management software and library in the past, but are now experiencing problems reading and writing data, check the following:

Check this...	If...
Write-protect switch setting	You are having trouble writing data to a cartridge. Make sure that the cartridge is write-enabled (see Preparing Cartridges for Use on page 199) before importing it into the library.
Cartridge age	A cartridge was in use for a long time or if it was used frequently, try using a new cartridge.
Drive cleaning	The drive indicates that a cleaning is required. Follow the instructions in Cleaning a Drive on page 442 to clean the drive. **Note:** If the storage partition is associated with a cleaning partition and the cleaning partition contains a usable cleaning cartridge, drives are automatically cleaned whenever necessary.

4. If you experience problems accessing the drives in the library from the storage management software on the host, check the following:

Check...	To...
Interface connections	Make sure that the connections to the drives are secure. See Troubleshooting Library Hardware Issues on page 354 drive interface issues. **Important:** After you power on the library and the Fibre Channel arbitrated loop or fabric completes its initialization, avoid disconnecting the Fibre Channel drives from the network. If you need to disconnect a drive from the network, use the utility provided with your switch or hub to bypass the affected ports before breaking the connection. The bypass sets the port to a non-participating state on the network. After you reconnect the drive to the library, use the utility to return the port to a participating state.
Software installation	Make sure that your host application is installed and configured correctly (refer to your software documentation). Pay special attention to steps that describe how to configure the software for use with the drive(s).
Drive addressing	Make sure that the drive address configured in the host application is the same one you specified when you configured the partition containing the drive (see Creating a Storage Partition on page 174).
Host and software documentation	Determine whether a device driver is required. Some operating environments require you to install device drivers before the application software can correctly communicate with the drives. When you update the drive firmware, you may also need to update the device driver for the drive. See Updating Drive Device Drivers on page 462 for instructions.

Interpret the Detailed Drive Information

The Drive Details screen includes information about the drive and drive sled firmware versions, the location-based Spectra serial number, and the manufacturer's serial number. It also shows additional detailed status information, including the state the single-character display (SCD) on the drive. See View Robot Utilization Information on page 147 for information about accessing this screen.

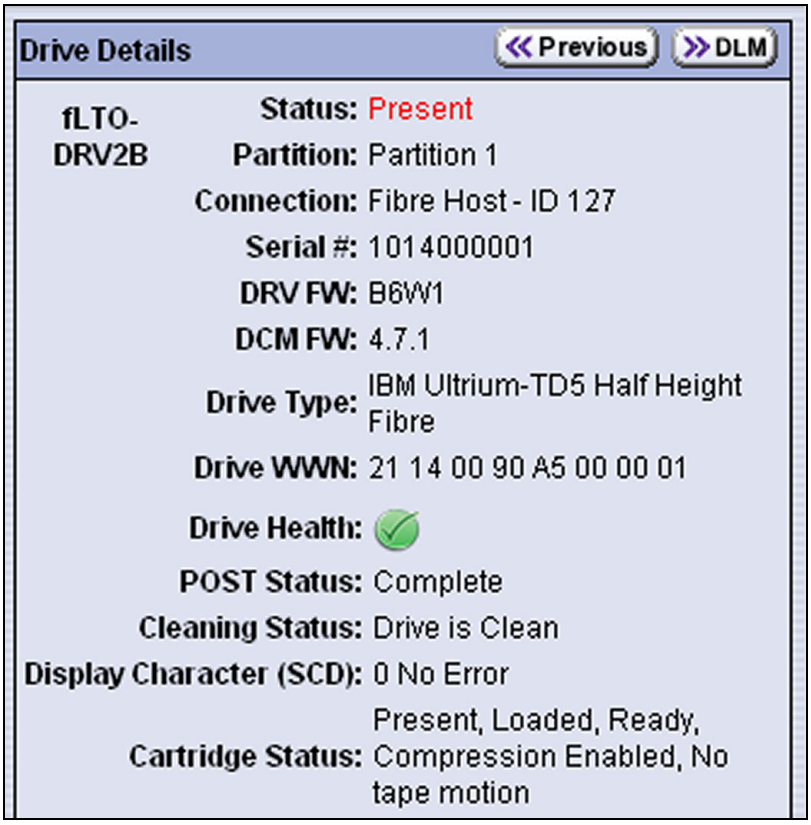


Figure 273 Use the information on the Drive Details screen to help troubleshoot drive problems (Fibre Channel drive shown).

The following sections describe how to use information on the Drive Details screen to help troubleshoot drive problems.

Responding to the Drive Cleaning Notification

Whenever a tape is loaded or unloaded, the read/write heads are physically cleaned by a brush located within the drive. However, after reading and writing a large amount of data (the exact amount varies by drive type and generation) or if read or write errors occur, the drive requests to be cleaned with a cleaning cartridge. The request is made by sending a Tape Alert message to the host, and displaying a **C** on the SCD The notification is also posted to the library's Drive Details screen (Figure 273) and the DLM drive health icon for the drive changes to yellow (see Using the Drive Health Icons on page 282 for additional information).

If needed, clean the drive as described in Cleaning a Drive on page 442. Use only a certified LTO cleaning cartridge. To order cleaning cartridges, see Media and Media Accessories on page 493.

Interpreting the SCD Codes

The Display Character (SCD) field on the Drive Details screen shows the current state of the single-character display on the drive.

Permanent Errors If the drive detects a permanent error and displays an SCD error code other than zero (0), it automatically generates a drive trace. If you force a new drive trace to be generated, the existing trace is overwritten and data is lost. You might also lose the trace data if you turn off the power to the drive. See Retrieving a Drive Trace or Drive Dump File on page 401 for information about retrieving the trace data from the drive.

Notes:
- Some of the solutions listed in the following table include testing the drive. See Using DLM to Test an LTO Drive on page 414 for instructions.
- In some cases, additional tests using ITDT are required. Download and install the software as described in Use the IBM Tape Diagnostic Tool (ITDT) on page 404. Refer to the ITDT documentation for information about using this utility to retrieve the trace file. Contact Spectra Logic Technical Support if you need assistance (see Contacting Spectra Logic on page 7).

Multiple Errors The SCD is blank during normal operation. If multiple errors occur, the code with highest priority (lowest number) displays first. Once corrected, the code with the next highest priority displays, until none remain.

Note: The drive may need to be reset in order to clear the error code.

WORM Media LTO-3 and later generations of LTO drives support using WORM media. To learn more about WORM media, see LTO WORM Media on page 514.

The following conditions cause WORM media errors to occur:

- Information in the servo manufacturer's word on the tape must match information from the cartridge MAM. If it does not match, the drive's SCD displays error code **7**.
- Inserting a WORM tape cartridge into a drive that is not compatible with WORM media causes the cartridge to be treated as an unsupported medium. The drive's SCD displays error code **7**.

SCD Code Descriptions for LTO-3 and Later Generation Drives The following table shows the SCD codes and, where applicable the associated DLM Drive Health icon, for LTO-3 and later generations of LTO drives. See the table on page 282 for a description of what each of the Drive Health icons indicates.

Note: The single-character display does not use the characters B, D, G, I, O and Z to prevent misinterpretation as the characters 8, 0, 6, 2, and 1.

Code	DLM Health Icon	Cause and Solution
0		**No error occurred.** No action is required. The power was cycled or diagnostics finished with no errors.
1		**Cooling problem.** The recommended operating temperature was exceeded. Perform one or more of the following: ▪ Make sure that the cooling fan is rotating and is quiet. ▪ Remove any blockage that prevents air from flowing freely through the drive. ▪ Make sure that the operating temperature and airflow is within the specified range (refer to the tape drive documentation for these specifications). If the operating temperature is within the specified range and the problem persists, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7). **Note:** The error code clears when you reset or power cycle the drive or when you place it in maintenance mode.
2		**Power problem.** The externally supplied power is approaching the specified voltage limits (the drive is still operating) or is outside the specified voltage limits (the drive is not operating). **If the problem is only exhibited by one drive in the library:** ▪ Make sure that the drive is correctly seated in the drive bay. ▪ If the problem persists, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7). **Note:** The error code clears when you reset or power cycle the drive or when you place it in maintenance mode. **If the problem is exhibited by multiple drives in the library:** The power throughout the library needs to be checked. Contact Spectra Logic Technical Support for assistance.

Code	DLM Health Icon	Cause and Solution
3		**Firmware problem.**  **Important:** Do not force a drive dump; one already exists. The drive determined that a firmware error occurred. Perform the following: **1.** Collect the drive trace file (see Retrieving a Drive Trace or Drive Dump File on page 401). **2.** Reset the drive (see Resetting a Drive on page 408), then retry the operation that produced the error. **3.** If the problem persists, contact Spectra Logic Technical Support and send the drive trace file to them, if requested (see Contacting Spectra Logic on page 7). **Note:** The error code clears when you reset or power cycle the drive or when you place it in maintenance mode.
4		**Firmware or drive problem.**  **Important:** Do not force a drive dump; one already exists. A firmware or drive hardware failure occurred. Perform the following: **1.** Collect the drive trace file (see Retrieving a Drive Trace or Drive Dump File on page 401). **2.** Reset the drive (see Resetting a Drive on page 408), then retry the operation that produced the error. **3.** If the problem persists, contact Spectra Logic Technical Support and send the drive trace file to them, if requested (see Contacting Spectra Logic on page 7). **Note:** The error code clears when you reset or power cycle the drive or when you place it in maintenance mode.
5		**Drive hardware problem.**  **Important:** Do not force a drive dump; one already exists. The drive determined that a tape path or read/write error occurred. To prevent damage to the drive or cartridge, the drive does not allow you to insert a cartridge if the current cartridge was successfully ejected. If the problem persists, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7). Perform the following: **1.** Collect the drive trace file (see Retrieving a Drive Trace or Drive Dump File on page 401). **2.** Reset the drive (see Resetting a Drive on page 408), then retry the operation that produced the error. **3.** If the problem persists, contact Spectra Logic Technical Support and send the drive trace file to them, if requested. **Note:** The error code clears when you reset or power cycle the drive or when you place it in maintenance mode.

Code	DLM Health Icon	Cause and Solution
6		**Drive or media error.** See Chapter 8 – Configuring and Using Media Lifecycle Management, beginning on page 233 for information about using MLM to determine the health of the cartridge. See Chapter 9 – Using Drive Lifecycle Management, beginning on page 279 for information about using DLM to determine the health of the drive. The drive determined that an error occurred, but it cannot isolate the cause. Ensure the cartridge is the correct media type: ▪ See LTO Read/Write Compatibility on page 513 for information about which media is compatible with each LTO drive generation. ▪ A drive automatically ejects an expired cleaning cartridge without attempting to use it. ▪ A drive does not accept a WORM cartridge when running diagnostic tests in Maintenance Mode. ▪ A drive does not write over existing data sets on a WORM cartridge. Ensure you are appending data sets on WORM media rather than attempting to write over existing data sets.

		Confirm that the cartridge is the correct media type. If it is, determine whether the problem is associated with writing or reading data to a single cartridge or multiple cartridges.
		Problems Writing Data on a Cartridge with a Known Volume Serial Number
		Retry the operation with a different cartridge.
		▪ If the operation succeeds, the original cartridge was defective. If possible, copy data from the defective cartridge and set the original cartridge aside. If additional tests confirm that the cartridge was the source of the error, you can discard it.
		▪ If the operation fails and another drive is available, insert the original cartridge into the other drive and retry the operation.
		  ▪ If the operation fails, discard the defective cartridge.
		  ▪ If the operation succeeds, use the Drive Health Verification wizard to test the original drive (see Using DLM to Test an LTO Drive on page 414).
		  ▪ If the drive fails the DLM drive test, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).
		  ▪ If the drive passes the DLM drive test, the error was temporary.
		▪ If the operation fails and another drive is not available, use the Drive Health Verification wizard to test the drive.
		  ▪ If the drive fails the DLM drive test, contact Spectra Logic Technical Support.
		  ▪ If the drive passes the DLM drive test, retry the operation to determine whether the error was temporary. If the operation fails again, discard the cartridge.

Code	DLM Health Icon	Cause and Solution

6 (cont.)		**Problems Reading Data on a Cartridge with a Known Volume Serial Number**
		Perform one of the following procedures:
		▪ If another drive is available, insert the cartridge into the other drive and retry the operation.
		  ▪ If the operation fails, discard the defective cartridge.
		  ▪ If the operation succeeds, use the Drive Health Verification wizard to test the original drive (see Using DLM to Test an LTO Drive on page 414).
		  ▪ If the drive fails the DLM drive test, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).
		  ▪ If the diagnostics succeed, the error was temporary.
		▪ If another drive is not available, use the Drive Health Verification wizard to test the drive.
		  ▪ If the drive fails the DLM drive test, contact Spectra Logic Technical Support.
		  ▪ If the drive passes the DLM drive test, retry the operation to determine whether the error was temporary. If the operation fails again, discard the cartridge.

		**Problems with One or More Cartridges with Unknown Volume Serial Numbers** If the problem occurs with multiple cartridges or if you do not know the cartridge's volume serial number, use the Drive Health Verification wizard to test the drive (see Using DLM to Test an LTO Drive on page 414). ▪ If the drive fails the DLM drive test, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7). ▪ If the drive passes the DLM drive test, the problem is not related to the drive.

Code	DLM Health Icon	Cause and Solution

7		**High probability of media error.** An error occurred because of a faulty cartridge.
		▪ Ensure the cartridge is the correct media type:
		  ▪ See LTO Read/Write Compatibility on page 513 for information about which media is compatible with each LTO drive generation.
		  ▪ A drive does not accept an expired cleaning cartridge.
		  ▪ A drive does not accept a WORM cartridge when running diagnostic tests in Maintenance Mode.
		  ▪ A drive does not write over existing data sets on a WORM cartridge. Ensure you are appending data sets on WORM media rather than attempting to write over existing data sets.
		▪ If the cartridge is the correct media type, try another cartridge in the drive.
		▪ If problem does not occur with multiple cartridges, try the questionable cartridge in a different drive.
		  ▪ If the operation fails in the other drive and the SCD displays **6** or **7**, replace the cartridge.
		  ▪ If the operation succeeds, use the Drive Health Verification wizard to test the original drive (see Using DLM to Test an LTO Drive on page 414).
		CAUTION: When you use ITDT to run the Test Cartridge & Media diagnostic, data on the suspect tape is overwritten.
		  ▪ If the Test Cartridge & Media diagnostic fails, replace the media.
		  ▪ If the diagnostic runs successfully, use the Drive Health Verification wizard to test the drive (see Using DLM to Test an LTO Drive on page 414).
		  ▪ If the drive fails the DLM drive test, replace the drive.
		  ▪ If the drive passes the DLM drive test, repeat the operation that produced the initial media error.
		Note: The error code clears when you reset or power cycle the drive or when you place it in maintenance mode.

8		**SCSI interface or Fibre Channel failure.** A failure occurred in the drive hardware or in the SCSI bus. The error code clears after 10 seconds if the error does not recur. If the error persists, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).
9		**RS-422 error**. The drive determined that a drive interface or library interface failure occurred. The error code clears after 10 seconds if the error does not recur. If the error persists, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

Code	DLM Health Icon	Cause and Solution
A		**Degraded operation.** The drive determined that a problem occurred that degraded the operation of the drive, but it did not restrict continued use. The drive is usable, though the single-character display (SCD) continues to indicate an error and the status light flashes amber. The error code may clear when you cycle power to the drive. **1.** Reset the drive (see Resetting a Drive on page 408) to clear the error code. **2.** Confirm that the drive is using the current firmware version (see Updating Drive Firmware on page 450) and update the firmware if necessary. **3.** Use the Drive Health Verification wizard to test the drive (see Using DLM to Test an LTO Drive on page 414). **4.** If the problem persists, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).
C		**Cleaning indicator.** The drive needs to be cleaned, or is in the process of loading the cleaning cartridge or being cleaned. The error code clears when you clean the drive and unload the cleaning cartridge. See Cleaning a Drive on page 442 for instructions.
d		Two drives on the Fibre Channel loop have the same Arbitrated Loop Physical Address.
E		The Fibre Channel port connection is off-line.
e		The drive detected a configuration error during a BlueScale encryption operation. **1.** Make sure that you are using LTO-4 or later generation data cartridges. BlueScale encryption is only supported for LTO-4 and later generation cartridges. **2.** Retry the encryption operation with the suspect cartridge in another encryption enabled drive. **3.** Replace the cartridge if you see the same problem in multiple drives.

Code	DLM Health Icon	Cause and Solution
F		**Drive Fibre Channel error.** The Fibre Channel drive does not detect light or a related diagnostic failed to detect light through the fiber optic connection to the drive. ▪ Verify the fiber cables and connections between the drive and the host are the correct type and are working properly. Verify all equipment and devices are powered ON. ▪ Verify the configuration settings for the drive are set correctly and are compatible with the topology of the network. ▪ Verify that the host Fibre Channel adapter and port are working properly and are compatible with the topology of the network. ▪ Verify that the Fibre Channel switch ports are working properly and are compatible with the topology of the network. ▪ Verify that the fiber cable is connected to Port A (0) of the drive. ▪ Verify that Port A (0) on the Fibre Channel drive is working properly by using ITDT to run the "Function Code 6: Run Host Interface Wrap Test."
J		**Incompatible Media.** The drive determined that incompatible media was loaded into the drive.
P		The cartridge in the drive is write-protected. The storage management software cannot write data to a write-protected cartridge. The library cannot update the cartridge MAM when the cartridge is write-protected.
u		Firmware update is in progress.
b, c, H, h, n, o	**N/A**	Reserved or not actively in use, or no error or message assigned. There may be a problem with the SCD. Reset the drive and determine whether all segments on the SCD are lit. ▪ If they are all lit, confirm that the drive is using the current firmware version (see Updating Drive Firmware on page 450) and update the firmware if necessary. ▪ If the problem persists, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).
...	**N/A**	The message display has lost communication with the drive. This message appears on Line 2 of the message display. The three dots may occasionally display during normal processing.

RETRIEVING A DRIVE TRACE OR DRIVE DUMP FILE

Spectra Logic uses drive traces and drive dumps to help diagnose problems with a drive. A drive trace is a set of logs collected by the library to help diagnose drive errors. A drive dump is a file generated by the drive when it encounters an error state. You only need to retrieve a drive trace or drive dump when instructed to do so by Spectra Logic Technical Support.

There are three tools for collecting drive traces and dumps. The best tool to use depends on the type of file requested and the ability to download and install ITDT.

- To retrieve a drive trace from LTO-5 and later generation drives, Use the Drive Traces Button.
- To retrieve a drive dump, if possible, Use the IBM Tape Diagnostic Tool (ITDT) on page 404.
- To retrieve a drive dump when you cannot use ITDT, Use the BlueScale Retrieve Drive Dump Utility on page 405.

Use the Drive Traces Button

Drive traces for LTO-5 and later generation drives can be generated and retrieved using the Drive Traces button on the Drives screen.

Before You Begin

Before you begin generating a drive trace using the Drive Trace button, make sure you fulfill the following prerequisites.

Emailing Results If you plan to email the drive trace file directly from the library, make sure that you previously configured the intended email recipient as a mail user (see Configure Mail Users on page 107).

Saving Results to USB If you plan to save the drive trace file to a USB device, you must plug the USB device into one of the USB ports on the LCM and allow time for the device to mount before you click **Drive Traces** (see Using a USB Device on page 152).

> **Note:** If a USB device is not plugged into the LCM, the option to save the drive trace file to a USB device is not available. You can, however, still email the trace file or download the file.

User Privilege Requirements Only a user with superuser or administrator privileges can use the BlueScale software to retrieve a drive trace file.

Generate the Trace

1. Log into the library as a user with superuser or administrator privileges.
2. Select **Menu** ···⁘ **Configuration** ···⁘ **DLM** (or **Drives**) to display the Drives screen.

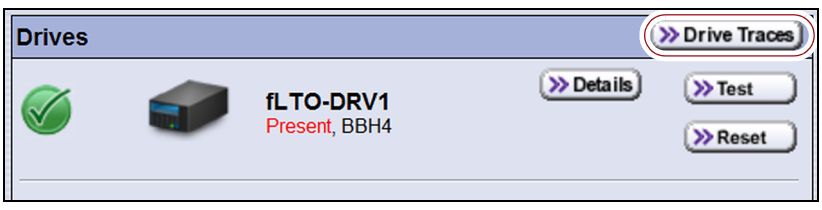


Figure 274 Click **Drive Traces** on the Drives screen.

3. Click **Drive Traces**. The Drive Traces screen displays.

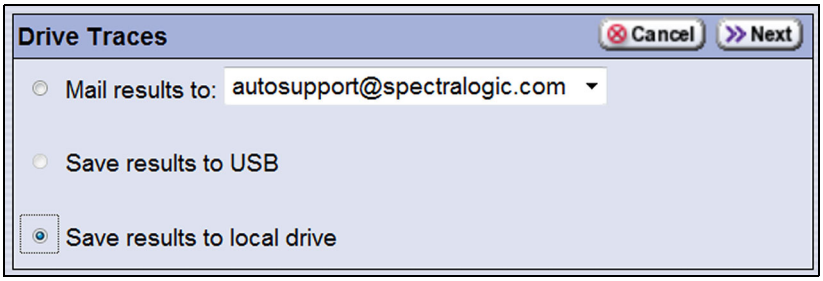


Figure 275 The Drive Traces screen.

4. Select what you want to do with the drive trace file.

Option	Description
Mail results to	Sends the drive trace file to a previously configured email recipient. Use the drop-down list to select the recipient for the trace file. Only previously configured email recipients are listed. To send the email with the attached trace file to someone who is not listed, exit the utility, configure that person as an email recipient (see Configure Mail Users on page 107), and then run the utility again. **Note:** Do not use the default autosupport@spectralogic.com email recipient. Spectra Logic does not save emailed drive trace files unless they are specifically requested for troubleshooting.
Save results to USB	Saves the drive trace file to the USB device connected to the LCM. **Note:** This option is only available if you connected a USB device to one of the USB ports on the LCM before accessing the Utilities screen.
Save results to local drive	Downloads the drive trace file to your local computer. Use your web browsers download features to open or save the file. **Note:** This option is only available if you are accessing the library through the BlueScale web interface.

5. Click **Next**. The second Drive Traces screen displays.

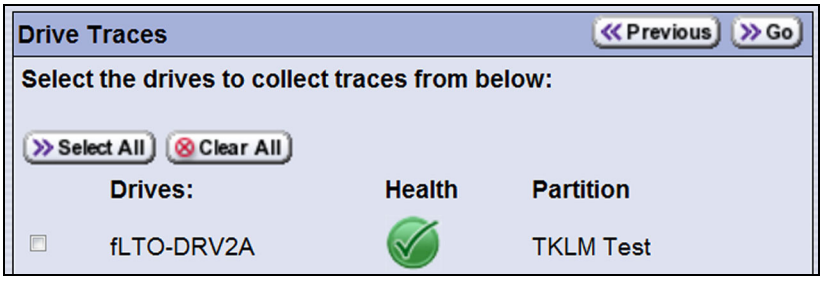


Figure 276 The second Drive Traces screen.

6. Select the drives from which you want to generate traces. The drive trace file contains a subdirectory for each drive.
7. Click **Go**. The wizard generates the traces and saves or sends the drive trace file as selected.

Use the IBM Tape Diagnostic Tool (ITDT)

Download ITDT and its related documentation directly from IBM's Fix Central website. For information about navigating IBM's website and downloading the version of ITDT that is appropriate for your operating system, log on to the portal (see Accessing the Technical Support Portal on page 472), open the Knowledge Base, and search for KBA-01768, *Downloading and installing ITDT (IBM Tape Diagnostic Tool)*.

Important Use the latest version of ITDT to gather a drive dump from the latest generation of drives.

Use the following steps to download and install ITDT on a computer that is connected to the same Fibre Channel arbitrated loop or fabric as the drives in the library.

1. Log into IBM's website at http://www.ibm.com/support/fixcentral, using your individual IBM ID.
2. Select the following options:
   - **Product Group** = System Storage
   - **Select from System Storage** = Tape systems
   - **Select from Tape Systems** = Tape drivers and software
   - **Select from Tape drivers and software** = IBM Tape Diagnostic Tool (ITDT)
   - **Platform** = Select your operating system from the drop-down list and click **Continue**.
3. On the next page, select the version of ITDT that you want to download. If desired, you can select multiple versions.

   Note: If you are unsure which version to select, click **Show Fix Details** to see additional information.
4. Click **Continue.** If you are not logged into the website yet, you are prompted to do so now.
5. Choose one of the following methods to download the selected ITDT installation files:
   - **Download using your browser (HTTP)**
   - **Download using bulk FTP**
   - **Download using Download Director**
6. Download and read the ITDT documentation for assistance in using and setting up the program.
7. Refer to the ITDT documentation for information about using ITDT to retrieve drive dump files. Contact Spectra Logic Technical Support if you need assistance (see Contacting Spectra Logic on page 7).

Use the BlueScale Retrieve Drive Dump Utility

If for some reason you cannot install and use ITDT in your environment, use the BlueScale Retrieve Drive Dump utility to collect the dump file from a drive.

Before You Begin

Before you begin the dump utility, make sure you fulfill the following prerequisites.

Insert USB Device This utility saves the drive dump file to a USB device connected to the LCM. You must plug the USB device into one of the USB ports on the LCM and allow time for the device to mount before you access the Utilities screen (see Using a USB Device on page 152).

User Privilege Requirements Only a user with superuser or administrator privileges can use BlueScale to retrieve a drive dump file.

Run the Utility

1. Determine the BlueScale identifier for the drive from which you want to retrieve the dump file.

   Note: Drives are identified according to their physical location in the library. See Identify the Drives in the Library on page 154 for detailed information.

2. Log into the library as a user with superuser or administrator privileges.
3. Click **MENU** ⋯⁘ **Maintenance** ⋯⁘ **Utilities**. The Basic Utilities screen displays.

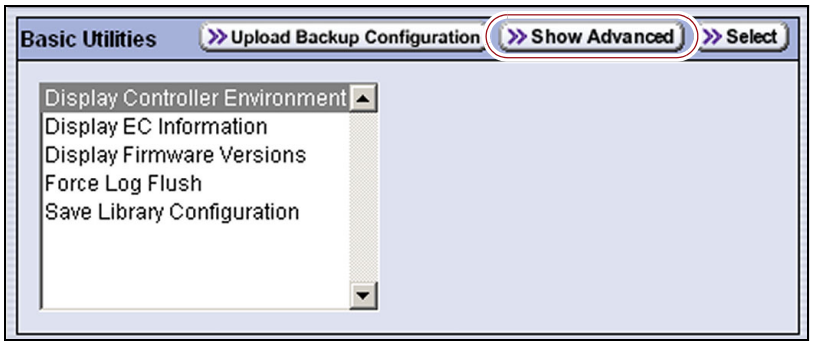


Figure 277 Click **Show Advanced** on the Basic Utilities screen.

4. Click **Show Advanced**. The Advanced Utilities Confirmation screen displays.

5. Click **Yes** to acknowledge the warning about using the advanced utilities. The Advanced Utilities screen displays a list of the advanced utilities.

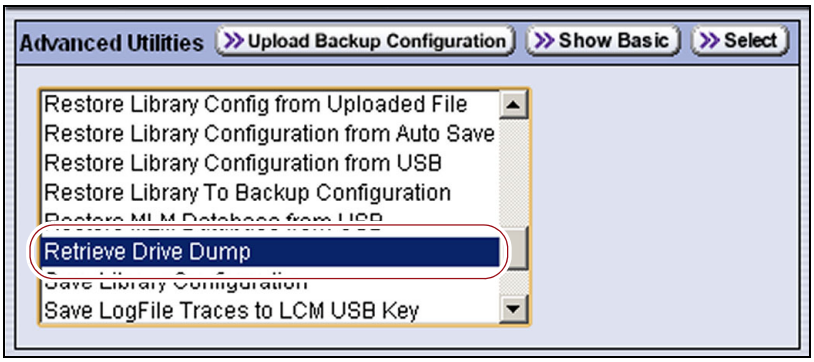


Figure 278 Select the **Retrieve Drive Dump** utility.

6. Scroll through the list of advanced utilities and select **Retrieve Drive Dump**.
7. Click **Select**. The Description screen shows a description of the utility.
8. Click **Next** and use the **Select a drive** list to select the drive from which you want to retrieve the dump file.

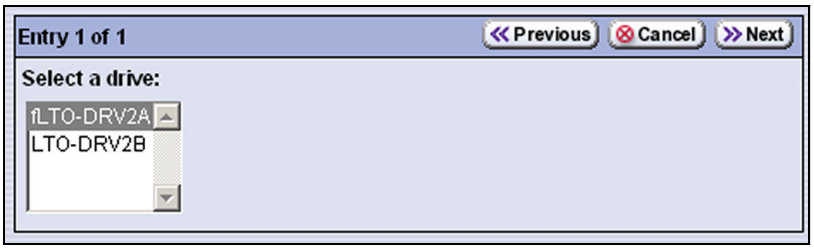


Figure 279 Select the drive from which you want to retrieve the dump file.

9. Click **Next**. The Destinations screen displays.

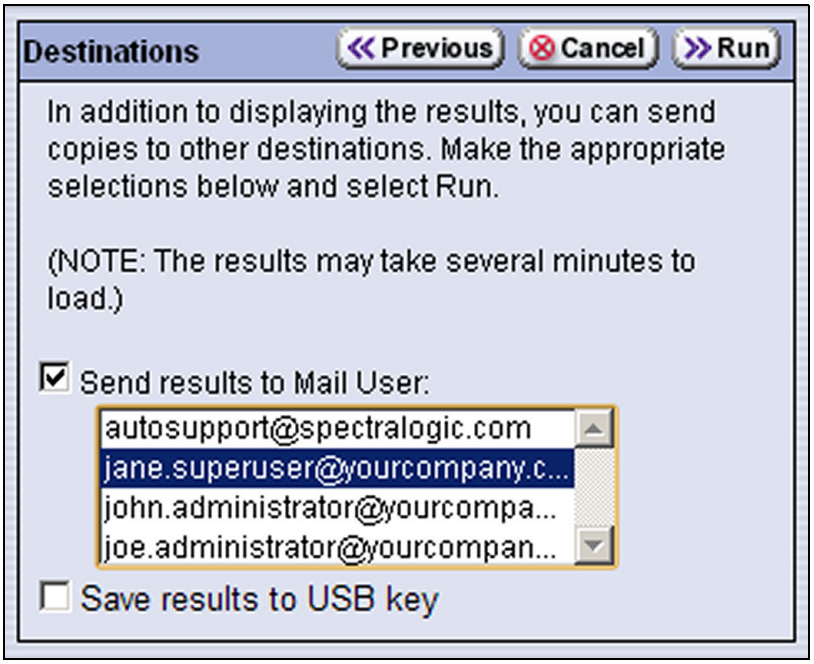


Figure 280 Select the destination for the output of the Retrieve Drive Dump utility.

10. If you want to save the output from the utility, use the check boxes on the Destination screen to select the location; otherwise skip to Step 11.

