SPECTRA STACK LIBRARY USER GUIDE

SpectraLogic.com

COPYRIGHT

NOTICES

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

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

TRADEMARKS

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

90970035 Revision M

Revision History

Revision	Date	Description
A	March 2018	Initial release.
B	April 2018	Corrections and expanded instructions.
C	December 2018	Updated for the BlueVision 1.8 release.
D	March 2019	Updated for the BlueVision 1.9 release.
E	June 2021	Updated for the BlueVision 2.0 release.
F	December 2021	Updated for the BlueVision 2.1 release.
G	December 2022	Added Power Consumption and LTO Specifications.
H	January 2023	Updated for the BlueVision 2.3 release.
I	September 2023	Updated for the Encryption Professional feature.
J	October 2023	Updated for the BlueVision 2.4 release.
K	September 2024	Updated for the BlueVision 2.5 release.
L	June 2025	Updated for the BlueVision 2.51 release.
M	October 2025	Updated for the BlueVision 2.61 release.

Notes:

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

a. 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.

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

Contents

About This Guide

Document Purpose

This document provides information to configure, maintain, and troubleshoot the Spectra® Stack Tape Library. The instructions are intended for the System Administrators and trained Users who need physical and functional knowledge of the Stack library.

The main components are:

- Controller module: STACK BASE
- Expansion module: STACK EXP

Product Warranty Caution

Customers should only perform the service and repair actions on the tape library components using replacement instructions available on the Spectra Logic support portal. Any other actions must be performed by authorized service personnel.

The warranty for the tape library shall not apply to failures of any unit when:

- The tape library is repaired or modified by anyone other than the manufacturer's personnel or approved agent.
- The tape library is physically abused or used in a manner that is inconsistent with the operating instructions or product specification defined by the manufacturer.
- The tape library fails because of accident, misuse, abuse, neglect, mishandling, misapplication, alteration, faulty installation, modification, or service by anyone other than authorized service personnel.
- The tape library is repaired by anyone, including approved technicians, in a manner that is contrary to the maintenance or installation instructions supplied by the manufacturer.
- The manufacturer's serial number tag is removed.
- The tape library is damaged because of improper packaging on return.

The warranty becomes immediately void in the event of unauthorized repairs or modifications.

General Warnings

Document 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 or 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.

WARNING Lisez le texte marqué par l'icône «Avertissement» pour les informations que vous devez connaître pour éviter les blessures.

CAUTION Lisez le texte marqué par l'icône «Attention» pour obtenir des informations que vous devez connaître pour éviter d'endommager la bibliothèque ou les lecteurs de bande, ou de perdre des données.

IMPORTANT Lisez le texte marqué par l'icône «Important» pour obtenir des informations qui vous aident à terminer une procédure ou à éviter des étapes supplémentaires.

Remarque: Lisez le texte marqué par «Remarque» pour obtenir des informations supplémentaires ou des suggestions sur le sujet actuel.

General Product Warnings

WARNING

High voltage

Risk of electric shock

- Do not remove covers (top, bottom or rear). No user-serviceable parts are inside.
- Refer servicing to qualified service personnel.
- Plug the power cord into a grounded (earthed) electrical outlet that is easily accessible at all times.

WARNING

Haute tension

Risque de choc electrique

- Ne retirez pas les capots (supérieur, inférieur ou arrière). Aucune pièce réparable par l'utilisateur ne se trouve à l'intérieur.
- Confiez l'entretien à un personnel qualifié.
- Branchez le cordon d'alimentation dans une prise électrique reliée à la terre et facilement accessible à tout moment.

WARNING

Product Weight. See Physical Specifications on page 274.

Risk of personal injury

Before lifting a module:

- Observe local health and safety requirements and guidelines for manual material handling.
- Remove all tapes to reduce the weight.
- Remove all tape drives to reduce the weight.
- Obtain adequate assistance to lift and stabilize the module during installation or removal.

Risk of damage to library

When placing a module into or removing the module from a rack:

- Extend the rack's levelling jacks to the floor.
- Ensure that the full weight of the rack rests on the levelling jacks.
- Install stabilizing feet on the rack.
- Extend only one rack component at a time.

WARNING

Poids du produit. Voir Spécifications physiques à la page 205.

Risque de blessure corporelle

Avant de soulever un module:

- Respectez les exigences locales en matière de santé et de sécurité et les directives pour la manutention manuelle des matériaux.
- Retirez toutes les bandes pour réduire le poids.
- Retirez tous les lecteurs de bande pour réduire le poids.
- Obtenez une assistance adéquate pour soulever et stabiliser le module pendant l'installation ou le retrait.

Risque d'endommagement de la bibliothèque

Lors du placement d'un module dans ou du retrait du module d'un rack:

- Déployez les crics de mise à niveau du rack vers le sol.
- Assurez-vous que tout le poids du rack repose sur les vérins de mise à niveau.
- Installez les pieds de stabilisation sur le rack.
- Prolongez un seul composant de rack à la fois.

WARNING

In earthquake- prone areas, the rack must have stabilizing equipment or be anchored to the floor to eliminate the risk of tipping, which could lead to personal injury.In erdbebengefährdeten Gebieten muss das Rack stabilisierende Ausrüstung oder am Boden verankert, um die Kippgefahr, die zu Verletzungen führen können beseitigt werden.

WARNING

Dans les zones sujettes aux tremblements de terre, le rack doit être équipé d'un équipement de stabilisation ou être ancré au sol pour éliminer le risque de basculement, qui pourrait entraîner des blessures.

WARNING

Only trained personnel should operate this equipment. Read all documentation and procedures before installation or operation. This product is intended for installation and operation in a computer rack with the front and rear doors closed and secured. Only personnel with technical and product safety training should be provided access to the library. Such personnel are referred to as users throughout this document. Do not insert any tools or any part of your body into openings of an operating library.

WARNING

Seul un personnel formé doit utiliser cet équipement. Lisez toute la documentation et les procédures avant l'installation ou l'utilisation. Ce produit est conçu pour être installé et utilisé dans un rack d'ordinateur avec les portes avant et arrière fermées et sécurisées. Seul le personnel ayant une formation technique et sur la sécurité des produits doit avoir accès à la bibliothèque. Ce personnel est appelé utilisateur tout au long de ce document. N'insérez aucun outil ni aucune partie de votre corps dans les ouvertures d'une bibliothèque opérationnelle.

MECHANICALHAZARD

Danger Risk of hand pinching, can trap hands, fingers and cause serious injury. Keep hands clear during operation.

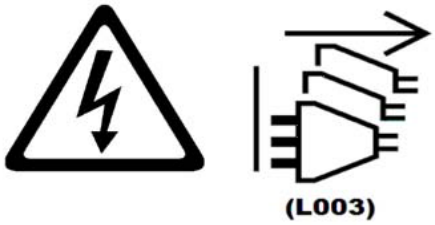
DANGER MÉCANIQUE

Danger Risque de se coincer la main et de se coincer les mains ainsi que les doigts le tout pouvant entrainer de graves blessures. Gardez les mains à l'écart pendant le fonctionnement.

Achtung:
Vor Öffnen des Gerätes
alle Netzstecker ziehen!

Attention:
Remove all power cords
before opening the unit!

Attention:
Débranchez toutes les fiches d'alimentation avant d'ouvrir l'équipment!



(L003)

Acronyms and Abbreviations

Acronym or Abbreviation	Meaning
FC	Fibre Channel
FH	Full Height
HBA	Host Bus Adapter
HH	Half Height
LUN	Logical Unit Number
OCP	Operator Control Panel (the library LCD screen)
RMI	Remote Management Interface (the web interface)
SAN	Storage Area Network
SAS	Serial Attached SCSI
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
UID	Unit Identification
USB	Universal Serial Bus
WORM	Write Once, Read Many
WWNN	World-Wide Node Name
WWPN	World-Wide Port Name

ADDITIONAL PUBLICATIONS

For additional information about the Spectra Stack Library and its drives, refer to the publications listed in this section.

Spectra Stack Library

This guide and the following documents related to the Spectra Stack Library are available as PDF files on the Spectra Logic website at: *support.spectralogic.com/documentation.*

- The *Spectra Stack Library Installation and Quick Configuration Guide* provides instructions for installing and configuring basic library functions.
- The *Spectra Stack SCSI Developer's Guide* provides information about the SCSI Command set for the stack library.

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

- The Spectra Stack Library Release Notes and Documentation Updates provides the most up-to-date information about the Spectra Stack Library, drives, and media.
- The following Field Replacement Unit Instructions:
  - *Spectra Stack Spool Robotics Replacement Instruction*
  - *Spectra Stack Fan Replacement Instructions*
  - *Spectra Stack Power Supply Replacement Instructions*
  - *Spectra Stack Base-Exp Module Controller Replacement Instructions*
  - *Spectra Stack Base Bezel With OCP Replacement Instructions*
  - *Spectra Stack DC-DC Converter Replacement Instructions*
  - *Spectra Stack Magazine Replacement Instructions*
  - *Spectra Stack Rack Mount Instructions*
  - *Spectra Stack Base-Exp Chassis Replacement Instructions*
  - *Spectra Stack MigrationPass Instructions*

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*

For drive-specific information, search for the product name (for example, LTO 6) on the documentation page on the IBM website. You can also search the IBM Support Portal at: *http://www-947.ibm.com/support/entry/portal/Documentation*.

KMIP

See the documentation specific to your server.

BlueVision User Interface Screens

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

CHAPTER 1 - PRODUCT OVERVIEW

Built with maximum flexibility at its core, the Spectra Stack tape library meets your backup, archive, and perpetual storage requirements. Designed to be easily installed, expanded, and managed, the Spectra Stack is rated at 100% duty cycle - meaning it is built to perform in a 24/7 environment.

WARNING

Only trained personnel should operate this equipment. Read all documentation and procedures before installation or operation. This product is intended for installation and operation in a computer rack with the front and rear doors closed and secured. Only personnel with technical and product safety training should be provided access to the library. Such personnel are referred to as users throughout this document. Do not insert any tools or any part of your body into openings of an operating library.

SUPPORTED LIBRARY CONFIGURATIONS

All Spectra Stack library installations begin with the 6U controller module, with capacity for 80 tape cartridges and up to six half-height LTO tape drives, up to three full-height LTO tape drives, or a combination of half-height and full-height drives.

The Spectra Stack library is expandable, allowing a user to grow the tape storage capacity as data requirements increase. As data storage needs grow, the Spectra Stack library can also grow by adding one or more 6U expansion module(s). Each expansion module supports an additional 80 tape cartridges and an additional six half-height LTO tape drives or three full-height LTO tape drives.

Up to six expansion modules can be added to a controller module, bringing the total library capacity to 560 tape cartridges and 42 half-height drives, 21 full-height drives, or a combination of half- and full-height drives in a single 19-inch NEMA rack.

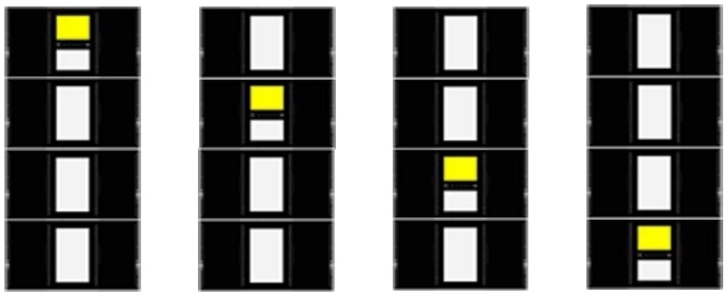
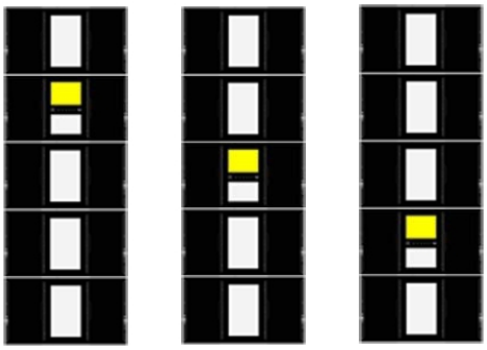
The controller module is depicted in this manual by the image on the left with the Operator Control Panel shown in yellow. Each expansion module is represented by the image on the right with a large clear viewing window in the center.

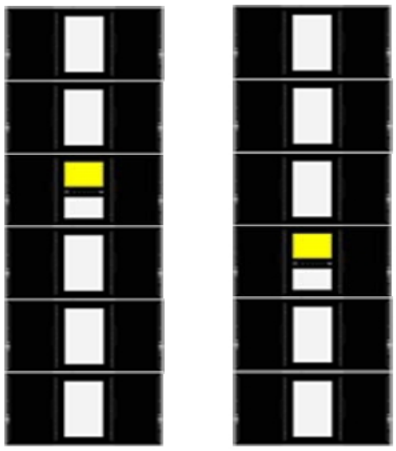
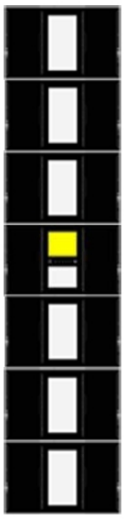
Figure 1 The controller module.

Figure 2 The expansion module.

Up to three expansion modules can be installed above and below the controller module. The table below shows the supported library configurations.

Module Quantity	Supported Library Configurations
1 Module Library • Controller Module	
2 Module Library • Controller Module • 1 Expansion Module	

Module Quantity	Supported Library Configurations
3 Module Library • Controller Module • 2 Expansion Modules	
4 Module Library • Controller Module • 3 Expansion Modules	
5 Module Library • Controller Module • 4 Expansion Modules	

Module Quantity	Supported Library Configurations
6 Module Library • Controller Module • 5 Expansion Modules	
7 Module Library • Controller Module • 6 Expansion Modules	

FRONT PANEL

This section describes the features accessible from the front panel of the library.

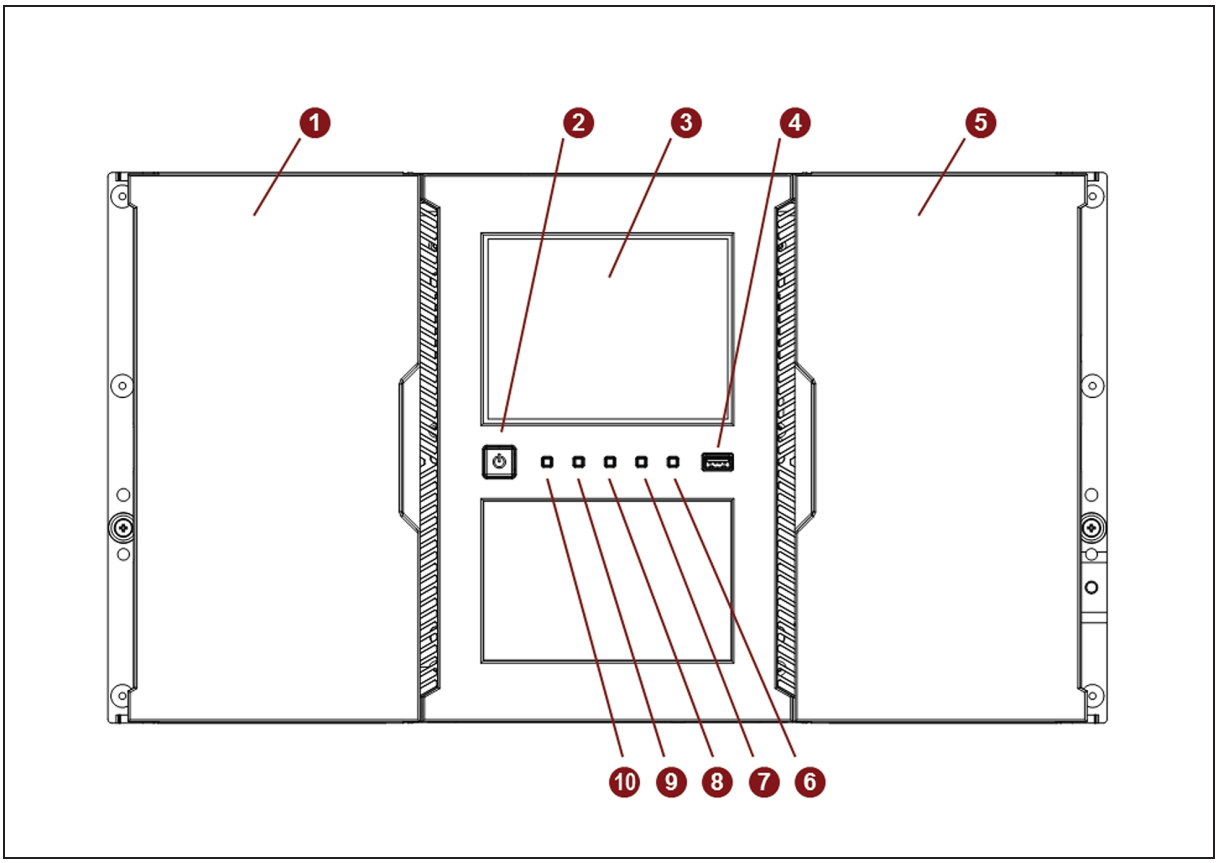


Figure 3 The front view of the Spectra Stack library.

Number	Component	Description
1	**Left Magazine Access Door**	Provides access to the magazine on the left side of the module.
2	**Power Button**	**Controller Module Only**
3	**Operator Control Panel (OCP)**	**Controller Module Only**
4	**USB Port**	**Controller Module Only**

Number	Component	Description
5	**EE Port/Right Magazine Access Door**	Provides access to the magazine and EE port on the right side of the module.
6	**Error LED - Amber**	**Controller Module Only** - This LED illuminates when the library detects an unrecoverable tape drive or library error and is not capable of operation. Details of the error are displayed on the front panel screen.
7	**Attention LED - Amber**	**Controller Module Only** - This LED illuminates when the library detects a condition which requires manual intervention, but the library can still perform most operations.
8	**Clean LED - Amber**	**Controller Module Only** - This LED illuminates when a tape drive cleaning is needed.
9	**Ready LED - Green**	**Controller Module Only** - This LED is steady green when the library is on, and blinks green when there is library robotics activity.
10	**Unit Identification LED - Blue**	**Controller Module Only** - The unit identification LEDs on the front and back of the controller module are controlled by a user through the OCP and RMI **Maintenance > UID LED Control** screen. These lights are helpful for locating the library in a data center.

REAR PANEL

This section describes the features accessible from the rear panel of the library.

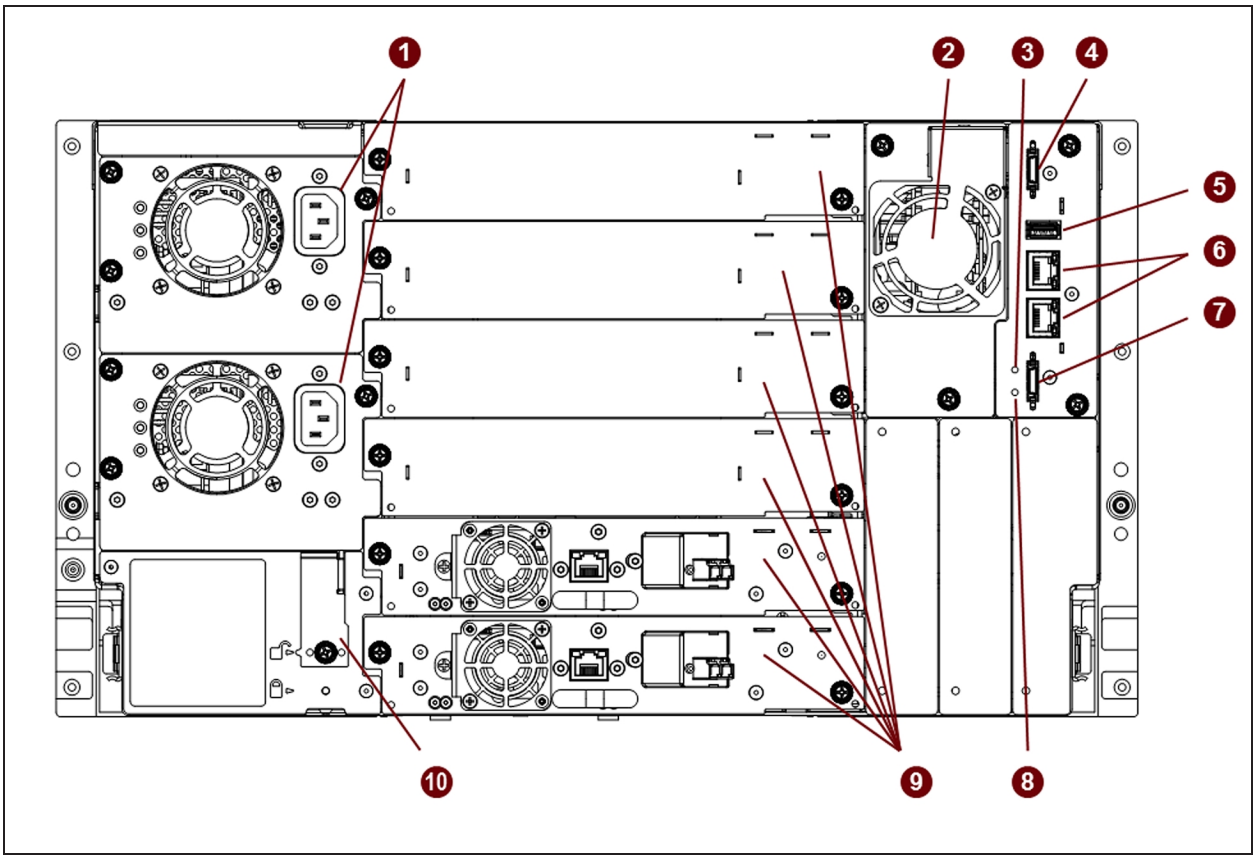


Figure 4 The rear view of the Spectra Stack library.

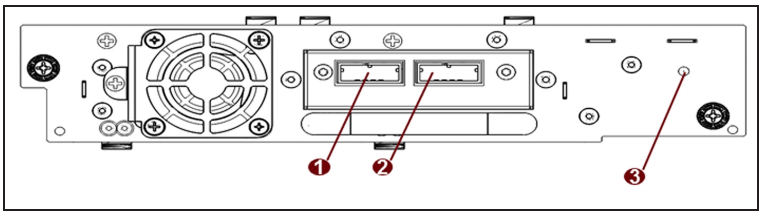
Number	Component	Description
1	**Power Supplies**	1 (standard) or 2 (redundant)
2	**Chassis Fan**	Provides cooling for the library module.
3	**Controller Health Status LED - Green**	Indicates the module controller is operating normally.
4	**Upper Expansion Module Connection Port**	If there is a module above this module, a cable connects from this port to the Lower Expansion Module Connection Port in the upper module.

Number	Component	Description
5	**USB Port**	**Controller Module Only**
6	**Ethernet Ports**	**Controller Module Only** - Only one Ethernet port is usable.
7	**Lower Expansion Module Connection Port**	If there is a module below this module, a cable connects from this port to the Upper Expansion Module Connection Port in the lower module.
8	**Unit Identifier LED - Blue**	
9	**Drive Bays**	Half-height drive bays shown. Full-height drives use the space of two half-height drive bays.
10	**Module Alignment Mechanism**	When there is an expansion module below this module, the alignment mechanism is extended to lock into the lower module.

TAPE DRIVE BACK PANELS

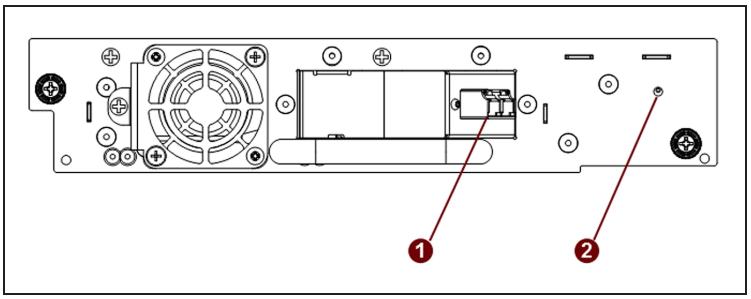
This section describes the elements of LTO tape drives used in the library.

IBM LTO-5/6/7/8/9/10 Half-Height SAS Drive



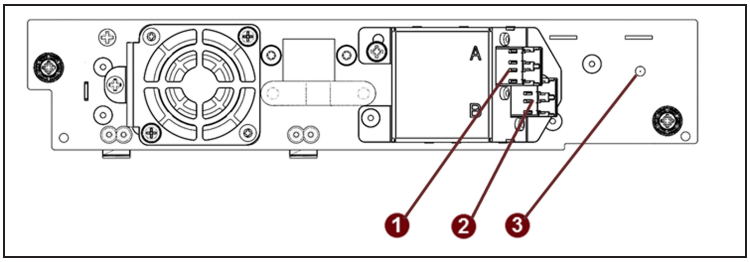
1	SAS Port A
2	SAS Port B
3	Tape Drive Power LED - Green

IBM LTO-5/6/7/8/9/10 Half-Height Single FC Port Drive



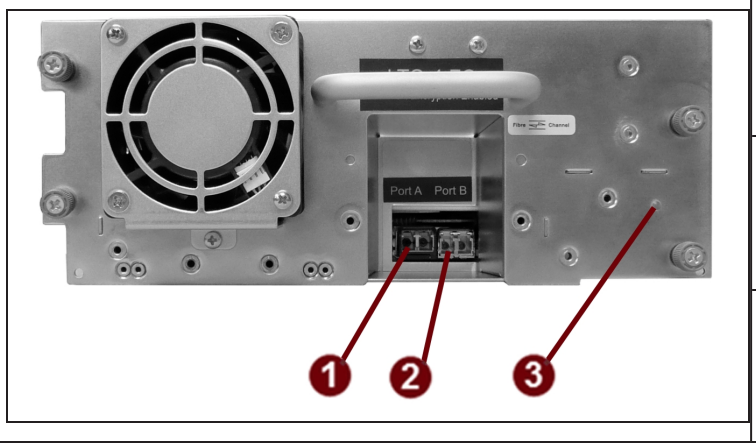
1	Fibre Channel Port A
2	Tape Drive Power LED - Green

IBM LTO-5/6/7/8/9/10 Half-Height Dual FC Port Drive



1	Fibre Channel Port A
2	Fibre Channel Port B
3	Tape Drive Power LED - Green

IBM LTO-9 & LTO-10 Full-Height Dual FC Port Drive



1	Fibre Channel Port A
2	Fibre Channel Port B
3	Tape Drive Power LED - Green

POWER SUPPLY BACK PANEL

This section describes the power supply LEDs.

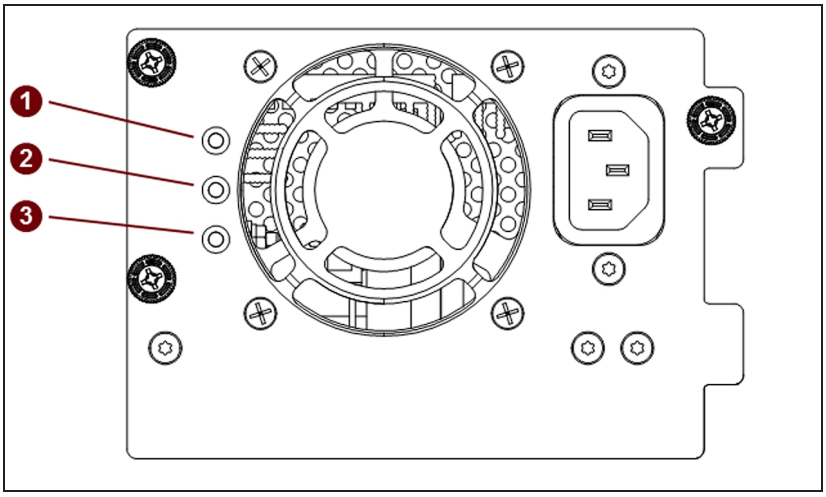


Figure 5 The library power supply LEDs.

Number	LED Color	Meaning
1	White	AC power is connected, but the library is powered off.
2	Amber	Power supply fault condition. This can occur if the power supply fan fails, or if the temperature or electrical power output is outside of specification.
3	Green	Module powered on.

Element Numbering

The library generally displays the logical numbering of modules, storage slots, and drives, from the bottom of the library to the top.

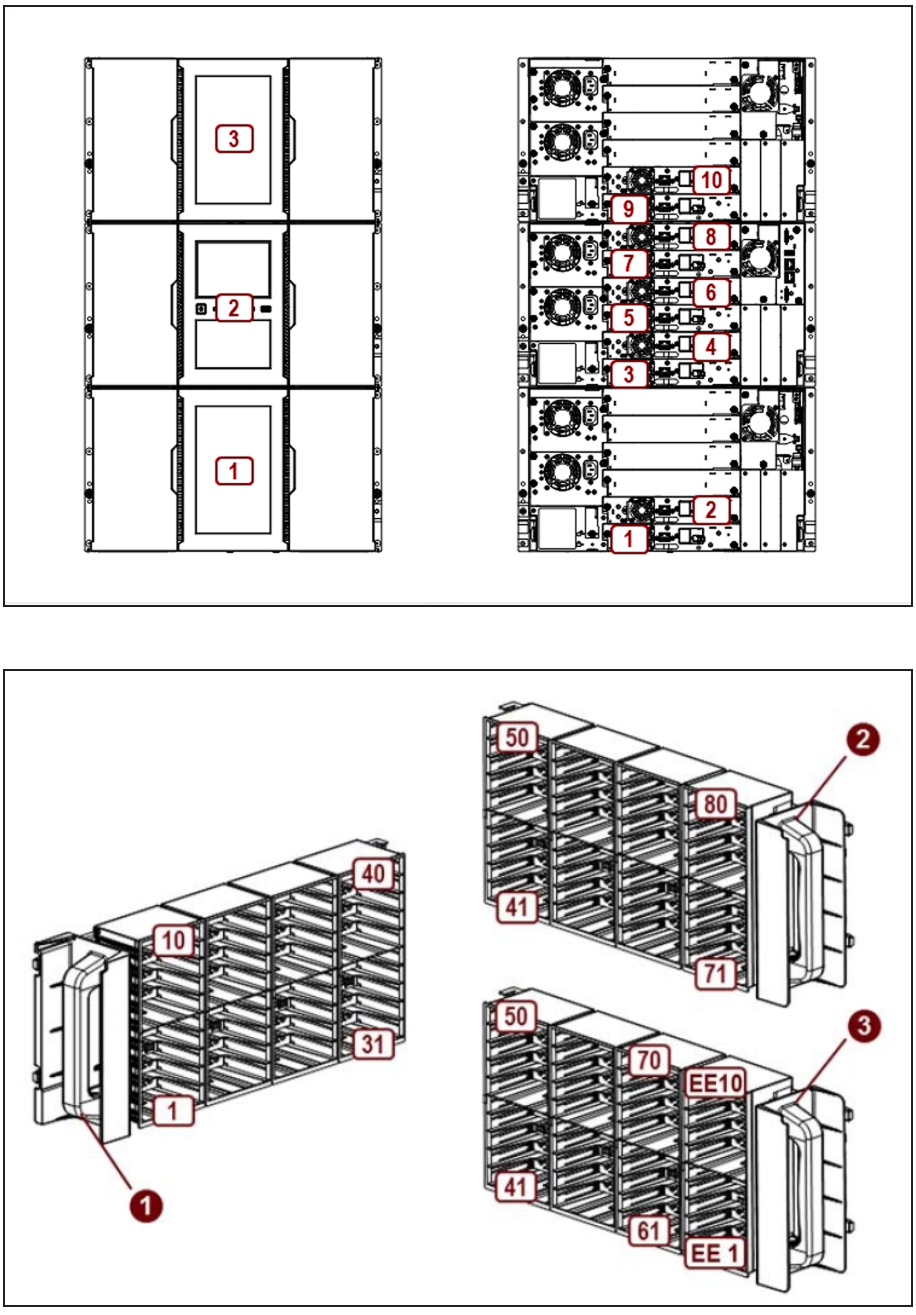


Figure 6 Example of library element numbering.

Number	Type of Magazine Description
1	Left magazine
2	Right magazine with EE port disabled
3	Right magazine with EE port enabled

ENCRYPTION

Encryption protects data written to tape from unauthorized access and use. The data is changed into a form that cannot be read until it is deciphered with the key used to encrypt the data.

LTO-5 and later generation tape drives include hardware that is capable of encrypting data while writing, and decrypting data when reading. Hardware-based data encryption can be used with or without compression while maintaining the full speed and capacity of the tape drive and media. LTO tape drives use the AES-256 encrypting algorithm to protect your data.

To use KMIP key management, you need the associated license key and a server with KMIP software.

The tape drives can read encrypted data from and write encrypted data to some earlier generation media. See Read and Write Compatibility on page 44.

TAPE CARTRIDGES

Use the Ultrium data cartridges designed for your model of drives. All drive generation use the Ultrium universal cleaning cartridge

LTO Media Generation	Native Capacity (Compressed Capacity)
LTO-5 and LTO-5 WORM	1.5 TB (3 TB [a])
LTO-6 and LTO-6 WORM	2.5 TB (6.25 TB [b])
LTO-7 and LTO-7 WORM	6 TB (15 TB [b])
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])
LTO-10 and LTO-10 WORM	30 TB (75 TB [b])

Note: LTO-5 and later tape drives support both rewriteable and WORM data cartridges. Write-Once, Read-Many (WORM) data cartridges provide an enhanced level of data security against accidental or malicious alteration of data on the tape cartridge. The WORM data cartridge can be appended to maximize the full capacity of the tape cartridge, but you cannot erase or overwrite data on the cartridge.

[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.

Using and Maintaining Tape Cartridges

CAUTION Do not degauss LTO data cartridges! These data cartridges are pre-recorded with a magnetic servo signal. This signal is required to use the cartridge with LTO tape drives. Keep magnetically charged objects away from the cartridge.

To ensure the longest possible life for your data cartridges, follow these guidelines:

- Use only the data cartridges designated for your drives. See Read and Write Compatibility on page 44.
- Clean the tape drive when the Clean drive LED is illuminated.
- Use only Ultrium Universal cleaning cartridges.
- Be careful not to drop a cartridge. Excessive shock can damage the internal contents of the cartridge or the cartridge case itself, making the cartridge unusable.
- Do not expose data cartridges to direct sunlight or sources of heat, including portable heaters and heating ducts.
- The operating temperature range for data cartridges is 50° F to 95° F (10° C to 35° C). The storage temperature range is -40° F to 140° F (-40° C to 60° C) in a dust-free environment in which relative humidity is always between 20% and 80% (non-condensing).
- If a data cartridge is exposed to temperatures outside the specified range, acclimate the cartridge at room temperature for the same length of time it was exposed to extreme temperatures or 24 hours, whichever is less.
- Do not place data cartridges near sources of electromagnetic energy or strong magnetic fields such as computer monitors, electric motors, speakers, or X-ray equipment. Exposure to electromagnetic energy or magnetic fields can destroy data and the embedded servo code written on the media by the cartridge manufacturer, which can render the cartridge unusable.
- Place identification labels only in the designated area on the cartridge.

Labeling Tape Cartridges

The library contains a barcode reader that reads the tape labels and stores the barcode data as part of the library inventory. The library then provides the inventory information to the host application, OCP, and RMI. Having a barcode label on each tape cartridge enables the barcode reader to identify the cartridge quickly, thereby speeding up inventory time.

IMPORTANT The tape library does not support unlabeled media. Make sure every cartridge has a barcode label in place.

IMPORTANT All barcode labels must be checksummed or non-checksummed. You cannot mix the two types in the library.

A proper barcode label includes the media identifier in the last two characters of the barcode. The library will not load an incompatible cartridge, based on the barcode media identifier, into a tape drive. For example, the library will not load a cartridge labeled as LTO-3 into an LTO-6 tape drive. This saves the time needed to load the cartridge and have the tape drive reject it.

Though not recommended, disabling barcode checking in the **Configuration > Ignore Barcode Media ID** screen allows all media moves regardless of the barcode media identifier.

Your host software may need to keep track of the following information via the associated barcode:

- Date of format or initialization
- Tape's media pool
- Data residing on the tape
- Age of the backup
- Errors encountered while using the tape (to determine if the tape is faulty)

IMPORTANT Misusing and misunderstanding barcode technology can result in backup and restore failures. Use only high quality labels. Self-printed labels are not recommended as they are often a source of barcode reading issues.

IMPORTANT The barcode label should only be applied as shown, with the alphanumeric portion facing the hub side of the tape cartridge. Never apply multiple labels onto a cartridge because extra labels can cause the cartridge to jam in a tape drive.

LTO tape cartridges have a recessed area located on the face of the cartridge next to the write-protect switch. Use this area for attaching the adhesive-backed barcode label. Only apply labels as shown:

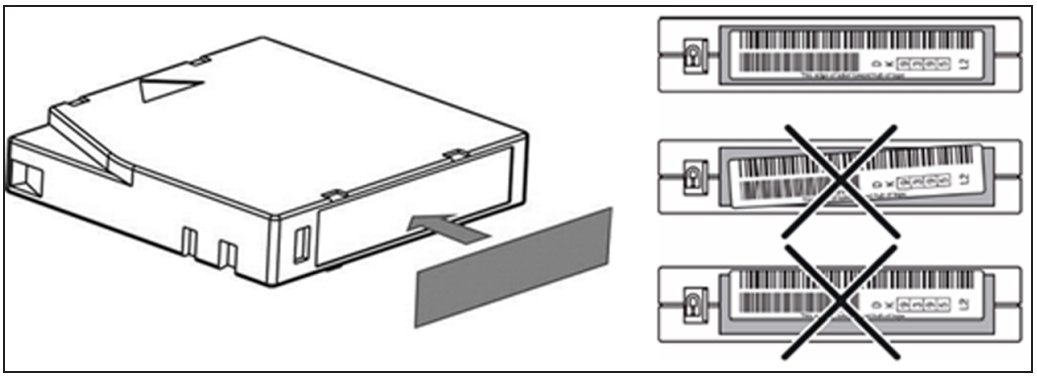


Figure 7 Tape cartridge barcode location.

Note: For detailed information on tape barcode specifications, see Barcode Label Specifications on page 283.

Write Protecting Tape Cartridges

All rewriteable data cartridges have a write-protect switch to prevent accidental erasure or overwriting of data. Before loading a cartridge into the library, make sure the write-protect switch on the front of the cartridge is in the desired position.

- Slide the switch to the left to allow the drives to write data to the cartridge.
- Slide the switch to the right to write-protect the cartridge. An indicator, such as a red mark or small padlock, is visible showing that the cartridge is write-protected.

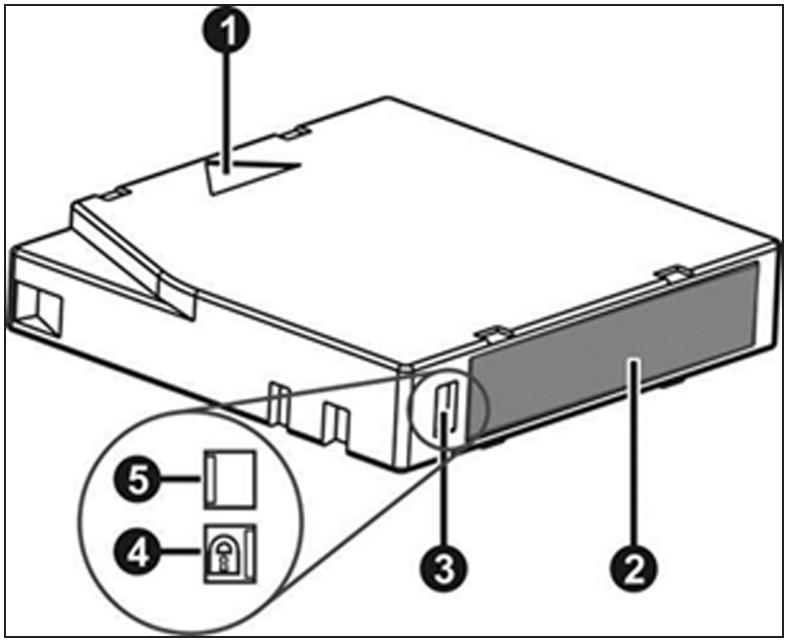


Figure 8 Tape cartridge features.

Callout	Feature
1	Insertion Arrow
2	Barcode Label
3	Write-Protect Switch
4	Write-Protected
5	Write-Enabled

Read and Write Compatibility

Drive Gen	LTO-5 Media	LTO-6 Media	LTO-7 Media	M8 Media	LTO-8 Media	LTO-9 Media	LTO-10 Media
LTO-5	**Read/write**	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported
LTO-6	**Read/write**	**Read/write**	Not supported	Not supported	Not supported	Not supported	Not supported
LTO-7	*Read only*	**Read/write**	**Read/write**	Not supported	Not supported	Not supported	Not supported
LTO-8	Not supported	Not supported	**Read/write**	**Read/write**	**Read/write**	Not supported	Not supported
LTO-9	Not supported	Not supported	Not supported	Not supported	**Read/write**	**Read/write**	Not supported
LTO-10	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	**Read/write**

INTEGRATION WITH A BLACKPEARL SYSTEM

Spectra Stack libraries can be used with BlackPearl systems running BlackPearl OS 4.1.2, or later. For information on using a Stack library in a BlackPearl system, see the *Spectra BlackPearl User Guide*.

CHAPTER 2 - USING THE BLUEVISION INTERFACE

This chapter provides information on using the BlueVision interface.

The library provides two main interfaces:

- **Operator Control Panel (OCP)** - With the OCP, you can monitor, configure, and control the library from the LCD screen on the controller module.
- **Remote Management Interface (RMI)** - With the RMI, you can monitor, configure, and control the library from a web browser. The RMI hosts a dedicated, protected website that displays a graphical representation of the library.

The OCP and RMI are similar in design and functionality.

Before using the RMI, you must configure the library network settings and set the administrator password with the OCP. This is typically done using the Initial Configuration Wizard, see Using the Initial Configuration Wizard on page 59.

When possible, it is recommended that the RMI be used as the primary library interface because the web interface provides access to additional features, such as configuring SNMP, IPv6, encryption, and partitions, includes online help, and is easier to use.

USING THE OPERATOR CONTROL PANEL

The OCP has a power button, an LCD touch screen, five indicator LEDs, and a USB port (see Figure 3 on page 30). With the OCP you can monitor, configure, and operate most library functions from the library LCD screen on the controller module. To navigate the OCP, click on the LCD touch screen.

Front Panel LED Indicators

Indicator	Meaning
Module ID	Blue when activated. The unit identification (UID) LEDs are controlled by the user through the OCP and RMI **Maintenance > UID LED Control** screen. The UIDs on the OCP and back panel UID are activated and deactivated together. The UIDs are helpful for locating the library in a data center.
Ready	Steady green when the library is on, and blinking green when there is library robotic assembly activity.
Clean	Amber when a tape drive requires cleaning.
Attention	Amber blinking if the library detects a condition for which user attention is necessary, but which does not prevent the library from performing most operations.
Error	Amber if an unrecoverable tape drive or library error occurs. A corresponding error message displays on the LCD screen. User intervention is required; the library is not capable of performing some operations.

USING THE REMOTE MANAGEMENT INTERFACE

With the RMI, you can monitor, configure, and operate most library functions from a web browser.

IMPORTANT Starting with BlueVision 2.60, you must use HTTPS to connect to the library using RMI.

To start the RMI, open the latest version of a supported HTML browser and enter the IP address of the library in the browser's address bar. Supported browsers include Internet Explorer, Firefox, Chrome, and Safari.

IMPORTANT Check the online help in the RMI for additional information. The help pages are updated with firmware updates and often contain up-to-date technical details that might not be contained in this document. To access RMI help, click the **?** icon on the right side of the RMI top banner.

LIBRARY USER TYPES

The library offers four types of user, each with different levels of access to library functions.

- **Administrator** – The administrator user has access to all functionality except for the log configuration, service features, and encryption features.

IMPORTANT By default, the administrator password is not set. You must set the administrator password from the OCP (see Configuring the Library on page 57) before you can access the administrator functions on the RMI.

- **User** – The user account provides access to status information, but not configuration, maintenance, or operation functions.

IMPORTANT By default, the user password is not set.

- **Service** – This user is for use by service personnel only. The service password is set at the factory. To access the service features of the library, both the administrator and service passwords must be entered.
- **Security** - The security user has access to all administrator functionality and can also configure security features and change the security user password.

IMPORTANT By default, the security password is set to `security`. You must change the security password from the OCP before the account can be used from the RMI (see Configuring the Library on page 57).

LOGGING INTO THE LIBRARY

Use the instructions in this section to log into the library. The process is similar when using either the OPC or RMI.

1. Access the user interface:
   - **Using the OCP** - touch the screen to clear the screen saver and display the login screen.
   - **Using the RMI** - open a web browser and enter the HTTPS IP address of the library in the browser address bar.

   The Login screen displays.

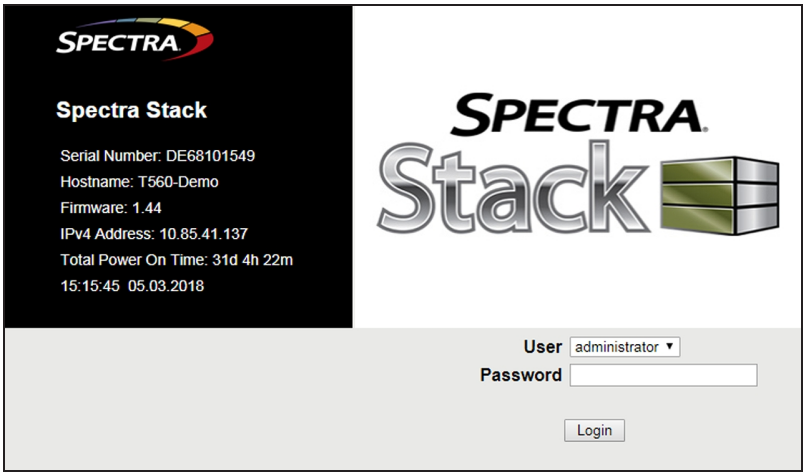


Figure 9 The Login screen.

2. Using the drop-down menu, select the desired **User**.
3. If necessary, enter the **Password** for the user.
4. Click **Login**.
5. If the user has two-factor authentication enabled, enter the **TOTP**(Time-Based One-Time Password) six digit code from the authenticator application on your host computer or phone, then click **Login**.

USING THE LIBRARY MAIN SCREEN

The library main screen is organized into the following regions:

- **Top Banner** - Contains the home button and displays the overall library status and information about the library and the current user. See Top Banner Elements on the next page.
- **Left Pane** - Displays the library identity and all module statuses. See Left Pane Elements on page 53.
- **Right Pane** - (RMI only) Displays a log of recent events or a navigation menu after clicking one of the center buttons. See Right Pane Elements on page 55.
- **Center Pane** - Provides access to operate and configure the library, and to view additional status information. See Center Pane Elements on page 55.

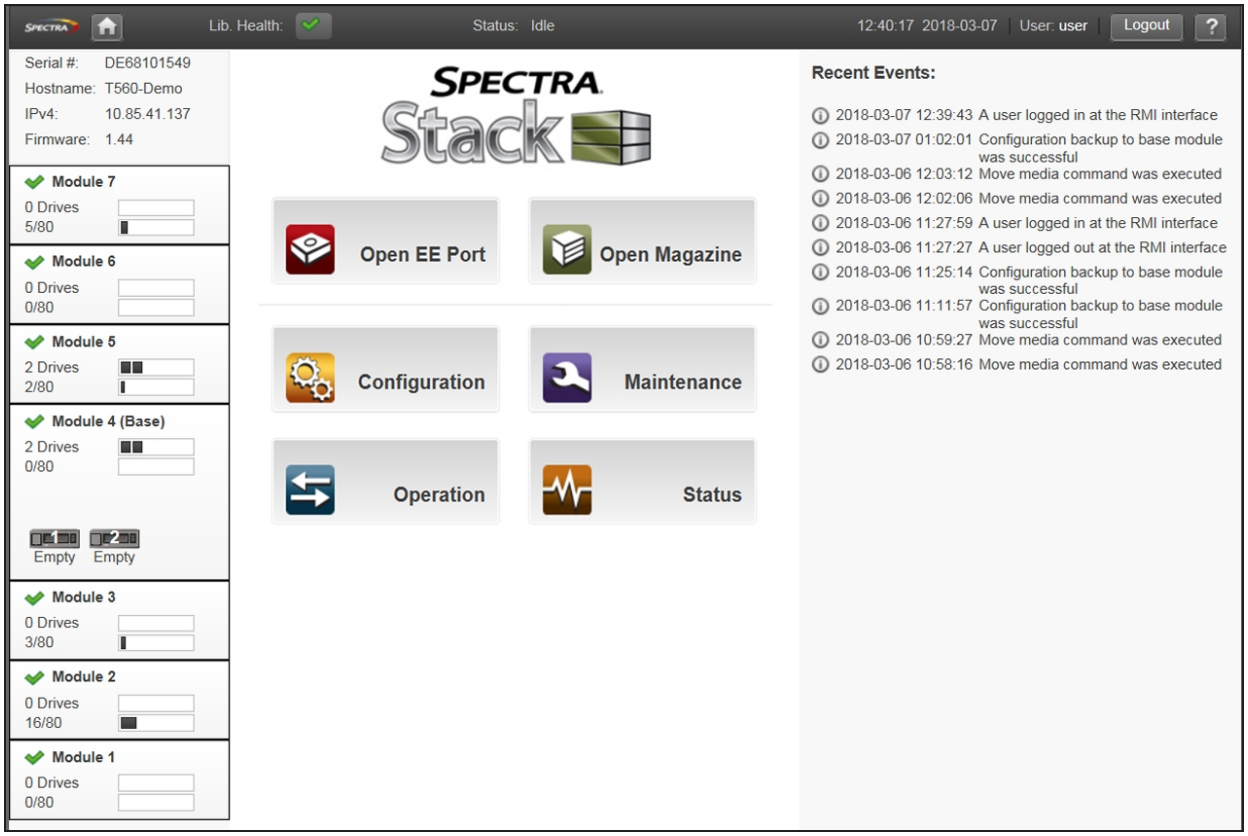


Figure 10 Spectra Stack main screen.

Top Banner Elements

Figure 11 The BlueVision top banner.

