Spectra Encryption User Guide

SpectraLogic.com

Copyright

Notices

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

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

Trademarks

Part Number

90940012 Revision M

Revision History

Revision	Date	Description
A	March 2006	Initial release.
B- E		Corrections and updates.
F	April 2012	New template. Update for BlueScale 12 release.
G	December 2012	Added Spectra SKLM.
H	April 2015	Corrections. Trademark update.
I	April 2016	Added LTO-7.
J	August 2016	Corrections.
K	January 2017	Updated for KMIP encryption key management.
L	June 2017	Updated for KMIP encryption key management with TS11xx technology drives.
M	August 2022	Updated for Spectra Stack, LTO-8, and LTO-9.

Notes:

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

End User License Agreement

1. READ CAREFULLY

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

2. OWNERSHIP

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

3. GENERAL

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

4. SOFTWARE PRODUCT

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

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

5. **GRANT OF LICENSE AND RESTRICTIONS**

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

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

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

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

6. **DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS**

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

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

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

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

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

7. **ALL RESERVED**

All rights not expressly granted herein are reserved by Spectra.

8. TERM

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

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

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

9. INTELLECTUAL PROPERTY RIGHTS

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

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

10. U.S. GOVERNMENT END USERS

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

11. EXPORT LAW ASSURANCES

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

12. DISCLAIMER OF WARRANTIES

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

13. LIMITATION OF LIABILITY

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

14. CONTROLLING LAW AND SEVERABILITY

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

Contacting Spectra Logic

To Obtain General Information

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

United States Headquarters

Spectra Logic Corporation
6285 Lookout Road
Boulder, CO 80301
USA
Phone: 1.800.833.1132 or 1.303.449.6400
International: 1.303.449.6400
Fax: 1.303.939.8844

European Office

Spectra Logic Europe Ltd.
329 Doncastle Road
Bracknell
Berks, RG12 8PE
United Kingdom
Phone: 44 (0) 870.112.2150
Fax: 44 (0) 870.112.2175

Spectra Logic Technical Support

Technical Support Portal: **support.spectralogic.com**

United States and Canada
Phone:
Toll free US and Canada: 1.800.227.4637
International: 1.303.449.0160

Europe, Middle East, Africa
Phone: 44 (0) 870.112.2185
Deutsch Sprechende Kunden
Phone: 49 (0) 6028.9796.507
Email: spectralogic@stortrec.de

Mexico, Central and South America, Asia, Australia, and New Zealand
Phone: 1.303.449.0160

Spectra Logic Sales

Website: **www.spectralogic.com/shop**

United States and Canada
Phone: 1.800.833.1132 or 1.303.449.6400
Fax: 1.303.939.8844
Email: sales@spectralogic.com

Europe
Phone: 44 (0) 870.112.2150
Fax: 44 (0) 870.112.2175
Email: eurosales@spectralogic.com

To Obtain Documentation

Spectra Logic Website: **support.spectralogic.com/documentation**

Contents

About This Guide 12

Chapter 1 – Encryption Overview and Strategies 15

Chapter 2 – Using Spectra SKLM Encryption Key Management 35

Chapter 3 – Using KMIP Encryption

About This Guide

This guide contains information about Spectra® SKLM encryption key management, KMIP encryption key management, and BlueScale® Encryption key management for Spectra Tape Libraries.

Spectra SKLM Encryption Key Management

- Requires a purchased option key to activate, which enables library access to the Spectra SKLM server. See Using Spectra SKLM Encryption Key Management on page 35 for more information.

KMIP Encryption Key Management

- Requires a purchased option key to activate, which enables library access to a KMIP server. See Using KMIP Encryption Key Management on page 44 for more information.

BlueScale Encryption Key Management

- **Standard Edition** — Included as a standard feature of the BlueScale software. See Using BlueScale Encryption Standard Edition on page 61 for more information.
- **Professional Edition** — Requires a purchased option key to activate and provides additional security and flexibility features. See Using BlueScale Encryption Professional Edition on page 80 for more information.

Notes:

- The *Spectra T50e Library User Guide* contains the instructions for using encryption on the T50e library.
- The *Spectra Stack User Guide* contains the instructions for using encryption on the Stack library.

Intended Audience

This guide is intended for data center administrators and operators who maintain and operate backup systems. This guide assumes that you are familiar with data backup and data protection strategies.

Related Information

Additional Publications

For detailed information on the configuration and use of the library, see the Spectra Logic publications specific to your library.

- The library's user guide describes the configuration and use of the library, including specifications and troubleshooting information. The most up-to-date versions of all library documentation are available on Spectra Logic's website at support.spectralogic.com/documentation.
- The library's release notes provide the most up-to-date information about the BlueScale software as well as the library, drives, and media. Release Notes can be accessed after logging into your Support portal account at http://support.spectralogic.com.

Spectra SKLM Server

For additional information that can assist you during the installation and configuration of your server, see the following website: *IBM Security Key Lifecycle Manager welcome page*.

KMIP

See the documentation specific to your server.

LTO Ultrium Tape Drives

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

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

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

- *IBM TotalStorage LTO Ultrium Tape Drive: SCSI Reference* (LTO-1 through LTO-4)
- *IBM TotalStorage LTO Ultrium Tape Drive: SCSI Reference* (LTO-5 through LTO-7)

For drive-specific information, search for the product name (for example, LTO 5) on the documentation page on the IBM website. You can also search the IBM Support Portal at: http://www-947.ibm.com/support/entry/portal/Documentation.

TS11xx Technology Drives

The following documents provide information that is applicable to TS11xx technology drives.

- *IBM System Storage Tape Drive 3592 SCSI Reference*
- *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.

BlueScale User Interface Screens

The BlueScale 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.

Typographical Conventions

This document uses the following conventions to highlight important information:

Note: Read notes for additional information or suggestions about the current topic.

Important Read text marked by the "Important" icon for information to help you complete a procedure or avoid extra steps.

Caution Read text marked by the "Caution" icon for information you must know to avoid damaging the library, the tape drives, or losing data.

WARNING Read text marked by the "Warning" icon for information you must know to avoid personal injury.

WARNUNG Lesen Sie markierten Text durch die "Warnung"-Symbol für die Informationen, die Sie kennen müssen, um Personenschäden zu vermeiden.

This document uses an arrow (⇢) to describe a series of menu selections. For example:

Select **Configuration** ⇢ **Partitions** ⇢ **New**.

— means —

Select **Configuration**, then select **Partitions**, and then select **New**.

CHAPTER 1

Encryption Overview and Strategies

ENCRYPTION OVERVIEW

Spectra Logic libraries can encrypt data and manage encryption keys, using either the Spectra SKLM key management system, the KMIP management system, or BlueScale Encryption key management. Spectra SKLM and KMIP are stand-alone, centralized key managers, while BlueScale Encryption key management is integrated within, and specific to, each library.

The following table shows the encryption features and functionality provided by Spectra SKLM key management, KMIP key management, and BlueScale Encryption key management.

Feature	Spectra SKLM	KMIP with HPE ESKM	BlueScale
Library Integrated Server			✓
Stand-alone Server	✓	✓	
Supports T50e, T120, T200, T380, T680, T950, TFinity Libraries	✓	✓	✓
Multi-vendor Support (dual vendor shops)	✓	✓	
Graphical User Interface	✓	✓	✓
Command Line Interface	✓	✓	
LTO-4 Drive Support			✓
LTO-5 Drive Support	✓		✓
LTO-6 through LTO-9 Drive Support	✓	✓	✓
TS11xx Technology Drive Support (Tfinity, T950, T380)	✓	✓	✓
Spectra Stack		✓	✓
Multi-library/ Multi-site Support	✓	✓	
AES-256 Bit Encryption	✓	✓	✓
Secure Initialization Mode			✓
Maximum Number of Encryption Keys	1,000,000+	1,000,000+	30
MLM PostScan Media Verification			✓
Key per Tape	✓	✓	
M-of-N Key Shares			✓
Symmetric Shares	✓	✓	✓
Asymmetric Shares	✓	✓	
Role-based Access Control	✓	✓	✓
Key Grouping	✓	✓	
Device Grouping	✓	✓	
Key Group and Rotation Policies	✓	✓	
Key Lifecyle Status	✓	✓	
Audit Verified Key Deletion	✓	✓	
Certificates of Authority	✓	✓	
Audit Trail	✓	✓	
FIPS Certification	✓	✓	
IKEv2-SCSI Compliance	✓		
Configuration, Policies, & Keystore Backup	✓	✓	
LDAP Support	✓	✓*	

* Not currently supported by the BlueScale software.

Spectra SKLM Key Management Overview

Spectra Security Key Lifecycle Manager (Spectra SKLM) is a centralized key management system that allows you to manage the lifecycle of the encryption keys and security certificates for your library. Spectra SKLM provides role-based access control, based on user privileges, for tasks that range from creating and assigning encryption keys to the backup and restoration of data.

Spectra SKLM is installed on an external server, which is connected to the library by Ethernet. All administrative activities are performed on the server, including configuration; administration of groups, users, and roles; and management of keys, key groups, and devices. Encryption is performed at the drive level, through encryption-enabled LTO-5 and later generation tape drives and TS11xx technology tape drives.

After Spectra SKLM key management is enabled, the drives in an encryption-enabled partition request a key from the Spectra SKLM server. The server sends the encryption key to the drive, and the drive uses the key to automatically encrypt data as it is written to tape.

Before you configure your library to implement Spectra SKLM key management, there are three required components:

- **Spectra SKLM Encryption-Capable Drives —** Spectra SKLM key management is only compatible with LTO-5 and later generation tape drives and TS11xx technology tape drives.
- **Spectra SKLM Option Key —** Purchase and install the Spectra SKLM option key to activate Spectra SKLM key management. For more information on how to install the option key on your library, see your *Tape Library User Guide*.
- **Spectra SKLM Server —** Install and configure Spectra SKLM on your server. Spectra SKLM is available for either Linux® or Windows® operating systems. For additional information that can assist you during the installation and configuration of your server, see the following website: *IBM Security Key Lifecycle Manager welcome page*.

Notes:

- Spectra SKLM key management is not compatible with KMIP encryption key management or BlueScale Encryption key management. Data encrypted using on type of encryption key management cannot be decrypted using a different type of encryption key management.
- Spectra SKLM encryption is not compatible with PostScan. In the Partition Creation wizard, if PostScan is enabled, Spectra SKLM Encryption is not selectable on the Encryption screen.

KMIP USING HP ESKM

The Key Management Interoperability Protocol (KMIP) using the HP Enterprise Secure Key Manager (ESKM) is a centralized key management system that allows you to manage the lifecycle of the encryption keys and security certificates for your library. The library software uses the HP ESKM server to generate, store, and retrieve security keys used by tape drives for data encryption.

Before you configure your library to implement KMIP key management, there are three required components:

- **KMIP Encryption-capable Drives —** KMIP is only compatible with LTO-6 and later generation tape drives and TS11xx drives.

Important To use KMIP encryption key management the library must use BlueScale12.7.01 or later with LTO drives or BlueScale12.7.02 or later with TS11xx drives. The drives must have the following firmware:

- LTO-6 drives must use firmware version G352 or later
- LTO-7 drives must use firmware version G5S2 or later
- LTO-8 and later generation drives can use any firmware supported by the library
- TS1140 technology drives must use firmware version 3B0E or later
- TS1150 technology drives must use firmware version 4718 or later
- TS1155 technology drives must use firmware version 47A2 or later
- TS1160 technology drives must use firmware version 544F or later

- **KMIP Option Key** — Install the KMIP option key to enable the KMIP feature on the tape library. See your *Tape Library User Guide* for detailed instructions. The tape library must be using BlueScale 12.7.01 or later.
- **KMIP Server —** Install and configure KMIP on your server.

Notes:

- At this time, the library only supports connections to Hewlett Packard Enterprise (HPE) Enterprise Secure Key Manager (ESKM) servers.
- KMIP encryption key management is not compatible with Spectra SKLM or BlueScale encryption key management, because they cannot share encryption keys. Data encrypted using on type of encryption key management cannot be decrypted using a different type of encryption key management.
- KMIP encryption is not compatible with PostScan. In the Partition Creation wizard, if PostScan is enabled, KMIP Encryption is not selectable on the Encryption screen.

BLUESCALE ENCRYPTION KEY MANAGEMENT OVERVIEW

BlueScale Encryption key management is tightly integrated into your Spectra library. Encryption is handled through encryption-enabled LTO-4 and later generation drives or through encryption-enabled F-QIPs, if any are in use. BlueScale Encryption key management is provided through the library's user interface.

Understanding the Components

The BlueScale Encryption key management system contains two major components:

- **The BlueScale Encryption Key management Software —** The key management feature is accessed through the library's user interface, either using the operator panel or a remote connection through the BlueScale web interface. Spectra BlueScale encryption key management is available in Standard and Professional Editions to meet your site security requirements (see Standard Edition vs. Professional Edition on page 20).
- **The Encryption Chip in the LTO-4 or Later Generation Drives or in Encryption-Enabled F-QIPs —** Using encryption-enabled hardware makes encryption extremely fast and places no burden on your network. After encryption is enabled, data is automatically encrypted as it is written to tape.

Notes:

- LTO-3 and earlier generation tape drives do not support drive-based encryption and cannot be used in a partition configured to use drive-based encryption. However, you can use F-QIP-based encryption with these drives.
- Encryption-enabled LTO drives use the same encryption algorithm, ensuring that tapes encrypted by one LTO drive generation can be read by another generation of drive as long as the tape itself is compatible with the drive.
- Libraries without one or more F-QIPs installed can only use drive-based encryption.

- The encryption performed by encryption-enabled LTO drives is not compatible with the encryption performed by an encryption-enabled F-QIP.
  - If encryption-enabled F-QIPs and encryption-enabled drives are both installed and are configured in different partitions, both can be used for encryption.
  - If a single partition includes both an encryption-enabled F-QIP and encryption-enabled LTO drives, Spectra Logic recommends that you choose drive-based encryption for compatibility with libraries without F-QIPs.
  - F-QIPs are no longer available for purchase. If your library does not already contain an encryption-capable F-QIP, you must use drive-based encryption.
- BlueScale Encryption key management is not compatible with Spectra SKLM key management or KMIP encryption key management. Data encrypted using on type of encryption key management cannot be decrypted using a different type of encryption key management.

Standard Edition vs. Professional Edition

To determine a BlueScale Encryption key management strategy appropriate for your site and your data, decide on the security level required for your site, and the amount and kinds of data to encrypt. See Best Practices on page 23 for things to consider when determining your encryption requirements and processes. After you decide on the appropriate security level and whether data sets need to be isolated, you can decide which edition of BlueScale Encryption meets your needs.

BlueScale Encryption Standard Edition Standard Edition is included as a standard feature on the library. It is suitable for sites with a primary goal of securing data while it is transported to a remote location and stored there for long-term archival. See Low Security Site Example on page 28 for an example of setting up encryption using BlueScale Encryption Standard Edition.

For information about configuring and using BlueScale Encryption Standard Edition, see Chapter 4 – Using BlueScale Encryption Standard Edition, beginning on page 61.

BlueScale Encryption Professional Edition Professional Edition provides additional choices for defining the level of security you implement in your data center. It is suitable for sites that want the added security of multi-password access to the encryption configuration controls and for importing and exporting encryption keys, and the added flexibility of storing up to 30 encryption keys on the library. See Medium Security Site Example on page 29 and High Security Site Example on page 30 for examples of setting up encryption using BlueScale Encryption Professional Edition.

For information about configuring and using BlueScale Professional Edition, see Chapter 5 – Using BlueScale Encryption Professional Edition, beginning on page 80.

The following table compares the major differences between the Standard and Professional Editions.

Feature	Standard Edition	Professional Edition
Availability	Included as a standard feature on the library.	Requires a purchased option key to activate.
Encryption Login Passwords	Single encryption password accesses all encryption features.	Choice of using one or three passwords to access all encryption features. Using the three-password option requires the following: ▪ Three unique encryption passwords must be configured. ▪ Any one of the three passwords must be entered to enable encryption when the library is in Secure Initialization mode. ▪ Any one of the three passwords must be entered to access encryption key management and configuration options, excluding key import and export. ▪ Two of the three passwords must be entered to import and export keys.
Keys (Data Set Isolation)	▪ Single encryption key stored on the library at a time. ▪ The same key is used for all partitions configured to use encryption.	▪ Up to 30 encryption keys stored on the library. ▪ Separate encryption keys can be assigned to each storage partition to isolate data sets.
Key Export and Import	A single password is used when exporting and importing the encryption key. The encryption key is exported in a single file.	Choice of using one or M-of-N shares with multiple passwords to export and import keys. With the M-of-N shares option, a single file of encrypted key data is split into multiple parts, or shares (N), and some specified subset (M) is required to import the file containing the key data.
Compression	Drive-based compression only.	Drive- or F-QIP-based compression.
Compatibility between Software Editions	Data encrypted using either software edition (Standard or Professional) can be decrypted by a library running the other edition as long as the key used to encrypt the data is present on the library attempting to decrypt the data.	

Best Practices

To effectively use encryption and to ensure data security, create an encryption strategy and back it up with the appropriate staff and custom strategies based on your security requirements.

People

Identify the key people who are responsible for managing the encryption of data written to tape.

Superuser One or more people with superuser privileges on the library. Only a superuser can access and configure the encryption features. See "User Security" in the *User Guide* for your library for information about the three types of user groups and the privileges for each user group.