Option	Description
Send results to Mail User	As an attachment to an email sent to the specified mail recipient. Use the drop-down list to select the recipient for the report file. Only previously configured mail recipients are listed. To send the email with the attached trace file to someone who is not listed, exit the utility, configure that person as a mail user (see Configure Mail Users on page 107), and then run the utility again. **Note:** Do not select autosupport@spectralogic.com as a recipient unless Spectra Logic Technical Support specifically instructs you to send the utility results to them. Spectra Logic does not save emailed files unless they are specifically requested for troubleshooting.
Save results to USB key	To a USB device connected to the USB port on the LCM. **Note:** This option is only available if you connected a USB device to one of the USB ports on the LCM port before clicking **Drive Traces**.

11. Click **Run** to retrieve the dump file from the selected drive.

Important Do not use the drive from which you are retrieving the trace file for any other purpose while the utility runs.

When the dump is saved, the Utility Results screen displays, showing that the utility ran successfully.

RESETTING A DRIVE

Overview You may occasionally need to reset a drive as part of a firmware upgrade or for troubleshooting.

Important Resetting the tape drive that provides the robotic control path (the exporting drive) to the partition causes both the library (the media changer) and tape drive to disappear and reappear from the host's perspective. As a result, your storage management software may stop communicating with the entire library. Consult your storage management software documentation for instructions on how to restore communications to the library after you finish resetting the drive.

Important Drives can be reset using the reset button on the Drives screen or using the Power Drive On/Off utility. This utility should ONLY be run on a drive that is not assigned to a partition. **Do not** use the advanced Power Drive on/off utility to reset a drive that is assigned to a partition. Running this utility on a drive assigned to a partition disables the host interface.

User Privilege Requirements Only a user with superuser or administrator privileges can use the BlueScale software to reset a drive.

Perform the Reset

The following steps describe how to reset a drive using the Reset button on the Drives screen.

1. Determine the BlueScale identifier for the drive you want to reset.

   Note: Drives are identified according to their physical location in the library. See Identify the Drives in the Library on page 154 for detailed information.

2. Log into the library as a user with superuser or administrator privileges.
3. Click **MENU** ⋯⁘ **Configuration** ⋯⁘ **DLM** (or **Drives** if MLM is not enabled) to display the Drives screen.

Figure 281 Click **Reset** next to the drive that you want to reset.

4. Identify the drive that you want to reset and click **Reset**.

5. Confirm that you stopped all backup operations to the library, then click **Next** in response to the Drive Controller Reset warning screen.

   A progress screen displays while the library performs the reset process. When the drive completes its POST and becomes ready, the Drives screen redisplays. The drive is ready for use.

   Note: When the drive resets, the library posts system messages that the drive disappeared and reappeared.

USING A GLOBAL SPARE DRIVE

Overview The Global Spare option lets you remotely replace a failed drive using a drive that is already installed in the library. Using a Global Spare allows you to continue your backup operations and replace the failed drive the next time you are physically present at the library.

Usage Requirements Before you can use the Global Spare option, the following requirements must be met.

- One or more Global Spare drives must already be configured in the partition where the failed drive is located (see Assign a Global Spare Drive on page 179).

Important

The drives that are configured as Global Spares must be connected to the same Fibre Channel arbitrated loop or fabric (SAN) as the drives they replace. If they are not connected to the SAN, they are not be accessible to the application software.

After the Global Spare is activated, you may need to reconfigure your switch to access the spare drive.

- The failed drive must be idle, with no pending backup or restore operations. Backups to the other drives in the partition can continue.

  Note: You cannot use a Global Spare drive to replace a failed drive while the library is actively running the Drive Firmware Update wizard in the partition.

Cartridge Inventory If the failed drive contains a cartridge when it is replaced by the Global Spare, that cartridge is removed from the partition's inventory. If you are able to remove the cartridge from the failed drive after you remove it from the library, reimport the cartridge (see Importing Cartridges on page 203).

PostScan Requirements If a partition is configured to use either FullScan or QuickScan using Global Spares, keep in mind that the PostScan process "owns" the Global Spare drive it is using until it has processed all of the cartridges in the PostScan queue for the partition. As a result, a Global Spare drive that is being used for PostScan is not available for use as a spare.

If all of the Global Spare drives assigned to the partition are in use by the MLM PostScan process, you must pause PostScan to make a Global Spare drive available, as described in Pause the PostScan Process on page 261.

Storage Management Software Guidelines Keep in mind the following storage management software guidelines when using a Global Spare.

- **Backup Exec™ software running on a Windows server**—After sparing or unsparing a drive, you must restart the Backup Exec Device and Media Service for the software to function properly with the spared drive.
- **General guidelines**—In a few rare cases, your backup may fail if a cartridge is loaded into any of the other drives in the partition at the same time that the library is in the process of activating a Global Spare drive for use (as described in this section). Most applications retry the backup operation, but some fail it. If your backup operation fails, wait for the library to complete the Global Spare activation and retry the backup.

User Privilege Requirements Only a user with superuser or administrator privileges can activate or reclaim a Global Spare drive.

Use the Global Spare Drive

Follow these steps to use a Global Spare drive as a temporary replacement for a failed drive.

1. If necessary, use your storage management software to stop any attempts to read from or write to the failed drive. Refer to your storage management software documentation for instructions.
2. Log into the library as a user with superuser or administrator privileges.
3. If the failed drive contains a cartridge, use your storage management software to move the cartridge back to its storage location.

   If you cannot use your storage management software, then move the cartridge as described in Move Cartridges Within a Partition on page 226.

   Note: Continue with the Global Spare process even if you are unable to move the cartridge from the drive.

4. Click **MENU** ⋯⁘ **Configuration** ⋯⁘ **Partitions** to display the Partitions screen.

Figure 282 Click **Global Spare** to begin the process of replacing a partition drive with a Global Spare drive.

5. Click **Global Spare** for the partition that contains the failed drive to display the Global Spare Usage screen.

   Note: The Global Spare button is not present if a drive is not configured as a Global Spare for the partition (see Assign a Global Spare Drive on page 179).

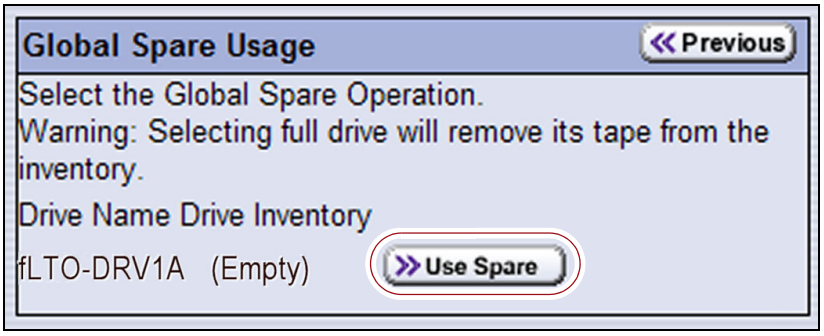


Figure 283 Click **Use Spare** for the drive you want to replace.

6. Click **Use Spare** next to the drive for which you want to substitute the Global Spare drive. Wait for the library to complete the sparing operation.

   Notes:
   - When you select the drive to replace, the BlueScale software disables the selected drive and configures an available Global Spare drive to report the same WWN and serial number as the drive it is replacing. The failed drive can then be removed and replaced the next time you are physically at the library.
   - If you have more than one available Global Spare drive, the library automatically selects a drive in no particular order.

7. If desired, click **MENU** ⋯⁘ **Configuration** ⋯⁘ **DLM** to view the Drives screen. The drive icons on the screen change to indicate the failed drive and the Global Spare that replaced it.

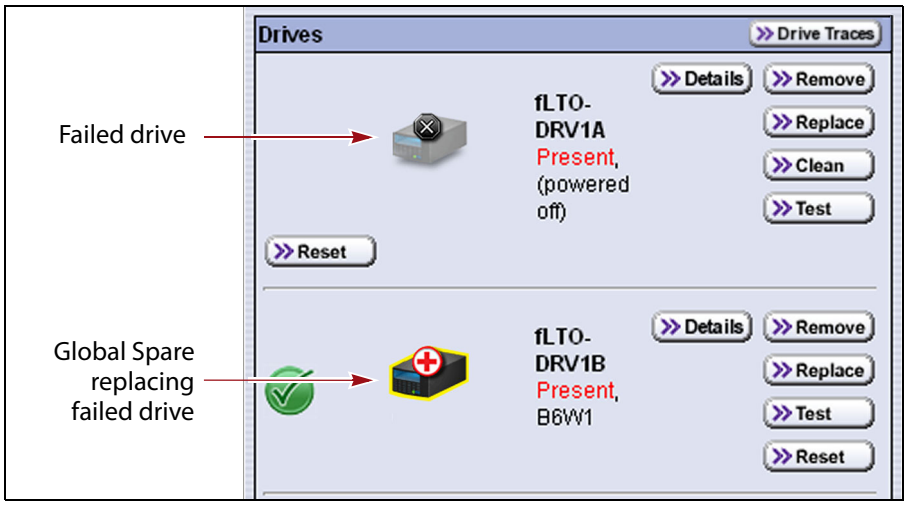


Figure 284 Check the Drives screen to confirm that the failed drive was replaced by a Global Spare drive.

8. If necessary, use your storage management software to bring the Global Spare drive that replaced the failed drive online. Refer to your storage management software documentation for instructions.

Important Replace the failed drive as soon as possible and reconfigure the spare drive to return it to a Global Spare configuration.

Note: If your storage management software cannot access the Global Spare drive, confirm that the drive is properly connected to the same SAN as the failed drive. You may also need to reconfigure the Fibre Channel switch.

Undo the Global Spare Drive

After you physically replace the failed drive (see Replace a Drive on page 466), use the following steps to begin using the replacement drive and return the Global Spare to the pool of available spare drives.

1. Log into the library as a user with superuser or administrator privileges.
2. Physically replace the failed drive with the new drive that you received from Spectra Logic (see Replace a Drive on page 466).

3. Use your storage management software to prepare the Global Spare drive. Refer to your storage management software documentation for information.
   a. Stop all storage management software activity to the Global Spare drive that replaced the failed drive.
   b. If necessary, use your storage management software to eject the cartridge from the drive and return it to its slot.
   c. Take the Global Spare drive offline.
4. When the Global Spare drive is empty and offline, click **MENU** ⋯⁘ **Configuration** ⋯⁘ **Partitions** to display the Partitions screen (see Figure 282 on page 411).
5. Click **Global Spare** for the partition that contained the failed drive to display the Global Spare Usage screen.

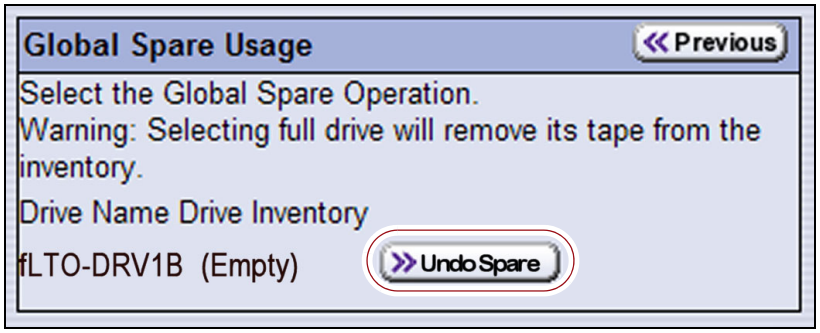


Figure 285 Click **Undo Spare** to begin using the replacement drive you installed.

6. Click **Undo Spare** next to the drive you physically replaced.

   The BlueScale software stops substituting the Global Spare for the drive it replaced and reconfigures the replacement drive back into the partition. The Global Spare is then available to be used again, as needed.
7. Use your storage management software to bring the newly installed drive online and resume backup operations. Refer to your storage management software documentation for instructions.

USING DLM TO TEST AN LTO DRIVE

Overview BlueScale Drive Lifecycle Management (DLM) lets you monitor the DLM health information of each LTO drive in the library and helps you identify drives that experience a high number of errors or other problems during operation. See Chapter 9 – Using Drive Lifecycle Management, beginning on page 279 for detailed information about using DLM to monitor the health of LTO drives.

If you suspect that a drive is experiencing problems or if the Drive Lifecycle Management report indicates that a drive is experiencing repeated errors, you can use the DLM Drive Health Verification wizard to test the drive. This test, when used in conjunction with other DLM data and MLM data, can help you determine whether a drive or the media is the source of the errors you are investigating.

User Privilege Requirements Only a user with superuser or administrator privileges can perform a DLM Drive Health test.

Requirements for Using the Wizard Before you can run the DLM Drive Health Verification wizard, the following requirements must be met:

- The drive must not contain a cartridge.
- The drive must be cleaned just before beginning the test.
- A scratch tape that is the same LTO generation as the drive being tested must be available in the partition's entry/exit pool. The scratch tape health must be Good (green) for an MLM-enabled cartridge or Usable for a cartridge that is not MLM-enabled. You can use MLM to determine the health of the cartridges currently in the storage partition containing the drive you want to test (see Generate MLM Reports on page 262).
- The scratch cartridge must have a barcode label.
- The scratch cartridge must not be write-protected.
- If the scratch cartridge is encrypted using BlueScale encryption, the encryption key must be present on the library.

Caution Make sure that the scratch tape does not contain data that you need to retain. The test process overwrites all data on the tape.

Important The DLM Drive Health test requires the scratch tape used for the testing to be the same generation as the drive. If the tape is not the same generation as the drive, the test fails.

Important The test fails if the scratch cartridge health is not Good or Usable.

Notes:
- If the cartridge health is unknown (that is, it is not currently listed in the library's MLM database), the library loads the cartridge into a drive to determine the health before beginning the test.

Run the DLM Drive Health Verification Wizard

Use the following steps to launch the DLM Drive Health Verification wizard.

1. Log into the library as a user with superuser or administrative privileges.
2. Clean the drive you plan to test (see Cleaning a Drive on page 442).
3. Import or move a scratch cartridge to the E/E slot (see Move Cartridges Within a Partition on page 226).

   Note: If you use the Import/Export screen to import the cartridge, do not move the cartridge to a slot; leave it in the E/E slot.

4. Click **MENU** ⋯⁘ **Configuration** ⋯⁘ **DLM** to display the Drives screen.

   Note: The **Test** button is not present if DLM is not enabled.

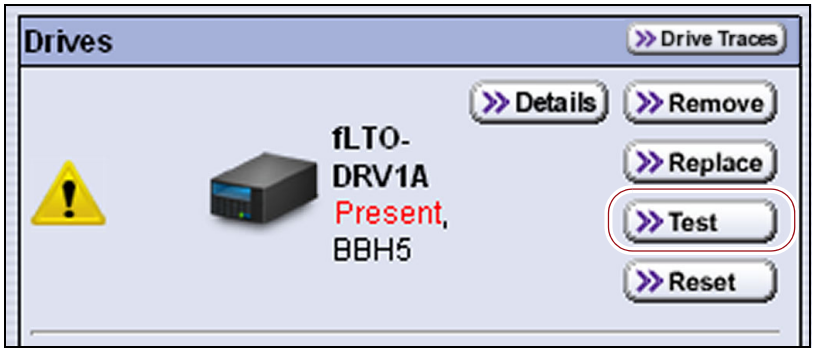


Figure 286 Click **Test** on the Drives screen to launch the wizard.

5. Click **Test** next to the drive you want to test to start the DLM Drive Health Verification wizard.

   The wizard determines whether all of the requirements for the test are met.

   All Requirements Met If all of the requirements for performing the test are met, the Drive Health Verification screen displays a warning about the upcoming test process. Proceed to Step 6 on page 417.

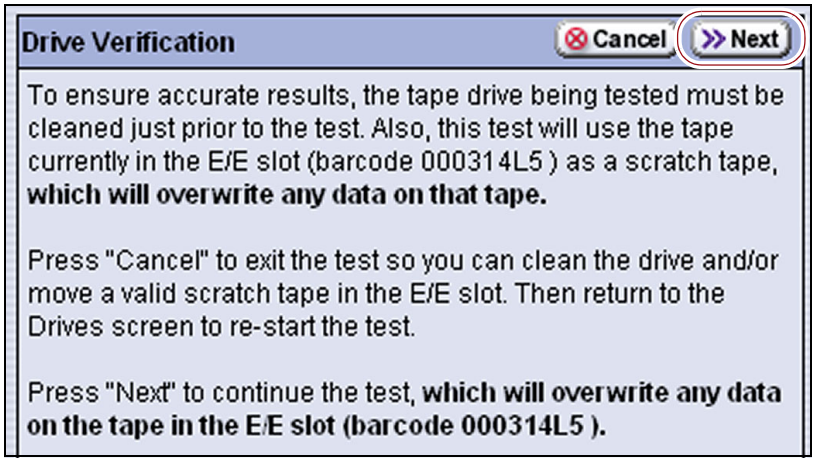


Figure 287 Click **Next** on the Drive Health Verification screen to begin the verification process.

Requirements Not Met If one or more requirement are not met, the Drive Health Verification screen displays information about what needs to be done.

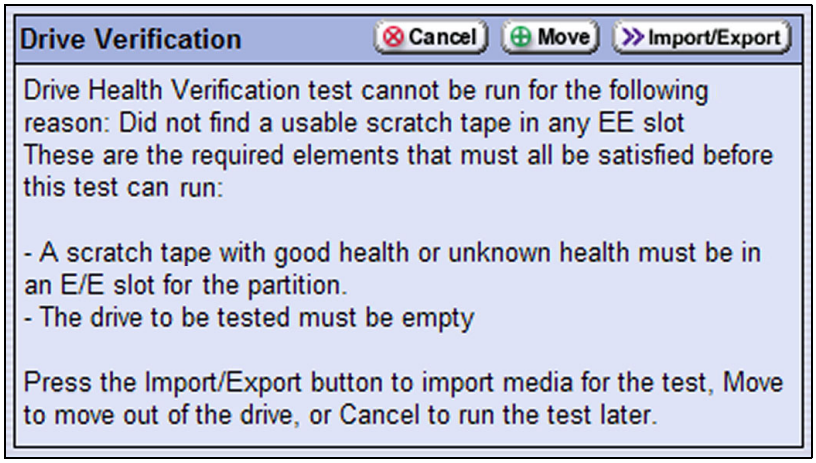


Figure 288 Address all of the requirements on the Drive Health Verification screen.

Note: If you are accessing the library remotely using the BlueScale web interface and either the scratch cartridge or the cleaning cartridge is not available, then **Cancel** is the only option available.

Use the following steps to address the requirements listed on the Drive Health Verification screen.

a. Click **Move** or **Import/Export**, as required, to move a cartridge out of the drive or import a scratch cartridge and a cleaning cartridge into the partition.

b. After you complete the necessary actions, begin the entire process again, starting with Step 4 on page 415.

c. When all of the requirements are met, proceed to Step 6.

6. Click **Next** to begin the automatic test process. A series of status screens lets you know how the test is progressing. The test process requires approximately 15 minutes to complete.

7. When the test is complete, review the DLM Test Results screen to determine the outcome of the test and respond as required.

- If the drive passes the test, the drive health is set to Good (green). You can continue using the drive.

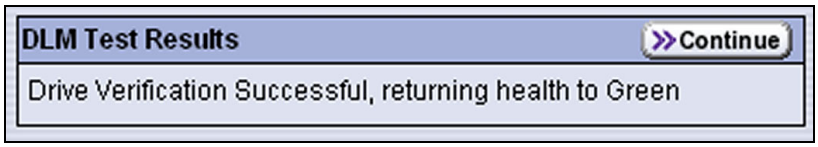


Figure 289 The DLM Test Results screen (test successful).

- If the drive fails the test, the drive health is set to Poor (red). Make a note of the error code in the results message and contact Spectra Logic for assistance (see Contacting Spectra Logic on page 7).

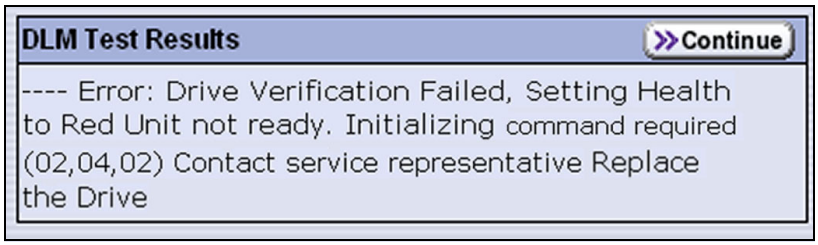


Figure 290 The DLM Test Results screen (test failed).

8. Click **Continue** to return to the Drives screen.

CHAPTER 14

Maintaining the Library

This chapter describes the common maintenance tasks for the T50e library. See Chapter 15 – Maintaining the Drives, beginning on page 441 for detailed information about maintaining the library's drives.

Important Contact Spectra Logic Technical Support before making any changes to your library hardware or performing any maintenance operations.

UPDATING, SERVICING, OR MOVING THE LIBRARY

Contact Spectra Logic Technical Support before making any changes to your library hardware or performing any service operations.

Installing Additional Drives

Installing an additional drive causes the library to reassign element addresses when the drive is added to a partition. To avoid errors, reconfigure your storage management software after adding a new drive (refer to your software documentation for instructions).

Servicing the Library

In the event that it is necessary to replace a component, make sure that you have instructions for performing the procedure *and* you either:

- Are instructed to do so by Spectra Logic Technical Support,

  —OR—

- Have a support contract such as Assisted Self-Maintenance (ASM).

RENEWING THE BLUESCALE SOFTWARE SUPPORT KEY

You must have a current support agreement and corresponding BlueScale Software Support key entered in the library before you can update the library's BlueScale software and the component firmware. You are able to download updated BlueScale packages from the Technical Support portal; however, without a valid BlueScale Software Support key installed on the library, you are not be able to apply the updates to the library.

Notes:
- Spectra Logic sends you an email notification before your current support key expires.
- The library also generates informational messages to let you know that the support key is about to expire.

If your BlueScale Software Support key expires, the following screen displays when you attempt to update the library.

Figure 291 The BlueScale Software Support Key Expired screen.

You must renew the BlueScale Software Support key before you can continue. You must have a current service contract to generate a new BlueScale Software Support key, if you do not have a current service contract, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

If your library is covered by warranty or a service contract, and you need a BlueScale Software Support key, follow these steps:

1. Log into your account on the Technical Support portal at support.spectralogic.com.

   Note: See Accessing the Technical Support Portal on page 472 for information about creating an account and accessing the Technical Support portal.

2. Select **Incidents & Inventory ⋯ Service Key Generation**.

3. On the Service Key Generation page, click the name of the library type for which you want to generate a service key. Only the library types you own are listed.

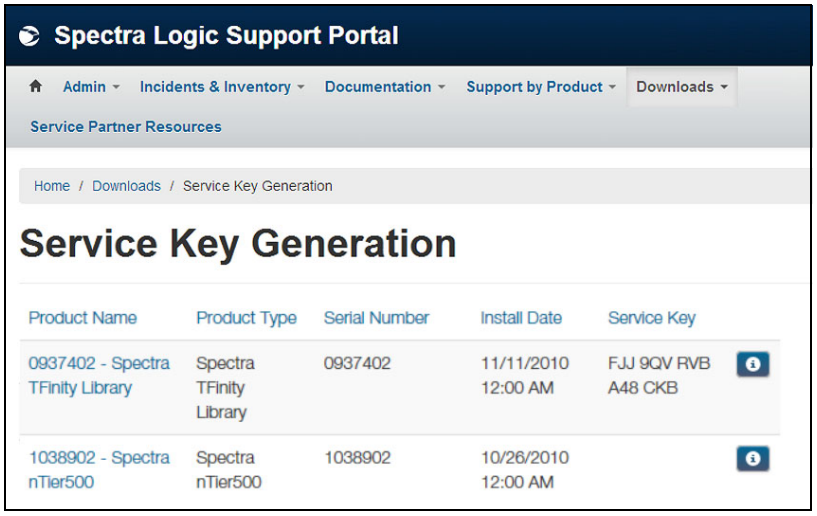


Figure 292 The Service Key Generation screen.

4. On the Software Support Keys Generator page, the **Product Name**, **Product Type**, and **Serial Number** fields are populated with the information for your library. Click **Generate Key**. The page refreshes to display the new Product Service Key.

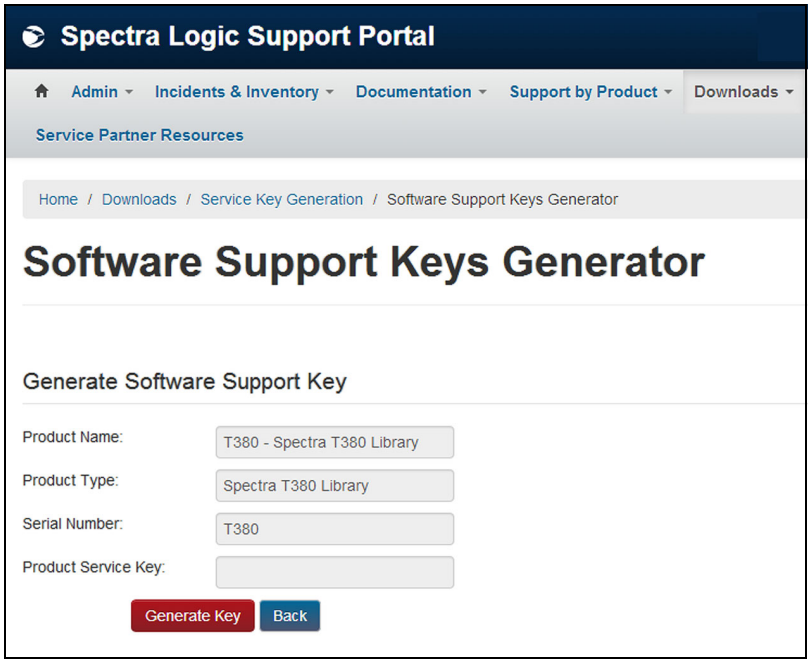


Figure 293 The Software Support Key Generator page.

5. After you generate your key, enter it into the library as described in Enter Activation Keys on page 115.

UPDATING THE BLUESCALE SOFTWARE AND LIBRARY FIRMWARE

Overview The BlueScale software and library firmware are updated regularly to provide new functionality and resolve issues. Spectra Logic recommends that you keep your library up-to-date at all times. If your library is not using the most current BlueScale version, updating it to the most current version is strongly recommended.

Important

Your library must either still be under warranty or you must have a current service contract with Spectra Logic Technical Support before you can perform BlueScale updates, including firmware updates for the library components. The BlueScale Software Service key associated with your service contract must be entered into the System Configuration screen before you can update the library.

- For instructions on how to renew and enter your BlueScale Software Support key, see Renewing the BlueScale Software Support Key on page 419.
- If you have questions about your service agreement, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

New Package Availability The most currently released version of the BlueScale package for the library is available on the Product Software page on the Technical Support portal.

If Auto Download is configured (see Configure a Package Server on page 132), the library checks configured package servers once a week for a library update package newer than what the library is currently running. If a new package is available, the library downloads it, sends a system message, and displays an icon on the status bar to indicate the update is available (see Auto Download Icon on page 83). If the library already downloaded an update package, you can continue with Prepare for the BlueScale Package Update on page 428.

Package Support Packages are groupings of program code that contain the BlueScale software and the firmware for the library components. Spectra Logic provides complete support for the two most recently released BlueScale packages. If your library is not running the most current BlueScale version, you may be required to update your library to resolve an issue or to verify that the problem still exists.

The *Spectra T50e Library Release Notes and Documentation Updates*, available on the Technical Support portal, provides information about the updates in the current BlueScale package, as well as updates to this guide and other documentation.

User Privilege Requirements All users can view the BlueScale version that the library is using on the status bar at the top of each screen (see Figure 294 on page 423). Only a user with superuser or administrator privileges can access the Maintenance menu to view component firmware versions and update the BlueScale software and library firmware. See Understanding User Groups and Security on page 94 for information about the three types of user groups and what types of privileges each has.

Check the Library BlueScale Software Version

Use the following steps to determine the BlueScale software version currently running on the library.

1. Log into the library as a user with superuser or administrator privileges.
2. Determine the BlueScale software version currently running on the library.
   - The status bar at the bottom of each BlueScale screen shows the BlueScale version running on the library.

Figure 294 Locate the BlueScale software version on the status bar.

—OR—

   - Click **MENU**, then select **Maintenance** ···⁘ **Package Update** to view the full version number for the current package on the Package Update screen.

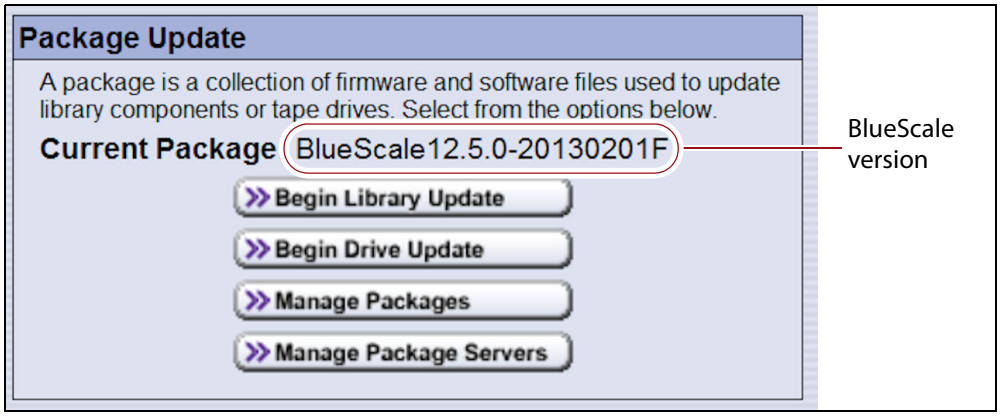


Figure 295 The BlueScale version shown on the Package Update screen.

Check Component Firmware Versions (Optional)

Note: This procedure is not necessary unless recommended by Spectra Logic Technical Support.

1. Log into the library as a user with superuser or administrator privileges.

2. If you want to save the information about the firmware versions to a USB device, connect a USB device to a USB port on the LCM and allow time for the device to mount.

   Note: The option to save the information to USB is only displayed if you plug a USB device into the LCM before you select **Utilities** (see Using a USB Device on page 152).

3. Click **MENU**, then select **Maintenance ⋯⁘ Utilities**. The Basic Utilities screen displays.

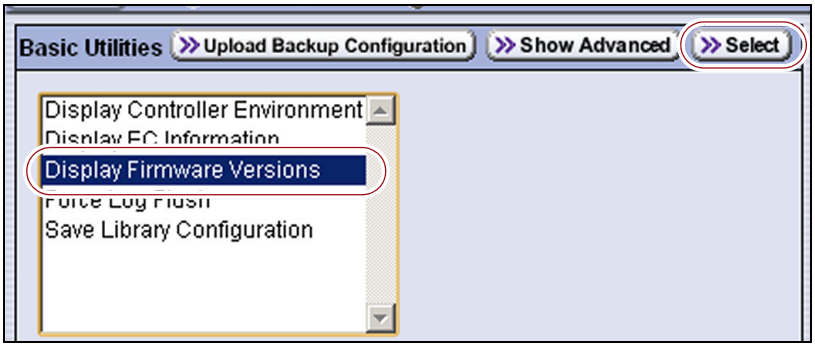


Figure 296 Select **Display Firmware Versions**.

4. Select **Display Firmware Versions**, then click **Select**. The Description screen shows the details for the utility.
5. Click **Next**. The Destinations screen displays.