Icon	Meaning
Home Icon	Returns to the library main screen.
Library Health	An icon indicating the overall health status of the library. **OK** - The green check mark icon indicates the library is fully operational. **Warning** - The yellow exclamation point icon indicates that user attention is necessary, but the library can continue most operations. **Error** - The red X icon indicates that the library experienced an error that prevents it from continuing normal operations, and user intervention is required.
Status	The status of the library robotics: • **Idle** - The library robotics is ready to perform an action. • **Moving** - The library robotics is moving a cartridge. • **Scanning** - The library robotics is performing an inventory of cartridges. • **Offline** - The library robotic assembly has been taken offline by the library.
Library Time & Date	Helpful when analyzing event logs and support tickets, and might be needed when contacting support.
User	The user account for this session.
Logout	Logs out of this session.
?	Accesses online help. When using RMI, you can search the online help for a specific term by pressing CTRL+F on the keyboard.

Left Pane Elements

The left pane displays general library information and module status information.

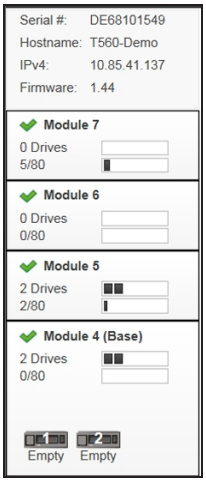


Figure 12 The BlueVision left pane.

Library Information

Parameter	Meaning
Serial #	The controller module serial number.
Hostname	The library hostname.
Network Configuration	The internet protocol version (IPv4, IPv6, or both) and IP address.
Firmware	The current library firmware version.

Module Status Overview

The module status overview provides a summary of each module's configuration and health. Selecting a module displays additional information.

Parameter	Meaning
Module Health Icon	 **OK** - The green check mark icon indicates the library is fully operational.  **Warning** - The yellow exclamation point icon indicates that user attention is necessary, but the library can continue most operations.  **Error** - The red X icon indicates that the library experienced an error that prevents it from continuing normal operations, and user intervention is required.
Module Number	Modules are numbered based on their location in the physical library. The bottom module is Module 1. The controller module is annotated with "(Base)".
Drive Status	The number of drives installed in the module and the health of each drive. Click the drive to display drive configuration and status information in the center pane. • A **black** square indicates that the drive is fully operational and that no user intervention is required. • A **yellow** square indicates that user attention is necessary, but that the drive can still perform most operations. • A **red** square indicates that user intervention is required or the drive is not capable of performing some operations.
Magazine Slot Usage	The number of cartridge slots used and the number available formatted as *xx*/*yy* where *xx*= slots used and *yy*=slots available.
Drive Operation Status	The current drive activity for each drive in the module. The drive operation status is only displayed for the selected module. • **Write** - The drive is performing a write operation. • **Read** - The drive is performing a read operation. • **Idle** - A tape cartridge is in the drive but the drive is not performing an operation. • **Empty** - The drive is empty. • **Encryp** - The drive is configured to read and write encrypted data.

Right Pane Elements

The right pane displays a log of recent events or a navigation menu after clicking one of the center buttons described in Center Pane Elements below.

Center Pane Elements

Figure 13 The BlueVision home page center pane.

Selection	Meaning
Open EE Port (Administrator or Security user only)	Click to access the **Operations > Open EE Port** screen to see the status of EE port(s) and select an EE port to open. EE ports must be enabled before the slots can be used as EE ports. See Enabling or Disabling EE Ports on page 82.
Open Magazine (Administrator or Security user only)	Click to access the **Operation > Open Magazine** screen to select a magazine to open. Only one magazine in the library can be open at a time. See Opening a Magazine on page 154.
Configuration (Administrator or Security user only)	Click to configure the library system, network, drives, EE ports, partitions, encryption, user accounts, and web management settings. See Configuring the Library on page 57.

Selection	Meaning
Maintenance (Administrator or Security user only)	Click to access maintenance functions including running system tests, collecting logs and traces, upgrading software, downloading drive logs, rebooting the system, rebooting drives, controlling the UID LEDs, and moving the robotic assembly to the control module. See Maintaining the Library on page 197.
Operation (Administrator or Security user only)	Click to access operation functions including moving media, cleaning drives, rescanning inventory, and forcing drive media ejection. See Operating the Library on page 150.
Status	Click to access cartridge inventory, status information, and Media Lifecycle Management (MLM). See Viewing Library Status on page 159 and Configuring and Using Media Lifecycle Management on page 179.

CHAPTER 3 - CONFIGURING THE LIBRARY

This chapter contains instructions for configuring the Spectra Stack library. Before using this chapter, install the library using the *Spectra Stack Library Quick Start Guide*.

USING THE INITIAL CONFIGURATION WIZARD

The Initial Configuration Wizard guides you through setting the administrator password, configuring the time zone, date and time, and library network settings, and then starting an initial system test. You can skip items and stop the wizard at any time. Once you have configured the network settings and set the administrator password from the OCP, you can initiate the wizard from the RMI or use the OCP to complete the remaining configurations. For a detailed description of the Initial Configuration Wizard, see the *Spectra Stack Library Quick Start Guide*.

SAVING, RESTORING, AND RESETTING THE LIBRARY CONFIGURATION

You can save the library configuration settings to a file, restore the settings, or reset the library configuration to the default settings from the **Configuration > System > Save/Restore Configuration** screen. The saved configuration database makes it easier to recover the library configuration if you need to replace the controller module or the controller in the controller module.

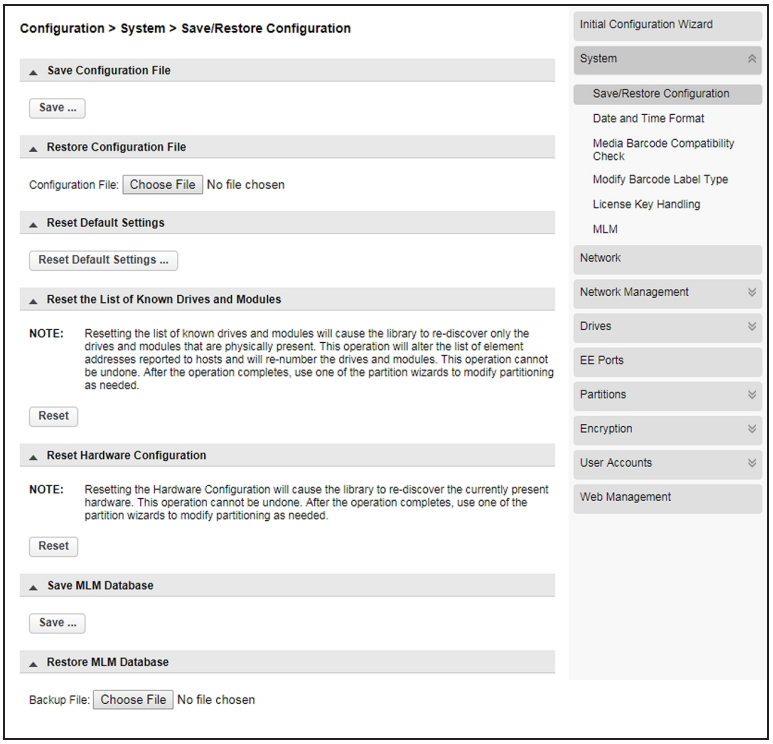


Figure 14 The Save/Restore System Configuration screen.

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.

Note: The library configuration backup does not contain the MLM database. To backup the MLM database, see Backup the MLM Database on page 194.

The library configuration backup can be generated using the library operator control panel to save the file to a USB device, or using the RMI to download the backup file.

The following settings are not saved in the backup configuration file:

- The administrator password
- Date and time
- Library hostname
- KMIP certificates
- License keys
- Library MAC address
- Library, controller, and chassis serial numbers
- Robot calibration data
- Operator control panel calibration data
- Library hardware configuration

Note: If you have previously saved a configuration backup file and want to use the file to restore the library configuration, see Restoring the Library Configuration on the next page.

Saving the Library Configuration

1. Login to the library as a user with administrator privileges.
2. Navigate to the **Configuration > System > Save/Restore Configuration** screen as shown Figure 14.
3. If necessary, click **Save Configuration File** to expand the section.
4. If you are using the OCP, insert a USB device into one of the USB ports on the controller module.
5. Click **Save**.

   Note: It takes approximately three minutes for the library to display **Download** and **Cancel** buttons.

   The destination location depends on how you are accessing the library:

   - **RMI** — (RMI only) Downloads the configuration file through the browser to the system running the RMI.
   - **USB Device** — (OCP only) Downloads the configuration file to a USB device inserted into the USB port on the front or the back of the library.
6. Click **Download**.

Verify the Configuration Backup File

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 a host computer.
2. Examine the list of files on the USB device and locate the ZIP file containing the system configuration backup. The file is named: syslog-*LibraryName-PackageLevel-Timestamp*.ZIP.
3. Open the ZIP file and confirm the file "details.bin" is present and greater than 0 bytes.

Note: The ZIP file also contains text files of different library messages. If no messages of a given type are present in the library, the log for that message type is 0 bytes.

When Saved to a Host Computer

1. Locate the ZIP file containing the system configuration backup. The file is named: syslog-*LibraryName-PackageLevel-Timestamp*.ZIP.
2. Open the ZIP file and confirm the file "details.bin" is present and greater than 0 bytes.

Note: The ZIP file also contains text files of different library messages. If no messages of a given type are present in the library, the log for that message type is 0 bytes.

Restoring the Library Configuration

Note: Restoring the configuration from a saved configuration file restores passwords for the users with security and user roles, but does not restore an administrator user password.

1. Login to the library as a user with administrator privileges.
2. Navigate to the **Configuration > System > Save/Restore Configuration** screen.
3. If necessary, click **Restore Configuration File** to expand the section.

4. If you are using the OCP to restore the configuration file from a USB device, copy the configuration file you want to restore onto the USB device and remove any other configuration files from the USB device.

   Note: If multiple library configuration backups are present on the USB device, the library uses the most recent backup to restore the configuration.

   Insert the USB device containing the configuration file into one of the USB ports on the controller module.

5. Select the source location:

   - **RMI** — (RMI only) Restores the configuration file from the computer running the RMI. Select **Choose File** and use your web browser to select the configuration file you want to restore.
   - **USB Device** — (OCP only) Restores the configuration file from a USB device inserted into the USB port on the front or the back of the library.

6. Click **Upload File & Restore**. The library reboots to restore the configuration.

Resetting to the Default Settings

To reset the library configuration to the default settings, you must be logged in as the Administrator or Security user.

1. Log in as the security user.
2. Navigate to the **Configuration > System > Save/Restore Configuration** screen shown above.
3. If necessary, click **Reset Default Settings** to expand the section.
4. Click **Reset Default Settings**.

   For the detailed listing of the default settings, see Default Settings on page 279.

CONFIGURING THE DATE AND TIME FORMAT

You can configure the date and time format, the current date and time, and an SNTP server from the **Configuration > System > Date and Time Format** screen.

Note: The library does not adjust its time for daylight savings; the time must be adjusted manually.

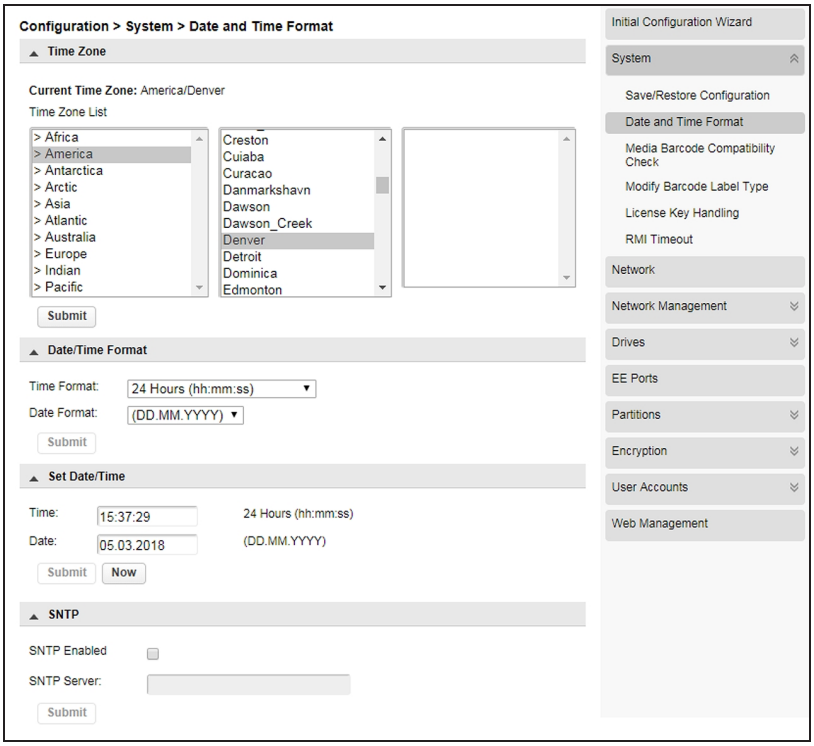


Figure 15 The Date and Time Format screen.

Setting the Time Zone

1. On the Date and Time Format screen, if necessary, click **Time Zone** to expand the section.

   A list of continents, countries, and regions is displayed. When an item proceeded with '>', for example '>US', is selected, a submenu is displayed in the next column.

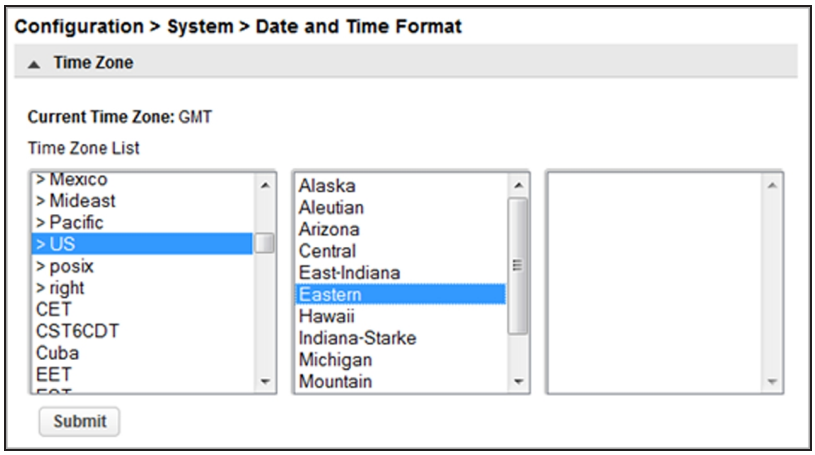


Figure 16 Select the time zone.

2. Expand the time zone list, as necessary, until a location with the appropriate time zone is visible.
3. Select a location with the appropriate time zone.
4. Click **Submit**.

Setting the Date and Time Format

1. On the Date and Time Format screen, if necessary, click **Date/Time Format** to expand the section.

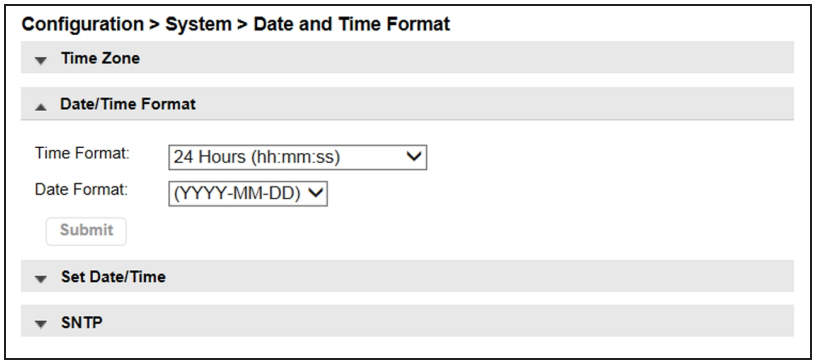


Figure 17 Select the date and time format.

2. Select a **Time Format** (12 Hours or 24 Hours).
3. Select a **Date Format**:

   For example, February 28, 2018 is displayed as:

- DD.MM.YYYY - 28.02.2018
- MM/DD/YYYY - 02/28/2018
- YYYY-MM-DD - 2018-02-28

4. Click **Submit**.

Setting the Date and Time

1. On the Date and Time Format screen, if necessary, click **Set Date/Time** to expand the section.

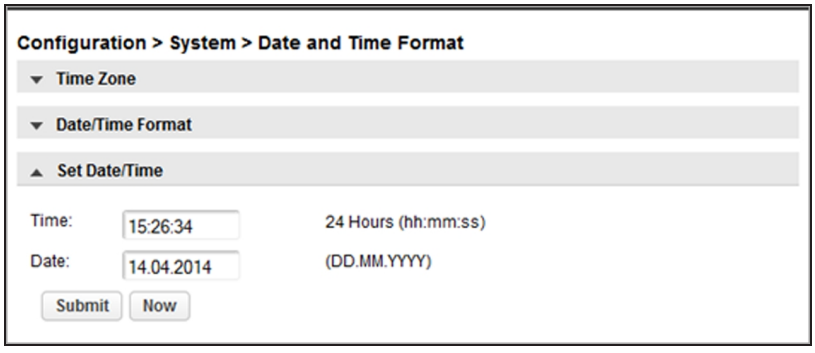


Figure 18 Set the date and time.

2. Set the time and date.

   To set the time and date manually:

   a. Enter the time in the configured time format.

   b. Enter the date or select it from the calendar.

   To synchronize the time and date with the computer running the browser, click **Now**.

3. Click **Submit**.

Enabling SNTP (Simple Network Time Protocol) Synchronization

To enable SNTP, the library must have network access to an SNTP server.

Note: If you plan to enable two-factor authentication for a user(s), you must enable SNTP before you can use two-factor authentication.

1. On the Date and Time Format screen, if necessary, click **SNTP** to expand the section.

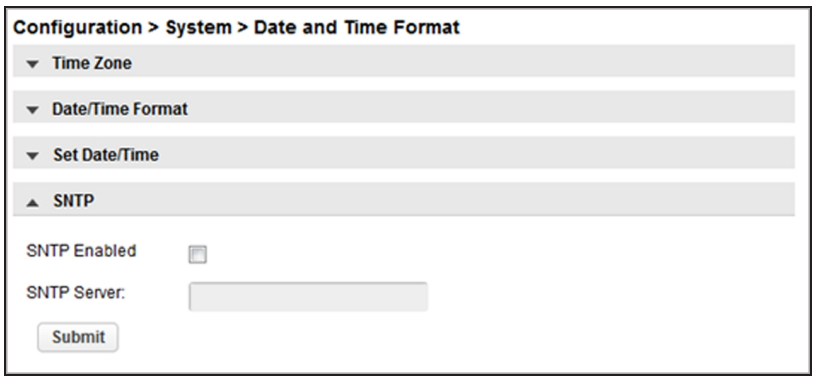


Figure 19 Enable SNTP.

2. Select the **SNTP Enabled** check box.
3. Enter the **SNTP Server** address.
4. Click **Submit**.

Configuring Media Barcode Compatibility Checking

The barcode media identifier is the last two characters of the barcode. The library uses the media identifier to verify the media is compatible with the tape drives installed. If the last two characters of the barcode do not match to any known identifier, then barcode is non-standard, and the barcode compatibility check is not possible.

When **Barcode Media ID Restriction** is enabled, the library fails a move of an incompatible tape cartridge into a tape drive. It is enabled by default. For example, an LTO-8 labeled cartridge is not allowed to move into an LTO-6 tape drive. Unknown media is treated as compatible by the library.

When **Barcode Media ID Restriction** is disabled, the library does not check the compatibility of a tape cartridge with the tape drives before moving it. If the cartridge is incompatible with the tape drive, the drive generates an error.

Note: It is strongly recommended that all cartridges have barcode labels with the correct media identifier, and that the **Barcode Media ID Restriction** is enabled.

On the **Configuration > System > Media Barcode Compatibility Check** screen, select or clear the **Barcode Media ID Restriction** and click **Submit**.

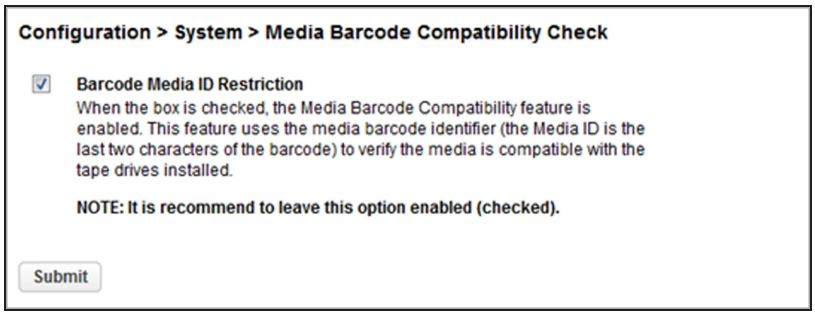


Figure 20 The Media Barcode Compatibility Check screen.

MODIFY BARCODE LABEL CHECKSUM TYPE

You can select the checksum behavior from the **Configuration > System > Modify Barcode Label Type** screen. You cannot mix checksummed and non-checksummed barcodes in a library. Checksummed barcodes are selected by default.

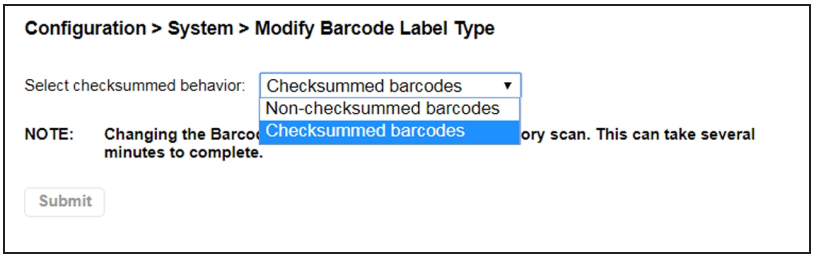


Figure 21 The Modify Barcode Label Type screen.

From the drop-down menu, select whether the library uses **Non-checksummed barcodes** or **Checksummed barcodes**, and then click **Submit**. Changing the setting initiates an inventory scan which can take several minutes to complete.

ADD A LICENSE KEY

1. To add a license key, navigate to the **Configuration > System > License Key Handling** screen.

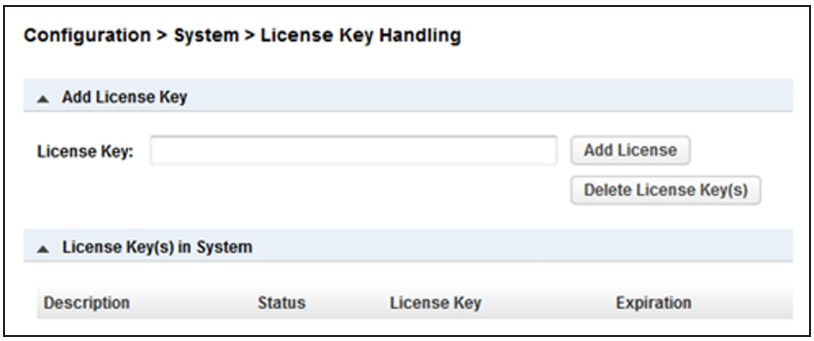


Figure 22 The License Key Handling screen.

2. If necessary, click **Add License Key** to expand the section.
3. Enter the license key. The license key needs to have a length of 15 characters.
4. Click **Add License.**

Note: The button for deleting license key(s) is only available with the Service login.

CONFIGURING THE LIBRARY NETWORK SETTINGS

You can configure the library network settings from the **Configuration > Network** screen.

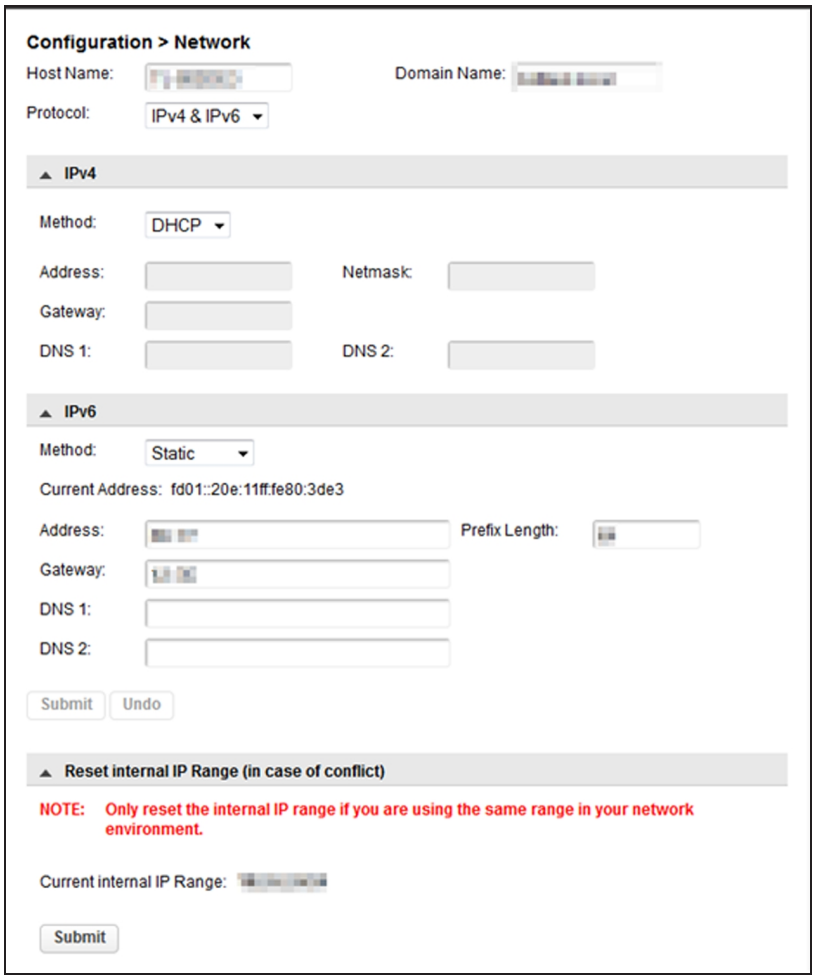


Figure 23 The Configuration > Network screen.

Note: It may be helpful to have your System Administrator assist you in configuring the network settings.

1. If desired, enter a new **Host Name**.
2. If desired, enter a **Domain Name**.

3. Using the **Protocol** drop-down menu, select IPv4, IPv6, or both.

- If you selected IPv4 or IPv4 & IPv6:
  - i. If necessary, click **IPv4** to expand the section.
  - ii. Using the **Method** drop-down menu, select either DHCP or Static addressing.
  - iii. If you are configuring a static IP address, enter the **Address**, **Netmask**, and **Gateway** addresses.
  - iv. If desired, enter **DNS** server information.
- If you selected IPv6 or IPv4 & IPv6:
  - i. If necessary, click **IPv6** to expand the section.
  - ii. Using the Method drop-down menu, select Static or Stateless.
  - iii. If you are configuring a static IP address, enter the **Address**, **Prefix Length**, and **Gateway**.
  - iv. If desired, enter **DNS** server information.

4. Click **Submit**.

IMPORTANT To view the network settings set using the DHCP or Stateless method, use the OCP and see Viewing Network Status on page 176.

Note: If you are using the RMI to access the Spectra Stack library and you have changed the IP address, you lose your connection to the user interface when you click **Submit**. To re-establish the connection, enter the new IP address in your browser and log in again.

RESET THE INTERNAL IP RANGE

For internal communication between modules, the tape library uses an Ethernet connection with an internal IP address range. To prevent any conflict between the internal IP address range and the external IP addresses, it is required to select the internal IP range before the tape library connects to the external Ethernet network.

Use the following instructions if you need to change the internal IP range after its initial configuration during the library installation:

1. Navigate to the **Configuration > Network** screen.
2. If necessary, click **Reset Internal IP Range (in case of conflict)** to expand the section and then click **Submit**. The library reboots. When the library completes its initialization, the Internal and External IP Conflict Prevention screen displays on the OCP.

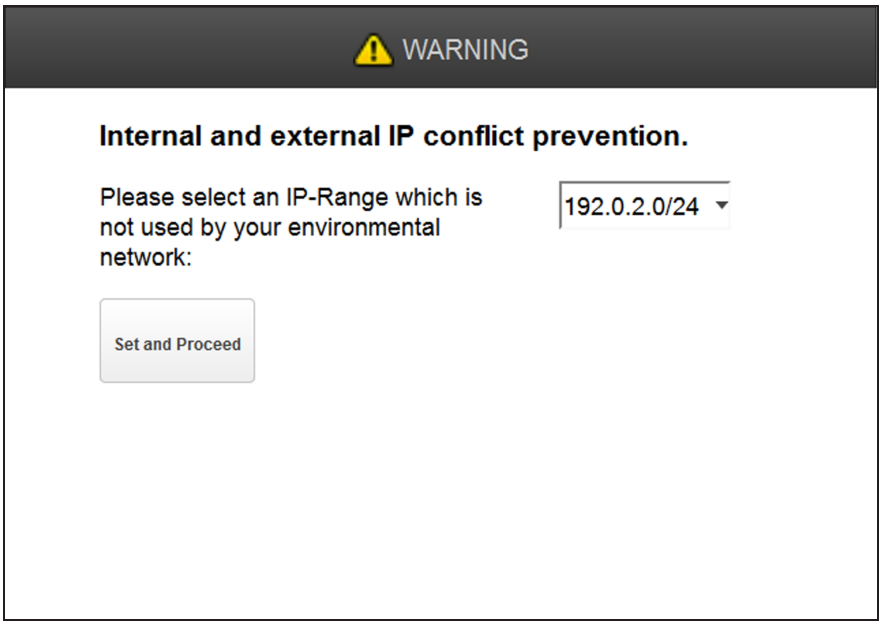


Figure 24 The IP Conflict Prevention Screen.

3. Using the drop-down menu, select one of the three default IP address ranges that is not used by your external network.

Note: If none of the three pre-entered address ranges is suitable for use in your network, contact Spectra Logic Technical Support.

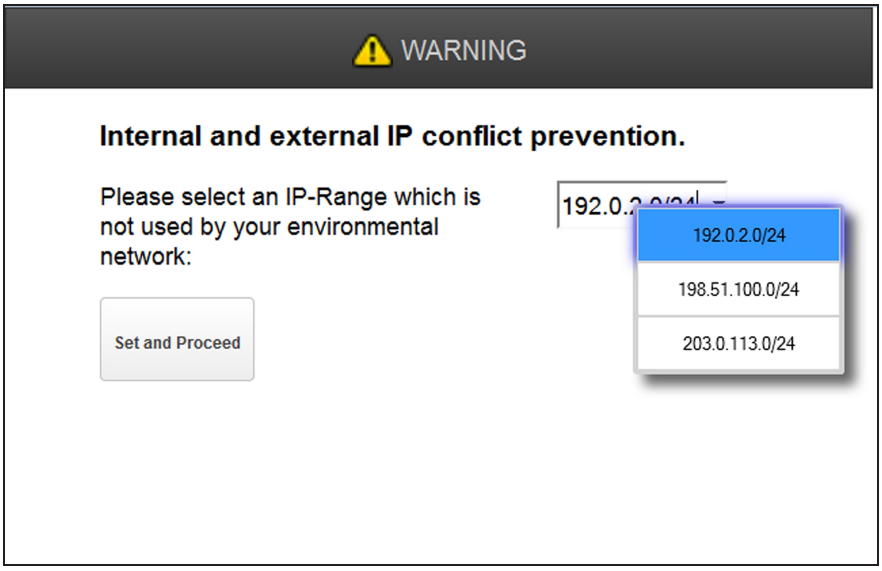


Figure 25 Select an IP address range using the drop-down menu.

4. Click **Set and Proceed**. The library reboots and displays the login screen (see Figure 9 on page 50).

CONFIGURING SNMP

Use the **Configuration > Network Management** screen to enable and configure SNMP (Simple Network Management Protocol), which allows applications to monitor the library. The library supports both SNMP configuration and SNMP traps.

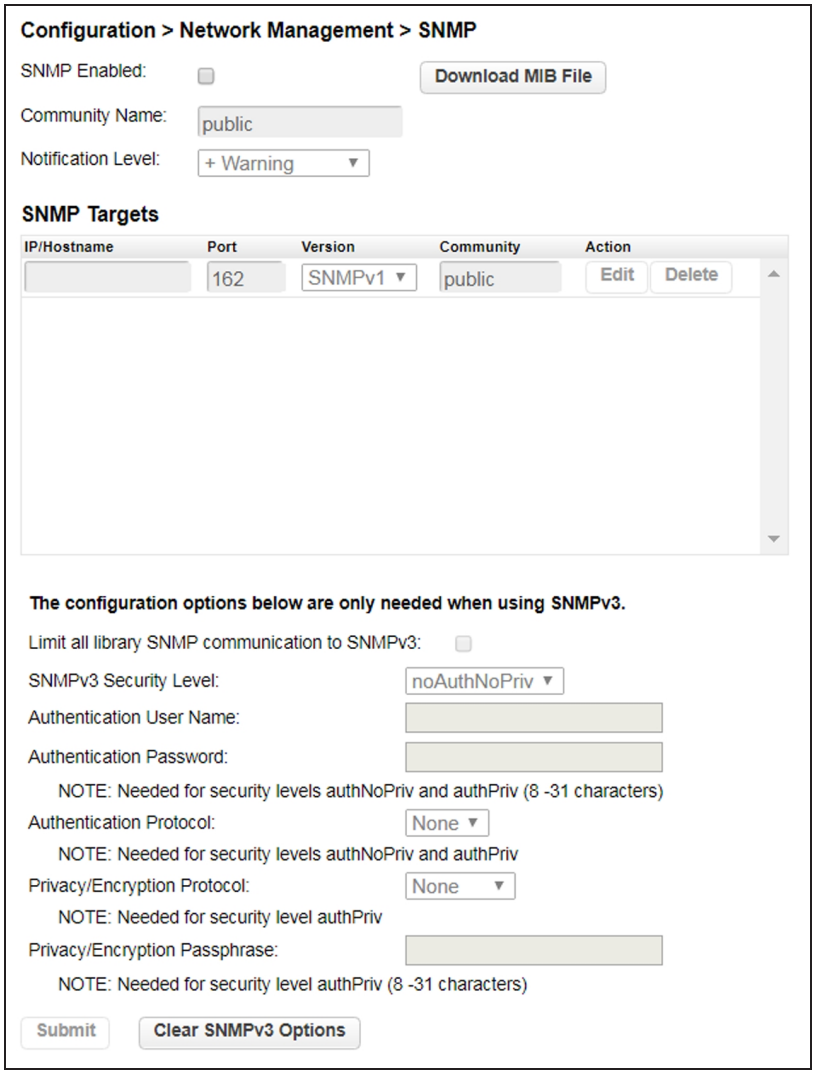


Figure 26 The SNMP screen.

1. Select the **SNMP Enabled** check box to enable SNMP. When selected, the configuration entry fields become accessible.

2. In the **Community Name** text box, enter a string used to match the SNMP management station and the library. Both the management station and the library must use the same Community Name. The default community name is `public`.
3. Use the drop-down menu to select the **Notification Level**.
4. The SNMP Targets pane lists all configured SNMP targets.

To add or edit an SNMP target:

a. Click **Edit** for the appropriate SNMP target. To add a new SNMP target, click **Edit** on the row with a blank IP/Hostname.

b. Enter the required information:

Field	Description
IP/Hostname	The target IP address or hostname.
Port	The port on which to communicate with the SNMP target. The default is 162.
Version	The SNMP version supported by the SNMP target.
Community	The SNMP community string for the target.

c. Click **Submit**.

To delete an SNMP target:

a. Click **Delete** next to the target to be deleted.

b. Click **Submit**.

5. If any targets use SNMP version SNMPv3, enter the SNMPv3 configuration options and click **Submit**.

Field	Description
SNMPv3 Security Levels	• **noAuthnoPriv** — Permits communication without authentication or privacy. • **authNoPriv** — Permits communication with authentication and without privacy. • **authPriv** — Only permits communication with authentication and privacy. **Note:** Selecting SNMPv3 does not disable SNMPv1 and SNMPv2.
Authentication User Name	The user name for authentication on the SNMPv3 trap receiver.
Authentication Password	The authentication password is needed for security levels authNoPriv and authPriv.
Authentication Protocol	The supported authentication protocols are MD5 and SHA (Secure Hash Algorithm).
Privacy/Encryption Protocol	The supported privacy protocols are DES (Data Encryption Standard) and AES (Advanced Encryption Standard).
Privacy/Encryption Passphrase	The passphrase is needed for security level authPriv.

To clear SNMPv3 configuration options:

a. Click **Clear SNMPv3 Options**.

b. Click **Yes** when prompted to confirm this action.

CONFIGURING EVENT NOTIFICATION PARAMETERS

You can enable SMTP (Simple Mail Transfer Protocol) functionality and configure email notification of library events to one email address from the **Configuration > Network Management > SMTP** screen. The library must have network access to an SMTP server.

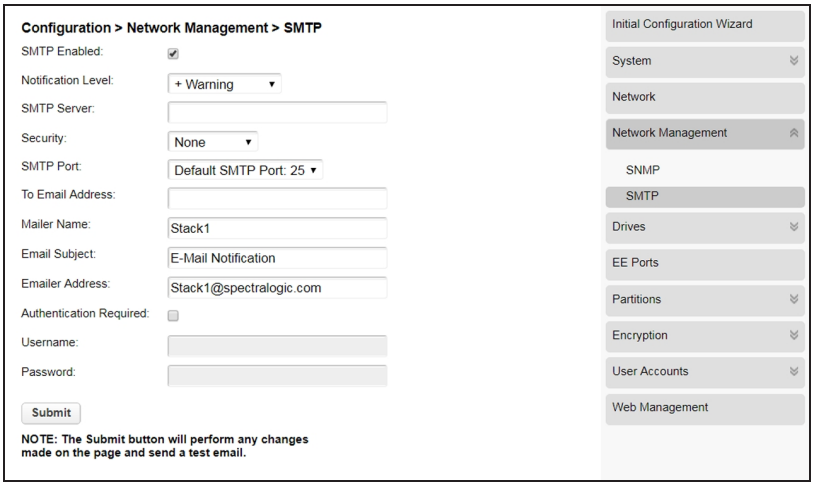


Figure 27 The SMTP screen.

1. Select the **SMTP Enabled** check box to enable SMTP. When selected, the configuration entry fields become accessible.
2. Enter the required information.

Field	Description
Notification Level	The types of events for which the library should send email. • **Inactive**—No events are sent. • **Critical**—Only critical events are sent. • **+ Warnings**—Only critical and warning events are sent. • **+ Configuration**—Only critical, warning, and configuration events are sent. • **+ Information**—All events are sent.
SMTP Server	The Hostname (if DNS is configured) or IP address (if DNS is not configured) of the SMTP server.

Field	Description
Security	The security protocol for accessing the SMTP server. • **None** • **SSL => SSL/TLS** • **TLS = STARTTLS**
SMTP Port	The default port for the selected protocol is selected. You can choose one of the default ports or configure a custom port. • **Default SMTP Port: 25** • **SMTP Over SSL: 465** • **Alternate Port: 587** • **Custom** - If selected, enter a port number.
To Email Address	The email address to receive the reported events (for example *firstname.lastname @ example.com*). If desired, multiple email addresses can be configured.
Mailer Name	Name to display as the sender of the email.
Email Subject	Subject line for the email message.
Emailer Address	The email address that displays as the sender whenever the library generates an email. This email address should uniquely identify the library to assist in troubleshooting, and be recognized by the SMTP server as a valid domain address.
Authentication Required	When selected, a username and password are required to access the SMTP server.
Username	User account for logging into the SMTP server when authentication is required.
Password	Password associated with the Username when authentication is required.

3. Click **Submit**.

CONFIGURING TAPE DRIVES

You can see and modify drive configuration from the **Configuration > Drives** screen.

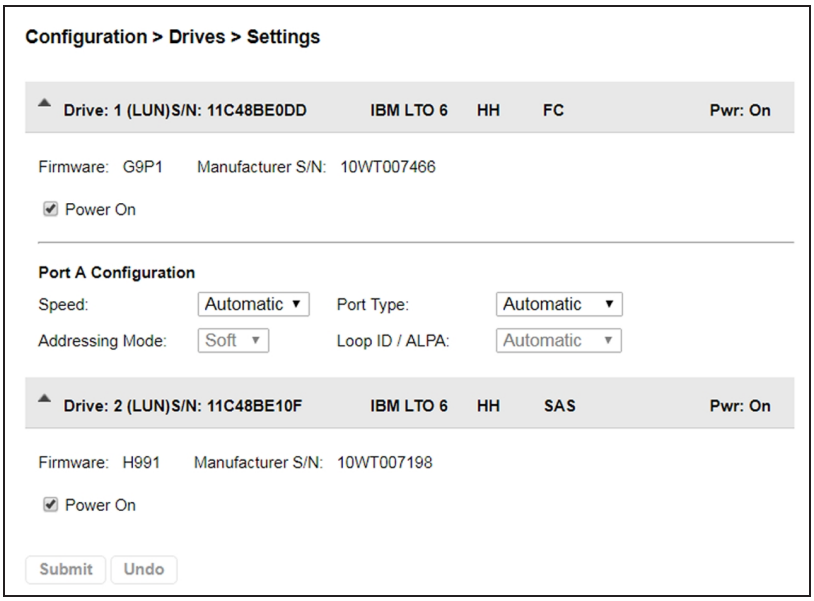


Figure 28 The Drives Settings screen.

Click the drive number to expand the section. The following information displays for each tape drive:

Field	Description
Drive Number	Tape drives are numbered from the bottom of the library up to the top beginning with "1". The drive currently hosting the SCSI communication for the library is designated with (LUN).
Serial Number	The serial number assigned to the tape drive by the Spectra Stack library. This serial number is reported to host applications. The serial number cannot be modified. **Note:** This is not the serial number assigned to the tape drive by the tape drive manufacturer; the serial number assigned by the manufacturer is shown in Manufacturer S/N.
LTO generation	The LTO generation of the drive.
Drive form factor	• **HH** - half height

Field	Description
	• **FH** - full height
Drive interface	• **FC** - Fibre Channel • **SAS** - Serial Attached SCSI
(Modified)	When present, this indicates that a setting has been changed, but not applied. To apply the changes, click **Submit**. To reset all changed fields to their previously saved values, click **Undo**.
Pwr	Indicates whether the drive is currently powered on or off.
Firmware	The version of firmware currently installed in the tape drive.
Manufacturer S/N	The serial number assigned to the drive when it was manufactured. Use this serial number when working with your service provider.
Power On	Selected when the drive is powered on. **Note:** Always power off a tape drive before removing it from the library or moving it to a new location within the library.

Port configuration (FC only)	The drive port configuration.
	• **Speed** -The currently selected Fibre Port speed. The default is Automatic.
	• **Port Type**
	  • Automatic (default)
	  • Fabric
	  • Loop - Enables selection of the Addressing Mode.
	• **Addressing Mode** - When **Port Type** is set to Loop, **Addressing Mode** can be set to Soft or Hard addressing.
	• **ALPA** - When Addressing Mode is set to Hard, you can choose an ALPA address from the drop down list.

To modify the configuration of one or more tape drives:

1. Modify any of the configurable values.
2. Click **Submit**.

ENABLING OR DISABLING EE PORTS

The **Configuration > EE Port** screen lists each of the EE ports and shows whether each is enabled or disabled. Disabled EE ports are available as storage slots.

Partitions do not need to have EE port slots. If a partition does not have EE port slots, the magazine must be accessed to import or export cartridges. Opening a magazine takes the library offline, while opening an EE port does not.

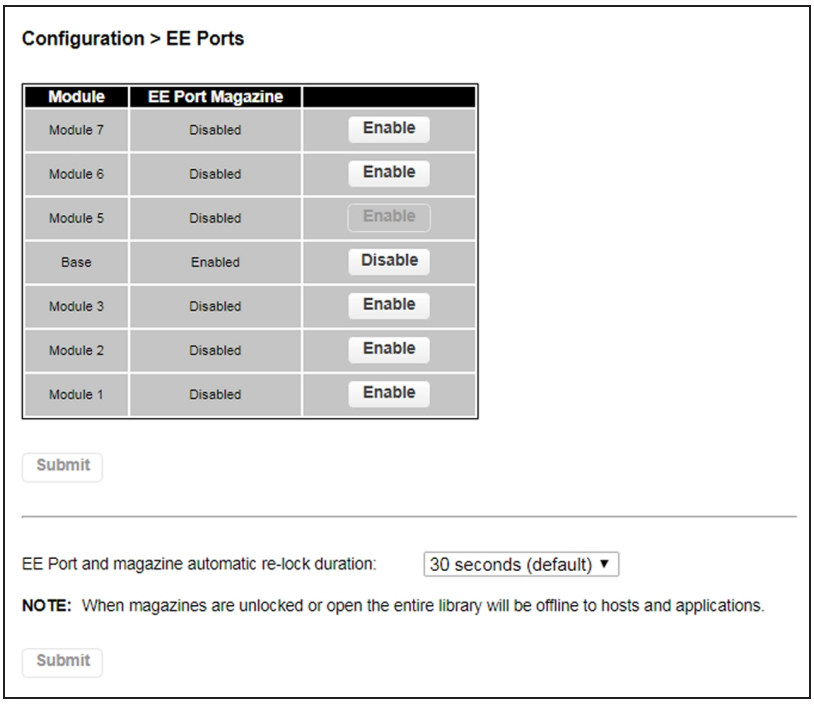


Figure 29 The Configuration EE Ports screen.

1. To change the EE port state, click **Enable** or **Disable** next to the appropriate module.
2. If desired, use the **EE port and magazine automatic re-lock duration** drop down list to change the amount of time before EE ports or magazines automatically re-lock if you do not open the door and access the EE port or magazine. The choices are 30 seconds (default) or 5 minutes.
3. Click **Submit** to save your selections.

CONFIGURING LIBRARY PARTITIONS

IMPORTANT Partitions can only be created using the RMI (Remote Management Interface).

Partitions on the Spectra Stack library have the following restrictions:

- Each partition must have at least one tape drive. One drive in each partition hosts the robotics interface (the library LUN) for the partition.
- The maximum number of partitions allowed is 20.
- Magazine slots are allocated in five-slot groups.
- EE ports must be enabled for a module before they can be allocated to a partition. See Enabling or Disabling EE Ports on the previous page.
- A partition does not need to have an EE port. If a partition does not have an EE port, the magazine must be accessed to import or export cartridges. Opening a magazine takes the library offline, while opening an EE port does not.
- Although the EE port is shared between partitions, the EE port elements are assigned individually to partitions.
- All of the partitions in the library go offline while partitions are configured. Ensure that host operations for all partitions are idle before running a partition wizard.

Partition configuration wizards guide you through the process. The wizards are only accessible from the RMI. Use the Basic Partition Wizard to configure partitions that have similar resources. Use the Expert Partition Wizard to configure partitions that have different resources or to adjust resource assignments for existing partitions.

- Basic Partition Wizard - Any currently configured partitions are deleted. You specify the number of partitions and the wizard assigns drives and storage slots as evenly as possible to the partitions. Any extra drives or slots are assigned to the first partition.
- Expert Partition Wizard - Can be used to edit or remove current partitions or create the first or an additional new partition. New partitions are created individually and you control the library resources assigned.

Using the Basic Partition Wizard

You must create at least one partition before you can use your Stack library for data backup operations. The following instructions guide you through partition creation using the Basic Wizard, which creates one or more partitions using all tape drives and licensed slots in the library.

IMPORTANT With the Basic Wizard, all previously configured partitions are deleted. Ensure that host operations for all partitions are idle before running the partition wizard.

Note: If you want to configure advanced partition settings, see Using the Expert Partition Wizard on page 87 for instructions on using the partition Expert Wizard. Use the Expert Wizard to create additional partitions without deleting current partitions, to configure partitions that have different resources or to adjust resource assignments for existing partitions.

Use the instructions below to create partitions using the Basic Partition Wizard:

1. From the home screen of the library interface, select **Configuration > Partitions**. The Configuration screen displays.

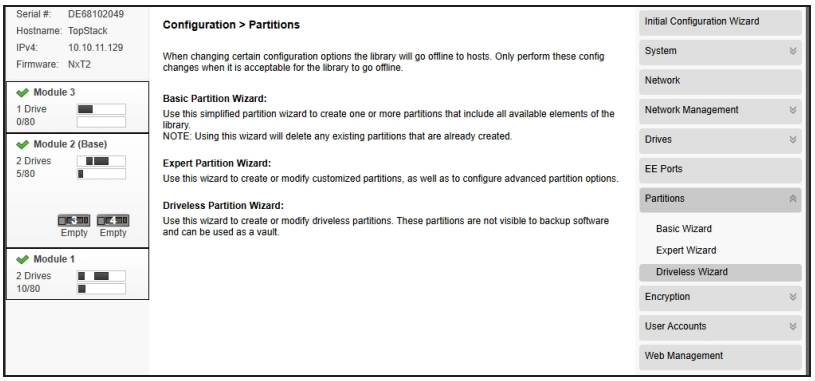


Figure 30 The Configuration screen.

2. On the right-hand pane, select **Basic Wizard**. The Information screen of the Basic Wizard displays.

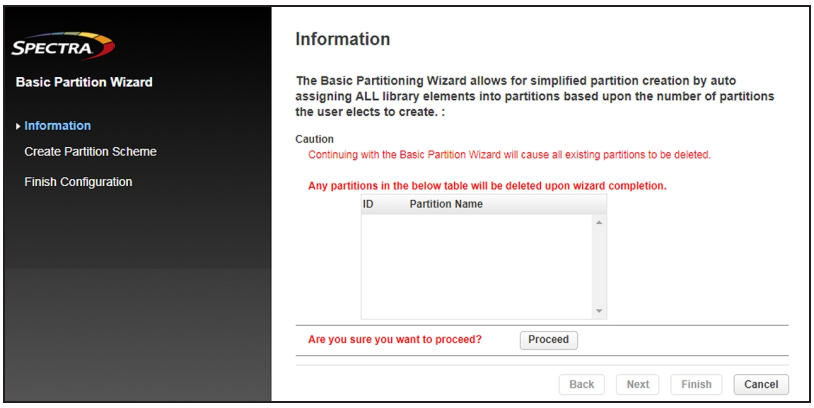


Figure 31 The Information screen.

3. A warning displays that the Basic Wizard deletes any existing partitions. Click **Proceed** and then click **Next**. The Create Partition Scheme screen displays.

Notes:
- If you want to enable or disable EE ports, click **Cancel** to leave the wizard and update the EE port configuration (see Enabling or Disabling EE Ports on page 82) before configuring partitions.
- If the resources displayed do not match your configuration, you may need to install license keys. See Add a License Key on page 70.