Encryption Password Holder One or more superusers with the library's encryption password(s).

When determining the number of superusers and encryption password holders, balance the needs for security and availability for the encrypted data. It may be wise for more than a single user to be familiar with passwords, depending on the size of your organization, so that if one person is not available, another can take over.

Processes

Consider the following when establishing your encryption procedures:

Startup Security

- Develop procedures for tracking user names and passwords. Make sure only the authorized users know the encryption passwords, and that the passwords themselves are secure. Refer to Passwords and Other Identifiers on page 26 for more information on setting up passwords.
- Optionally, identify a primary and secondary encryption team, to create redundancy in your encryption strategy. Although that means the information required to decrypt data is spread across more people, it also means that restoration of encrypted data may be much easier, and creates additional data protection given the extra layer of coverage; for example, if a user leaves, you are not left with inaccessible data.

- Determine the level of security to use at startup. Both editions of BlueScale encryption permit a standard mode and a secure initialization mode. In standard mode, data is encrypted and restored as soon as the library is started with no further action required. In secure initialization mode, the partitions configured to use encryption are not accessible for backup or restore operations until a user with superuser privileges logs into the library and enters the encryption password. Spectra SKLM does not use the secure initialization mode.

Data to Encrypt

- Decide whether to encrypt all data or a subset. If all of the site's data is to be encrypted on backup, then a single partition could be sufficient. If, however, you are backing up some data without encryption you need to create a partition dedicated to encrypted data, and another for non-encrypted data.
- Determine whether the encrypted data can be grouped together or if it must be isolated into sets. If sets of encrypted data need to be isolated from each other, create several encrypted storage partitions, each using a different encryption key. For example, your site may store financial data as one set and consumer identity information as a separate set.

BlueScale Encryption Key Protection

BlueScale Encryption uses AES-256 encryption, which is a symmetric, private key encryption method. BlueScale Encryption identifies each key by the moniker (nickname) used to generate the key; the key itself is never displayed. In addition, keys are encrypted before they are exported and the file containing the key is password-protected.

Best practices dictate that you make copies of the key immediately following the key's creation. To ensure security, make sure that you track each copy of an encryption key.

- Decide on the number of copies to make of each key and keep a record of each copy's location. Consider storing multiple copies of keys, that you then track carefully, storing the copies in separate places and away from the data encrypted using those keys.

⚠ **Caution** As a matter of best practice, Spectra Logic recommends exporting encryption keys to a USB device instead of using email.

Although emailing encryption keys is supported by the library, using email presents security issues, including the following:

- Copies of encryption keys may be left on the email servers used for sending and receiving email and are thus subject to compromise.
- The difficulty in verifying where all the copies of emailed encryption keys may be located can make security audits more challenging.

- Establish a key rotation plan that specifies how often to create and use new keys. The rotation plan may be a simple schedule such as changing keys once every six months, and destroying the keys only after the last set of data encrypted using that key is overwritten or destroyed.

  Note: BlueScale Encryption Standard Edition stores one key on the library at a time; you must delete the key currently on the library before you can create or import another key, which can be very disruptive. Professional Edition permits multiple decryption keys for a partition.

- Establish a procedure for tracking keys. Make sure you track the information required to access and identify keys, along with the location of stored data that uses each encryption key. Make sure this information is not stored with the encrypted data. Keep it on a system or in an archive that is not available on a network. For additional security, encrypt this information as well.
- Before you delete a key from the library, make sure that at least one copy is exported and stored securely. It is important to make sure that at least one copy of each key is secure and readable (that is, uncorrupted), to ensure that you can restore your data.

  Keeping a copy of an exported key is essential; after a key is deleted from the library, it is not recoverable. Once the key is gone, the data is inaccessible; for legal and practical purposes the data is typically considered to be deleted.

Process Testing and Exception Handling

- Run drills to confirm that your data is being encrypted properly, that keys are stored properly, and that you can recover your data. Make sure that these drills are included with your overall organizational security strategy.
- Create procedures to handle encrypted data that is, or might be, compromised. Make sure you can identify the data associated with any compromised key or keys. You may want to take all compromised data and decrypt it and then re-encrypt it and store it in an alternate location to minimize the potential for unauthorized access. You also need to investigate the incident involving compromised data and take appropriate actions if identity-related data was exposed.

Special Considerations When Using BlueScale Encryption Professional Edition

- Drive-based encryption only allows one encryption key per cartridge, regardless of the number of keys stored on the library.
- To simplify data restoration in case of disaster recovery and to achieve business continuity goals, make sure that critically important data is stored on a separate, well-identified cartridge and that only one key is used for encrypting all of the data on the cartridge.
- You may want to take advantage of the M-of-N shares option. This option lets you split an exported encryption key into multiple files, or shares, each stored on a separate USB device or emailed to separate mail recipients. Some specified subset of the shares is required to import the encryption key into the library. Splitting an exported key into multiple shares further protects data from unauthorized access.

  For example, if you choose the 2-of-3 shares option, the exported encryption key is split into three shares (N). In order to import the encryption key into the library, two of the shares (M), each on a separate USB device, must be present.

Passwords and Other Identifiers

BlueScale Encryption requires you to supply passwords and monikers (key names) when configuring and using the encryption feature. Your site may want to consider implementing specific rules that govern how these are created.

Superuser Login/Encryption Passwords BlueScale encryption requires a separate password from the one used to log into the library in order to access the library's encryption features. This password must be entered after a user with superuser privileges logs into the library.

If you are using Professional Edition, you may optionally set three separate encryption passwords. If you choose to use this option, two of the three encryption passwords must be entered in order to import BlueScale encryption keys into the library or export them from the library.

The following passwords are required with both editions of BlueScale Encryption:

- **Superuser Password—**Only a user logged into the library with superuser privileges can access the Encryption User Login screen.
- **Encryption Password —** Lets you access encryption features. This password must be entered after the superuser logs in.

Password(s) for Key Import and Export Passwords are also used to encrypt keys for export and when importing previously exported keys. Your site may consider whether to create different rules for these passwords, such as requiring that these passwords are longer than the encryption access password(s), and therefore more secure. Optionally, in Professional Edition, you can require two different passwords in order to import and export keys.

Monikers A moniker is an alphanumeric identifier that is tied to the never-revealed true key value, which is a 256-bit encryption key. The library uses monikers to generate unique encryption keys. The library displays the moniker, not the encryption key itself, whenever it references the encryption key. The actual value of an encryption key is **never** displayed. The moniker helps to protect data encrypted using the key by eliminating the need to display or type the actual key value.

Your site may want to create rules governing naming conventions for key monikers to ensure that each key is unique.

Recommended Make a habit of using a single case (all upper or all lower) for monikers. After the encryption key is created and exported, the library ignores the case used in the moniker.

For example, the library interprets Spectra1, spectra1, and SPECTRA1 as the same moniker when importing a key. However, the key generated by each variation is unique.

⚠ **Caution** If you create two monikers that are identical except for case, you may not be able to retrieve your data after importing a key created using a different variation of the moniker.

Password and Moniker Standards Create standards to govern passwords and moniker names based on your site's security requirements. For example, if your site requires a high level of security for access to encryption partitions, your passwords and monikers may need to incorporate some combination of the following requirements:

- Use a minimum number of characters.
- Use both alphabetic and numeric characters.
- Use both uppercase and lowercase letters for passwords.
- Do not use words found in a dictionary.
- Change the passwords at regularly scheduled intervals.

Site Security

The following sections provide examples of different security scenarios.

Low Security Site Example

The following table describes the security considerations and the suggested encryption configuration for a small company with 75 employees.

Security Consideration	Strategy
Security goals	Protecting company from legal liability associated with unauthorized access to data stored on tape, both onsite and offsite, including transport to the offsite location.
Encryption principals	IT administrator, company president, corporate legal counsel.
Data to encrypt	Financial and consumer identity data.
Level of security to implement	BlueScale Standard Edition: single key per library is sufficient. Standard initialization mode: encryption partitions are enabled at start-up.
Data sets requiring isolation	None. A single partition for encrypted data is sufficient.
Key escrow method	Staff at company escrows keys at a site remote from the data storage location.
Copies of each key to store and their locations	Keep three copies of each key: one with the senior IT administrator, one with the company president, one in a corporate safety deposit box.
Key rotation plan	Create a new key every six months.
Tracking key monikers and passwords	On a non-networked computer that supports encryption, create one or more charts or lists with this data, including key monikers, dates used, encryption and superuser passwords, and passwords used to encrypt exported keys. For additional security, you may want to avoid tracking the relationship between monikers and the encrypted cartridges. The library prompts for the required moniker when you restore encrypted data from a cartridge.
Multiple encryption teams (optional)	Configure a separate set of users who are responsible for managing encrypted data. These users may be the same as those identified as the encryption principals.
Decrypt and restore encrypted data	Regularly review data encryption and decryption procedures to make sure that backups and restores are working properly. Run tests to ensure that encrypted data can be decrypted and restored when needed.
Passwords	▪ Require passwords with a minimum of 12 characters, including at least one number and one letter, to access the encryption features. ▪ Require passwords with a minimum of 30 characters, including at least one number and one letter, to export and import encryption keys.

Medium Security Site Example

The following table describes the security considerations and the suggested encryption configuration for a medium-sized organization with 250 employees.

Security Considerations	Strategy
Security goals	Protecting company from legal liability associated with unauthorized access to data stored on tape onsite and offsite, including transport to the offsite location.
Encryption principals	IT senior staff, chief operating officer.
Data to encrypt	Intellectual property, financial, customer, and inventory data.
Level of security to implement	▪ BlueScale Professional Edition, with multiple keys ▪ Standard initialization mode: encryption partitions are enabled at start-up ▪ Multi-user mode, with three encryption passwords
Data sets requiring isolation from other encrypted data	Separate partitions and keys for these data sets: financial data, inventory data, customer data, and intellectual property data. With this requirement, the site must use a minimum of four encryption-enabled partitions, along with partition(s) for non-encrypted data.
Key escrow method	Store key copies with corporate legal counsel and a paid, trusted, third-party escrow service.
Number of copies of each key to store, and locations	Keep three copies of each key: store one with corporate legal counsel, two with the key escrow service.
Key rotation plan	Create a new key every quarter for each partition dedicated to encryption.
Tracking key monikers, exported key passwords, and password to permit access to encryption features	Send to key escrow service an encrypted document that includes the password used to access encryption features, superuser password, and all passwords necessary to import encryption keys. This file cannot be created or stored on a networked computer. Delete the file from the computer after the document or file is transmitted securely to the key escrow service.
Multiple encryption teams (optional)	Three IT administrators, along with the senior IT admin and the COO.
Schedule and run drills	Annual evaluation and review, along with wider corporate security plan.
Passwords	▪ Passwords to access encryption features: minimum of 12 characters, including at least one number and one letter ▪ Password to export and import encryption keys: minimum of 30 characters, including at least one number and one letter

High Security Site Example

The following table describes the security considerations and the suggested encryption configuration for an enterprise organization.

Security Considerations	Strategy
Security goals	Protecting all stored data.
Encryption principals	IT senior staff, chief operating officer, chief security officer, chief technology officer.
Data to encrypt	All.
Level of security to implement	▪ BlueScale Professional Edition, with multiple keys ▪ Secure Initialization Mode: After the library power is turned on, the encryption user must enter the password to enable partitions dedicated to encryption ▪ Multi-user mode, with three encryption passwords
Data sets requiring isolation	Each data set is separately keyed, as defined by the department generating data.
Key escrow method	Store key copies with two remote corporate legal counsel offices and also with a paid, trusted third-party escrow service.
Copies of each key to store, and the stored key locations	Keep three copies of each key: store one at the main office of corporate legal counsel, two with the key escrow service.
Key rotation plan	Create a new key every month for each partition dedicated to encryption.
Tracking key monikers and passwords	Send to the key escrow service an encrypted file with encryption access passwords and superuser passwords. Send to corporate legal office a list of passwords used to export keys. Files with this data cannot be created or stored on a networked computer; delete file or files from the computer once data is transmitted securely.
Multiple encryption teams (optional)	Senior IT admin, chief operating officer, chief security officer, chief technology officer.
Schedule and run drills	Quarterly evaluation and review, in conjunction with wider corporate security plan.
Passwords	▪ Passwords to access encryption features: minimum of 15 characters, including at least one number and one letter ▪ Password to export and import encryption keys: minimum of 40 characters, including at least one number and one letter

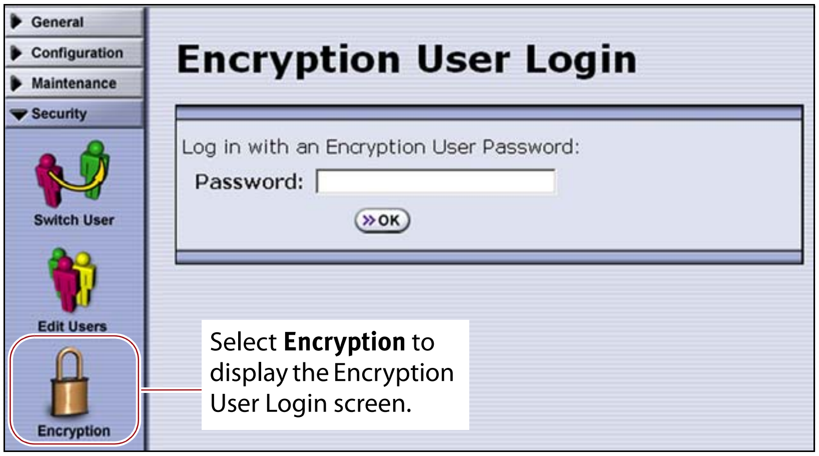
Accessing the Encryption Feature

Use the following steps to access the encryption feature to configure the library to use either Spectra SKLM or BlueScale Encryption Key Management.

Log Into the Encryption Feature

User Privilege Requirements Only users with superuser privileges can access and use the encryption feature on the library.

1. Log into the library as a user with superuser privileges. Select **Security → Encryption**. The Encryption User Login screen displays.



Encryption User Login

Log in with an Encryption User Password:

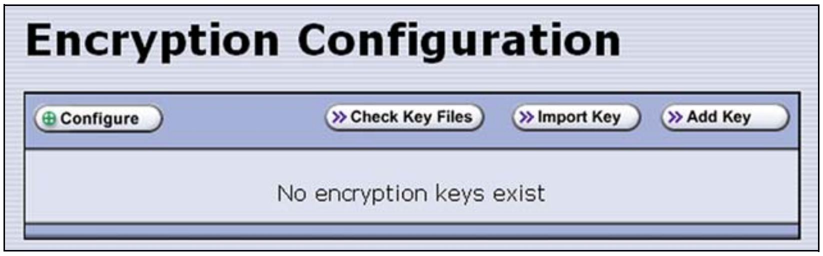
Password:

Select **Encryption** to display the Encryption User Login screen.

Figure 1 Enter the encryption user password to access the encryption feature.

2. Enter the encryption password (if one is set) and then click **OK**. The Encryption Configuration screen displays the moniker for any BlueScale encryption keys currently stored in the library.

Notes:
- The default encryption password is blank.
- If you are configuring encryption for the first time or you are using Spectra SKLM key management, no encryption key monikers display.



Encryption Configuration

No encryption keys exist

Figure 2 The Encryption Configuration screen displays after you log into the encryption feature.

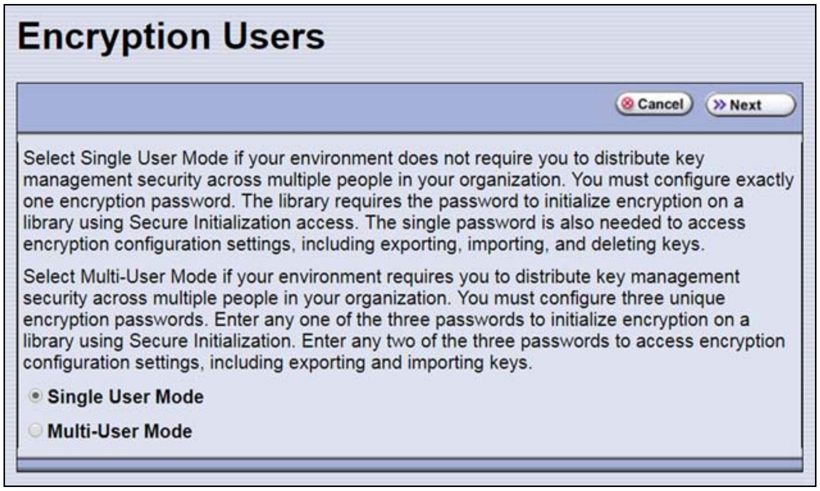
Configure the User Mode (BlueScale Encryption Professional Only)

If you are configuring BlueScale Encryption Professional Edition, use this section to set the encryption user mode.

If you are configuring Spectra SKLM or BlueScale Encryption Standard Edition, the User Mode option does not apply.

- If you are configuring Spectra SKLM, proceed to Configure the Password on page 34.
- If you are configuring BlueScale Encryption Standard Edition proceed to Configure Secure Initialization Mode (BlueScale Encryption Only) on page 33.

1. From the Encryption Configuration screen, click **Configure.** The Encryption Users screen displays.



Encryption Users

Select Single User Mode if your environment does not require you to distribute key management security across multiple people in your organization. You must configure exactly one encryption password. The library requires the password to initialize encryption on a library using Secure Initialization access. The single password is also needed to access encryption configuration settings, including exporting, importing, and deleting keys.