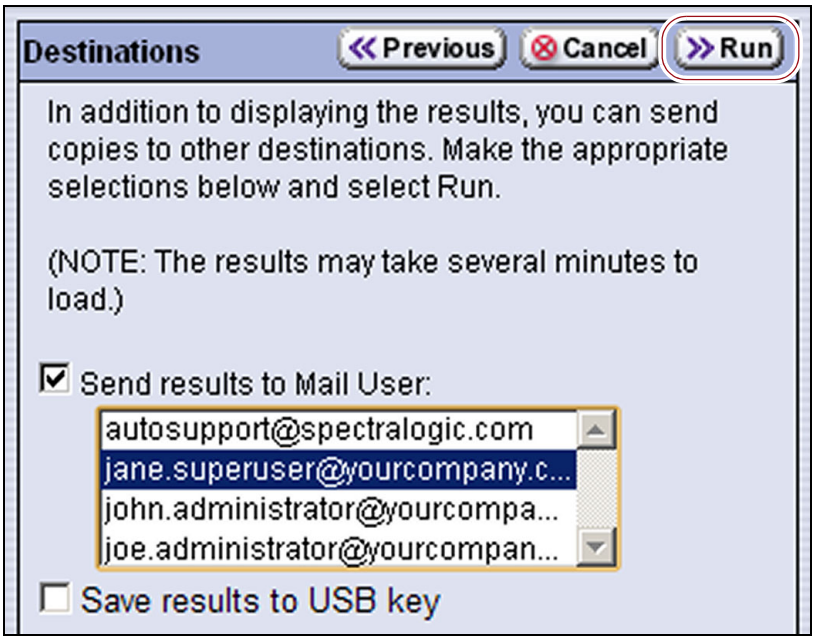


Figure 297 Select additional destinations.

6. If you want to save the output from the utility, use the check boxes at the top of the screen to select the location; otherwise skip to Step 7.

Selecting...	Saves the output...
Send results to Mail User	As an attachment to an email sent to the specified mail recipient. Use the drop-down list to select the recipient for the report file. To send the email with the output to someone who is not already listed as a library user, you must first configure that person as an email recipient (see Configure Mail Users on page 107). **Note:** Do not select autosupport@spectralogic.com as a recipient unless Spectra Logic Technical Support specifically instructs you send the output from the utility to them. Spectra Logic does not save emailed results files unless they are specifically requested for troubleshooting.
Save results to USB key	To a USB device connected to a USB port on the LCM. **Note:** This option is only available if you inserted a USB device in Step 2 on page 424.

7. Click **Run**. After a brief delay, the Utility Results screen displays the current component firmware versions. Scroll as necessary to view all of the data.

   Note: You can drag the bottom right corner of the scroll box containing the component firmware version information to adjust the length and width of the scroll box.

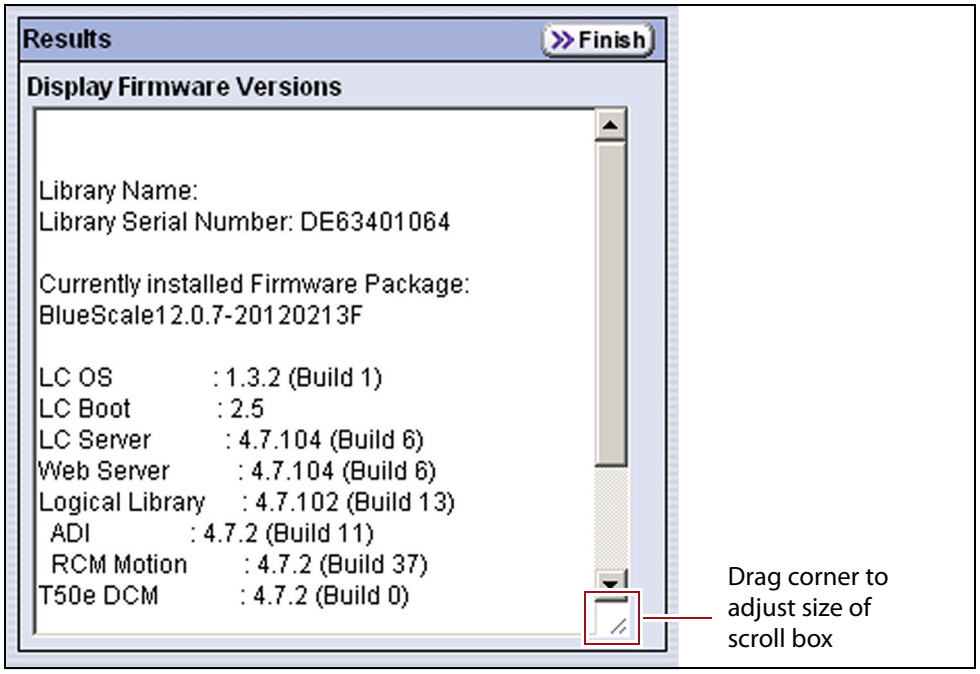


Figure 298 View the output of the View Firmware Versions utility.

8. If you chose to save the results to a USB device, a message displays showing the filename for the results file.

   If you are connected to the library using a web browser, you can also copy and paste the results from the Utility Result screen into a text file and email it to Spectra Logic Technical Support if they request it.

9. Click **Finish** to return to the Utilities screen.
10. If requested to do so, send this information to Spectra Logic Technical Support (see Contacting Spectra Logic on page 7) for advanced troubleshooting.

Check the Currently Released BlueScale Version

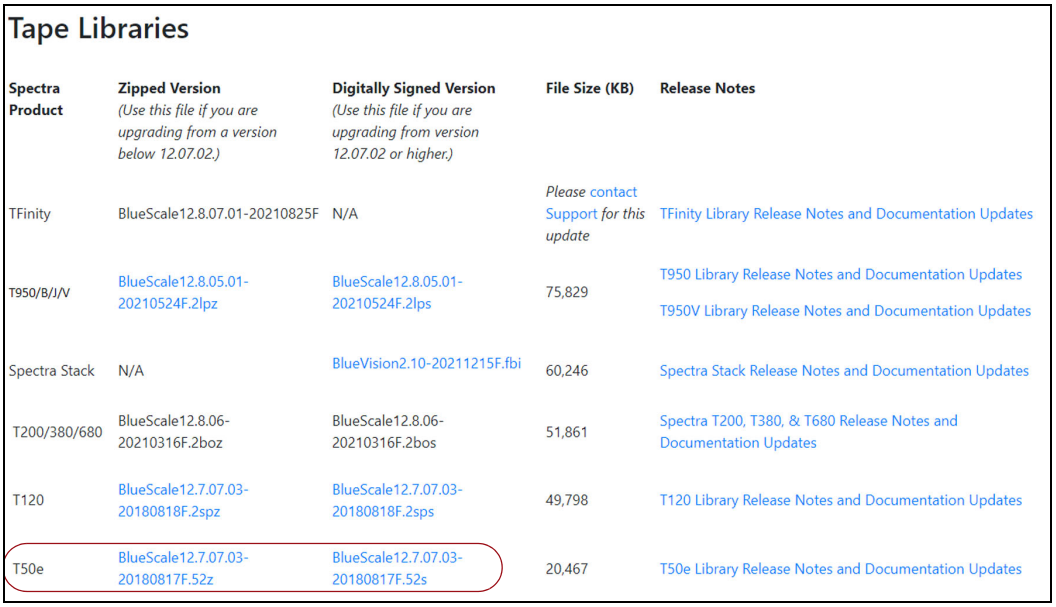
Follow these steps to check the currently recommended BlueScale version.

Note: Figures in this section show the Spectra TFinity library. When performing these steps, make sure you select T50e.

1. Log into your user account on the Technical Support portal at support.spectralogic.com.

   Note: See Accessing the Technical Support Portal on page 472 for information about creating an account and accessing the Technical Support portal.

2. Select **Downloads** ⋯ **Product Software**.
3. On the Product Software page, locate your library type in the **Spectra Product** column. The currently released BlueScale version is listed in the **Current Version** column.



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	BlueScale12.8.07.01-20210825F	N/A	*Please contact Support for this update*	TFinity Library Release Notes and Documentation Updates
T950/B/J/V	BlueScale12.8.05.01-20210524F.2lpz	BlueScale12.8.05.01-20210524F.2lps	75,829	T950 Library Release Notes and Documentation Updates T950V Library Release Notes and Documentation Updates
Spectra Stack	N/A	BlueVision2.10-20211215F.fbi	60,246	Spectra Stack Release Notes and Documentation Updates
T200/380/680	BlueScale12.8.06-20210316F.2boz	BlueScale12.8.06-20210316F.2bos	51,861	Spectra T200, T380, & T680 Release Notes and Documentation Updates
T120	BlueScale12.7.07.03-20180818F.2spz	BlueScale12.7.07.03-20180818F.2sps	49,798	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

Figure 299 The Product Software screen.

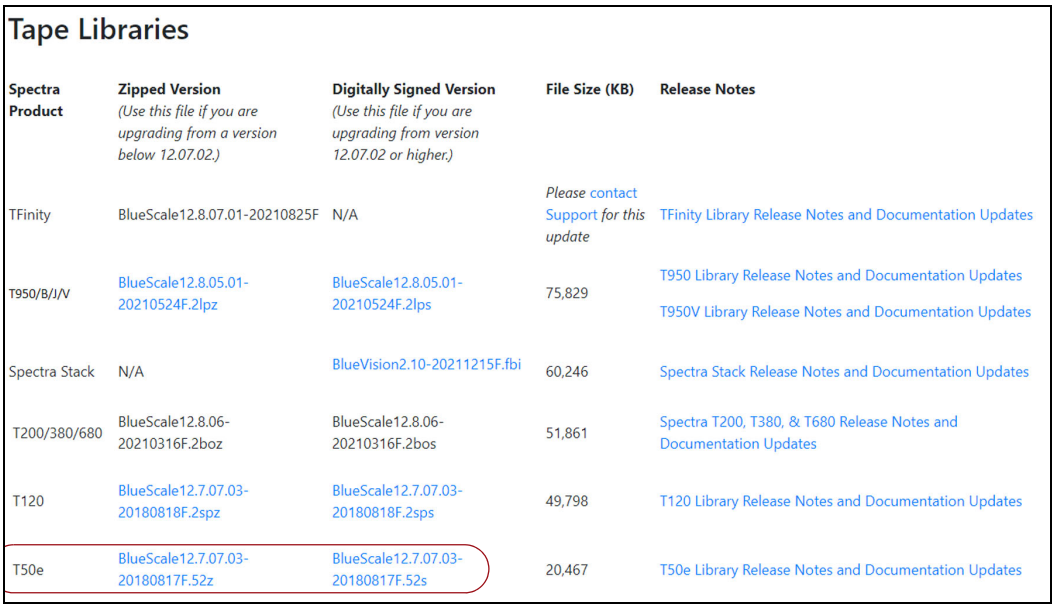
4. Compare the Current Version available for the library to the version installed on the library.

Download the BlueScale Package

If Auto Download is configured (see Configure a Package Server on page 132) or your library has Internet access and you plan to download the BlueScale package directly to the library from the Spectra Logic package server, skip to Prepare for the BlueScale Package Update on page 428.

If your library cannot access an outside website because of security or firewall requirements, use the following steps to download the BlueScale package from the Technical Support portal. You can save the BlueScale package to a USB device or a previously configured package server.

1. Log into your account on the Technical Support portal at support.spectralogic.com.
2. Select **Downloads** ⋯ **Product Software**. The Product Software page displays.



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	BlueScale12.8.07.01-20210825F	N/A	*Please contact Support for this update*	TFinity Library Release Notes and Documentation Updates
T950/B/J/V	BlueScale12.8.05.01-20210524F.2lpz	BlueScale12.8.05.01-20210524F.2lps	75,829	T950 Library Release Notes and Documentation Updates T950V Library Release Notes and Documentation Updates
Spectra Stack	N/A	BlueVision2.10-20211215F.fbi	60,246	Spectra Stack Release Notes and Documentation Updates
T200/380/680	BlueScale12.8.06-20210316F.2boz	BlueScale12.8.06-20210316F.2bos	51,861	Spectra T200, T380, & T680 Release Notes and Documentation Updates
T120	BlueScale12.7.07.03-20180818F.2spz	BlueScale12.7.07.03-20180818F.2sps	49,798	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

Figure 300 The Product Software screen.

3. Locate your library type in the **Spectra Product** column. The currently released BlueScale version is listed in the **Current Version** column.
4. Click the name of the BlueScale package next to your library type. The BlueScale package begins downloading through your web browser.

   Note: If you are updating a library running BlueScale12.7.03 or later, select a package ending with the letter "s", which indicates a digitally signed package. If you are updating a library running a BlueScale version prior to 12.7.03, select a package ending with the letter "z", which indicates an unsigned zip package.

5. When the download completes, do not unzip the downloaded file. Copy the file to one of the following locations:
   - The root directory of a USB device.

   Notes:
   - The library only recognizes FAT-formatted, not NTFS-formatted, USB devices.
   - Not all USB devices are compatible with the library. If you are unable to access a USB device from the library, remove it and use a different one.

   —OR—
   - A previously configured package server.

Prepare for the BlueScale Package Update

Use the following sections to prepare to update the BlueScale software and library component firmware.

Make Sure Your BlueScale Software Support Key Is Current

Updating the BlueScale software and the firmware for the library components requires a current service contract with Spectra Logic Technical Support. If your service contract expires, renew it as described in Renewing the BlueScale Software Support Key on page 419.

Prepare the Library

- Stop all library- and host-based operations.

Important

Confirm that all of the following conditions are met before beginning the update:
- All backup processes are complete
- All storage management software daemons are stopped
- All drives are empty

To ensure that no commands are sent to the controllers, Spectra Logic suggests disconnecting fibre cables to any tape drives used as a robotic exporter.

- Back up your MLM database (see Back Up the MLM and DLM Databases on page 270).

  Note: Backing up the MLM database also backs up the DLM database.
- Back up all of your BlueScale encryption keys (see Exporting and Protecting Encryption Keys on page 314).
- Download and read the *Spectra T50e Library Release Notes and Documentation Updates* for the most current information about updated BlueScale packages.

Important

If the release notes provide special requirements or procedures for updating the library, make sure that you follow them.

Select the BlueScale Package and Update Options

1. Log into the library as a user with superuser or administrator privileges.
2. If you downloaded the BlueScale package to a USB device, plug the USB device into the LCM's USB port and allow time for the device to mount **before** continuing (see Using a USB Device on page 152).
3. If you receive an error message stating that your disk is full when the library attempts to unzip a BlueScale package, you need to delete downlevel packages before you can continue. See Manage Update Packages on page 437.
4. Click **MENU**, then select **Maintenance** ⋯ **Package Update**. The Package Update screen displays.

   Note: If the library notifies you that your BlueScale Software Support key expires, see Renewing the BlueScale Software Support Key on page 419.

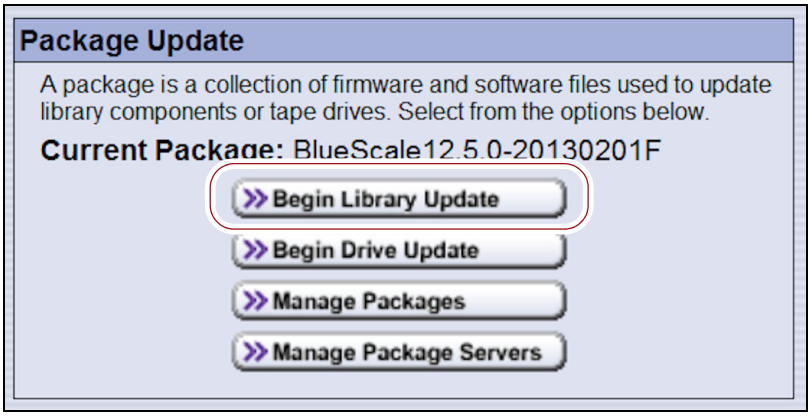


Figure 301 Click **Begin Library Update** to start the process.

5. Click **Begin Library Update**. If the License Agreement screen displays, read the license agreement, then click **Accept**.

   Note: If you decline the agreement, you are not be able to update the library.

6. The Select Package screen displays, listing the file names for the available BlueScale packages.

   Note: The file names begin with the BlueScale version number, followed by the date of release in YYYYMMDD format.

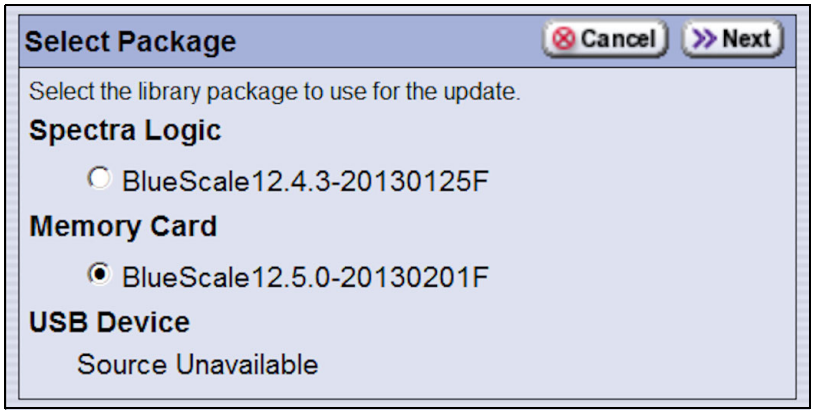


Figure 302 Select the BlueScale package.

7. Select the BlueScale package.

   Note: If the Package does NOT display in the USB or Package server section, you may have downloaded the package for the wrong library type or the wrong signed/unsigned package type.

   BlueScale packages may be found on the sources described in the table below.

Source	Description
Spectra Logic	Select and download the desired BlueScale package from Spectra Logic's package server to the memory card in the LCM and then install it. **Notes:** ▪ The library must have a connection to the Internet before you can use this option (see Configure Network Settings on page 98). ▪ If directed to do so by Spectra Logic Technical Support, update the IP address and package directory for the Spectra Logic package server (see Configure a Package Server on page 132).
Memory Card	Select the desired BlueScale package from packages already stored on the memory card in the LCM.
USB Device	Select the desired BlueScale package from packages stored on a USB device. There is a brief delay while the library accesses the USB device when you select this option. **Notes:** ▪ The **USB Device** option is only available if you previously connected a USB device containing the BlueScale package to a USB port on the LCM in Step 2 on page 429. ▪ The BlueScale package must be stored in the root directory of the USB device. ▪ The USB device must be FAT-formatted, not NTFS-formatted.

Source	Description
Configured Package Server (server name varies)	Select the desired BlueScale package stored on a previously configured package server, if you have one available. **Note:** This option is only available if you previously configured a package server. See Configure a Package Server on page 132 for information about configuring a package server.

8. Click **Next**. The Package Options screen displays.

   The Package Options screen only lists options that are enabled by your previous selections while configuring the library.

   Note: Clicking **Update** immediately starts the update process.

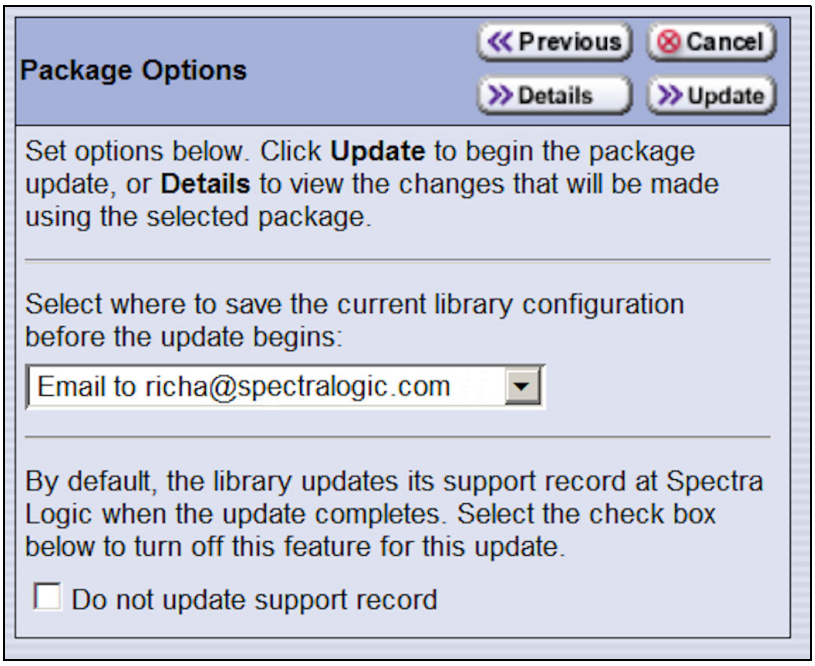


Figure 303 The Package Options screen.

9. On the Package Options screen, select whether and where you want to backup the library configuration before performing the update.

   Note: The backup of the library configuration does not include the MLM or DLM databases.

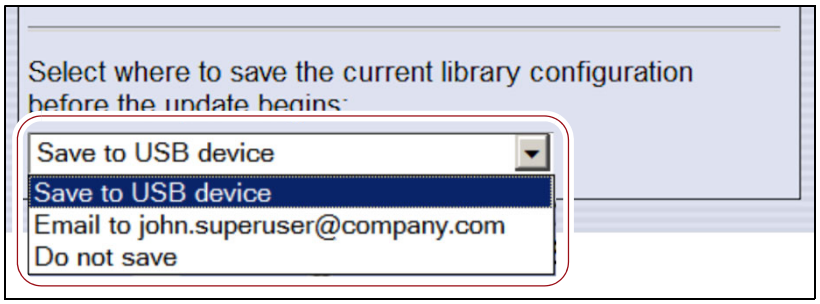


Figure 304 Select whether and where you want to backup the library configuration.

Choice	Action
Save to USB device	Saves a backup of the library configuration to a USB device. Using this option is highly recommended to ensure that you can easily restore the library if necessary. **Notes:** ▪ The **Save to USB device** option is only available if you previously connected a USB device to a USB port on the LCM in Step 2 on page 429. ▪ The USB device must be FAT-formatted, not NTFS-formatted.
Email to...	Emails a backup of the library configuration file to an already-configured email recipient. **Note:** The **Email to** option is only available if you previously configured email recipients (see Configure Mail Users on page 107).
Do not save	Updates the library without saving a backup of the library configuration. If you backed up the library configuration before starting the package update procedure, you can select **Do not save**.

10. On the Package Options screen, select whether or not an email is sent to Spectra Logic Technical Support to update the library's support records.

Notes:
- Sending a notification to Spectra Logic Technical Support is highly recommended.
- This notification does not include the configuration backup file.
- This option is only available if you previously configured the autosupport@spectralogic.com mail user's SMTP IP address (see Create or Modify a Profile on page 335).

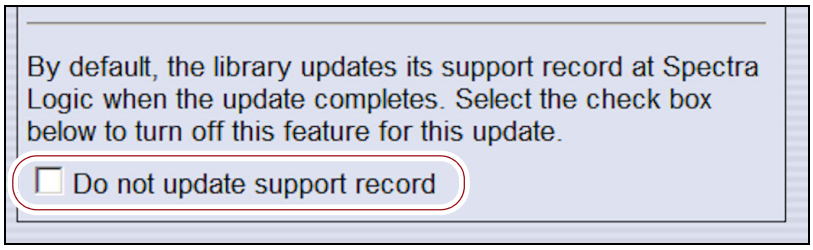


Figure 305 Select whether or not you want to send an update to Technical Support.

11. (**Optional**) To view a list of components affected by the BlueScale package, click **Details** to view the Package Options screen. A Package Details screen, similar to the one shown, displays.

Any items that need to be upgraded or downgraded to match the BlueScale package you chose are automatically selected.

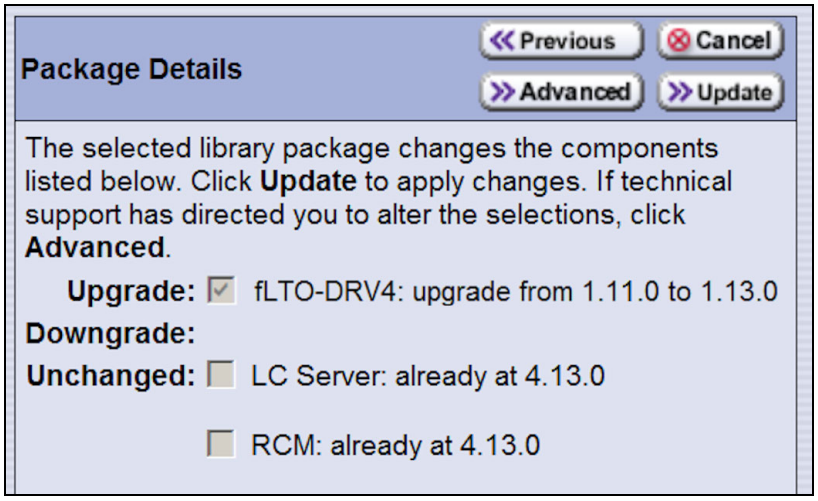


Figure 306 The Package Details screen.

12. (**Optional**) Use the advanced firmware update procedure to update a specific component's firmware.

Important Use the advanced firmware update procedure only when directed to do so by Spectra Logic Technical Support.

a. Click **Advanced** on the Package Details screen. A Package Advanced screen, similar to the one shown, displays.

b. Select or clear the check box next to the library components:

- Clear the check box to prevent the component from upgrading or downgrading.
- Select the check box to force a component to update to the firmware level supplied by the BlueScale package. Depending on the firmware, this could be an upgrade, downgrade, or reapplying the current firmware.

For example, clear everything except **LC Server** to update just the LC Server firmware.

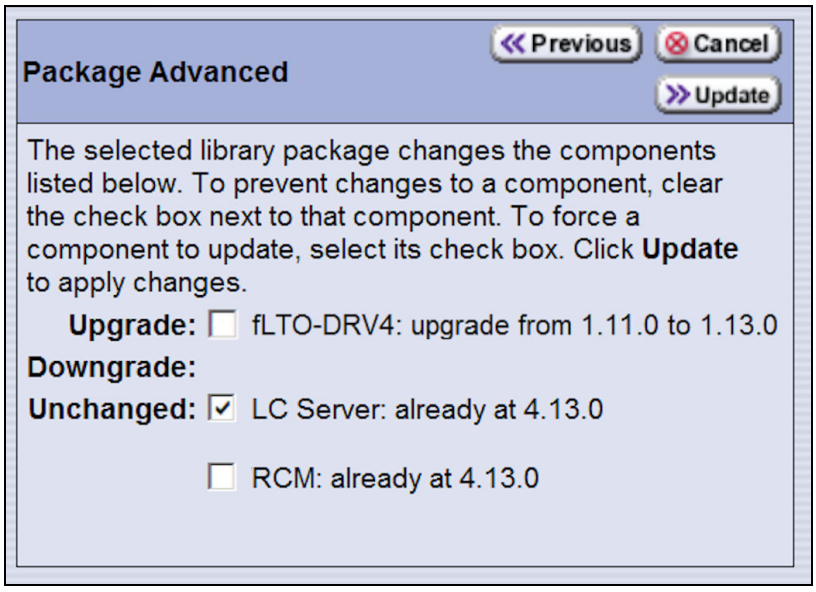


Figure 307 The Package Advanced screen.

Notes:

- Updating all of the automatically selected components is highly recommended.
- Occasionally, Spectra Logic Technical Support may instruct you to update a firmware component even if it is already at the same level as the component in the selected BlueScale package.

Begin the Update

1. Click **Update** to begin the update process.

   Note: If you are updating a library running BlueScale 12.7.03 or later, at the start of a package update that includes LCM updates, the library shuts down all drive exporters so that they do not accept additional moves and then waits for any moves in progress to complete before starting to update the selected components. The drive exporters are re-enabled to accept moves when the package update completes

Important Once the update process starts, it cannot be canceled.

Important Do not turn off power to the library or power-down any component being updated during the update process.

2. The library begins the update process and displays a progress screen, which remains for the duration of the update. Depending on what components are updated, the process can take from several minutes to an hour or more.
3. When complete, the Package Update Results screen displays, showing that the update completed successfully or that a component failed to update.

   Note: If the update fails, examine any system messages and the package update log to determine the cause of the failure. Resolve the problems and retry the update. For further information, see Troubleshooting on page 436.

4. If you used a USB device during the update process, disconnect it from the LCM.
5. Click **Finish** to complete the update. Updates do not take effect until the library completes the update process.

Important Always click **Finish** to complete the BlueScale update process. **Do not** manually reboot the LCM, power-cycle the library, or perform any other operations on the library when you see the Package Results screen. Doing so may cause the update process to fail.

   Note: If you are using the BlueScale web interface to perform the update, the connection to the library is lost when the LCM reboots. Allow sufficient time for the LCM to complete its initialization, then enter the library's IP address in your web browser to reconnect.

6. When the update is complete, the library automatically sends an email to Spectra Logic Technical Support if it is configured as a mail recipient and you selected this option in Step 10 on page 433.
7. After the update is complete, use your storage management software to restart any backup processes.

Troubleshooting

The information in this section may help resolve specific update-related problems.

When you encounter problems while performing a package update, examine any system messages and the package update log to determine the cause of the failure. Resolve the problems and retry the update.

LCM does not automatically reboot When you click **Finish**, make sure at least five minutes have passed to allow for the LCM to complete its initialization. Then, reset the LCM and perform the Package Update process again.

Component failed to update Click **Finish** to complete the update. When the LCM resets, perform the Package Update process again.

Library configuration is corrupted during the update process Use the following steps to restore the library's configuration if it becomes corrupted during the package update process.

Caution

The **Restore Configuration from Checkpoint** utility should only be used immediately after a package update is performed.

Any data that was saved between the time that the package update was performed and the utility is run are lost.

Note: The library automatically saves a Checkpoint Configuration Backup file prior to beginning a package update.

1. From the toolbar menu, select **Maintenance** ···⁘ **Utilities**. The Utilities screen displays.
2. Click **Show Advanced**. The Advanced Utilities Confirmation screen displays.
3. Click **Next**. The Utilities screen refreshes to show a list of the advanced utilities.
4. Scroll through the list of advanced utilities and select **Restore Configuration from Checkpoint**. The screen refreshes to show the details for the utility.

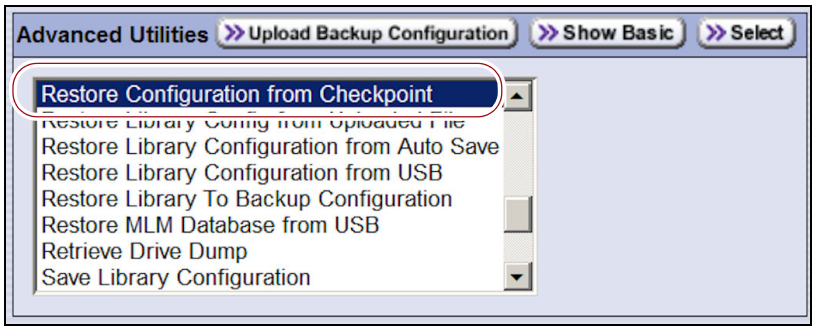


Figure 308 The Advanced Utilities screen.

5. Click **Run Utility** to restore the library to the Checkpoint library configuration.
6. After the library configuration restores, perform the Package Update process again.

Manage Update Packages

The BlueScale packages downloaded to the library reside on the memory card in the LCM. Over time, the packages (one per update) accumulate on the card and the library may post an error message notifying you that the memory card is full. You must delete downlevel packages before you can continue; you can also choose to delete downlevel packages at other times.

Deleting a package file *does not* delete the BlueScale software or component firmware already applied to the library; it simply removes the package file from local storage on the LCM.