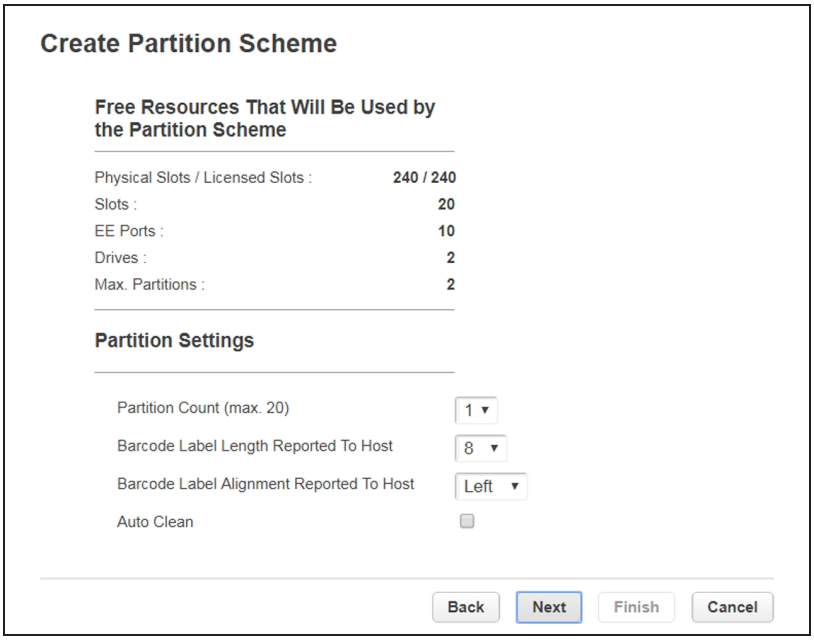


Figure 32 The Create Partition Scheme screen.

4. Use the **Partition Count** drop-down menu to select the number of partitions you want to create up to the maximum number of licensed partitions. With the Basic Wizard, the resources in the library (drives and media) divide evenly between each partition.

   Note: Magazine slots are allocated in five-slot groups. The wizard assigns the drives and storage slots as evenly as possible to the partitions, assigning . Any extra drives or slots are assigned to the first partition.

5. Use the **Barcode Label Length Reported To Host** drop-down menu to select the number of digits on a tape barcode that are reported to your backup software. This option provides interchange compatibility with libraries with more limited barcode reading capabilities. The maximum barcode character length is 15 and the default is 8. This configuration applies to all partitions.

   Note: The industry standard length for LTO barcode labels is eight characters. Barcode labels longer than eight characters might scan incorrectly, particularly if they are not high quality labels.

6. Use the **Barcode Label Alignment Reported To Host** drop-down menu to configure the library to report the barcode digits to the backup software starting from the left or right side of the barcode. The default setting is left. For example, when reporting only six characters of the barcode label 12345678, if alignment is left, the library reports 123456. If alignment is right, the library reports 345678. The default is left.

7. If desired, select **Auto Clean** to configure the library to automatically clean a tape drive when it requests cleaning using a cleaning tape stored in the partition or in an unassigned slot.

8. Click **Next**. The Finish Configuration screen displays with details for the partition(s) configured using the wizard.

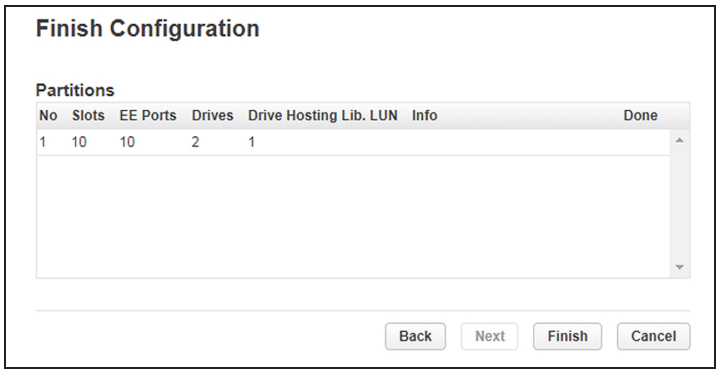


Figure 33 The Finish Configuration screen.

9. Click **Finish** to create the partition(s) and exit the wizard.

Using the Expert Partition Wizard

Select **Configuration > Partitions > Expert Wizard** to start the wizard. The Manage Partitions screen lists the current partitions, if any, and the free resources. Use this wizard to configure one partition at a time.

Notes:
- If you want to enable or disable EE ports, click **Cancel** to leave the wizard and update the EE port configuration (see Enabling or Disabling EE Ports on page 82) before configuring partitions.
- All of the partitions in the library go offline while partitions are configured. Ensure that host operations for all partitions are idle before running the partition wizard.

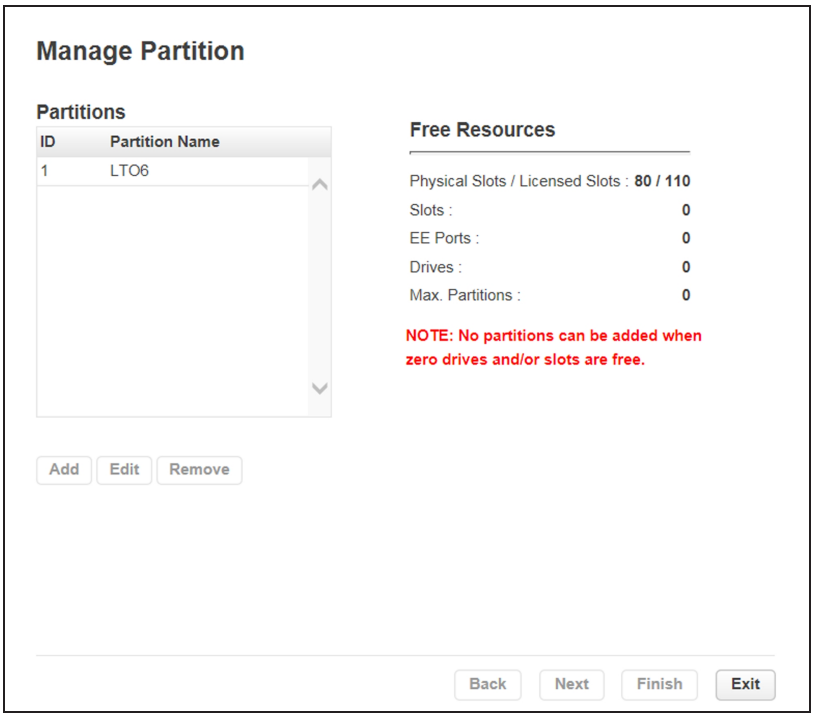


Figure 34 The Manage Partitions screen.

Using the Driveless Partition Wizard

Driveless partitions allow Administrator level users with two-factor authentication enabled to store tapes inside the library. To create a driveless partition, select **Configuration > Partitions > Driveless Wizard** to start the wizard.

1. On the Manage Driveless Partition screen, select **Add** and click **Next**.

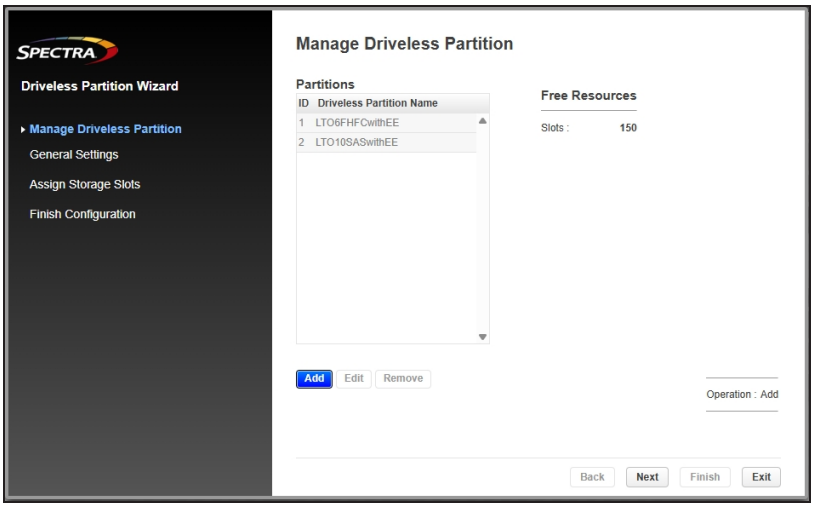


Figure 35 The Manage Driveless Partitions screen.

2. On the General Settings screen, enter a **Partition Name**. If desired, select **Auto Move to Driveless Partition** then select an existing partition from the drop-down menu.

   Enabling this feature automatically moves tapes exported from the selected partition to the driveless partition.

   Click **Next**.

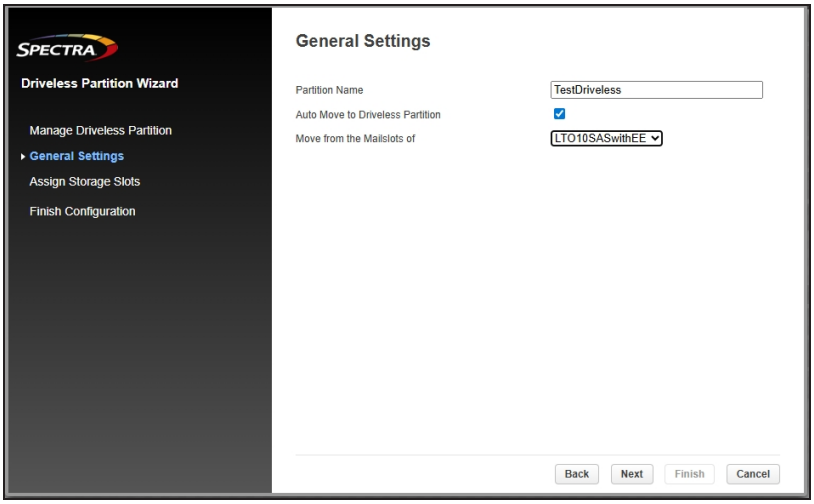


Figure 36 The General Settings screen.

3. Assign storage slots to the partition and click **Next**.
4. Click **Finish** to create the driveless partition.

Add or Edit a Partition

Use the instructions below to create partitions using the Expert Partition Wizard:

1. Click **Add** to create a new partition or select the partition and click **Edit** to edit an existing partition, and then click **Next**. The General Settings screen displays.

Note: The **Add** button is only active if there are available resources. If there are no available resources, either edit a partition to free up resources for a new partition, or remove a partition.

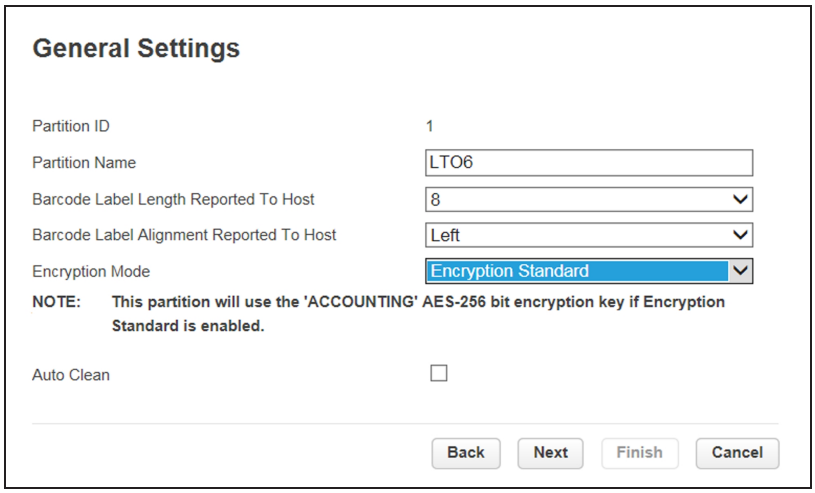


Figure 37 The General Settings screen.

2. Enter a **Partition Name**.
3. Use the **Barcode Label Length Reported To Host** drop-down menu to select the number of digits on a tape barcode that are reported to your backup software. This option provides interchange compatibility with libraries with more limited barcode reading capabilities. The maximum barcode character length is 15 and the default is 8. This configuration applies to all partitions.

Note: The industry standard length for LTO barcode labels is eight characters. Barcode labels longer than eight characters might scan incorrectly, particularly if they are not high quality labels.

4. Use the **Barcode Label Alignment Reported To Host** drop-down menu to configure the library to report from the left or right end of the barcode label to the host application when reporting fewer than the maximum number of characters.

   For example, when reporting only six characters of the barcode label 12345678, if alignment is left, the library reports 123456. If alignment is right, the library reports 345678. The default is left.

5. Use the **Encryption Mode** drop-down menu to select the type of encryption used by the partition. To disable encryption, select **Controlled by Backup Application.**

   Note: This field is only visible if you are logged in as a security user or if the security user has configured permission for the administrator user to configure encryption used by a partition using the Expert Partition Wizard. See Configuring the Library on page 57.

6. If desired, select **Auto Clean** to configure the library to automatically clean a tape drive when it requests cleaning using a cleaning tape stored in the partition or in an unassigned slot.

7. If desired, select **LTO7 + Multi-initiator SCSI Conflict Detection**.

   LTO-7 and later generation tape drives track which hosts (SCSI initiators) send commands to the drive. When **LTO7 + Multi-initiator SCSI Conflict Detection** is enabled for a partition, the library monitors the initiator lists for all of the LTO-7 and later generation drives in that partition. If the library detects more than a one host system connecting to any of the tape drives in this partition, the library generates an LTO-7 Multi-initiator SCSI Conflict Detection warning event. The event lists all of the host WWNNs for the given tape drive, so the administrator can remove access to any host that should not be sending commands to the drive.

Notes:
- The **LTO7 + Multi-initiator SCSI Conflict Detection** setting only appears if one or more LTO-7 or later generation drives are detected in the library.
- Do not enable this feature if your storage architecture requires multiple hosts sending commands to any drive in the partition.

8. Click **Next.** The Assign Storage Slots screen displays.

Figure 38 The Assign Storage Slots screen.

In the Assign Storage Slots screen, select the groups of slots that you want to move into or out of the partition and using the >> and << buttons make the change. Clicking **Select All** selects all unassigned, licensed slots. Storage slots are assigned in five slot groups and are displayed in the format *module.slot-module.slot* where:

- *module* - The module number. Modules are numbered based on their location in the physical library. The bottom module is Module 1.
- *slot* - The slot number as shown in Figure 6 on page 37.

9. Click **Next**. If you have enabled EE ports (see Enabling or Disabling EE Ports on page 82), the Assign EE Ports screen displays.

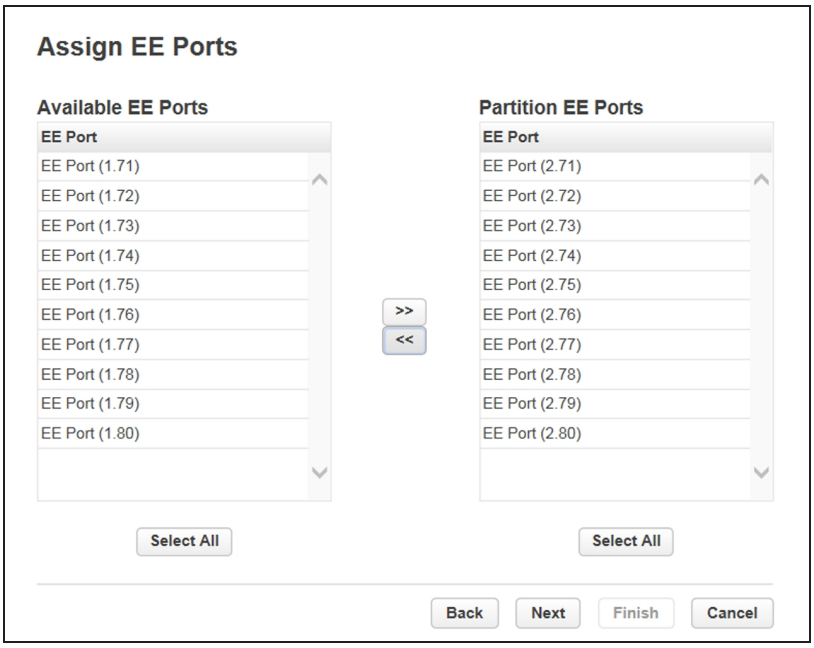


Figure 39 The Assign EE Ports screen.

In the Assign EE Ports screen, use the >> and << buttons to assign EE ports to the new partition. EE Port locations are shown in the format *module.slot-module.slot* where:

- *module* - The module number. Modules are numbered based on their location in the physical library. The bottom module is Module 1.
- *slot* - The slot number as shown in Figure 6 on page 37.

Note: The EE port can be shared by partitions, but individual slots cannot. Importing or exporting cartridges in a partition without assigned EE slots requires magazine access, which takes all partitions in the library offline. EE port access does not take partitions offline.

10. Click **Next**. The Assign Drives screen displays.

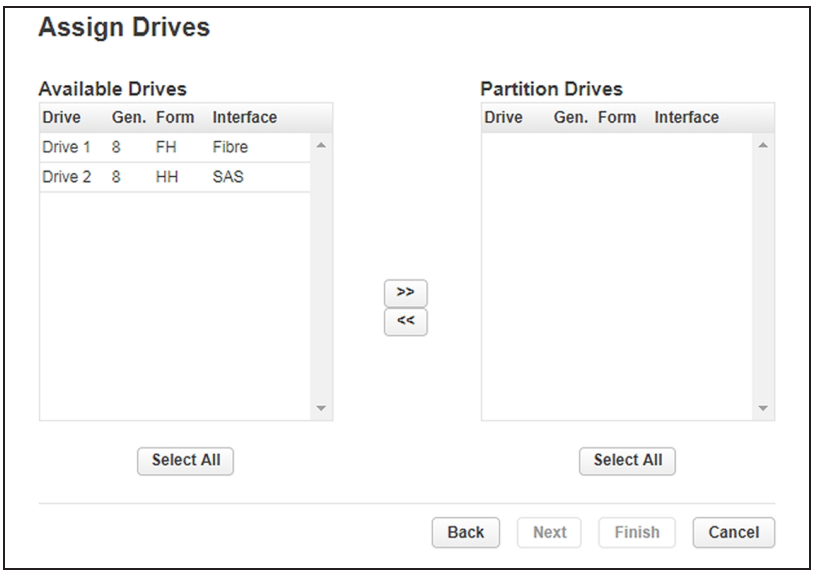


Figure 40 The Assign Drives screen.

11. In the Assign Drives screen, use the >> and << buttons to assign drives to the new partition.

12. Click **Next**. The Select Library LUN Drive screen displays.

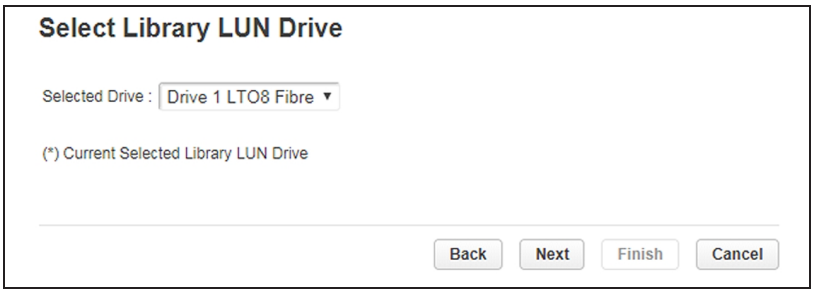


Figure 41 The Select Library LUN Drive screen.

13. If the partition has multiple tape drives, select the drive to host the SCSI communication for the partition.

Note: The lowest numbered drive in the partition is selected as the default.

14. Click **Next**. The Finish Configuration screen displays.

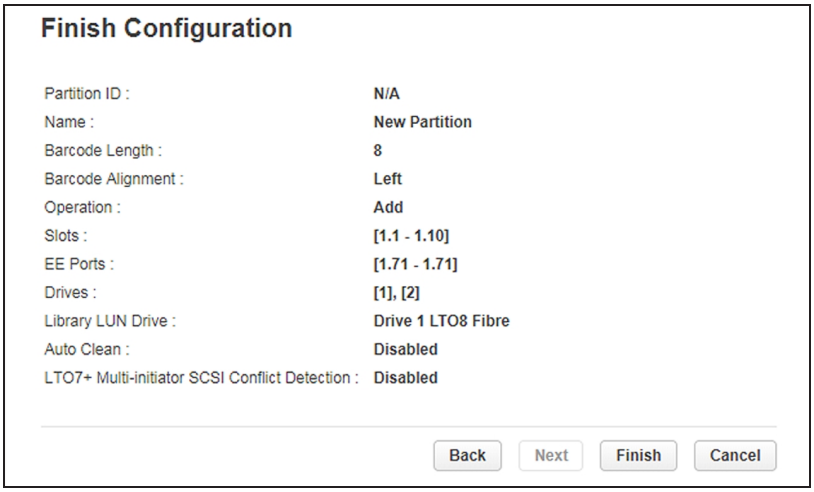


Figure 42 The Finish Configuration screen.

15. Verify the partition configuration and then click **Finish**.

    After the wizard creates or reconfigures the partition, the library comes online automatically.

Remove a Partition

1. On the Manage Partitions screen (see Figure 34 on page 87), select the partition to remove.
2. Click **Remove**, and then click **Next**.
3. Verify that you want to remove the partition and click **Finish**.

   After the wizard removes the partition, the library comes online automatically.

CONFIGURE USER ACCOUNTS

Configure User Account Settings

Logged in as a Security user or an Administrator user, from the **Configuration > User Accounts > User Accounts Settings** screen you can set the password rules that apply for all users.

Note: When the settings are changed, they are applied to new passwords. Existing passwords remain the same.

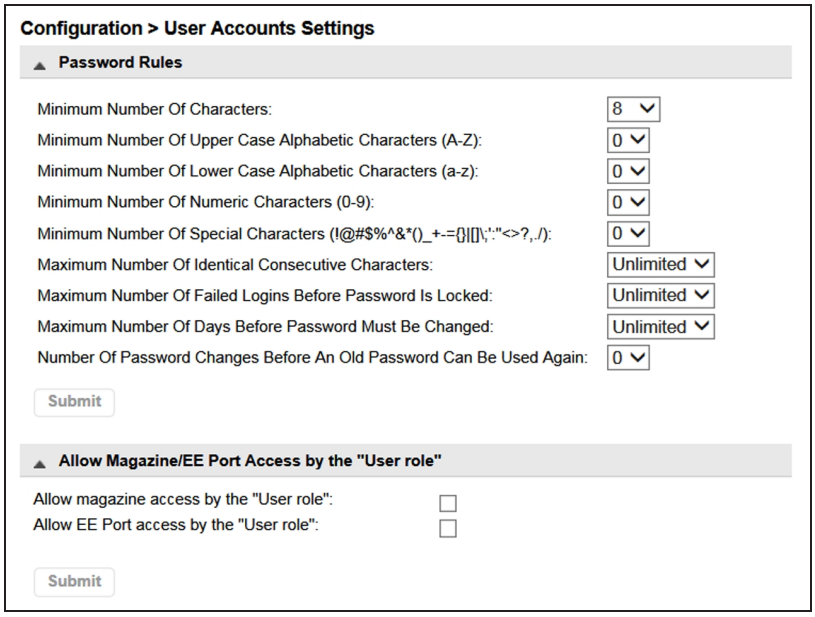


Figure 43 The User Account Settings screen.

Configure Password Rules

Select any password rules that you want to apply and then click **Submit**.

- **Minimum Number Of Characters**—Choose the minimum password length. The factory default value is 8. Possible range for this option is from 8 to 20. The maximum password length is 128.
- **Minimum Number Of Upper Case Alphabetic Characters (A-Z)**—Choose the minimum number of upper case alphabetic characters. The factory default value is 0. Possible range for this option is from 0 to 3.

- **Minimum Number Of Lower Case Alphabetic Characters (a-z)**—Choose the minimum number of lower case alphabetic characters. The factory default value is 0. Possible range for this option is from 0 to 3.
- **Minimum Number Of Numeric Characters (0-9)**—Choose the minimum number of numeric characters. The factory default value is 0. Possible range for this option is from 0 to 3.
- **Minimum Number Of Special Characters (!@#$%^&*()_+-={}|[]\;':" <>?,./)**—Choose the minimum number of special characters. The factory default value is 0. Possible range for this option is from 0 to 3.
- **Maximum Number Of Identical Consecutive Characters**—Choose the maximum number of identical consecutive characters. The factory default value is unlimited. Possible range for this option is from 1 to 3, or unlimited.
- **Maximum Number Of Failed Logins Before Password Is Locked**—Choose the maximum number of failed logins before the password is locked. The factory default value is unlimited. Possible range for this option is from is from 1 to 10, or unlimited.

CAUTION When a password is locked, the login cannot continue. Either the user must complete a valid login with an administrator account where the administrator can change a password or request a temporary password.

- **Maximum Number Of Days Before Password Must Be Changed**—Choose the maximum number of days before the password must be changed. The factory default value is unlimited. Possible range for this option is from is from 1 to 365, or unlimited.
- **Number Of Password Changes Before An Old Password Can Be Used Again**—Choose the number of password changes before the password can be re-used. The factory default value is 0. Possible range for this option is from is from 1 to 6.

Allow Magazine/EE Port access by the "User role"

By default, only the administrator and security users are allowed to open the EE Ports or magazines. The administrator and security users can enable accounts with the user role to access to the magazines and EE Ports. Select the desired access permission(s) and click **Submit**.

- To allow access the magazines, select **Allow magazine access by the "User role"**.
- To allow access to the EE Ports, select **Allow EE Port access by the "User role"**.

Two-Factor Authentication

The Spectra Stack library offers two-factor authentication as part of Attack Hardened storage, which enhances the security of your library by using an authenticator application to confirm the identity of a user trying to log in to the library. This prevents unauthorized access to the library even if the user credentials needed to access the system are compromised.

Two-factor authentication works on a per-user basis by generating a token in the form of a QR code for a selected system user. The user scans the QR code using an authenticator application to complete the account creation. After the QR code is scanned, the authenticator generates a six-digit number every 30 seconds and does not require cell or internet access to generate these codes.

After two-factor authentication is enabled, when the user attempts to log in to the Stack user interface, after entering their username and password, they must enter the six-digit number generated by the authenticator within 30 seconds to complete the login.

Spectra Logic has tested the Google Authenticator phone application, the Microsoft Authenticator phone application, and the *authenticator.cc* plugin to the Google Chrome browser.

Note: If you plan to enable two-factor authentication for a user(s), you must enable SNTP before you can use two-factor authentication. See Enabling SNTP (Simple Network Time Protocol) Synchronization on page 67.

Configure Local User Accounts

From the **Configuration > User Accounts > Local User Accounts** screen you can add local users or set a new password for the user, administrator, or security accounts.

Notes:
- An Administrator user can add a user or change the password for a user with an administrator or user role.
- A Security user can add a security user or change the password for a security user.
- A user with the user role cannot access this screen.

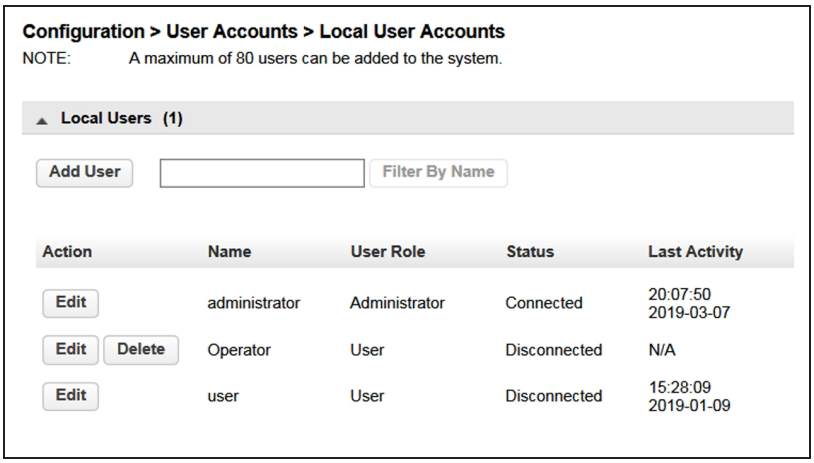


Figure 44 The Local User Accounts screen (Administrator logged in).

Change Passwords

1. Click **Edit** next to the user for which you want to change the password. The Modify User Password dialog box displays.

Notes:
- A password is not required for the default user account.
- The library initially has a null administrator password. A password must be set using the OCP before the Administrator can access the library from the RMI. Once the Administrator password has been set from the OCP, it can be changed by the Administrator user from either the OCP or RMI.
- The default password for the Security user is **security**. The password must be modified using the OCP before the Security user can access the library from the RMI. Once the Security password has been set from the OCP, it can be changed by the Security user from either the OCP or RMI.

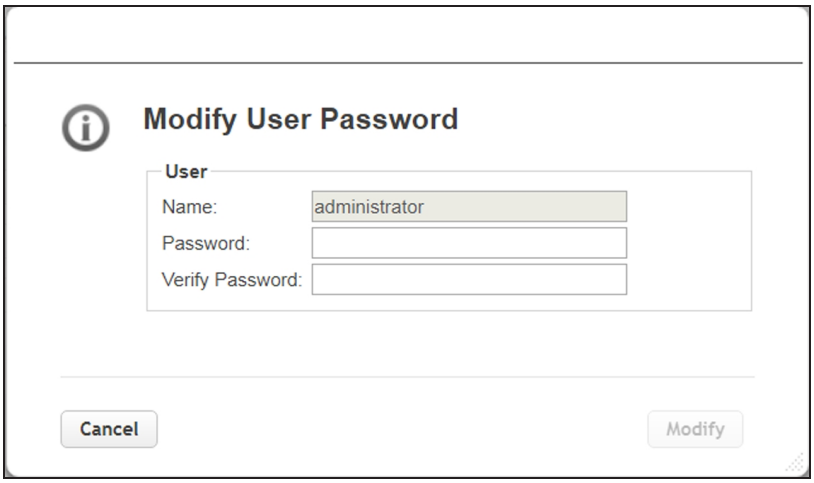


Figure 45 The Modify User Password dialog box.

2. Enter and verify the new password, and then click **Modify**. The dialog box closes to display the Local User Account screen.

Add a User

1. From the **Configuration > User Accounts > Local User Accounts** screen (see Figure 44 on page 98), click **Add User**. The Add User screen displays.

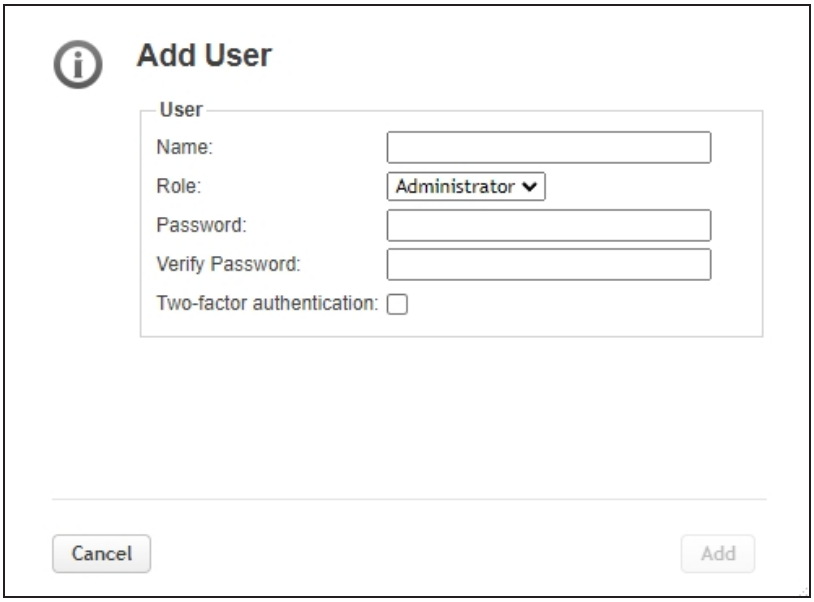


Figure 46 The Add User screen (Administrator logged in).

2. Enter the **Name** for the user.

3. Select a **Role** for the user:
   - **User** — A user account allows access to library status information and does not allow access to configuration, maintenance, or operation features. A password is not required for the default user account, but is required for additional user accounts.
   - **Administrator** — The Administrator account allows access to all configuration, maintenance, and operation features other than encryption.
   - **Security** — A security user has access to all administrator functionality and can also configure security features and change the security user password.
4. Enter and verify the password. The password must meet the configuration options selected in Configure User Account Settings on page 95.
5. If desired, select **Two-factor Authentication** to require the user to enter a six digit TOTP (Time-Based One-Time Password) each time they log in to the library. The user must configure an Authentication application the next time they log in.
6. Click **Add**. The dialog box closes to display the Local User Accounts screen.

Enable Two Factor Authentication for Current User

Use the instructions in this section to edit the current user to enable two-factor authentication.

Note: You must enable SNTP before you can use two-factor authentication. See Enabling SNTP (Simple Network Time Protocol) Synchronization on page 67.

1. From the **Configuration > User Accounts > Local User Accounts** screen (see Figure 44 on page 98), click **Edit** next to the user you for which you want to enable two-factor authentication. The Modify User screen displays.

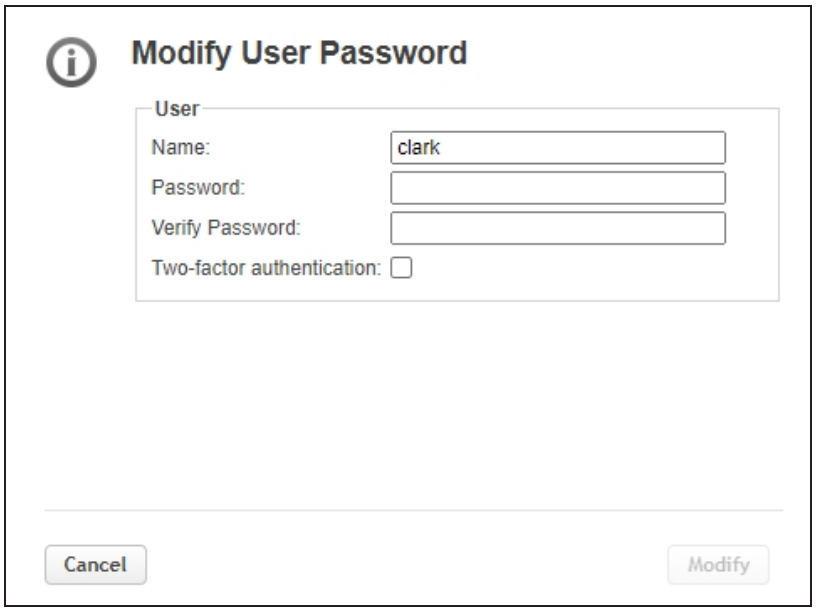


Figure 47 The Modify User screen.

2. Select **Two-factor Authentication**, then click **Modify**.
   - If you are modifying the currently logged in user, the Setup Authenticator App screen displays. Continue with Step 3.
   - If you are editing a different user, the window closes and the user must configure two-factor authentication the next time they log into the library.
3. Scan the QR code with your phone or similar device, or enter the authentication seed code manually in the **Custom Seed** field. The library appears in your authentication application under the name of your stack library.

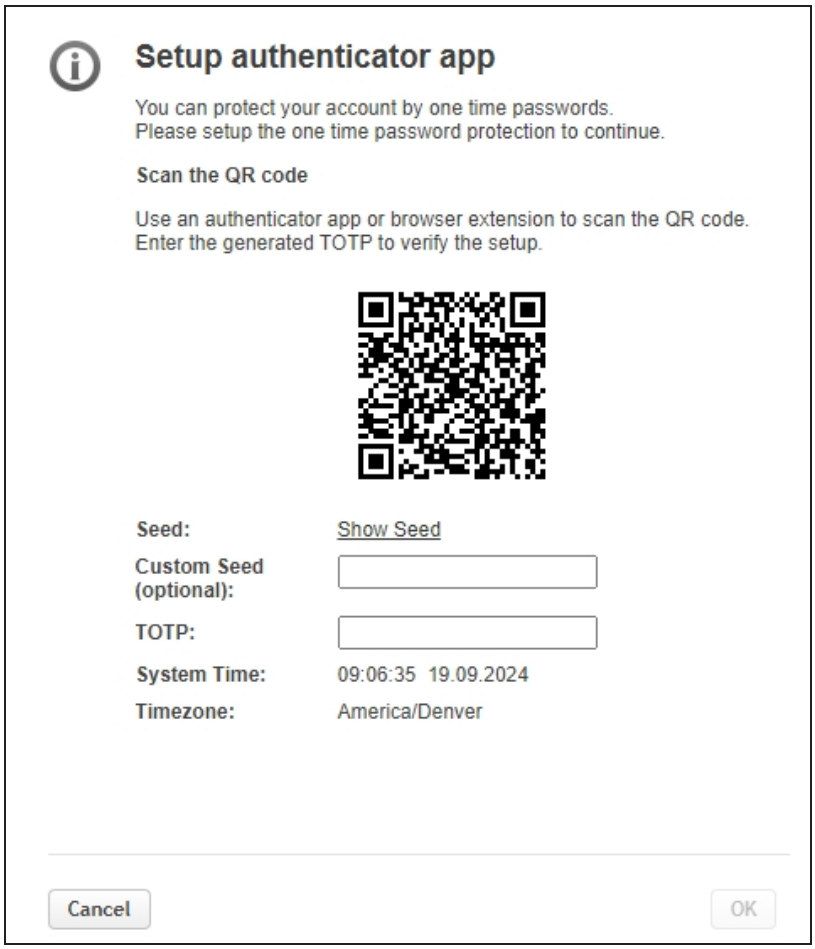


Figure 48 The Modify User screen.

4. Enter the code displayed for the library in your authenticator application in the **TOTP** (Time-Based One-Time Password) field.
5. Click **OK**. The user is now asked for the TOTP code each time they log in to the library.

Configure LDAP

From the **Configuration > User Accounts > LDAP** screen, manage LDAP (Lightweight Directory Access Protocol) servers and users.

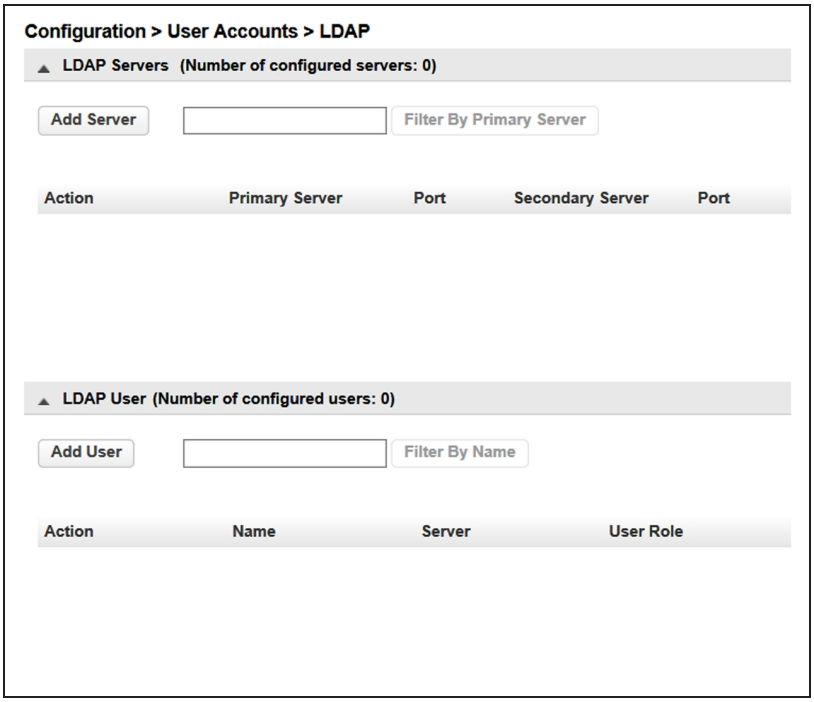


Figure 49 The **Configuration > User Accounts > LDAP** screen.

Add Server

To add an LDAP server, click **Add Server**, the Add Server dialog box displays.

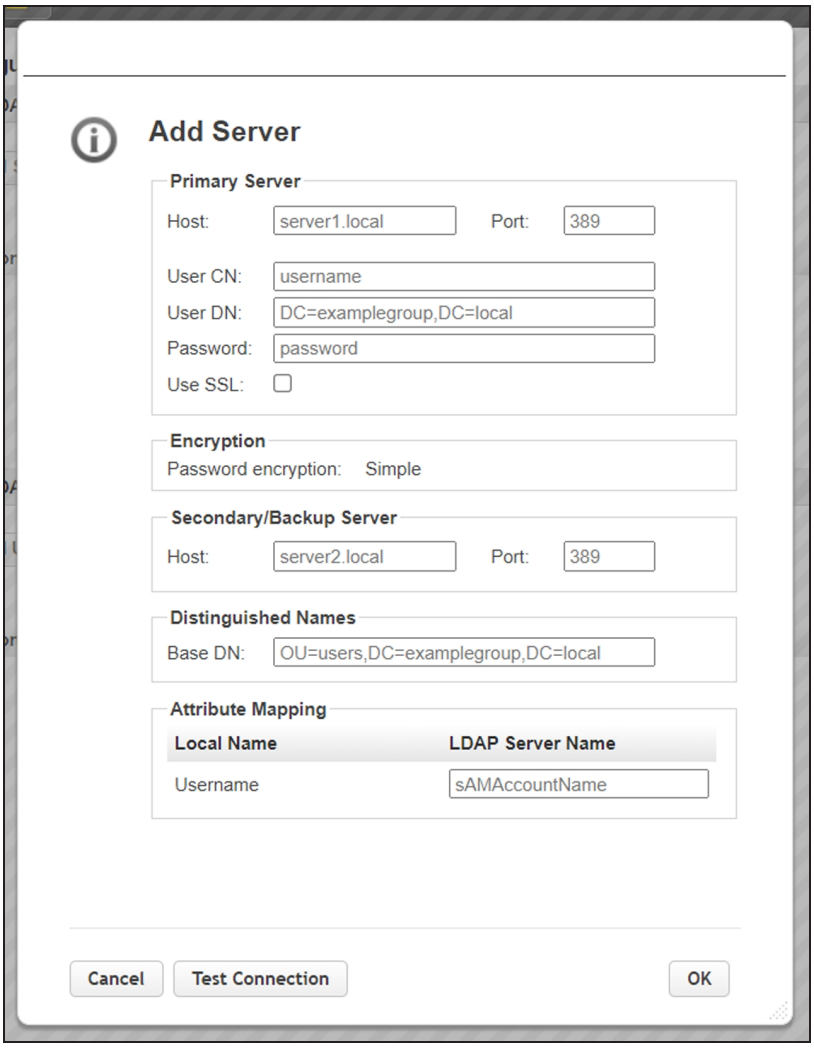


Figure 50 The LDAP Add Server dialog box.

1. Enter the information for the primary server.

Field	Description
Host	The IP address for the LDAP server.
Port	The port on which to communicate with the host. The default is 389.
User CN	The common name for a user with permission to connect to the LDAP server. Many environments use the format “Surname, Name” or the email address for a group of library administrators.

Field	Description
User DN	The distinguished name for the user with the entered User CN. For example: `DC=Examplegroup,DC=local`.
Password	The password for the user with the entered User CN. This password might be the User CN's Windows password or an environment-specific password.
Use SSL	If required, select **Use SSL** and then paste the appropriate CA certificate.

2. Enter the Secondary/Backup Server **Host** address and **Port** number.
3. Enter the **Base DN** for Distinguished Names. These are the LDAP parameters needed to identify the LDAP domain. For example: `OU=users,DC=Examplegroup,DC=local`.
4. In the Attribute Mapping pane, enter the **LDAP Server Name** for the specified user account.
5. Click **Test Connection** to verify the server configuration.
6. After verifying the server configuration, click **OK**.

Add User

To add an LDAP user, click **Add User**, the Add User dialog box displays.

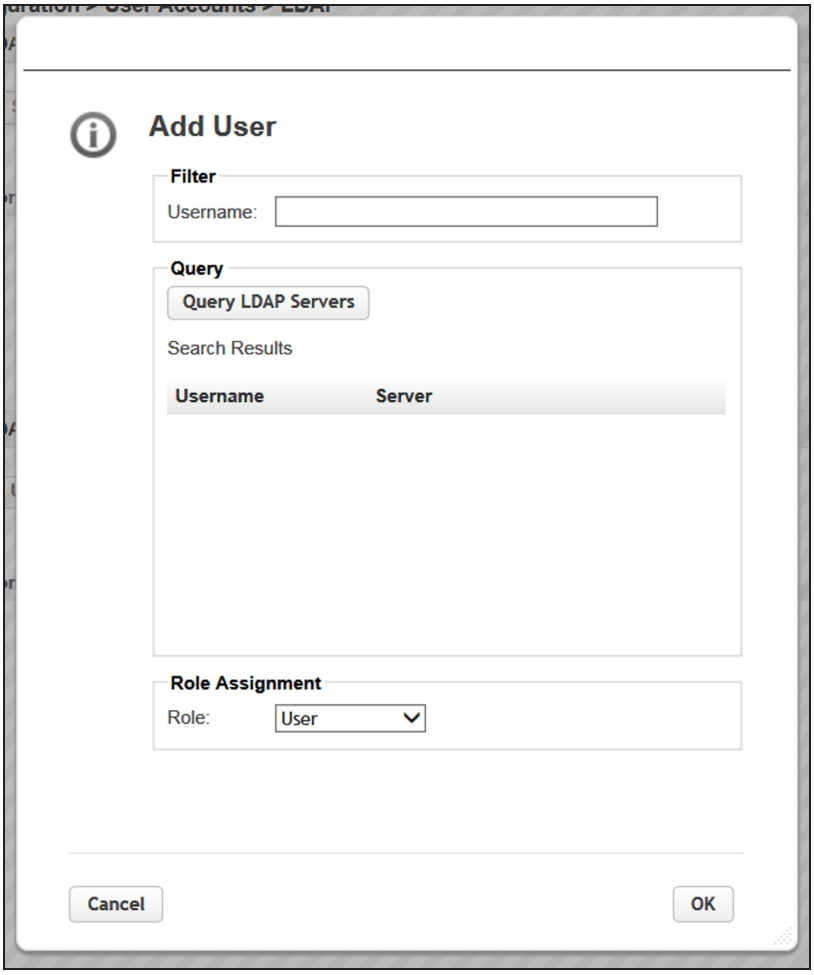


Figure 51 The LDAP Add User dialog box.

1. Click **Query LDAP Servers** to see a list of available users.
2. Select a user name and then assign the user a **Role** (User, Administrator, or Security).
3. Click **OK**.

WEB MANAGEMENT

Use the instructions in this section to configure advanced web management features for the RMI.

Enabling SSL or SSH

Enable or disable secure access to the RMI using Secure Socket Layer (SSL) or Secure Shell (SSH) from the **Configuration > Web Management** screen.

- When SSL is enabled, connections to the RMI must use HTTPS. The default is disabled.
- When SSH is enabled, the library accepts SSH connections. The default is enabled.

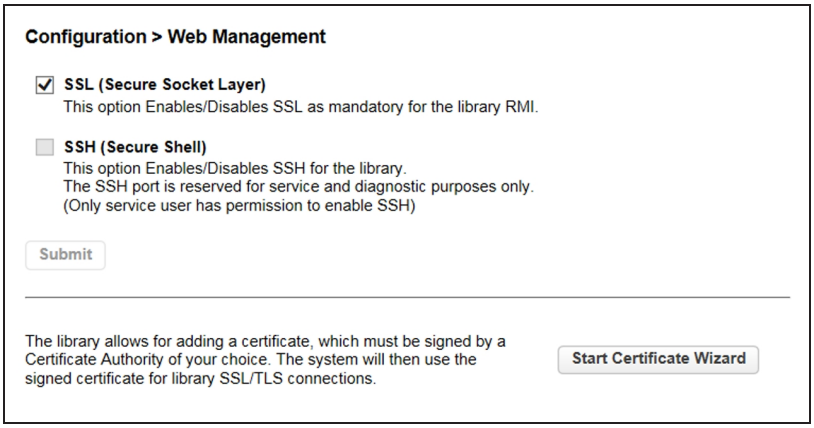


Figure 52 The SSL/SSH pane of the **Configuration > Web Management** screen.

Select or clear the SSL and SSH check boxes as desired, and click **Submit**.

Note: SSH is not available on the Spectra Stack library.

Security Certificates

From the **Configuration > Web Management** screen select certificate settings and manage security certificates.

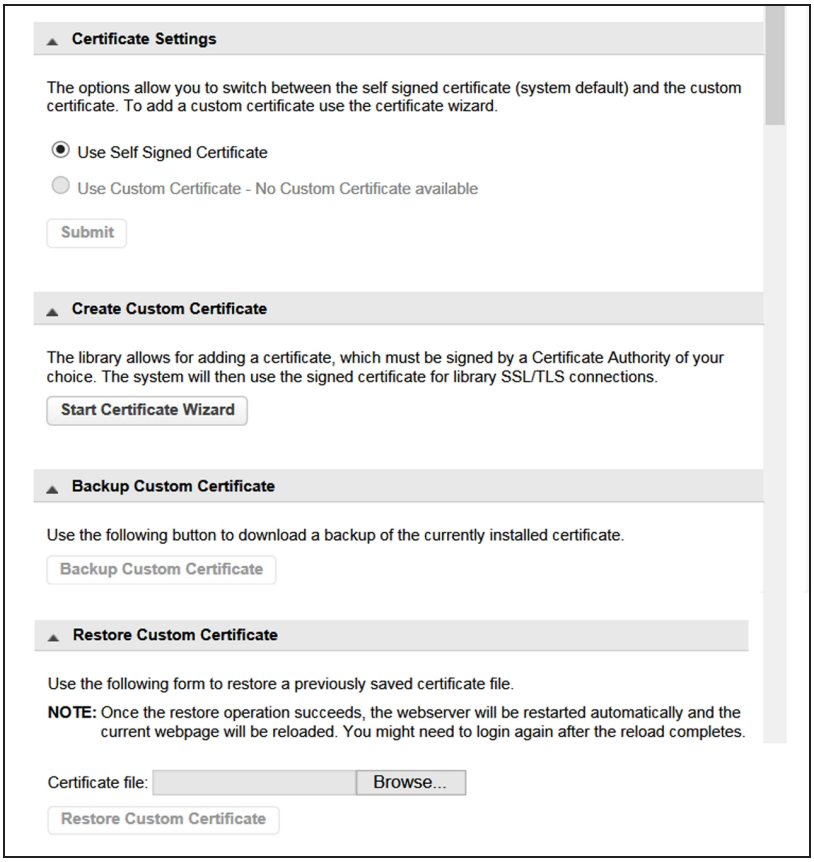


Figure 53 The Security Certificate panes of the **Configuration > Web Management** screen.