Select Multi-User Mode if your environment requires you to distribute key management security across multiple people in your organization. You must configure three unique encryption passwords. Enter any one of the three passwords to initialize encryption on a library using Secure Initialization. Enter any two of the three passwords to access encryption configuration settings, including exporting and importing keys.

● Single User Mode

○ Multi-User Mode

Figure 3 Select **Single User Mode** or **Multi-User Mode**.

2. Select either **Single User Mode** or **Multi-User Mode**.

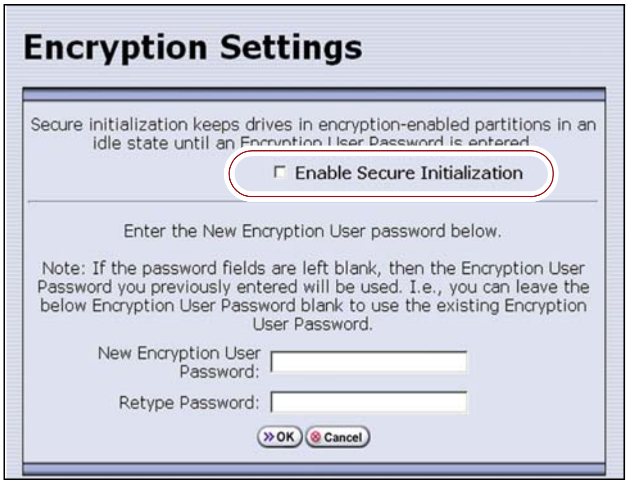
User Mode	Description
Single User Mode	Only one encryption password can be configured and only one is required to access all encryption features.
Multi-User Mode	Three unique encryption passwords must be configured. After you set up the three passwords, they are used as follows: ▪ Enter any one of the three to initialize encryption on a library using Secure Initialization mode, to add a new key, or to delete a key. ▪ Enter any two of the three passwords, when prompted, to access configuration settings and export or import encryption key features.

Configure Secure Initialization Mode (BlueScale Encryption Only)

If you are configuring Spectra SKLM, the Secure Initialization mode option does not apply. Proceed to Configure the Password on page 34.

If you are configuring BlueScale Encryption key management, use the following steps to set the Secure Initialization mode.

1. Click **Next**. The Encryption Settings screen displays.



Encryption Settings

Secure initialization keeps drives in encryption-enabled partitions in an idle state until an Encryption User Password is entered

☐ Enable Secure Initialization

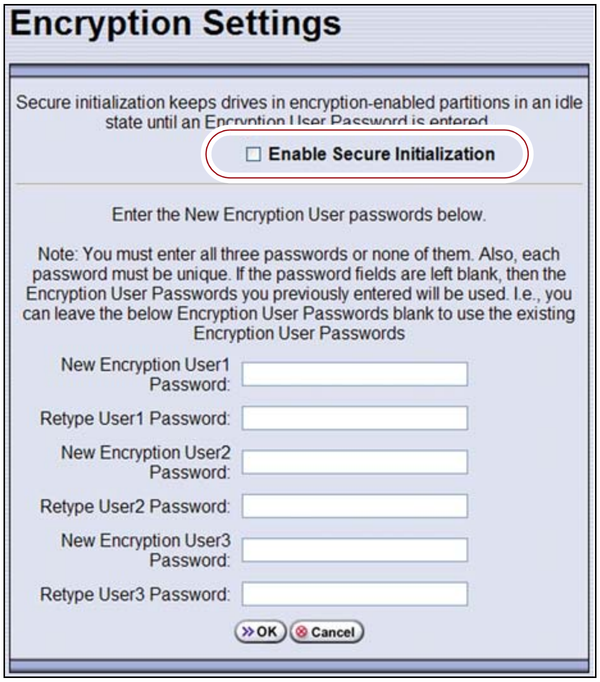
Enter the New Encryption User password below.

Note: If the password fields are left blank, then the Encryption User Password you previously entered will be used. I.e., you can leave the below Encryption User Password blank to use the existing Encryption User Password.

New Encryption User Password:

Retype Password:

Figure 4 Select the desired initialization behavior (BlueScale Standard Edition or Professional Edition Single User mode).



Encryption Settings

Secure initialization keeps drives in encryption-enabled partitions in an idle state until an Encryption User Password is entered

☐ Enable Secure Initialization

Enter the New Encryption User passwords below.

Note: You must enter all three passwords or none of them. Also, each password must be unique. If the password fields are left blank, then the Encryption User Passwords you previously entered will be used. I.e., you can leave the below Encryption User Passwords blank to use the existing Encryption User Passwords

New Encryption User1 Password:

Retype User1 Password:

New Encryption User2 Password:

Retype User2 Password:

New Encryption User3 Password:

Retype User3 Password:

Figure 5 Select the desired initialization behavior (BlueScale Professional Edition Multi-User mode).

2. Select or clear the **Enable Secure Initialization** check box to configure the desired initialization mode used.

Initialization Mode	Description
Standard mode	The partitions configured to use encryption are accessible to the hosts as soon as the library completes its initialization. Data can be backed up to partitions that support encryption without entering an encryption password. To use Standard Mode, make sure that the **Enable Secure Initialization** check box is *cleared*. Standard mode is the default setting.

Initialization Mode	Description
Secure initialization mode	The partitions configured to use BlueScale Encryption key management are not accessible to the hosts until the encryption password is entered through the Encryption User Login screen. Until that time, any backup or restore operations using partitions that use encryption cannot run. To initialize the encryption partitions and make them available for use, each time the library is initialized, a user with superuser privileges must first log into the library and then log into the encryption feature using the encryption password. To enable Secure Initialization mode, make sure that the **Enable Secure Initialization** check box is *selected*. Secure Initialization mode becomes active after the library is power-cycled.

Configure the Password

1. If you want to change the current encryption user password(s), enter the new password(s) in the **New Encryption User Password** field(s) using any combination of the numbers **0–9**, lower and upper case alphabetic characters (**a–z** and **A–Z**), and the at symbol (@), dash (–), underscore (_), and period (**.**) characters.

⚠ **Caution** The BlueScale encryption user password is separate from the password used to log into the library. Make sure you keep a record of this password. If you lose this password, you cannot configure the encryption settings.

If you are using BlueScale Encryption, you cannot import or export encryption keys that were already assigned and used with encrypted data.

Notes:

- The encryption user password is separate from both the BlueScale login password and the encryption key password you define when you export a BlueScale encryption key (see Export the Encryption Key on page 67).
- Security is greatly enhanced when the user who knows the encryption password is different from the user who performs day-to-day operations such as importing or exporting cartridges.
- If you selected BlueScale Professional edition Multi-User mode, you must enter three unique encryption passwords.

2. Retype each password in the **Retype User Password** field and then click **OK**. The Encryption Configuration screen displays.

CHAPTER 2

Using Spectra SKLM Encryption Key Management

This chapter describes configuring and using Spectra SKLM encryption key management.

- If you are using KMIP Encryption Key Management, see Chapter 3 – Using KMIP Encryption Key Management, beginning on page 44.
- If you are using BlueScale Encryption Key Management — Standard Edition, see Chapter 4 – Using BlueScale Encryption Standard Edition, beginning on page 61.
- If you are using BlueScale Encryption Key Management — Professional Edition, see Chapter 5 – Using BlueScale Encryption Professional Edition, beginning on page 80.

SPECTRA SKLM ENCRYPTION KEY MANAGEMENT

Overview Spectra SKLM Encryption Key Management configuration entails creating an encryption password, configuring one or more Spectra SKLM servers, and designating one or more partitions as encryption-enabled. The encryption password lets a superuser access the library's encryption configuration settings. Encryption administrative activities are performed on the Spectra SKLM server, including configuration; administration of groups, users, and roles; and management of keys, key groups, and devices.

After Spectra SKLM is enabled, the drives in an encryption-enabled partition request a key from the Spectra SKLM server. The server sends the encryption key to the drive, and the drive uses the key to automatically encrypt data as it is written to tape.

Before you configure your library to use Spectra SKLM, make sure you have the following:

- **Spectra SKLM Encryption-capable Drives —** Spectra SKLM is only compatible with LTO-5 and later generation tape drives and TS11xx technology tape drives.
- **Spectra SKLM Option Key —** Install the Spectra SKLM option key. See your *Tape Library User Guide* for detailed instructions.
- **Spectra SKLM Server** — Install and configure Spectra SKLM on your server. Spectra SKLM is available for either Linux or Windows. For additional information that can assist you during the installation and configuration of your server, see the following website: *IBM Security Key Lifecycle Manager welcome page*.
- Spectra SKLM is not compatible with KMIP Encryption Key Management or BlueScale Encryption Key Management, because they cannot share encryption keys. Data encrypted using Spectra SKLM key management cannot be decrypted using KMIP or BlueScale encryption key management, and vice versa.

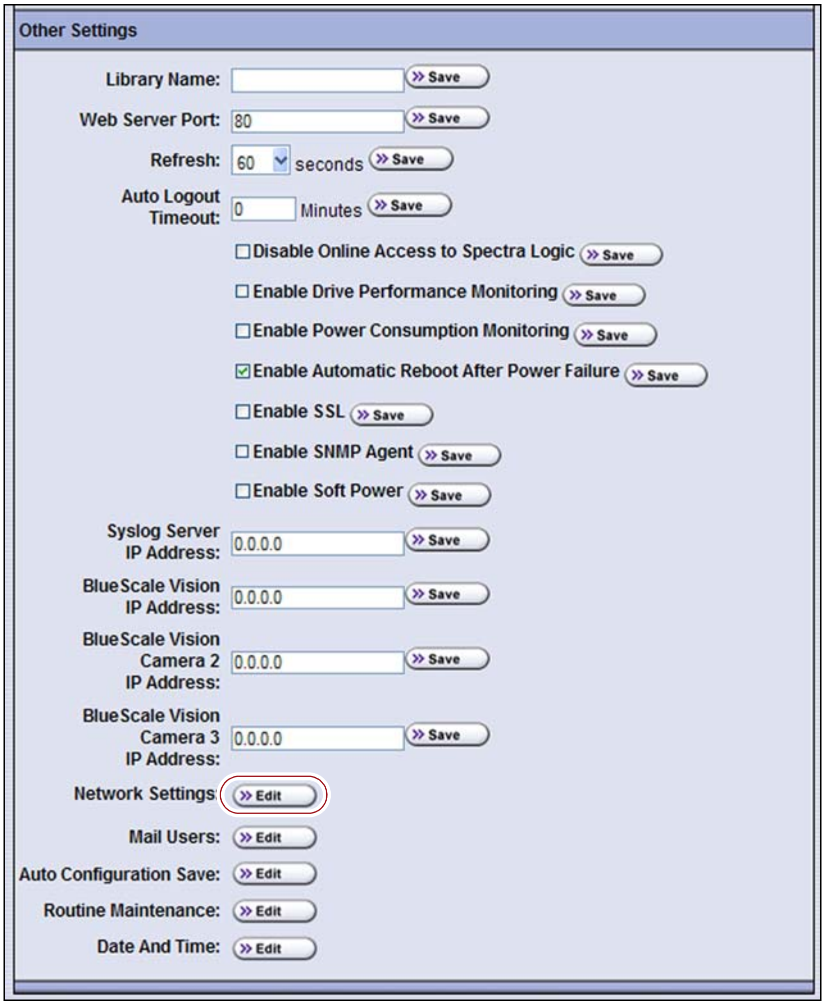
Configure a Spectra SKLM Server

Use the following steps to configure the Spectra SKLM server.

User Privilege Requirements Only users with superuser privileges can configure the encryption features.

1. To configure a Spectra SKLM server, you must enter the IP address or hostname for the server. If you plan to use a hostname, instead of an IP address, you must configure at least one DNS server. If you plan to use an IP address, skip to Step 2 on page 38.

   a. From the toolbar menu, select **Configuration ⇢ System**. The System Setup screen displays.



Other Settings

Library Name:

Web Server Port: 80

Refresh: 60 seconds

Auto Logout Timeout: 0 Minutes

☐ Disable Online Access to Spectra Logic

☐ Enable Drive Performance Monitoring

☐ Enable Power Consumption Monitoring

☑ Enable Automatic Reboot After Power Failure

☐ Enable SSL

☐ Enable SNMP Agent

☐ Enable Soft Power

Syslog Server IP Address: 0.0.0.0

BlueScale Vision IP Address: 0.0.0.0

BlueScale Vision Camera 2 IP Address: 0.0.0.0

BlueScale Vision Camera 3 IP Address: 0.0.0.0

Network Settings:

Mail Users:

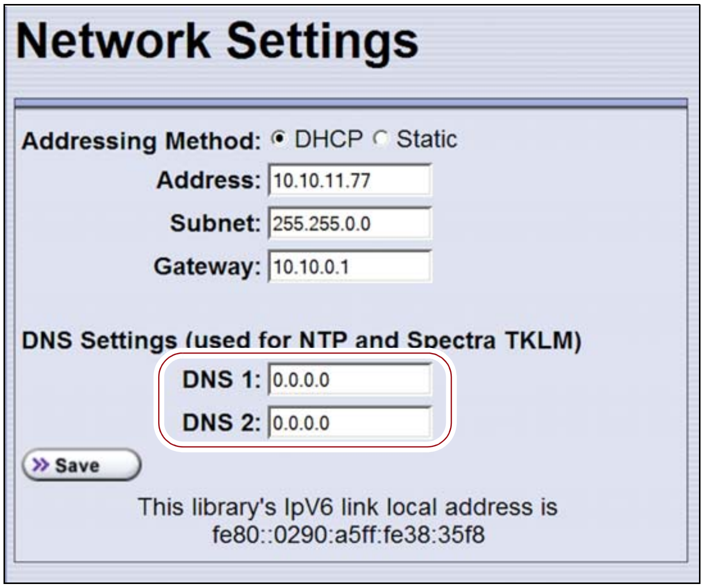
Auto Configuration Save:

Routine Maintenance:

Date And Time:

Figure 6 The Other Settings pane of the System Setup screen.

b. In the Other Settings pane, click **Edit** next to Network Settings. The Network Settings screen displays.



Network Settings

Addressing Method: ● DHCP ○ Static
Address: 10.10.11.77
Subnet: 255.255.0.0
Gateway: 10.10.0.1

DNS Settings (used for NTP and Spectra TKLM)
DNS 1: 0.0.0.0
DNS 2: 0.0.0.0

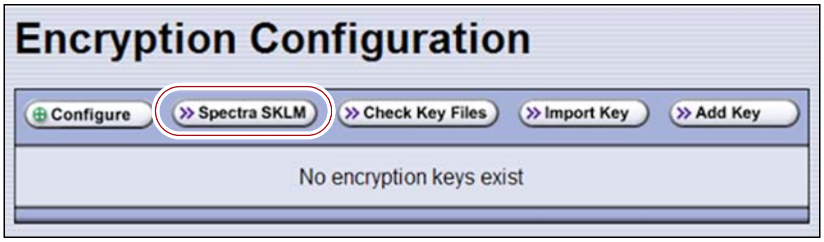
This library's IpV6 link local address is fe80::0290:a5ff:fe38:35f8

Figure 7 The Network Settings screen.

c. Enter an IP address for at least one DNS server, and then click **Save**.

2. Access the encryption feature (see Log Into the Encryption Feature on page 31).

3. On the Encryption Configuration screen, click **Spectra SKLM.** The Spectra SKLM Server Status screen displays.



Encryption Configuration

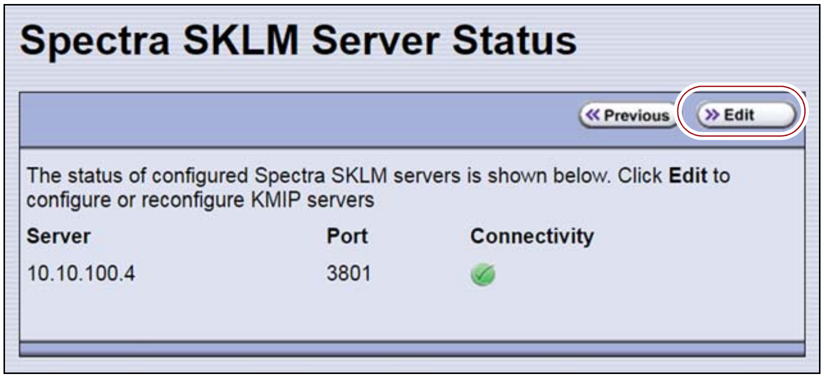
No encryption keys exist

Figure 8 Access the Spectra SKLM Server Status Screen.

4. The Spectra SKLM Server Status screen displays a list of previously configured Spectra SKLM servers (if any). Up to four Spectra SKLM servers are supported; each is listed by its IP address or hostname.

Note: When read or write processes begin, a green check mark appears in the Connectivity column next to servers the library can access. A red **X** in the Connectivity column indicates the library is currently unable to connect to that server.

On the Spectra SKLM Server Status screen, click **Edit** to add or modify Spectra SKLM servers.



Spectra SKLM Server Status

The status of configured Spectra SKLM servers is shown below. Click **Edit** to configure or reconfigure KMIP servers

Server	Port	Connectivity
10.10.100.4	3801	✓

Figure 9 Click **Edit** to add or modify a server.

5. The SKLM Server Configuration screen displays an editable list of configured Spectra SKLM servers (if any). Enter the appropriate information for the server you want to configure.