Caution There is no confirmation request before the selected package is deleted. Make sure that you no longer need access to a package file *before* you delete it.

The following steps describe how to delete unwanted package files from the memory card in the LCM.

1. Log into the library as a user with superuser or administrator privileges.
2. From the toolbar menu, select **Maintenance** ⋯⁘ **Package Update**. The Package Update screen displays (see Figure 301 on page 429).
3. Select **Manage Packages**. The Manage Packages screen displays with a list of all the BlueScale packages currently stored on the memory card in the LCM.

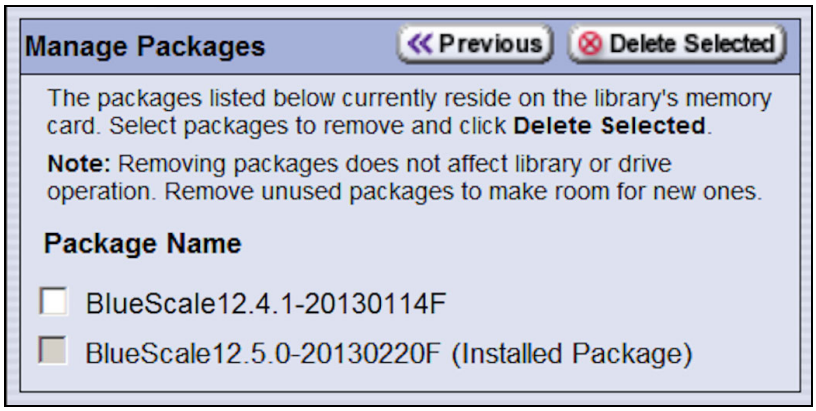


Figure 309 Select the BlueScale packages you want to delete.

4. Select the file(s) that you want to delete, then click **Delete Selected**. The file delete process begins.

CALIBRATING THE TOUCH SCREEN

If the touch points on the library's touch screen do not properly align with the user interface graphics, perform the following procedure to recalibrate the position of the touch points.

Note: You must perform this procedure while standing in front of the touch screen. The utility is not available when accessing the library through the BlueScale web interface.

1. Log into the library as a user with superuser or administrator privileges.
2. Click **MENU**, then select **Maintenance ⋯⁘ Utilities**. The Basic Utilities screen displays.

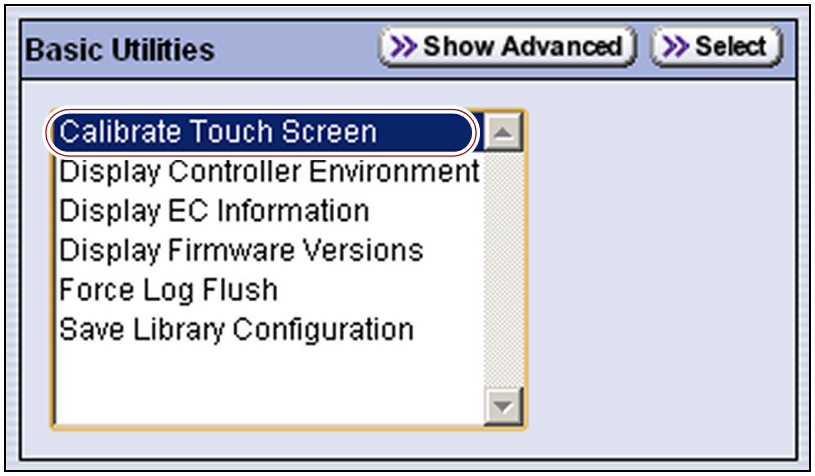


Figure 310 Select the **Calibrate Touch Screen** utility.

3. Select **Calibrate Touch Screen**, then click **Select**. The Description screen shows a description of the utility.

   Note: The **Calibrate Touch Screen** utility is not available if you are accessing the library using the BlueScale web interface.

4. Click **Run**. The touch screen displays a series of calibration target points.
5. Using the stylus, touch each target as it displays to recalibrate the touch points on the screen.

   Note: Touch each point at a straight-on angle as close to the center of the target as possible.

6. When the calibration routine is complete, the Utilities screen redisplays.

Adding Capacity to Your Library

The library ships with ten slots licensed. If you purchased additional capacity when you purchased the library, the additional capacity is licensed during installation of the library. You can also purchase additional capacity at a later date—up to the physical limits of the library.

1. Follow the instructions in Library Upgrades on page 496 to purchase the additional capacity.
2. Follow the instructions in Enter Activation Keys on page 115 to enter the activation key. After you license the new slots, you can add the slots to any existing partition and can then import media into the slots.

   Note: To use slots 48 through 50, you must both purchase the additional capacity and replace a half-height drive bay with a capacity expansion slot for each slot (see Installing Capacity Expansion Slots (Optional) on page 60).

Removing a Capacity Expansion Slot

The Spectra T50e provides expansion slots as an option to enable your library to use up to 50 slots. Each capacity expansion slot takes the place of a single half-height tape drive.

If you previously installed one or more capacity expansion slots and now want to remove one or more of them from the library, follow the steps in this section.

Note: Use the first available location (going from top to bottom) to remove expansion slots.

1. Power the library off (press and hold the front panel power button for one second). The power-off sequence takes approximately two minutes while the library allows applications to shut down gracefully.
2. Access the back of the library.
3. Loosen the screws securing the capacity expansion slot.

4. Slide the capacity expansion slot straight out of the library and place it in its original packaging.

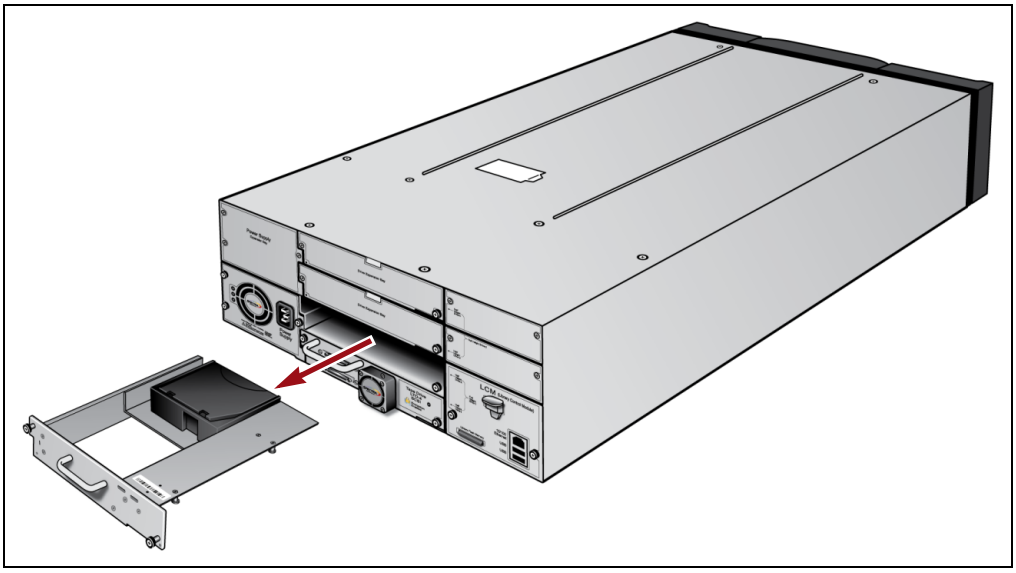


Figure 311 Removing a capacity expansion slot.

5. Install a half-height drive in the location previously occupied by the capacity expansion slot (see Installing the Tape Drives on page 52).

   —OR—

   Replace the drive bay cover that you removed when you initially installed the capacity expansion slot (see Figure 23 on page 61).

Important Do not leave any openings uncovered. All openings must be covered for safety and for proper library cooling.

6. Power the library on (press and hold the front panel power button for two to three seconds or until the button's LED illuminates). Wait while the library completes its power-on sequence, which takes six to seven minutes, depending on the library configuration. During the power-on sequence, the library initializes all of its installed components and performs inventory.

CHAPTER 15

Maintaining the Drives

This chapter describes the common maintenance tasks for drives in the T50e library. See Chapter 14 – Maintaining the Library, beginning on page 418 for information about maintaining the library.

CLEANING A DRIVE

Overview Whenever a tape is loaded or unloaded, the read/write heads are physically cleaned by a brush located within the drive. However, after reading and writing a large amount of data (the exact amount varies by drive type and generation) or if read or write errors occur, the drive requests to be cleaned with a cleaning cartridge. The request is made by sending a Tape Alert message to the host, and displaying a **C** on the SCD The notification is also posted to the library's Drive Details screen (Figure 313 on page 444) and the DLM drive health icon for the drive changes to yellow (see Using the Drive Health Icons on page 282 for additional information).

Using drives with dirty heads can reduce drive performance, decrease usable tape capacity, and result in read/write failures which eventually interrupt data storage.

If you have Auto Drive Clean enabled and the drive is in a partition with an associated cleaning partition, these cleanings are performed automatically. See Creating a Cleaning Partition on page 170 for information about configuring a cleaning partition.

It may also be possible to configure the host software to automatically clean the drives, with a cleaning tape stored in the partition, when the software is notified that drive cleaning is necessary.

If no automatic cleaning process is configured, you must manually clean the drive. If you ignore a cleaning request for too long, the library generates a warning system message.

User Privilege Requirements When Auto Drive Clean is enabled for the storage partition and a cleaning cartridge is available in the cleaning partition, cleanings are performed automatically and do not require user intervention.

If Auto Drive Clean is not enabled, any user with operator privileges who is assigned to the partition and all users with superuser or administrator privileges can manually clean a drive without an associated cleaning partition by placing a cleaning cartridge into the storage partition's entry/exit slot and using the Inventory screen to manually move the cleaning cartridge to the drive (see No Cleaning Partition Present on page 448).

Only a user with superuser or administrator privileges can manually clean a drive by importing a cleaning cartridge directly into a storage partition. See Understanding User Groups and Security on page 94 for information about the three types of user groups and what types of privileges each has.

Determine Whether Cleaning is Required

Clean the library's drives when any of the following occurs:

- The drive indicates that it needs cleaning (see Identify the Problem on page 390) by sending a message to the storage management software.
- The SCD information on the Drive Details screen for an LTO drive displays a **C**.
- The Cleaning Status on the Drive Details screen indicates that the drive requires cleaning (see Figure 313 on page 444).

  Note: In order for the library to monitor drive status, the drive must be configured in a partition.

Use the following steps to use the Drive Details screen to determine whether a drive requires cleaning.

1. Log into the library as a user with superuser or administrator privileges.
2. Click **MENU**, then select **Configuration** ···⁘ **DLM** (or **Drives** if MLM is not enabled). The Drives screen displays.

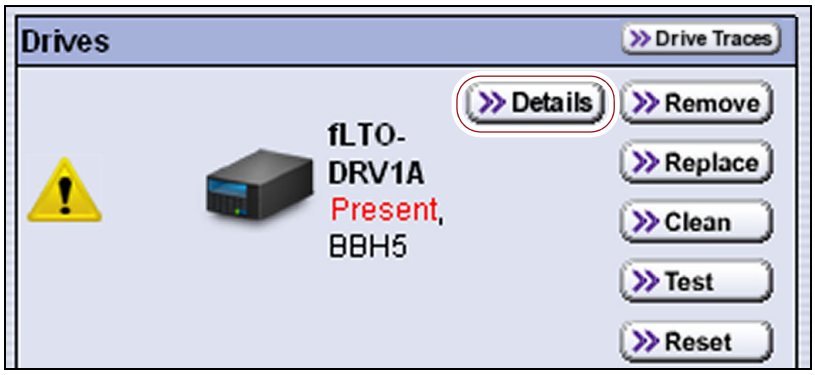


Figure 312 Click **Details** on the Drives screen.

3. Click **Details** next to the drive you want to check. The Drive Details screen displays.

   If the Cleaning Status displays "Drive Cleaning Required," clean the drive as described in the following sections.

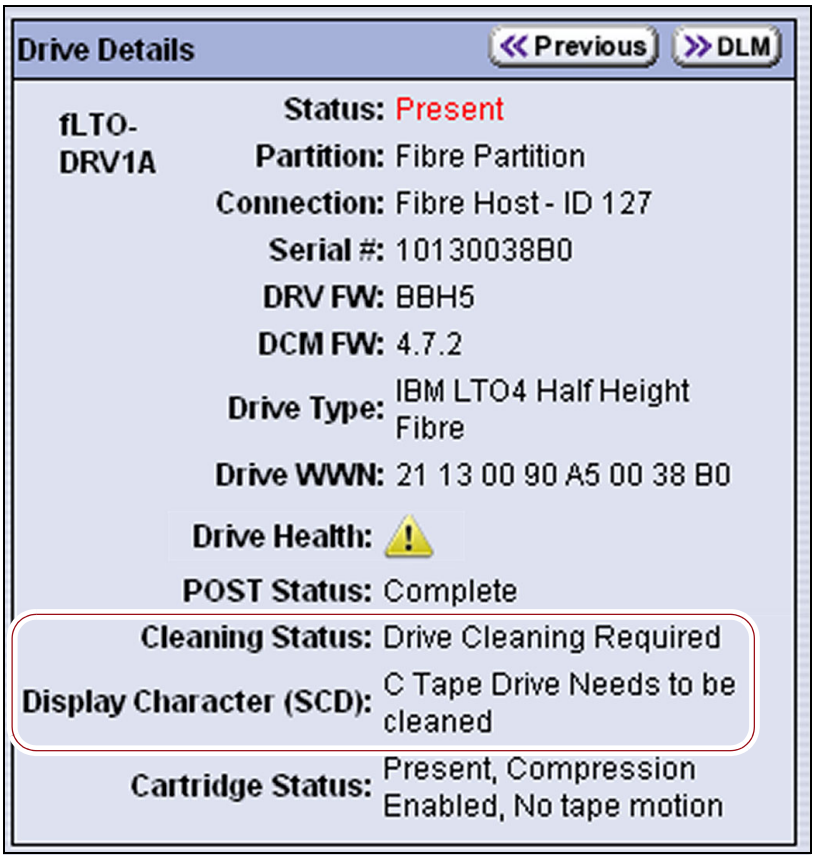


Figure 313 The Drive Details screen shows that cleaning is required.

Prepare the Library for Drive Cleaning

Before you can clean the drive, you must address the following requirements:

Required Tools and Materials You must have a cleaning cartridge for the type of drive(s) to be cleaned. Cleaning cartridges can be purchased from Spectra Logic. If the cartridge has a barcode label, be sure to note the barcode, including any leading zeros. This information helps you locate the cleaning cartridge after it is loaded into the library.

Caution Carefully follow all instructions and recommendations provided with the cleaning cartridge. Do not rewind and reuse the material in a cleaning cartridge. Reusing the material may redistribute contaminants previously removed from the tape path. If all of the cleaning material was used, discard the cartridge and use a new cleaning cartridge.

Important Using only Spectra Certified cleaning cartridges to clean your drives is highly recommended. For information on ordering these cartridges, see Media and Media Accessories on page 493.

Continuing Backups A drive is unavailable for use while it is being cleaned. However, the library's other drives remain available for use.

Determine the Cleaning Method

The method you use to clean the drive depends on the following factors:

If...	Then...
Auto Drive Clean is enabled and a cleaning partition is associated with the storage partition,	The library automatically cleans the drives, including any Global Spares, as needed. See Creating a Cleaning Partition on page 170 for information about configuring a cleaning partition and associating it with one or more storage partitions. You can also clean the drive manually using a cleaning cartridge in the cleaning partition (see Cleaning Partition Present on page 446).
A cleaning partition is not associated with the storage partition; your software package includes features that allow for scheduled drive cleanings,	Use your storage management software to perform regularly scheduled drive cleanings. Refer to your storage management software user manual or vendor for instructions on how to set up scheduled automatic cleanings. You may choose to leave a cleaning cartridge in each storage partition, particularly if you can configure your storage management software to perform regular automated cleanings. **CAUTION:** Make sure that the cleaning cartridge has a barcode label. Your software must be able to identify the cleaning cartridge and use it only for cleaning drives. Any attempts to use a cleaning cartridge for data storage causes backup failures.

If...	Then...
A cleaning partition is not associated with the storage partition and your software package does not have features that allow for scheduled drive cleanings,	Import a cleaning cartridge into the partition and clean the drive manually as described in No Cleaning Partition Present on page 448. You may choose to leave a cleaning cartridge in each storage partition so that it is available whenever you need it. **CAUTION:** Make sure that the cleaning cartridge has a barcode label. Your software must be able to identify the cleaning cartridge and use it only for cleaning drives. Any attempts to use a cleaning cartridge for data storage causes backup failures.
A Global Spare drive requires cleaning and a cleaning partition is not present,	Prepare and clean the drive as follows: **1.** Pause the PostScan operation if it is using the Global Spare drive that needs cleaning (see Pause the PostScan Process on page 261). **2.** Temporarily substitute the Global Spare drive for a drive in a partition that is associated with the Global Spare drive (see Use the Global Spare Drive on page 410). **3.** Clean the drive manually (see No Cleaning Partition Present on page 448). **4.** Reclaim the Global Spare drive so that it is again available for use as a spare (see Undo the Global Spare Drive on page 412).

Manually Cleaning a Drive

The process for loading a cleaning cartridge into the drive depends on whether or not a cleaning partition is associated with the storage partition containing the drive you need to clean.

Cleaning Partition Present

If a cleaning partition is present and contains a cleaning cartridge, you can use the **Clean** feature on the Drives screen to manually clean a drive. See Creating a Cleaning Partition on page 170 for information about configuring a cleaning partition.

1. Log into the library.
2. If necessary, create a move queue to import a cleaning cartridge into the cleaning partition (see Move Cartridges Within a Partition on page 226).

3. Click **MENU**, the select **Configuration** ···⁘ **DLM** (or **Drives** if MLM is not enabled). The Drives screen displays.

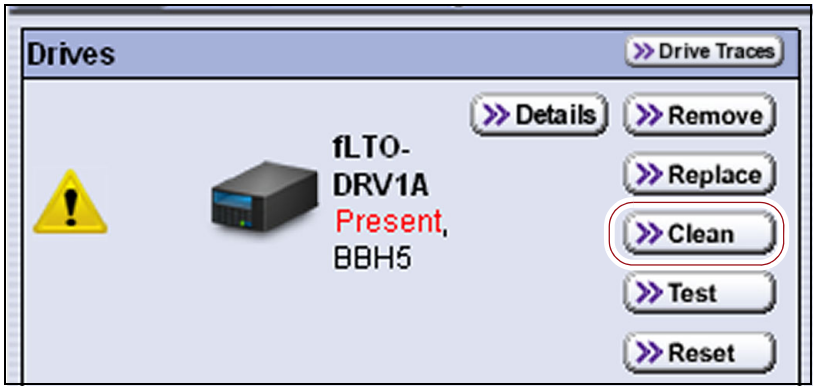


Figure 314 Click **Clean** on the Drives screen.

4. Click **Clean** next to the drive that needs cleaning. The library retrieves a cleaning cartridge from the cleaning partition and inserts it into the drive. The Drive Cleaning Progress screen displays while the cleaning is in progress.
5. When the cleaning is complete, the library returns the cleaning cartridge to the cleaning partition and displays a status message.

   If the cleaning cartridge is MLM-enabled, the cartridge health and Cleans Remaining are updated in the MLM database.
6. Check the Drive Details screen to confirm that the cleaning was successful.

   If the cleaning cartridge is expired, the drive automatically ejects the cartridge and does not perform the cleaning. The Drive Details screen still indicates that the drive needs cleaning. If a drive still needs cleaning, perform the following steps:

   a. Export the expired cleaning cartridge.

   b. Import an unexpired cleaning cartridge.

   c. Repeat Step 3 on page 448 through Step 6 on this page to clean the drive.
7. If you have additional drives to clean, repeat Step 3 on page 447 through Step 6 on this page for each drive.

No Cleaning Partition Present

If a cleaning partition is not associated with the storage partition containing the drive you need to clean, a cleaning cartridge must be present in the storage partition.

Use the following steps to clean the drive.

1. Log into the library.

   Note: You must be logged in as a superuser or administrator in order to import a cartridge into the partition.

2. If a cleaning cartridge is not stored in the storage partition, import one into the storage partition containing the drive that needs cleaning.

   - If there is an empty slot in the storage partition, create a move queue to move a cleaning cartridge from the access port to the empty slot in the partition (see Move Cartridges Within a Partition on page 226).

     —OR—

   - If there is not an empty slot in the storage partition, create a move queue to move a data cartridge to the access port. Exchange the data cartridge for a cleaning cartridge and then move the cleaning cartridge to the slot vacated by the data cartridge.

3. Use the cleaning cartridge barcode label information to determine its location, as described in Locate a Specific Cartridge on page 225.

4. Create a move queue to move the cleaning cartridge from the slot where it is stored to the drive that needs cleaning (see Move Cartridges Within a Partition on page 226).

   The drive automatically performs the cleaning, which takes approximately one minute, and ejects the cartridge when finished.

5. Create a move queue to move the cleaning cartridge from the drive back to the slot from which it came.

6. Check the Drive Details screen to confirm that the cleaning was successful.

   If the cleaning cartridge was expired before the cleaning started, the drive automatically ejects the cartridge and does not perform the cleaning. The Drive Details screen still indicates that the drive needs cleaning. Perform the following steps:

   a. Export the expired cleaning cartridge.

   b. Import an unexpired cleaning cartridge.

   c. Repeat Step 3 on page 448 through Step 6 on this page to clean the drive.

7. If you have additional drives to clean, repeat Step 3 on page 448 through Step 6 on this page for each drive.
8. If you do not want to store the cleaning cartridge in the library, create a move queue to move the cleaning cartridge to the access port and, if necessary, exchange it for the data cartridge you exported in Step 2 on page 448.
9. Make sure that you track the number of times the cleaning cartridge is used (see Track Cleaning Cartridge Use on page 449).

   Note: If you used an MLM-enabled LTO cleaning cartridge, the cartridge usage is tracked in the MLM database.

Track Cleaning Cartridge Use

Cleaning cartridges have a limited number of uses. Spectra Logic recommends marking the cleaning cartridge label after each use so that you know when it reaches the end of its life cycle.

If you enabled Media Lifecycle Management (MLM) and use MLM-enabled cleaning cartridges, the library tracks the number of cleanings remaining on the cartridge and notifies you when a cleaning cartridge is nearing the end of its useful life. See Chapter 8 – Configuring and Using Media Lifecycle Management, beginning on page 233 for detailed information about using MLM-enabled cleaning cartridges.

To purchase MLM-enabled Spectra Certified cleaning cartridges, contact your sales representative or visit the Spectra Logic website at www.spectralogic.com/shop.

UPDATING DRIVE FIRMWARE

Overview Whenever you update your library firmware, confirm that your drives are using the correct firmware version. Drive firmware updates are also occasionally required to resolve drive issues. When updated drive firmware is available, schedule a drive firmware update at your earliest convenience.

The method you use to update the drives depends on the type of drives you are updating and your operating environment.

Note: If you cannot use any of the methods described in the following sections, contact Spectra Logic Technical Support for assistance (see Contacting Spectra Logic on page 7).

	Suggested Use
IBM Tape Diagnostic Tool (ITDT) To use, install the ITDT utility on a Solaris, Linux, or Windows host connected to the drives to be updated. The update takes 1-2 minutes per drive.	Recommended
Update Drive Firmware Utility Requires a firmware update tape at the latest firmware level. The update takes about 5 minutes per drive. Updates are performed serially.	Available
Drive Update through Package Update	Not Recommended [a]

a. Contact Technical Support before using this wizard to update LTO-2 through LTO-4 drives. These drives must remain empty and idle during the update, which may take up to 8 hours per drive.

User Privilege Requirements The user privileges required to perform a drive firmware update depend on the method used.

- **ITDT** — Any user with permissions to use the host computer on which ITDT is installed.
- **Drive Update Firmware utility** — Only a user with superuser or administrator privileges.

Important Always download drive firmware from the Spectra Logic Technical Support portal to ensure that the latest firmware posted by the drive manufacturer was qualified by Spectra Logic.

Important After the drive firmware update is complete, you may need to reset the hosts accessing the drives.

Important Some operating environments require you to install device drivers before the application software can correctly communicate with the drives. When you update the drive firmware, you may also need to update the device driver for the drive (see Updating Drive Device Drivers on page 462 for further instructions).

Important DO NOT downgrade the firmware on a drive unless specifically instructed to do so by Spectra Logic Technical Support.

Important If you update an LTO-5 drive to firmware level D2A0, you may need to manually reboot the drive at the end of the update process. If you update multiple drives, you can save time by rebooting the library instead of each individual drive.

Prepare for the Update Process

Before you begin the update procedure, make sure you fulfill the prerequisites described in this section.

Determine the Drive Generation and Firmware Version

Use the following steps to determine the generation and current firmware version for each drive you plan to update.

1. Log into the library as a user with superuser or administrator privileges.
2. Click **MENU**, then select **Configuration** ···⁘ **DLM** (or **Drives** if DLM is not enabled) to display the Drives screen.
3. For each drive, click **Detail** to display the Drive Details screen.

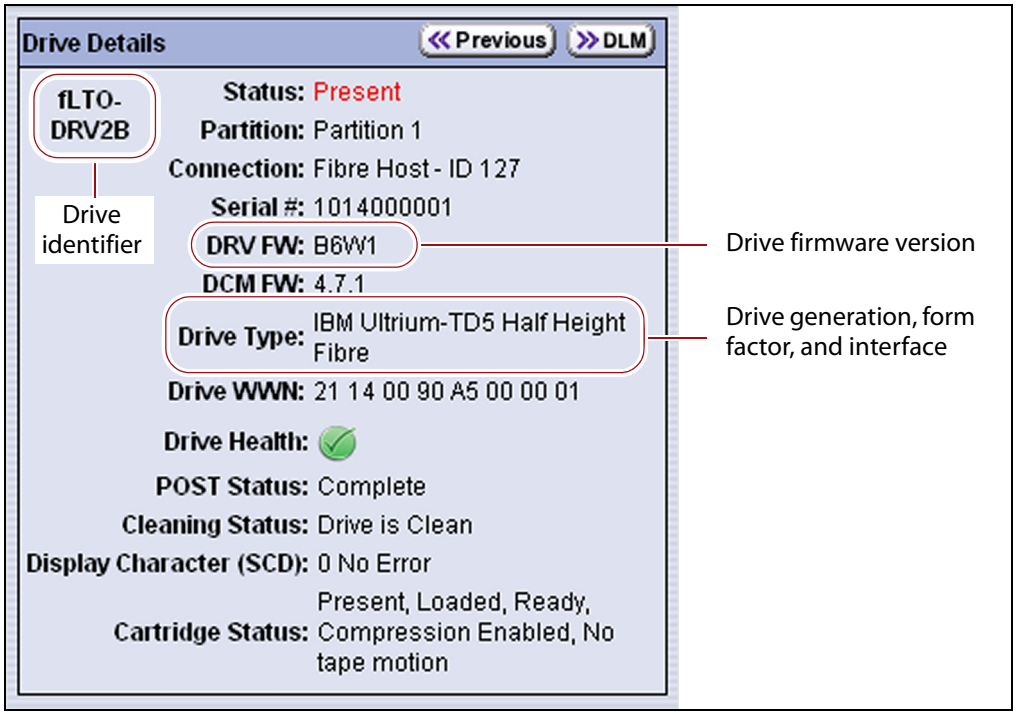


Figure 315 Determine the drive generation, form factor, and interface.

4. Make a note of the following information for each drive you need to update:
   - **Drive firmware version**—The firmware version the drive is currently using
   - **Drive type and generation**—LTO (listed as IBM Ultrium-TD*n*, where *n* is the generation)
   - **Drive form factor**—Full-height or half-height
   - **Interface**—Shown in both the Drive Type field and in the Drive Identifier field. See BlueScale Drive Identifiers on page 154 for detailed information about drive identifiers.

Determine Whether an Update is Available

Use the Spectra Logic Technical Support portal to check the currently recommended firmware version for the drives in your library and download updated firmware if it is available.

Important Always download drive firmware from the Spectra Logic Technical Support portal to ensure that the latest firmware posted by the drive manufacturer was qualified by Spectra Logic.

1. Log into your account on the Technical Support portal at support.spectralogic.com.

   Note: See Accessing the Technical Support Portal on page 472 for information about accessing the Technical Support portal and setting up an account associated with your library.

2. Select **Downloads ⋯ Tape Drive Firmware**.

3. On the Tape Drive Firmware page, locate the appropriate drive firmware with respect to drive type (LTO) and generation (for example, LTO-4) and then interface type (for example, SCSI or Fibre) and form factor (full-height or half-height).

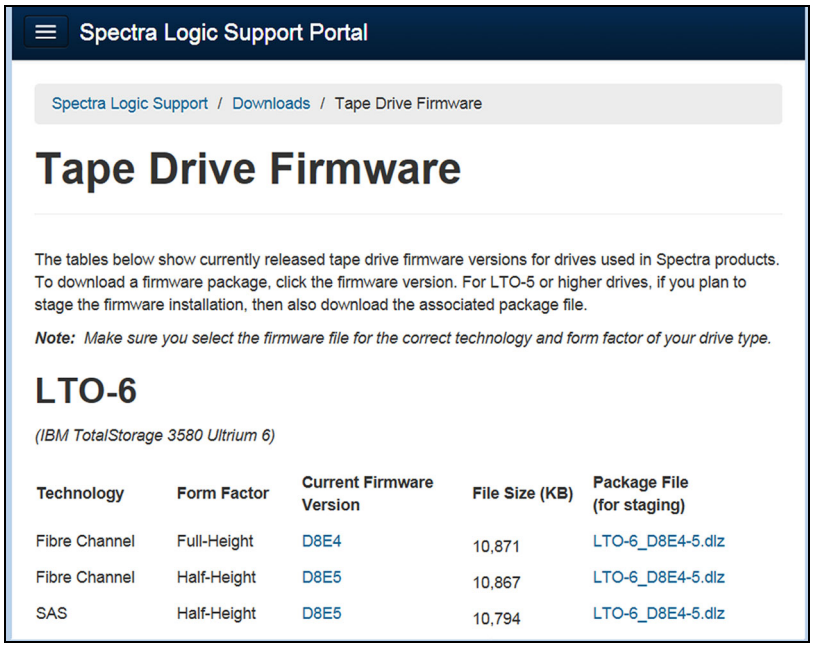


Figure 316 A portion of the Tape Drive Firmware page.

4. Compare the recommended drive firmware version for each of the drives in your library with the version currently in use (see Determine the Drive Generation and Firmware Version on page 451).

Updating Using ITDT

The easiest way to update your LTO tape drive firmware is with the IBM Tape Diagnostic Tool (ITDT).

Note: If your operating system is not supported by ITDT or you cannot use ITDT in your environment, proceed to Updating Using the Update Drive Firmware Utility on page 455.

After you check the firmware on the Technical Support portal for the currently recommended firmware version (see Determine Whether an Update is Available on page 452), follow the instructions in this section to update your drive firmware using ITDT.

Download and Install ITDT

Download ITDT and its related documentation directly from IBM's Fix Central website. For information about navigating IBM's website and downloading the version of ITDT that is appropriate for your operating system, log on to the portal (see Accessing the Technical Support Portal on page 472), open the Knowledge Base, and search for KBA-01768, *Downloading and installing ITDT (IBM Tape Diagnostic Tool)*.

Important Use the latest version of ITDT to update the latest generation of drives.