Select Certificate Settings

On the **Configuration > Web Management** screen (Figure 53), select **Use Self Signed Certificate** or, if a custom certificate is available, **Use Custom Certificate**, and click **Submit**. If you want to use a custom certificate, but one is not available, continue with Add a Security Certificate on the next page.

Add a Security Certificate

Use the following instructions to add a security certificate.

1. On the **Configuration > Web Management** screen, click **Start Certificate Wizard** to start the wizard. The Information screen displays.

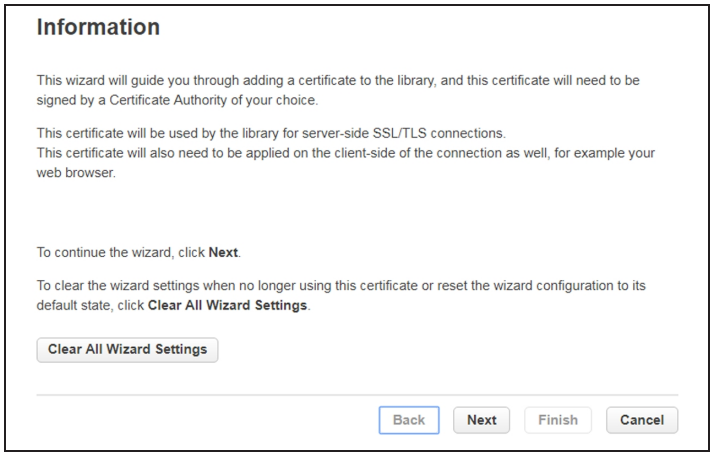


Figure 54 The Certificate Wizard Information screen.

2. If you want to clear all current wizard settings before continuing, click **Clear All Wizard Settings**.
3. Click **Next** to continue. The Certificate Signing Request screen displays.

Figure 55 The Certificate Signing Request screen.

4. Enter the Certificate Request Data and click **Generate CSR**. The certificate displays in the Certificate Sign Request pane.
5. Click **Select CSR** and copy the certificate. Provide the certificate you copied to your Certificate Authority. Once the certificate is signed, select and copy the entire certificate, and then click **Next**. The Signed Certificate screen displays.

Figure 56 The Signed Certificate screen.

6. Paste the certificate in the Signed Certificate pane and click **Next**. The Finish screen displays.

Figure 57 The Finish screen.

7. Click **Finish** to save the certificate and end the wizard.

Backup Custom Certificate

Once you have saved a custom security certificate, click **Backup Custom Certificate** (see Figure 53 on page 108) and use your browser to save the file.

Restore Custom Certificate

To restore a previously saved custom certificate, click **Browse** and use your browser to locate the certificate file. Then click **Restore Custom Certificate** (see Figure 53 on page 108).

Session Timeout

On the **Configuration > Web Management** screen, use the Session Timeout pane to configure the session timeout for the RMI/OCP.

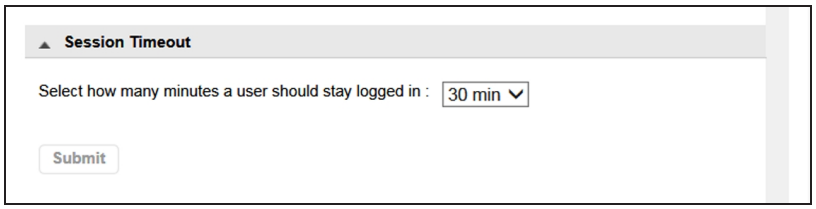


Figure 58 The Session Timeout pane of the **Configuration > Web Management** screen.

Using the drop-down, select how long the user should remain logged in (5 or 30 Minutes) and click **Submit**.

OCP/RMI Session Locking

The library supports only one OCP or RMI session at a time for Administrator, Security, or Service users. By default, when a new user logs in to the RMI or OCP, the existing user session is terminated. Use the OCP/RMI Session Locking pane of the **Configuration > Web Management** screen to change this behavior.

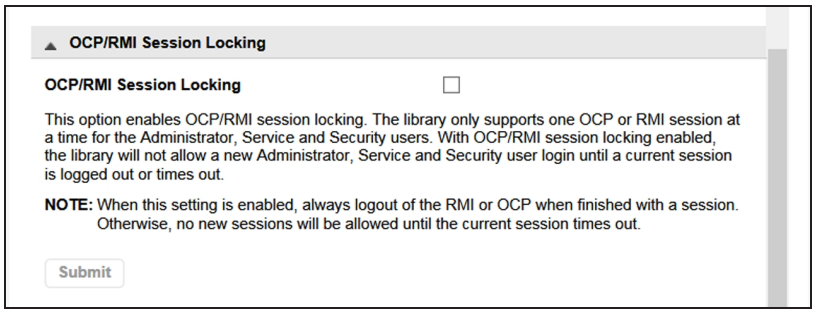


Figure 59 The OCP/RMI Session Locking pane of the **Configuration > Web Management** screen.

When OCP/RMI Session Locking is enabled, a new session does not terminate the current session and the new user will not be able to log in. Select the **OCP/RMI Session Locking** check box and click **Submit** to enable this option.

Restrict RMI Access

To restrict RMI access for the administrator and security users, in the Restricted Remote Management Interface (RMI) Login pane of the **Configuration > Web Management** screen, select the **Restricted Remote Management Interface (RMI) Login** check box and click **Submit**.

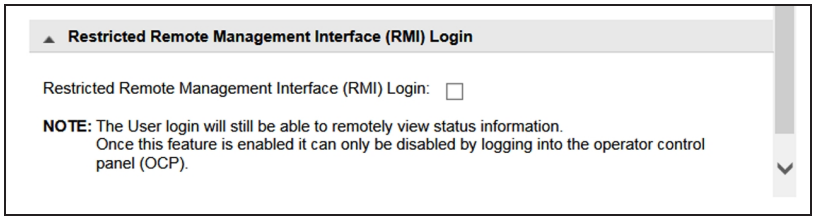


Figure 60 The Restricted Remote Management Interface (RMI) Login pane of the **Configuration > Web Management** screen.

This can be used in high security environments where policies require all configuration changes to occur from the physical library front panel.

Note: Many settings cannot be configured from the OCP.

The user and service users are still able to log in with the RMI. To remove all RMI access, unplug the Ethernet cable from the library controller.

Chapter 3 - Configuring and Using Encryption

This chapter contains instructions for configuring and using encryption in the Spectra Stack library.

CONFIGURING ENCRYPTION KEY MANAGEMENT

The **Configuration > Encryption** screen displays the available data encryption key manager types.

Notes:
- Encryption configuration changes cannot be made while media is loaded in any drive in the library.
- Encryption configuration is only accessible from the RMI.
- By default, to configure encryption, you must be logged in as the Security user. The security user can allow the administrator user to configure the type of encryption assigned to a partition.

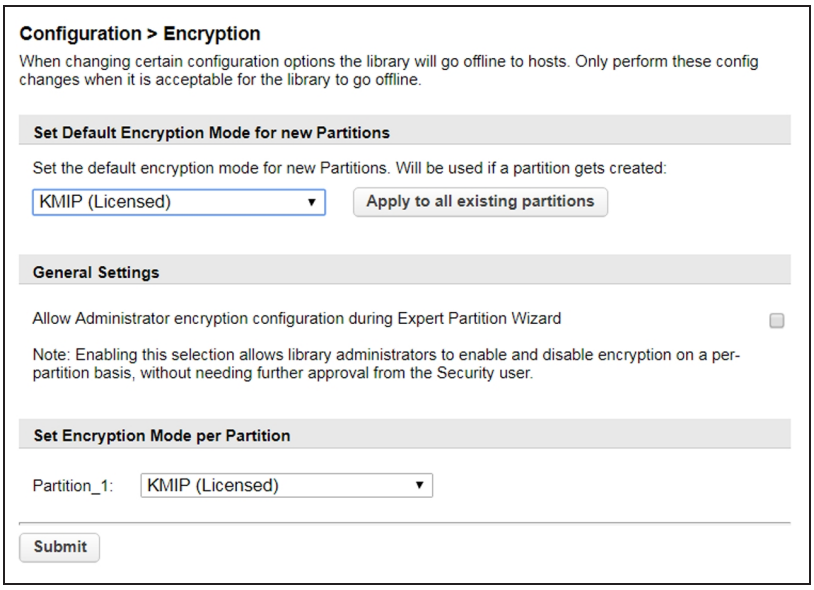


Figure 61 The Encryption screen.

Set the general encryption settings as required. If you are making multiple changes, you can select all changes and then click **Submit** once.

- To change the configured default encryption mode for a new partition, select the encryption mode and then click **Submit** at the bottom of the page.
- To apply the default settings to all existing partitions, click **Apply to all existing partitions** and then click **Submit** at the bottom of the page.
- By default, only the security user is allowed to change encryption configurations. To allow the administrator user to change encryption settings select the **Allow Administrator encryption configuration during Expert Partition Wizard** check box and then click **Submit** at the bottom of the page.
- The encryption mode can be configured for each partition in the Set Encryption Mode per Partition pane. Select the encryption mode for each partition and then click **Submit**.

CONFIGURING KMIP

If you plan to use KMIP encryption key management in some or all of your partitions, use the Key Management Interoperability Protocol (KMIP) Wizard to configure use of KMIP key management servers with the library. Access to the wizard from the Encryption menu on the RMI is only available to the Security user and requires the KMIP license key (see Configuring and Using Encryption on page 113).

After configuring and enabling KMIP encryption, a drive in a KMIP encryption-enabled partition use a secure TLS connection to request a key from the KMIP server. The server sends the encryption key to the drive, and the drive uses the key to automatically encrypt data as it is written to tape or decrypt data when it is read from tape.

For additional information on configuring KMIP servers for use with the library, see the documentation that came with your KMIP server.

Before running the wizard, verify that:

- The library configuration is complete, including defining all library partitions.
- The KMIP server is available on the network and has been configured for use with this library.

Use the following instructions to set up KMIP encryption management.

1. Select **Configuration > Encryption > KMIP Wizard**. The Wizard Information screen displays.

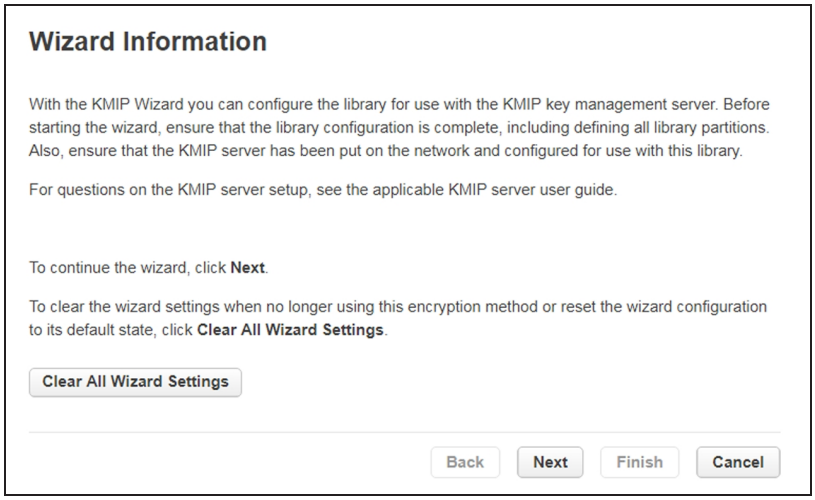


Figure 62 The KMIP Wizard Information screen.

2. To disable KMIP encryption, click **Clear All Wizard Settings**. To set up KMIP encryption, click **Next**. The Certificate Authority Information screen displays.

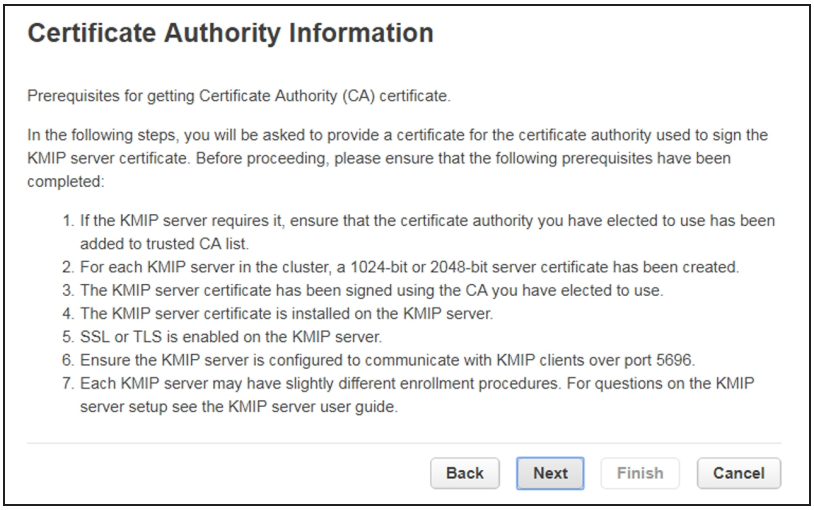


Figure 63 The Certificate Authority Information screen.

3. Ensure that all prerequisites for using the KMIP certificate are met and click **Next**. The Certificate Authority Certificate Entry screen displays.

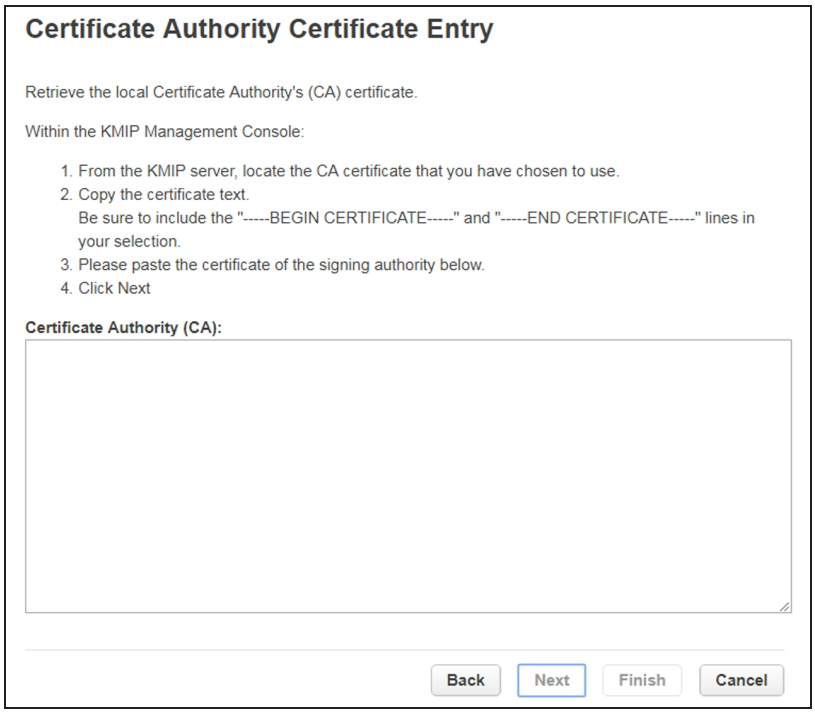


Figure 64 The Certificate Authority Certificate Entry screen.

4. Follow the on-screen instructions to obtain and copy the certificate from the KMIP server management console. Paste the certificate into the wizard and then click **Next**. The Library Certificate Information screen displays.

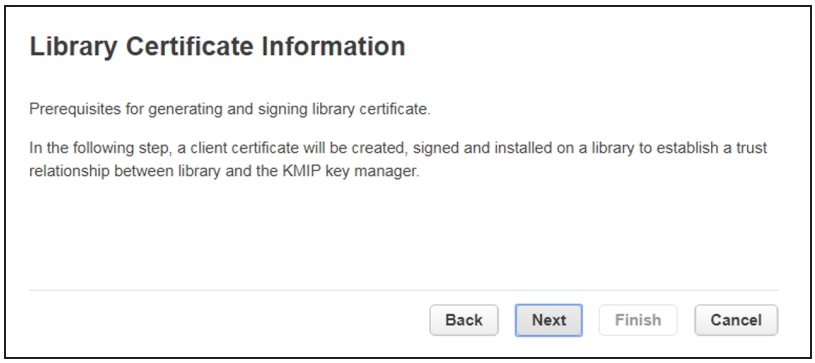


Figure 65 The Library Certificate Information screen.

5. The Library Certificate Information screen displays information about the next wizard steps. Click **Next**. The KMIP Client Configuration screen displays.

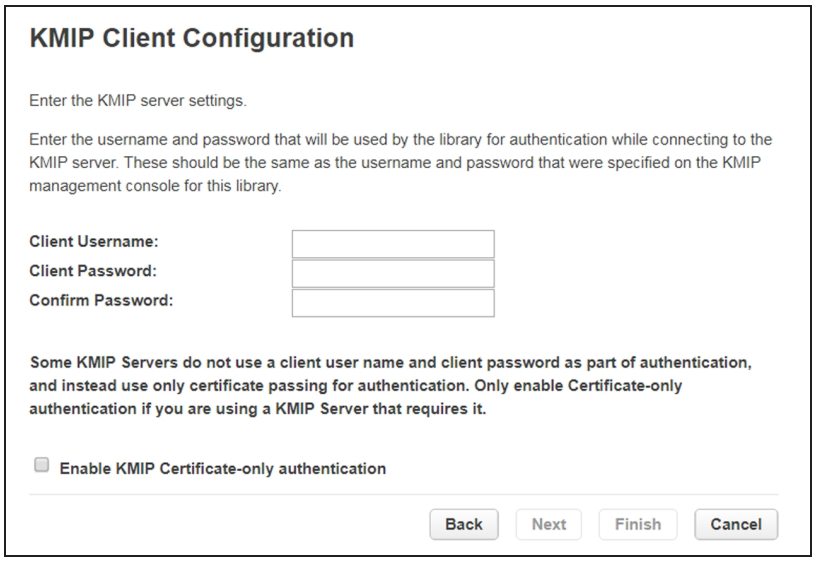


Figure 66 The KMIP Client Configuration screen.

6. The KMIP Client Configuration screen provides options for two types of server authentication.
   - If your KMIP server uses a client username and password for authentication, enter the username and password that were specified on the KMIP management console for the library. This is recommended if available.
   - If your KMIP server uses only certificate passing for authentication, select **Enable KMIP Certificate-only authentication**. Only select this option if you are using a KMIP server that requires it and you do not have a client username and password.
7. Click **Next**. The Certificate Generation screen displays.

Figure 67 The Certificate Generation screen.

8. The Certificate Generation screen displays the current library certificate, if one exists.
   - To use the current certificate, select **Keep Current Certificate** and then click **Next**. The KMIP Server Configuration screen displays. Skip to Step 10 on page 121.
   - To generate a new certificate, select **Generate New Certificate**. The wizard generates and displays a new library certificate. Click **Select Certificate** and press **CTRL-C** to copy the new certificate text, and then click **Next**. The Sign Library Certificate screen displays.

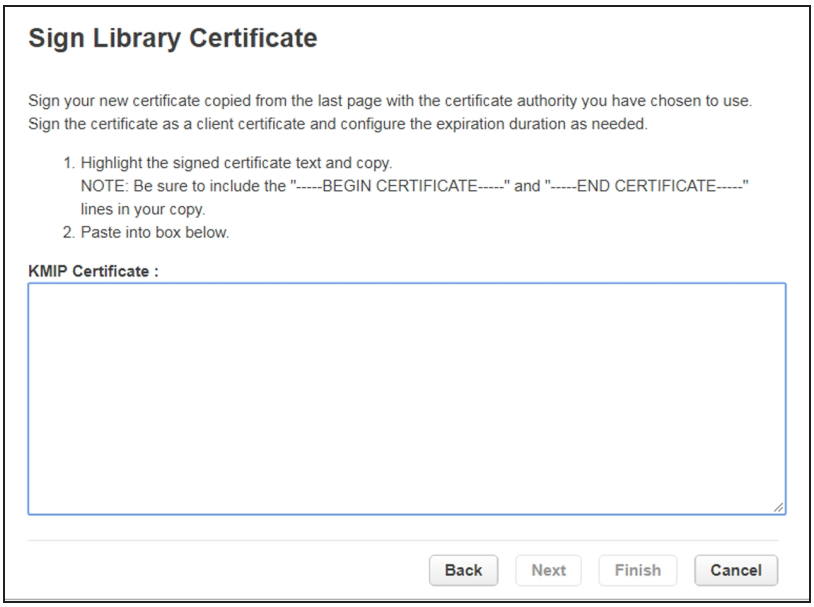


Figure 68 The Sign Library Certificate screen.

9. Sign the new library certificate with the certificate authority as a client certificate. Press CTRL-V to paste the new KMIP certificate in the box, and then click **Next**. The KMIP Server Configuration screen displays.

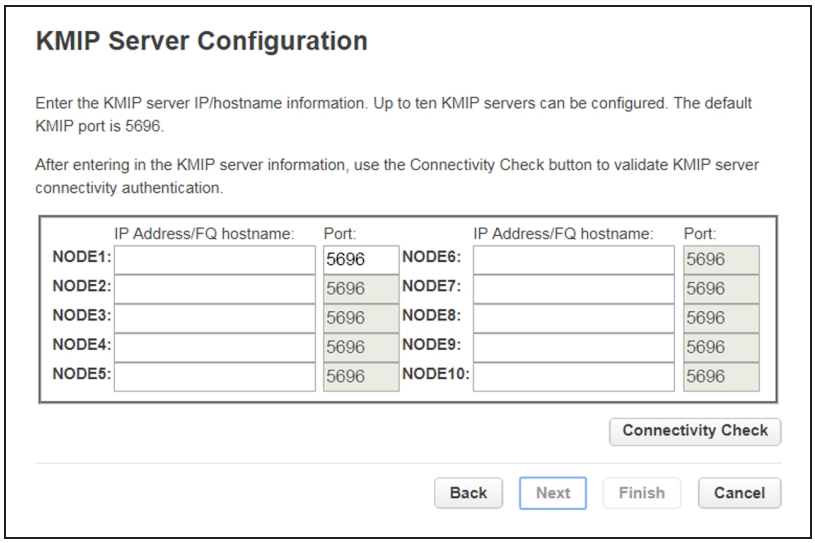


Figure 69 The KMIP Server Configuration screen.

10. In the KMIP Server Configuration screen, enter the IP address or fully-qualified hostname and port number for up to ten KMIP servers. To verify access to the KMIP server(s), click **Connectivity Check**. Click **Next** to continue. The Setup Summary screen displays.

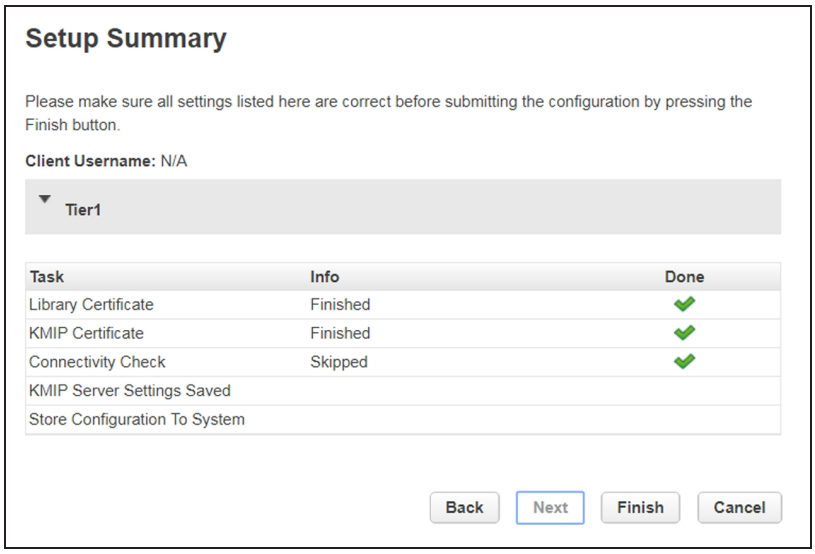


Figure 70 The Setup Summary screen.

11. The Setup Summary screen displays the settings that were configured by the wizard. Verify that the settings are correct and that no errors display in the Done column. If you need to modify any settings or fix any issues, either click **Back** to reach the applicable screen or **Cancel** out of the wizard to fix the issues and return later. When the setting are all correct, click **Finish**. The **Configuration > Encryption** screen displays (see Figure 61 on page 114).

12. Use the Set Encryption Mode per Partition pane to select **KMIP** as the encryption mode for the desired partition(s) and then click **Submit**.

    —OR—

    If you want all partitions to use KMIP Encryption, select **KMIP** as the default encryption mode, click **Apply to all existing partitions**, and click **Submit**.

CONFIGURE ENCRYPTION STANDARD

Encryption Standard is automatically included in your Spectra Stack library. For information about Encryption Pro, see Configure Encryption Professional on page 127

Log Into Encryption Standard

Only the security user can add, import, or export encryption keys, and set the Encryption User Password. If allowed by a security user, the administrator user can configure the type of encryption assigned to a partition.

1. Log into the library as the security user. **Select Configuration > Encryption > Encryption Standard**. The **Encryption User Login** screen displays.

Figure 71 Enter the encryption user password to access the encryption feature.

2. Enter the encryption password and then click **Login**.

Note: If the Encryption Password was never set, the **password is blank.**

The **Configuration > Encryption > Encryption Standard** screen displays.

Figure 72 The Encryption Standard screen.

Set or Change the Encryption Password

1. Access the encryption feature (see Log Into Encryption Standard above). The **Configuration > Encryption > Encryption Standard** screen displays (see Figure 72 on page 123).
2. To set or change the current encryption user password, enter and confirm the desired Encryption User Password and click **Submit**.

Create an Encryption Key

1. Access the encryption feature (see Log Into Encryption Standard above). The **Configuration > Encryption > Encryption Standard** screen displays (see Figure 72 on page 123).
2. Click **Add Key.** The Add Key dialog box displays.

Note: Encryption Standard only supports using one encryption key at a time. The **Import Key** and **Add Key** buttons do not display if there is already an encryption key stored in the library. If you delete the existing key, as described in Deleting an Encryption Key from the Library on page 145, they display again.

Figure 73 Enter a moniker to create a new encryption key.

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, with a maximum of 32 characters. To improve readability, use an underscore to separate words. Do not use any space characters.
- Each moniker must be a unique string of characters 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.

CAUTION If you create two monikers that are identical except for case, you are not able to retrieve your data after importing or creating a key using a different variation of the moniker.

4. Click **Submit**. The **Configuration > Encryption > Encryption Standard** screen displays showing the moniker for the newly created encryption key.

Note: If the key is not yet assigned to a partition, **N/A** displays in the **Primary Key For** column.

Figure 74 The new encryption key is listed in the Encryption Key Handling pane.

5. Export the newly created encryption key and save it to a secure location (see Export the Encryption Key on page 136).

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 135 for additional information.

Enable Encryption Standard in a Partition

How you enable Encryption Standard in a partition depends on whether you are a security user or an administrator user with permission to configure partition encryption using the Expert Partition Wizard.

Note: All of the partitions in the library go offline while partitions are configured. Ensure that host operations for all partitions are idle before running the partition wizard.

Security User

1. Navigate to **Configuration > Encryption** to access the main encryption screen.

   Figure 75 The Encryption screen.

2. In the Set Encryption per Partition pane, select **Encryption Standard** next to the partition for which you want to enable encryption and click **Submit**. The partition is updated to use the currently stored encryption key to encrypt and decrypt data in the partition.

   —OR—

   If you want all partitions to use Encryption Standard, select **Encryption Standard** as the default encryption mode, click **Apply to all existing partitions**, and click **Submit**.

Administrator User

1. Select **Configuration > Partitions > Expert Wizard** to start the Expert Partition Wizard. The Manage Partitions screen lists the current partitions.

   Figure 76 The Manage Partitions screen.

2. Select the partition for which you want to enable Encryption Standard, click **Edit,** and then click **Next**. The General Settings screen displays.

Figure 77 The General Settings screen.

3. Using the **Encryption Mode** drop-down menu, select **Encryption Standard** to enable encryption.

Note: This field is only visible if you are logged in as a security user or if the security user has configured permission for the administrator user to configure encryption used by a partition using the Expert Partition Wizard. See Configuring Encryption Key Management on page 114.

4. Click **Next** to advance through the remaining screens in the wizard. The partition is updated to use the currently stored encryption key to encrypt and decrypt data in the partition.

CONFIGURE ENCRYPTION PROFESSIONAL

Encryption Professional allows you to use multiple encryption keys in a partition.

Notes:
- A maximum of one primary and eight secondary keys can be added to a partition.
- A maximum of 100 keys can be stored in the library.

Enter License Key

Use the instructions in Add a License Key on page 70 to enable Encryption Pro in the Spectra Stack Library

Log Into Encryption Professional

Only the security user can add, import, or export encryption keys, and set the Encryption User Password. If allowed by a security user, the administrator user can configure the type of encryption assigned to a partition.

1. Log into the library as the security user. Select **Configuration > Encryption > Encryption Professional**. The **Encryption User Login** screen displays.

Figure 78 Enter the encryption user password to access the encryption feature.

2. Enter the encryption password and then click **Login**.

Note: If the Encryption Password was never set, the **password is blank.**

The **Configuration > Encryption > Encryption Professional** screen displays.

Figure 79 The Encryption Professional screen.

Set or Change the Encryption Password

1. Access the encryption feature (see Log Into Encryption Standard on page 123). The **Configuration > Encryption > Encryption Professional** screen displays (see Figure 72 on page 123).
2. To set or change the current encryption user password, enter and confirm the desired Encryption User Password and click **Submit**.

Create an Encryption Key

1. Access the encryption feature (see Log Into Encryption Standard on page 123). The **Configuration > Encryption > Encryption Professional** screen displays (see Figure 72 on page 123).

2. Click **Add Key.** The Add Key dialog box displays.

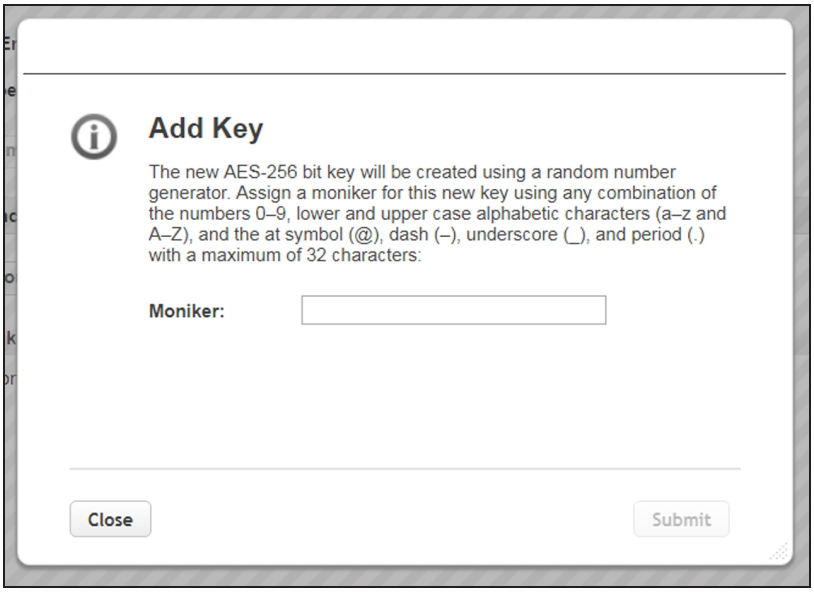


Figure 80 Enter a moniker to create a new encryption key.

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, with a maximum of 32 characters. To improve readability, use an underscore to separate words. Do not use any space characters.
- Each moniker must be a unique string of characters 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.

CAUTION If you create two monikers that are identical except for case, you are not able to retrieve your data after importing or creating a key using a different variation of the moniker.

4. Click **Submit**. The **Configuration > Encryption > Encryption Professional** screen displays showing the moniker for the newly created encryption key.

Note: If the key is not yet assigned to a partition, **N/A** displays in the **Primary Key For** column.

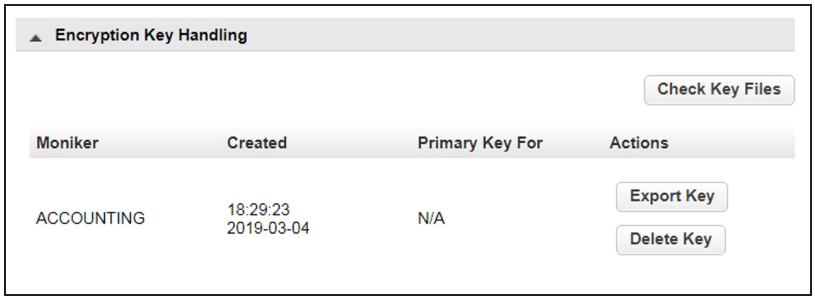


Figure 81 The new encryption key is listed in the Encryption Key Handling pane.

5. Export the newly created encryption key and save it to a secure location (see Export the Encryption Key on page 136).

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 135 for additional information.

Enable Encryption Professional in a Partition

Enabling Encryption Professional in a partition depends on whether you are a security user or an administrator user with permission to configure partition encryption using the Expert Partition Wizard.

Note: All of the partitions in the library go offline while partitions are configured. Ensure that host operations for all partitions are idle before running the partition wizard.

Security User

1. Navigate to **Configuration > Encryption** to access the main encryption screen.

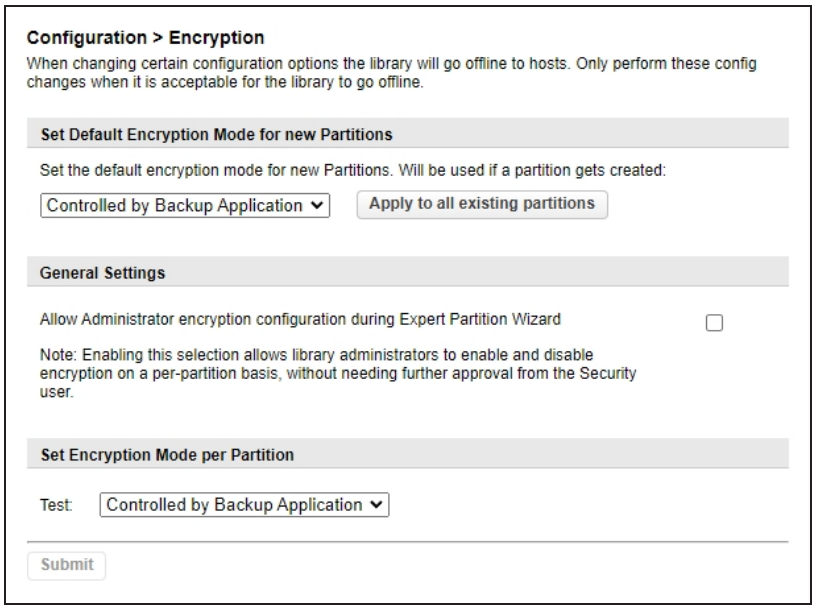


Figure 82 The Encryption screen.

2. In the Set Encryption per Partition pane, select **Controlled by Backup Application** next to the partition for which you want to enable encryption and click **Submit**. The partition is updated to use the currently stored encryption key to encrypt and decrypt data in the partition.

   —OR—

   If you want all partitions to use Encryption Professional, select **Controlled by Backup Application** as the default encryption mode, click **Apply to all existing partitions**, and click **Submit**.

Administrator User

1. Select **Configuration > Partitions > Expert Wizard** to start the Expert Partition Wizard. The Manage Partitions screen lists the current partitions.

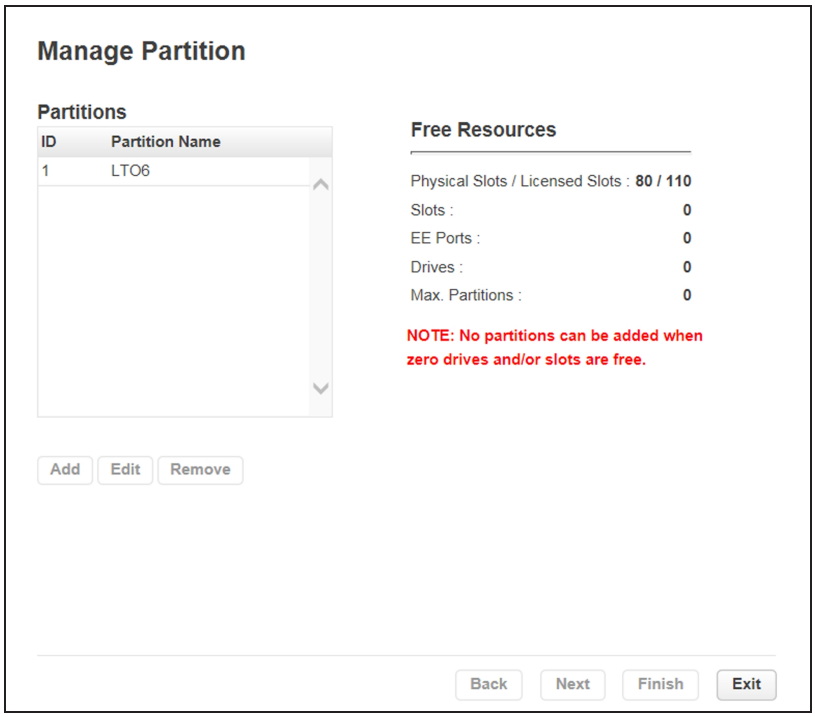


Figure 83 The Manage Partitions screen.

2. Select the partition for which you want to enable Encryption Professional, click **Edit**, and then click **Next**. The General Settings screen displays.

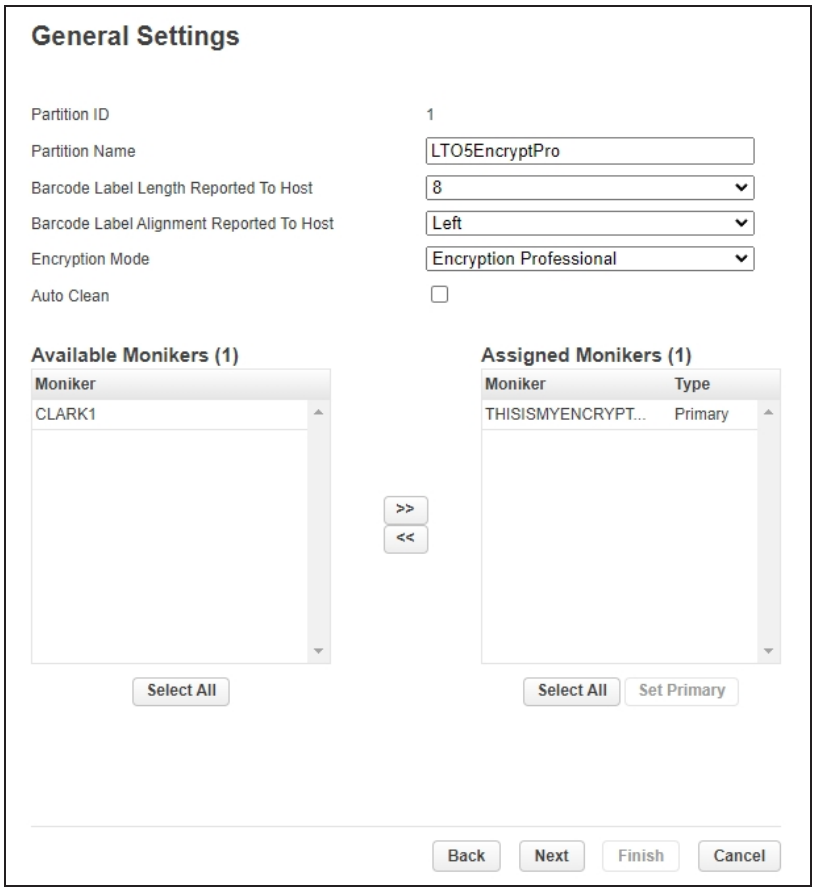


Figure 84 The General Settings screen.

3. Using the **Encryption Mode** drop-down menu, select **Encryption Professional** to enable encryption.

Note: This field is only visible if you are logged in as a security user or if the security user has configured permission for the administrator user to configure encryption used by a partition using the Expert Partition Wizard. See Configuring Encryption Key Management on page 114.

4. In the **Available Monikers** pane, select an encryption key moniker and click **>>** to assign the key to the partition.

Notes:
- A maximum of one primary and eight secondary keys can be added to a partition.
- To add all available keys, click **Select All**, then click **>>**.

5. If you added multiple encryption key monikers to the partition, set the primary key by clicking on the desired key and then click **Set Primary**.

Note: Only one primary key can be assigned to the partition.

6. Click **Next** to advance through the remaining screens in the wizard. The partition is updated to use the currently stored encryption key to encrypt and decrypt data in the partition.
7. When the wizard completes updating the partitions, click **Exit**.

EXPORTING AND PROTECTING ENCRYPTION KEYS

Creating 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 as soon as possible after you create them.

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.

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; keep them as secure (and as backed up) as your data.

As a matter of best practice, Spectra Logic recommends exporting encryption keys to a USB device instead of using email or RMI download.

Although emailing and RMI download of encryption keys are supported by the library, they present 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 or downloaded encryption keys may be located can make security audits more challenging.

Export the Encryption Key

Use the following steps to export the current encryption key:

1. Access the encryption feature (see Log Into Encryption Standard on page 123).
2. If you want to export the encryption key to a USB device, plug a USB device into the USB port on the Controller Module.
3. From the **Configuration > Encryption > Encryption Professional** screen, click **Export Key**. The Export Key dialog box displays.

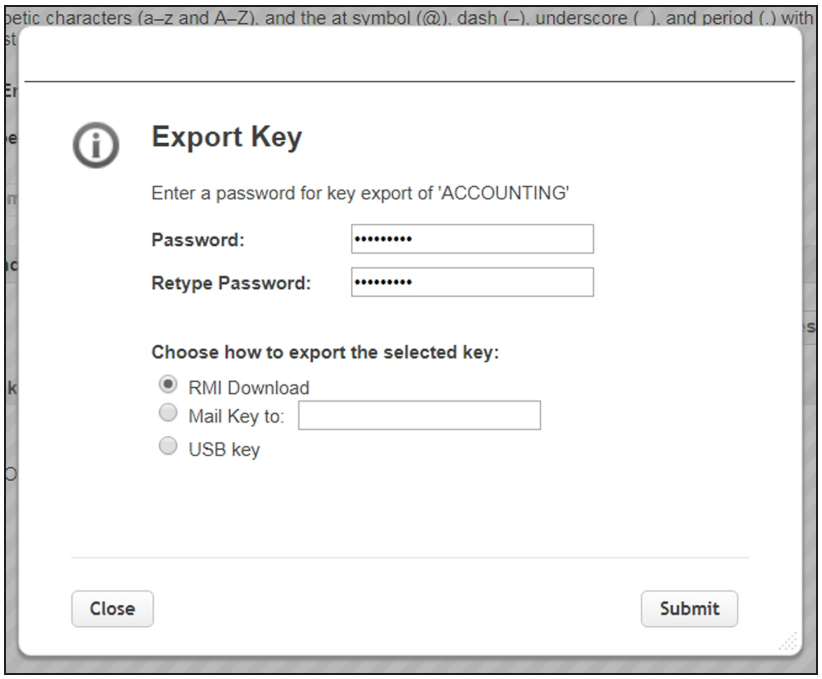


Figure 85 The Export Key dialog box.

4. On the Export Key screen, enter and verify a 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 password is used to encrypt the exported key.

5. Select the desired option and click **Submit**. An export status screen displays.

Export Type	Description
RMI Download	Save the exported key to the default location for the browser used for RMI access.
Mail Key to	Sends the encryption key as an email attachment to the email address provided. To use this option, SMTP must be enabled and the SMTP server entered. See Configuring and Using Encryption on page 113.
USB key	Saves the exported encryption key to the USB device connected to the Controller Module.

6. Make a record of the encryption key password; you need it 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.

7. Confirm that the encryption key was correctly exported.
   - **If you exported the encryption key using an RMI download** — Confirm the file exported correctly as described in Verify the Exported Encryption Key.
   - **If you exported the encryption key to a USB device**—Immediately confirm that the encrypted key copied correctly by clicking **Check Key Files** (see Figure 74 on page 124) 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.
   - 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, and then export the key again using a different USB device, beginning with Step 2 on page 136.
   - **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. Confirm that the email attachment contains a key file as described in Verify the Exported Encryption Key on the next page.

Verify the Exported Encryption Key

After exporting an encryption key, verify that the export was successful as soon as possible.

When Exported as RMI Download

1. Locate the file called *name*.bsk where *name* is the moniker you assigned to the key when it was created.
2. 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.

   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 the Encryption Key on page 136.
3. If desired, print or save a screen capture showing the attachment name and file size for an audit record showing that the file was saved, and that the key file contained information.

When Saved to a USB Device

1. Plug the USB device into a computer.
2. Examine the contents of the USB device to verify that it contains a file called *name*.bsk where *name* is the moniker you assigned to the key when it was created.
3. 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.

   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 the Encryption Key on page 136 using a different USB device.
4. If desired, save or print a screen capture of the USB directory for an audit record showing that the USB device was readable, and that the key file contained information.
5. Store the USB device in a safe location.

When Sent as an Email Attachment

1. Open the email attachment and verify that it contains a file called *name*.bsk where *name* is the moniker you assigned to the key when it was created.
2. 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.

   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 the Encryption Key on page 136.
3. If desired, print or save a screen capture showing the attachment name and file size for an audit record showing that the file was received, and that the key file contained information.
4. Save the email attachment to a safe location from which you can copy it to a USB device, if needed.

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 the Encryption Key on page 136).

CAUTION

As a matter of best practice, Spectra Logic recommends exporting encryption keys to a USB device or RMI download 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 was successfully exported 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 library. 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 142.
- 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 key copies:	
Location of each copy:	
Password(s) associated with exported copy of the moniker:	
Location of cartridges containing data 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 and assigned to the partition containing the encrypted tape(s), 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 and assigned to the partition before the data can be decrypted. Once the required encryption key is assigned to the partition, standard restore procedures are unchanged.

Use the Key Stored in the Library

This section describes how to restore data if the key used to encrypt the data is currently stored in the library.

Note: If the data was not encrypted using the currently loaded key, 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 before the data can be restored.

If the encryption key is not currently assigned to the partition, modify the partition as described in Enable Encryption Standard in a Partition on page 125. If the encryption key is assigned to a partition, continue with the following steps.

1. If necessary, import the cartridges containing the data to be restored into the library partition to which the encryption key is assigned.
2. 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 is not present in 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 and 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 data on the cartridge is decrypted when read from tape.

IMPORTANT In addition to the file containing the exported key, you need the key password in order to import the key into the library. Without the key password, you are not able to import the encryption key.

Note: If an encryption key is already stored in the library, you must first delete that key as described in Deleting an Encryption Key from the Library on page 145. You can then import another key.

Use the following steps to import a key from the RMI or a USB device:

1. If you are importing the key from a USB device, plug the USB device containing the exported encryption key you want to import into the Controller Module.
2. Access the encryption feature (see Log Into Encryption Standard on page 123 or Log Into Encryption Standard on page 123). The Encryption screen displays.

Figure 86 The Encryption Professional screen.

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

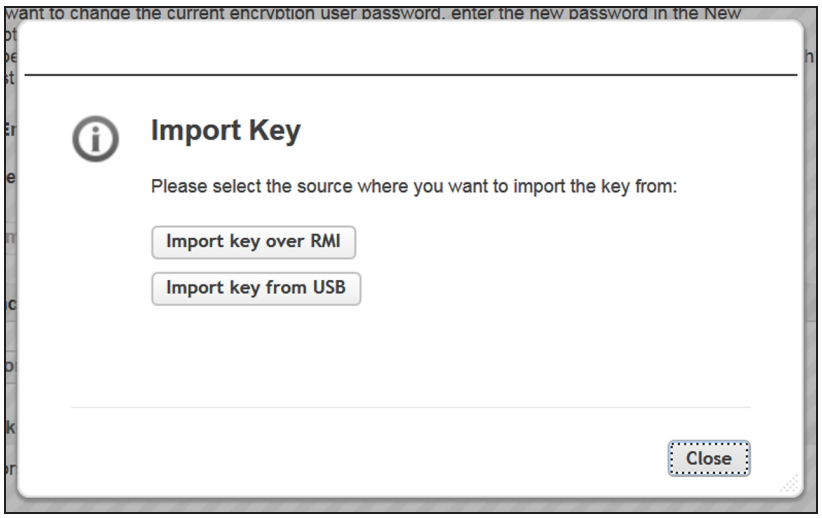


Figure 87 The Import Key dialog box.

- **If you select Import key over RMI**, the dialog box updates. Use your browser to locate the key file and enter the password used to export the key file and then click **Submit**.

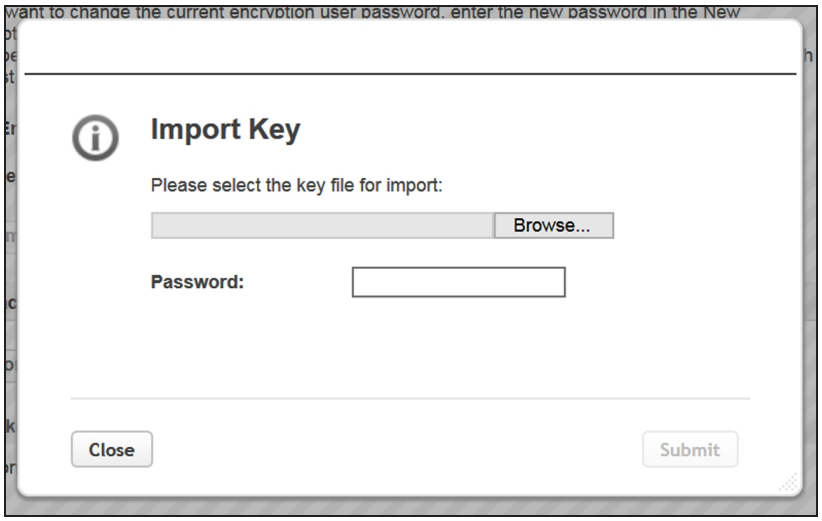


Figure 88 Import a key over RMI.