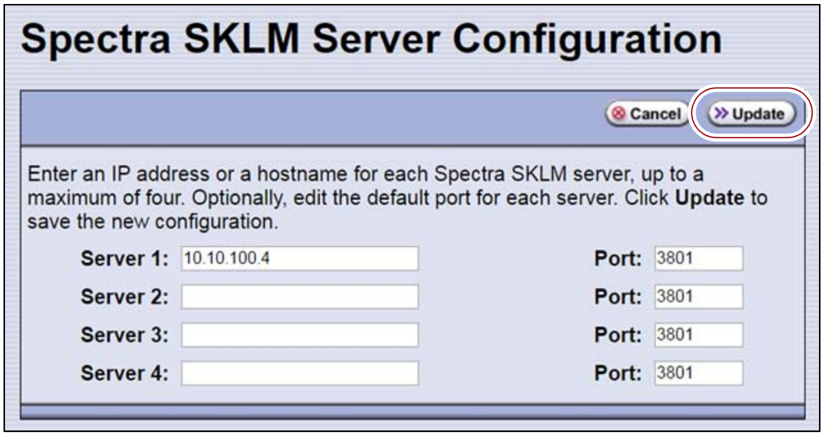
Note: If you want to delete a server, delete its IP address or hostname.

a. Enter the IP address or hostname of the server.

b. If desired, change the port setting. The default port setting is 3801.

Note: When you set up the Spectra SKLM server, you must add a firewall rule to allow connections to this port. Otherwise, the library is not be able to access the server.

c. Click **Update** to save the changes. The library attempts to connect to the server and the Encryption Server Update Result screen displays the success or failure of the Spectra SKLM server configuration.



Spectra SKLM Server Configuration

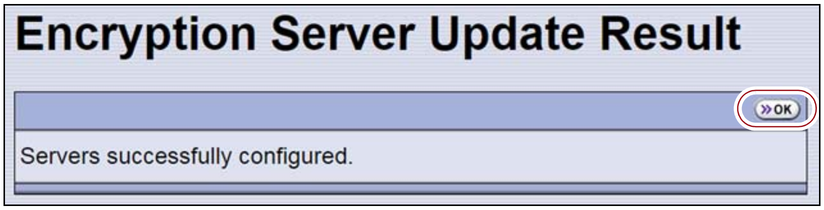
Enter an IP address or a hostname for each Spectra SKLM server, up to a maximum of four. Optionally, edit the default port for each server. Click **Update** to save the new configuration.

Server 1:	10.10.100.4	**Port:**	3801
Server 2:		**Port:**	3801
Server 3:		**Port:**	3801
Server 4:		**Port:**	3801

Figure 10 Click **Update** to save the changes.

6. If the Encryption Server Update Result screen indicates a failure, reenter the information in Step 5 on page 39. Otherwise, click **OK** to return to the KMIP Server Status screen.

Note: The list of servers on the KMIP Server Status screen includes successfully added servers. If the library could not connect to the server or verify it as a KMIP server, it does not appear in the list.



Encryption Server Update Result

Servers successfully configured.

Figure 11 The Encryption Server Update Result screen.

Configuring a Partition to Use a Spectra SKLM Server

Overview After configuring a Spectra SKLM server, you can enable Spectra SKLM Encryption Key Management for one or more partitions.

⚠ **Important** To use Spectra SKLM, LTO-5 drives must be updated to firmware version C7RC, or later. All LTO-6 or later generation or TS11xx technology drive firmware supported for use with the library can be used with Spectra SKLM.

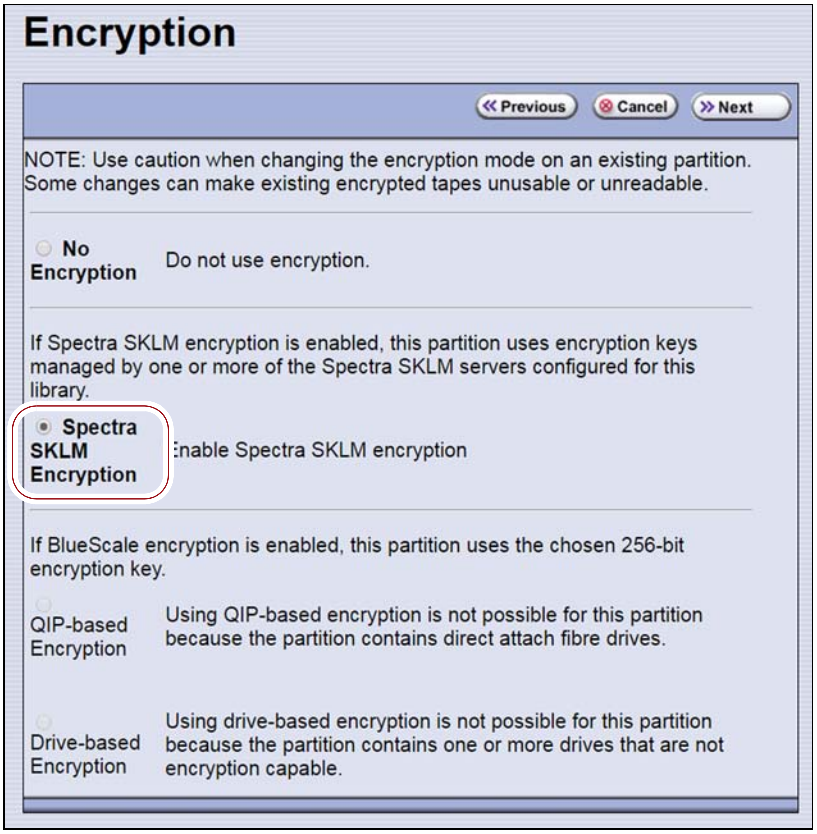
Notes:

- The Encryption screen in the partition wizard lets you enable the encryption features for the partition. Depending on the version of BlueScale software, the Encryption screen does not display, or displays with all options grayed out, unless you are logged into the library as an encryption user and have either created one or more BlueScale encryption keys, or configured a Spectra SKLM or KMIP server. See Configure a Spectra SKLM Server on page 37.
- Spectra SKLM is not compatible with BlueScale Encryption Key Management, because they cannot share encryption keys. Data encrypted using Spectra SKLM cannot be decrypted using BlueScale Encryption Key Management, and vice versa.
- Spectra SKLM is only compatible with LTO-5 and later generation tape drives and TS11xx technology tape drives.

Use the following steps to assign a Spectra SKLM server to the partition:

1. Access the encryption feature (see Log Into the Encryption Feature on page 31).
2. Select **Configuration ⇢ Partitions**. The Shared Library Services screen displays.
3. Click **New** to create a partition, or click **Edit** to modify the settings for an existing partition (see “Creating a Storage Partition” in your *Tape Library User Guide* for more information about creating or editing partitions).

4. Proceed through the partition wizard until you reach the Encryption screen.



NOTE: Use caution when changing the encryption mode on an existing partition. Some changes can make existing encrypted tapes unusable or unreadable.

○ **No Encryption** Do not use encryption.

If Spectra SKLM encryption is enabled, this partition uses encryption keys managed by one or more of the Spectra SKLM servers configured for this library.

● **Spectra SKLM Encryption** Enable Spectra SKLM encryption

If BlueScale encryption is enabled, this partition uses the chosen 256-bit encryption key.

○ QIP-based Encryption Using QIP-based encryption is not possible for this partition because the partition contains direct attach fibre drives.

○ Drive-based Encryption Using drive-based encryption is not possible for this partition because the partition contains one or more drives that are not encryption capable.

Figure 12 The Encryption screen.

5. Choose the type of encryption to use.

Encryption Option	Description
No Encryption	Turns off encryption. All subsequent data written to tapes in this partition is not encrypted. Any tapes previously written using encryption remain encrypted.
Spectra SKLM Encryption	Turns on Spectra SKLM encryption key management for drive-based encryption. **Note:** If PostScan is enabled for the partition, do not select Spectra SKLM Encryption.
BlueScale Encryption	Turns on BlueScale encryption key management for either drive-based or QIP-based encryption. See Chapter 4 – Using BlueScale Encryption Standard Edition, beginning on page 61 or Chapter 5 – Using BlueScale Encryption Professional Edition, beginning on page 80 for more information.

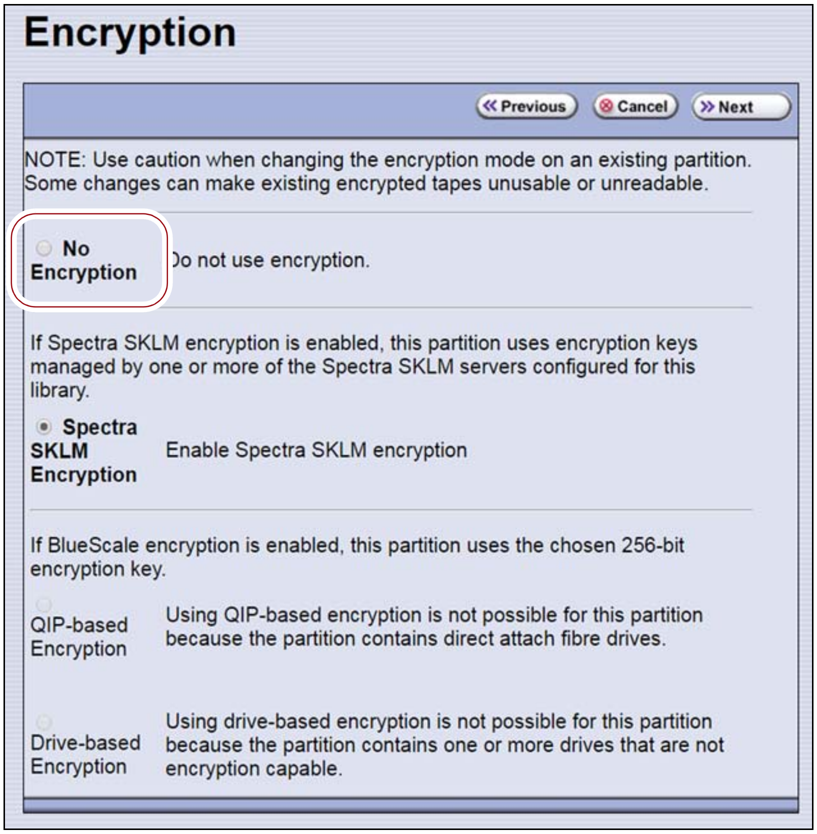
6. Proceed through the remaining partition configuration screens.

7. When you reach the Save Partition screen, click **Save**.

DISABLING ENCRYPTION IN A PARTITION

Use the following steps to disable encryption in a partition.

1. Access the encryption feature (see Log Into the Encryption Feature on page 31).
2. Select **Configuration ···> Partitions**. The Shared Library Services screen displays.
3. Select the partition for which you want to disable encryption. Click **Edit**.
4. Click **Next** to navigate through the partition wizard screens until you reach the Encryption screen.



Encryption

NOTE: Use caution when changing the encryption mode on an existing partition. Some changes can make existing encrypted tapes unusable or unreadable.

○ **No Encryption** Do not use encryption.

If Spectra SKLM encryption is enabled, this partition uses encryption keys managed by one or more of the Spectra SKLM servers configured for this library.

● **Spectra SKLM Encryption** Enable Spectra SKLM encryption

If BlueScale encryption is enabled, this partition uses the chosen 256-bit encryption key.

○ QIP-based Encryption Using QIP-based encryption is not possible for this partition because the partition contains direct attach fibre drives.

○ Drive-based Encryption Using drive-based encryption is not possible for this partition because the partition contains one or more drives that are not encryption capable.

Figure 13 The Encryption screen.

5. Select **No Encryption**.
6. Navigate through the remaining partition configuration screens by clicking **Next**.
7. When you reach the Save Partition screen, click **Save**.

CHAPTER 3

Using KMIP Encryption Key Management

This chapter describes configuring and using KMIP Encryption Key Management.

- If you are using Spectra SKLM Encryption Key Management, see Chapter 2 – Using Spectra SKLM Encryption Key Management, beginning on page 35.
- If you are using BlueScale Encryption Key Management — Standard Edition, see Chapter 4 – Using BlueScale Encryption Standard Edition, beginning on page 61.
- If you are using BlueScale Encryption Key Management — Professional Edition, see Chapter 5 – Using BlueScale Encryption Professional Edition, beginning on page 80.

KMIP Encryption Key Management

Overview Configuration of KMIP encryption key management entails creating a Certificate Signing Request, getting the certificate signed, configuring one or more KMIP servers, adding the new user to the server, importing artifacts from the server, configuring the library to access one or more KMIP servers, and designating one or more library partitions as encryption-enabled. All encryption administrative activities are performed on the KMIP server, including configuration; administration of groups, users, and roles; and management of keys, key groups, and devices.

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.

Before you configure your library to use KMIP encryption key management, make sure you have the following:

- **KMIP Encryption-capable Drives —** KMIP is only compatible with LTO-6 and later generation tape drives and TS11xx drives.

Important To use KMIP encryption key management the library must use BlueScale12.7.01 or later with LTO drives or BlueScale12.7.02 or later with TS11xx drives. The drives must have the following firmware:

- LTO-6 drives must use firmware version G352 or later
- LTO-7 drives must use firmware version G5S2 or later
- LTO-8 and later generation drives can use any firmware supported by the library
- TS1140 technology drives must use firmware version 3B0E or later
- TS1150 technology drives must use firmware version 4718 or later
- TS1155 technology drives must use firmware version 47A2 or later
- TS1160 technology drives must use firmware version 544F or later

- **KMIP Option Key** — Install the KMIP option key to enable the KMIP feature on the tape library. See your *Tape Library User Guide* for detailed instructions. The tape library must be using BlueScale 12.7.01 or later.
- **KMIP Server —** Install and configure KMIP on your server.

Notes:

- At this time, the library only supports connections to Hewlett Packard Enterprise (HPE) Enterprise Secure Key Manager (ESKM) servers.
- KMIP encryption key management is not compatible with Spectra SKLM or BlueScale encryption key management, because they cannot share encryption keys. Data encrypted using KMIP key management cannot be decrypted using Spectra SKLM or BlueScale encryption key management, and vice versa.

CONFIGURE KMIP ENCRYPTION

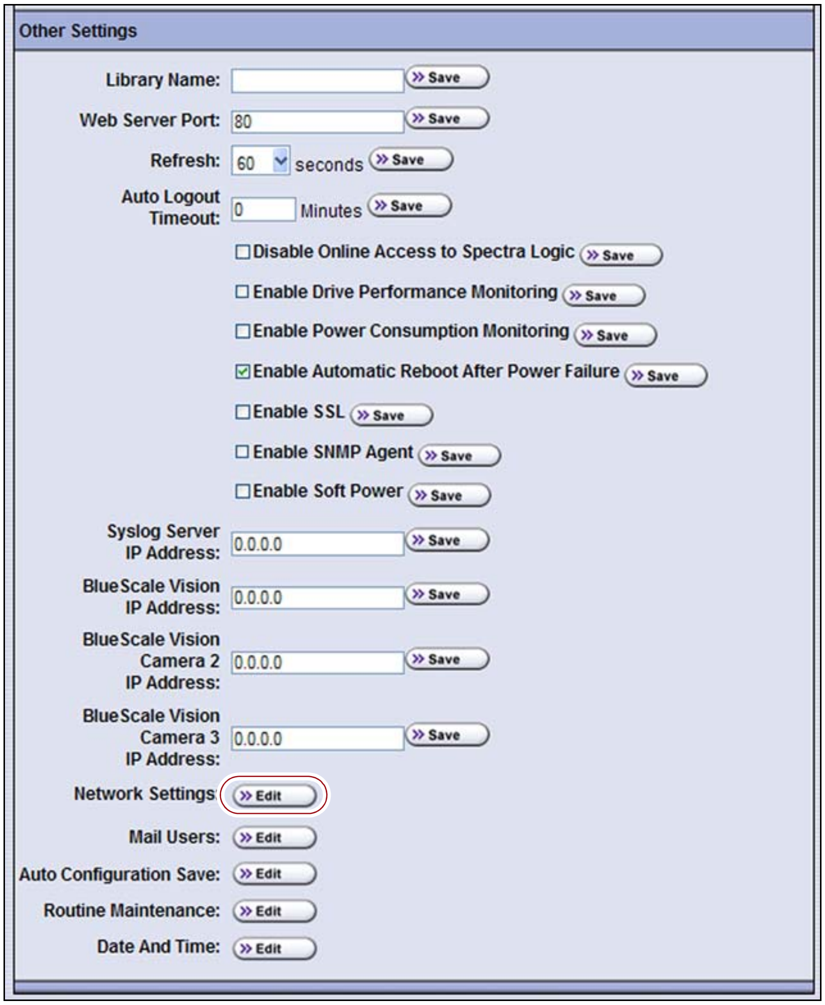
Use the following steps to configure the library to use KMIP encryption.

User Privilege Requirements Only users with superuser privileges can configure the encryption features.

Configure a DNS Server

To configure a KMIP server, you must enter the IP address or hostname for the server. If you plan to use a hostname, instead of an IP address, you must configure at least one DNS server for the library. If you plan to use an IP address, skip to Create a Certificate Signing Request (CSR) on page 47.

1. From the toolbar menu, select **Configuration ⇢ System**. The System Setup screen displays.
2. In the Other Settings pane, click **Edit** next to Network Settings. The Network Settings screen displays.