Use the following steps to download and install ITDT on a computer that is connected to the same Fibre Channel arbitrated loop or fabric as the drives in the library.

1. Log into IBM's website at http://www.ibm.com/support/fixcentral, using your individual IBM ID.
2. Select the following options:
   - **Product Group** = System Storage
   - **Select from System Storage** = Tape systems
   - **Select from Tape Systems** = Tape drivers and software
   - **Select from Tape drivers and software** = IBM Tape Diagnostic Tool (ITDT)
   - **Platform** = Select your operating system from the drop-down list and click **Continue**.
3. On the next page, select the version of ITDT that you want to download. If desired, you can select multiple versions.

   Note: If you are unsure which version to select, click **Show Fix Details** to see additional information.
4. Click **Continue.** If you are not logged into the website yet, you are prompted to do so now.

5. Choose one of the following methods to download the selected ITDT installation files:
   - **Download using your browser (HTTP)**
   - **Download using bulk FTP**
   - **Download using Download Director**
6. Refer to the ITDT documentation for information about using ITDT. Contact Spectra Logic Technical Support if you need assistance (see Contacting Spectra Logic on page 7).

Download the Drive Firmware

1. After ITDT is installed, launch the program so that it creates the **Input** and **Output** folders required during the firmware update process.
2. Log into your account on the Spectra Logic Technical Support portal at support.spectralogic.com.
3. Select **Downloads ⋯⁘ Tape Drive Firmware**.
4. On the Tape Drive Firmware page (see Figure 316 on page 452), locate the appropriate drive firmware considering drive type (LTO) and generation (for example, LTO-4) and then interface type (for example, SCSI or Fibre) and form factor (full-height or half-height).
5. Click the firmware version name in the column labeled **Current Firmware Version**.

   Note: The link in the column labeled **Package File (For Staging)** is for using Package Update to update the drive firmware. This is not supported on the T50e. Do not select this file.
6. Use your web browser to save the file to the ITDT **Input** folder on the computer where ITDT is installed.

Discontinue Background Operations

You cannot update drive firmware if the library is actively running any background operations, including Media Auto Discovery, PreScan, and PostScan.

If you do not want to wait for a Media Auto Discovery, PreScan, or PostScan operation to complete, you can stop the Media Auto Discovery or PreScan operation or pause the PostScan operation. For other background operations, wait for the process to complete.

- Click **Stop Discovery** on the Media Lifecycle Management Tools screen to stop a Media Auto Discovery or PreScan operation.
- Click **Pause PostScan** on the Media Lifecycle Management Tools screen to pause the PostScan operation for one hour.

Discontinue Backups and Empty the Drives

Before beginning the drive firmware update process, discontinue all backup operations and remove any cartridges from the drives.

Caution Attempting to update the firmware while the library is busy or when the drives contain tapes may result in the update failing, failed backup jobs, or permanent damage to the drives. If you have not already done so, stop all backup operations and remove all tapes from the drives you are updating.

- If possible, use your storage management software to move any cartridges that are currently in drives back to their storage locations.
- If you cannot use your storage management software, then move the cartridges as described in Move Cartridges Within a Partition on page 226.

Update Drives Using ITDT

1. Follow the instructions in the ITDT documentation to update the drive firmware.
2. Reset the updated drives to restore their configuration settings.
3. After the update is complete, use your storage management software to restart any backup processes.

Updating Using the Update Drive Firmware Utility

The advanced Update Drive Firmware utility uses a firmware update tape to update one drive at a time while you wait.

Requirements

- The drives to be updated must be configured in a storage partition.
- The firmware update tape must be stored in the E/E slot.
- The drives are updated one partition at a time.
- To update the firmware of a Global Spare, first substitute the Global Spare drive for a drive assigned to a partition. After the Global Spare drive completes the firmware update process, it can be removed from the partition and returned to the pool of spare drives (see Use the Global Spare Drive on page 410 for more information).

Discontinue Background Operations

You cannot update drive firmware if the library is actively running any background operations, including Media Auto Discovery, PreScan, and PostScan.

If you do not want to wait for a Media Auto Discovery, PreScan, or PostScan operation to complete, you can stop the Media Auto Discovery or PreScan operation or pause the PostScan operation. For other background operations, wait for the process to complete.

- Click **Stop Discovery** on the Media Lifecycle Management Tools screen to stop a Media Auto Discovery or PreScan operation.
- Click **Pause PostScan** on the Media Lifecycle Management Tools screen to pause the PostScan operation for one hour.

Discontinue Backups and Empty the Drives

Before beginning the drive firmware update process, discontinue all backup operations and remove any cartridges from the drives.

Caution

Attempting to update the firmware while the library is busy or when the drives contain tapes may result in the update failing, failed backup jobs, or permanent damage to the drives. If you have not already done so, stop all backup operations and remove all tapes from the drives you are upgrading.

- If possible, use your storage management software to move any cartridges that are currently in drives back to their storage locations.
- If you cannot use your storage management software, then move the cartridges as described in Move Cartridges Within a Partition on page 226.

Import the Firmware Update Tape

1. Log into the library as a user with superuser or administrator privileges.
2. Click **MENU**, then select **General** ⋯ **Import/Export**. The Import/Export screen displays showing information for the last partition that was viewed on either the Import/Export screen or the Inventory screen.

3. Select the partition you want to use from the drop-down list, then click **Go**. The Import/Export screen refreshes to show the current status of the slots assigned to the selected partition.

   Note: If the library only has one partition configured, the Import/Export screen shows that partition and does not include a drop-down list.

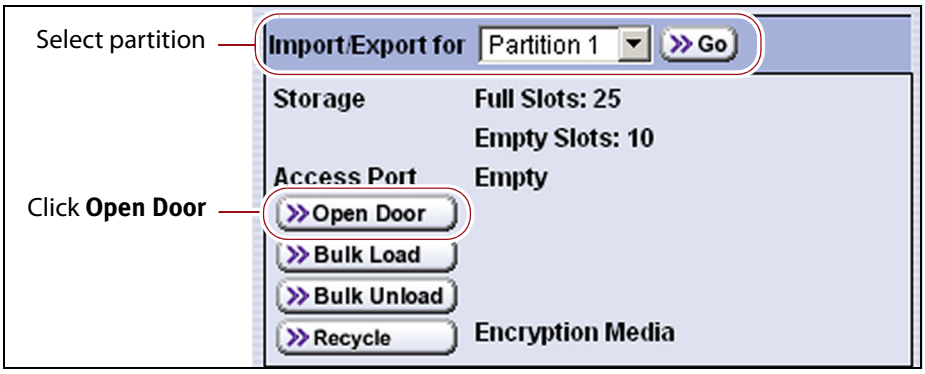


Figure 317 Select the partition and then click **Open Door** to open the access port.

4. Click **Open Door**. A progress screen displays describing the process.
5. When the access port opens, insert the cartridge into the E/E slot, smooth side up and with the barcode label facing out. Push the cartridge into the slot until the latch on the slot engages the ridges on the cartridge.

Important The slot is keyed to only accept a correctly oriented cartridge. Do not force the cartridge into the slot.

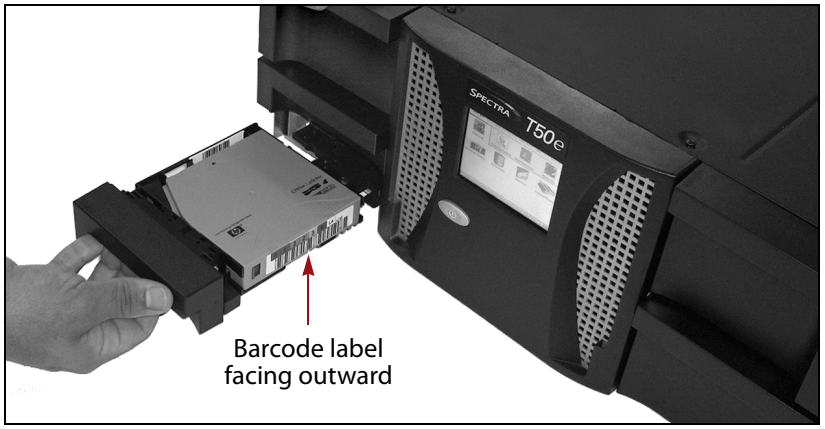


Figure 318 Insert the cartridge into the E/E slot.

6. Wait for a message prompting you to close the access port.
7. Gently push the access port closed.

Important Do not use force to push the access port closed, and do not close the port before you are prompted to do so.

Perform the Update

1. If you want to save the information about the firmware versions to a USB device, connect a USB device to a USB port on the LCM and allow time for the device to mount.

   Note: The option to save the information to a USB device is only displayed if you plug a USB device into the LCM before you select **Utilities** (see Using a USB Device on page 152).

2. Click **MENU**, then select **Maintenance** ···⁘ **Utilities** to display the Utilities screen.

3. Click **Show Advanced**. The Advanced Utilities Confirmation screen displays.

4. Click **Yes** to acknowledge the warning about using the advanced utilities. The Advanced Utilities screen displays a list of the advanced utilities.

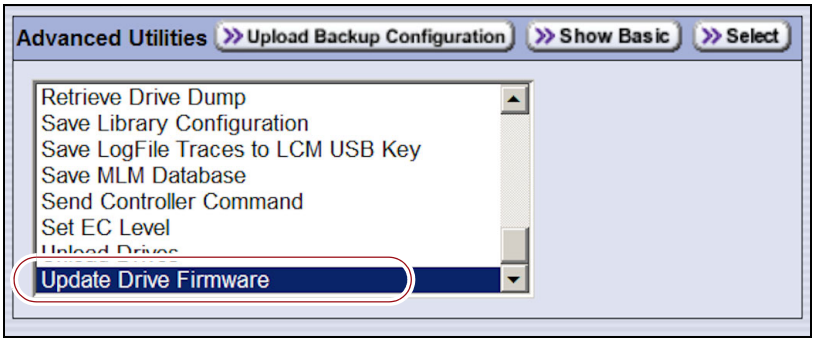


Figure 319 Select the **Update Drive Firmware** utility.

5. Scroll through the list of advanced utilities and select **Update Drive Firmware**.

6. Click **Select**. The Description screen shows a description of the utility.

7. Click **Next** and use the **Select drive or partition to upgrade** list to select the drives you want to update.

   Note: Do not select a cleaning partition if one is listed. There are no drives associated with a cleaning partition.

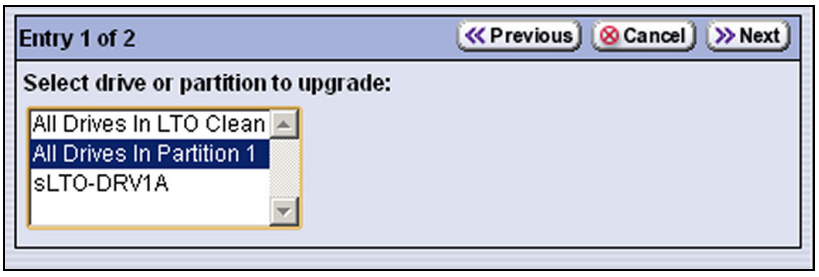


Figure 320 Select the drive or partition that you want to update.

8. Click **Next** and use the **Select EE slot of the firmware tape** drop-down list to select the firmware update tape in the E/E slot.

Figure 321 Select the cartridge in the E/E slot.

9. Click **Next**. The Destinations screen displays.

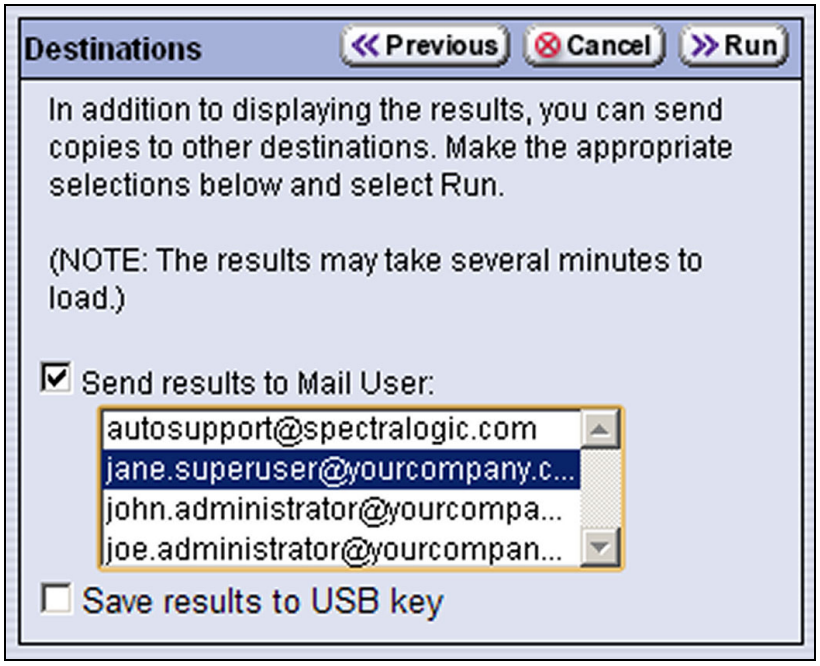


Figure 322 Select other destinations for the results of the firmware update.

10. If you want to save the output from the utility, use the check boxes on the Destination screen to select the location; otherwise skip to Step 11 on page 460.

Selecting this option...	Saves the results file...
Send results to Mail User	As an attachment to an email sent to the specified mail recipient. Use the drop-down list to select the recipient for the report file. Only previously configured mail recipients are listed. To send the email with the attached trace file to someone who is not listed, exit the utility, configure that person as a mail user (see Configure Mail Users on page 107), and then run the utility again. **Note:** Do not select autosupport@spectralogic.com as a recipient unless Spectra Logic Technical Support specifically instructs you to results file to them. Spectra Logic does not save emailed files unless they are specifically requested for troubleshooting.
Save results to USB key	To a USB device connected to the USB port on the LCM. **Note:** This option is only available if you inserted a USB device in Step 1 on page 458.

11. Click **Run** to start the update process.

- The library retrieves the firmware tape and inserts it into the drive. When the drive completes the update, it ejects the tape. The library then either returns the tape to the E/E slot or inserts it in the next drive to be updated.
- A progress screen displays for the duration of the update, which may take several minutes. When completed, a Utility Results screen displays, showing that the update completed successfully.

Important

- Once the firmware update process starts, it cannot be canceled.
- Do not power off the library or any component being updated during the firmware update process.
- If you use the wrong firmware tape or try to update a drive that is not compatible with the firmware tape, the update operation fails.

12. Repeat the steps for all drives in all partitions, as needed.

Export the Firmware Tape from the Library

Follow these steps to export the tape from the library:

1. Click **MENU**, then select **General** ···⁘ **Import/Export**. The Import/Export screen displays showing information for the last partition that was viewed on either the Import/Export screen or the Inventory screen.
2. If necessary, select the partition from the drop-down list, then click **Go**.
3. Click **Open Door**. A progress screen displays describing the process.

4. When the access port opens, insert a finger through the opening in the back of the access port and carefully push the cartridge out of the E/E slot.

Caution Be careful not to drop or jar the cartridge when you remove it. Mishandling cartridges can result in failures when you attempt to use the cartridge.

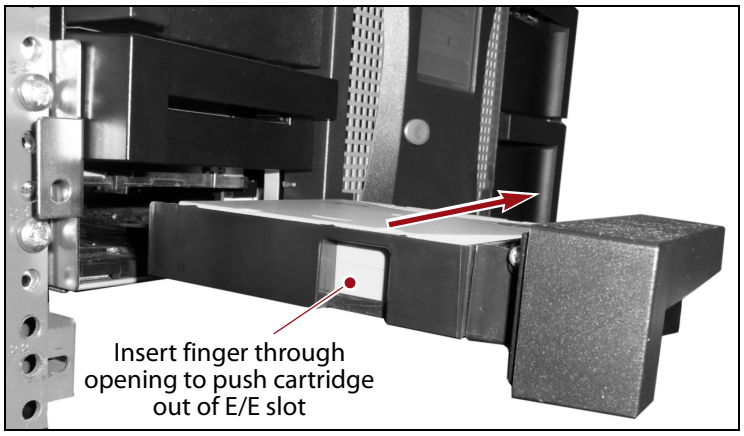


Figure 323 Remove the cartridge from the E/E slot.

5. Wait for a message prompting you to close the access port.
6. Gently push the access port closed.

Important Do not use force to push the access port closed, and do not close the port before you are prompted to do so.

7. After the update is complete, use your storage management software to restart any backup processes.

Store the Firmware Update Tape for Future Use

After exporting the firmware update tape, store it for future use. You can use it to update the firmware in a replacement drive if it is at a lower firmware level.

Important If you have a tape drive with a more current firmware version than what is on the firmware tape DO NOT use the tape to down-level the firmware on the tape drive unless specifically instructed to do so by Spectra Logic Technical Support.

UPDATING DRIVE DEVICE DRIVERS

Overview Some operating environments require you to install device drivers before the application software can correctly communicate with the drives. When you update the drive firmware, you may also need to update the device driver for the drive.

Use the following instructions to locate and download the IBM LTO drive device driver on the IBM Support Fix Central website.

Notes:
- You must have an IBM account to log in and download the drivers.
- You can connect to the Fix Central website either from the Spectra Logic Technical Support portal or directly at http://www.ibm.com/support/fixcentral. If you connect directly, skip to Step 4 in the following instructions.

1. Log into your account on the Technical Support portal at support.spectralogic.com

   Note: See Accessing the Technical Support Portal on page 472 for information about accessing the Technical Support portal.

2. Select **Downloads ⋯⁘ Device Drivers**.
3. On the Device Drivers page, click **IBM LTO-2, LTO-3, and LTO-4, LTO-5, LTO-6, and LTO-7 (IBM TotalStorage 3580 Ultrium 2, 3, 4, 5, 6, and 7)** to open IBM Fix Central in a new web page.
4. Click the **Select Product** tab.
5. Select the following options:
   - **Product Group** = System Storage
   - **Select from System Storage** = Tape systems
   - **Select from Tape Systems** = Tape drivers and software
   - **Select from Tape drivers and software** = Tape device drivers
   - **Platform** = Select your operating system from the drop-down list and click **Continue**.
6. Click **Continue** to display a list of the available drivers on the Select fixes page.
7. Click **Show Fix Details** to view information about each driver.
8. Select the driver you want to download and click **Continue**. If required by your IT department, select the WHQL certified driver, if available.
9. Complete the remaining pages to begin the download process.
10. Save the file containing the driver to a known location on the server that is using the drive.
11. Install the device driver following the instructions in the documentation for your operating environment.

ADDING OR REPLACING A DRIVE

Important Only use tape drives obtained from Spectra Logic in the library. When replacing a drive that is assigned to a partition, the new drive must be the same technology and generation as the one you replace.

Prepare the Library and the Host Computer

Before adding or replacing a drive, make sure you address the requirements in the following sections.

Discontinue Backups

If you are replacing or removing an existing drive, discontinue backup or restore operations as required.

Fibre Channel or SAS drives Backups running to other drives in the library (or partition) can safely continue while you replace a drive, as long as that drive is not the one exporting the library (that is, providing the robotic control path for the partition). If the malfunctioning drive is the exporting drive for the partition, stop backup or restore operations to the partition.

SCSI drives If you plan to power-off the host before installing or replacing a SCSI drive, stop backup or restore operations to all of the drives connected to the host. If you choose not to power-off the host, the requirement to stop backup or restore operations depends on how the drive is connected and configured in the library.

- **Exporting drive**—If the drive that you are replacing is the exporting drive for the partition, stop backup or restore operations to all of the drives in the partition before removing the drive.
- **LTO-3 or LTO-4 drive is not daisy-chained**—If the drive is not the exporting drive and is not daisy-chained with another drive, operations to the other drives can continue.
- **Two drives daisy-chained (LTO-3 only)**—If two SCSI drives are daisy-chained on the same SCSI bus, removing a drive in the chain interrupts communications on the bus. Before removing a drive, stop backup or restore operations to both of the drives in the daisy chain.

Power-Off the SCSI Host

Spectra Logic recommends that you shut down and power-off the host before installing or replacing a SCSI drive; this is not required for Fibre Channel or SAS drives.

Caution Improperly adding or removing a device from a SCSI bus can cause the host computer to crash. If you leave the host running during this procedure, Spectra Logic assumes no responsibility for damage to data or equipment.

Ensure ESD Protection

The environment for the library must be free of conditions that could cause electrostatic discharge (ESD). To protect the library from ESD, follow these procedures:

- Place a static protection mat on the work surface used while removing and installing library components. Use a 1-megohm resistor to ground the static protection mat.
- Wear a static protection wrist band whenever you handle library components that are removed from their antistatic bags. Connect this wrist band to the static protection mat or to other suitable ESD grounding.
- Keep all components in antistatic bags when not in use.

Add a Drive to the Library

If your library has unused drive bays, you can purchase additional drives from Spectra Logic and add them to the library.

Important Adding drives to an existing partition can cause the library to reassign element addresses. To avoid errors, make sure that when you install a new drive, you reconfigure the element addresses your storage management software uses to access the drives (refer to your software documentation for instructions).

Install the New Drive

1. Log into the library as either a superuser or administrator.
2. Click **MENU**, then select **Configuration** ⋯ **DLM** (or **Drives** if DLM is not enabled) to view a list of all the drives currently installed in the library.

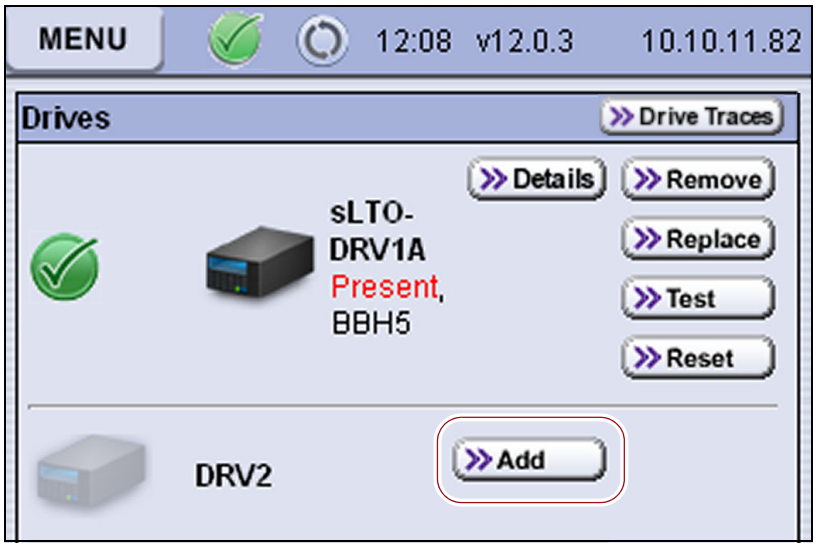


Figure 324 Click **Add** next to the identifier for the drive bay where you plan to install the new drive.

3. Click **Add** next to a drive location that does not have a drive installed.

   Note: See Identify the Drives in the Library on page 154 to determine the physical location that corresponds to the BlueScale drive bay identifier.

4. A Feedback Required screen prompts you to confirm that you want to add the drive. Click **OK**.

5. Watch the front panel for a Feedback Required screen indicating that the library is ready for the drive to be installed.

Important Do not respond to the prompt in the Feedback Required screen or perform any other operations from the user interface (either locally or remotely) until you complete the installation procedure.

6. Install the new tape drive in the unused drive bay you selected in Step 2 (see Install the Tape Drives on page 54).

7. Connect the appropriate interface cable (SCSI, Fibre Channel, or SAS) to the drive (see Connect the Tape Drives to the Host on page 56).

   Note: If you installed a SCSI drive, install a SCSI terminator if the drive is the last SCSI device on the SCSI bus. Fibre Channel and SAS drives do not require termination.

8. After you install the drive, return to the Feedback Required screen displayed on the user interface (see Step 5 on page 465) and click **OK**.

   The library powers on the new drive and begins the process of configuring it. A progress screen displays information about the process. When the configuration is complete, the Drives screen displays showing that the new drive is present in the library.

9. You must create a new partition or modify an existing partition to use the new drive before you can use it. You can also configure it as a Global Spare drive. See Chapter 6 – Configuring and Managing Partitions, beginning on page 159 for information about creating and modifying partitions.

Test the New Drive

After installing the new drive, use the following steps to confirm that the host can communicate with it.

1. Use the library to move a tape to the drive and then eject it to make sure that the newly installed tape drive is functioning properly.

2. Power on the host computer, if you powered it off.

3. Make sure that your operating system sees the tape drive and robotics for the library before proceeding.

4. Determine whether your storage management software and tape drive are communicating properly by using the software to back up several megabytes of data to the tape drive. Perform a comparison check on the backup data to confirm that it was written correctly.

Replace a Drive

Use the following steps to replace a drive assigned to a partition with a new one.

Important When replacing a drive that is assigned to a partition, the replacement drive must have the same interface as the drive you are replacing. If the replacement drive is a different technology generation, make sure that it is compatible with the data cartridges used in the library. See LTO Read/Write Compatibility on page 513.

1. Prepare the library and host for the drive replacement (see Prepare the Library and the Host Computer on page 463).
2. Log into the library as either a superuser or administrator.
3. If the drive you are replacing contains a cartridge, use your storage management software to move the cartridge back to its storage location.

   If you cannot use your storage management software, then move the cartridge to a slot as described in Move Cartridges Within a Partition on page 226.

   Note: Continue with the replacement process even if you are unable to move the cartridge from the drive.
4. Click **MENU**, then select **Configuration** ⋯ **DLM** (or **Drives** if DLM is not enabled) to view a list of all the drives currently installed in the library.

Figure 325 Click **Replace** next to the drive you need to replace.

5. Click **Replace** next to the drive that you need to replace.

   A Feedback Required screen prompts you to confirm that you want to replace the drive.

Important *Do not select* **Remove**. This option removes the drive from the partition. When the replacement drive is installed, it is not assigned to the partition from which the malfunctioning drive was removed.

If you select **Remove** and the selected drive is the only drive in the partition, the partition is deleted.

6. Click **OK**. Wait for the library to power off the drive.
7. Watch the front panel for a Feedback Required screen indicating that the drive was successfully shut down.

Important Do not respond to the prompt in the Feedback Required screen or perform any other operations from the user interface (either locally or remotely) until you complete the replacement procedure. If you respond before you replace the drive, the drive you just powered down powers on and configures itself.

8. Replace the drive.
   a. Access the back of the library and identify the drive you need to remove.

   Note: See Identify the Drives in the Library on page 154 to determine the physical location that corresponds to the drive identifier for the drive you are replacing.

   b. If the drive has two interface connectors, make a note of the connecter to which the interface cable is connected. You must use the same connector when you connect the new drive.
   c. Disconnect the interface cable from the drive.

   Note: If you are replacing a SCSI drive that has a terminator installed, remove the terminator and set it aside to be installed on the new drive.

   d. Using your fingers or a #2 Phillips screwdriver, loosen the captive screws that secure the drive sled to the chassis.

   Note: The half-height drive has two captive screws and the full-height drive has four captive screws.

e. While supporting the drive with both hands, use the handle to slide the drive out of the library. Set the drive aside to return to Spectra Logic.

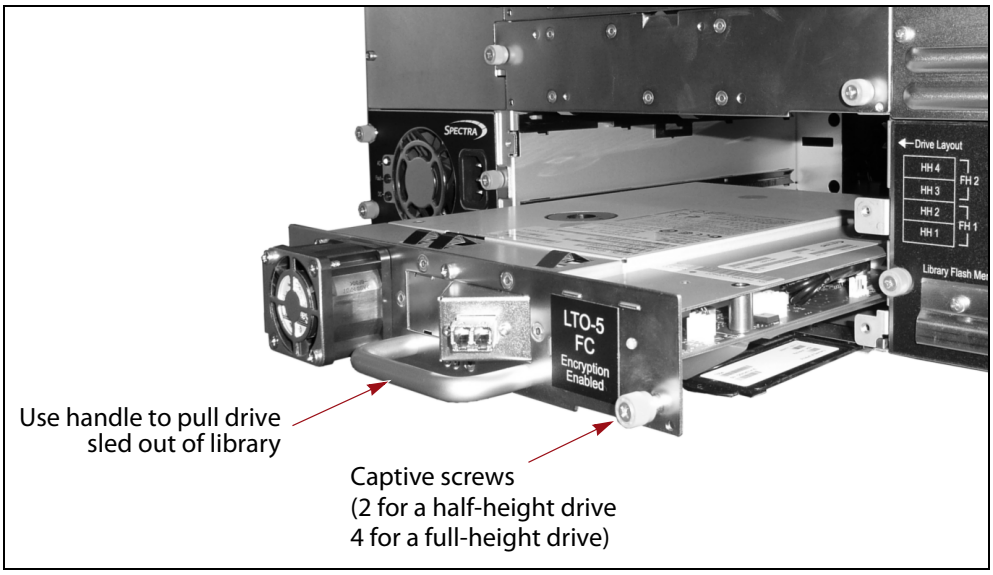


Figure 326 Use the handle to pull the drive out of the drive bay.

f. Remove the replacement drive from its packaging and install it in the vacated drive bay (see Installing the Tape Drives on page 52).

Note: Keep the packaging to be used when returning the failed drive to Spectra Logic.

g. Connect the cable that you removed from the malfunctioning drive to the new drive. Make sure that you connect it to the same interface connector that was used on the drive you removed.

Important Make sure that you connect the cable to the SAME location that was used on the drive you removed. Connecting the cable to the other connector may prevent the host system from recognizing the new drive.

Important Wait for several minutes for the drive to initialize. Pushing any other buttons on the front panel before initialization completes causes an error.

Note: If you installed a SCSI drive, install a SCSI terminator if the drive is the last SCSI device on the SCSI bus.

9. After you install the new drive, return to the Feedback Required screen displayed on the user interface (see Step 7 on page 467) and click **OK**.

The library powers on the new drive and begins the process of configuring it. A progress screen displays information about the process. When the configuration is complete, the Drives screen displays showing the new drive functioning in the old drive's location. The new drive assumes the old drive's configuration, so it can be used immediately.

10. After you replace the drive, do the following to resume operation:
    - If you used the Global Spare option to temporarily replace the malfunctioning drive, you can now reclaim the Global Spare drive so that it is again available for use (see Undo the Global Spare Drive on page 412). The library automatically switches all incoming communications to the new drive.
    - If you did not use the Global Spare option, use your storage management software to restart any backup processes that were running to the replaced drive. This restart ensures that the software recognizes the drive as working and available.
11. Package the malfunctioning drive and ship it to Spectra Logic (see Returns on page 479).
12. Test the drive to confirm that the host can communicate with it (see Test the New Drive on page 465).

Removing a Drive from the Library

Use the following to permanently remove drive from the library.

Important If you select **Remove** and the selected drive is the only drive in the partition, the partition is deleted.

1. Prepare the library and the hosts for the removal (see Prepare the Library and the Host Computer on page 463).
2. If the drive you are removing contains a cartridge, use your storage management software to move the cartridge back to its storage location.

   If you cannot use your storage management software, then move the cartridge to a slot as described in Move Cartridges Within a Partition on page 226.

   Note: Continue with the replacement process even if you are unable to move the cartridge from the drive.

3. Click **MENU**, then select **Configuration** ···⁘ **DLM** (or **Drives** if DLM is not enabled) to view a list of all the drives currently installed in the library.

Figure 327 Click **Remove** next to the drive you want to permanently remove from the library.