- **If you select Import key from USB**, the dialog box updates to show all key files found on the USB device. Select the file you want to import, enter the password used to export the key, and click

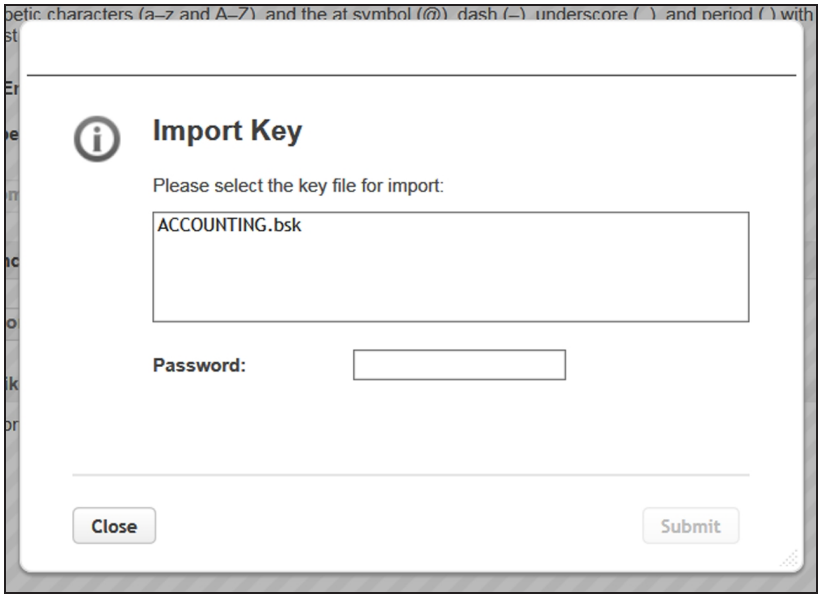


Figure 89 Import a key from USB.

4. When the key import completes, the **Configuration > Encryption > Encryption Professional** screen displays, showing the moniker of the newly imported key (see Figure 74 on page 124).
5. Assign the imported key to the partition which contains the encrypted cartridge (see Enable Encryption Standard in a Partition on page 125).
6. Use your storage management software to restore the data.

Deleting an Encryption 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 Encryption Standard on page 123 or Log Into Encryption Standard on page 123).
2. Export at least one copy of the key and store it in a safe location (see Export the Encryption Key on page 136).
3. If the encryption key you plan to delete is assigned to a partition, edit the partition to disable encryption (see Disabling Encryption in a Partition on the next page).

   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 re-import the key.

4. From the **Configuration > Encryption > Encryption Professional** screen (see Figure 74 on page 124), click **Delete Key** next to the key you want to remove from the library. The Delete Key confirmation dialog box displays.

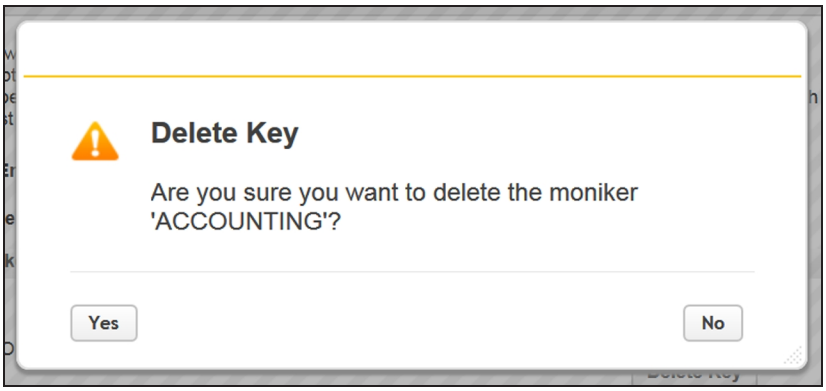


Figure 90 The Delete Key confirmation dialog box.

5. Click Yes to delete the key.
6. A key deletion successful message briefly displays and then the **Configuration > Encryption > Encryption Professional** with the moniker is no longer listed on the screen.

Disabling Encryption in a Partition

How you disable encryption in a partition depends on whether you are a security user or an administrator user with permissions to configure partition encryption using the Expert Partition Wizard.

Note: All of the partitions in the library go offline while partitions are configured. Ensure that host operations for all partitions are idle before running the partition wizard.

Security User

1. Navigate to **Configuration > Encryption** to access the main encryption screen.

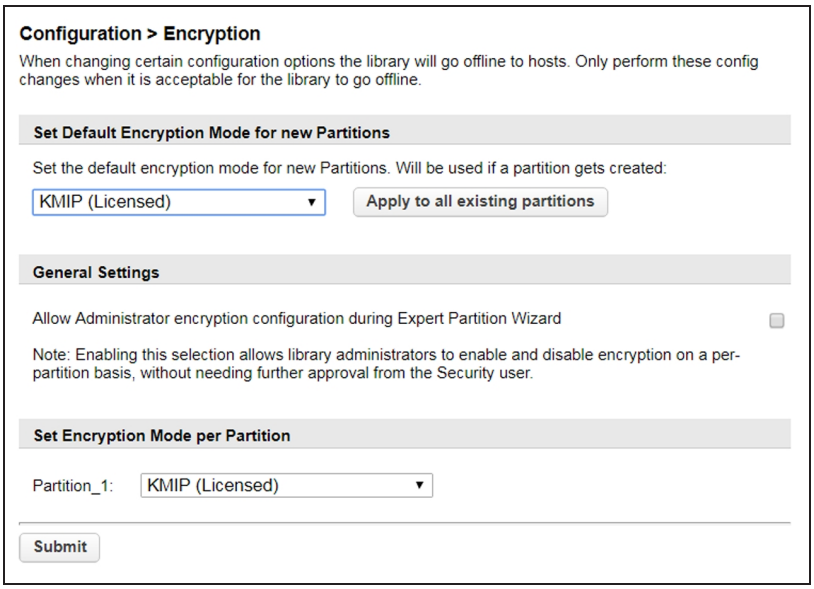


Figure 91 The Encryption screen.

2. In the Set Encryption per Partition pane, select **Controlled by Backup Application** next to the partition for which you want to disable encryption and click **Submit**. The partition is updated.

   —OR—

   If you want to disable encryption in all partitions, select **Controlled by Backup Application** as the default encryption mode, click **Apply to all existing partitions**, and click **Submit**.

Administrator User

1. Select **Configuration > Partitions > Expert Wizard** to start the wizard. The Manage Partitions screen lists the current partitions.

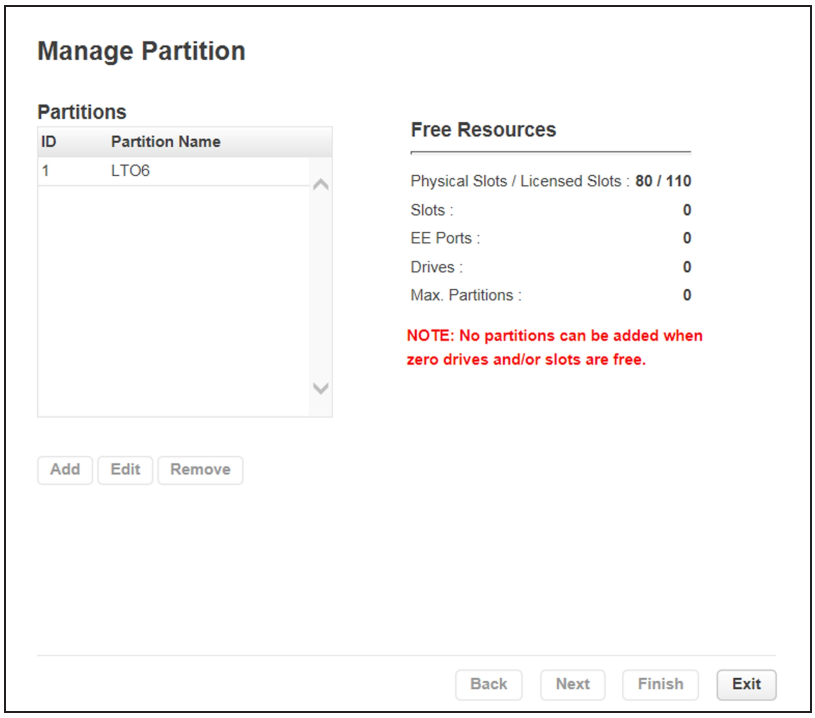


Figure 92 The Manage Partitions screen.

2. Select the partition in which you want to disable encryption, click **Edit,** and then click **Next**. The General Settings screen displays.

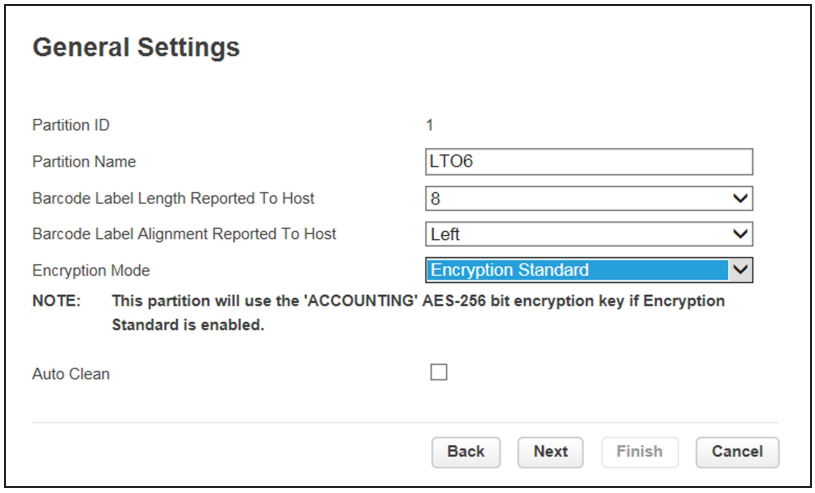


Figure 93 The General Settings screen.

3. Using the **Encryption Mode** drop-down menu, select **Controlled by Backup Application** to disable encryption.

   Note: This field is only visible if you are logged in as a security user or if the security user has configured permission for the administrator user to configure encryption used by a partition using the Expert Partition Wizard. See Configuring Encryption Key Management on page 114.

4. Click **Next** to advance through the remaining screens in the wizard.

CHAPTER 4 - OPERATING THE LIBRARY

This chapter contains instructions for using your Spectra Stack tape library. Click **Operations** on the Home screen to access the operations features.

MOVING MEDIA

You can move a tape cartridge located in a source element to an available destination element within the same partition from the **Operation > Move Media** screen.

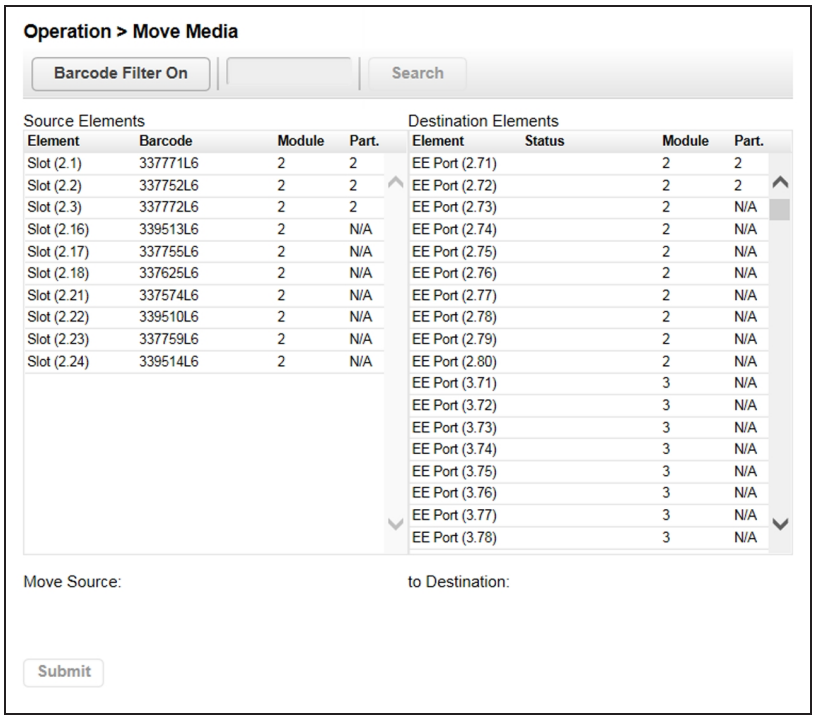


Figure 94 The Move Media screen.

- **Source Elements** - Tape drives, enabled EE ports, and storage slots that contain a tape cartridge
- **Destination Elements** - Tape drives, enabled EE ports, and storage slots that do not contain a tape cartridge

Tape drives are in the order of their drive numbers. Tape drives are numbered from the physical bottom of the library starting with Drive (1).

Slots are listed in the order of the slot numbers. Slots are numbered (*m*.*s*), where *m* is the module number and *s* is the slot within the module. For example, the tape numbered (1, 5) is present in the 5th slot of the first module.

Filtering Based on Barcode

To see a subset of the cartridges in the library based on tape barcodes, enter some or all of the barcode label characters in the search area, and click **Search**. The Source Element list updates to display only the cartridges with labels that include the characters in the search box.

To perform a different search or display all of the available cartridges, click **Barcode Filter Off**.

Moving a Cartridge

1. Select the cartridge from Source Elements.
2. Select the destination element from Destination Elements.
3. Click **Submit**.

OPENING THE EE PORT

From the Home screen, click **Open EE Port** or navigate to **Operations > Open EE Port** to see the status of EE port(s) and open any enabled EE port in the library. An EE port must be enabled before it can be opened. To enable an EE port, see Enabling or Disabling EE Ports on page 82. To determine which magazine slots belong to a partition, see Using Partition Map Graphical View on page 168.

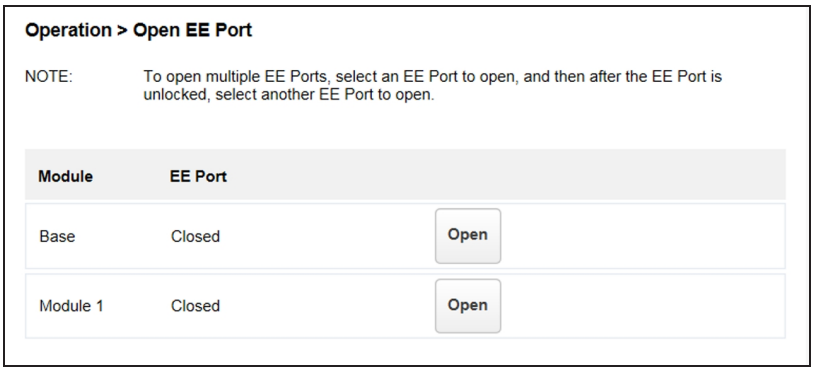


Figure 95 The Open EE Port screen.

To open an EE port, click **Open** for the appropriate EE port. The library releases the lock. Open the door in the appropriate module and then pull the EE port out of the library to access the EE slots. Close the magazine access door after reinserting the EE port.

WARNING Hazardous moving parts exist inside this product. Do not insert tools or any portion of your body into the interior of the library through the EE port door.

Note: If you do not open the door and access the EE port within the automatic re-lock duration, the EE port re-locks. See Enabling or Disabling EE Ports on page 82 to change the automatic re-lock duration.

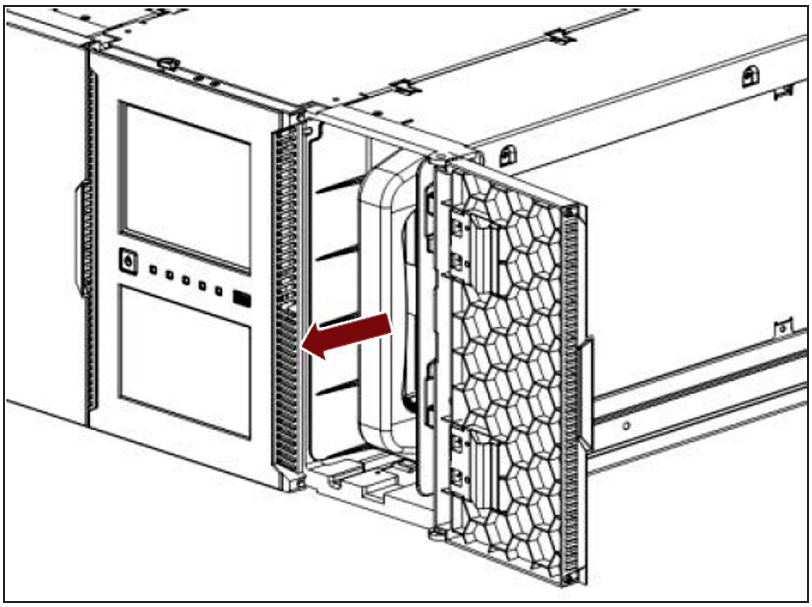


Figure 96 Pull the EE Port magazine out of the library.

OPENING A MAGAZINE

You can unlock any magazine in the library from the **Operation > Open Magazine** screen. To determine which magazine slots belong to a partition, see Using Partition Map Graphical View on page 168.

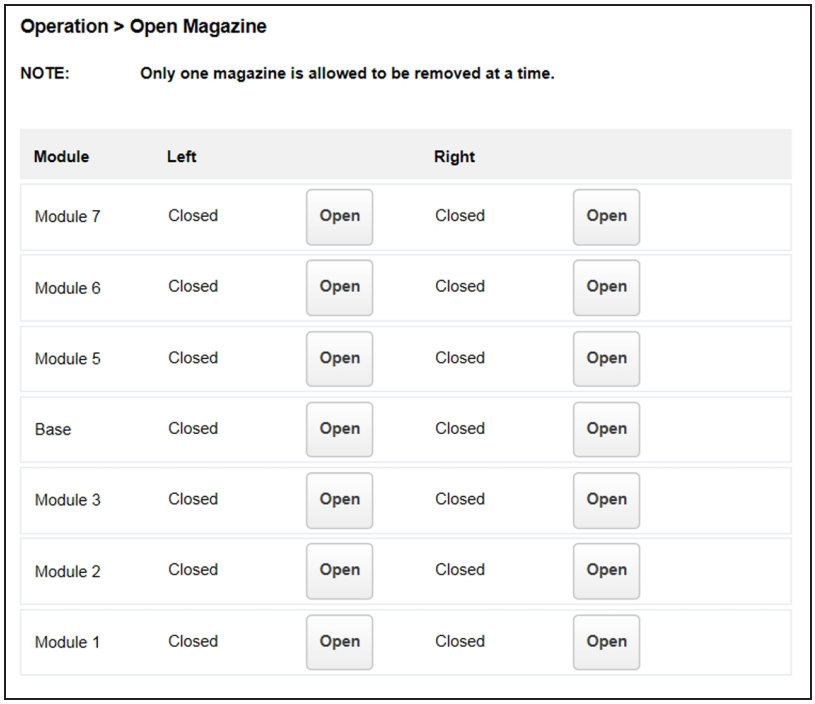


Figure 97 The Open Magazine screen.

To unlock a magazine, click **Open** for the appropriate magazine. The library releases the lock. You can then open the appropriate door and pull the magazine out of the library to access the storage slots.

Notes:
- Opening a magazine takes the entire library offline.
- If you do not open the door and access the magazine within the automatic re-lock duration, the magazine re-locks. See Enabling or Disabling EE Ports on page 82 to change the automatic re-lock duration.

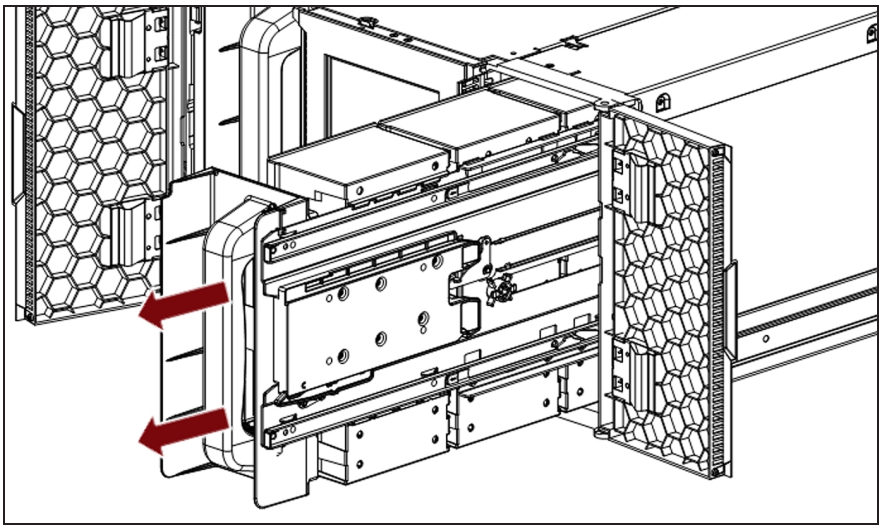


Figure 98 Pull the magazine out of the library.

Close the magazine access door after reinserting the magazine.

CLEANING A TAPE DRIVE

You can initiate a drive cleaning operation from the **Operation > Clean Drive** screen.

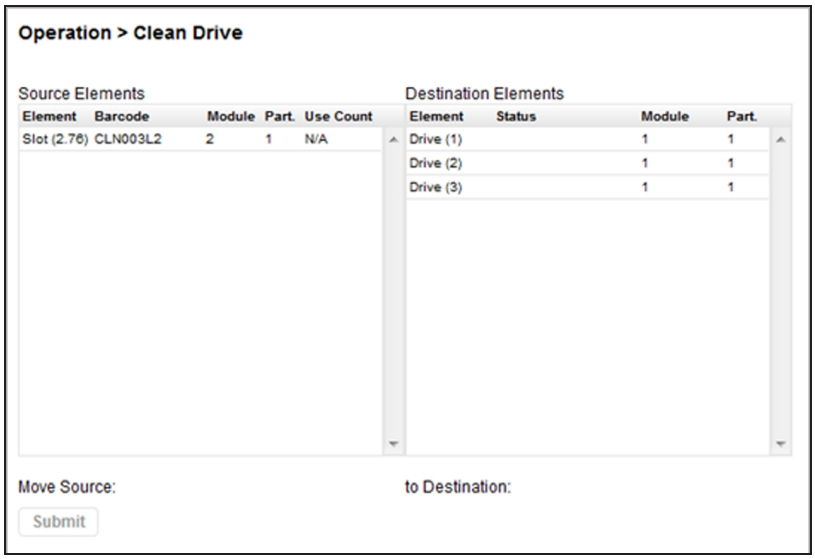


Figure 99 The Clean Drive screen.

1. Select a cleaning cartridge from the Source Elements list. The library uses the barcode label to identify cleaning cartridges.

   If no cleaning cartridges are available, load one into an EE port or magazine slot.

2. Select the tape drive to be cleaned from the Destination Elements list.

   Tape drives currently containing a cartridge are not listed. To clean a tape drive not listed, move the cartridge out of the drive.

3. Click **Submit**.

FORCING A DRIVE TO EJECT A CARTRIDGE

The force drive media eject operation attempts to force the tape drive to eject the cartridge and place it into an open slot. Only the Administrator user can force eject a tape cartridge.

Before performing this operation, it is recommended that you attempt to eject the tape using your backup software or a library move media operation (see Moving Media on page 151). While a cartridge is being force ejected, a window indicating the process is ongoing displays. No operations are available until the force eject completes.

Note: If the drive has difficulty ejecting the cartridge, the media is possibly bad or damaged. Contact Spectra Logic Technical Support for assistance. See Contacting Spectra Logic on page 10.

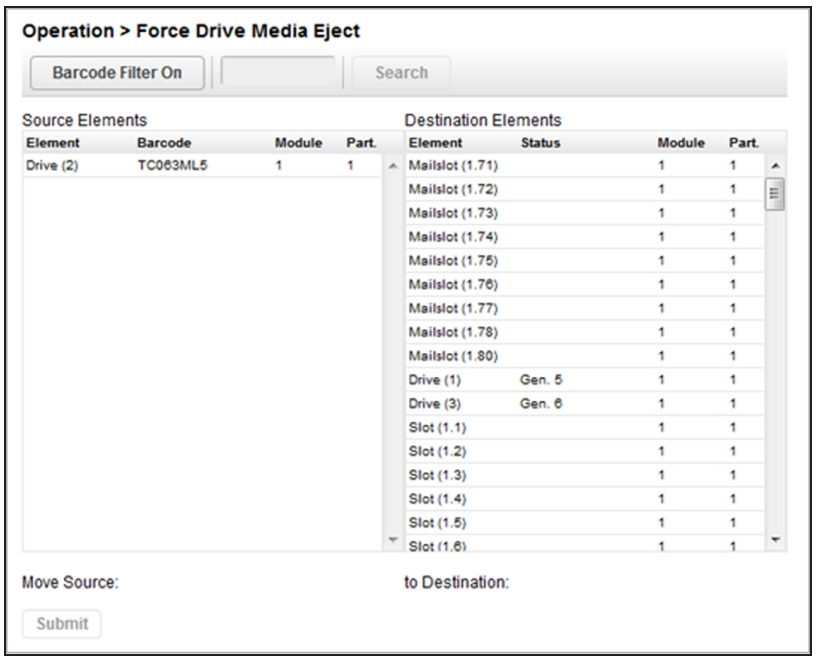


Figure 100 The Force Drive Media Eject screen.

1. Navigate to the **Operation > Force Drive Media Eject** screen.
2. Select the drive for which you want to force a tape ejection in the **Source Elements** list.
3. Select the destination in the **Destination Elements** list.
4. Click **Submit**.

RESCANNING THE CARTRIDGE INVENTORY

To rescan the cartridges in the library, navigate to the **Operation > Rescan** screen and click **Rescan**. The library changes to Scanning status and is unavailable to perform other operations until the scan completes.

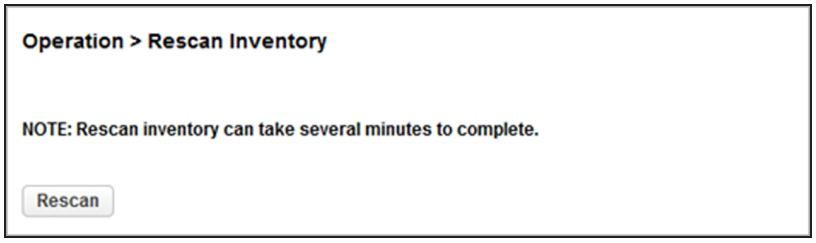


Figure 101 The Rescan Inventory screen.

Chapter 5 - Viewing Library Status

This chapter contains instructions for viewing library status. To access the status area, from the Home screen, click **Status**.

VIEWING LIBRARY AND MODULE STATUS

Summary information and status is displayed in the top banner and left side bar of the interface. For additional library module configuration and status information navigate to the **Status > Library Status** screen.

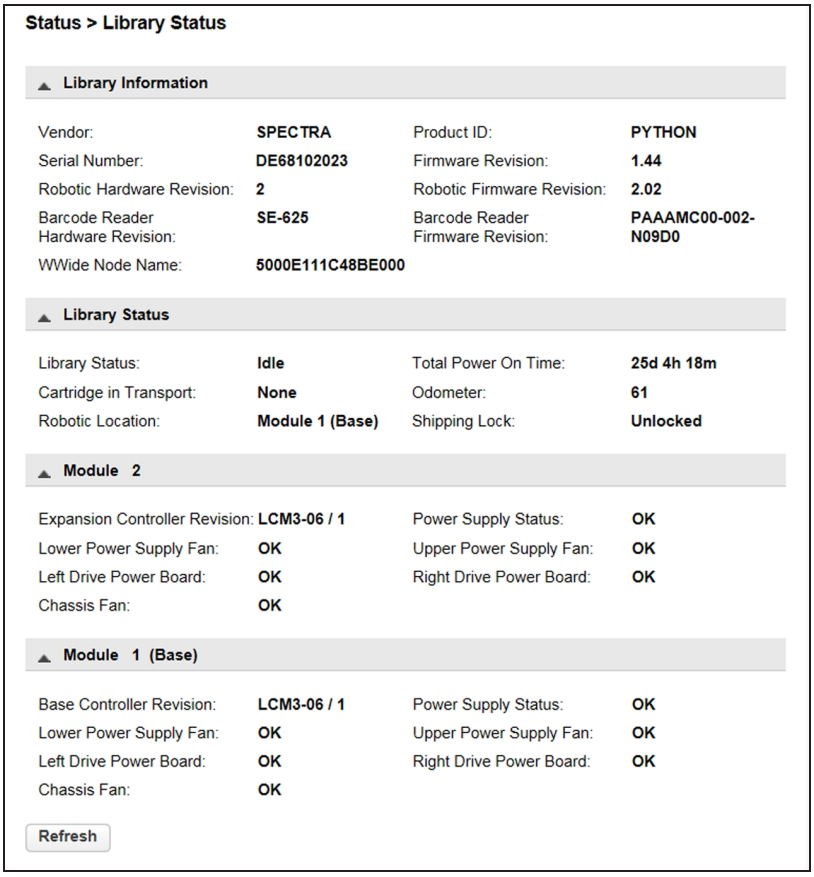


Figure 102 The Library Status screen.

Field	Description
Library Information	
Vendor	SPECTRA
Serial Number	Library serial number.

Field	Description
Robotic Hardware Revision	Hardware revision of the robotic hardware.
Barcode Reader Hardware Revision	Hardware revision of the barcode reader.
WWide Node Name	A worldwide unique identifier that the library reports over SCSI and can be used by operating systems or software applications to identify and track the library.
Product ID	PYTHON
Library Information (continued)	
Firmware Revision	Version of the currently installed library firmware.
Robotic Firmware Revision	Version of the currently installed robotic assembly firmware. The robotic assembly firmware is bundled and installed with the library firmware.
Barcode Reader Firmware Revision	Version of the currently installed barcode reader firmware. The barcode reader firmware is bundled and installed with the library firmware.
Library Status	
Library Status	• **Idle** - The library robotic assembly is ready to perform an action. • **Moving** - The library robotic assembly is moving a cartridge. • **Scanning** - The library robotic assembly is performing an inventory of cartridges. • **Offline** - The library robotic assembly has been taken offline by the library.
Cartridge in Transport	When applicable, displays the barcode label of the cartridge currently in the robotic assembly.
Total Power On Time	Total time that the controller module has been powered on since it was manufactured using the format *dd-hh-mm*.
Odometer	Robotic assembly move count.

Field	Description
Robotic Location	Displays the module where the robotic assembly is currently located.
Shipping Lock	Indicates whether the robotic assembly is unlocked or locked for shipment. For normal library operations the lock should always display as **Unlocked**.
Module Status	
Base Controller Revision or Module Controller Revision	Hardware revision of the controller board currently installed in the module.
Left Drive Power Board Status	Status of the drive power board for the top three half-height drive slots in the module.
Right Drive Power Board Status	Status of the drive power board for the lower three half-height drive slots in the module.
Power Supply Status	Displays the status of power supplies.
Lower/Upper Power Supply Fan	Displays the status of power supply fans.
Chassis Fan	Displays the status of the chassis fan.

USING INVENTORY LISTS

The inventory list displays elements, such as slots and tape drives, as well as information about any cartridges currently located in an element.

- To view the elements organized by module, use **Status > Cartridge Inventory > List View**.
- To see the elements organized by logical library or partition, use **Status > Partition Map > List View**.

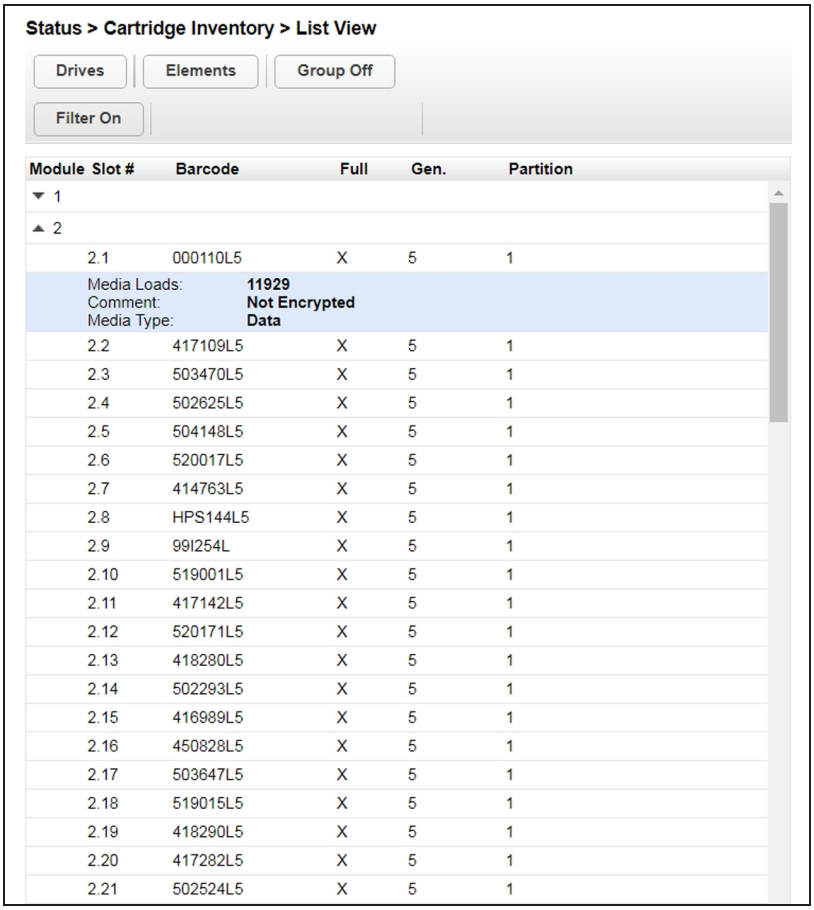


Figure 103 The Cartridge Inventory List View screen.

The Inventory List screen displays the following information:

Field	Description
Module	The module number. Click the arrow to the left of the module number to expand or collapse the inventory display for that module.
Slot #	The slot number in the form <*module*>.<*slot*>, where *module* is the module number and *slot* is the slot number in that module. See Element Numbering on page 37.
Label	The barcode label of the tape cartridge present in the element.
Full	An **X** displays if a cartridge is present in the element.
Gen	The LTO generation of the cartridge.
Partition	The partition number to which the element is assigned. To determine the partition name associated with the partition number, see Using Partition Map Configuration Status on page 170.

Clicking a full slot displays the following information about the media in the slot:

Field	Description
Media Loads	The number of media loads.
Encryption	Indicates whether data on this media is encrypted or not encrypted.
Media Type	Indicates whether the cartridge is a data or cleaning cartridge.

Filtering by Barcode Label

Use the following instructions to see a subset of the cartridges in the library based on tape barcodes.

1. Click **Filter On**. The search box displays.
2. Enter characters into the search box and click **Search**.

Notes:
- The characters can be anywhere in the barcode label.
- The search characters are not case sensitive.
- There are no wildcards.

To disable filtering, click **Filter Off**.

Listing Just Drives or Cartridges

- To limit the list to tape drives, click **Drives**. The button changes to read **Slots.** Click **Slots** to return to viewing all elements.
- To limit the list to tape cartridges, click **Cartridges**. The button changes to read **Elements**. Click **Elements** to return to viewing all elements.

Viewing Elements by Group

When the list is grouped, you can expand or contract the list for each group by clicking the triangle next to the number in the first column (Partition or Module). Grouping is enabled by default.

To disable grouping, click **Group Off**.

To enable grouping, click **Group On**.

USING THE CARTRIDGE INVENTORY GRAPHICAL VIEW

The cartridge inventory graphical view displays library elements, such as slots and tape drives, with information about the cartridge stored in the element.

- To see the elements organized by module, from **Status**, navigate to **Cartridge Inventory > Graphical View**.
- To see the elements organized by logical library or partition, see Using Partition Map Graphical View on page 168.

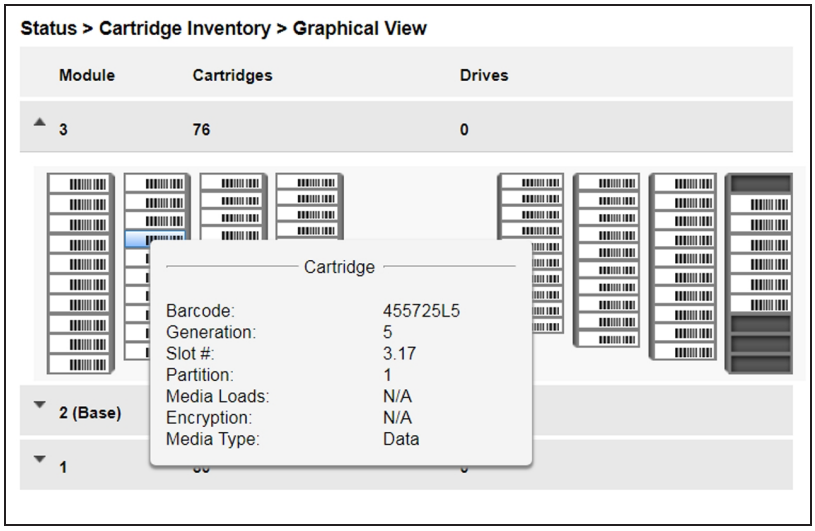


Figure 104 The Cartridge Inventory Graphical View screen.

Moving the mouse over a drive or cartridge to display additional information in a pop-up window.

Field	Description
Drive Information	
Drive	LTO generation of drive and format (Full Height or Half Height).
Drive #	The drive number. Tape drives are numbered from the bottom of the library up to the top beginning with "1".

Field	Description
Serial #	The serial number assigned to the tape drive by the library.
Cartridge Information	
Barcode	Barcode data on label.
Generation	LTO generation of the cartridge.
Slot #	The slot number in the form <*module*>.<*slot*>, where *module* is the module number and *slot* is the slot number.
Partition	The partition number to which the cartridge is assigned. To determine the partition name associated with the partition number, see Using Partition Map Configuration Status on page 170.
Media Loads	The number of media loads.
Encryption	Indicates whether data on this media is encrypted or not encrypted.
Media Type	Indicates whether the cartridge is a data or cleaning cartridge.

Warning states and error states for drives and cartridges are indicated with icons. See

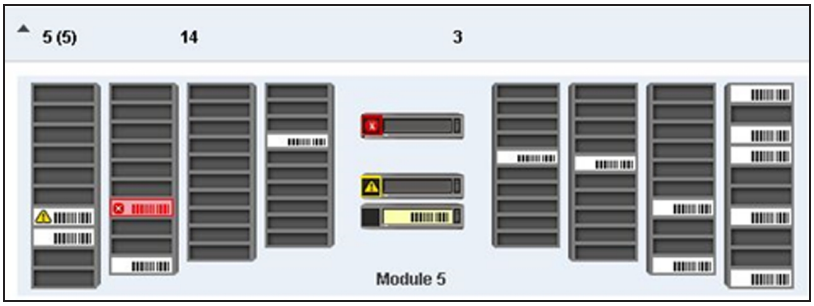


Figure 105 The Cartridge Inventory Graphical View warnings.

USING PARTITION MAP GRAPHICAL VIEW

To see the elements organized by logical library or partition, navigate to **Status > Partition Map > Graphical View**.

For each module, the graphical view of the partition map, from left to right, displays the left magazine banks from front to back, the drives in the module, and the right magazine banks from back to front. Storage slots display in groups of five. If the EE port in the module is enabled, the right most bank displays single slots with slot numbers preceded by the letters “EE”. If an element is configured in a partition, the partition number displays on the element. To determine the partition name associated with the partition number, move the mouse over the partition number.

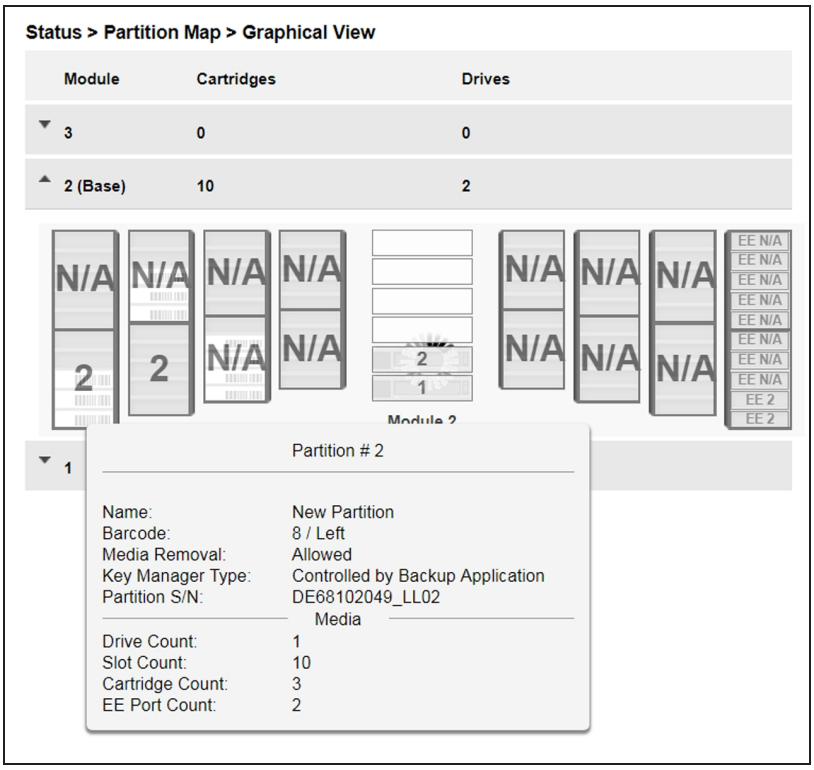


Figure 106 The Partition Map Graphical View screen.

Moving the mouse over a partition or drive displays additional information in a pop-up window:

Field	Description
Partition Information	

Field	Description
Name	Partition name.
Barcode	Barcode reporting settings. See Step 3 and Step 4 on page 90 for more information.
Media Removal	Indicates whether media removal is allowed or prevented by the host.
Key Manager Type	The type of encryption used by the partition.
Partition S/N	Serial number of the partition as seen by the host software.
Drive Count	Number of drives configured in this partition.
Slot Count	Number of slots configured in this partition.
Media Count	Number of cartridges in this partition.
EE Port Count	Number of EE ports configured in this partition.
Drive Information	
Drive #	The drive number. Tape drives are numbered from the bottom of the library up to the top beginning with "1".
Drive	LTO generation of the drive and format (Full Height or Half Height).
Serial #	The serial number assigned to the tape drive by the library.
Partition	The partition number to which the drive is assigned.
If a cartridge is loaded in the drive	
Partition	The partition number to which this cartridge is configured.
Barcode	Barcode data on label.
Generation	LTO generation of the cartridge.

USING PARTITION MAP CONFIGURATION STATUS

To see the configuration of a partition, its elements and their status, from **Status**, navigate to **Partition Map > Configuration Status**.

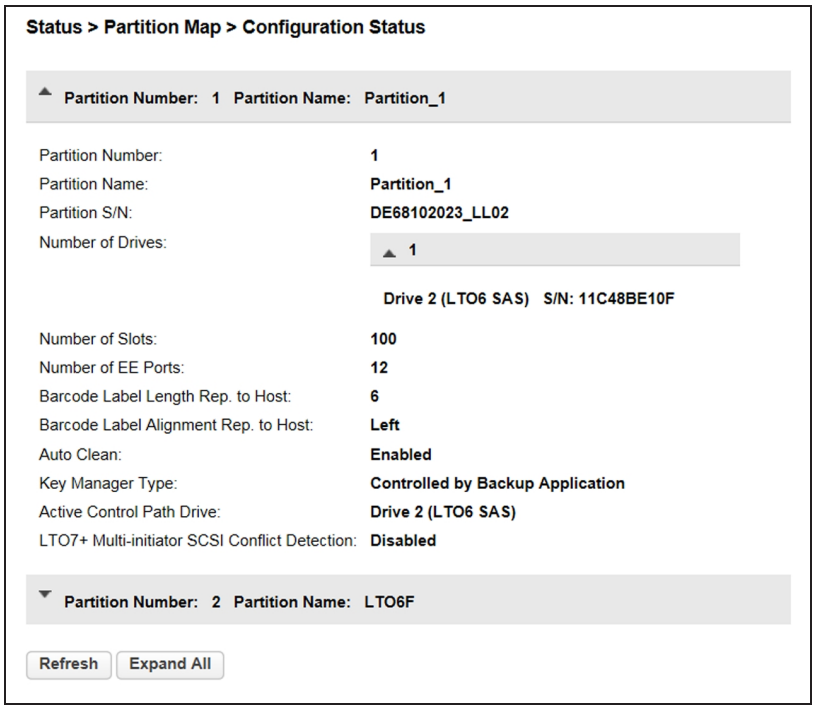


Figure 107 The Partition Map Configuration Status screen.

The Configuration Status screen displays the following information:

Field	Description
Partition Number	The partition number.
Partition Name	The partition name.
Partition S/N	The partition serial number.
Number of Drives	Number of drives configured in this partition.
Number of Slots	Number of slots configured in this partition.
Number of EE Ports	Number of EE ports configured in this partition.

Field	Description
Barcode Label Length Rep. to Host	Barcode length and direction reported to the host. See Step 3 and Step 4 on page 90 for more information.
Barcode Label Alignment Rep. to Host	Barcode alignment reported to the host.
Auto Clean	Indicates whether automatic cleaning of drives is enabled or disabled.
Key Manager Type	The type of encryption (host or KMIP) used by the partition. See Configuring the Library on page 57 for more information.
Active Control Path Drive	A drive configured in the partition that provides the control path to the library robotics.
LTO7+ Multi-initiator SCSI Conflict Detection	Whether the library generates a warning event if it detects more than a single host WWNN accessing a drive. See Step 7 on page 90 for more information.

Listing Just Drives or Partitions

To limit the list to tape drives, click **Drives**. The button changes to read **Partition.** Click **Partitions** to return to viewing all elements.

VIEWING DRIVE STATUS

In the **Status > Drive Status** screen you can see the configuration and status of each drive installed in the library.

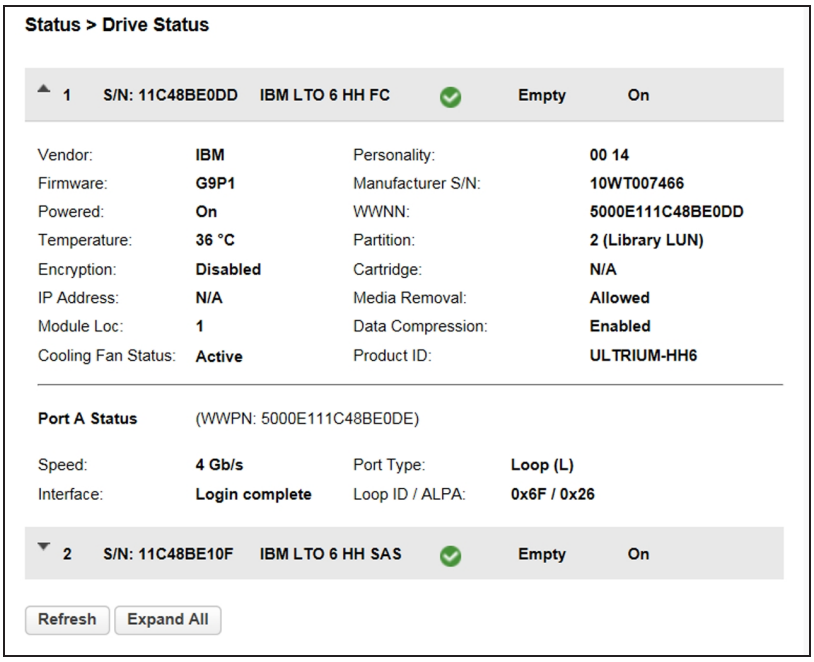


Figure 108 The Drive Status screen.

In the Drive Status screen you can see:

Field	Description
#	The drive number. Drives are numbered logically from the bottom of the library up to the top beginning with "1".
S/N	The serial number assigned to the tape drive by the library. This serial number is reported to host applications. The serial number cannot be modified. **Note:** This is not the serial number assigned to the drive by the manufacturer; the serial number assigned by the manufacturer is shown in Manufacturer S/N.

Field	Description
Drive Type	The drive type in the form *Vendor* LTO *gen ff int* where. • *Vendor* is the manufacturer • *gen* is the generation • *ff* is the form factor (**HH**: half-height or **FH**: full-height) • *int* is the interface (**FC**: Fibre Channel or **SAS**: Serial Attached SCSI)
Drive Health Icon	• **OK** - The green check mark icon indicates the drive is fully operational. • **Warning** - The yellow exclamation point icon indicates that user attention is necessary, but the drive can continue most operations. • **Error** - The red X icon indicates that the drive experienced an error that prevents it from continuing normal operations, and user intervention is required. Click the Library Health icon in the top banner for more information about current warnings and errors.
Drive Activity Status	The activity status of the drive. • **Write**—The drive is writing data. • **Read**—The drive is reading data. • **Idle**—A cartridge is present in the drive, but the drive is not performing any operations. • **Empty**—The drive is empty. • **Encryp**—The drive is writing encrypted data.
Power Status	Indicates whether the drive is currently powered on or off.
Vendor	The manufacturer of the drive.
Firmware	The currently installed drive firmware version.
Powered	Indicates whether the drive is currently powered on or off.

Field	Description
Temperature	The temperature measured by the tape drive in degrees Celsius.
Encryption	Whether encryption is enabled or disabled.
IP Address	The IP address for the drive. If the drive is does not have an Ethernet connection, a status of "N/A" displays.
Module Loc	The module in which the tape drive is located.
Cooling Fan Status	Whether the tape drive cooling fan is currently active.
Personality	The SCSI Standard Inquiry Data Page which identify the drive vendor.
Manufacturer S/N	The serial number assigned to the drive when it was manufactured. Use this serial number when working with your service provider.
WWNN	The world wide node name assigned to the drive.
Partition	The partition number to which the drive is assigned. If the drive provides the active control path for the partition, "(Library LUN)" displays also.
Cartridge	The barcode of the cartridge in the drive, if applicable.
Media Removal	Indicates whether media removal is allowed or prevented by the host.
Data Compression	Whether data compression is enabled or disabled.
Product ID	ULTRIUM-*ff-gen*. where *ff* is the form factor (**HH**: half-height or **FH**: full-height) and *gen* is the generation.

Field	Description

Port Status - Fibre Channel Drive	• The drive port configuration.
	• **WWPN**-The world wide port name for the port.
	• **Speed** -The currently selected Fibre Port speed. The default is Automatic.
	• **Port Type**
	  • Automatic
	  • Fabric
	  • Loop- Enables selection of the Addressing Mode.
	• **Interface**
	• **Loop ID/ALPA** - When Addressing Mode is set to Hard, the ALPA address displays.

Port Status - SAS Drive	• The drive port configuration. • **WWPN**-The world wide port name for the port. • **Interface** - The connected interface type • **Speed** -The currently configured SAS port speed.

VIEWING NETWORK STATUS

To see the network status, navigate to **Status > Network**.