Other Settings

Library Name:

Web Server Port: 80

Refresh: 60 seconds

Auto Logout Timeout: 0 Minutes

□ Disable Online Access to Spectra Logic

□ Enable Drive Performance Monitoring

□ Enable Power Consumption Monitoring

☑ Enable Automatic Reboot After Power Failure

□ Enable SSL

□ Enable SNMP Agent

□ Enable Soft Power

Syslog Server IP Address: 0.0.0.0

BlueScale Vision IP Address: 0.0.0.0

BlueScale Vision Camera 2 IP Address: 0.0.0.0

BlueScale Vision Camera 3 IP Address: 0.0.0.0

Network Settings

Mail Users:

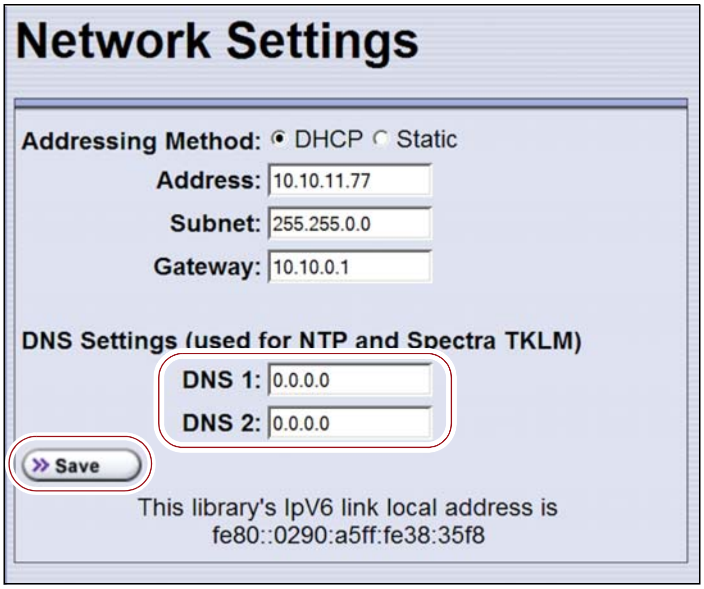
Auto Configuration Save:

Routine Maintenance:

Date And Time:

Figure 14 The Other Settings pane of the System Setup screen.

3. Enter an IP address for at least one DNS server, and then click **Save**.



Network Settings

Addressing Method: ● DHCP ○ Static

Address: 10.10.11.77

Subnet: 255.255.0.0

Gateway: 10.10.0.1

DNS Settings (used for NTP and Spectra TKLM)

DNS 1: 0.0.0.0

DNS 2: 0.0.0.0

This library's IpV6 link local address is fe80::0290:a5ff:fe38:35f8

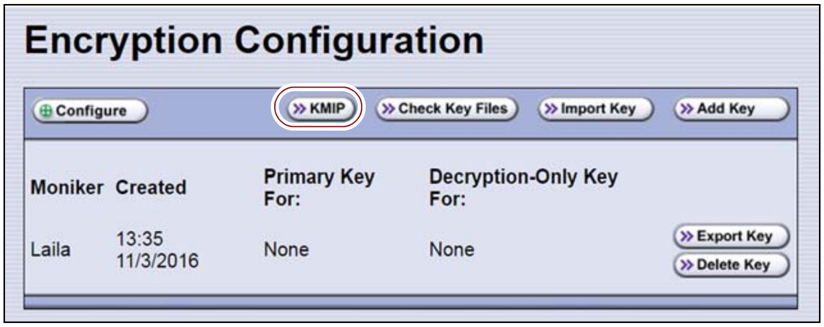
Figure 15 The Network Settings screen.

Create a Certificate Signing Request (CSR)

1. Using RLC, access the encryption feature (see Log Into the Encryption Feature on page 31).

   Note: You are not able to copy the CSR from the front panel, so you must use RLC to create the CSR.

2. On the Encryption Configuration screen, click **KMIP**. The KMIP Configuration screen displays.

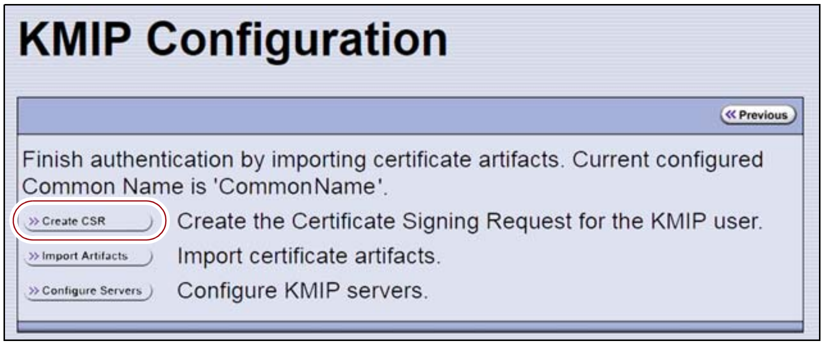


Encryption Configuration

Moniker	Created	Primary Key For:	Decryption-Only Key For:
Laila	13:35 11/3/2016	None	None

Figure 16 Access the KMIP Configuration Screen.

3. Click **Create CSR**. The Certificates Characteristics screen displays.



KMIP Configuration

Finish authentication by importing certificate artifacts. Current configured Common Name is 'CommonName'.

Create the Certificate Signing Request for the KMIP user.

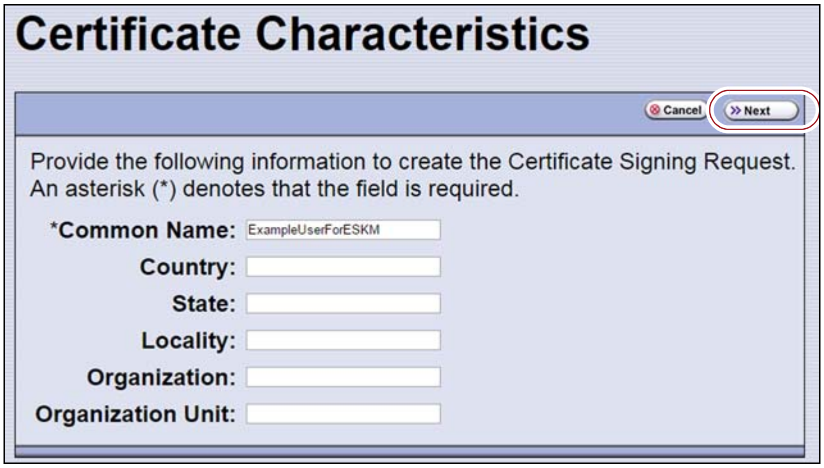
Import certificate artifacts.

Configure KMIP servers.

Figure 17 Click **Create CSR**.

4. On the Certificate Characteristics screen, enter the Common Name.

Notes:
- For HPE ESKM servers, the Common Name becomes the library's username when you register the library as a user.
- The Common Name must have fewer than 65 characters and can contain any combination of the numbers 0-9, lower and upper case alphabetic characters (a-z and A-Z), and the at symbol (@), dash (-), underscore (_), period (.), forward slash (/), and space characters.



Certificate Characteristics

Provide the following information to create the Certificate Signing Request. An asterisk (*) denotes that the field is required.

*Common Name: ExampleUserForESKM

Country:

State:

Locality:

Organization:

Organization Unit:

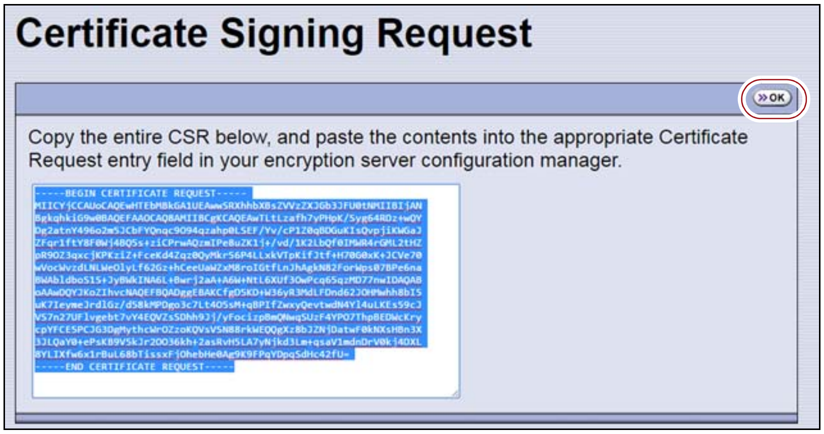
Figure 18 Enter the **Common Name** and click **Next**.

5. If desired, enter the remaining information and click **Next**. The library generates a key pair, and presents the CSR.

Notes:

- Country must either be left blank, or else must contain exactly two characters including any combination of the numbers 0-9, lower and upper case alphabetic characters (a-z and A-Z), the dash (-), underscore (_), period (.), and forward slash (/) characters.
- All other fields must have fewer than 65 characters including any combination of the numbers 0-9, lower and upper case alphabetic characters (a-z and A-Z), and the at symbol (@), dash (-), underscore (_), period (.), forward slash (/), and space characters .

6. Copy all of the CSR text, including the dashes, onto the clipboard or into a file. Click **OK**. The KMIP Configuration screen displays (see Figure 17 on page 48).



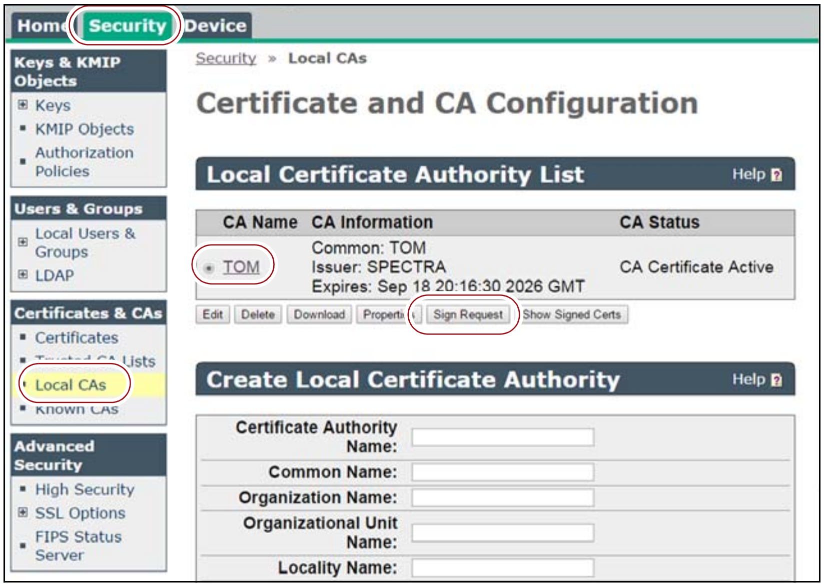
Copy the entire CSR below, and paste the contents into the appropriate Certificate Request entry field in your encryption server configuration manager.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICYjCCAUoCAQEwHTEbMBkGA1UEAwwSRXhhbXBsZVVzZXJGb3JFU0tNMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwTLtLzafh7yPHpK/Syg64RDz+wQY
Dg2atnY496o2m5JCbFYQnqc9O94qzahp0LSEF/Yv/cP1Z0qBDGuKIsQvpjiKWGaJ
ZFqr1ftY8F0Wj4BQ5s+ziCPrwAQzmIPe8uZK1j+/vd/1K2LbQf0IMWR4rGML2tHZ
pR9OZ3qxcjKPKziZ+FceKd4Zqz0QyMkrS6P4LLxkVTpKifJtf+H70G0xK+JCVe70
wVocWvzdLNLWeOlyLf62Gz+hCeeUaWZxM8roIGtfLnJhAgkN82ForWps07BPe6na
BWAbldboS15+JyBWkINA6L+Bwrj2aA+A6W+NtL6XUf3OwPcq65qzMD77nwIDAQAB
oAAwDQYJKoZIhvcNAQEFBQADggEBAKCfgOSKD+W36yR3MdLFDnd62JOHMwhh8bIS
uK7IeymeJrdlGz/d58kMPDgo3c7Lt4O5sM+qBPIfZwxyQevtwdN4Yl4uLKEs59cJ
VS7n27UFlvgebt7vY4EQVZsSDhh9Jj/yFocizp8mQNwqSUzF4YPO7ThpBEDWcKry
cpYFCESPCJG3DgMythcWrOZzoKQVsVSN8BrkWEQQgXz8bJZNjDatwF0kNXsHBn3X
3JLQaY0+ePsKB9V5kJr2OO36kh+2asRvH5LA7yNjkd3Lm+qsaV1mdnDrV0kj4DXL
8YLIXfw6x1rBuL68bTissxFjOhebHe0Ag9K9FPqYDpqSdHc42fU=
-----END CERTIFICATE REQUEST-----
```

Figure 19 Copy the text of the CSR.

Sign the Certificate Request Using HPE ESKM

1. Log into the HPE ESKM server.
2. On the main screen, select the **Security** tab, and then on the left hand menu, select **Local CAs**. The Certificate and CA Configuration screen displays.



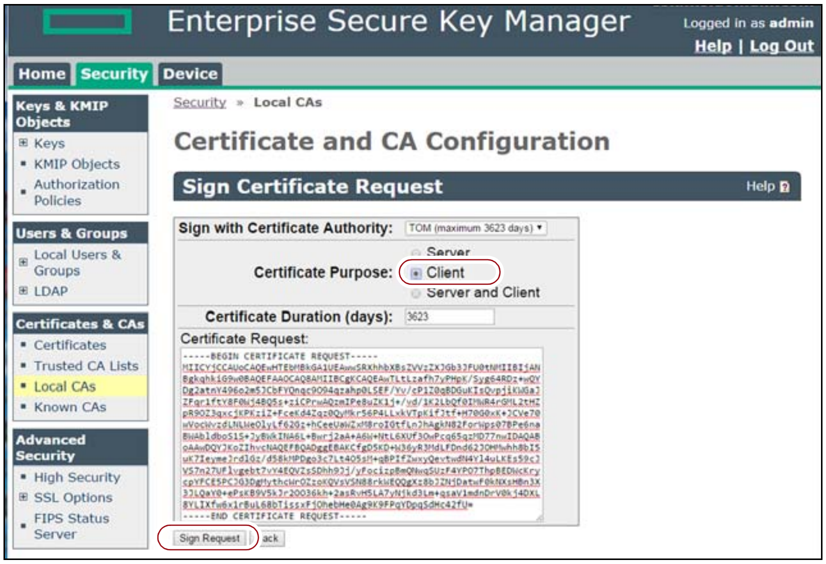
CA Name	CA Information	CA Status
● TOM	Common: TOM Issuer: SPECTRA Expires: Sep 18 20:16:30 2026 GMT	CA Certificate Active

Figure 20 Navigate to the Certificate and CA Configuration screen.

3. From the Local Certificate Authority List, select the radio button next to the CA entry you want to use to sign the client certificate (in this example, it is named "TOM"), and then click **Sign Request**. The Certificate and CA Configuration screen updates to show the Sign Certificate Request section.

   Note: If there are no local certificate authorities listed, use your standard process for creating a local certificate authority.

4. Select **Client** for the Certificate Purpose.



Certificate and CA Configuration

Sign Certificate Request

Sign with Certificate Authority: TOM (maximum 3623 days)

Certificate Purpose: ○ Server ● Client ○ Server and Client

Certificate Duration (days): 3623

Certificate Request:

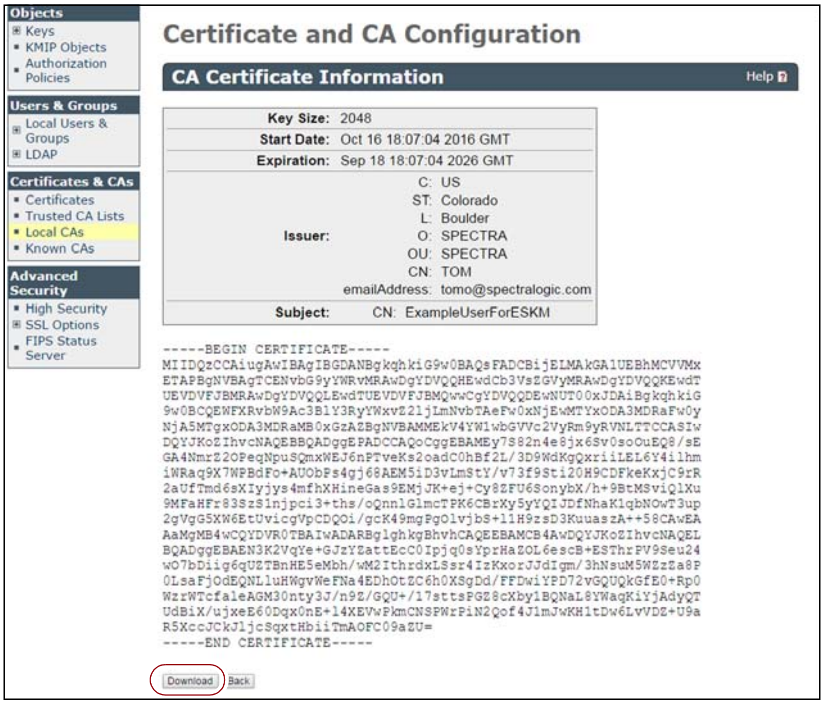
```
-----BEGIN CERTIFICATE REQUEST-----
MIICYjCCAUoCAQEwHTEbMBkGA1UEAwwSRXhhbXBsZVVzZXJGb3JFU0tNMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwTLtLzafh7yPHpK/Syg64RDz+wQY
Dg2atmY496o2m5JCbFYQnqc9O94qzahp0LSEF/Yv/cP1Z0qBDGuKIsQvpjiKWGaJ
ZFqr1ftY8F0Wj48Q5s+ziCPrwAQzmIPe8uZK1j+/vd/1K2LbQf0IMWR4rGML2tHZ
pR9OZ3qxcjKPKziZ+FceKd4Zqz0QyMkr56P4LLxkVTpKifJtf+H70G0xK+JCVe70
wVocWvzdLNLWeOlyLf62Gz+hCeeUaWZxM8roI0tfLnJhAgkN82ForWps07BPe6na
BWAbldboS1S+JyBWkINA6L+Bwrj2aA+A6W+NtL6XUf3OwPcq65qzMD77nwIDAQAB
oAAwDQYJKoZIhvcNAQEFBQADggEBAKCfgD5KD+W36yR3MdLFDnd62JOMMwhh8bI5
uK7IeymeJrdlGz/d58kMPDgo3c7Lt4O5sM+qBPIfZwxyQevtwdN4Yl4uLKEs59cJ
VS7n27UFlvgebt7vY4EQVZsSDhh9Jj/yFocizp8mQNwqSUzF4YPO7ThpBEDWcKry
cpYFCE5PCJG3DgMythcWrOZzoKQVsV5N88rkWEQQgXz8bJZNjDatwF0kNXsM8n3X
3JLQaY0+ePsKB9V5kJr2OO36kh+2asRvH5LA7yNjkd3Lm+qsaV1mdnDrV0kj4DXL
8YLIXfw6x1r8uL68bTissxFjOhebMe0Ag9K9FPqYDpqSdMc42fU=
-----END CERTIFICATE REQUEST-----
```

Figure 21 The SIgn Certificate Request section of the Certificate and CA Configuration screen.

5. Paste the CSR text from the library's BlueScale interface Certificate Signing Request screen (Step 6 on page 49) into the Certificate Request entry field.

6. Click **Sign Request**. The CA Certificate Information screen displays.

7. Copy the client certificate to the clipboard or click **Download** to save it to a file on your local host. You will use the certificate as new user credentials for the HPE ESKM server, and the library will use it to make Transport Layer Security (TLS) connections to the KMIP server.



Certificate and CA Configuration

CA Certificate Information

Key Size: 2048

Start Date: Oct 16 18:07:04 2016 GMT

Expiration: Sep 18 18:07:04 2026 GMT

Issuer: C: US
ST: Colorado
L: Boulder
O: SPECTRA
OU: SPECTRA
CN: TOM
emailAddress: tomo@spectralogic.com

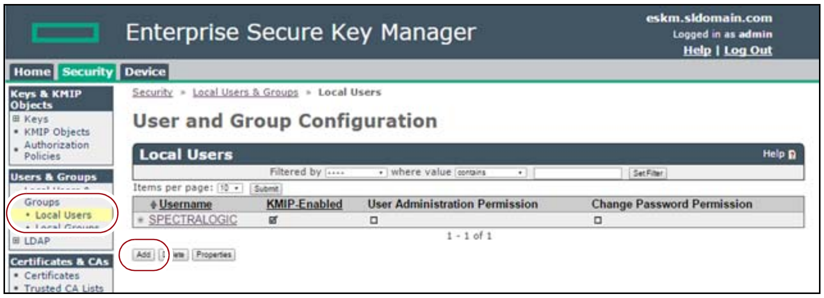
Subject: CN: ExampleUserForESKM