4. Click **Remove** next to the drive that you want to permanently remove from the library.

   A Feedback Required screen prompts you to confirm that you want to remove the drive.

5. Click **OK**. Wait for the library to power off the drive.

6. Watch the front panel for a Feedback Required screen indicating that the drive was successfully shut down.

Important

Do not respond to the prompt in the Feedback Required screen or perform any other operations from the user interface (either locally or remotely) until you complete the removal procedure. If you respond before you remove the drive the drive you just powered down powers on and configures itself.

7. Remove the drive.

   a. Access the back of the library and identify the drive you need to remove.

   Note: See Identify the Drives in the Library on page 154 to determine the physical location that corresponds to the drive identifier for the drive you are removing.

   b. Disconnect the interface cable and the SCSI terminator, if one is installed, from the drive.

   c. Loosen the captive screws securing the drive sled to the library chassis, grasp the handle, and pull the drive straight out of the library while supporting it with both hands (see Figure 326 on page 468).

d. If you do not plan to install a new drive, install the drive bay cover you removed when you originally installed the drive over the empty drive bay.

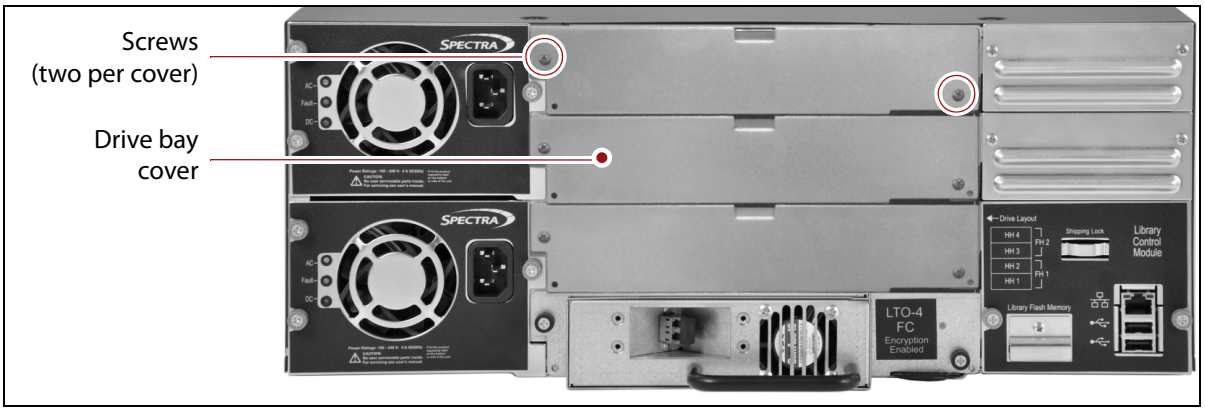


Figure 328 Install the drive bay cover over the empty drive bay.

Important Do not leave any openings uncovered. All openings must be covered for safety and for proper library cooling.

8. After you remove the drive, return to the Feedback Required screen displayed on the user interface (see Step 6 on page 470) and click **OK**.

9. The Drives screen redisplays to show that the drive is no longer present.

10. Package the malfunctioning drive and return it to Spectra Logic, as described in Returns on page 479.

CHAPTER 16

Technical Support

Spectra Logic Technical Support provides a worldwide service and maintenance structure, refined over many years to provide timely, professional service.

Important A valid warranty or support contract is required in order to obtain technical support (see Service Contract Extension on page 495).

ACCESSING THE TECHNICAL SUPPORT PORTAL

The Spectra Logic Technical Support portal provides access to the Knowledge Base, the current version of BlueVision software for the library, drive firmware, drive device drivers, and additional service and support tools. You can also open or update a support incident.

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 BlueVision software, or to open a support incident.

1. Access the Technical Support portal login page at support.spectralogic.com.
2. On the home page, click **Register Now**.

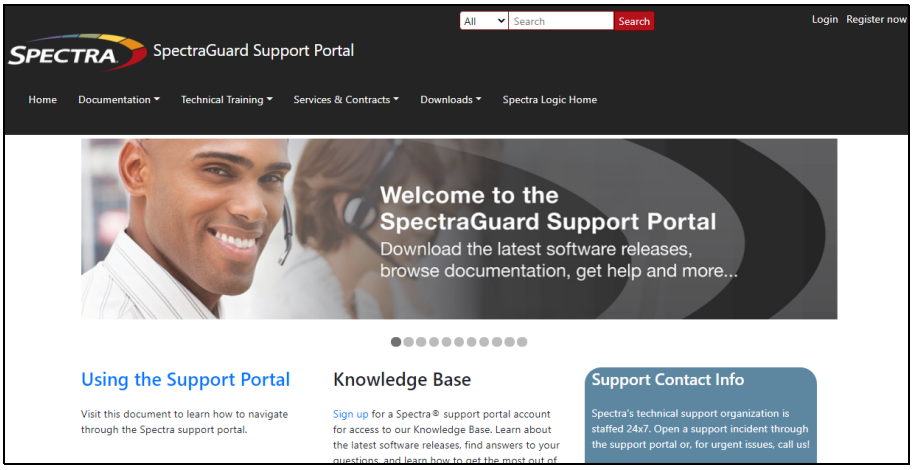


Figure 329 The Spectra Logic Technical Support portal home page.

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.

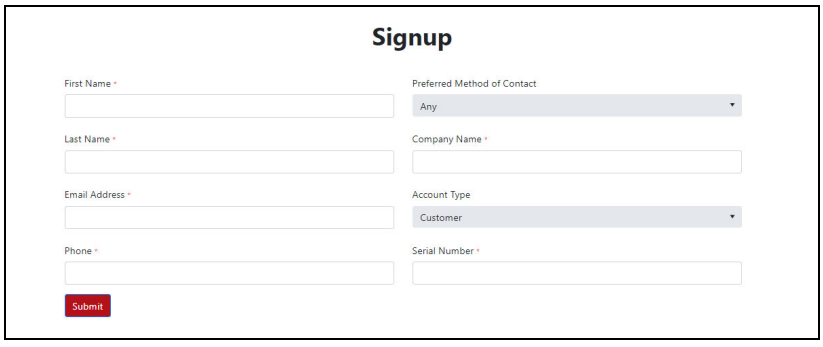


Figure 330 The Signup screen.

   - If you do not have an invitation, enter the requested information to create your account. When you are finished, click **Submit**.

When the account is approved, you receive an email with an 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

Use your email address and password to log into the Technical Support Portal.

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 through the portal, or skip to Contact Spectra Logic Technical Support by Phone on page 478.

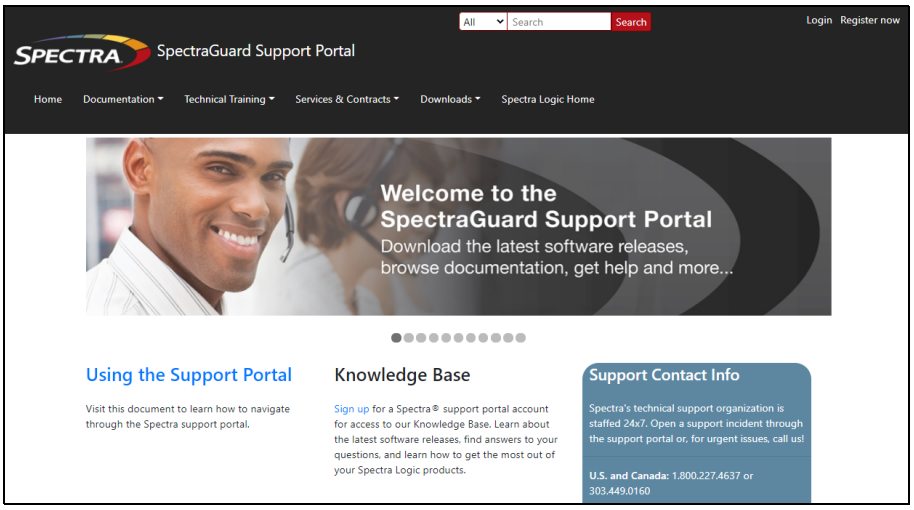


Figure 331 The Spectra Logic Technical Support portal home page.

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 Hardware ID on page 113)
   - 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 Accessing the Technical Support Portal on page 472 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 477.
     a. From any page, select **Incident⋯Incidents & Inventory**.

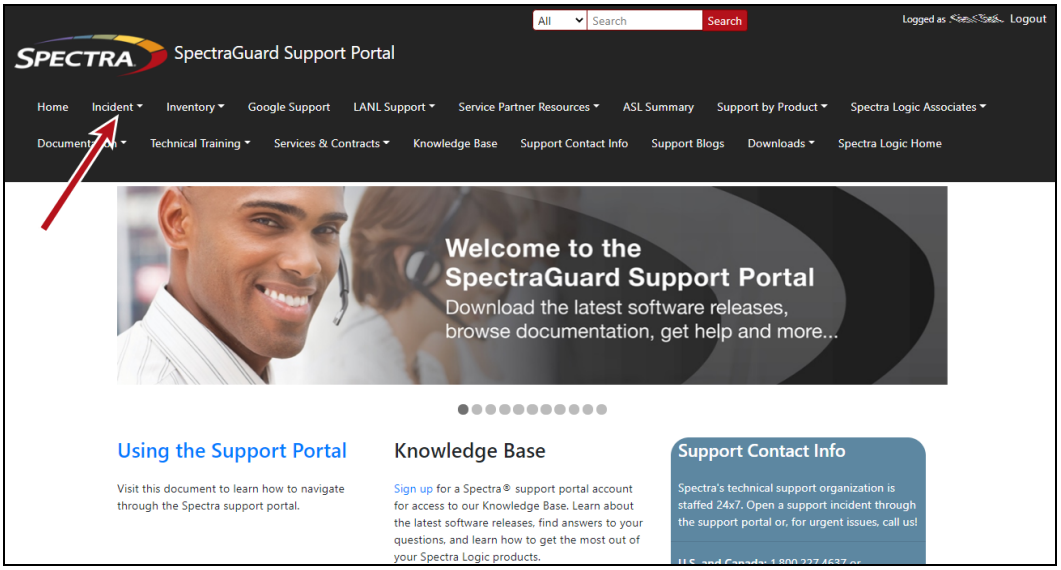


Figure 332 Select **Incidents⋯Incidents & Inventory**.

     b. Select **Open or View Incidents**.

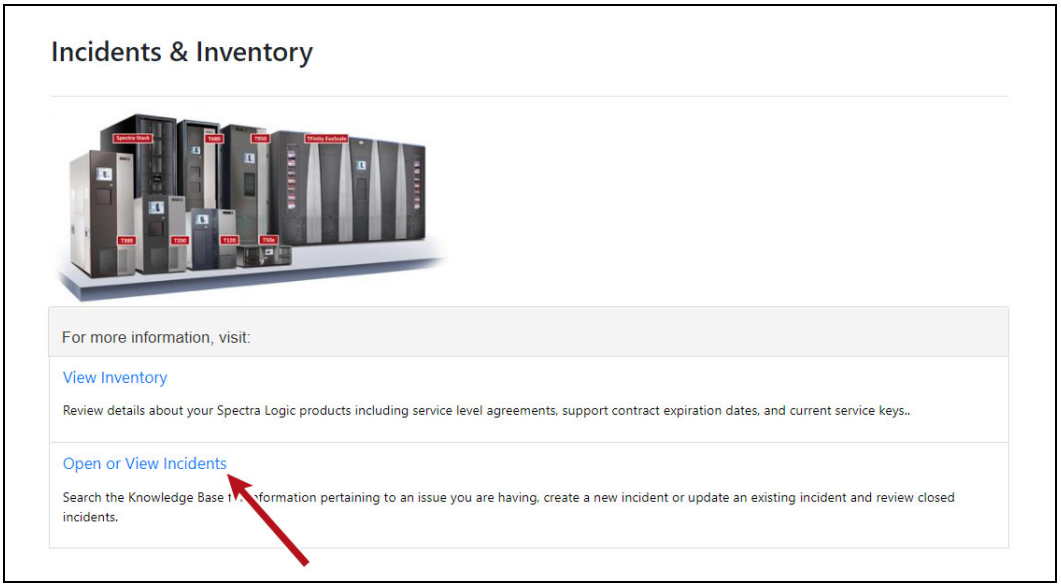


Figure 333 Select **Open or View Incidents**.

c. In the Search dialog box, enter a term or phrase about your problem (**1**) and click **Search** (**2**).

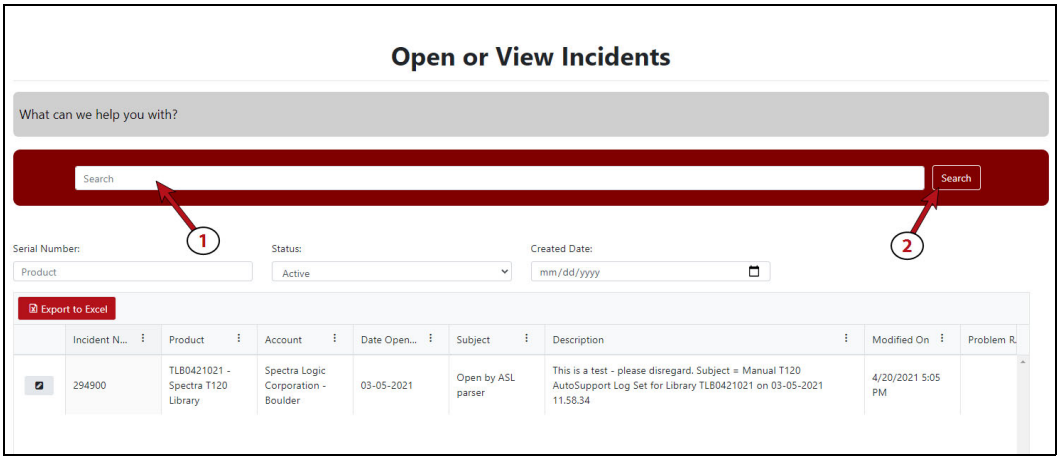


Figure 334 Enter a search phrase and click **Search**.

d. If the search does not provide an answer, click **Open a New Incident**.

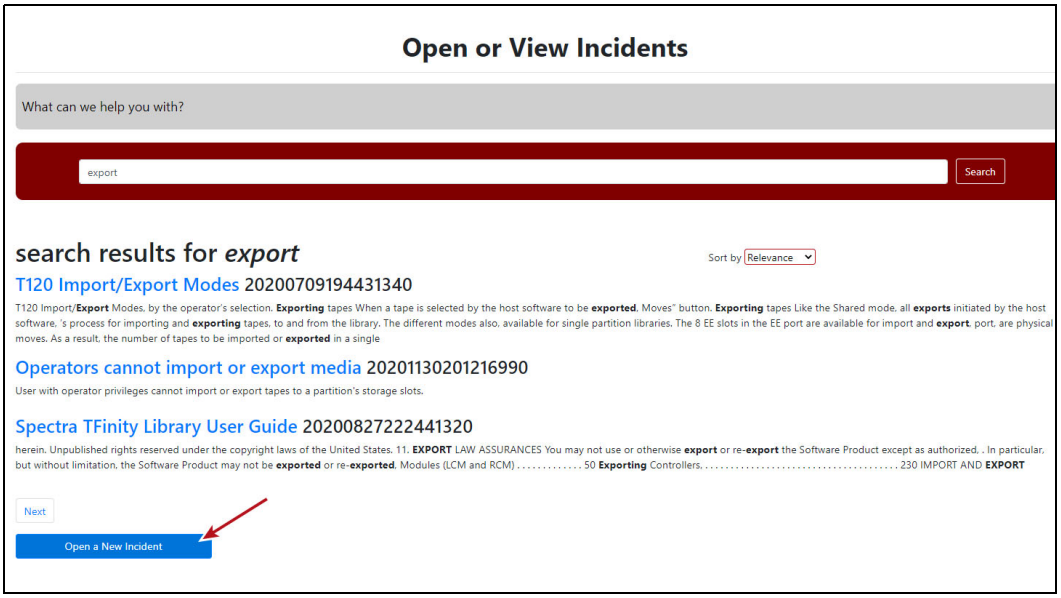


Figure 335 Click **Open a New Incident**.

e. Continue with Step 5 on page 478.

- Submit an Incident Directly

  a. From any page, select **Inventory⋯My Inventory**.

  b. Locate the row of the product for which you want to submit an incident and click **Create Incident**.

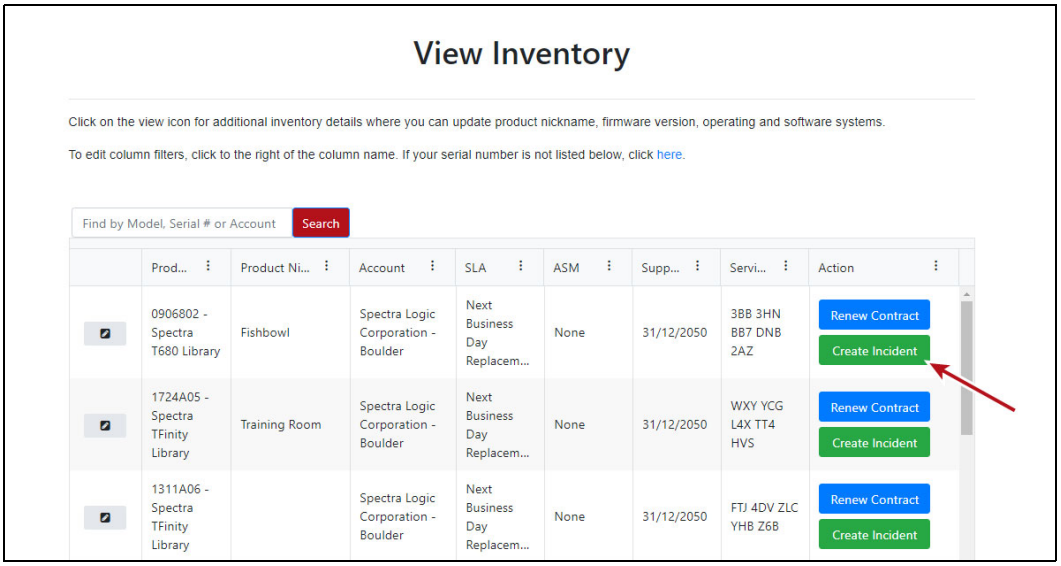


Figure 336 Click **Create Incident**.

c. Continue with Step 5 on page 478.

5. On the Create Incident page, enter the requested information providing as much detail as possible. When you are finished, click **Submit**.

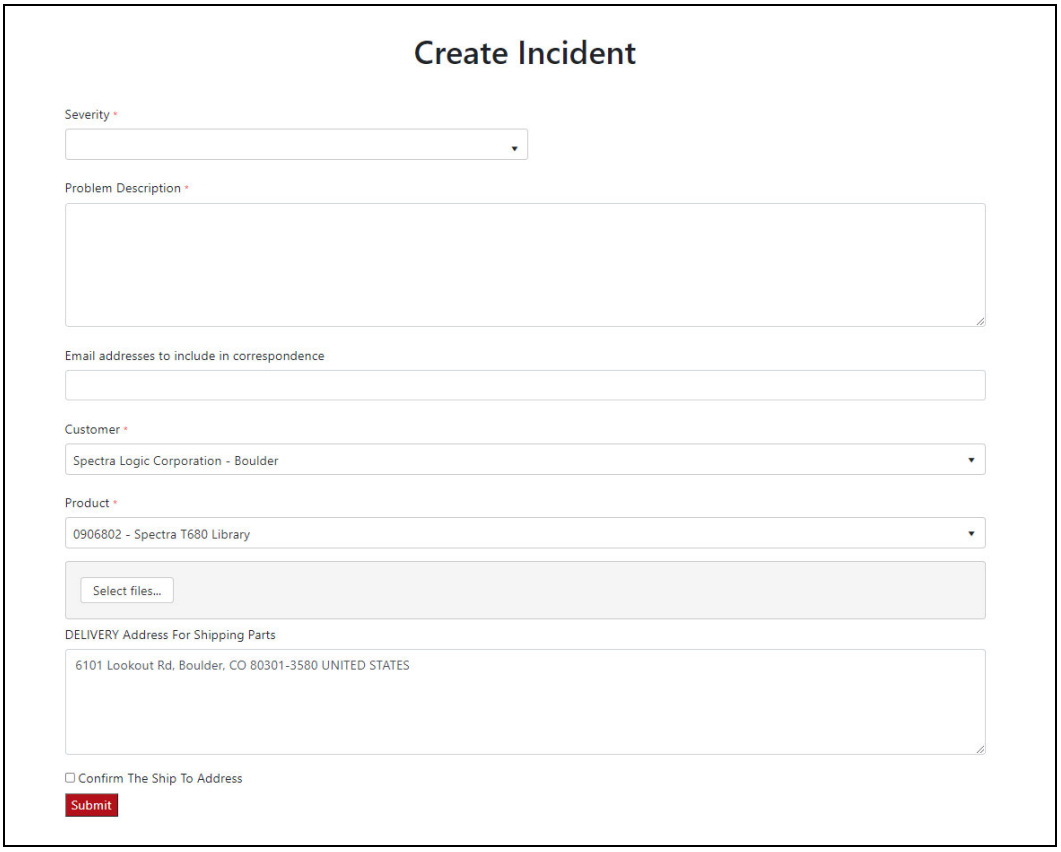


Figure 337 Enter information about your incident and click **Submit**.

Notes:
- If you have multiple libraries and need to determine the serial number of the affected library, see Determine the Hardware ID on page 113.
- If the serial number of the affected library is not listed, contact Technical Support (see Contacting Spectra Logic on page 7).

- Contact Spectra Logic Technical Support by Phone

To contact Spectra Logic Technical Support by telephone, see Contacting Spectra Logic on page 7.

RETURNS

Your Technical Support representative may ask you to return a problem component to Spectra Logic for analysis and servicing. After you complete a replacement procedure, return the defective part using ALL of the packaging that the replacement part arrived in (including any anti-static bags or foam inserts). If you are returning the entire library, see the *Spectra T50e Preparing for Shipment Guide* for information on preparing the library for safe shipment.

Caution Severe damage can occur if the component is not packaged correctly. You may be invoiced if it is damaged due to improper or insufficient packaging.

Use the return label and instructions that were included with the replacement part when preparing to ship the component you are returning. If you cannot locate these, contact Spectra Logic for another copy (see Contacting Spectra Logic on page 7). The return label and Return Merchandise Authorization (RMA) printed on it are used to associate the returned component with your account. To avoid being invoiced for failure to return the component, do not ship the component back to Spectra Logic without the RMA return label.

APPENDIX A

Best Practices

This appendix reviews best practices for using Media Lifecycle Management (MLM), protecting library configuration data, and working with media.

MLM Best Practices

To effectively use MLM and ensure that the MLM and DLM databases are protected, plan a strategy based on your data center needs and develop policies and procedures to support that strategy. Having sound management policies and procedures for media rotation and management is essential for consistent, effective implementation.

Implementation Guidelines

Consider the following best practice guidelines as you prepare to implement MLM in your environment.

Guideline	Description
Identify the people responsible for backing up data	The people who perform data backup at your site are typically the ones who are responsible for implementing and following MLM backup procedures.
Identify the users who have responsibilities that involve MLM	It may be wise to have more than a single user familiar with policies, depending on the size of your organization, so that if one person is not available, another can take over.
Be consistent with partition names	Using consistent naming simplifies identifying a specific partition. Spectra's suggested naming practice is to list the location, followed by the library name, followed by the storage management software. For example, Dallas/T50e/Netbackup.
On an organizational level, determine the level of management your media requires	The level of media management depends on the requirements for your environment. For example, you may choose to use Spectra's guidelines for retirement for all media, or you may choose to retire tapes that hold financial or legal data sooner than recommended. See the Error and Warning health scores in Generate MLM Reports on page 262 for information on when cartridges should be retired.

Usage Policy Guidelines

Consider the following guidelines when establishing your Media Lifecycle Management policies.

Guideline	Description
Select a retirement guideline	When implementing MLM, decide at the beginning on the criteria to be used when determining when to retire a cartridge. Spectra suggests using the Media Lifecycle Management health icon, visible on the MLM Reports screen (Figure 169 on page 262) and on the Details screen (Figure 170 on page 264) for each tape, to assess the overall health of individual tapes. See Generate MLM Reports on page 262 for information about using the health icon to assess media health.

Guideline	Description
Only use MLM-enabled media and cleaning cartridges in MLM-compatible libraries and drives	For the most accurate tracking, do not import your MLM-enabled media into non-Spectra Logic libraries or drive generations earlier than LTO-4. The cartridge MAM is not updated with information about usage in those locations. As a result, the information about usage in those locations is not recorded in the MLM database when the cartridge is returned to your library.
Use only Spectra Certified Media with MLM support (both data and cleaning cartridges) in the library	To ensure the best possible performance, use Spectra Certified Media. Check the Spectra Logic website for the most up-to-date media availability. Do not use any media that is not approved by Spectra Logic for use in the library. The library uses information in the MLM database to monitor the health of the media in the library. For MLM-enabled media, the detailed health reports let you determine whether a particular data cartridge is past its useful threshold or determine whether a particular cartridge is experiencing high errors rates or retries. For MLM-enabled cleaning cartridges, you are notified when a cartridge is approaching the end of its useful life. Although MLM tracks the general health of media that is not MLM-enabled, detailed health information is not available for this media.
Do not routinely share LTO-4 media between LTO-4 and LTO-5 drives	Beginning with BlueScale12.0.7, after an LTO-4 cartridge is loaded into an LTO-5 or later generation drive, the algorithm used to calculate the media health score whenever the cartridge is subsequently loaded in an LTO-4 drive is adjusted to maintain consistent media health reporting regardless of the generation drive used with the cartridge. As a best practice for your LTO-4 media, Spectra Logic recommends that you configure LTO-4 drives in separate partitions from LTO-5 and later generation drives and that you do not routinely share LTO-4 media between LTO-4 and LTO-5 or later generation drives.
Do not reformat LTO-5 data cartridges to use LTFS until after each cartridge is loaded into an LTO-5 drive	LTO-5 and later generation drives support a tape format called Linear Tape File System (LTFS). LTFS uses an area in the LTO-5 cartridge MAM that was previously used for MLM data. Before reformatting LTO-5 cartridges to use LTFS, make sure they are properly prepared, as described in Support for LTFS for LTO-5 Data Cartridges on page 201.
Always operate the library with Media Lifecycle Management enabled	If you disable and then re-enable Media Lifecycle Management, any loads, reads, writes, errors, and any other tape related events that occur while MLM is disabled are not recorded in the MLM database.

Guideline	Description
Enable load count alerts	Load count alerts, used in combination with the media health icon, let you monitor the health of individual tapes. Tapes with low load counts, but with a yellow or red health icon are vulnerable to high errors rates or retries. For higher levels of notification, configure a threshold for the maximum number of times a data cartridge can be loaded before an alert is generated (see Enable MLM and Configure Settings on page 242). When the number of loads exceeds this threshold, MLM generates a system message listing the barcode of the tape. You can also enable an alert to notify you when the load count recorded on the cartridge MAM differs from the load count stored in the MLM database but none of the other data was changed. This type of discrepancy can indicate that the tape was loaded into a non-Spectra Logic library. Use this alert as a security feature to let you know when a tape was removed and loaded into a drive in a different library.
Regularly back up your MLM database	Determine how frequently to export the MLM database for storage. You can save the MLM database to a USB device or email it to a previously configured mail recipient. The database can be loaded back into the library in the event of an error. See Disaster Recovery Planning on page 484 and Restore the MLM and DLM Databases on page 384 for detailed information. See Configure Mail Users on page 107 for information about configuring mail recipients. Backing up the MLM database produces a point-in-time snapshot of the MLM database. Based on the number of tapes you routinely import into and export from the library, determine how frequently backups are needed to ensure that you can easily restore the MLM database.
Enable non-MLM media alerts	Alerts for non-MLM-enabled media notify you when a cartridge that is not MLM-enabled is loaded into a drive.
Track exported cartridges	When a cartridge is exported from the library, an asterisk (*) next to the barcode indicates that it is currently out of the library. However, all of the MLM data for the cartridge is still available. Define the frequency with which you generate the complete MLM report and make a note of all exported tapes.
Select relevant information for saved reports	When you save an MLM report (see Generate MLM Reports on page 262), you can select between saving all MLM data or just the data from the most recently viewed report. You can save a copy of the MLM report as a comma-separated text file (*.rpt) to a USB device, mail the saved report to previously configured email recipient, or both. If desired, you can zip the file before saving it (see Save an MLM Report on page 267).

Disaster Recovery Planning

As a part of best-practice disaster recovery planning and processes, Spectra Logic strongly recommends backing up the MLM database to a USB device or emailing it to a preconfigured mail recipient automatically after using MLM for some period of time. In the event of a disaster, you can use the backup to restore the MLM database information for the media in your library instead of rebuilding it by loading each cartridge into a drive (see Restore the MLM and DLM Databases on page 384).

Important

The weekly Auto Configuration Save file reflects the state of the MLM database at the time the backup was created. If MLM-enabled cartridges are imported into or exported from the library during the period between the weekly Auto Configuration Save operation, the backup of the MLM database may not accurately reflect the library's inventory.

If you plan to import or export a large number of MLM-enabled cartridges, back up the MLM database using the procedure described in Back Up the MLM and DLM Databases on page 270 when you are finished to ensure that you have a backup that accurately reflects the information in the database.

Notes:

- Backing up the MLM database also backs up the DLM database.
- For extra security, the Auto Configuration Save feature automatically backs up the library's configuration and the MLM and DLM databases to the LCM memory card once a week and whenever a partition is created or modified (see Back Up the Library Configuration Automatically on page 117).
- If email is enabled for the Auto Configuration Save feature, the backups are emailed to the designated mail users (see Email Auto Configuration Save on page 111).
- See Back Up and Protect the Library Metadata on page 485 for additional disaster planning information.

BACK UP AND PROTECT THE LIBRARY METADATA

To ensure the availability of your library and encrypted data, protect library metadata by following the procedures described in this section. Library metadata includes library configuration data, the MLM and DLM databases, and all BlueScale encryption key-related data.

Note: The DLM database is included in any operations that back up or restore the MLM database.

Having reliable backups of the library metadata is *very* important in the case of disaster recovery and other situations where you need to restore the library.

Caution

Losing your library's metadata can have catastrophic effects—as can losing keys in any encryption key management system. If you lose all copies of all metadata:

- Your encrypted data is lost—you are unable to decrypt encrypted data without the encryption keys.
- You need to completely reconfigure your library.
- You lose stored data about your media that is time-consuming to recover.

Back Up the Library Metadata

Use the following methods to create backup copies of all of your library's metadata. The following table shows the file names and locations of the data saved during each type of backup operation.

This backup method...	Creates...
Auto Configuration Save Option	A time-stamped zip file containing the library configuration, the MLM and DLM databases, and any BlueScale encryption keys stored in the library. The zip file is named `<date-time>cfg.zip`, where `<date-time>` is the time stamp for when the zip file was created. The file is stored on the memory card in the LCM and can be sent as an email attachment to a previously configured mail recipient. ▪ See Email Auto Configuration Save on page 111 for information about configuring the Auto Configuration Save feature so that the library automatically sends an email with the current auto-save configuration file to a pre-configured mail recipient once a week and whenever you create or modify a library partition. ▪ See Back Up the Library Configuration Automatically on page 117 for information about using this method to back up the library configuration and the MLM and DLM databases. **Note:** The Auto Configuration Save feature does not automatically create a backup when you make other configuration changes to the library.