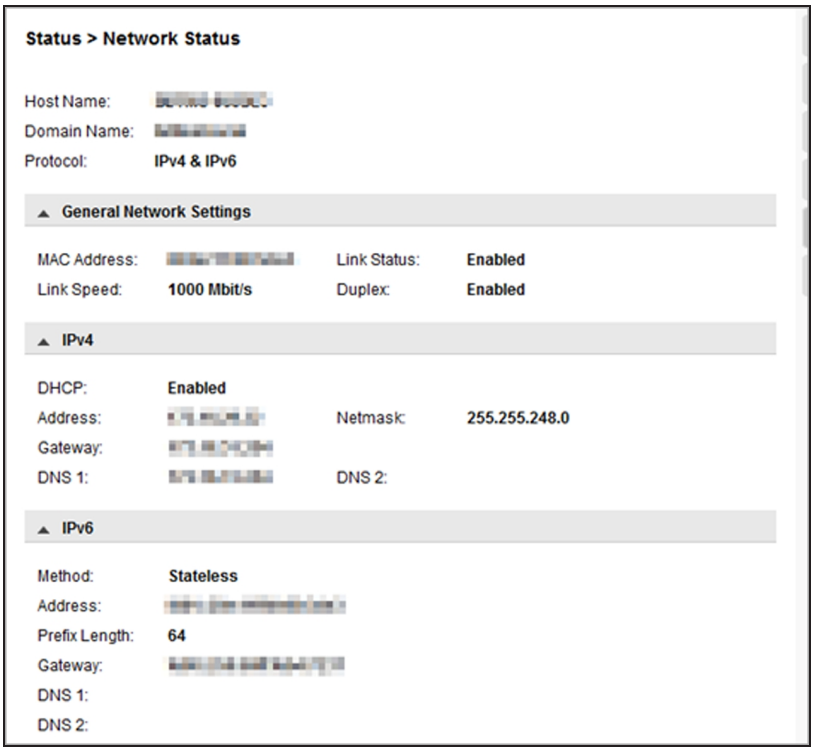


Figure 109 The Network Status screen.

In the Network Status screen you can see:

Field	Description
Host Name	Library hostname.
Domain Name	The domain name for your network where the library resides.
Protocol	Whether the library network uses IPv4, IPv6, or both addressing methods.
MAC Address	A unique identifier for the library controller network port.
Link Status	Enabled or disabled.

Field	Description
Link Speed	Speed of the Ethernet connection to the library.
Duplex	Enabled or disabled.
IPv4 Settings	
DHCP	When Enabled, the library requests an IP address from a DHCP server each time the library is powered on.
Address	The IP address in use by the library. If DHCP is enabled, this address was obtained from the DHCP server. If DHCP is disabled, the address was manually configured.
Netmask	The network mask of the library controller used when DHCP is disabled.
Gateway	The gateway used when DHCP is disabled.
DNS 1	The first domain name server to access.
DNS 2	The second domain name server to access.
IPv6 Settings	
Stateless Addressing	When enabled, the library generates an address for itself based on the routing information obtained from a router advertisement and the MAC address. The library can manage up to five global addresses at the same time, which can be assigned from different routers.
Static Addressing	When enabled, the library uses a statically-configured address.

VIEWING ENCRYPTION STATUS

Navigate to the **Status > Security** screen to see the status of any key management servers configured for use with the library, as well as the encryption status of the tape drives and partitions.

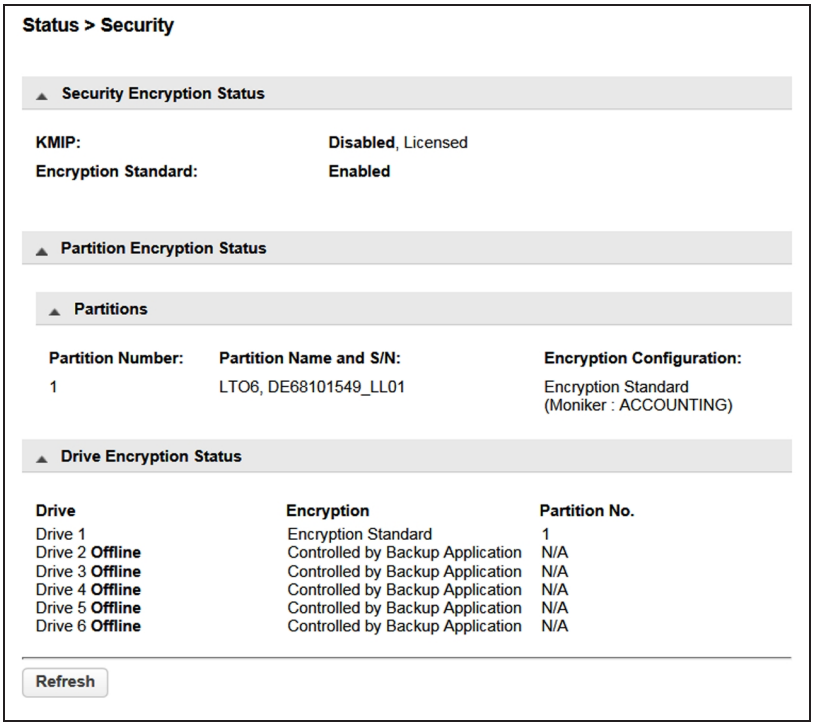


Figure 110 The **Status > Security** screen.

The Security Encryption Status pane shows what types of encryption are available in the library, and whether each type is enabled or disabled.

The Partition Encryption Status pane shows what type of encryption is used by each partition and configured Monikers or KMIP servers as applicable. Click **Connectivity Check** (not shown) to initiate a KMIP server connectivity check.

The Drive Encryption Status pane shows whether a drive is configured to encrypt data using an Encryption Standard key or a key from the KMIP key server configured for the drive's partition.

Chapter 6 - Configuring and Using Media Lifecycle Management

This chapter describes how to use BlueVision Media Lifecycle Management to proactively monitor and report on the health of the cartridges in your library.

BLUEVISION MEDIA LIFECYCLE MANAGEMENT

This section describes the major features of BlueVision Media Lifecycle Management (MLM). The remainder of the chapter provides detailed information about using MLM.

Overview

BlueVision 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 data cartridges and 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.

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 report as s a comma-separated-value (CSV) file to a USB device, email the report, or download to a host computer.

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 MLM-enabled cartridge is discovered 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 185 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 10,000 records. When this limit 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.

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 185). When a cartridge is retired or permanently exported from the library, its record can be deleted from the MLM database.

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 Save an MLM Report on page 190).

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 accumulated. 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.

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.

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.

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

If a cleaning cartridges is 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 does not attempt to use the expired cartridge for subsequent cleanings.

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.

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 tape records from the MLM database when the tape is retired or permanently exported from the library. You can also download the MLM database as a comma-separated-value (CSV) file and open the file in any software application that supports this type of file (for example, spreadsheet software).

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 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.

MLM Usage Guidelines

Consider the following guidelines when establishing your Media Lifecycle Management policies:

Chose a Retirement Guideline

When implementing MLM, decide at the beginning on the criteria to be used when determining when to retire a cartridge.

Regularly Backup 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.

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.

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

Use the instructions below to generate an MLM report.

1. Log into the library.
2. From the toolbar menu, select **Status > MLM**. The MLM Reports screen displays.
3. Select either **Total Library** or a specific partition from the **Partition** drop-down list. The screen refreshes to show the selected information.
4. Select the type of report you want from the **Report** drop-down list.

Notes:
- Information about MLM-enabled cleaning cartridges only appears in the Exported Media, Media Health, and Born on Date reports.
- To view the number of cleans remaining for a cleaning tape, you must save a MLM report as described in Save an MLM Report on page 190 and look for the Cleans Remaining column in the .csv file..

This report...	Displays...
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, the overall health (media health), and the load count (the number of times the cartridge was loaded into a drive) for each non-MLM-enabled cartridges in the selected location. • Use the **Filter** drop-down menu to display media by health rating.

This report...	Displays...
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. • This report does not include 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 does not include non-MLM-enabled cartridges.
Write Errors	The number of soft errors and the load count for each MLM-enabled data cartridge. **Note:** This report does not include non-MLM-enabled cartridges.
Cleans Remaining	The number of cleanings remaining and the born on date for each MLM enabled cleaning cartridge. **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 does not include non-MLM-enabled cartridges.
Exported Media	A list of all the MLM-enabled cartridges (both data and cleaning) that were exported from the library. The report displays the export time and 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 does not include non-MLM-enabled cartridges.

The MLM Reports screen refreshes to display the selected report with a list of the barcode labels for all media in the selected location.

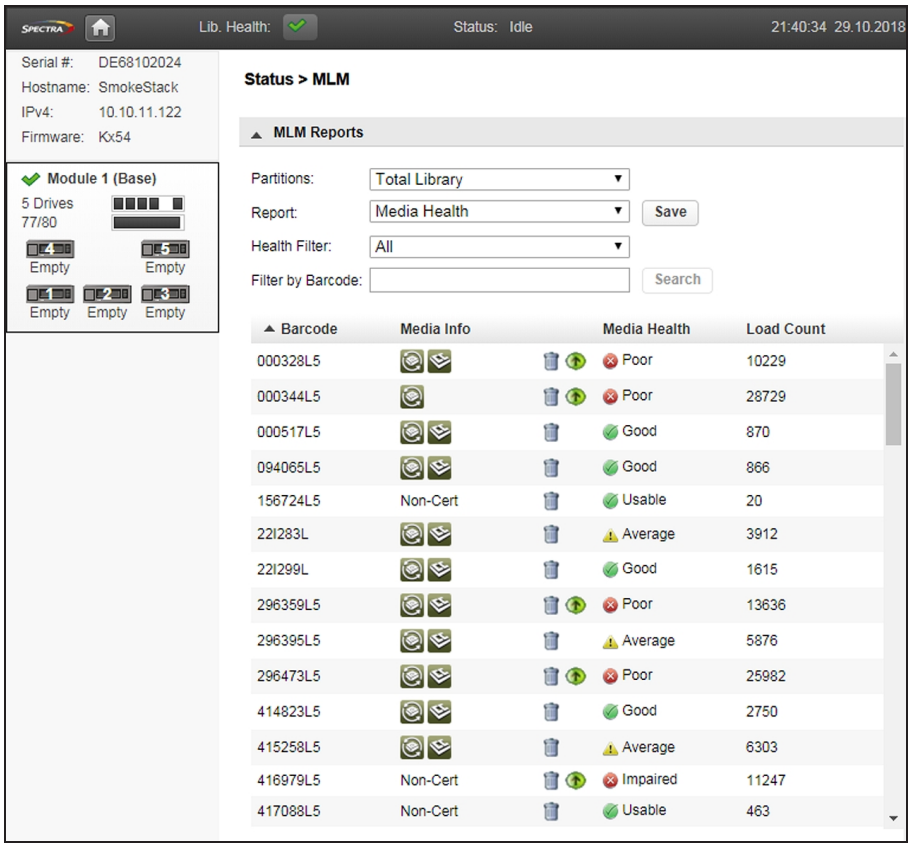


Figure 111 Use the health icons on the MLM Reports screen to quickly assess media health.

The following table describes the meaning of each media health icon. Click a row in the MLM report to view detailed information about that specific piece of media.

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 new data and reading previously written data. • **Cleaning cartridge:** More than 10 cleaning cycles remain on the cartridge.

Icon	Health score	Meaning
	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 were 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 10). • **Cleaning cartridge:** The cleaning cartridge is expired. No more cleaning cycles remain. Replace the cleaning cartridge.

Icon	Health score	Meaning
		The media health is **Unknown.** The status of the media cannot be determined.

5. If you want to view detailed information about a specific cartridge, use one of the following methods to locate the cartridge.

To find a cartridge using the...	Follow these steps...
Cartridge list	Scroll through the list of cartridges on the MLM Reports screen to locate the desired cartridge.
Barcode label information	1. Enter the barcode label information for the cartridge you want to locate in the **Find by Barcode** field. 2. Click **Search**. The list of cartridges refreshes to show the requested cartridge.

6. Click a row in the MLM report to view detailed information about that specific piece of media. The Details screen for the selected cartridge displays.

Note: Media health 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.

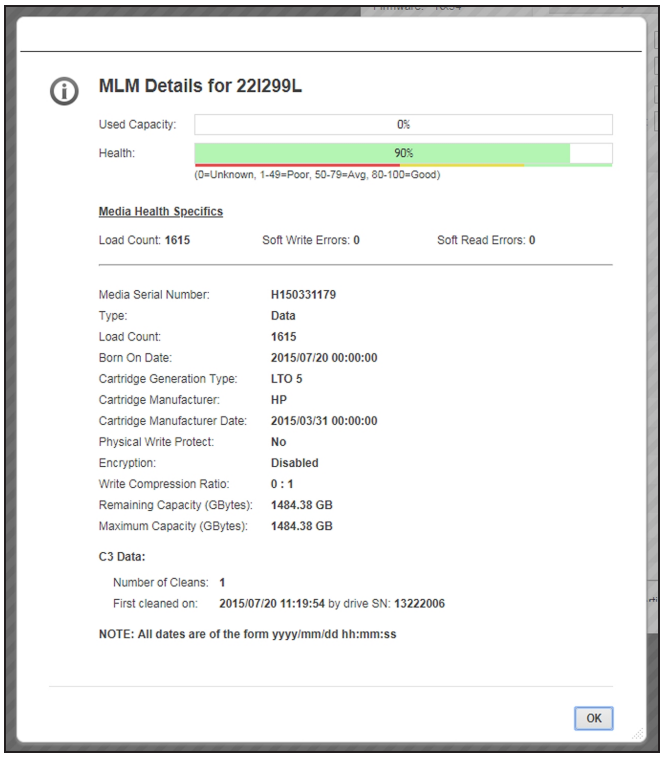


Figure 112 The detailed MLM report for the selected media.

When using CarbideClean™ media, the Details screen includes additional information related to the CarbideClean process. This information is not present for MLM media that was not put through the CarbideClean process.

7. Click **OK** to return to the main MLM Reports screen (Figure 111 on page 187).

Save an MLM Report

You can choose to save a copy of the MLM report, which is a comma-separated text file (*.csv), to a USB device, email the report, or save the report to your host computer.

1. If you want to save a specific report, generate the desired report as described in Generate MLM Reports on page 185. Otherwise, continue with Step 2 to save all MLM data.
2. If you want to save the MLM report to a USB device, connect the device to a USB port on the LCM or operator panel and allow time for the device to mount before continuing.

3. Click **Save** to display the Save MLM Report screen.

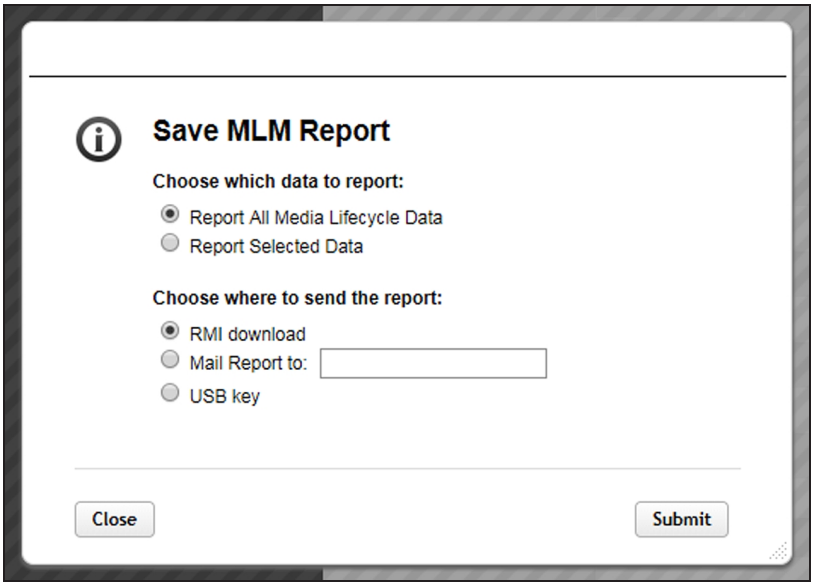


Figure 113 Select the desired options on the Save MLM Report screen.

4. Select the data to include in the saved report.

This option...	Saves...
Report All Media Lifecycle Data	A report containing all of the available detailed MLM data for MLM-enabled media in 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 111 on page 187). **Note:** The headings in the saved report reflect the fields displayed in the report you selected in the MLM Reports screen.

5. Select how you want the report saved

Selection	Destination
RMI download	Download the report to your host computer.
Mail Report to	Enter an email address to which the report is sent.
USB key	Save the report to the USB device.

6. Click **Submit** to send the report to the selected destination. Click **Close** 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 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 until the cartridge health returns to either Good or Average.

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 Media Health report as described in Generate MLM Reports on page 185.
2. Locate the barcode of the cartridge for which you need to reset the health (see Step Chapter 6 on page 179).
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.

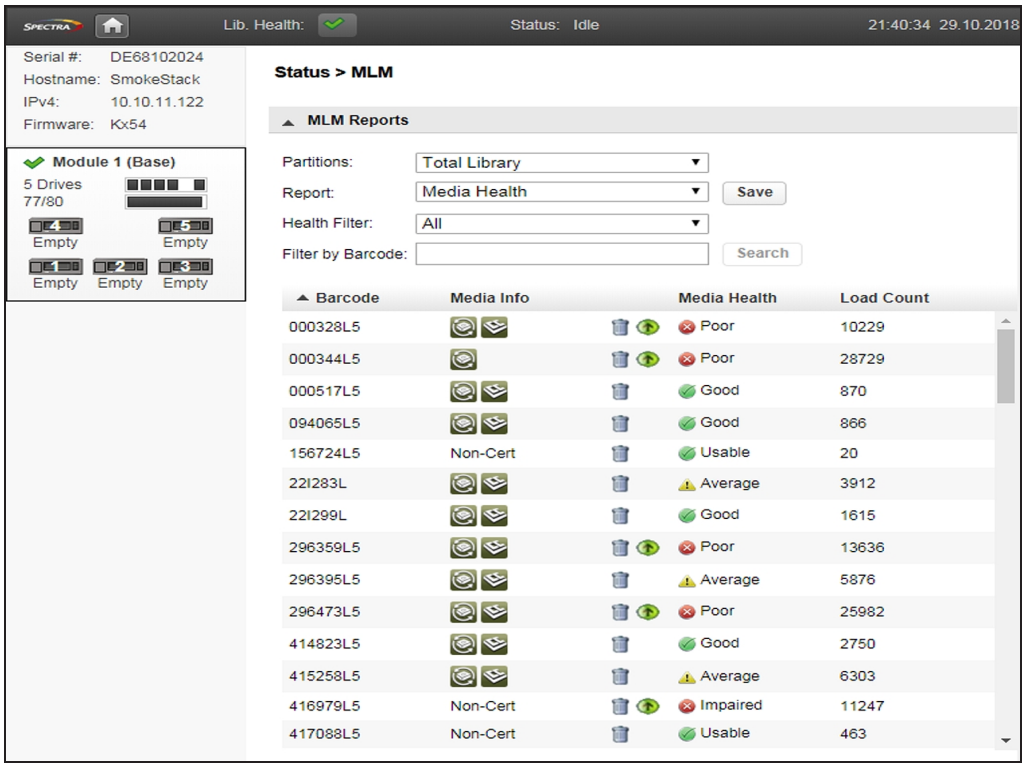


Figure 114 Click the green override button to reset the reported health for an MLM-enabled LTO cartridge.

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 history, health, and the verification data for all of the MLM-enabled cartridges in your library.

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.

Backup the MLM Database

Based on your environment, determine how frequently backups are needed, then use the following steps to create a backup. You must use the RMI to backup the MLM database.

1. Use your storage management software to stop all backup or restore operations on the library.
2. Log into the library as a user with administrator privileges.
3. From the toolbar menu, select **Configuration > System > Save/Restore Configuration**.
4. Click **Save MLM Database** to expand the section.
5. Click **Save** The Save MLM Database dialog box displays.
6. Click **Download**. The database backup file saves to your local computer.

Verify the Database Backup File

After backing up the MLM database, use the instructions below to confirm that the backup file was generated correctly.

1. Open the ZIP archive file downloaded in Backup the MLM Database.
2. Confirm the .ENC file is greater than 0 kilobytes.
3. Confirm the SQLTE file is greater than 0 kilobytes.

Restore the MLM Backup File

If you need to reset your library to factory defaults, it is helpful to restore the MLM database so you do not have to manually rediscover MLM cartridge information. You must use the RMI to restore an MLM database.

Use the instructions below to restore a previously saved MLM database to your Stack library.

1. Log into the library as a user with administrator privileges.
2. From the toolbar menu, select **Configuration > System > Save/Restore Configuration**.
3. Click **Restore MLM Database** to expand the section.
4. Click **Choose File** and browse to the location where the MLM database backup file is stored.
5. Click **Upload File & Restore**. The library restores the MLM database.

Delete MLM Records From the Database

If desired, you can delete the MLM record of a tape at any time. This is useful when a tape is retired or permanently exported from the library. If you delete the record of a tape that remains in the library, the MLM record is re-populated the next time the tape is loaded into a drive.

Note: MLM records for a tape can only be deleted after the tape is exported from the library.

1. Log into the library as a user with administrator privileges.
2. Display a Media Lifecycle Report as described in Generate MLM Reports on page 185.
3. Locate the barcode of the cartridge you want to remove from the MLM database (see Step Chapter 6 on page 179).

4. Click the trash can icon next to the barcode to delete the record.

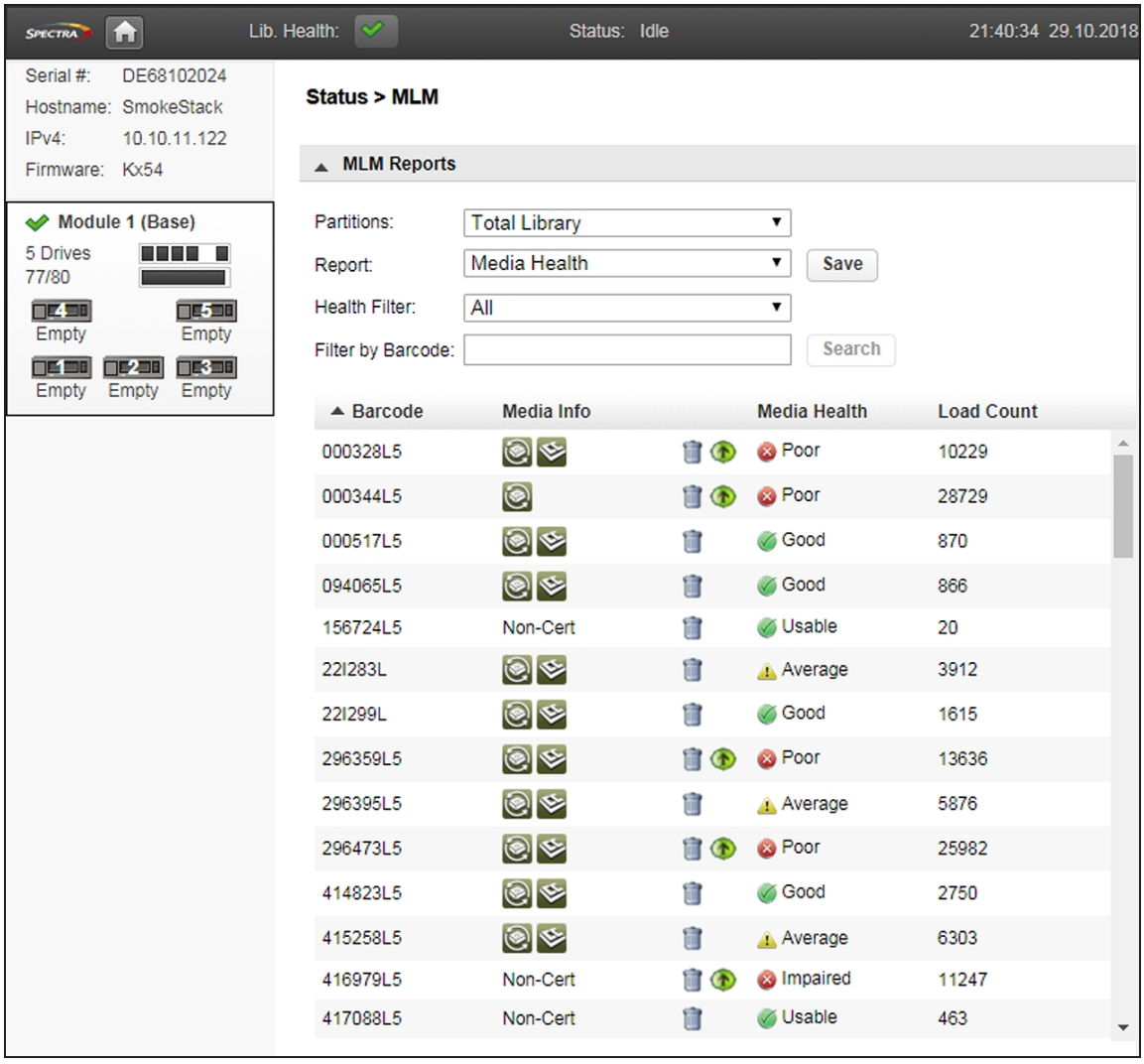


Figure 115 Use the trash can icon to delete individual records from the MLM database.

5. Respond to the confirmation message to delete the record.

CHAPTER 7 - MAINTAINING THE LIBRARY

This chapter contains instructions for maintaining the library. From the Home screen click **Maintenance** to access the library maintenance features.

LIBRARY TESTS

System Test

The system test exercises overall library functionality by moving cartridges within the library.

- During each cycle, the library moves a cartridge from a full slot to an empty slot and then returns it to its original slot. You can select the number of cycles for the test. If the test is canceled, the library returns the cartridge to its original slot.
- The library does not move cleaning cartridges during the test.
- The test operates over the whole library and does not take into account partition configuration.
- During the test the library is offline.

To run the system test, navigate to the **Maintenance > Library Tests > System Test** screen, select the number of cycles, and then click **Start Test**.

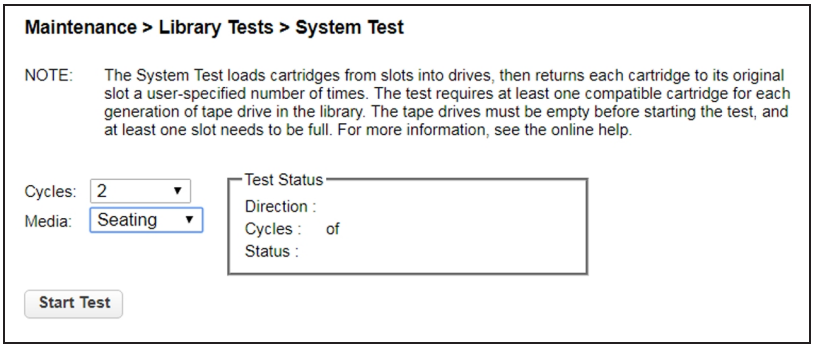


Figure 116 The System Test screen.

Slot to Slot Test

The slot to slot test randomly exchanges cartridges between slots to verify that the library is operating correctly. At the end of the test, the cartridges are not returned to their original slots. If a tape is moved to an incompatible drive, the drive rejects the tape, as designed.

CAUTION The test can move cartridges between partitions.

For service and diagnostics, use the Robotics Test on page 204.

To run the slot to slot test, navigate to the **Maintenance > Library Tests > Slot to Slot Test** screen, select the number of cycles, and click **Start Test**.

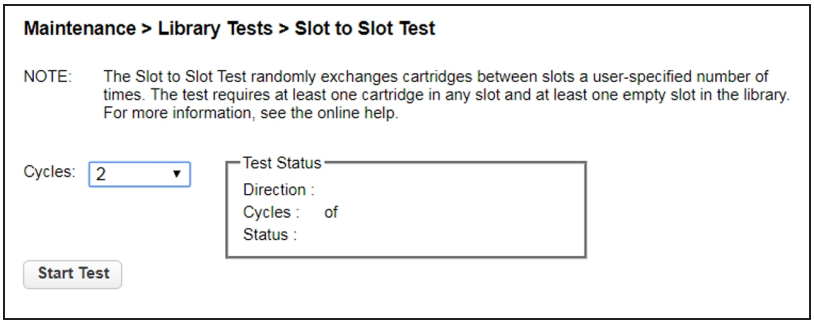


Figure 117 The Slot to Slot Test screen.

Element to Element Test

The element to element test moves a selected cartridge to a selected slot or tape drive, and then returns it to the original slot. If the selected destination is a tape drive, the tape is loaded and unloaded before it is returned. You can select the number of times to move the selected cartridge to the destination location and back.

The element to element test is intended to show that the library is operating correctly. To diagnose problems with the robotic assembly or verify that it has been correctly replaced, use the Robotics Test on page 204.

To run the element test:

1. Navigate to the **Maintenance > Library Tests > Element to Element Test** screen.

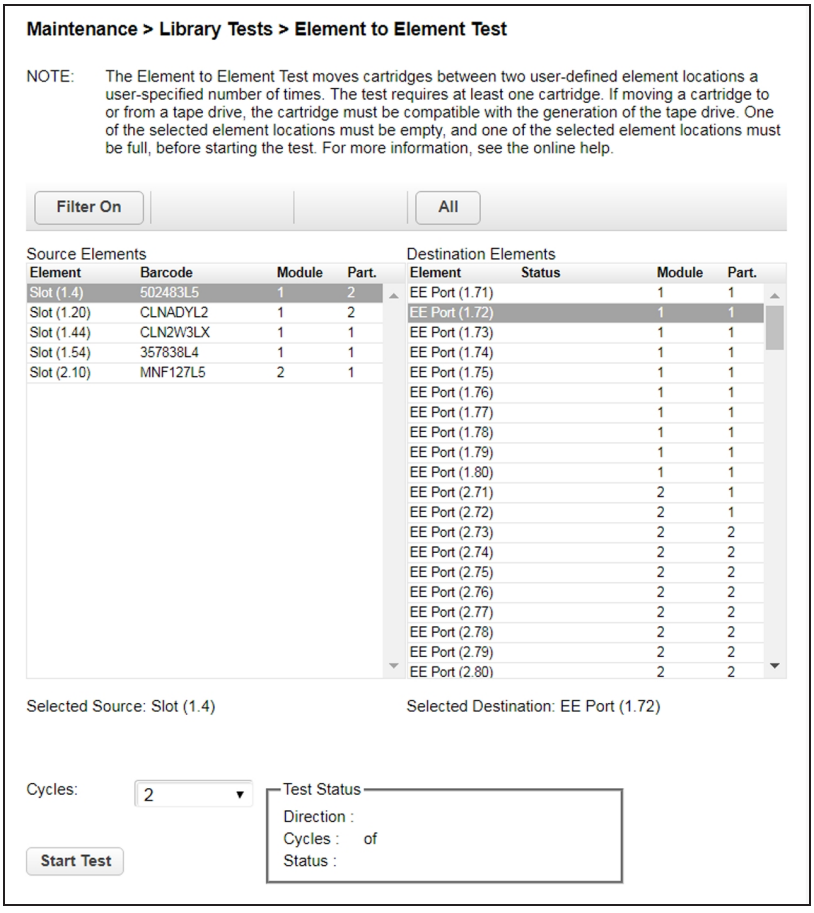


Figure 118 The Slot to Slot Test screen.

2. Select a cartridge from the Source Elements list.

   To view a subset of the cartridges by barcode:

   a. Click **Filter On**.

   b. Enter characters into the search box and then click **Search**.

   The Source Elements list is updated to only include cartridges with barcode labels including the search characters.

3. Select a location from the Destination Elements list.
4. Using the drop-down menu, select the number of **Cycles**.
5. Click **Start Test**.

Position Test

The Position Test moves the robotic assembly vertically between two selected elements. The test does not move cartridges.

1. To run the position test, navigate to the **Maintenance > Library Tests > Position Test** screen.

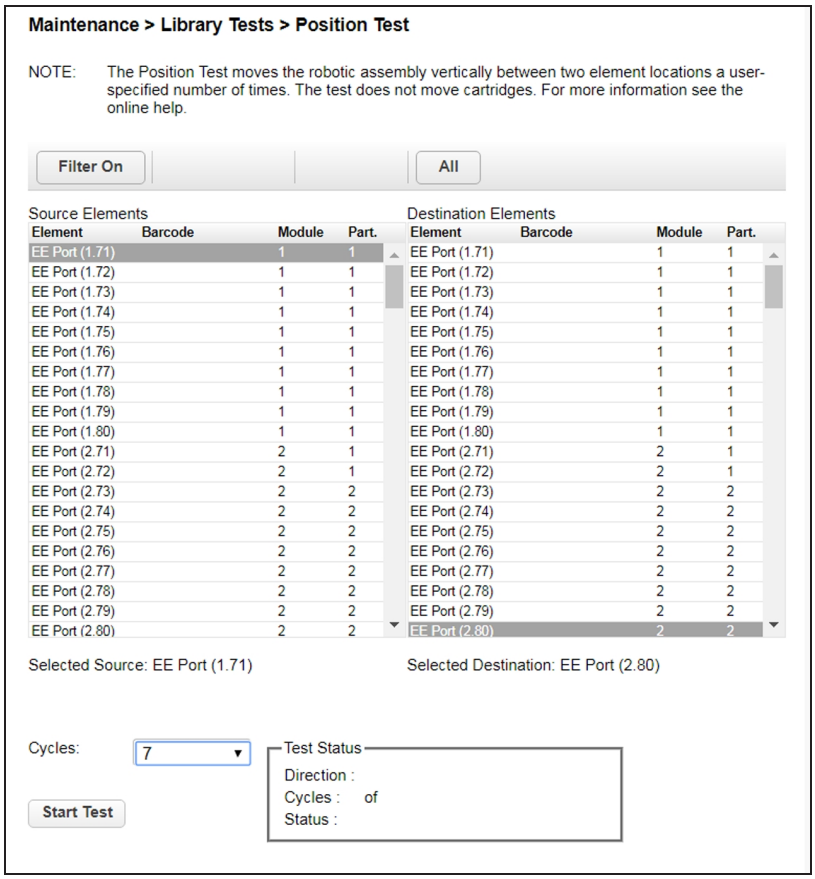


Figure 119 The Position Test screen.

2. Select one element from the Source Element list and another from the Destination Element list.
3. Using the drop-down menu, select the number of **Cycles**, and click **Start Test**.

Wellness Test

The wellness test performs a general health check on the library functionality by running the following tests:

- Basic Hardware Review
- Robotics Initialization Test
- Barcode Scanning Test
- Magazine/EE Port Unlock Motor Test
- Move Media Test

Keep the following in mind when running the Wellness test:

- Running the test requires at least one drive and one tape cartridge in the library.
- After the test has started, the **Stop Test** button is active. Clicking **Stop Test** aborts the wellness test, but not before the current test has completed.
- The test operates over the entire library and does not take into account partition configuration.
- During the test the library is offline.
- The Info column notifies the user of the status and result of each test.

To run the system test, navigate to the **Maintenance > Library Tests > Wellness Test** screen, and then click **Start Test**.

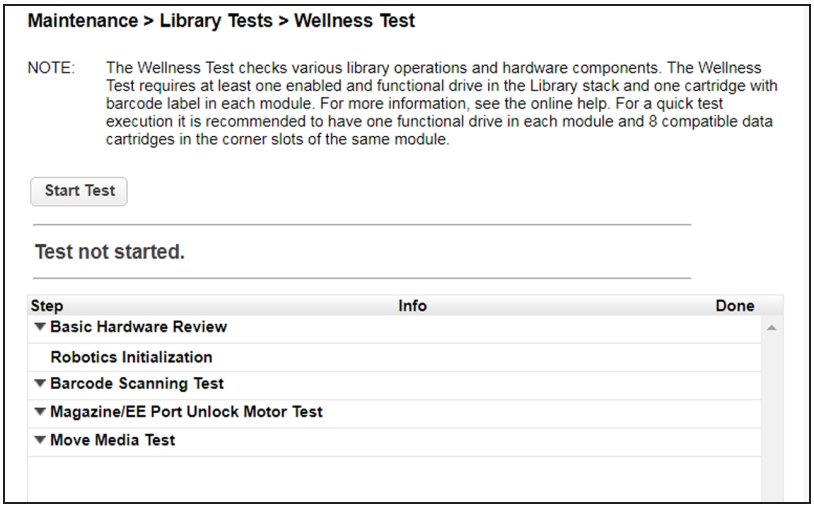


Figure 120 The Wellness Test screen.

Robotics Test

The robotics test performs a full inventory and exercises all robotic assembly movements and sensors.

To run the robotics test, navigate to the **Maintenance > Library Tests > Robotic Test** screen, then click **Start Test**.

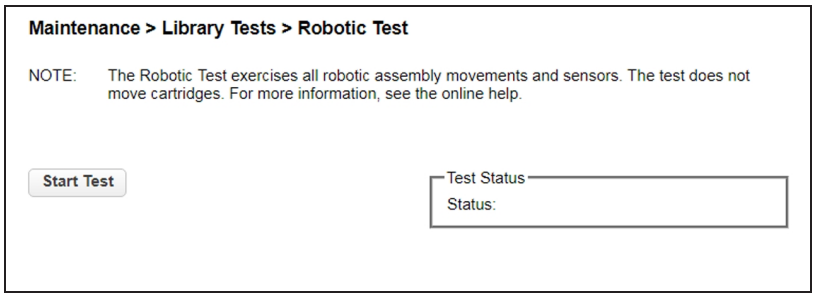


Figure 121 The Robotic Test screen.

OCP Test and Calibration

1. To test or calibrate the OCP, navigate to the **Maintenance > Library Tests > OCP Test** screen.

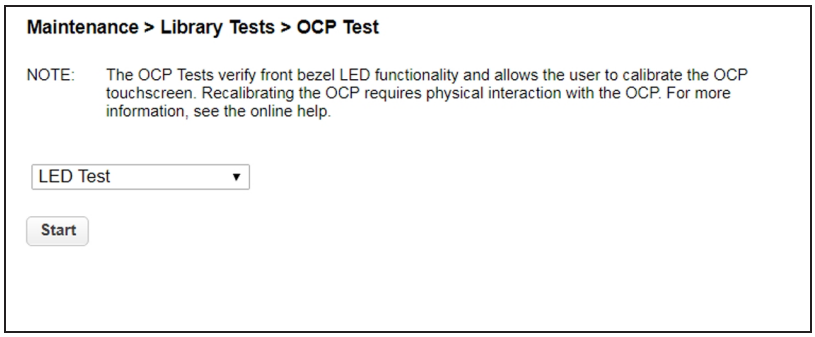


Figure 122 The OCP Test screen.

2. Select the desired test:
   - LED test - illuminates each of the front panel LEDs
   - Touch panel calibration test - allows you to calibrate the LCD touch screen
   - OCP reboot - reboots the LCD touch screen
3. Click **Start**.
4. Follow the instructions on the screen.

LOGS AND TRACES

Viewing Log Files

To view the library log files, navigate to the **Maintenance > Logs and Traces > View Logs** screen and then select one of the logs. The available logs are:

- Event Ticket Log - Records library error and warning events
- Information Log - Records library information warnings
- Configuration Log - Records configuration changes

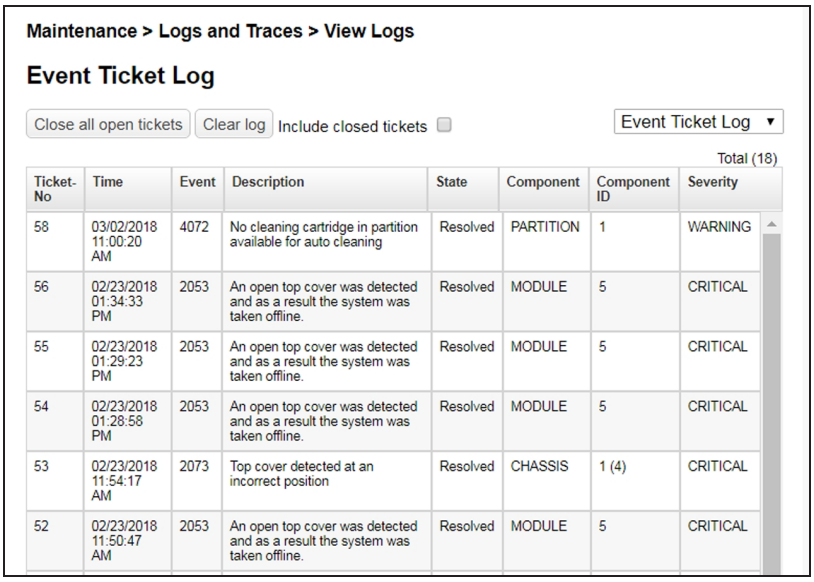


Figure 123 The View Logs screen.

The log entries are displayed in order of most recent to oldest. The log entries contain a date and time code, event code, severity, component identifier, and event details. The format for the date and time is: *YY.MM.DD HH.MM.SS.ss*.

- *YY.MM.DD* - The date displayed as Year.Month.Day
- *HH.MM.SS.ss* - The time displayed as Hour.Minute.Second.Hundredths of a second

Downloading Log and Trace Files

To download the library log and trace files from the RMI, navigate to the **Maintenance > Logs and Traces > Download Logs and Traces** screen and click **Save**.

Figure 124 The Download Logs and Traces screen.

Configuring Remote Logging

If desired, you can configure remote logging to send system messages to a remote logging server.

1. From the home screen of the library interface, select **Configuration**. The Configuration screen displays.
2. Select **Network Management**, then select **Remote Logging (rsyslog)**. The Remote Logging (rsyslog) screen displays.

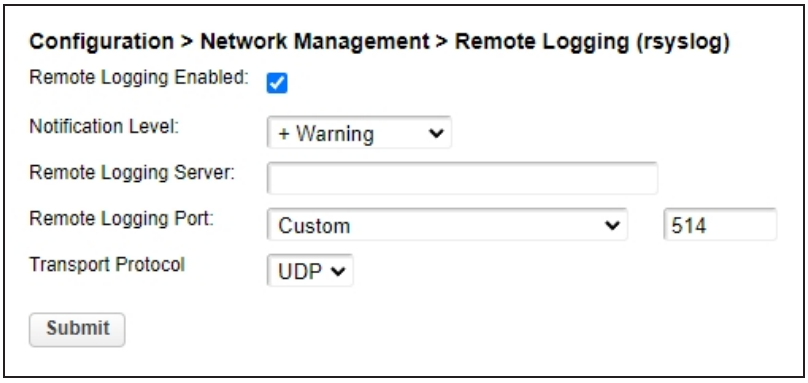


Figure 125 The Remote Logging (rsyslog).

3. Select or clear **Remote Logging Enabled**.

4. Using the **Notification Level** drop-down menu, select the notification level you want to receive.

Selection	Description
Inactive	No events are sent to the syslog server.
Critical	All critical events are sent to the syslog server.
+ Warning	Critical and warning events are sent to the syslog server.
+ Configuration	Critical, warning, and configuration events are sent to the syslog server.
+ Information	All events are sent to the syslog server.

5. Enter an IP address for the **Remote Logging Server**.
6. Using the **Remote Logging Port** drop-down menu, select to use the **Default** port, or to set a **Custom** port. The default port is 514.
7. If you selected Custom in Step 6, enter the port number.
8. Using the **Transport Protocol** drop-down menu, select either **UDP** or **TCP** as the transport protocol.
9. Click **Submit**.

SOFTWARE UPGRADES

Managing System Firmware

Check the Library Firmware Version

The firmware version currently installed on the library is displayed in the library status area on the Home page.

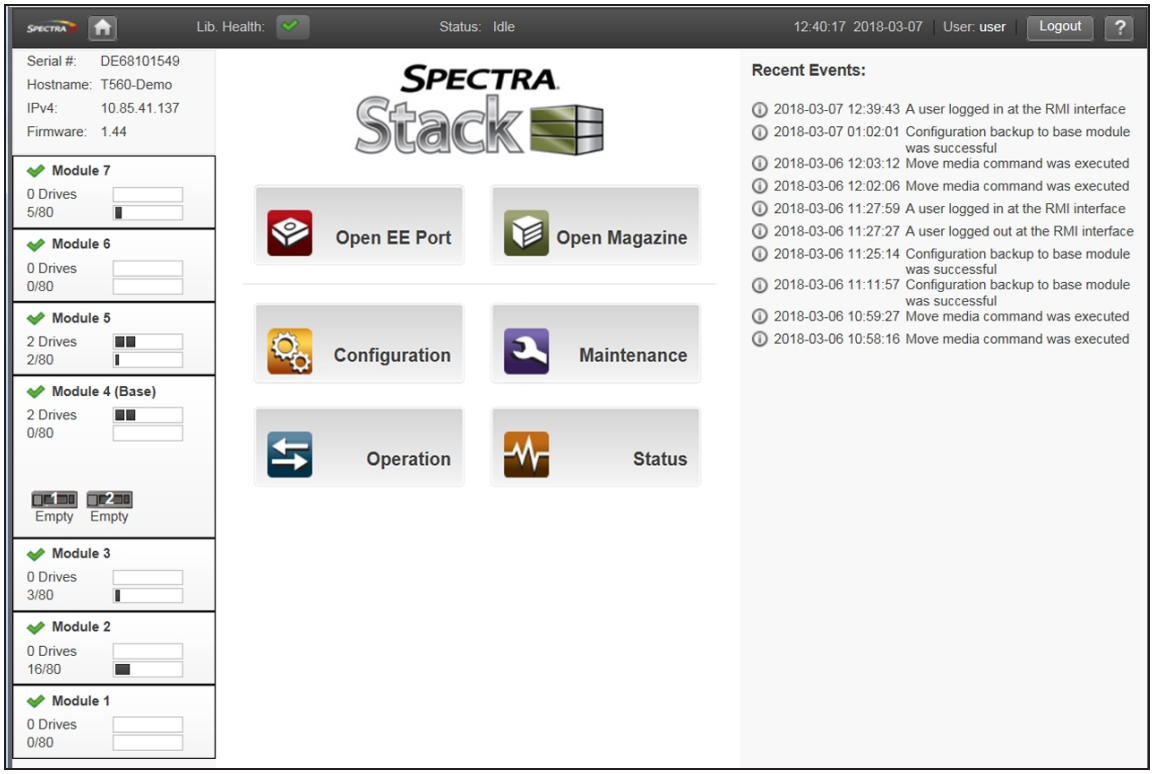


Figure 126 Spectra Stack Main screen.

Check and Download the Currently Released BlueVision Version

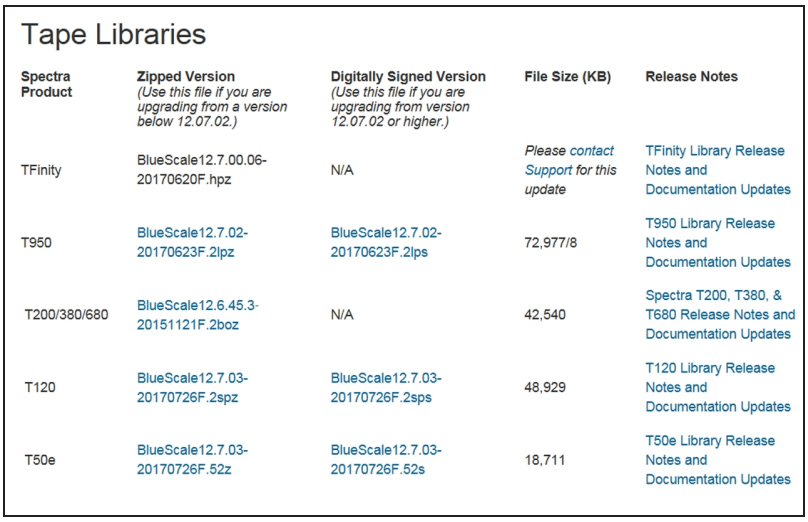
Follow these steps to check the currently recommended BlueVision version:

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

   Note: See Accessing the Technical Support Portal on page 264 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 BlueVision 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	BlueScale12.7.00.06-20170620F.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 127 The Product Software screen (T950 library firmware shown).

4. Compare the Current Version available for the library to the version installed on the library.
5. If there is a new version of the library firmware, click the name of the BlueVision package. The package begins downloading through your web browser.

Upload Library Firmware

You upload the library firmware from the **Maintenance > Software Upgrades > System Firmware** screen.

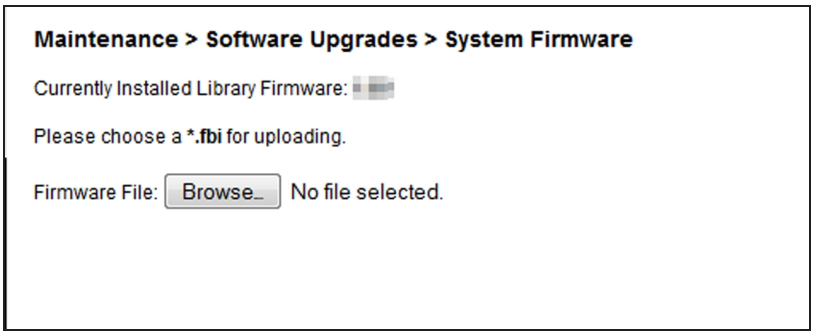


Figure 128 The System Firmware screen.

To update library firmware from the RMI:

1. Use your web browser to select the firmware file from the local computer.
2. Click **Start Upgrade**. The update process starts immediately and cannot be canceled.

To update the library firmware from the OCP:

1. Copy the firmware file to a USB device.
2. Insert the USB device into the USB port on the front of the library.

   The library detects the USB device.
3. Select the firmware file.
4. Click **Start Upgrade**. The update process starts immediately and cannot be canceled.

When you update the library firmware, the library updates the firmware of the expansion modules to a compatible version.

Managing Drive Firmware

Drive firmware can be updated on multiple drives of the same type at the same time. Drive firmware can only be updated from the RMI. Each drive will only accept appropriate firmware.

Check the Drive Firmware Version

To see the firmware version currently installed on the drives, navigate to the **Status > Drive Status** screen.

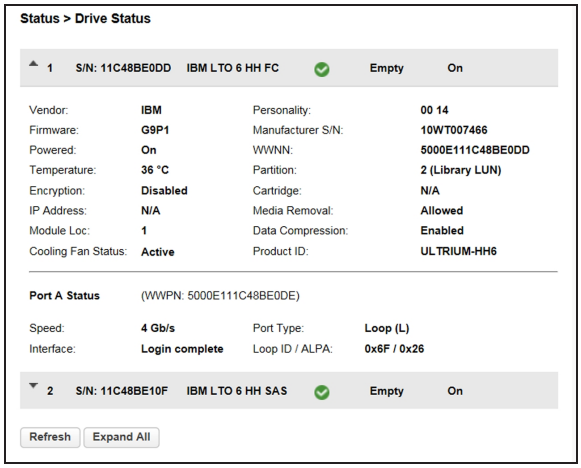


Figure 129 The Drive Status screen.