```
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIBGDANBgkqhkiG9w0BAQsFADCBijELMAkGA1UEBhMCVVMx
ETAPBgNVBAgTCENvbG9yYWRvMRAwDgYDVQQHEwdCb3VsZGVyMRAwDgYDVQQKEwdT
UEVDVFJBMRAwDgYDVQQLEwdTUEVDVFJBMQwwCgYDVQQDEwNUT00xJDAiBgkqhkiG
9w0BCQEWFXRvbW9Ac3BlY3RyYWxvZ21jLmNvbTAeFw0xNjEwMTYxODA3MDRaFw0y
NjA5MTgxODA3MDRaMB0xGzAZBgNVBAMMEkV4YW1wbGVVc2VyRm9yRVNLTTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMEy7S82n4e8jx6Sv0soOuEQ8/sE
GA4NmrZ2OPeqNpuSQmxWEJ6nPTveKs2oadC0hBf2L/3D9WdKgQxriiLEL6Y4ilhm
iWRaq9X7WPBdFo+AUObPs4gj68AEM5iD3vLmStY/v73f9Sti20H9CDFkeKxjC9rR
2aUfTmd6sXIyjys4mfhXHineGas9EMjJK+ej+Cy8ZFU6SonybX/h+9BtMSviQlXu
9MFaHFr83SzS1njpci3+ths/oQnnlGlmcTPK6CBrXy5yYQIJDfNhaK1qbNOwT3up
2gVgG5XW6EtUvicgVpCDQOi/gcK49mgPgOlvjbS+l1H9zsD3KuuaszA++58CAwEA
AaMgMB4wCQYDVR0TBAIwADARBglghkgBhvhCAQEEBAMCB4AwDQYJKoZIhvcNAQEL
BQADggEBAEN3K2VqYe+GJzYZattEcC0Ipjq0sYprHaZOL6escB+ESThrPV9Seu24
wO7bDiig6qUZTBnHE5eMbh/wM2IthrdxLSsr4IzKxorJJdIgm/3hNsuM5WZzZa8P
0LsaFjOdEQNLluHWgvWeFNa4EDhOtZC6h0XSgDd/FFDwiYPD72vGQUQkGfE0+Rp0
WzrWTcfaleAGM30nty3J/n9Z/GQU+/17sttsPGZ8cXby1BQNaL8YWagKiYjAdyQT
UdBiX/ujxeE60Dqx0nE+14XEVwPkmCNSPWrPiN2Qof4J1mJwKH1tDw6LvVDZ+U9a
R5XccJCkJljcSqxtHbiiTmAOFC09aZU=
-----END CERTIFICATE-----
```

Figure 22 Copy or download the signed certificate.

Add a New Local User to HPE ESKM

1. From the left hand menu on the HPE ESKM screen, select **Local Users**. The Users and Group Configuration screen displays.



User and Group Configuration

Local Users

Filtered by ---- where value contains Set Filter

Items per page: 10 Submit

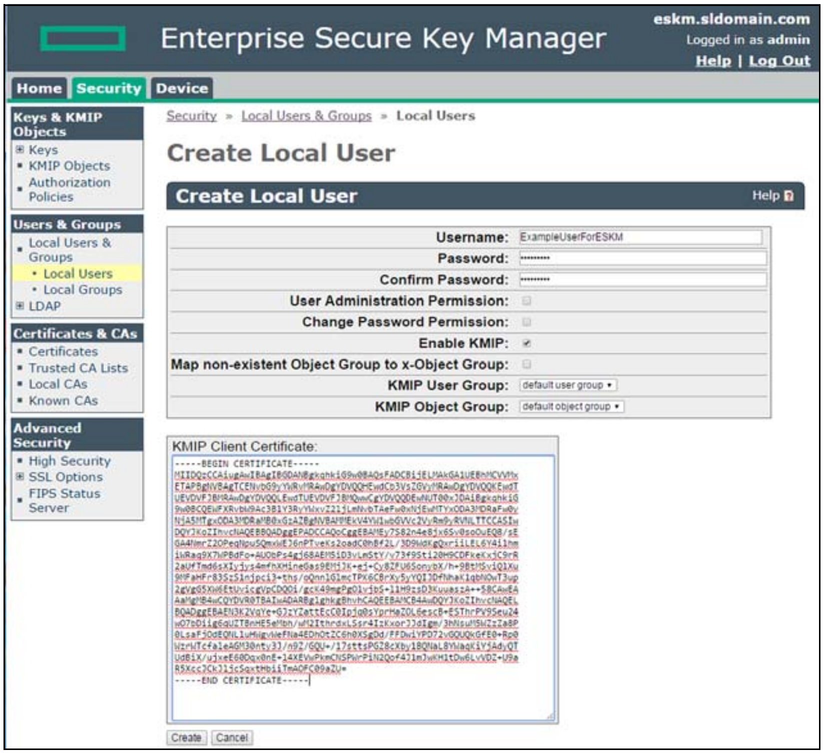
Username	KMIP-Enabled	User Administration Permission	Change Password Permission
SPECTRALOGIC	☑	□	□

1 - 1 of 1

Figure 23 The Users and Group Configuration screen.

2. Click **Add** to display the Create Local User screen.

3. For Username, enter the name you configured as the Common Name in Step 4 on page 48.



Create Local User

Create Local User

Username: ExampleUserForESKM
Password: ••••••••••
Confirm Password: ••••••••••
User Administration Permission: □
Change Password Permission: □
Enable KMIP: ☑
Map non-existent Object Group to x-Object Group: □
KMIP User Group: default user group
KMIP Object Group: default object group

KMIP Client Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIBGDANBgkqhkiG9w0BAQsFADCBijELMAkGA1UEBhMCVVMx
ETAPBgNVBAgTCENvbG9yYWRvMRAwDgYDVQQHEwdCb3VsZGVyMRAwDgYDVQQKEwdT
UEVDVFJBMRAwDgYDVQQLEwdTUEVDVFJBMQwwCgYDVQQDEwNUT00xJDAiBgkqhkiG
9w0BCQEWFXRvbW9Ac3B1Y3RyYWxvZ21jLmNvbTAeFw0xNjEwMTYxODA3MDRaFw0y
NjA5MTgxODA3MDRaMB0xGzAZBgNVBAMMEkV4YW1wbGVVc2VyRm9yRVNLTTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMEy7S82n4e8jx6Sv0soOuEQ8/sE
GA4NmrZ2OPeqNpuSQmxWEJ6nPTveKs2oadC0hBf2L/3D9WdKgQxriiLEL6Y4i1hm
iWRaq9X7WPBdFo+AUObPs4gj68AEMSiD3vLmStY/v73f9Sti20H9CDFkeKxjC9rR
2aUfTmd6sXIyjys4mfhXHineGas9EMjJK+ej+Cy8ZFU6SonybX/h+9BtMSviQ1Xu
9MFaHFr83SzS1njpci3+ths/oQnn1G1mcTPK6C8rXy5yYQIJDfNhaK1qbNOwT3up
2gVgG5XW6EtUvicgVpCDQ0i/gcK49mgPg01vjbS+11M9zsD3KuuaszA++58CAwEA
AaMgMB4wCQYDVR0TBAIwADARBglghkgBhvhCAQEEBAMCB4AwDQYJKoZIhvcNAQEL
BQADggEBAEN3K2VqYe+GJzYZattEcC0Ipjq0sYprHaZ0L6escB+ESThrPV9Seu24
wO7bDiig6qUZTBnHE5eMbh/wM2IthrdxLSsr4IzKxorJJdIgm/3hNsuM5WZzZa8P
0LsaFjOdEQNL1uMWgvWeFNa4EDhOtZC6h0XSgDd/FFDwiYPD72vGQUQkGfE0+Rp0
WzrWTcfaleAGM30nty3J/n92/GQU+/17sttsPG28cXby18QNaL8YWaqKiYjAdyQT
UdBiX/ujxeE60Dqx0nE+14XEVwPkmCNSPWrPiN2Qof4J1mJwKH1tDw6LvVDZ+U9a
R5XccJCkJ1jcSqxtHbiiTmAOFC09aZU=
-----END CERTIFICATE-----
```

Figure 24 Enter the information to create a local user.

4. Enter any suitable Password and then confirm the password.

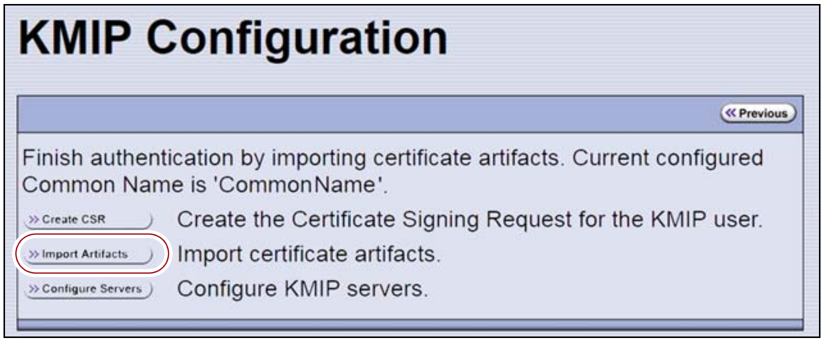
   Note: The library does not use this password at this time.

5. Paste the client certificate copied or downloaded in Step 7 on page 51 into the KMIP Client Certificate field.

6. Click **Create.**

Import Artifacts

1. On the KMIP Configuration screen in the library BlueScale interface, click **Import Artifacts**. The Import Signed Client Certificate screen displays.



KMIP Configuration

Finish authentication by importing certificate artifacts. Current configured Common Name is 'CommonName'.

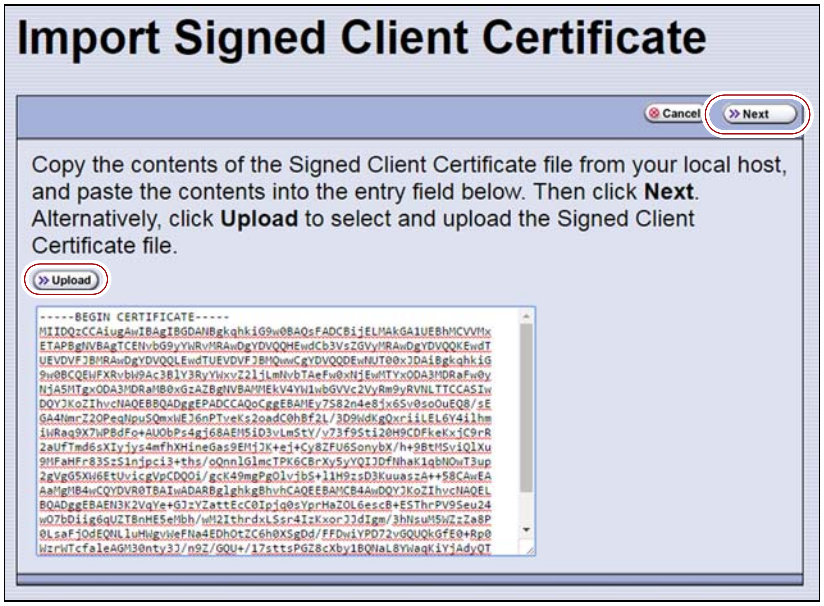
Create the Certificate Signing Request for the KMIP user.

Import certificate artifacts.

Configure KMIP servers.

Figure 25 Click **Import Artifacts**.

2. Paste the signed client certificate copied in Step 7 on page 51 into the entry field, or if you downloaded the certificate file onto your local host, click **Upload** and use your web browser to upload the file, and then click **Next**. The Import Local CA for Server Certificate screen displays.



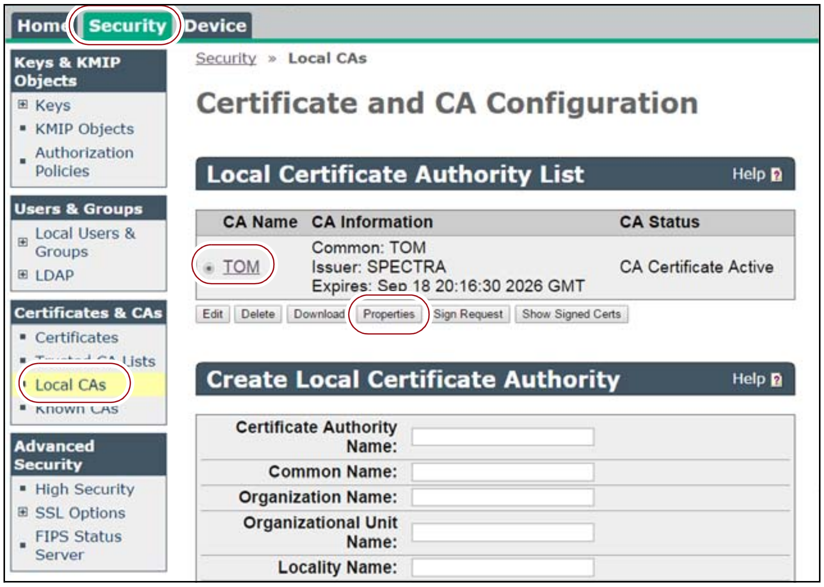
Import Signed Client Certificate

Copy the contents of the Signed Client Certificate file from your local host, and paste the contents into the entry field below. Then click **Next**. Alternatively, click **Upload** to select and upload the Signed Client Certificate file.

```
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIBGDANBgkqhkiG9w0BAQsFADCBijELMAkGA1UEBhMCVVMx
ETAPBgNVBAgTCENvbG9yYWRvMRAwDgYDVQQHEwdCb3VsZGVyMRAwDgYDVQQKEwdT
UEVDVFJBMRAwDgYDVQQLEwdTUEVDVFJBMQwwCgYDVQQDEwNUT00xJDAiBgkqhkiG
9w0BCQEWFXRvbW9Ac3BlY3RyYWxvZ2ljLmNvbTAeFw0xNjEwMTYxODA3MDRaFw0y
NjA5MTgxODA3MDRaMB0xGzAZBgNVBAMMEkV4YW1wbGVVc2VyRm9yRVNLTTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMEy7S82n4e8jx6Sv0soOuEQ8/sE
GA4NmrZ2OPeqNpuSQmxWEJ6nPTveKs2oadC0hBf2L/3D9WdKgQxriiLEL6Y4ilhm
iWRaq9X7WPBdFo+AUObPs4gj68AEM5iD3vLmStY/v73f9Sti20H9CDFkeKxjC9rR
2aUfTmd6sXIyjys4mfhXHineGas9EMjJK+ej+Cy8ZFU6SonybX/h+9BtMSviQlXu
9MFaHFr83SzS1njpci3+ths/oQnnlGlmcTPK6CBrXy5yYQIJDfNhaK1qbNOwT3up
2gVgG5XW6EtUvicgVpCDQOi/gcK49mgPgOlvjbS+l1H9zsD3KuuaszA++58CAwEA
AaMgMB4wCQYDVR0TBAIwADARBglghkgBhvhCAQEEBAMCB4AwDQYJKoZIhvcNAQEL
BQADggEBAEN3K2VqYe+GJzYZattEcC0Ipjq0sYprHaZOL6escB+ESThrPV9Seu24
wO7bDiig6qUZTBnHE5eMbh/wM2IthrdxLSsr4IzKxorJJdIgm/3hNsuM5WZzZa8P
0LsaFjOdEQNLluHWgvWeFNa4EDhOtZC6h0XSgDd/FFDwiYPD72vGQUQkGfE0+Rp0
WzrWTcfaleAGM30nty3J/n9Z/GQU+/17sttsPGZ8cXby1BQNaL8YWaqKiYjAdyQT
```

Figure 26 The Import Signed Client Certificate screen.