This backup method...	Creates...
Save MLM Database Advanced Utility	A time-stamped file containing the entire contents of the current MLM and DLM databases. The file is saved to a USB device or emailed to a previously configured mail recipient. If the backup file was saved to a USB device, it is located in a folder called `\SavedMLMDB`. The filename includes the time stamp `<date-time>` to indicate when the backup was created. The filename extension depends on whether the backup file was zipped when it was created attachment. ▪ **Unzipped file** — `cminfo_<date-time>.dat` ▪ **Zipped file** — `cminfo_<date-time>.zdt` Back Up the MLM and DLM Databases on page 270 provides instructions for using the utility. **Important:** To ensure that you always have a current backup of the MLM and DLM databases, back them up regularly.
Partition Wizard —AND— **Save Library Configuration Utility**	Multiple configuration files with the format `cnnnnnn.cfg`, where `n` is a number between 0 and 9. You can select to save the library configuration data to a USB device or email it to a previously configured mail recipient. ▪ If the backup files are saved to a USB device, they are located in a folder called `SavedConfigs\<date-time>`, where `<date-time>` is the time stamp for when the backup was created. ▪ If the backup is sent as an email attachment, the configuration files are in a zip file named `<date-time>cfg.zip`, where `<date-time>` is the time stamp for when the zip file was created. **Important:** The backup file of the library configuration does not include the MLM and DLM databases. **Important:** Backing up the library configuration also backs up any BlueScale encryption keys that are stored in the library at the time the file is created. ▪ **Partition Wizard** — The partition wizard prompts you to save the library configuration whenever you create or modify a partition. See Chapter 6 – Configuring and Managing Partitions, beginning on page 159 for detailed information about creating and modifying partitions. ▪ **Save Library Configuration Utility** — Use the Save Library Configuration utility to back up the updated library configuration whenever you make a configuration change to the library. This is especially important when you make configuration changes that do not result in an Auto Configuration Save file being generated. See Back Up the Library Configuration Manually on page 118 for instructions.

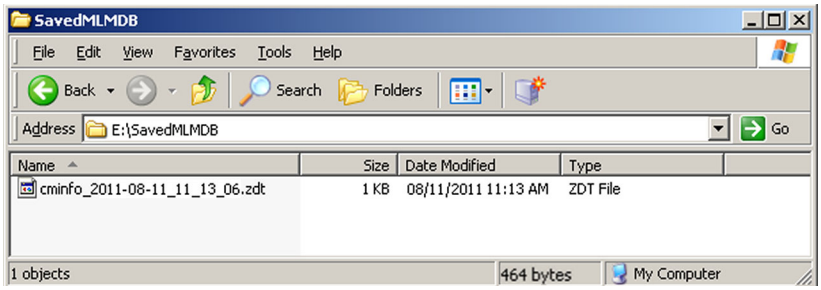
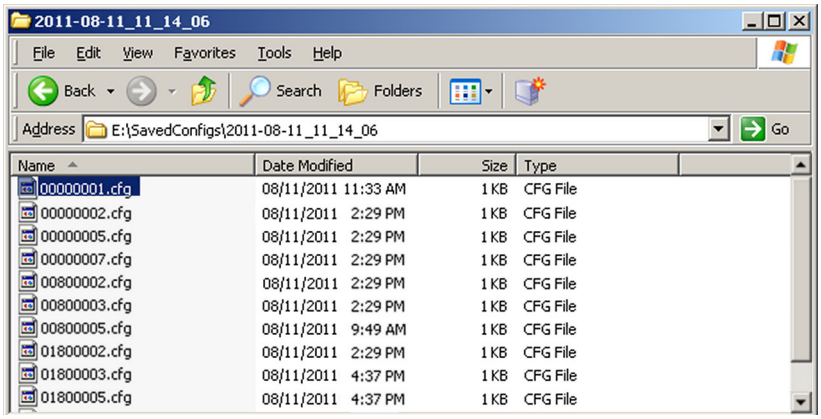
This backup method...	Creates...
Export Key Option (BlueScale Encryption)	A file containing the exported BlueScale encryption key. ▪ If the key was exported as a single file, the key filename is *name*.bsk, where *name* is the moniker you assigned to the key when you created it. ▪ If the key was split into M-of-N shares when it was exported, the filename for each share file is *name*.bss. Use the BlueScale **Export Key** option to export BlueScale encryption keys as soon as you create them. You can select to save the exported key file to a USB device or email it to a previously configured mail user. The exported keys are encrypted and password protected. See Exporting and Protecting Encryption Keys on page 314 for instructions. **CAUTION:** As a matter of best practice, Spectra Logic recommends exporting BlueScale encryption keys to a USB device instead of using email. Although emailing encryption keys is supported by the library, doing so presents security issues, including the following: ▪ Copies of encryption keys may be left on the email servers used for sending and receiving email and are thus subject to compromise. ▪ The difficulty in verifying where all of the copies of emailed encryption keys may be located can make security audits more challenging.

Verify and Protect the Metadata Backup

Do the following to ensure that your metadata is protected and available when you need it:

1. As soon as you create and export the backup files, check the exported data to make sure the correct files are present and accessible.
   - Plug the USB device into a computer or laptop.
   - If you emailed the metadata (the data is sent as an attachment), save the data to a USB device, and then check the data in the email attachment and the data on the USB device.

Examples The following figures show examples of the files that display when you check your USB device or the email attachment.

Saved Data	Details
BlueScale encryption key (T50e_SF2.bsk)	 **Note:** The screen shown here also includes the SavedMLMDB and SavedConfigs folders.
MLM and DLM data	 **Note:** In this example the file has a .zdt extension because the file was zipped when it was created.
Configuration data	 **Note:** The files are located in the `\SavedConfigs\<date-time>` folder, where `<date-time>` in this example is 2011-08-11_11_14_06.

2. Store at least one USB device containing the backup files off-site. After you have several weeks of backups stored off-site, rotate back through them.
3. When you run through disaster recovery exercises, test restoring the library using the backup files from both your USB devices and your saved email attachments. See Restoring the Library Configuration on page 374 for instructions.

USING CARTRIDGES

Note: See MLM Best Practices on page 481 for additional guidance when using Spectra Certified Media with MLM support.

The following sections describe best practices for using cartridges and for managing your media inventory. All library user groups have privileges that allow them to use the library's user interface to perform the cartridge handling and media management operations described in this section. Because handling cartridges requires physical interaction with the library, much of the information in this section is not applicable when you are accessing the library using the BlueScale web interface.

Use Spectra Certified Media

To ensure the best possible performance, use Spectra Certified Media (both data and cleaning cartridges) in the library. See Spectra Certified Media on page 493 for more information about Spectra Certified Media.

If you do not use Spectra Certified Media, use only cartridges from vendors approved by Spectra Logic. Check the Compatibility Matrices page on the Spectra Logic web site for a list of approved vendors.

Labeling Cartridges

If you are not using pre-labeled Spectra Certified Media (both data and cleaning cartridges), be sure to label all cartridges with the appropriate barcode labels. Position each label in the indented area on the cartridge, as illustrated in Figure 338. See Barcode Label Specifications for Half-Inch Media on page 514 for detailed information about preparing and using barcode labels.

Caution Do not place labels on any surface of the cartridge except the area shown in Figure 338. A loose label can become dislodged and damage the drive.

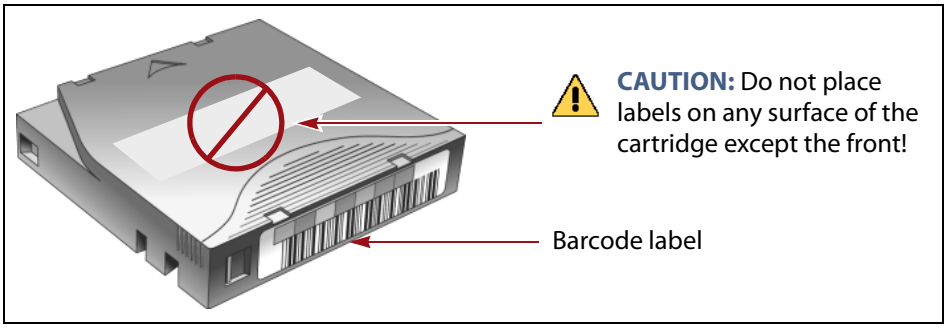


Figure 338 Properly barcode label all cartridges.

Handling Cartridges

Incorrect handling or an incorrect environment can damage the LTO cartridge or the magnetic tape inside it. To avoid damage to your cartridges and to ensure the continued high reliability of your drives, use the following guidelines:

- Do not drop the cartridge. If the cartridge drops, slide the cartridge door back and ensure that the leader pin is properly seated in the pin-retaining spring clips. Inspect the cartridge to make sure that there are no gaps in the seam of the cartridge case.
- Do not open any part of the cartridge other than the cartridge door. The upper and lower parts of the case are held together with screws; separating them destroys the usefulness of the cartridge.
- Do not handle tape that is outside of the cartridge. Handling the tape can damage the tape's surface or edges, which may interfere with read or write reliability. Pulling on tape that is outside of the cartridge can damage the tape and the brake mechanism in the cartridge.
- If tape is outside of the cartridge, slide the cartridge door back and turn the hub to gently spool the tape back into the cartridge. Test the tape by using your storage management software to write to the tape and then run a PostScan.
- Before you use a cartridge, let it acclimate for at least 24 hours to the normal operating environment.
- Ensure that all surfaces of a cartridge are dry before use.
- Do not stack more than six cartridges.
- Do not expose the tape cartridge to moisture or direct sunlight.
- Do not degauss a tape cartridge that you intend to use/reuse. Degaussing makes the tape unusable.
- Do not expose recorded or blank tape cartridges to stray magnetic fields (such as terminals, motors, video equipment, X-ray equipment, or high-current cables or power supplies). Such exposure can cause the loss of recorded data or make the blank cartridge unusable.
- Maintain the environmental conditions specified in LTO Cartridge Specifications on page 512.

Storing Cartridges

When the cartridges are *outside* of the library, Spectra Logic recommends storing them in TeraPack® magazines with dust covers.

Figure 339 TeraPack with barcode labeled cartridges and plastic dust cover.

Storing and handling cartridges in magazines helps to eliminate errors resulting from mishandling individual cartridges, which is the leading cause of cartridge damage. An optional plastic dust cover snaps onto the magazine to protect the cartridges.

Whenever you remove cartridges from your library, be sure to store them properly to maximize archival life and ensure data integrity. Follow these guidelines for proper cartridge storage:

- Store cartridges in a suitable environment (see LTO Cartridge Specifications on page 512).
- Keep the storage location as free of airborne particulates as possible. To eliminate obvious sources of particulates, do not permit anyone to smoke, eat, or drink near the storage area, and do not store cartridges near a copier or printer that may emit toner and paper dust.
- Store cartridges with the write-protect switch in the protected position (see Preparing Cartridges for Use on page 199).
- Store cartridges as soon as possible after you remove them from the library. Immediate storage helps avoid many of the conditions that can damage tapes, such as temperature and humidity fluctuations, particulate contamination, and excessive handling.
- If you plan to ship a TeraPack magazine, make sure that you have a proper shipping container and that you use adequate packing material. The TeraPack carrying cases available from Spectra Logic are designed for safely transporting TeraPack magazines off site and are compatible with Iron Mountain.

Using Cartridges in the Library

This section describes the best practices for using cartridges in the library.

- Use only cartridges from approved vendors in the library. See Spectra Certified Media on page 493 for more information about Spectra Certified Media.
- During an import or export operation, do not leave the library unattended for more than a few minutes. If you do, the import or export operation times out so that the library can continue automated backup tasks. To continue, restart the operation when you are ready.
- Enable Auto Drive Clean and configure a cleaning partition to clean drives whenever required to help ensure optimal performance. If you do not use the Auto Drive Clean feature, periodically check the Drive Details screen to determine whether the drives require cleaning (see Determine Whether Cleaning is Required on page 443).
- Confirm the quality of your media and verify data integrity by occasionally running restores using different drives.
- Confirm the quality of both media and drives by running periodic disaster recovery drills. These drills test the overall ability to recover all of your data using your backups.

APPENDIX B

Media and Upgrades

This appendix describes media, accessories, and upgrades that can be purchased for use with the T50e libraries. It also describes how to renew or extend the service contract for the library.

MEDIA AND MEDIA ACCESSORIES

Spectra Logic offers a variety of media and media accessories for the library.

Spectra Certified Media

Media formulations There are two distinct formulations for LTO media: Metal Particle (MP) and Barium Ferrite (BaFe). LTO-2 through LTO-5 media are only available in the Metal Particle formulation. LTO-6 media can be purchased in either the Metal Particle or the Barium Ferrite formulation. LTO-6 drives are designed to run both MP and BaFe media. The two formulations can be used in the same partition. LTO-7 and later media are only available in the Barium Ferrite formulation.

Certification process Spectra Certified Media begins with the highest quality data cartridges received directly from the manufacturer. During certification, each LTO cartridge is MLM-enabled. In addition, LTO data cartridges undergo the unique CarbideClean process, which removes embedded particles and smooths the imperfections in the tape surface that are a result of the manufacturing process. By cleaning the tape of the debris that exists on all new media, CarbideClean reduces signal loss and excessive tape head wear, thereby increasing the reliability, availability, and longevity of the drives and media.

Barcode labels For your convenience, all Spectra Certified Media is available pre-labeled with sequential barcode labels. Optional custom barcode sequences can be ordered, if desired. Using Spectra sequential pre-labeled media ensures that you never have to deal with the problem of duplicate barcodes. Spectra Logic's barcode labels carry the same lifetime guarantee that protects each Spectra Certified Media cartridge.

Media Storage Spectra Logic offers both TeraPack magazines and Maintenance TeraPack magazines pre-loaded with Spectra Certified Media data cartridges or cleaning cartridges, respectively. The magazines are available with or without a protective dust cover to protect the cartridges when they are not stored in the library. Empty magazines are also available. Check the Spectra Logic website at www.spectralogic.com for the most up-to-date media availability.

Media and Accessories

Spectra Logic offers the following media and accessories:

Media or Accessory	Description
Certified media packs	Each pack contains one TeraPack magazine filled with Spectra Certified Media (ten LTO data cartridges) with standard barcode labels. The media packs are available with or without a protective dust cover. **Note:** With the exception of LTO-2 and WORM media, all Spectra Certified LTO media is MLM-enabled.
Certified media pack with custom barcode labels	Each pack contains one TeraPack magazine filled with Spectra Certified Media (ten LTO data cartridges) with custom barcode labels. The media packs are available with or without a protective dust cover. You must order a minimum of four custom-labeled packs at a time.
Cleaning cartridges	Spectra Certified cleaning cartridges are available in Maintenance TeraPack magazines containing either five or ten cartridges. The cleaning cartridges have "CLN" at the beginning of the barcode sequence on their labels. **Note:** All Spectra Certified LTO cleaning cartridges are MLM-enabled. The cleaning cartridges are stored in Spectra Maintenance TeraPack magazines, which are identified by unique labels.
Barcode labels (in series of 300)	High-contrast, high-resolution labels for reliable operation. Labels are available either with a standard barcode numbering sequence or with a custom barcode numbering sequence. Barcode labels for cleaning cartridges are also available. The barcode labels for cleaning cartridges have "CLN" at the beginning of the barcode sequence.
TeraPack magazines	Empty ten-slot TeraPack magazines for storing LTO tapes or ten-slot Maintenance magazines for LTO cleaning cartridges are available. The magazines are available with or without a protective dust cover.
TeraPack magazine carrying cases	Carrying cases are designed for safely carrying TeraPack magazines off site. Cases are compatible with Iron Mountain.

LIBRARY SUPPORT AND UPGRADES

The library ships with the service contract and options purchased with the library. You can renew your service contract or purchase more capacity or additional options described in this section at a later date.

Service Contract Extension

Your initial library purchase includes a BlueScale Software Support key that is valid for the duration of the warranty period, or for the duration of any uplifted or extended service contract you purchased with the library, whichever is longer. A valid BlueScale Software Support key is required in order to update the library's BlueScale software and the firmware for library components, and to obtain technical support.

Important When you renew or extend your service contract, you must generate a new BlueScale Software Support key and enter the new key into the library to allow continued access to updates (see Enabling BlueScale Software Support, Options, and Upgrades on page 112). If you have questions about your service agreement, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

When the original warranty or service contract expires, a renewal contract can be purchased to continue service. Contact Spectra Logic to purchase a renewal contract (see Contacting Spectra Logic on page 7).

BlueScale Software Updates

Upgrades to the library's BlueScale software are free of cost to customers who have a current service contract with Spectra Logic Technical Support. When a service contract is renewed, you must generate a new BlueScale Software Support key and enter it into the library to allow continued access to updates. See Enabling BlueScale Software Support, Options, and Upgrades on page 112 for information.

Important Updating the BlueScale software and the firmware for the library components requires a current service contract with Spectra Logic Technical Support. The BlueScale Software Support key associated with your service contract must be stored in the library by entering it into the System Configuration screen. See Enabling BlueScale Software Support, Options, and Upgrades on page 112 for additional information.

If you have questions about your service agreement, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

See Updating the BlueScale Software and Library Firmware on page 421 for upgrade instructions.

Library Upgrades

Upgrades available for purchase include BlueScale software options and library hardware upgrades. You can purchase options and upgrades from your sales representative (see Contacting Spectra Logic on page 7).

Options

The following table describes the BlueScale software options that are available. See Enabling BlueScale Software Support, Options, and Upgrades on page 112 for information about enabling these options.

Library Option	Description
Spectra SKLM Encryption Key Management System	Spectra Tivoli Key Lifecycle Manager (Spectra SKLM) is a centralized key management system that allows you to manage the lifecycle of the encryption keys and security certificates for your library. Spectra SKLM provides role-based access control, based on user privileges, for tasks that range from creating and assigning encryption keys to the backup and restoration of data. See Encryption and Key Management Overview on page 289 for more information about the Spectra SKLM Encryption key management system.
BlueScale Encryption Professional Edition	In addition to the features of the standard edition, BlueScale Encryption Professional Edition supports multiple keys on a library and additional security features so that you can implement more customized data encryption regimens. See Encryption and Key Management Overview on page 289 for more information about BlueScale Encryption.
Capacity-On-Demand (CoD)	The Capacity-On-Demand (CoD) feature lets you purchase a library that meets your current storage needs and then purchase additional capacity later as required. CoD reduces up-front costs, because users only pay for what they currently need. As more capacity is required, it can be added in increments by purchasing activation codes to license additional slots in the library.
Shared Library Services (SLS)	Shared Library Services (SLS) partitioning logically divides the library into multiple virtual libraries. With SLS, one library can provide dedicated library services to multiple user groups. The default library configuration includes support for a single storage partition. If you need additional storage partitions, you must purchase a Shared Library Services (SLS) key. See Partition Overview on page 160 for more information about using partitioning in the library using SLS.

Hardware Expansion and Upgrades

The library is designed to expand to meet changing storage requirements, as well as to achieve storage consolidation goals. These expansion and upgrade options can be purchased through a Spectra Logic sales representative (see Contacting Spectra Logic on page 7).

The following table describes the types of hardware expansion and upgrades that are available.

Hardware	Description
Drives	The library accommodates one or two full-height tape drives and from one to four half-height tape drives. If fewer tape drives are installed, you can purchase additional tape drives to increase data throughput. See LTO Tape Drives on page 32 for information about the supported drives. **Important:** Do not attempt to install drives purchased from other vendors in the library. The drives used in the library are specifically configured for use in the library and must be purchased from Spectra Logic.
Power Supplies	The library requires one power supply. Adding another power supply provides N+1 redundancy and failover protection. The power supply needed for the N+1 power redundancy configuration is an option you can purchase separately or when you order the library.
Capacity Expansion Slots	You can add up to three additional cartridge capacity slots to the Spectra T50e library. See Installing Capacity Expansion Slots (Optional) on page 60 for information.
USB Device	You can use a USB device for saving backups of the library configuration and MLM database, when you are updating the library's BlueScale software, or as a troubleshooting tool for use as instructed by Spectra Logic Technical Support. USB devices are available for purchase from Spectra Logic for a nominal charge.

How to Order

To purchase library upgrades, including a renewed or extended service contract, determine your library Hardware ID (see Determine the Hardware ID on page 113) and then contact your sales representative (see Contacting Spectra Logic on page 7).

Replaceable Components

Some library components are extremely easy to remove and install. They are classified as customer-replaceable units (CRUs) and they are available for purchase based on your service contract with Spectra Logic Technical Support (see Chapter 16 – Technical Support, beginning on page 472).

The following library components are considered CRUs:

- Drives
- Capacity expansion slots
- Library Control Module (LCM)
- Memory card (used in the LCM)
- Power supply modules
- Robotics

APPENDIX C

Specifications

This appendix provides specifications for the Spectra T50e library and LTO tape drives, as well as the media (cartridges) used in the library:

Note: The specifications in this chapter are subject to change without notice.

LIBRARY SPECIFICATIONS

This section provides the specifications for the library.

Size and Weight

The following table shows the size and weight specifications for the T50e library and other components.

Note: All dimensions and weights are approximate.

Component	Specification	
	Installed	**Shipping and Storage**
Library Height	▪ **Tabletop:** 7.3 in. (18.5 cm) ▪ **Rack-mounted:** 6.9 in. (17.5 cm)	13.5 in. (34.3 cm)
Width	17.5 in. (44.4 cm)	23.5 in. (59.7 cm)
Depth	31.6 in. (80.3 cm)	39.1 in. (99.3 cm)
Weight [a]	▪ **One full-height tape drive:** 71.9 lb (32.6 kg) ▪ **Two full-height tape drives:** 79.8 lb (36.2 kg) ▪ **One full-height and two half-height tape drives:** 81.9 lb (37.1 kg) ▪ **Two half-height tape drives:** 74.0 lb (33.6 kg) ▪ **Four half-height tape drives:** 84.0 lb (38.1 kg)	Approximately 66.4 lb (30 kg) [b]
Drive Weight	Included in weight specification above	▪ **Full-Height—LTO-2 through LTO-4:** 7.9 lb (3.6 kg) ▪ **Half-Height—LTO-4 through LTO-6:** 5.0 lb (2.3 kg)
Data Cartridge Weight	▪ **LTO-3:** 0.463 lb (210 grams) ▪ **LTO-4 through LTO-9:** 0.441 lb (200 grams)	N/A
Cleaning Cartridge Weight	0.254 lb (115 grams)	N/A
TeraPack Magazine Weight [c]	N/A	5.1 lb (2.3 kg) each
Power Supply Weight	3.3 lb (1.5 kg)	
Component Box Weight	N/A	Varies [d]

a. Includes the chassis, the LCM, listed drives, and one power supply. Does not include cartridges. To calculate the approximate weight of a loaded library, add the weight of each cartridge and the second power supply, if present, to the weight of the library and installed drives.

b. Includes chassis, the LCM, and one power supply, as well as the following items: the rack-mounting kit, power cord, Ethernet cable, and product documentation. Does not include drives, cartridges, or a second power supply, if included in your purchase.

c. Includes 10 LTO cartridges.

d. The size and weight depends on the number and type of components in the box. To calculate the approximate weight of all the components, add the weight for each TeraPack magazine full of cartridges, each drive, and a second power supply, if included in your purchase, to the shipping weight of the library.

Rack-Mounting Specifications

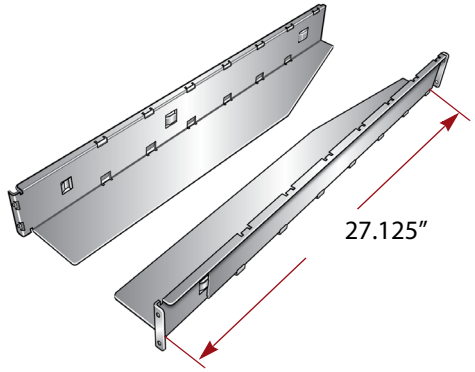
The Spectra T50e is designed to fit into a standard 4-post rack using just 4U of rack space. This section provides basic rack-mounting specifications.

- See Install the Library in a Rack on page 45 for rack-mounting installation instructions and a list of the components in the rack-mounting kit.
- See Library Specifications on page 498 for the library weight and dimension specifications.

The rack must be located near the AC power outlets and network connections.

Caution The rack must be located on a level, hard-surfaced floor such as cement or tile. Do not place the rack on a carpeted floor or anywhere else that poses risk for static discharge that could damage your library and its tape drives.

The following table provides the minimum rack-mounting dimensions.

Component	Dimension
Rail assemblies (shown collapsed) 	Rail length: Collapsed (minimum): 27.125 in. (68.9 cm) Extended (maximum): 43.0 in. (109.2 cm) **WARNING** The library must be installed in the rack that is delivered with the library, or if none is included, in a standard 19 in. (48 cm), four-post rack. A two-post rack cannot support the weight of the library. Ensure your floor has adequate structural integrity, and follow the rack manufacturer's instructions when installing and securing the rack.
Mounting brackets (attached to library) 	Center to center: 18 in. (45.7 cm)

Recommendations

Follow these recommendations to ensure that your library has enough clearance:

- Use a 4-post rack that is at least 43 inches (110 cm) deep.
- Allow an additional 6 inches (15.2 cm) at the back for cable clearance and a minimum of 12 inches (30.4 cm) at the front for operating the access port.

Power Specifications

This section describes the power specifications for the library.

Input Power Requirements

The following table shows the input power requirements for the library with one to four LTO tape drives installed. Each input must be protected by a circuit breaker rated for 15 amps.

Electrical Rating	Current Rating (Maximum)
100–127 VAC, 50/60 Hz	4 amps per cord
200–240 VAC, 50/60 Hz [a]	2 amps per cord

a. Requires a 220–240 VAC AC power cord with a twist-lock male connector. See Power Cord Specifications on page 501 for detailed information about power cord requirements.

When using the redundant AC power configuration, connect each power supply input to a separate branch circuit. Using separate circuits allows for failover in the event of a power failure in one of the circuits. The two AC inputs must be on the same phase, and the voltages must be the same within a few volts.

Caution

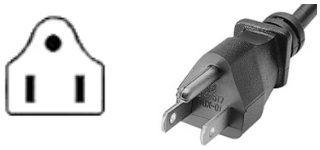
The library is designed to be used on single phase power only. If the power sources for the dual AC inputs are not on the same phase, damage to the library could result.

Power Cord Specifications

The power cord included with the library is considered part of the library and is not intended for use with any other equipment.

Notes:

- The supply-end connector is considered the disconnect for the unit. Make sure that the socket-outlet for the AC connections is in an accessible location near the library.
- To use the library outside of North America, the power cord must meet the specifications for that country.

Part Number	Power Input Connector Style	Supply-end Connector Style	Supply-end Connector Appearance	Power Cordage
3136	IEC 60320-C13, female	Standard NEMA 5-15 110-120V (wall power connector)		Three-conductor, 18 AWG
8296	IEC 60320-C13, female	PDU Connection IEC-60320 C14 110-240V, 50-60Hz (library power connector)		Three-conductor, 16 AWG

Power Consumption and Cooling Requirements

The power and cooling requirements for the library depend on the number of tape drives installed. The following table provides the power consumption and heat load for the base library with one power supply and with one drive installed. Use this information to calculate the maximum power consumption and heat load values, which can be used to build a power budget for the library.

All values are measured at the AC input and include power supply efficiency. The values are averages of observed hardware. In general, the lighter the load on the power supplies, the less efficient they are. The power supply efficiency in turn affects the power draw of all components.

Component	Power Consumption (watts)	Heat Load, Continuous (BTU/hour)
Base library [a]	▪ **Moving a cartridge:** 31 ▪ **Idle:** 24	▪ **Moving cartridges:** 106 ▪ **Idle:** 82
LTO-4 half-height drive, Fibre Channel or SAS [b]	▪ **Read/write:** 39 ▪ **Idle:** 19	**Read/write:** 133
LTO-4 half-height drive, SCSI [b]	▪ **Read/write:** 37 ▪ **Idle:** 18	**Read/write:** 126
LTO-5 half-height drive, Fibre Channel or SAS [b]	▪ **Read/write:** 24 ▪ **Idle:** 6	**Read/write:** 82
LTO-6 half-height drive, Fibre Channel or SAS [b]	▪ **Read/write:** 24 ▪ **Idle:** 6	**Read/write:** 82
LTO-7 half-height drive, Fibre Channel or SAS [b]	▪ **Read/write:** 31 ▪ **Idle:** 20 [b]	**Read/write:** 106
LTO-8 Fibre Channel or SAS Half-Height	▪ **Read/write:** 43 ▪ **Idle:** 14 [b]	**Read/write:** 164
LTO-9 Fibre Channel or SAS Half-Height	▪ **Read/write:** 35	**Read/write:** 119

a. Includes the chassis, the LCM, and one power supply. Does not include drives.
b. Includes the drive sled used to mount the drive in the library.

Environmental Specifications

This section describes environmental specifications for the library. The library is equipped with internal fans to keep the library's internal temperature within specifications as long as the operating environment is within specifications.

Caution When the library is moved from a cold environment to a warm environment, it should not be used for at least 24 hours. This adjustment period prevents condensation damage.

The following tables list the general environmental specifications for the library.

Mode	Dry-bulb Temperature	Maximum Temperature Rate of Change [a]	Relative Humidity (non-condensing)	Maximum Humidity Rate of Change	Maximum Altitude
Allowable Environment	16° C to 32° C (60° F to 90° F)	5° C per hour 9° F per hour	20% to 80% 22° C dew point max (72° F)	5% per hour with no condensation	3048 m (10,000 ft)
Recommended Environment	16° C to 25° C (60° F to 77° F)	5° C per hour 9° F per hour	20% to 50% 22° C dew point max (72° F)	5% per hour with no condensation	3048 m (10,000 ft)

a. The temperature and humidity must be allowed to stabilize in the specified ambient environment for 24 hours.

Storing[a] and Shipping (Non-Operating) Environment	
Humidity	10% to 90% (non-condensing)
Temperature	–22° F to 140° F (–30° C to 60° C)
Altitude	Sea Level to 45,000 feet (13,716 meters)

a. The library in its original packaging. The packaging is designed to protect the library from condensation caused by extreme temperature variations (15° C or more). When the library is moved from a cold storage environment to a warm operating environment, it must be acclimated in its packaging for at least 24 hours before opening to prevent serious condensation damage from occurring.

Shock and Vibration

The library operates normally after experiencing shock loads as specified in the following table. The operating shock levels indicate how much shock the library can withstand while the enclosed tape drives are reading and writing data. The non-operating and storage shock levels indicate how much shock the library can withstand when it is not operating.

Specification	Operating Environment	Non-Operating Environment [a]
Shock	11 ms @ 4 G half sine	▪ **Storing (tabletop model):** 81 G sine wave with pulse duration of 3ms or less ▪ **Shipping drop test height:** 30 inches for up to a maximum weight of 77.6 lb (35.2 kg).
Vibration (Swept Sine)	Not applicable	5 Hz – 500 Hz – 5 Hz at 0.5 G
Vibration (Random)	5 – 500 Hz at 0.25 Grms	▪ **Storing:** 5 – 200Hz at 2.1 Grms ▪ **Shipping:** 5 – 200 Hz at 1.35 Grms (Six faces for 30 minutes/side)

a. Library is in its original packaging.