Check and Download the Currently Released Drive Firmware

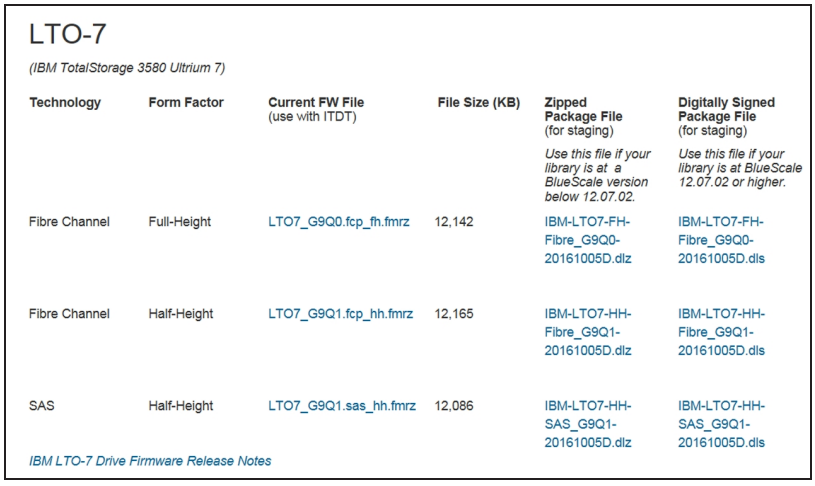
Download the recommended drive firmware from the Spectra Logic Technical Support portal, and save it to your local computer.

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

   Note: See Accessing the Technical Support Portal on page 264 for information about creating an account and accessing the Technical Support portal.

2. Select **Downloads > Drive Firmware**.

3. On the Tape Drive Firmware page, locate the appropriate drive firmware with respect to drive type (LTO), generation (for example, LTO-6), interface type (for example, SAS or Fibre), and form factor (full-height or half-height).



LTO-7

(IBM TotalStorage 3580 Ultrium 7)

Technology	Form Factor	Current FW File (use with ITDT)	File Size (KB)	Zipped Package File (for staging) *Use this file if your library is at a BlueScale version below 12.07.02.*	Digitally Signed Package File (for staging) *Use this file if your library is at BlueScale 12.07.02 or higher.*
Fibre Channel	Full-Height	LTO7_G9Q0.fcp_fh.fmrz	12,142	IBM-LTO7-FH-Fibre_G9Q0-20161005D.dlz	IBM-LTO7-FH-Fibre_G9Q0-20161005D.dls
Fibre Channel	Half-Height	LTO7_G9Q1.fcp_hh.fmrz	12,165	IBM-LTO7-HH-Fibre_G9Q1-20161005D.dlz	IBM-LTO7-HH-Fibre_G9Q1-20161005D.dls
SAS	Half-Height	LTO7_G9Q1.sas_hh.fmrz	12,086	IBM-LTO7-HH-SAS_G9Q1-20161005D.dlz	IBM-LTO7-HH-SAS_G9Q1-20161005D.dls

IBM LTO-7 Drive Firmware Release Notes

Figure 130 A portion of the Tape Drive Firmware page.

4. Click the firmware version name in the column labeled **Current FW File**.

   Note: While the column header references that the file is for "use with ITDT", the file is also compatible with your Spectra Stack library.

5. Use your web browser's download features to save the file.

Update Drive Firmware

1. Navigate to the **Maintenance > Software Upgrades > Drive Firmware** screen. The tape drives are organized by drive type.

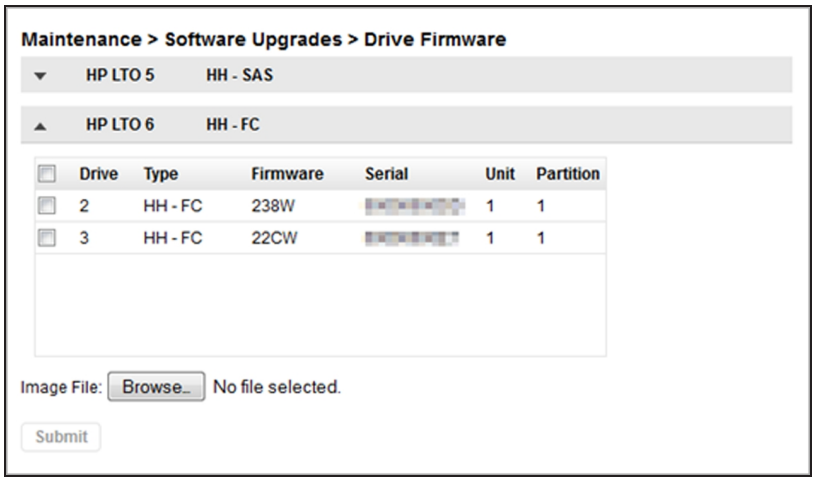


Figure 131 The Drive Firmware screen.

2. Expand the appropriate drive type and select one or more tape drives.
3. Click **Browse** and use your web browser to select the firmware file.
4. Click **Submit**.

Downloading Drive Logs

To download a drive log from the RMI:

1. Navigate to the **Maintenance > Download Drive Logs** screen.

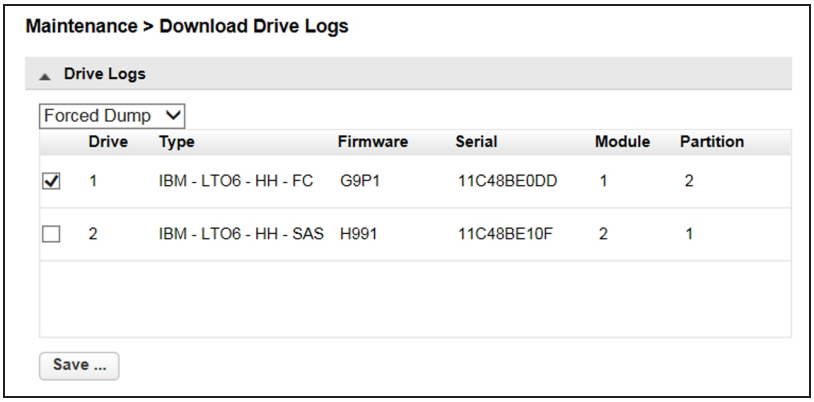


Figure 132 The Download Drive Logs screen.

2. Select the drive(s) from which you want to collect logs.
3. Select the type of log to collect (Regular Dump or Forced Dump).
4. Click **Save**.

Rebooting the Library

From the **Maintenance > System Reboot** screen, click **Reboot**.

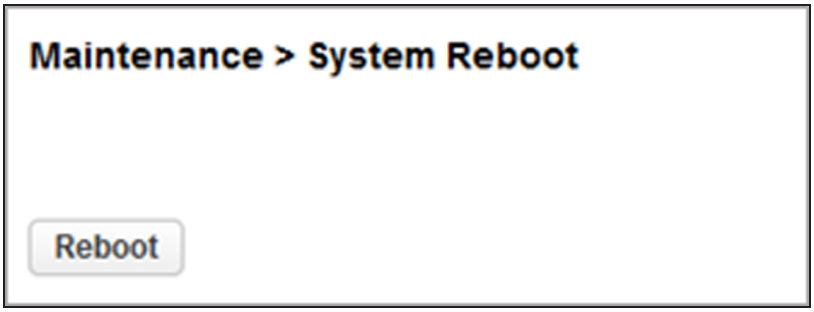


Figure 133 The System Reboot screen.

REBOOTING DRIVES

1. From the **Maintenance > Drive Reboot** screen, select the drive(s) you want to reboot and click **Submit**.

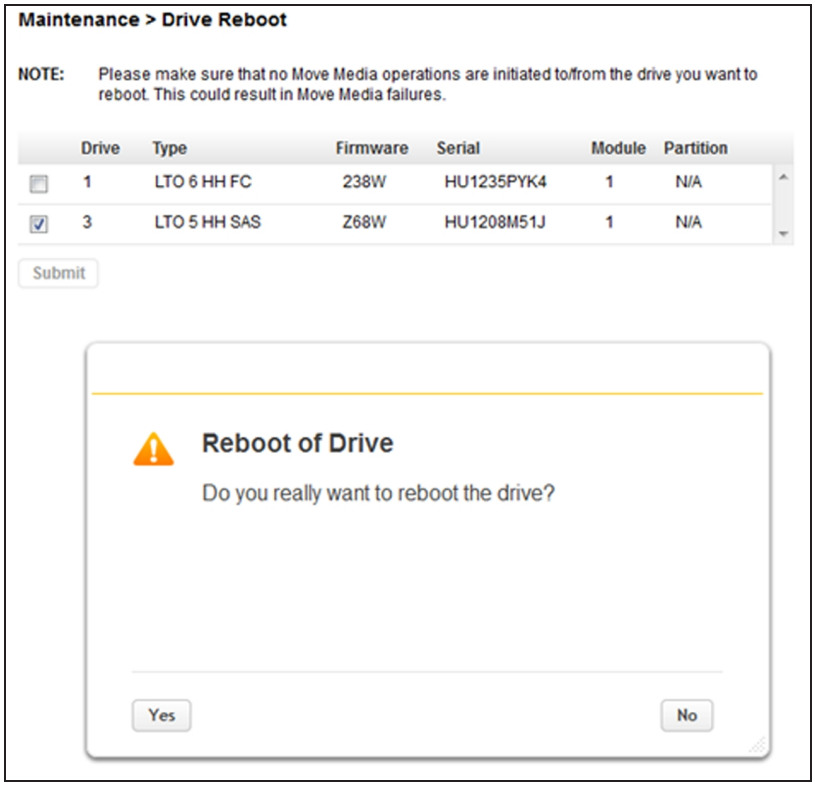


Figure 134 The Drive Reboot screen.

2. Click **Yes** on the dialog popup to start the reboot process.

CONTROLLING THE UID LED

The UID LEDs are a pair of blue LEDs - one on the OCP and the other on the controller module controller. The UID LEDs are useful for identifying the library in a data center. The UID LEDs are operated synchronously and controlled by the user. You can see if the LEDs are lit, and toggle the status from the **Maintenance > UID LED Control** screen.

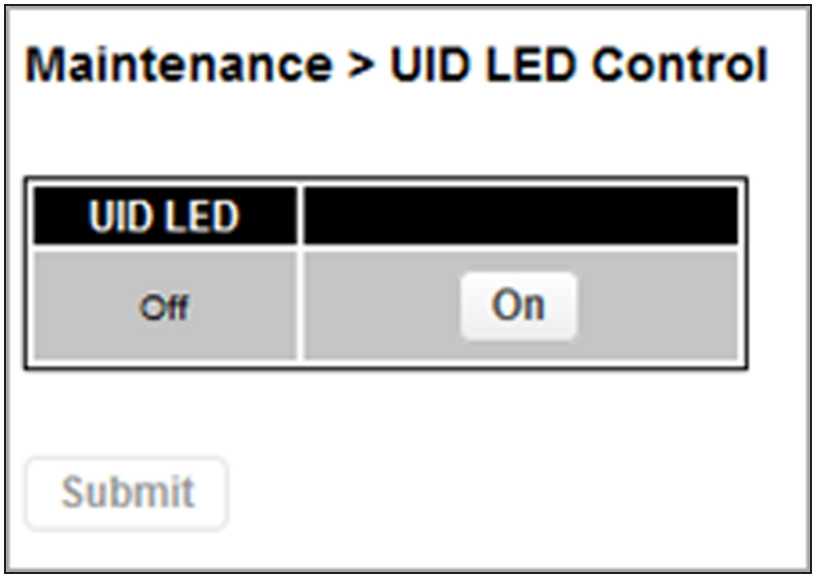


Figure 135 The Maintenance > UID LED Control screen.

MOVING THE ROBOTIC ASSEMBLY TO THE CONTROLLER MODULE

Before extending a module from the rack, the robotic assembly must return to its park position in the controller module. Under normal circumstances, when the library is powered off using the front power button, the robot automatically parks and locks into the controller module behind the OCP. After powering off the library and before proceeding with extending a module from the rack, look inside the controller module window to verify that the robotic assembly is behind the OCP.

Use the following instruction if the library did not move the robotic assembly to its park position:

1. Power on the library.
2. Log into the library as an Administrator user.
3. Navigate to the **Maintenance > Move Robotic to Base Library** screen.

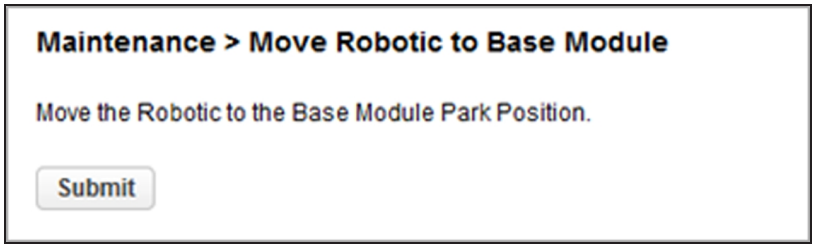


Figure 136 The Move Robotic to Base Module screen.

4. Click **Submit**.

   If the robot still did not park and locks into the controller module, contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10.

LTO-9 New Media Initialization

The LTO-9 cartridge initialization includes a media calibration process that increases the initialization time to up to two hours per cartridge. To assist with this, you can use this wizard to start a bulk initialization of LTO-9 cartridges in the tape library.

IMPORTANT	After the LTO-9 New Media Initialization starts, it is possible to abort the process; however, any media that has been loaded into a drive MUST complete its initialization before the wizard aborts and the processing of remaining media stops. Shutting down the initialization process can take up to two hours.
IMPORTANT	All Spectra Certified LTO-9 media is initialized before it ships and does not need to go through this process.

Use the instructions below to initialize LTO-9 media using the LTO-9 New Media Initialization Wizard.

1. Navigate to the **Maintenance > LTO-9 New Media Initialization Wizard** screen. The LTO-9 New Media Initialization Wizard screen displays.

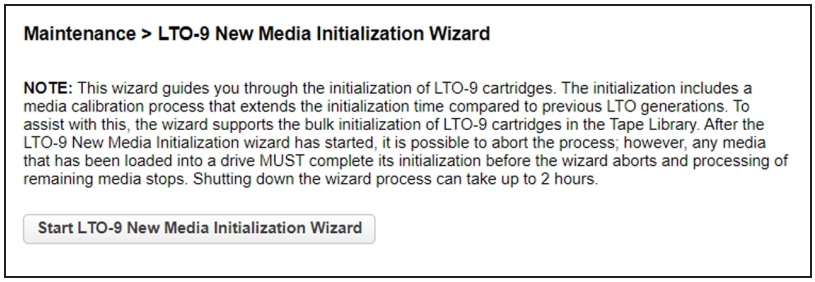


Figure 137 The LTO-9 New Media Initialization Wizard screen.

2. Click **Start LTO-9 New Media Initialization Wizard.** The Information screen displays.

Figure 138 The Information screen.

3. Read the note for the wizard and click **Next**. The Select Cartridges screen displays.

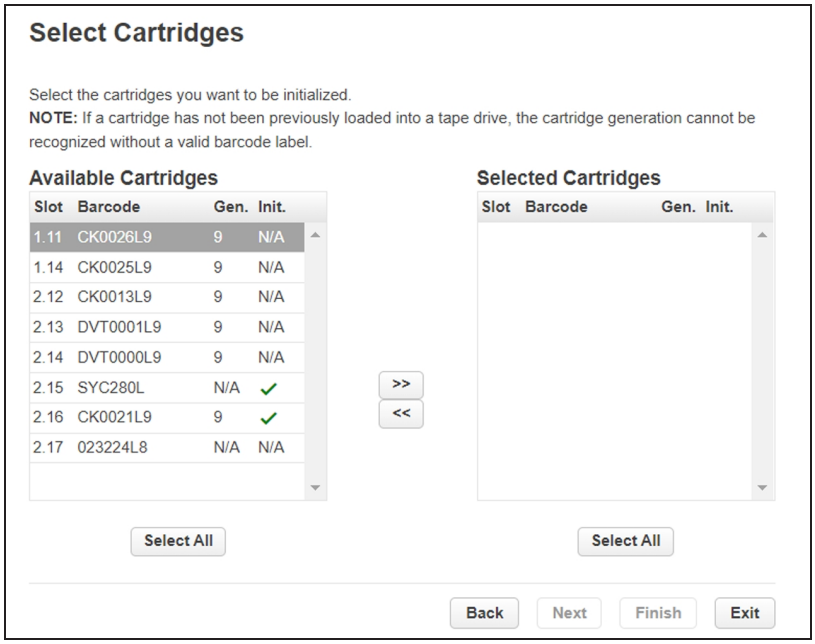


Figure 139 The Select Cartridges screen.

4. Select the LTO-9 cartridges that you want to initialize and click >> to move them to the Selected Cartridges column. When all of the cartridges that you want initialized are in the Selected Cartridges column, click **Next**. The Select Drives screen displays.

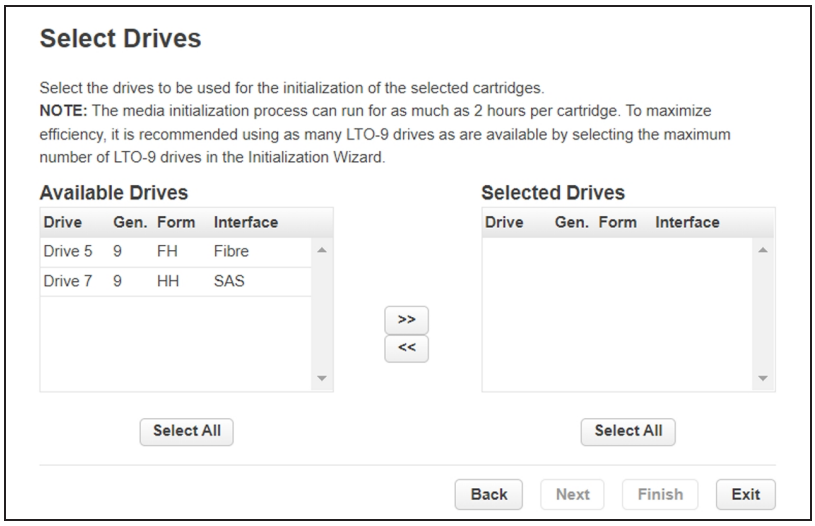


Figure 140 The Select Drives screen.

5. Select the LTO-9 drives that you want to use to initialize the cartridges and click >> to move them to the Selected Drives column. To maximize efficiency, select as many LTO-9 drives as possible. When all of the drives that you want to use to initialize cartridges are in the Selected Drives column, click **Next**. The Finish screen displays.

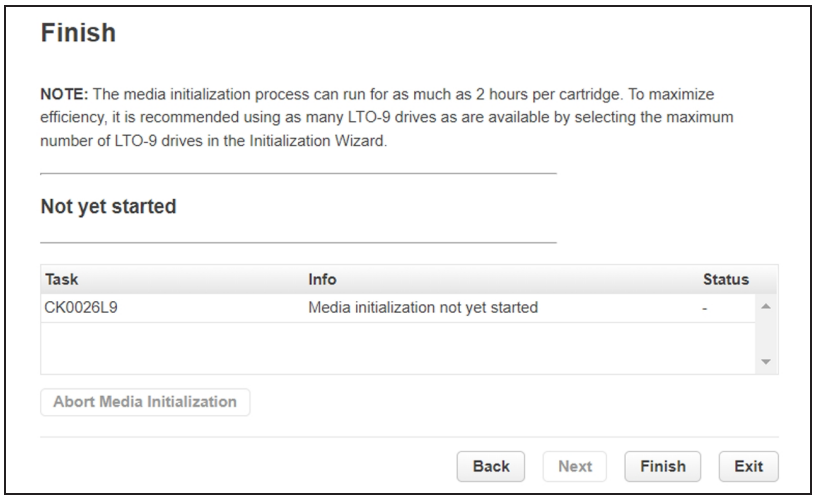


Figure 141 The Finish screen.

6. Click **Finish**. The initialization process begins.

7. If necessary, click **Abort Media Initialization** to stop initializing cartridges before all cartridges are initialized; however, any media that has been loaded into a drive MUST complete its initialization before the initialization aborts and the processing of remaining media stops. Shutting down the wizard process can take up to two hours.

CHAPTER 8 - LIBRARY TROUBLESHOOTING

CAUTION This library is designed to operate when installed in a rack using the rack rail kit. Operating the library without installing it in the rails, such as on a table or rack shelf, may result in library errors. Placing any weight on top of the library might also cause errors.

FIBRE CHANNEL CONNECTION PROBLEMS

Use the **Status> Drive Status** screen to check the link connection for your tape drive.

If the screen shows Logged Out:

- Check that the Fibre speed is set to **Automatic** or that the correct Fibre speed is selected. If you are unsure of the speed of the HBA or switch that the drive is connected to, select **Automatic**.
- Check that the correct port type, fabric or loop, is selected. Loop requires additional configuration. If you are unsure of the correct port type, select **Automatic**.

If the screen shows No Link, the Speed Status displays the '-' character, and the Link LED on the back of the drive is off:

- The speed is probably set incorrectly. Try setting the speed to **Automatic**.
- If there are still issues, change the port type to **Auto Detect**.

If the screen shows No Light:

- The cable is not plugged in correctly. Check that it is connected correctly to Port A of the tape drive.
- The cable is damaged. FC cables are delicate. If the cable has been bent or twisted sharply, it might be broken and must be replaced.

If the screen shows ALPA Conflict:

- There might be a conflict with the ALPA address on Loop ports. Select Soft for the Loop mode to allow the system to select an available address each time the tape drive connects to the FC fabric. If your server configuration does not support changing addresses, try using the Hard Auto-Select option for the Loop mode. This allows the system to select an available address when it first connects, and then retain that address for future connections.

Detection Problems after Installing a SAS Drive

Problems encountered after installation are often caused by improper SAS cable connections, storage management software configuration errors, or operating system configuration errors. If the storage management software or operating system does not communicate with the library after installation, determine the extent of the detection problem:

- Does the storage management software detect the tape drive?
- Does the storage management software detect the library?
- Does the operating system detect the tape drive?
- Does the operating system detect the library?
- Does the operating system detect the library, but list it as a generic device?

Based on the extent of the detection problem, check the following:

- If neither the storage management software nor operating system detects the tape drive, or they do not detect both the tape drive and the library:
  - Verify that all SAS cables are securely connected at both ends.
  - Check the length and integrity of your SAS cabling. For reliable operation, do not use a SAS cable longer than six meters. Do not use a cable adapter or converters between the HBA and the library.
  - Check the SAS connectors for damage or debris.
  - Verify that your HBA is supported by the host computer and qualified with the library.
  - Verify that your HBA has the latest firmware.
- If the storage management software or operating system detects the tape drive, but not the library:
  - Verify that multiple LUN support is enabled on the HBA. The library uses two Logical Unit Numbers (LUNs) to control the tape drive (LUN 0) and robotic assembly (LUN 1). The library requires an HBA with multiple LUN support and multiple LUN support must be enabled on the host computer. When multiple LUN support is disabled, the host computer can see the tape drive, but not the library.

  Note: Many RAID or array controllers do not provide multiple LUN support.

- If the storage management software or operating system does not detect any devices on the HBA:
  - Verify that the SAS host adapter is installed correctly. Refer to the manual that came with your host adapter for installation and troubleshooting instructions.
  - Verify that the proper device driver is installed for the SAS host adapter.
- If the library is detected by the operating system, but not by the storage management software:
  - Refer to the documentation included with your storage management application for instructions on how to verify proper installation. Some backup software packages require an additional driver to communicate with the robotics.
- If the library is detected by the operating system, but is listed as an unknown or generic device:
  - Make sure that the proper device driver, if applicable, is installed for the library. Check your storage management software provider's website for the latest drivers and patches.

If you continue to have problems with a SAS library, check the following:

- Ensure that the library is compatible with the SAS host adapter and storage management software you plan to use.
- Verify that your HBA is supported by the host computer and qualified with the library.
- Ensure you are using a compatible, high-quality cable.

OPERATION PROBLEMS

Power Problems

Problem	Solution
Library does not power on	1. Check all power cord connections. 2. Check the LEDs on the power supplies. 3. Make sure the power button on the front panel has been pressed, and the green Ready LED is lit. 4. Make sure the outlet has power. Try another working outlet. 5. Replace the power cord.
No message appears on the OCP display	1. Check all power cord connections. 2. Check the LEDs on the power supplies. 3. Make sure the power button on the front panel has been pressed, and the green Ready LED is lit. 4. Make sure the outlet has power. Try another working outlet.

Failure/Attention Indications Displayed on the Operator Control Panel

If the problem persists, contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10.

Problem	Solution
The OCP displays a warning or error icon	Click the icon to see more information about the event on the OCP.
The OCP displays an error code	Look up the error code, try to resolve the failure, and power cycle the library (see Event Codes on page 237).

Tape Movement Problems

Problem	Solution
Tape stuck in drive	Try the following steps, in this order, to remove the stuck tape. **Note:** The tape drive must rewind the tape before ejecting it. This can take as long as five minutes, depending on how much tape must be rewound. Once the tape is rewound, the eject cycle takes approximately 15 seconds. The Ready light flashes while the tape rewinds. Wait for the tape to finish rewinding before attempting another operation. 1. Attempt to unload the tape from your backup software. 2. Shut down the storage management software and stop the operating system's removable storage services. From the **Operation > Move Media** screen, attempt to unload or move the tape to a slot. 3. Power down the library and disconnect the cable from the drive. Power up the library, and wait until the tape drive is idle or ready. From the **Operation > Move Media** screen, attempt to unload or move the tape to a slot. 4. From the **Operation > Force Drive Media Eject** screen, attempt to force eject the tape . **IMPORTANT** Inspect the tape cartridge. Damage or misplaced labels on the cartridge may have caused the load/unload failure. Discard any tape cartridge found to have issues.
Tape cannot be removed from storage slot	1. Unlock the magazine from the **Operation > Open Magazine** screen and extend it to access the storage slot. 2. Grasp the cartridge and remove it from the storage slot. Some tapes need to be inserted and removed several times to condition them for free movement in and out of the magazine. 3. Check the barcode label and verity that it is secure to the cartridge. 4. Check the cartridge for damage. 5. Check the storage slot for damage.

Media Problems

Problem	Solution
Cleaning or data cartridge incompatible with drive	• Check the event log to see which cartridge is incompatible. • Make sure you are using data and cleaning cartridges that are compatible with the drive and that you are using the correct cartridge type for the operation. The drive automatically unloads incompatible cartridges, the Attention LED flashes. Export the media.
Cannot write to or read from tape	• Make sure that the cartridge is not a WORM cartridge that has already been used. • Make sure that the cartridge is write enabled (move the write-protect switch to the enabled position). • Make sure the data cartridge is compatible with the drive model. LTO-5 through LTO-7 tape drives can read data cartridges from two generations back and write to data cartridges one generation back. LTO-8 drives can read and write LTO-7 and LTO-8 tapes only. • Make sure that the cartridge has not been exposed to harsh environmental, magnetic, or electrical conditions and is not physically damaged in any way. • Many storage management applications do not read or write to cartridges that were created using a different application. In this case, you may have to perform an erase, format, or label operation on the cartridge. • Make sure you understand any data protection or overwrite protection schemes that your storage management application may be using, which could prevent you from writing to a given cartridge. • Retry the operation with a different, known good tape. • Clean the tape drive from the **Operation > Clean Drive** screen.

Attention LED is Lit

Problem	Solution
Both the Attention and Cleaning LEDs are lit	This is most likely caused by a dirty drive that cannot read a tape and marks the tape invalid. Log into the OCP or RMI and check the event log to see which drive has reported that it needs cleaning. Clean the drive with an approved Ultrium cleaning cartridge.
A particular cartridge sets off the cleaning light	Remove the cartridge from the library.
A cartridge recently imported from a different environment is causing issues	Media that is moved from one environment to another can cause issues until it has acclimated to the new conditions. A cartridge should be acclimated for at least 24 hours before use, particularly if it has been stored at a substantially different temperature or level of humidity than the library.
The Attention LED is lit but the Cleaning LED is not lit after a cartridge load	The library was unable to complete the requested operation with the selected tape cartridge. • Use only cartridges that are compatible with the drive type • Use the correct type of cartridges for the operation. For example, use a cleaning cartridge for cleaning. • Make sure you are using a Universal cleaning cartridge
The Cleaning LED is lit after using a cleaning cartridge	The cleaning cartridge has expired. A cleaning cartridge expires after 50 uses.
A particular cartridge sets off the Attention LED and possibly the Cleaning LED	Retry the operation with a different cleaning cartridge. If the Attention LED is cleared and the drive has been cleaned, and then immediately re-displays each time a particular cartridge is reloaded, that cartridge should be suspected as being defective. • If this occurs, export the cartridge and load a known good cartridge. • Any cartridge that is suspected of being defective or contaminated should NOT be reused in any drive. • If the bad cartridge is a cleaning cartridge, it might be expired.

Inventory Problems

Problem	Solution
The library displays incorrect barcodes	• Verify that the label is properly applied. • Verify that the label is not soiled.

RMI Network Connection Issues

Problem	Solution
Cannot connect to the RMI	• Verify that the Ethernet cable is connected to the controller module's controller board and to the LAN. • Verify that the link LED on the RJ45 (LAN) connector is lit when the library is powered on. If the LED is not lit, the library is not communicating with the LAN. See your network administrator for help. • Verify that the library has been configured with a valid static network address or DHCP has been enabled so the library can obtain a network address. If using DHCP, obtain the library's network address from the OCP login screen. If the library did not obtain a valid address via DHCP, verify that the DHCP server is up and the library has network access to it. If necessary, set a static network address instead. • Enter the library's IP address into the address bar of a web browser connected to the same LAN as the library. If the RMI web page does not display, ping the library's IP address. If the ping fails, verify that the library has a valid network address and that there are no firewalls or other obstructions to network traffic between the computer with the web browser and the library. See your network administrator for help.

Cleaning Problems

Problem	Solution
Cannot load the cleaning cartridge	• Make sure you are using an Ultrium cleaning cartridge. • Make sure the cleaning cartridge has not expired. A cleaning cartridge expires after 50 cleaning cycles. • Power cycle the library.

PERFORMANCE PROBLEMS

The storage management process involves many system components, from the files in the file system on the host computer, through the backup server, and out to the library, all managed by software running on an operating system. The storage management process only runs as fast as the slowest component in the system.

Performance issues are solved by identifying and addressing performance limitations in your system. See sections below for the following potential performance limitations:

- Average File Size below
- File Storage System on the next page
- Connection from the Backup/Archive Host Server to a Disk Array on the next page
- Backup/Archive Server on the next page
- Backup/Archive Software and Method on the next page
- Connection from the Backup/Archive Host Server to a Disk Array on the next page
- Media on page 233

Average File Size

The hard drive must seek to the position of a file before it can start reading. The more time the disk drive spends seeking to files, the lower the performance. Therefore, if the average file size is small, the read performance is lower.

To determine the average file size, divide the size of the backup by the number of files.

If the average file size is small (64 KB or less), consider using a sequential, image, or block backup method that backs up the whole hard drive or LUN image instead of individual files. The trade off for using one of these methods is that you might only be able to restore the entire image instead of individual files.

Note: File fragmentation also causes excessive drive seeking, which lowers performance, so ensure that files are regularly defragmented.

File Storage System

The file storage system determines the organization of the files on the disks. Using RAID controllers to spread files over multiple disks can improve performance because some disks can be seeking while others are reading. Storing files on a single non-RAID disk results in the slowest performance while storing files on a high-end disk array results in the fastest performance.

Converting standalone disks to RAID can improve performance.

Connection from the Backup/Archive Host Server to a Disk Array

The network connection between the host server and the disk array determines how much data can be transferred from the disks to the host computer at a time. A connection with insufficient bandwidth cannot provide enough data for the tape drives to write at full speed. For optimum performance, the storage subsystem must be able to provide data at the tape drive's maximum transfer rate. Backup systems using a lower speed Ethernet network should use multiple network connections.

Backup/Archive Server

The backup server must have enough RAM and processor power to transfer the files from the disk to the tape drive, in addition to running the backup or archive software, and any other processes.

Check the RAM and processor usage during a backup operation. If they are operating at capacity, adding RAM or processor capability can improve performance.

Backup/Archive Software and Method

Each backup method has its own impact on performance, depending on how well it can keep data streaming to a tape drive. In most cases, native applications don't have the features required to maximize performance for LTO tape drives. It is recommended to use a full-featured backup or archive application with this library.

File-by-file backup or archive methods provide the best restore performance if you only need to restore individual files. However, if the average file size is small, file-by-file methods significantly reduce performance.

Disk image, flash, or sequential backup methods provide the fastest performance because they back up an entire disk, partition, or LUN, which minimizes disk seeking. The disadvantage is that backup and restore operations work on an entire disk, partition, or LUN. You might not be able to back up a subset of files or restore a single file. If you can restore a single file, the restore process is slow.

Database backup performance varies based on the use model. To improve performance when backing up data from a database:

- Use specific backup agents for the database.
- Use the latest versions of the databases.
- Do not back up individual mailboxes.
- Do not back up specific records or do a record-by-record backup.
- Do not back up when the database is in heavy use.

Connection from the Archive/Backup Host Server to the Library

For the best performance, the connection from the host server to the library must have enough bandwidth to provide enough data to keep the tape drive streaming. Current LTO tape drives take advantage of some of the fastest interfaces available so the type of interface used to connect the library to the host server is not likely to be the cause of a performance issue. However, issues with cables and connectors can limit performance.

Note: Do not exceed recommended cable lengths.

Media

The type and condition of the media also affect backup performance. For best performance, use media that is the same LTO generation as the tape drives.

Finding Event Information

You can find error codes by viewing log files from the **Maintenance > Logs** and **Traces > View Logs** screen or downloading support tickets from the **Maintenance > Download Support Ticket** screen. See Viewing Log Files on page 205 or Downloading Drive Logs on page 213.

UNLOCKING THE MAGAZINE

It is recommended that you unlock the magazine using the OCP or RMI. If these methods fail, or if a magazine needs to be removed when the power to the library is off, you can release the magazine manually. Only one magazine or EE port can be open at a time.

Note: As a best practice, perform this procedure while applications are idle. While the magazine is extended, the library robotic assembly cannot move media.

Using the OCP or RMI

1. Log in as an administrator.
2. On the Home screen, click **Open Magazine**. The Open Magazine screen displays.

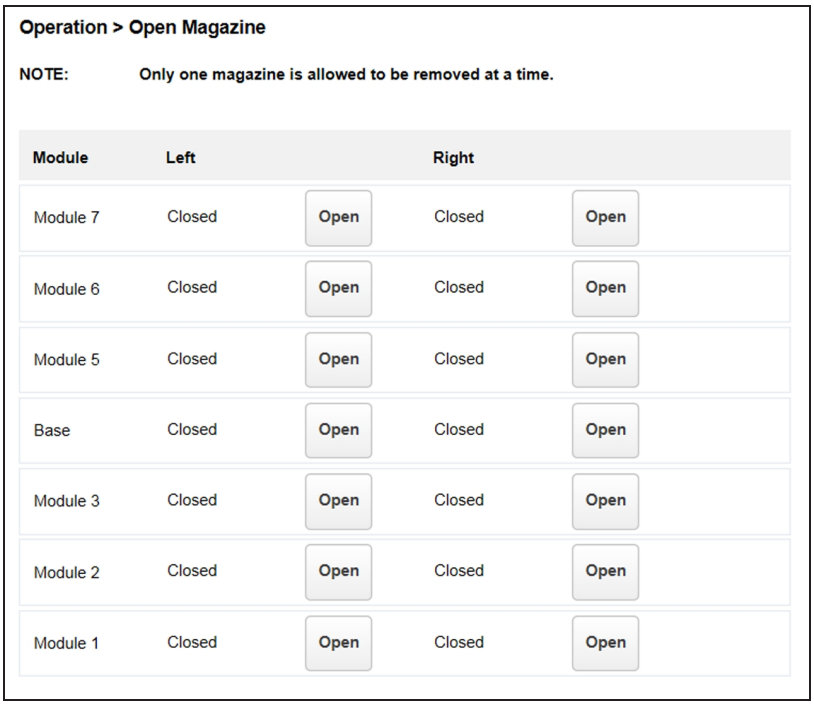


Figure 142 The Open Magazine screen.

3. Click **Open** in the left or right magazine column within the module containing the magazine you want to unlock.
4. Click **Submit**. A message box indicates when the magazine has been unlocked.

5. Click **OK** to close the message. The Open Magazine screen shows that the magazine is now unlocked. Close the magazine access door after reinserting a magazine.

Note: If not removed, the magazines and the EE port relocks after 30 seconds.

Using the Manual Release

1. Open the magazine access door.
2. Insert a small flat head screwdriver or Torx driver into the appropriate magazine release hole and gently push the tab in.

CAUTION Do not exert force once you encounter resistance. Doing so can damage the device.

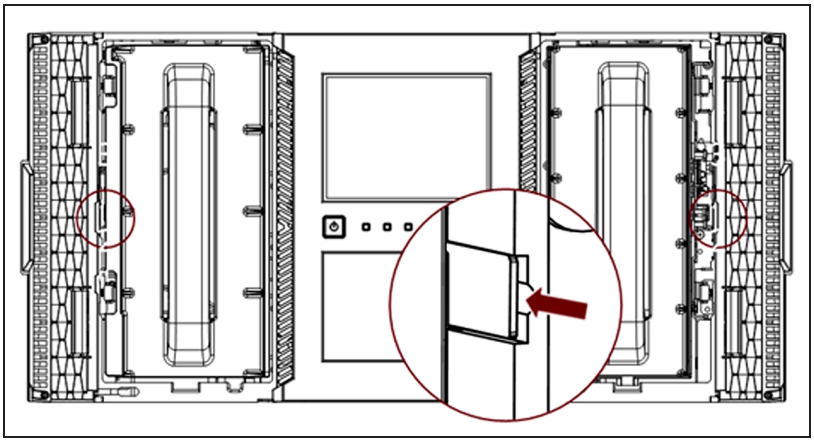


Figure 143 The magazine release.

3. Close the magazine access door after reinserting a magazine.

Unloading a Stuck Tape

If a tape is stuck in a tape drive, eject the tape from the drive from the **Operation > Force Drive Media Eject** screen.

If a tape is stuck in a magazine, open the magazine (see Unlocking the Magazine on the previous page), grasp the cartridge, and pull it out of the storage slot.

IDENTIFYING A FAILED COMPONENT

Using the OCP or RMI:

1. If necessary, activate the UID LEDs from the **Maintenance > UID LED Control** screen. This illuminates the blue LED on the front and rear of the controller module to identify the library containing the failed module or component.
2. Identify the module within the library that contains the failed component:
   a. In the upper left of the Home screen, locate the module that indicates an error.
   b. Click the module for information on the failed component.

Chapter 9 - Event Codes

This chapter provides descriptions and possible solutions for error event codes.

ERROR EVENTS

Event Code	Message Text and Description	Details and Solution
2000	Failed to move cartridge.	Verify the source and destination elements and retry the move operation.
2001	Failed to exchange the cartridge.	
2002	The initial module discovery (detection of expansion modules) failed.	Verify that all expansion modules are powered on and that the expansion interconnect cables are properly installed.
2003	The library's temperature has exceeded the critical limit.	1. Verify that the chassis fan in each module is functioning 2. Verify that the drive cover plates are installed in all open drive bays. 3. Verify that all power supplies are installed and working properly. 4. Verify that the ambient room temperature is within specified limits.
2004	Library startup failed.	1. If the robotic assembly fails to move through a certain area of the library: • Look through the window in the front panel and see if there are any obstructions. • Verify that both magazines in that module can be extended. 2. Verify that all modules have power and that any expansion modules are cabled correctly with the expansion interconnect cables.

Event Code	Message Text and Description	Details and Solution
		3. Verify that the top and bottom cover plates are properly installed on the library. 4. Verify that the module alignment mechanisms at the rear of the library are locked in the proper positions. 5. Reboot the library. 6. If the robotic assembly moves front to back, but not vertically, the robot shipping lock could be positioned incorrectly and should be moved to either the fully locked or fully unlocked position. If the robotic assembly **does not** unlock the shipping lock after reboot: 1. Move the robotic assembly to the base from the **Maintenance > Move Robotic to Base module** screen. See Moving the Robotic Assembly to the Controller Module on page 216. 2. Power off the library. 3. Remove all cables from the controller module and unlock the alignment mechanism. 4. Extend the controller module from the rack. 5. Reposition the lock. **Note:** If the error persists, review library events for additional information. See Viewing Log Files on page 205.

Event Code	Message Text and Description	Details and Solution
2005	Robotic spooling cable failure.	Ensure that the spooling cable is fully seated in the controller module and correctly connected to the robotic assembly.
2006	Cable to spooling mechanism has failed.	
2007	Move command failed due to spooling mechanism failure.	
2008	Exchange cartridge failed due to spooling mechanism failure.	
2009	Library test failed due to robotic assembly problem.	Review the test requirements and retry the test. If the test continues to fail, check for robotics obstructions or other robotics problems.
2010	Library test failed due to spooling mechanism defect.	Ensure that the spooling mechanism is fully seated in the controller module and installed correctly with the robotic assembly.
2011	Drive power board has failed. Some drives might be powered off.	1. *Ensure that the drive power boards are fully seated in the module. See "Installing the New Drive Power Board" in Spectra Stack DC-DC Converter Replacement Instructions*. 2. Power cycle the library.
2012	Multiple bottom covers detected.	Remove all bottom covers except for the bottom module in the library.
2013	Multiple top covers detected.	Remove all top covers except for the top module in the library.
2014	Bottom cover missing.	If the controller module cannot detect both a top and a bottom cover, the robotic mechanism will not move. 1. Install the bottom cover on the bottom module in library.

Event Code	Message Text and Description	Details and Solution
		2. Check the module interconnect cabling and module power cords.
2015	Top cover missing.	If the controller module cannot detect both a top and a bottom cover, the robotic mechanism will not move. 1. Install the top cover on the bottom module in library. 2. Check the module interconnect cabling and module power cords.
2016	Module alignment mechanism is not locked properly.	Ensure that the alignment mechanisms for all modules above the bottom module are engaged and locked.
2017	A communication problem between modules was detected.	1. Ensure that all modules are powered on. 2. Ensure that all module interconnect cables are properly attached. 3. Ensure that the alignment mechanisms for all modules above the bottom module are engaged and locked.
2018	Too many unit position transmitter or detector failures.	1. Ensure that the alignment mechanisms for all modules above the bottom module are engaged and locked. 2. Power cycle the library.
2021	Database access error.	1. Reboot the library.

Event Code	Message Text and Description	Details and Solution
		2. If the error persists, restore the library configuration. See Saving, Restoring, and Resetting the Library Configuration on page 60.
2022	Drive has been hot removed while in active status as LUN master. Tape drives must be powered off before removing them from the library.	Reinsert the removed drive in the same position from which it was removed.
2023	Internal software error.	Reboot the library.
2024	Exception thrown by application not handled.	An unrecoverable error occurred. Retry the operation and if the error persists reboot the library.
2025	Move failure due to vertical robotic assembly positioning problem.	1. Check for obstructions, such as a cartridge sticking out, in the vertical pathway of the robotic assembly. 2. Verify that the robotic assembly is aligned and level within the library. 3. Verify that the rack is level front to back and side to side.
2026	Failed moving the robot towards the back or front of the library.	Check for obstructions, such as a cartridge sticking out or cable impeding progress, in the horizontal pathway of the robotic assembly.
2027	Move failed pulling cartridge from element.	Check for labels or cartridge misalignments that would prevent the cartridge from coming out of the slot or drive.
2028	Move failed inserting cartridge to element.	Check for labels or cartridge misalignments that would prevent the cartridge from being inserted into the slot or drive.

Event Code	Message Text and Description	Details and Solution
2029	Initialization failure due to robot front to back positioning.	1. Check for obstructions, such as a cartridge sticking out, in the vertical pathway of the robotic assembly. 2. Ensure that the alignment mechanisms for all modules above the bottom module are engaged and locked. 3. Verify that the rack is level front to back and side to side. 4. Check to see if the robotic assembly is stuck in its locking mechanism. If so, move the robotic assembly out of the locking mechanism and then enable the locking mechanism properly.
2030	Failed during front to back movement.	Check for obstructions, such as a cartridge sticking out or cable impeding progress, in the horizontal pathway of the robotic assembly.
2031	Move failure due to right to left or left to right robot rotation failure.	
2032	Initialization failure due to robot gripper positioning error.	Check for obstructions, such as a cartridge sticking out, in the vertical pathway of the robotic assembly.
2033	Initialization failure due to robot vertical positioning error.	
2034	Cable to spooling mechanism has failed during initialization.	Ensure that the spooling mechanism is fully seated in the controller module and installed correctly with the robotic assembly.

Event Code	Message Text and Description	Details and Solution
2035	Initialization failure due to robot gripper positioning error.	Check for obstructions in the gripper pathway of the robot such as a cartridge sitting in the shuttle of the robot.
2036	Unintended termination of application process.	Reboot or power cycle system.
2037	Robotic firmware version upgrade failed.	Reboot or power cycle system. If the problem persists, contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10.
2038	Lost connection to Module.	Ensure that all modules are powered and have the interconnect cable properly attached. Reboot or power cycle the system.
2039	Cartridge left in robot gripper, unable to be moved to any open location.	Enable EE ports and ensure that some of them are free. Then power cycle library. If still failing, open covers and remove cartridge manually from gripper.
2040	Wellness test failed with critical error.	See codes 2041-2051.
2041	Wellness test failed because of unit lock failed.	Ensure that the alignment mechanism is engaged in every module that is above another module in the library
2042	Wellness test failed because of top cover is missing.	Install the top cover on the top module of the library. Also check the module interconnect cabling and module power cabling. If the controller module cannot detect both a top and bottom cover the robot will not move.

Event Code	Message Text and Description	Details and Solution
2043	Wellness test failed because of top cover is missing.	Install the bottom cover on the bottom module of the library. Also check the module interconnect cabling and module power cabling. If the controller module cannot detect both a top and bottom cover the robot will not move.
2044	Wellness test failed because of drive power board has failed.	1. *Ensure that the drive power boards are fully seated in the module. See "Installing the New Drive Power Board" in Spectra Stack DC-DC Converter Replacement Instructions*. 2. Power cycle the Library.
2045	Wellness test failed because of move media test failed.	Check for obstructions in the pathway of the robot such as a cartridge sticking out. Verify module alignment and frame alignment. Check if the robotic assembly is stuck in the lock mechanism. Move robotic assembly apart from lock mechanism and enable lock mechanism correctly.
2046	Wellness test failed because of drive communication test failed.	Remove and reseat the drive tray to ensure that the drive is fully seated. If the issue persists then reset the drive. Check the drive dump for more information. See Downloading Drive Logs on page 213.
2047	Wellness test failed because the barcode scanning test failed.	Verify that there is no obstruction in front of the barcode scanning module on the cartridge table located on the robotic assembly. If the error persists replace the robotic assembly. See the *Spectra Stack Spool Robotic Replacement Instruction.*

Event Code	Message Text and Description	Details and Solution
2048	Wellness test failed because the unlock of the right magazine failed.	Reboot the library and retry the test. If the error persists contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10.
2049	Wellness test failed because the unlock of the left magazine failed.	Reboot the library and retry the test. If the error persists contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10.
2050	Wellness test failed because the unlock of EE port bank failed.	Reboot the library and retry the test. If the error persists contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10.
2051	Wellness test failed because of the failing robotics test.	Check for obstructions in the pathway of the robot such as a cartridge sticking out. Verify module alignment and frame alignment. Check if the robotic assembly is stuck in the lock mechanism. Move robotic assembly apart from lock mechanism and enable lock mechanism correctly. Ensure that the spooling cable is fully seated in the controller module and connected correctly to the robotic assembly.
2052	An open magazine was detected in one or more modules and the robot movement has been stopped.	Ensure that all magazines are completely inserted and properly locked. Do not open magazines using the emergency release while the library is operating and the robot is moving.
2053	An open top cover was detected and the robot movement has been stopped.	Ensure that the top cover is completely inserted and properly locked. Do not open top cover using the emergency release while the library is operating and the robot is moving.

Event Code	Message Text and Description	Details and Solution
2054	An open bottom cover was detected and the robot movement has been stopped.	Ensure that the bottom cover is completely inserted and properly locked. Do not open bottom cover using the emergency release while the library is operating and the robot is moving.
2055	An open unit lock was detected and the robot movement has been stopped.	Ensure that all unit locks are properly locked. Do not open unit locks using the emergency release while the library is operating and the robot is moving.
2056	Initialization failure due to picker push pull positioning error.	Check for obstructions in the horizontal pathway of the robotic assembly such as a cartridge sticking out or a cable impeding progress.
2057	Robotic shipping lock in incorrect position.	Access the picker assembly and manually move the shipping lock lever to either a locked or unlocked position. After moving the shipping lock to the one of the correct positions, reboot the library.
2058	Maximum temperature for Drive Power Board 1 has exceeded. Shutting down the system.	Check the chassis fan and replace the fan if defective. See the *Spectra Stack Fan Replacement Instructions.*
2059	Maximum temperature for Drive Power Board 2 has exceeded. Shutting down the system.	Check the chassis fan and replace the fan if defective. See the *Spectra Stack Fan Replacement Instructions.*
2060	Chassis CPU maximum temperature exceeded. Shutting down the system.	Check the chassis fan and replace the fan if defective. See the *Spectra Stack Fan Replacement Instructions.*
2061	Move failed pulling cartridge from drive.	Check for labels or cartridge misalignments that would prevent the cartridge from coming out of the drive.

Event Code	Message Text and Description	Details and Solution
2062	Move failed inserting cartridge to drive.	Check for labels or cartridge misalignments that would prevent the cartridge from coming out of the drive.
2063	Move failed positioning picker in front of drive.	Contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10.
2064	Library test failed with critical error.	Contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10.
2065	Library startup process failed because of robotics initialization issue.	Contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10.
2066	Library startup process failed during inventory scan.	Contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10.
2067	For safety reason the robot movement was halted in place.	Ensure that all magazines, top or bottom covers and unit locks are completely inserted and properly locked. Do not open magazines using the emergency release or remove covers or unit locks while the library is operating and the robot is moving. Ensure that all modules are powered and have the interconnect cable properly attached.
2068	An emergency stop condition was detected in one or more modules and prevented the robotic assembly from initialization.	Ensure that all magazines, top or bottom covers and unit locks are completely inserted and properly locked. Please insert all open magazines and install all necessary covers and unit locks before powering on the library. Ensure that all modules are powered and have the interconnect cable properly attached.