3. Return to the HPE ESKM screen and select the **Security** tab, and then on the left hand menu, select **Local CAs**. The Certificate and CA Configuration screen displays.



Certificate and CA Configuration

Local Certificate Authority List

CA Name	CA Information	CA Status
○ TOM	Common: TOM Issuer: SPECTRA Expires: Sep 18 20:16:30 2026 GMT	CA Certificate Active

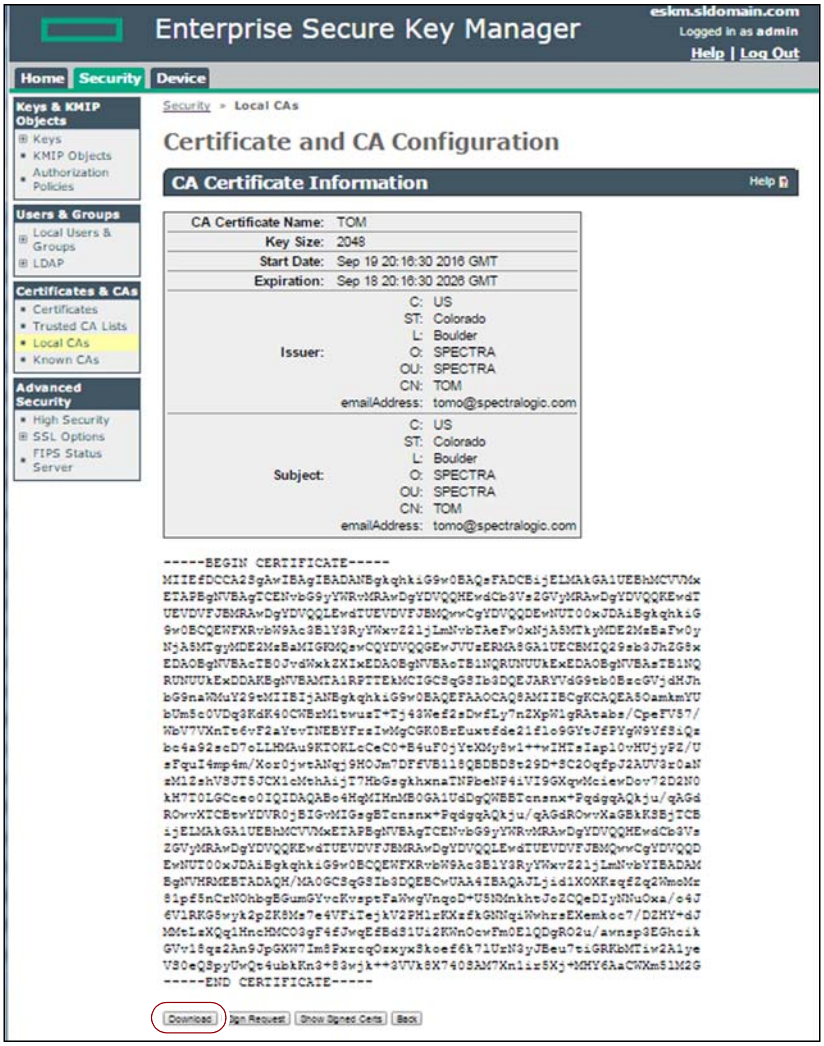
Create Local Certificate Authority

Certificate Authority Name:	
Common Name:	
Organization Name:	
Organizational Unit Name:	
Locality Name:	

Figure 27 Navigate to the Certificate and CA Configuration screen.

4. From the Local Certificate Authority List, select the radio button next to the CA entry you used to sign the client certificate (in this example, it is named "TOM"), and then click **Properties**. The CA Certificate Information displays.

5. Copy the CA certificate to the clipboard or click **Download** to save the information to a file on your local host.



Certificate and CA Configuration

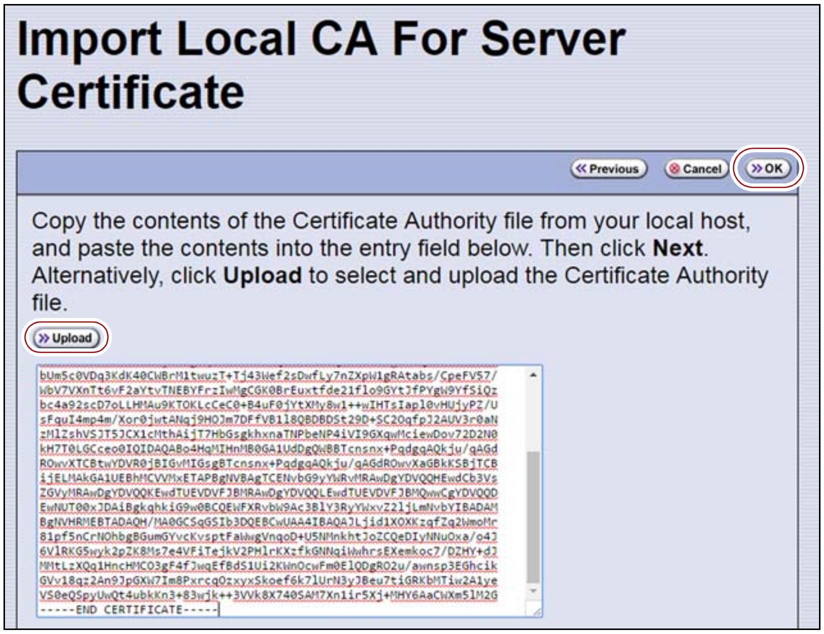
CA Certificate Information

CA Certificate Name:		TOM
Key Size:		2048
Start Date:		Sep 19 20:16:30 2016 GMT
Expiration:		Sep 18 20:16:30 2026 GMT
Issuer:	C:	US
	ST:	Colorado
	L:	Boulder
	O:	SPECTRA
	OU:	SPECTRA
	CN:	TOM
	emailAddress:	tomo@spectralogic.com
Subject:	C:	US
	ST:	Colorado
	L:	Boulder
	O:	SPECTRA
	OU:	SPECTRA
	CN:	TOM
	emailAddress:	tomo@spectralogic.com

```
-----BEGIN CERTIFICATE-----
MIIEfDCCA2SgAwIBAgIBADANBgkqhkiG9w0BAQsFADCBijELMAkGA1UEBhMCVVMx
ETAPBgNVBAgTCENvbG9yYWRvMRAwDgYDVQQHEwdCb3VsZGVyMRAwDgYDVQQKEwdT
UEVDVFJBMRAwDgYDVQQLEwdTUEVDVFJBMQwwCgYDVQQDEwNUT00xJDAiBgkqhkiG
9w0BCQEWFXRvbW9Ac3BlY3RyYWxvZ2ljLmNvbTAeFw0xNjA5MTkyMDE2MzBaFw0y
NjA5MTgyMDE2MzBaMIGKMQswCQYDVQQGEwJVUzERMA8GA1UECBMIQ29sb3JhZG8x
EDAOBgNVBAcTB0JvdWxkZXIxEDAOBgNVBAoTB1NQRUNUUkExEDAOBgNVBAsTB1NQ
RUNUUkExDDAKBgNVBAMTA1RPTTEkMCIGCSqGSIb3DQEJARYVdG9tb0BzcGVjdHJh
bG9naWMuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5OamkmYU
bUm5c0VDq3KdK40CWBrM1twuzT+Tj43Wef2sDwfLy7nZXpW1gRAtabs/CpeFV57/
WbV7VXnTt6vF2aYtvTNEBYFrzIwMgCGK0BrEuxtfde21flo9GYtJfPYgW9YfSiQz
bc4a92scD7oLLHMAu9KTOKLcCeC0+B4uF0jYtXMy8w1++wIHTsIap10vHUjyPZ/U
sFquI4mp4m/Xor0jwtANqj9HOJm7DFfVB118QBDBDSt29D+SC2OqfpJ2AUV3r0aN
zM1ZshV8JT5JCX1cMthAijT7HbGsgkhxnaTNPbeNP4iVI9GXqwMciewDov72D2N0
kH7T0LGCceo0IQIDAQABo4HqMIHnMB0GA1UdDgQWBBTcnsnx+PqdgqAQkju/qAGd
ROwvXTCBtwYDVR0jBIGvMIGsgBTcnsnx+PqdgqAQkju/qAGdROwvXaGBkKSBjTCB
ijELMAkGA1UEBhMCVVMxETAPBgNVBAgTCENvbG9yYWRvMRAwDgYDVQQHEwdCb3Vs
ZGVyMRAwDgYDVQQKEwdTUEVDVFJBMRAwDgYDVQQLEwdTUEVDVFJBMQwwCgYDVQQD
EwNUT00xJDAiBgkqhkiG9w0BCQEWFXRvbW9Ac3BlY3RyYWxvZ2ljLmNvbYIBADAM
BgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQAJLjid1XOXKzqfZq2WmoMr
81pf5nCrNOhbgBGumGYvcKvsptFaWwgVnqoD+U5NMnkhtJoZCQeDIyNNuOxa/o4J
6V1RKG5wyk2pZK8Ms7e4VFiTejkV2PH1rKXzfkGNNqiWwhrsEXemkoc7/D2HY+dJ
MMtLzXQq1HncHMCO3gF4fJwqEfBdS1Ui2KWnOcwFm0E1QDgRO2u/awnsp3EGhcik
GVv18qz2An9JpGKW7Im8PxrcqOzxyx3koef6k71UrN3yJBeu7tiGRKbMTiw2A1ye
VS0eQ8pyUwQt4ubkKn3+83wjk++3VVk8X740SAM7Xn1ir5Xj+MHY6AaCWXm51M2G
-----END CERTIFICATE-----
```

Figure 28 The CA Certificate Information screen.

6. Paste the CA certificate copied in Step 5 on page 55 into the entry field on the Import Local CA For Server Certificate screen, or if you downloaded the Certificate Authority file onto your local host, click **Upload** and use your web browser to upload the file, and then click **OK**. The KMIP Configuration screen displays.



Import Local CA For Server Certificate

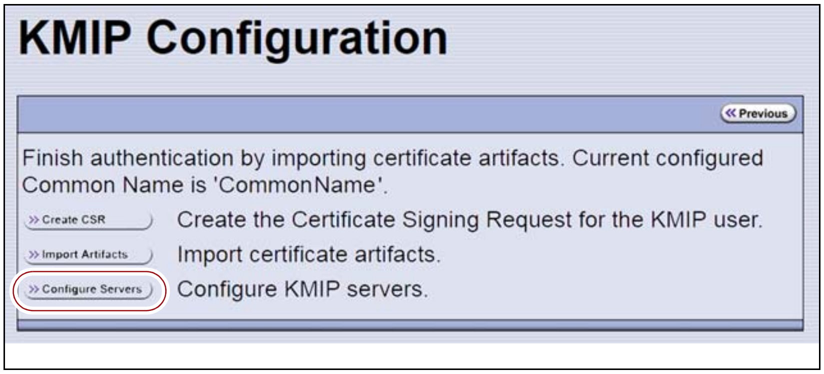
Copy the contents of the Certificate Authority file from your local host, and paste the contents into the entry field below. Then click **Next**. Alternatively, click **Upload** to select and upload the Certificate Authority file.

```
bUm5c0VDq3KdK40CWBrM1twuzT+Tj43Wef2sDwfLy7nZXpW1gRAtabs/CpeFV57/
WbV7VXnTt6vF2aYtvTNEBYFrzIwMgCGK0BrEuxtfde21flo9GYtJfPYgW9YfSiQz
bc4a92scD7oLLHMAu9KTOKLcCeC0+B4uF0jYtXMy8w1++wIHTsIapl0vHUjyPZ/U
sFquI4mp4m/Xor0jwtANqj9HOJm7DFfVB1l8QBDBDSt29D+SC2OqfpJ2AUV3r0aN
zMlZshVSJT5JCX1cMthAijT7HbGsgkhxnaTNPbeNP4iVI9GXqwMciewDov72D2N0
kH7T0LGCceo0IQIDAQABo4HqMIHnMB0GA1UdDgQWBBTcnsnx+PqdgqAQkju/qAGd
ROwvXTCBtwYDVR0jBIGvMIGsgBTcnsnx+PqdgqAQkju/qAGdROwvXaGBkKSBjTCB
ijELMAkGA1UEBhMCVVMxETAPBgNVBAgTCENvbG9yYWRvMRAwDgYDVQQHEwdCb3Vs
ZGVyMRAwDgYDVQQKEwdTUEVDVFJBMRAwDgYDVQQLEwdTUEVDVFJBMQwwCgYDVQQD
EwNUT00xJDAiBgkqhkiG9w0BCQEWFXRvbW9Ac3BlY3RyYWxvZ2ljLmNvbYIBADAM
BgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQAJLjid1XOXKzqfZq2WmoMr
81pf5nCrNOhbgBGumGYvcKvsptFaWwgVnqoD+U5NMnkhtJoZCQeDIyNNuOxa/o4J
6VlRKG5wyk2pZK8Ms7e4VFiTejkV2PHlrKXzfkGNNqiWwhrsEXemkoc7/DZHY+dJ
MMtLzXQq1HncHMCO3gF4fJwqEfBdS1Ui2KWnOcwFm0ElQDgRO2u/awnsp3EGhcik
GVv18qz2An9JpGXW7Im8PxrcqOzxyxSkoef6k7lUrN3yJBeu7tiGRKbMTiw2A1ye
VS0eQSpyUwQt4ubkKn3+83wjk++3VVk8X740SAM7Xn1ir5Xj+MHY6AaCWXm5lM2G
-----END CERTIFICATE-----
```

Figure 29 The Import Local CA for Server Certificate screen.

Configure KMIP Servers

1. On the KMIP Configuration screen, click **Configure Servers**. The KMIP Server Status screen displays.



KMIP Configuration

Finish authentication by importing certificate artifacts. Current configured Common Name is 'CommonName'.

Create the Certificate Signing Request for the KMIP user.

Import certificate artifacts.

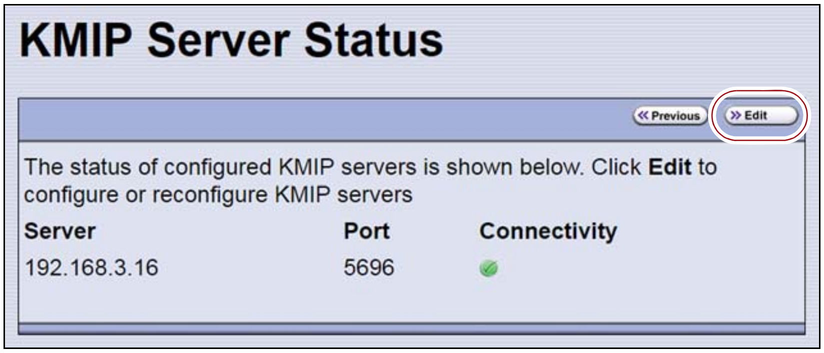
Configure KMIP servers.

Figure 30 Click **Configure Servers**.

2. The KMIP Server Status screen displays a list of KMIP servers known to the library. The library can use up to four KMIP servers; each is listed by its IP address or hostname.

   Note: A ✓ in a green circle appears in the Connectivity column next to servers the library can access. A red **X** in the Connectivity column indicates the library is currently unable to connect to that server.

   On the KMIP Server Status screen, click **Edit** to add or modify KMIP servers.



KMIP Server Status

The status of configured KMIP servers is shown below. Click **Edit** to configure or reconfigure KMIP servers

Server	Port	Connectivity
192.168.3.16	5696	✓

Figure 31 Click **Edit** to add or modify a server.