INTERFACE SPECIFICATIONS

This section provides information about the interfaces used to connect the library and tape drives to the host systems. It also provides information about the Ethernet interface used to access the library's BlueScale web interface.

Interface Connectors

The tape drives have either a Fibre Channel, SAS, or Ultra 320 LVD SCSI bus interface. One of the drives in the partition (the exporting drive) provides the interface from the host to the robotics. The motion commands from the host are routed to the robotics through LUN 1 of the exporting drive. The tape drive reports the robotics as "SPECTRA PYTHON" on LUN 1. LUN 0 is the tape drive itself.

Component	Physical Interface
Drive, Fibre Channel	The Fibre Channel tape drives support the Fibre Channel Protocol (FCP). ▪ Each full-height Fibre Channel drive has two Fibre Channel dual port multimode optical LC sockets, each with a multi-mode SFP installed. [a] ▪ Each half-height Fibre Channel drive has a single multimode optical LC socket with a multi-mode SFP installed. **Note:** For information about how LTO Ultrium tape drives support Fibre Channel communications, refer to the tape drive documentation, available from IBM at www.storage.ibm.com/tape/lto/oem/index.html.
Drive, SAS	SAS tape drives support the point-to-point Serial Attached SCSI protocol. ▪ **LTO-3 through LTO-8** - Connecting these drives to the host network requires an SFF-8088 SAS cable rated for 6 Gb/second that does not exceed 13 feet (4 m). ▪ **LTO-9** - Connecting these drives to the host network requires an SFF-8644 SAS cable rated for 12 Gb/second that does not exceed 13 feet (4 m).
Drive, SCSI	The SCSI drives support the SCSI protocol. ▪ Each full-height LTO-3 drive has two Ultra-3 SCSI "LVD" 68-pin Micro D female connector. ▪ Each half-height LTO-4 drive has two VHDCI SCSI connectors. **Note:** One wide Ultra320 SCSI Active SCSI terminator is provided with each SCSI tape drive.
LCM	The Ethernet port on the LCM is a pin-through-hole RJ-45 shielded connector.

a. Only one port at a time can be used to connect the drive to a Fibre Channel network. If desired, the two ports can be used to create a failover configuration.

Interface Cable Requirements

The type of cables required to connect the library and its drives to the network depend on the type of interface being used.

Interface Type	Cable Requirements
Fibre Channel	Connecting the Fibre Channel drives to the host arbitrated loop or fabric requires multimode optical cables with dual LC connectors. Depending on the wavelength, the cables must comply with the following specifications in the Fibre Channel standard (FC-PI-2): ▪ **50 micron**—400-M5-SN-I classification ▪ **62.5 micron**—400-M6-SN-I classification (not supported for LTO-6 or higher drives)
SAS	Connecting the SAS tape drives to the host require a SFF-8088 SAS cable rated for 6 Gb/second that does not exceed 13 feet (4 m).

SCSI [a, b]	Connecting a SCSI drive to a host SCSI bus requires an LVD SCSI cable that does not exceed 39 feet (12 m) with one of the following connectors:
	▪ Full-height SCSI LTO-3 tape drives use Ultra-3 SCSI "LVD" Fast & Wide, 68-pin Micro D male connectors.
	▪ Half-height SCSI LTO-4 tape drives use a male VHDCI to VHDCI connector or a male VHDCI to HD68 connector.
	▪ Each SCSI drive is shipped with one terminator.
	  ▪ Full-height SCSI drives use an active wide HD68 multi-mode, Ultra320 LVD/SE terminator
	  ▪ Half-height SCSI drives use an active VHCDI Ultra320 LVD/SE terminator

Ethernet	The Ethernet port on the LCM provides the connection to a 10/100BaseT Ethernet network for accessing the library using a standard web browser on a remote computer. To comply with EMC requirements, use shielded Category 5 (10/100BaseT connection) data-grade cables or a similar Category 5 cable that is compliant with EIA/TIA 568 for all Ethernet connections.

a. Spectra Logic does not support operating SCSI LTO tape drives on an SE bus.
b. Using an HBA connection for each drive is recommended. Daisy-chaining LTO-4 or later generation drives is not supported.

Universal Serial Bus (USB) Support

Spectra Logic supports using the USB ports on the library operator panel, the LCM, and the RCM for the following:

- Keyboards
- Pointer devices (for example, a computer mouse)
- External Drives (HD, CD, DVD, and Flash) with a USB interface

Spectra Logic does not support using the USB ports for the following:

- Cameras
- Multimedia devices (for example, MP3 players)

Important The library only recognizes FAT-formatted, not NTFS-formatted, USB devices.

NDMP Support

Spectra Logic tape libraries are compatible with local, remote, and three-way NDMP (Network Data Management Protocol) topologies, where the tape library is connected to the NDMP data mover host over Fibre Channel.

DATA STORAGE CAPACITY

The T50e library provides flexible storage capacity that expands from a minimum of 10 slots to a maximum of 50 slots. The following table shows the uncompressed capacity of the library for each of the supported LTO generations. See LTO Cartridge Specifications on page 512 for information about the capacity of individual cartridges.

Number of Storage Slots [a]	Native Capacity (TB)						
	LTO-4	LTO-5	LTO-6	LTO-7	LTO-7 type M	LTO-8	LTO-9
10 (minimum)	8	15	25	60	90	120	180
50 (maximum) [b]	40	75	125	300	450	600	900

a. The front slot in the lower left magazine is the access port. A cartridge in the access port cannot be used for data storage until it is moved to a storage slot.

b. The 50-slot configuration requires replacing the top three half-height drive bays with three capacity expansion slots.

TAPE DRIVE AND MEDIA SPECIFICATIONS

This section provides the basic specifications for the tape drives and media supported by the library. The specifications in this section are provided for convenience only and are subject to change without notice. Refer to the tape drive documentation for the most current specifications (see LTO Ultrium Tape Drives on page 19).

Note: LTO tape drives and cartridges are also referred to as LTO Ultrium or Ultrium tape drives and cartridges.

LTO Tape Drive Specifications

Note: See LTO Cartridge Capacities on page 512 for information about the media used in the library.

LTO-9 Drive

When connecting to a Fibre Channel network, LTO-9 Fibre Channel drives will attempt to connect at 8 Gb/second, but will auto-negotiate down to 4 Gb/second, or 2 Gb/second, depending on the requirements of the port to which the drive is connected.

LTO-9 SAS drives attempt to connect at 12 Gb/second, but auto-negotiate down to 6 Gb/second or 3 Gb/second, depending on the requirements of the port to which the drive is connected.

Parameter	Specification
Maximum sustained transfer rate [a, b]	400 MB/second, native 900 MB/second, compressed SAS 700 MB/second, compressed Fibre
Speed matching range	177 MB/second to 400 MB/second
Average space record time	TBD
Encryption capability	AES 256-GCM
WORM capability	Yes
MTBF	250,000 hours at 100% duty cycle
Uncorrected error rate, calculated	1×10^{-20} bits
Power consumption	Read/write: 34 watts typical Idle: TBD

a. Assuming a 2.5:1 compression ratio. Compression throughput depends on the type of data.

b. This is a per-drive value. Total sustained transfer rate for the library depends on the number of drives installed in the library.

LTO-8 Drive

When connecting to a Fibre Channel network, LTO-8 Fibre Channel drives will attempt to connect at 8 Gb/second, but will auto-negotiate down to 4 Gb/second, or 2 Gb/second, depending on the requirements of the port to which the drive is connected.

LTO-8 SAS drives attempt to connect at 6 Gb/second, but auto-negotiate down to 3 Gb/second or 1.5 Gb/second, depending on the requirements of the port to which the drive is connected.

Parameter	Specification
Maximum sustained transfer rate [a, b]	360 MB/second, native 750 MB/second, compressed
Speed matching range	112 MB/second to 360 MB/second
Average space record time	59 seconds
Encryption capability	AES 256-GCM
WORM capability	Yes
MTBF	250,000 hours at 100% duty cycle
Uncorrected error rate, calculated	1×10^{-19} bits
Power consumption	**Read/write:** 43 watts typical **Idle:** 14 watts

a. Assuming a 2.5:1 compression ratio. Compression throughput depends on the type of data.
b. This is a per-drive value. Total sustained transfer rate for the library depends on the number of drives installed in the library.

LTO-7 Drive

When connecting to a Fibre Channel network, LTO-7 Fibre Channel drives attempt to connect at 8 Gb/second, but auto-negotiate down to 4 Gb/second, or 2 Gb/second, depending on the requirements of the port to which the drive is connected.

LTO-7 SAS drives attempt to connect at 6 Gb/second, but auto-negotiate down to 3 Gb/second or 1.5 Gb/second, depending on the requirements of the port to which the drive is connected.

Parameter	Specification
Maximum sustained transfer rate [a, b]	300 MB/second, native 750 MB/second, compressed
Speed matching range	100 MB/second to 300 MB/second
Average space record time	60 seconds
Encryption capability	AES 256-GCM
WORM capability	Yes
MTBF	250,000 hours at 100% duty cycle

Parameter	Specification
Uncorrected error rate, calculated	1 x 10^{-19} bits
Power consumption	**Read/write:** 31 watts typical **Idle:** 20 watts

a. Assuming a 2.5:1 compression ratio. Compression throughput depends on the type of data.
b. This is a per-drive value. Total sustained transfer rate for the library depends on the number of drives installed in the library.

LTO-6 Drive

When connecting to a Fibre Channel network, LTO-6 Fibre Channel drives attempt to connect at 8 Gb/second, but auto-negotiate down to 4 Gb/second, 2 Gb/second, or 1 Gb/second, depending on the requirements of the port to which the drive is connected.

LTO-6 SAS drives attempt to connect at 6 Gb/second, but auto-negotiate down to 3 Gb/second or 1.5 Gb/second, depending on the requirements of the port to which the drive is connected.

Parameter	Specification
Maximum sustained transfer rate [a, b]	160 MB/second, native [c] 400 MB/second, compressed
Speed matching range	40 MB/second to 160 MB/second
Average space record time	77 seconds
Encryption capability	AES 256-bit
WORM capability	Yes
MTBF	250,000 hours at 100% duty cycle
Uncorrected error rate	1 x 10^{-17} bits
Power consumption	**Read/write:** 28 watts typical **Idle:** 8 watts

a. Assuming a 2.5:1 compression ratio. Compression throughput depends on the type of data.
b. This is a per-drive value. Total sustained transfer rate for the library depends on the number of drives installed in the library.
c. A 1.5 Gb interface speed does not stream an LTO-6 drive at 160 MB/second.

LTO-5 Drive

When connecting to a Fibre Channel network, LTO-5 Fibre Channel drives attempt to connect at 8 Gb/second, but auto-negotiate down to 4 Gb/second, 2 Gb/second, or 1 Gb/second, depending on the requirements of the port to which the drive is connected.

When connecting to a SAS network, LTO-5 SAS tape drives attempt to connect at 6 Gb/second, but auto-negotiate down to 3 Gb/second as needed.

Parameter	Specification
Maximum sustained transfer rate [a, b]	140 MB/second, native [c] 280 MB/second, compressed
Speed matching range	30 MB/second to 140 MB/second
Average space record time	75 seconds
Encryption capability	AES 256-bit
WORM capability	Yes
MTBF	250,000 hours at 100% duty cycle
Uncorrected error rate	1×10^{-17} bits
Power consumption [b]	**Read/write:** 27 watts typical **Idle:** 7.5 watts

a. Assuming a 2:1 compression ratio. Compression throughput depends on the type of data.
b. This is a per-drive value.
c. A 1 Gb interface speed does not stream an LTO-5 drive at 140 MB/second.

LTO-4 Drive

When connecting to a Fibre Channel network, LTO-4 Fibre Channel drives attempt to connect at 4 Gb/second, but auto-negotiate down to 2 Gb/second or 1 Gb/second, depending on the requirements of the port to which the drive is connected.

Parameter	Specification
Sustained transfer rate [a, b]	120 MB/second native [c] 240 MB/second compressed
Average space record time	70 seconds
Encryption capability	AES 256-bit
WORM capability	Yes
MTBF	250,000 hours at 100% duty cycle
Uncorrected error rate	1×10^{-17} bits
Power consumption - Fibre Channel [b]	**Read/write:** 29.5 watts typical **Idle:** 12.5 watts
Power consumption -SCSI [b]	**Read/write:** 26.5 watts typical **Idle:** 9.5 watts

a. Assuming a 2:1 compression ratio. Compression throughput depends on the type of data.
b. This is a per-drive value.
c. A 1 Gb interface speed does not stream an LTO-4 drive at 120 MB/second.

LTO Cartridge Specifications

This section provides specifications for the LTO cartridges supported by the library. See Media and Accessories on page 494 for information about ordering cartridges for your library.

Environmental Requirements

The following table lists the specifications for storage temperature and other environmental requirements for tape media. Do not allow the temperature and humidity in the storage environment to fluctuate.

Specification	Recommended Operating	LTO-9 Allowable Operating [a]	LTO-8 and Lower Allowable Operating [a]	Shipping [b]
Temperature	59° F to 77° F (15° C to 25° C)	59° F to 95° F (15° C to 35° C)	50° F to 113° F (10° C to 45° C)	–9° F to 120° F (–23° C to 49° C)
Relative humidity	20% to 50%	10% to 80%	10% to 80%	5% to 80%
Max dew point	72° F (22° C)	71.6° F (22° C)	79° F (26° C)	79° F (26° C)
Maximum humidity rate change	5% / hour with no condensation	5% / hour with no condensation	5% / hour with no condensation	
Maximum Altitude	10,000 ft 3048 m	10,000 ft 3048 m	10,000 ft 3048 m	40,000 ft 12192 m

a. The upper limit applies to the media, not the library. Be sure there is adequate air flow around the library at all times.

b. When media is moved from a cold shipping/storage environment to a warm operating environment, it must be acclimated in its packaging for at least 24 hours before opening to prevent condensation damage from occurring.

LTO Cartridge Capacities

The following table shows the capacities of the different generations of LTO Ultrium data cartridges.

LTO Media Generation	Native Capacity (Compressed Capacity)
LTO-4	800 GB (1.6 TB) [a]
LTO-4 WORM	
LTO-5	1.5 TB (3 TB) [a]
LTO-5 WORM	
LTO-6	2.5 TB (6.25 TB) [b]
LTO-6 WORM	

LTO Media Generation	Native Capacity (Compressed Capacity)
LTO-7	6 TB (15 TB [b])
LTO-7 WORM	
LTO-7 type M	9 TB (22.5 TB [b])
LTO-8 and LTO-8 WORM	12 TB (30 TB [b])
LTO-9 and LTO-9 WORM	18 TB (45 TB [b])

a. Assuming a 2:1 compression ratio. The compressed capacity depends on the type of data.
b. Assuming a 2.5:1 compression ratio. The compressed capacity depends on the type of data.

LTO Read/Write Compatibility

The following table shows the media read/write compatibility for each LTO drive generation supported by the library.

Drive Gen	LTO-4 Media	LTO-5 Media	LTO-6 Media	LTO-7 Media	M8 Media	LTO-8 Media	LTO-9 Media
LTO-4	**Read/ write**	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported
LTO-5	**Read/ write**	**Read/ write**	Not supported	Not supported	Not supported	Not supported	Not supported
LTO-6	*Read only*	**Read/ write**	**Read/ write**	Not supported	Not supported	Not supported	Not supported
LTO-7	Not supported	*Read only*	**Read/ write**	**Read/ write**	Not supported	Not supported	Not supported
LTO-8	Not supported	Not supported	Not supported	**Read/ write**	**Read/ write**	**Read/ write**	Not supported
LTO-9	Not supported	Not supported	Not supported	Not supported	Not supported	**Read/ write**	**Read/ write**

LTO Encryption Compatibility

Key AES-256 data encryption with a secret 256-bit encryption key is used to encrypt and decrypt data. The key is not retrievable from the encryption core and is automatically erased during the unload process; software is required to extract the key, keep it secure, and provide management tools to track, store, use, and delete keys as appropriate.

Notes:
- The encryption performed by encryption-enabled LTO-4 or later generation drives is not compatible with the encryption performed by an encryption-enabled F-QIP.

- Spectra SKLM key management is not compatible with BlueScale Encryption key management, because they cannot share encryption keys. Data encrypted using Spectra SKLM key management cannot be decrypted using BlueScale Encryption key management, and vice versa.

For more information about encryption, see Chapter 10 – Encryption and Key Management, beginning on page 289.

LTO WORM Media

Certain records retention and data security applications require a Write Once, Read Many (WORM) method for storing data on tape. LTO-3 and later generation drives enable WORM support when a WORM tape cartridge is loaded into the drive.

WORM Media Requirements Because standard read/write media are incompatible with the WORM feature, a specially formatted WORM tape cartridge is required. Each WORM cartridge has a unique, worldwide cartridge identifier (WWCID), which comprises the unique CM chip serial number and the unique tape media serial number.

Data Security on WORM Media Certain built-in security measures help ensure that the data written on a WORM cartridge does not become compromised, for example:

- The format of a WORM tape cartridge is unlike that of standard read/write media. This unique format prevents a drive that lacks WORM-capable firmware from writing on a WORM tape cartridge.
- When the drive senses a WORM cartridge, the firmware prohibits the changing or altering of user data already written on the tape. The firmware keeps track of the last appendable point on the tape.

LTO Cleaning Cartridges

The LTO cleaning cartridges are valid for 50 uses. Do not rewind and reuse the material in a cleaning cartridge. Reusing the material may redistribute contaminants previously removed from the tape path. If all of the cleaning material is used, discard the cartridge and use a new cleaning cartridge.

Barcode Label Specifications for Half-Inch Media

The Spectra Logic T50e supports barcode data strings consisting of a start character; from 1 to 16 characters, including alphanumeric characters and an optional checksum character; and the stop character. Quiet zones precede and follow the start and stop characters.

Note: BlueScale12.3.1 increases the number of barcode digits the T50e can recognize to 16 characters. Prior to BlueScale12.3.1, the library can recognize 8 characters, plus one checksum character.

Symbology The barcode labeling scheme used on Spectra Logic certified media uses the barcode symbology of USS-39. You can obtain a complete description and definition of this symbology from the *Automatic Identification Manufacturers (AIM)* specification, the *Uniform Symbol Specification (USS-39)*, and the *ANSI MH10.8M-1993 ANSI Barcode* specification.

Application and Orientation The barcode label must be applied to the cartridge so that it fits within the label recess on the edge of the cartridge without curling up on the sides or ends. The label must be oriented so that the barcode characters are along the edge closest to the hub side of the cartridge.

Printed Characters The label can have human-readable alphanumeric characters printed along the top or bottom edge of the label provided there is no conflict or interference with the automation code. This text must include the barcode data, but can also include additional text. The format and colors of the human readable characters is up to the customer and label vendor. For location restrictions, see Detailed Specifications on page 516.

Note: When using barcode labels with alphanumeric characters along the bottom edge, the label must be positioned so that barcode is at least 13.72 mm below the top edge of the cartridge to ensure that the barcode reader can read the label.

Dimensional Specifications Figure 340 shows the dimensional specifications for labels with the alphanumeric characters above the barcode.

Important The barcode label must only have one barcode on it. If multiple barcodes are present, the library's barcode scanner cannot determine which one to process when scanning the cartridge.

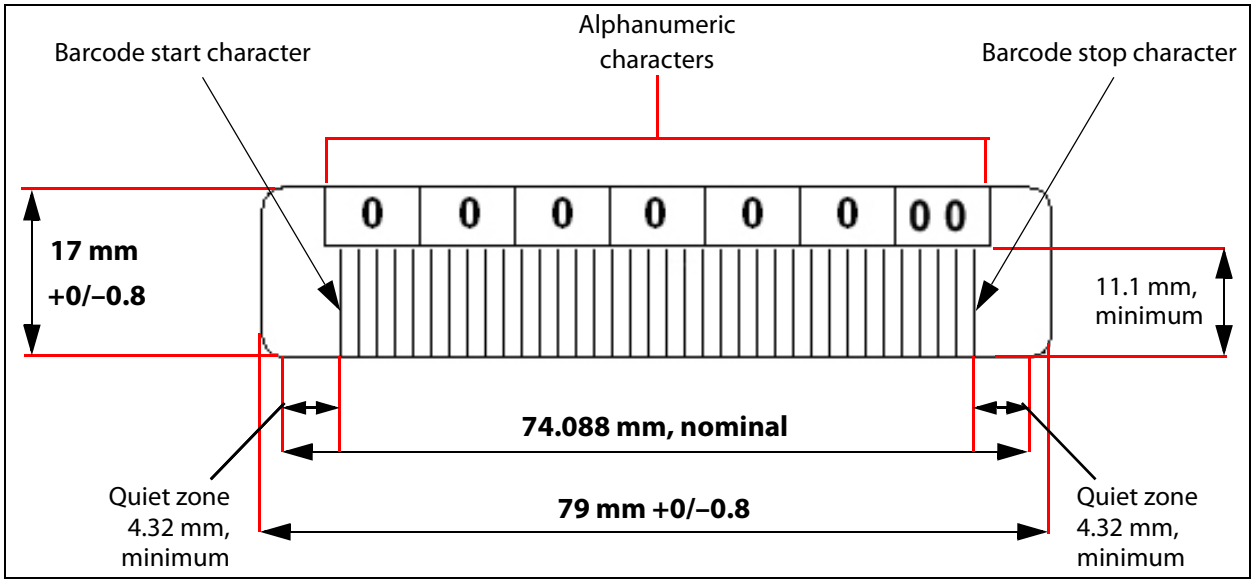


Figure 340 Barcode specifications for half-inch media; alphanumeric characters on top.

Detailed Specifications

For the official IBM barcode label specification, see http://www-01.ibm.com/support/docview.wss?uid=ssg1S7000429. Unless otherwise specified, tolerances are x.xxx ± 0.127 mm, y.yyy ± 0.762 mm.

Barcode Element Specifications

- Minimum symbol height is 11.1 mm, measured to the inside of the label's edge.
- The wide-to-narrow ratio is 2.75.
- The narrow element width is 0.432 mm +0.03 mm/–0.076 mm.
- The nominal width of the wide spaces and bars is 1.188 mm.
- The inter-character gap is 0.432mm +0.03/–0.076 mm.
- The minimum quiet zone at the beginning and end of a printed barcode string is 4.32 mm (10 times the narrow element width).
- The total nominal barcode string length (including quiet zones) is 74.088 mm.
- The edge of the barcode is the edge of all printed area attached to the bar. The edge roughness is the transition encountered as a horizontal line is moved vertically from all black to all white. The edge roughness maximum is 0.038 mm.
- Variation between all bars, white and black, must be less than ±0.0381 mm.

Physical Label Specifications

- Label stock must fit within the label recess on the face of the cartridge without curling up on the sides or ends (79 mm X 17 mm +0/–0.8).
- Minimum length sufficient for the quiet zones, start-stop, and data characters (nominal 74.088 mm).
- Minimum width no less than 1.5 mm narrower than the cartridge label recess width. Corners are cut with a 1.5 mm radius.
- Maximum label thickness, including the RFID tag if present, together with any associated layers and adhesives cannot exceed 0.40 mm.
- The label and adhesive must have an environmental performance to match or exceed the environmental specifications of the cartridge to which it is applied.

Human Readable Text

Human readable text is allowed provided there is no conflict or interference with the automation code. This text must include the barcode data, but can also include additional text. The format, colors, and location of the human readable characters is up to the customer and label vendor.

Barcode Data

The library supports barcode data strings consisting of a start character, eight characters, including alphanumeric characters and an optional checksum character, and the stop character. Quiet zones precede and follow the start and stop characters.

> **Note:** BlueScale12.3.1 increased the number of barcode digits the T50e can recognize to 16 characters. Prior to BlueScale12.3.1, the library can recognize 8 characters, plus one checksum character. If a checksum character is not included on the label, the barcode data string can contain up to nine alphanumeric characters.

- The first six (6) characters following the start character can be any combination of upper case A–Z or 0–9 (for example, ABC123) to identify the cartridge Volume Serial Number.
- The barcode string can be printed in either direction on the label and must begin and end with a valid start/stop character (*).
- The label must be printed so that the barcode data is positioned along the edge of the label that is closest to the hub side of the cartridge.

The *AIM Uniform Symbol USS-39* specification provides detailed information about the format of the start character, the series of characters that make up the barcode data, and the stop character.

Volume Identifier Formats

- The volume identifier field consists of six (6) left justified alphanumeric characters as described in the *SCSI-3 Medium Changer Commands (SMC) ANSI NCITS 314-199X* specification. The volume identifier only uses ASCII characters A–Z and 0–9. The use of "CLN" and "DG{space}" at the beginning of the volume identifier is reserved.

  Note: The library only supports barcodes with eight alphanumeric characters if the label includes a checksum character; nine alphanumeric characters can be used if the label does not include a checksum character.

- The volume identifier "CLN*vnn*" is reserved for cleaning cartridges. When a drive requires cleaning, it requests a specific type of cleaning cartridge.
  - The "*v*" field is an alphanumeric field to identify cleaning cartridge applications, "U" for Universal Cleaning Cartridges or a drive unique identifier.
  - The "*nn*" alphanumeric field is used to track individual cleaning cartridge activity (that is, usage and life).
- The volume identifier "DG{space}*vnn*" is reserved for diagnostic and service cartridges.
- The two character media identifier "L*g*" immediately follows the volume identifier.
  - The "L" identifies the cartridge as LTO.
  - The "*g*" represents and alphanumeric character that indicates the generation and capacity of the LTO cartridge.

    For example, L3 is LTO-3 media, and L4 is LTO-4 media.

In IBM LTO tape drives, the value of the media identifier on cleaning cartridges is ignored, although a valid value must be present.

Interoperability and Software Compatibility

You can find complete interoperability listings, as well as a list of the types of software that were tested and proven compatible with the library on the Spectra Logic Support portal at: support.spectralogic.com/documentation/compatibility-matrices/.

APPENDIX D

Regulatory and Safety Standards

When installed in accordance with this guide, the Spectra T50e library complies with the safety and regulatory agency standards listed in this appendix.

EU DECLARATION OF CONFORMITY

We:

Spectra Logic Corporation
6101 Lookout Road
Boulder, CO 80301 USA

declare under sole responsibility that the

Spectra model T50e Library

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.

Matt Starr
Chief Technical Officer, Spectra Logic Corporation

Standard	Specification Title
Application of Council Directives: ▪ 89/336/EEC ▪ CE-Directive 2006/95/EG	Essential health and safety requirements relating to electromagnetic compatibility.
EN 55022 (CISPR 22) Class A	Limits and methods of measurements of radio interference characteristics of information technology equipment.

Standard	Specification Title
EN 55024	Information Technology Equipment – Immunity Characteristics Limits and Methods of Measurement ▪ Power Line Harmonics: EN 61000-3-2 ▪ Power Line Flicker: EN 61000-3-3 ▪ Electrostatic Discharge: EN 61000-4-2 ▪ Radiated RF Immunity: EN 61000-4-3 ▪ Electrical Fast Transient/Burst: EN 61000-4-4 ▪ Surge Immunity: EN 61000-4-5 ▪ Conducted RF Immunity: EN 61000-4-6 ▪ Power Frequency H-field Immunity: EN 61000-4-8 ▪ Voltage Dips and Interrupts: EN 61000-4-11
EN 60950 (IEC 60950)	Safety requirements of information technology equipment including electrical machines.
Recast of RoHS directive 2011/65/ 2008	RoHS, Restriction of the use of certain hazardous substances in electrical and electronic equipment.
EU REACH Regulation (1907/ 2006)	This product contains less than 0.1% by weight of the substances on the EU SVHC Candidate List as of 18 June 2012.

EMISSION STANDARDS

Country	Standard
United States - FCC	CFR Title 47, FCC Part 15 (see FCC Notice)
Australia/ New Zealand	AS/NZS CISPR 22
Canada	ICES-003
Korea	RRA Notice 2011-02 (2011.01.21)
Japan	VCCI
Taiwan	CNS 13438

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 manual, 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.

CE Marking

The CE marking has been affixed on this device according to Module A of decision 768/2008.

Note: To meet CE certification requirements, you must be running your library on an uninterruptable power supply.

Safety Standards and Compliance

Product Safety Standards The Spectra T50e complies with the following domestic and international product safety standards.

- CAN/CSA C22.2 No. 60950-1-03 (Canada: cETL Mark)
- Electrical Equipment Law (Germany: GS Mark)
- IEC/EN 60950-1, Second Edition

Safety-relevant Provisions The Spectra T50e complies with all safety-relevant provisions referring to:

- Protection against electrical hazards
- Protection against hazards such as:
  - Mechanical hazards
  - Fire hazards
  - Noise
  - Vibration

Laser Warning

IBM Tape Drives

A Class 1 laser assembly, in the optical transceiver, is mounted on each IBM tape drive Fibre Channel electronics card. This laser assembly is registered with the DHHS and is in compliance with IEC825.

These products contain components that comply with performance standards that are set by the U.S. Food and Drug administration. This means that these products belong to a class of laser products that do not emit hazardous laser radiation. This classification was accomplished by providing the necessary protective housings and scanning safeguards to ensure that laser radiation is inaccessible during operation or is within Class 1 limits. External safety agencies have reviewed these products and have obtained approvals to the latest standards as they apply to this product type.

Intertek Accreditation

The safety issues of this information technology equipment type have been evaluated by a government-accredited European third-party organization, such as Intertek.

This Mass Storage Device has been evaluated and determined to comply with the Safety Requirements of the International Standard for Information Technology Equipment, IEC/EN 60950-1, Second Edition. The evaluation was conducted by Intertek. Intertek participates in the CB Scheme as a National Certification Body certified by the IECEE.

Intertek GS

The Spectra T50e Library is certified as safety tested through Intertek GS. This is a voluntary certification that complies with German safety regulations to meet the demands of the industry.

This user guide complies with this certification by providing all safety-relevant information in the German language.

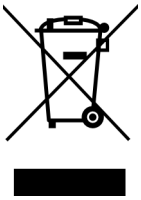
Deutsch: Die Spectra T50e Bibliothek ist zertifiziert durch Geprüfte Sicherheit durch Intertek. Dies ist eine freiwillige Zertifizierung, dass im Einklang mit den deutschen Sicherheitsvorschriften, um den Forderungen der Industrie.

Diese Bedienungsanleitung mit den Bestimmungen dieser Zertifizierung durch die Bereitstellung aller relevanten Sicherheits-Informationen in deutscher Sprache.

ENVIRONMENTAL REGULATIONS

The Spectra T50e complies with the following domestic and international hazardous materials directives.

Waste of Electronic and Electrical Equipment (WEEE) Directive



Note: For information on recycling your Spectra library, please check the Spectra Logic website. European Union users should contact their local waste administration for WEEE collection instructions for this product.

The WEEE symbol on the back of this product indicates that this product meets the European Directive 2012/19/EU 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.

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.

Measures for the Administration of the Control of Pollution by Electronic Information Products (China)

	T50e 有毒和有害物质及元素					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr(VI))	多溴联苯 (PBB)	多溴联苯醚 (PBDE)
底架	O	O	O	O	O	O
外壳	O	O	O	O	O	O
磁带机	X	O	O	O	O	O
电力安装	O	O	O	O	O	O

Recycling Your Library

For information on recycling your Spectra library, 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 are 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 is 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.

INDEX

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W