Event Code	Message Text and Description	Details and Solution
2069	Initialization failure due to barcode reader error.	Contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10.
2070	Inventory scan failed because of Elevator axis problem.	Check for obstructions in the vertical pathway of the robot such as a cartridge sticking out. Verify module alignment and rack alignment.
2071	Cartridge on picker when trying to scan.	Verify that there is no obstruction in front of the barcode scanning module on the cartridge table located on the robotic assembly. If the error persists replace the robotic assembly. See the *Spectra Stack Spool Robotic Replacement Instruction.*
2072	Top cover detected at an incorrect position.	Examine the library and adjust the cover to the proper position.
2073	Bottom cover detected at an incorrect position.	Examine the library and adjust the cover to the proper position.
2074	The library startup failed due to a GPIO error.	Reboot or power cycle system.
2075	The library startup failed due to an error when trying to open the robotic serial port.	Reboot or power cycle system.
2076	I2C bus signals invalid.	Contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10.
2078	Incompatible robotic assembly without encoder detected.	Upgrade the firmware to a version which supports encoder-less control (see Software Upgrades on page 208) or replace the robotic assembly with a compatible model with an encoder (see the *Spectra Stack Spool Robotic Replacement Instruction).*

WARNING EVENTS

Event Code	Message Text and Description	Details and Solution
4000	A reported drive canister fan speed is too slow.	Ensure that there are no obstructions to the drive fans.
4001	There is a Fibre Channel Loop ID conflict.	Change the FC to fabric or use a different loop setting.
4002	A drive sent a clean request.	Clean the drive with an approved cleaning cartridge.
4003	The drive configuration failed.	**1.** Remove the drive from the library, reinsert it and then retry the operation. **2.** If the drive installed is a different LTO generation than the drive previously installed, reset the library defaults and then reconfigure the drive. **3.** Check the drive dump for more information. See Downloading Drive Logs on page 213.
4004	The drive status request failed.	**1.** Remove the drive from the library, reinsert it and then retry the operation. **2.** If the problem persists, reset the drive. **3.** Check the drive dump for more information. See Downloading Drive Logs on page 213.
4005	Drive is reporting a critical TapeAlert.	**1.** Power cycle the drive and then verify whether the drive reports the same TapeAlert.

Event Code	Message Text and Description	Details and Solution
		2. Check the drive dump for more information. See Downloading Drive Logs on page 213.
4006	A drive temperature reported is above the threshold.	1. Verify that the drive fan is spinning and not obstructed. 2. Verify that the ambient temperature is within specification.
4007	Cartridge error.	1. Remove the cartridge and inspect it for damage. 2. Retry the operation with another cartridge.
4008	Cleaning tape expired.	Discard the cleaning cartridge and retry the cleaning operation with a new cleaning cartridge.
4009	Firmware upgrade of one or multiple expansion modules failed.	The controller module must be able to communicate with a powered on and connected expansion module to perform the upgrade. 1. Reseat the expansion module controller. 2. Check the module interconnect cable and power connections. 3. Retry the firmware upgrade.
4010	Drive is not compatible with this library.	Remove the incompatible drive. Only install drives that are supported by the library.
4011	Drive is not supported in this library.	
4012	Move cartridge operation filed due to drive issue.	1. Check events occurring at the same time for drive problems.

Event Code	Message Text and Description	Details and Solution
		2. Retry the operation with the same source and destination. If the problem persists, retry the operation with a different cartridge in the same drive. 3. Check the drive dump for more information. See Downloading Drive Logs on page 213.
4013	Exchange cartridge failed due to a drive issue.	1. Retry the operation with the same source and destination. If the problem persists, retry the operation with a different cartridge in the same drive. 2. Check the library event log for events associated with this drive. See Viewing Log Files on page 205. 3. Check the drive dump for more information. See Downloading Drive Logs on page 213.
4014	Library test failed due to a drive issue.	1. Verify the test parameters and then retry the test. 2. Check the library event log for events associated with this drive. See Viewing Log Files on page 205. 3. Check the drive dump for more information. See Downloading Drive Logs on page 213.
4015	Power supply has failed. Redundancy is not available.	1. Ensure that all power supplies are installed properly.

Event Code	Message Text and Description	Details and Solution
		2. Verify that all power sources are supplying power that is within the product requirements.
4016	Backup configuration data to controller module failed.	1. If possible, save the library configuration to a file. 2. Power cycle the library and retry the operation.
4017	Restore configuration data from chassis failed.	
4018	Firmware upgrade of one or more drives failed due to drive issue.	1. Verify that the firmware file is correct for the drive. 2. Ensure that the drive is in a healthy state and does not have a cartridge loaded. 3. Retry the operation.
4019	General drive firmware bundle upgrade failure.	
4020	Database has been reset due to a problem that prevented the library from powering up.	Restore previously saved configuration data.
4021	Drive has been hot removed while in active status as data transfer device. Drives must be powered off before removing them from the library.	Reinsert the removed drive in the same position from which it was removed.
4022	A full-height drive in incorrect boundary location. Full-height drives only operate in the very top, very bottom, or middle pair of half-height drive bays.	Reinstall the tape drive in an acceptable location.
4023	Drive not cable (ports not linked up).	The tape drive must have an FC or SAS cable attached to transfer data and communicate with host applications.
4024	One or two unit position transmitter/detector failures.	Contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10.

Event Code	Message Text and Description	Details and Solution
4025	Library test failed due to a cartridge error.	1. Remove the cartridge and inspect it for damage. 2. Retry the operation with another cartridge.
4027	Library Test failed due to a cartridge error.	
4028	Drive cannot use this media due to it being an unknown or unsupported format. Possibly the media is the wrong generation of media.	Check that the LTO generation of the tape cartridge is the same generation indicated on the barcode label. Remove cartridges which are not compatible to your tape drives.
4029	Incompatible media move operation blocked by media barcode ID check.	Check if Media barcode label is matching LTO generation. Replace label or remove incompatible media from your system.
4030	Move cartridge operation failed due to media error.	Remove the cartridge and inspect it for damage. Retry the operation with another cartridge.
4031	Exchange media failed due to media error.	Remove the cartridge and inspect it for damage. Retry the operation with another cartridge.
4041	Wellness test failed because of power supply redundancy test failed.	Ensure all power supplies are installed properly (two per module), and that each power supply is connected to a valid power source.
4044	One of the Library tests failed because of a source element or destination element is currently not accessible.	Contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10.
4054	Chassis fan failed.	Check the chassis fan and replace the fan if defective. See the *Spectra Stack Fan Replacement Instructions.*

Event Code	Message Text and Description	Details and Solution
4060	Connection to the KMIP server failed.	Verify username and password as well as all needed SSL certificates needed for connecting to the KMIP server. Verify that the KMIP server is reachable within the network.
4061	Key not found on KMIP server.	Verify that the requested key is available on the KMIP server. Check the KMIP server logs for additional details.
4062	Key creation on KMIP server failed.	Check the KMIP server logs for additional details about the key creation failure.
4063	KMIP configuration invalid.	Use the KMIP configuration wizard to verify the KMIP configuration.
4064	KMIP feature not licensed.	Disable KMIP or install appropriate license for KMIP feature.
4065	A tape alert flag was reported by a drive.	Contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10.
4067	Cleaning cartridge will expire soon and should be replaced.	Replace the cartridge.
4068	No cleaning cartridge found.	Auto cleaning is enabled, but the library contains no labeled cleaning cartridge. The library was unable to perform the auto clean function for one or more drives. Install a valid and labeled cleaning cartridge and then perform a load and unload on the drive that needs to be cleaned to initiate the auto cleaning.

Event Code	Message Text and Description	Details and Solution
4069	Configuring the drive default map ID was not possible.	Ensure the drive is powered up, is communicating with the library, and has up to date firmware. If this error persists, contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10.
4071	Power supply fan failed.	Verify the power supply fan is spinning and ensure there are no obstructions in the fan.
4072	No cleaning cartridge in partition available for auto cleaning.	Auto cleaning is enabled, but the partition contains no labeled cleaning cartridge. The library was unable to perform the auto clean function for one or more drives in this partition. Install a valid and labeled cleaning cartridge into the partition and then perform a load and unload on the drive that needs to be cleaned to initiate the auto cleaning.
4073	Medium source element empty.	Check the source slot visually and rescan inventory. Additionally check for valid and readable barcode label.
4074	Medium source element empty.	Check the source slot visually and rescan inventory. Additionally check for valid and readable barcode label.
4075	Cartridge lost while extracting it from slot/drive.	Check the source element and ensure that there are no obstructions in the pathway of the robot.

Event Code	Message Text and Description	Details and Solution
4077	Unlocking the right magazine failed.	Reboot the library and retry the operation. If the magazine needs to be removed to get access to the tape cartridges, first power down the library and then release the magazine manually. Only one magazine can be open at a time. If the problem persists, contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10
4078	Unlocking the left magazine failed.	Reboot the library and retry the operation. If the magazine needs to be removed to get access to the tape cartridges, first power down the library and then release the magazine manually. Only one magazine can be open at a time. If the problem persists, contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10
4079	Unlocking the EE port failed.	Reboot the library and retry the operation. If the EE port needs to be removed to get access to the tape cartridges, first power down the library and then release the entire magazine manually. Only one magazine can be open at a time. If the problem persists, contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10
4080	Wellness test failed with warning.	Contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10.

Event Code	Message Text and Description	Details and Solution
4082	Magazine release motor initialization failure.	Reboot the library and if the error persists contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10. If magazines need to be removed to get access to the tape cartridges, first power down the library and then release one by one magazine manually. Only one magazine can be open at a time.
4085	Too many retries of drive command needed because of UnitAttention or NotReady condition.	Contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 10.
4086	Move operation failed due to the inability accessing the database.	Ensure the network the library is connected to is operating normally and ensure the library is running the latest firmware. Library needs reboot.
4088	Library not properly calibrated. This may cause media movement failures.	The library needs to be re-calibrated. Reboot the library to initiate a re-calibration of the system. Ensure the library firmware is up to date. If this event persists after a reboot of the library, or if calibration does not begin automatically upon restart, login as the Service user and manually initiate calibration via the **Maintenance > Auto Calibration RMI** menu.
4093	Could not obtain an IP address from DHCP server.	Check the network configuration settings and check if the DHCP server is reachable. Use the network configuration menu or unplug the network cable and plug it in after a few seconds to trigger an automatic reconfiguration of the network interface.

CONFIGURATION CHANGE EVENTS

Event Code	Message Text and Description
8000	The configuration of a drive changed.
8001	The drive was added or removed from the system.
8002	A partition was added, removed, or changed.
8003	An EE port bank was enabled or disabled.
8004	Drive firmware changed due to firmware upgrade.
8005	The configuration of hostname/domain name has changed.
8006	The email configuration settings have changed.
8007	The configuration of a date/time format changed.
8008	The system language setting changed.
8009	The timezone configuration has changed.
8011	The network settings have changed.
8012	The firmware for all expansion modules has been upgraded.
8013	The NTP time synchronization configuration has changed.
8014	SSH access was enabled or disabled.
8015	Level of media generation checking has changed.
8016	Library reset to default settings invoked by user.
8017	Library firmware changed.
8019	Robotic firmware version upgraded.
8022	RMI/OCP Timeout configuration changed.
8024	EE port/Magazine access control configuration changed.
8025	EE port/Magazine automatic re-lock duration changed.

Event Code	Message Text and Description
8026	Robotics change detected.
8027	Power Board has changed.
8028	Power Supply has changed.
8029	The SNMP configuration changed.
8030	An SNMP target has been added.
8031	An SNMP target has been deleted.
8032	The SNMPv3 settings changed.
8033	The OCP module has been changed.
8034	Manual Drive reset executed.
8036	New chassis detected.
8037	Chassis has been removed.

INFORMATIONAL EVENTS

Event Code	Message Text and Description
9000	A tape alert flag was reported by a drive.
9001	A drive is present in the system but powered off.
9002	The library was powered on.
9003	A move media command was executed.
9004	Inventory scan was performed.
9005	The library was powered down from the front panel.
9006	The network interface was enabled.
9007	The network interface was disabled.
9008	The system time was synchronized with an SNTP server.
9009	A magazine was unlocked and opened.
9010	A magazine was closed and locked.
9011	An EE port bank was unlocked and opened.
9012	An EE port bank was closed and locked.
9013	A user logged into the RMI interface.
9014	A user logged out of the RMI interface.
9015	A user logged into the OCP interface.
9016	A user logged out of the OCP interface.
9024	Drive support ticket created.
9025	Library test started.
9026	Library test successfully finished.
9027	Library test stopped by user.

Event Code	Message Text and Description
9028	Configuration backup to controller module was successful.
9029	Configuration restore from controller module was successful.
9031	Library Health Status changed to "Status OK".
9032	Library health status changed to status "Warning".
9034	New system controller detected.
9035	New library chassis detected.
9037	The library was rebooted.
9038	The library was rebooted through user interface.
9041	Key on KMIP server created.
9042	Drive cleaning completed.
9043	Drive cleaning was started.
9045	Library configuration data failed to duplicate on to the controller module.
9046	Chassis fan speed could not be determine.

CHAPTER 10 - 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 BlueVision Software Support key is required in order to obtain technical support.

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**.

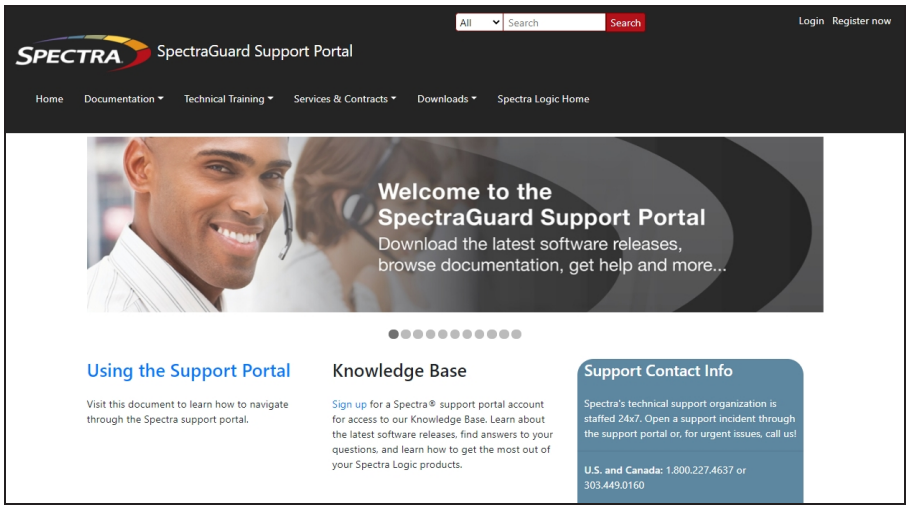


Figure 144 The Spectra Logic Technical Support portal home page.

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.

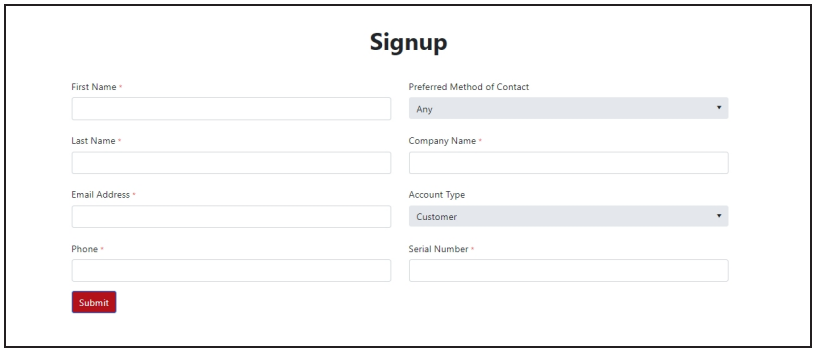


Figure 145 The Signup screen.

- 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.

Search for Help Online

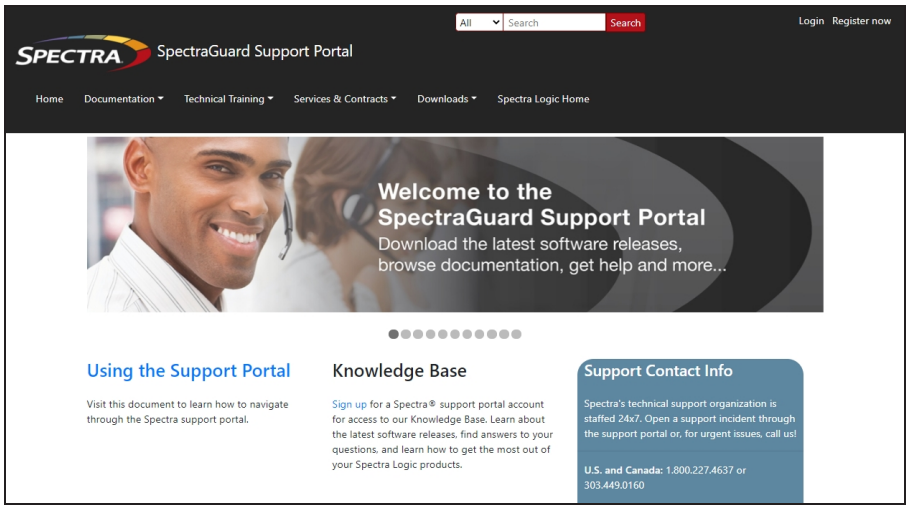


Figure 146 The Spectra Logic Technical Support portal home page.

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 on the **Configuration>Settings** screen.
   - 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 Technical Support on page 263 if you have not previously created an account on the Technical Support portal.

4. From any page, select **Incident>Incidents & Inventory**.

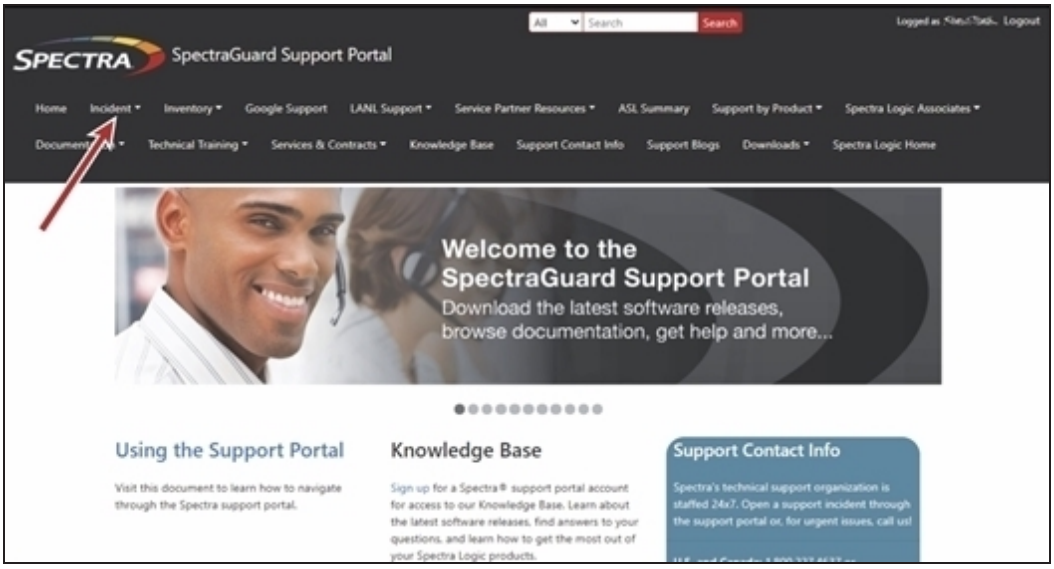


Figure 147 Select **Incidents>Incidents & Inventory**.

5. Select **Open or View Incidents**.

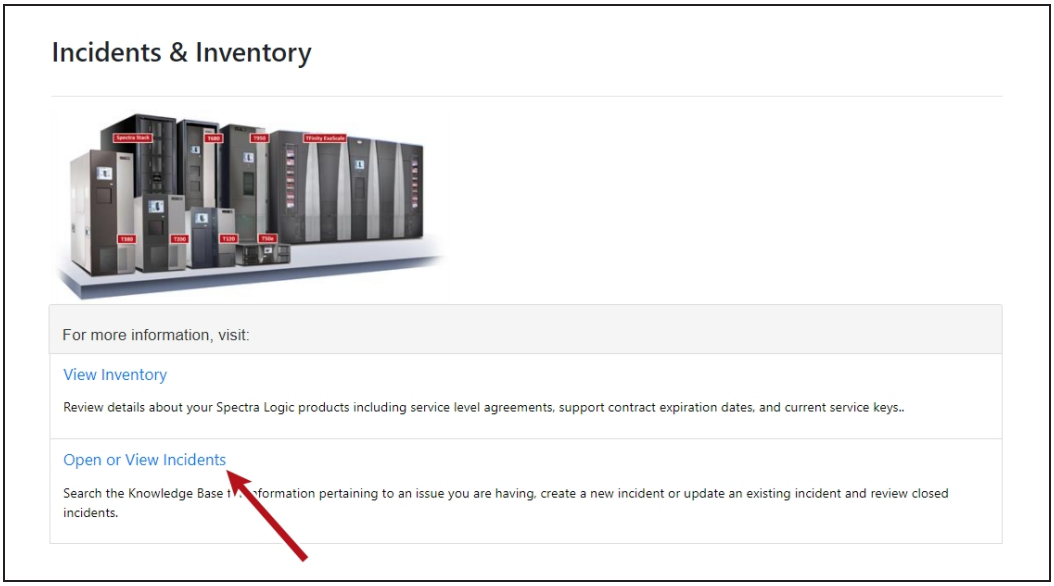


Figure 148 Select **Open or View Incidents**.

6. In the Search dialog box, enter a term or phrase about your problem (**1**) and click **Search** (**2**).

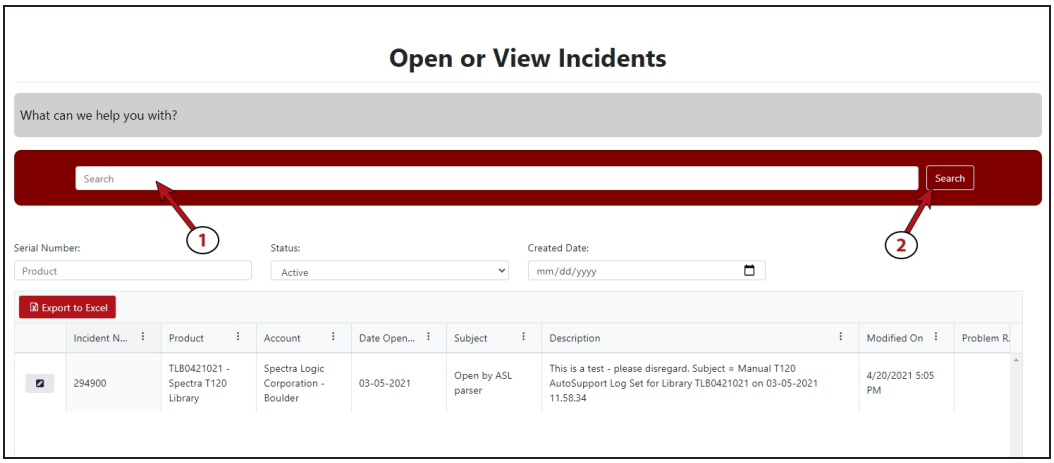


Figure 149 Enter a search phrase and click **Search**.

7. If the search does not provide an answer, click **Open a New Incident**.

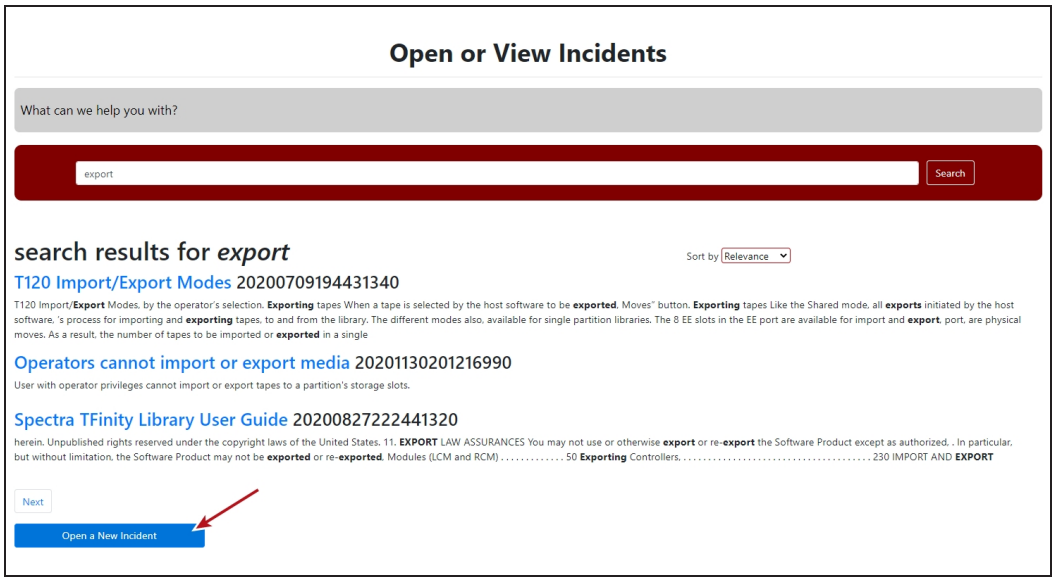


Figure 150 Click **Open a New Incident**.

8. On the Create Incident page, enter the requested information providing as much detail as possible. When you are finished, click **Submit**.

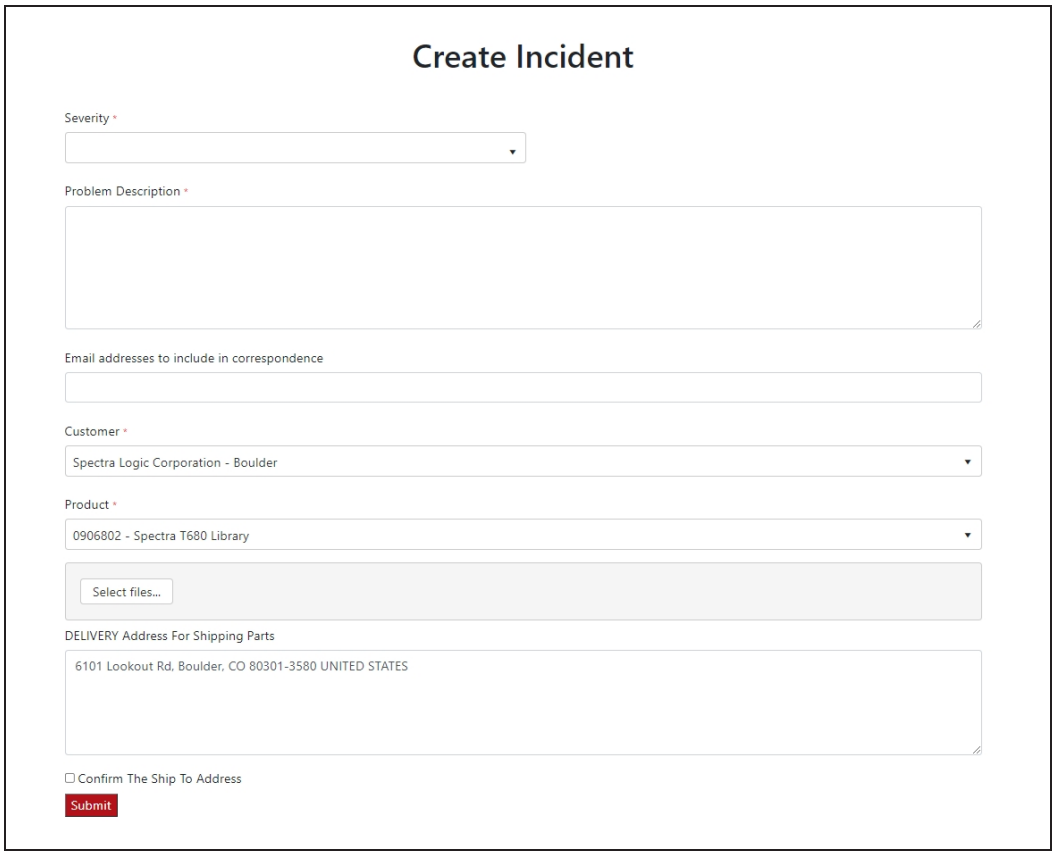


Figure 151 Enter information about your incident and click **Submit**.

Submit an Incident Online

1. Make notes about the problem, including what happened just before the problem occurred.
2. Gather the following information:
   - Your Spectra Logic customer number
   - Company name, contact name, phone number, and email address
   - The library serial number on the **Configuration>Settings** screen.
   - 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 Technical Support on page 263 if you have not previously created an account on the Technical Support portal.

4. From any page, select **Inventory>My Inventory**.
5. Locate the row of the product for which you want to submit an incident and click **Create Incident**.

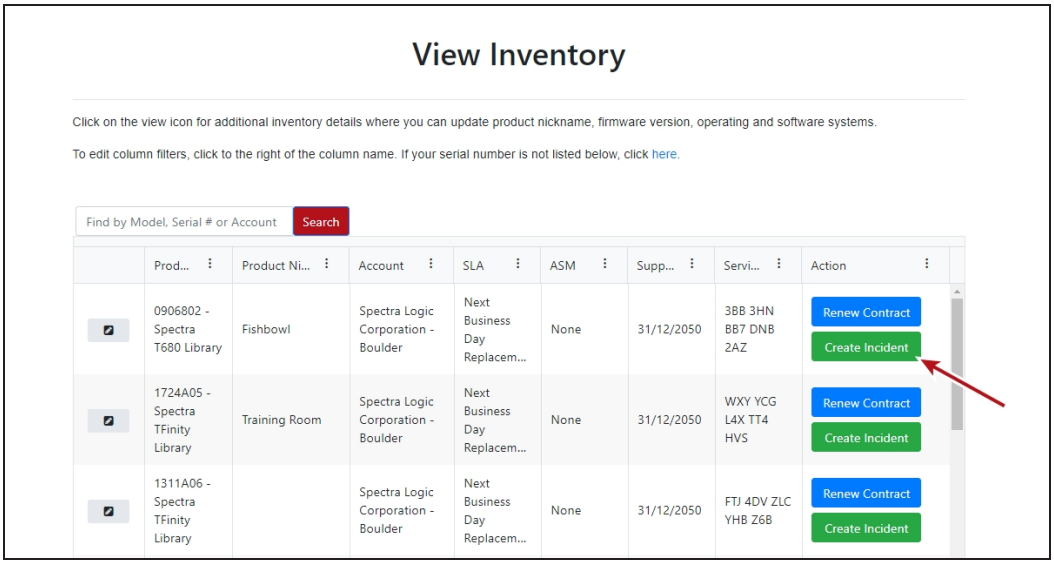


Figure 152 Click **Create Incident**.

6. On the Create Incident page, enter the requested information providing as much detail as possible. When you are finished, click **Submit**.

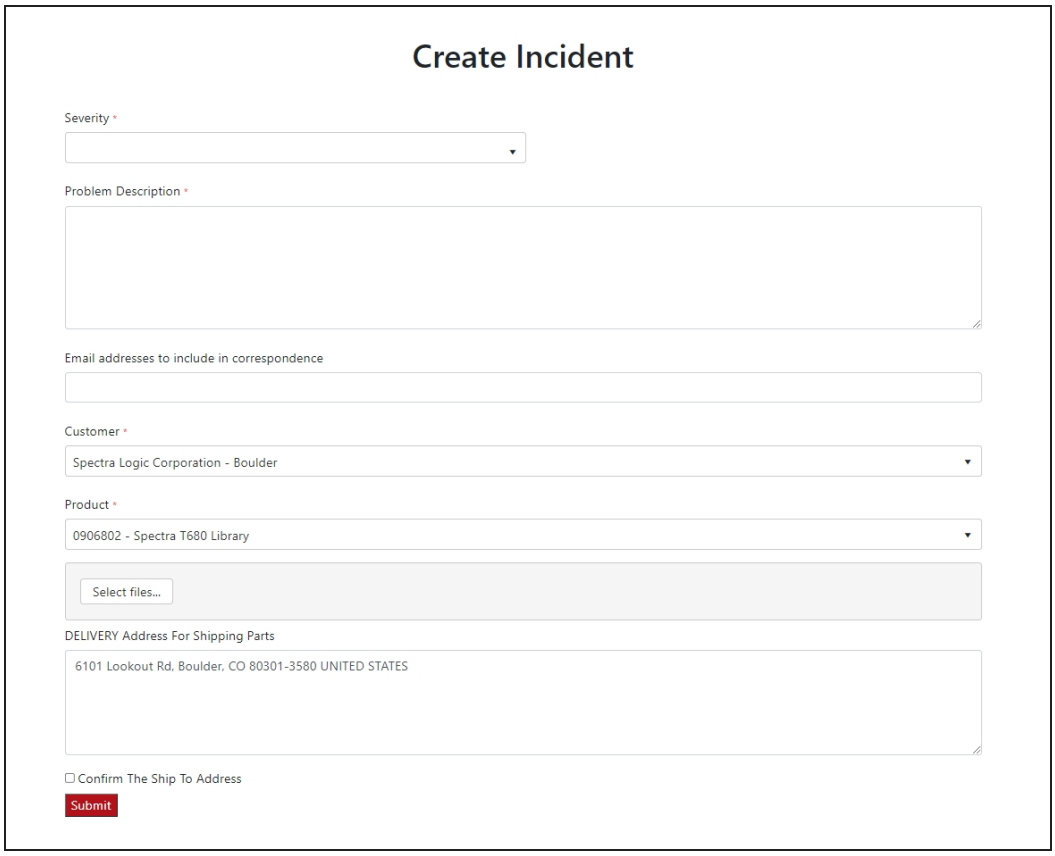


Figure 153 Enter information about your incident and click **Submit**.

Submit an Incident by Phone

Contact Spectra Logic Technical Support by phone using the information below.

Spectra Logic Technical Support	
Technical Support Portal: ***support.spectralogic.com***	
United States and Canada **Phone:** **Toll free US and Canada:** 1.800.227.4637 **International:** 1.303.449.0160	**Europe, Middle East, Africa** **Phone:** 44 (0) 870.112.2185 **Deutsch Sprechende Kunden** **Phone:** 49 (0) 6028.9796.507
Additional international numbers available at *support.spectralogic.com/home* **If you have a Spectra Logic Portal account, please log in for country-specific numbers at *support.spectralogic.com/support-contact-info***	

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).

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 10). 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 - SPECIFICATIONS

This appendix provides specifications for the Spectra Stack Tape library.

PHYSICAL SPECIFICATIONS

Parameter	Unpackaged	Packaged
Height	10.5 inches (268 mm)	24.2 inches (615 mm)
Width	18.7 inches (475 mm)	31.5 inches (800 mm)
Depth	35.1 inches (892 mm)	47.2 inches (1200 mm)
Weight	**Controller module:** 78.2 lb (35.5 kg) **Expansion module:** 68.3 lb (31.0 kg)	**Controller module:** 120.1 lb (54.5 kg) **Expansion module:** 110.2 lb (50.0 kg)

Rack Requirements

The rack for the Spectra Stack library must meet the following requirements.

CAUTION You must locate the rack 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 system or its drives.

The Spectra Stack library is designed to fit in a standard 19-inch, 4-post rack. Keep the following in mind when selecting a rack:

- Make sure that the distance between the mounting surfaces on the front and rear posts is between 26.6 inches (67.5 cm) and 30.8 inches (78.2 cm).

  Note: If you are using the adaptors to install the rack-mount kit in a rack with circular mounting cutouts, the distance between the front and rear posts must be at least 28.1 inches (71.3 cm), and not more than 32.3 inches (82 cm).

- Allow approximately 3 inches (8 cm) of additional depth at the back of the rack for cable clearance.
- Some racks may require at least 2 inches (5 cm) of clearance between the front door frame and the front mounting posts of the rack to allow the door to close.

- Check your rack's specifications to make sure it accommodates the weight and depth of the Spectra Stack library.

  Notes:
  - Spectra Logic does not support the use of a two-post rack with a Stack library.
  - Threaded round hole racks are not supported.
  - An enclosed 19-inch, four-post rack is available for purchase from Spectra Logic. The rack has two doors and removable side panels. Contact Spectra Logic Sales for more information (see Contacting Spectra Logic on page 4).

- In earthquake prone areas, provide restraints as necessary.

WARNING In earthquake- prone areas, the rack must have stabilizing equipment or be anchored to the floor to eliminate the risk of tipping, which could lead to personal injury.

ENVIRONMENTAL SPECIFICATIONS

Library Environmental Specifications

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)

Storing [b] and Shipping (Non-Operating) Environment Specification	
Humidity	10% to 95% (non-condensing)
Temperature	–40° F to 149° F (–40° C to 65° C)
Altitude	Sea level to 40,000 ft (12,192 m)

[a] The temperature and humidity must be allowed to stabilize in the specified ambient environment for 24 hours.

[b]The library is in its original packaging. The packaging is designed to protect the library from condensation caused by extreme temperature variations of 27° F (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.

ELECTRICAL SPECIFICATIONS

Parameter	Specification
Current	2.5 A
Voltage	100-240 V
Input Frequency	50-60 Hz
MAX Power	550 watts

REGULATORY SPECIFICATIONS (CSA TEST CONDITIONS)

Note: The CSA test conditions might differ from the product specification limits.

Parameter	Tested Condition or Value
Equipment mobility	Stationary - rack mount
Connection to the mains	Pluggable - Type A
Operating condition	Continuous
Access location	Operator accessible
Over voltage category (OVC)	OVCII
Mains supply tolerance (%) or absolute mains supply values	-10%, +6%
Tested for IT power systems	No
IT testing, phase-phase voltage (V)	N/A
Class of equipment	Class I
Considered current rating (A)	20 A (branch circuit protection)
Pollution degree (PD)	PD 2
IP protection class	IPXO
Altitude during operation (m)	Maximum 6565 feet (2000 meters)
Altitude of test laboratory (m)	125 feet (38 meters)
Mass of equipment (kg)	Maximum 55.1 lb (25 kg)
Manufacturer's Declared Ambient (0C)	104° F (40° C)

DEFAULT SETTINGS

Parameter	Default Setting	Reset During Reset Default Settings?
Users and Passwords		
Administrator login	**User:** administrator **Password:** blank	No
User login	**User:** user **Password:** blank	Yes
Network Configuration (EthO)		
DHCP	Enabled	
Host name	Blank	
IP address	(obtain from DHCP)	
Subnet mask	(obtain from DHCP)	
Default gateway	(obtain from DHCP)	
Network Configuration		
IPv4	Enabled	No
DHCPv4	Enabled	No
IPv6	Disabled	No
Static V6	Disabled	No
Stateless V6	Disabled	No
DNS Configuration	Blank	No
Network Access Services		
Primary network interface (ethO)	Enabled	
SSH	Enabled	

Parameter	Default Setting	Reset During Reset Default Settings?
SSL	Disabled	
LDAP	Disabled	Disabled with configuration retained
Slots		
EE ports	Disabled	Yes
Administrator password required for EE port removal	Enabled	Yes
Reserved slots	0	Yes
Partitions	Disabled (no partitions)	All deleted leaving a single partition
Date and Time		
NTP /SNTP setting	Disabled	Configuration retained
Date	Blank or existing	
Time	Blank or existing	
Time zone	GMT	
Email notifications (SMTP)	Disabled	Disabled with configuration retained
SNMP/SMI-S		
SNMP v1, v2	Disabled	Disabled with configuration retained
SCSI Defaults		
Library product ID - INQUIRY product ID string (Std Inquiry page)	Python	

Parameter	Default Setting	Reset During Reset Default Settings?
Library vendor ID - INQUIRY vendor ID string (Std Inquiry page)	Spectra	
SCSI element addressing	Starting element addresses **Values in decimal:** • Slot: 1001 • Picker: NA • Drives: 1 • I/E slots: 101 **Values in hexadecimal:** • Slot: Ox3E9 • Picker: NA • Drives: Ox1 • I/E slots: Ox65	Yes
Miscellaneous Settings		
Return drive serial numbers to host	Enabled	
Return barcodes to host (RES SCSI data)	Enabled	
Barcode format and length returned to host	8 digits, left justified	Yes
Language settings	English	Yes
Miscellaneous Settings Continued		
Auto unload (library controlled unload)	Enabled	
Log tracing	Continuous, all levels selected	Yes
Ignore barcode media ID	Disabled	Yes

Parameter	Default Setting	Reset During Reset Default Settings?
All licensed features	Disabled	Disabled, configuration retained where possible
Licenses	Not applicable	Not deleted
OCP		
Barcode format displayed on OCP	8 digits, left justified	Yes
OCP contrast		No
Screen saver		Yes
Drive Defaults		
Drive speed and topology setting	Auto speed/Fabric	Yes
Drive hosting the library LUN	Drive 1 or the lowest numbered existing drive	Yes
Drive power	All drives powered on	Yes
Auto clean	Disabled	Yes

BARCODE LABEL SPECIFICATIONS

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 for LTO Cartridge Barcodes on the next page.

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.

Barcode Data

The library supports barcode data strings consisting of from 1 to 16 characters, including an optional checksum character. Quiet zones precede and follow the start and stop characters.

The barcode data string on standard Spectra Logic barcode labels consists of a start character, eight alphanumeric characters, a checksum character, and the stop character. Quiet zones precede and follow the start and stop 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 use of “CLN” and “DG{space}” at the beginning of the volume identifier is reserved.

  - 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 last two (2) characters are the media identifier and indicate the cartridge Media Type (for example, "L" for LTO and "6" for an LTO-6 cartridge. In IBM LTO tape drives, the value of the media identifier on cleaning cartridges is ignored, although a valid value must be present.
- 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 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, the optional checksum character, and the stop character.

Detailed Specifications for LTO Cartridge Barcodes

Figure 154 shows the dimensional specifications for LTO labels with the alphanumeric characters above the barcode.

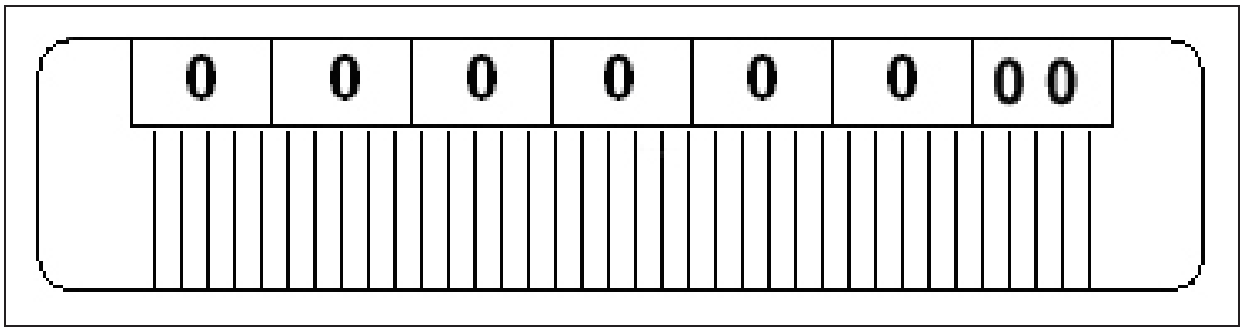


Figure 154 Barcode specifications for LTO media; alphanumeric characters on top.

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.

LTO Barcode Element Specifications

For the official IBM barcode label specification, see *https://ibm.com/support/docview.wss?uid=ssg1S7000429*. Unless otherwise specified, tolerances are X.XXX ± 0.127 mm, X.XXX ± 0.762 mm.

- 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 or –0.076 mm.
- The nominal width of the wide spaces and bars is 1.188 mm.
- The inter-character gap is 0.432 mm +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 the printed area associated with 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.

LTO 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.

ELECTROSTATIC DISCHARGE

To prevent damaging the system, be aware of the precautions you must follow when setting up the library or handling parts. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

Preventing Electrostatic Damage

To prevent electrostatic damage, observe the following precautions:

- Always be properly grounded when touching a static-sensitive component or assembly.
- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.

Grounding Methods

There are several methods for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm (± 10 percent) resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.
- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have an authorized reseller install the part.

Note: For more information on static electricity, or assistance with product installation, contact your authorized reseller.

Power Consumption and Cooling Requirements

The power and cooling requirements for the library depend on the number and type of drives installed and number of library modules. The following table provides the maximum power consumption and heat load for the base module fully loaded with half-height and full-height drives and expansion modules fully loaded with half-height and full-height drives. Use this information to calculate the total 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)
Spectra Stack with 3 Full-Height Drives	151	515
Spectra Stack with 6 Half-Height Drives	235	801
Spectra Stack and 6 Expansion Modules with 21 Full-Height Drives	883	3011
Spectra Stack and 6 Expansion Modules with 42 Half-Height Drives	1471	5016
LTO-9 Fibre Channel Full-Height	• **Read/write:** 40	**Read/write:** 136
LTO-9 Fibre Channel or SAS Half-Height	• **Read/write:** 40	**Read/write:** 136
LTO-9 Fibre Channel Full-Height	• **Read/write:** 35	**Read/write:** 119

Component	Power Consumption (watts)	Heat Load, Continuous (BTU/hour)
LTO-9 Fibre Channel or SAS Half-Height	• **Read/write:** 35	**Read/write:** 119
LTO-8 Fibre Channel Full-Height	• **Read/write:** 40	**Read/write:** 136
LTO-8 Fibre Channel or SAS Half-Height	• **Read/write:** 43	**Read/write:** 146
LTO-7 Fibre Channel Full-Height	• **Read/write:** 31	**Read/write:** 106
LTO-7 Fibre Channel or SAS Half-Height	• **Read/write:** 31	**Read/write:** 106
LTO-6 Fibre Channel	• **Read/write:** 28	**Read/write:** 95
LTO-5, Fibre Channel	• **Read/write:** 37	**Read/write:** 126

LTO Tape Drive Specifications

This section provides specifications for the LTO drives supported by the library. See Tape Media Specifications on page 555 for information about the media used in the library.

Note: LTO drives and media are also referred to as Ultrium or LTO Ultrium drives and media.

LTO-10 Drive

When connecting to a Fibre Channel network, LTO-10 Fibre Channel drives will attempt to connect at 32 Gb/second, but will auto-negotiate down depending on the requirements of the port to which the drive is connected.

LTO-10 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 1000 MB/second, compressed SAS 1200 MB/second, compressed Fibre
Speed matching range	157 MB/second to 407 MB/second
Average space record time	45 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: 39.8 watts typical Idle: 27.5 watts (empty drive)

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-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

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.

---

aAssuming a 2.5:1 compression ratio. Compression throughput depends on the type of data.

bThis is a per-drive value. Total sustained transfer rate for the library depends on the number of drives installed in the library.

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 [c] 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	Full-height: • **Read/write:** 40 W **Idle:** 15 W Half-height: • **Read/write:** 43 W **Idle:** 14 W

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.

[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-8 drive at 360 MB/second.

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	56 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	• Full-height: **Read/write:** 31 W **Idle:** 20 W • Half-height: **Read/write:** 36 W **Idle:** 20 W

LTO-6 Drive

When connecting to a Fibre Channel network, LTO-6 Fibre Channel drives will attempt to connect at 8 Gb/second, but will 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.

[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.

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	1×10^{-17} bits
Power consumption	Read/write: 28 watts typical Idle: 8 watts

LTO-5 Drive

When connecting to a Fibre Channel network, LTO-5 Fibre Channel drives will attempt to connect at 8 Gb/second, but will 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.

Parameter	Specification
Maximum sustained transfer rate [d, e]	140 MB/second, native [f] 280 MB/second, compressed
Speed matching range	30 MB/second to 140 MB/second

[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 Gb interface speed will not stream an LTO-6 drive at 160 MB/second.

[d] Assuming a 2:1 compression ratio. Compression throughput depends on the type of data.

[e] This is a per-drive value.

[f] A 1 Gb interface speed will not stream an LTO-5 drive at 140 MB/second.

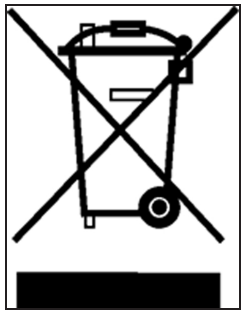
Parameter	Specification
Average space record time	75 seconds
Encryption capability	AES 256-bit
WORM capability	Yes
MTBF	250,000 hours at 100% duty cycle
Uncorrected error rate	1 x 10^{-17} bits
Power consumption [b]	Read/write: 27 watts typical Idle: 7.5 watts

Appendix B - Regulatory Information

Note: To comply with the following regulations and standards, the library must be properly installed in an office or industrial environment with shielded cables and adequate grounding of the SCSI bus and the input power.

Recycling and disposal

Disposal of waste equipment by users in private household in the European Union and Norway

	This symbol on the product or on its packaging indicates that this product must not be disposed of with your other household waste. Instead, it is your responsibility to dispose of your equipment by handling it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at this time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or the shop where you purchased the product.

CE mark

	The CE mark is a mandatory conformity mark on many products placed on the single market in the European Economic Area (EEA). The CE marking certifies that a product has met EU consumer safety, health or environmental requirements.

CCL MARK

FCC (UNITED STATES)

The computer equipment described in this manual generates and uses radio frequency (RF) energy. If the equipment is not installed and operated in strict accordance with the manufacturer's instructions, interference to radio and television reception might result.

This equipment complies with Part 15 of the FCC Rules. Operation is subject to the following conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Part 15, Class A, of the FCC Rules, is designed to provide reasonable protection against radio and television interference in a residential installation. Although the equipment has been tested and found to comply with the allowed RF emission limits, as specified in the above-cited Rules, there is no guarantee that interference will not occur in a particular installation. Interference can be determined by turning the equipment off and on while monitoring radio or television reception. The user may be able to eliminate any interference by implementing one or more of the following measures:

- Reorient the affected device and/or its receiving antenna.
- Increase the distance between the affected device and the computer equipment.
- Plug the computer and its peripherals into a different branch circuit from that used by the affected device.
- If necessary, consult an experienced radio/television technician for additional suggestions.

CANADIAN VERIFICATION

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations (ICES-003, Class A).