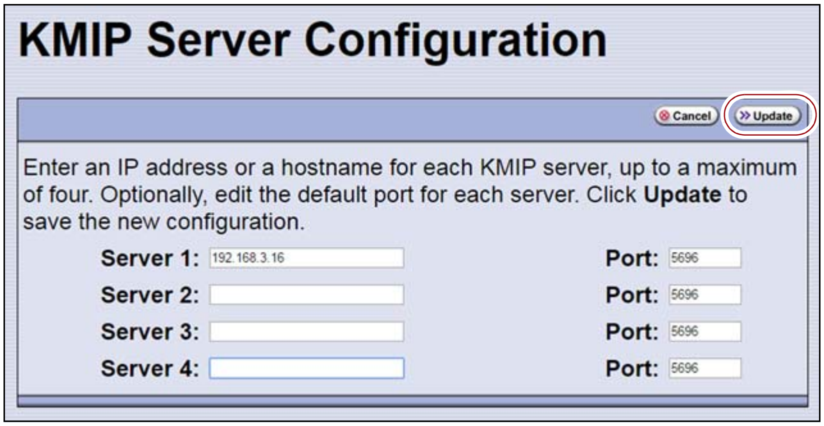
3. The KMIP Server Configuration screen displays an editable list of configured KMIP servers. Enter the appropriate information for the server you want to configure.

   Note: To delete a server, delete its IP address or hostname.

   a. Enter the IP address or hostname of the server.

   b. If desired, change the port setting. The default port setting is 5696.

   c. Click **Update** to save the changes. The library attempts to connect to the server and the Encryption Server Update Result screen displays the success or failure of the KMIP server configuration.



KMIP Server Configuration

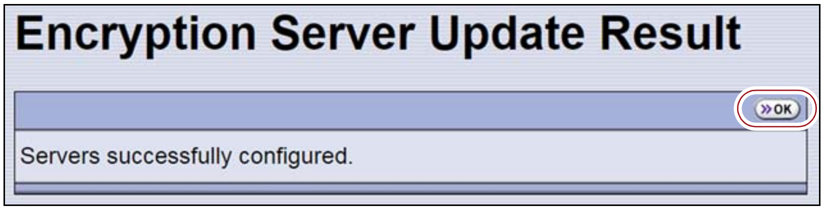
Enter an IP address or a hostname for each KMIP server, up to a maximum of four. Optionally, edit the default port for each server. Click **Update** to save the new configuration.

Server 1:	192.168.3.16	**Port:**	5696
Server 2:		**Port:**	5696
Server 3:		**Port:**	5696
Server 4:		**Port:**	5696

Figure 32 Click **Update** to save the changes.

4. If the Encryption Server Update Result screen indicates a failure, reenter the information in Step 3 on page 57. Otherwise, click **OK** to return to the KMIP Server Status screen.

Note: The list of servers on the KMIP Server Status screen includes successfully added servers. If the library could not connect to the server or verify it as a KMIP server, it does not appear in the list.



Encryption Server Update Result

Servers successfully configured.

Figure 33 The Encryption Server Update Result screen.

CONFIGURING A PARTITION TO USE A KMIP SERVER

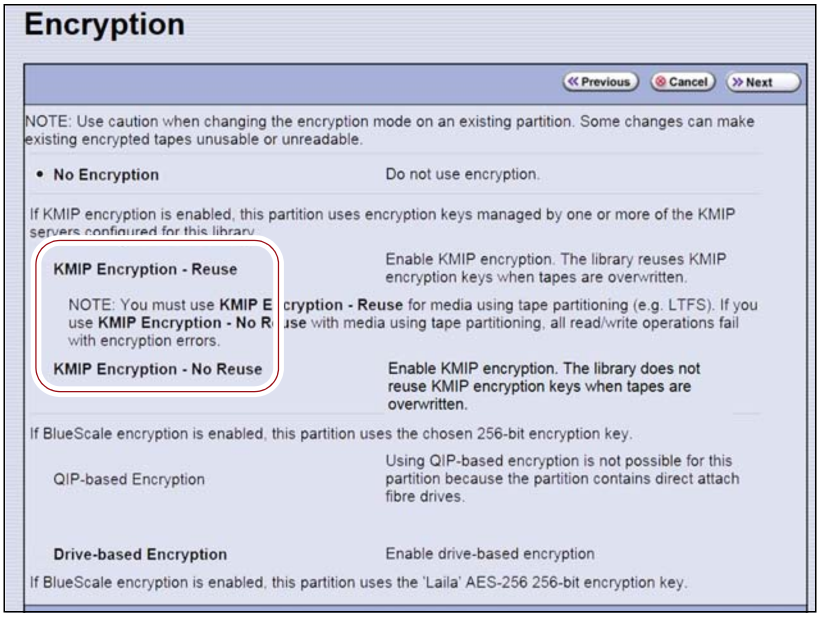
Overview After configuring a KMIP server, you can enable KMIP Encryption Key Management for one or more partitions.

Notes:

- The Encryption screen in the partition wizard lets you enable the encryption features for the partition. Depending on the version of BlueScale software, the Encryption screen does not display, or displays with all options grayed out, unless you are logged into the library as an encryption user and have either created one or more BlueScale encryption keys, or configured a Spectra SKLM or KMIP server. See Configure KMIP Encryption on page 46 for more information.
- KMIP encryption is not compatible with Spectra SKLM Encryption Key Management or BlueScale Encryption Key Management, because they cannot share encryption keys. Data encrypted using KMIP encryption cannot be decrypted using Spectra SKLM or BlueScale Encryption Key Management, and vice versa.
- KMIP encryption is only compatible with LTO-6 and later generation tape drives and TS11xx drives.
- KMIP encryption is not compatible with PostScan. Do not enable PostScan for the partition if you want to use KMIP encryption.
- You must use **KMIP Encryption - Reuse** for media using tape partitioning (for example, LTFS). If you use **KMIP Encryption - No Reuse** with media using tape partitioning, all read/write operations fail with encryption errors.

Use the following steps to assign a KMIP server to the partition:

1. Access the encryption feature (see Log Into the Encryption Feature on page 31).
2. Select **Configuration ···› Partitions**. The Shared Library Services screen displays.
3. Click **New** to create a partition, or click **Edit** to modify the settings for an existing partition (see “Creating a Storage Partition” in your *Tape Library User Guide* for more information about creating or editing partitions).
4. Proceed through the partition wizard until you reach the Encryption screen.



NOTE: Use caution when changing the encryption mode on an existing partition. Some changes can make existing encrypted tapes unusable or unreadable.

● **No Encryption** Do not use encryption.

If KMIP encryption is enabled, this partition uses encryption keys managed by one or more of the KMIP servers configured for this library.

KMIP Encryption - Reuse Enable KMIP encryption. The library reuses KMIP encryption keys when tapes are overwritten.

NOTE: You must use **KMIP E cryption - Reuse** for media using tape partitioning (e.g. LTFS). If you use **KMIP Encryption - No R use** with media using tape partitioning, all read/write operations fail with encryption errors.

KMIP Encryption - No Reuse Enable KMIP encryption. The library does not reuse KMIP encryption keys when tapes are overwritten.

If BlueScale encryption is enabled, this partition uses the chosen 256-bit encryption key.

QIP-based Encryption Using QIP-based encryption is not possible for this partition because the partition contains direct attach fibre drives.

Drive-based Encryption Enable drive-based encryption

If BlueScale encryption is enabled, this partition uses the 'Laila' AES-256 256-bit encryption key.

Figure 34 The Encryption screen.

5. Choose the type of encryption to use.

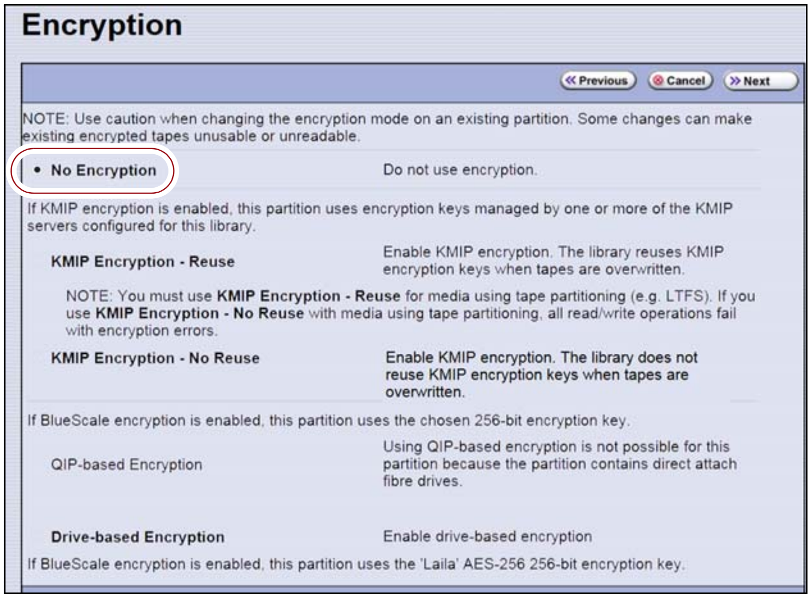
Encryption Option	Description
No Encryption	Turns off encryption. All subsequent data written to tapes in this partition is not encrypted. Any data previously written using encryption remains encrypted, but not readable unless encryption is re-enabled.
KMIP Encryption-Reuse	Turns on KMIP encryption key management for drive-based encryption. The library reuses KMIP encryption keys when tapes are overwritten.
KMIP Encryption - No Reuse	Turns on KMIP encryption key management for drive-based encryption. The library does not reuse KMIP encryption keys when tapes are overwritten.
BlueScale Encryption	Turns on BlueScale encryption key management for either drive-based or QIP-based encryption. See Chapter 4 – Using BlueScale Encryption Standard Edition, beginning on page 61 or Chapter 5 – Using BlueScale Encryption Professional Edition, beginning on page 80 for more information.

6. Proceed through the remaining partition configuration screens.
7. When you reach the Save Partition screen, click **Save**.

DISABLING ENCRYPTION IN A PARTITION

Use the following steps to disable encryption in a partition.

1. Access the encryption feature (see Log Into the Encryption Feature on page 31).
2. Select **Configuration** ⇢ **Partitions**. The Shared Library Services screen displays.
3. Select the partition for which you want to disable encryption. Click **Edit**.
4. Click **Next** to navigate through the partition wizard screens until you reach the Encryption screen.



NOTE: Use caution when changing the encryption mode on an existing partition. Some changes can make existing encrypted tapes unusable or unreadable.

● **No Encryption** — Do not use encryption.

If KMIP encryption is enabled, this partition uses encryption keys managed by one or more of the KMIP servers configured for this library.

KMIP Encryption - Reuse — Enable KMIP encryption. The library reuses KMIP encryption keys when tapes are overwritten.

NOTE: You must use **KMIP Encryption - Reuse** for media using tape partitioning (e.g. LTFS). If you use **KMIP Encryption - No Reuse** with media using tape partitioning, all read/write operations fail with encryption errors.

KMIP Encryption - No Reuse — Enable KMIP encryption. The library does not reuse KMIP encryption keys when tapes are overwritten.

If BlueScale encryption is enabled, this partition uses the chosen 256-bit encryption key.

QIP-based Encryption — Using QIP-based encryption is not possible for this partition because the partition contains direct attach fibre drives.

Drive-based Encryption — Enable drive-based encryption

If BlueScale encryption is enabled, this partition uses the 'Laila' AES-256 256-bit encryption key.

Figure 35 The Encryption screen

5. Select **No Encryption**. All subsequent data written to tapes in this partition is not encrypted. Any tapes previously written using encryption remain encrypted.
6. Navigate through the remaining partition configuration screens by clicking **Next**.
7. When you reach the Save Partition screen, click **Save**.

CHAPTER 4

Using BlueScale Encryption Standard Edition

This chapter describes configuring and using BlueScale Encryption Key Management — Standard Edition.

- If you are using Spectra SKLM Encryption Key Management, see Chapter 2 – Using Spectra SKLM Encryption Key Management, beginning on page 35.
- If you are using KMIP Encryption Key Management, see Chapter 3 – Using KMIP Encryption Key Management, beginning on page 44.
- If you are using BlueScale Encryption Key Management — Professional Edition, see Chapter 5 – Using BlueScale Encryption Professional Edition, beginning on page 80.

CONFIGURING BLUESCALE ENCRYPTION STANDARD EDITION

Overview BlueScale encryption key management configuration entails selecting an encryption startup mode, creating an encryption password, creating and using encryption keys, and designating one or more partitions as encryption-enabled. The encryption password lets a superuser access the encryption features. After encryption is enabled, data is automatically encrypted as it is stored in any partition that is encryption-enabled. See Standard Edition vs. Professional Edition on page 20 for a description of the differences between BlueScale Encryption Key Management Standard Edition and Professional Edition.

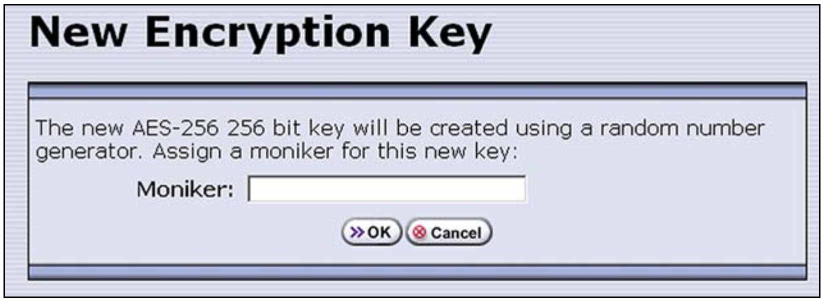
⚠ **Caution** The BlueScale encryption feature password is separate from the password used to log into the library. Make sure you keep a record of this password. If you lose this password, you are not able to configure encryption nor are you able to import/ export encryption keys that were already assigned and used on encrypted tapes.

User Privilege Requirements Only users with superuser privileges can access and use the BlueScale encryption features.

Create an Encryption Key

1. Access the encryption feature (see Log Into the Encryption Feature on page 31).
2. On the Encryption Configuration screen, click **Add Key.** The New Encryption Key screen displays.

   Note: The BlueScale Encryption Standard Edition 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 78, they display again.



New Encryption Key

The new AES-256 256 bit key will be created using a random number generator. Assign a moniker for this new key:

Moniker:

Figure 36 Enter a unique moniker to create a new encryption key.

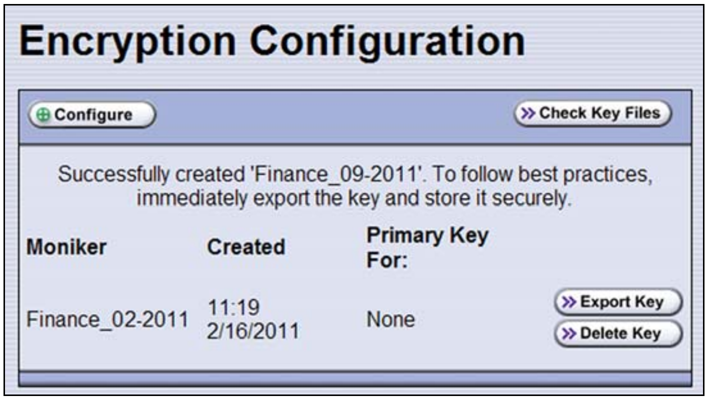
3. Enter a name for the encryption key in the **Moniker** field. Make sure that the moniker meets the following requirements:
   - A moniker can be any combination of the numbers **0–9**, lower and upper case alphabetic characters (**a–z** and **A–Z**), and the at symbol (@), dash (–), underscore (_), and period (.) characters. 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.

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

4. Click **OK**. The Encryption Configuration screen displays with a confirmation showing the moniker for the newly created encryption key and a message reminding you to create a copy of the key for safekeeping.

   Note: If the key is not yet assigned to a partition, **None** displays in the **Primary Key For** column.



Encryption Configuration

Successfully created 'Finance_09-2011'. To follow best practices, immediately export the key and store it securely.

Moniker	Created	Primary Key For:	
Finance_02-2011	11:19 2/16/2011	None	Export Key Delete Key

Figure 37 The new encryption key is listed on the Encryption Configuration screen.

5. Export the newly created encryption key and save it to a secure location (see Export the Encryption Key on page 67).

⚠ **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 67 for additional information.

Assigning an Encryption Key to a Partition

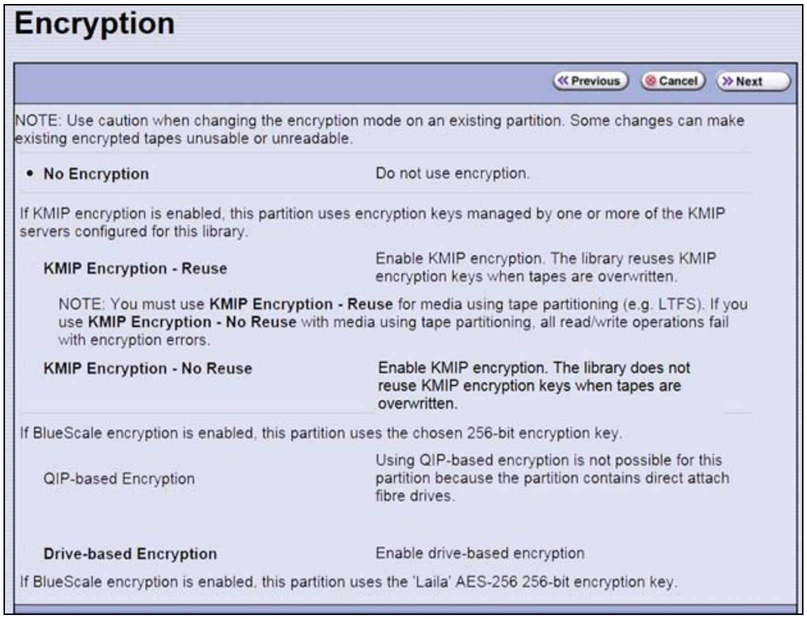
Overview After creating an encryption key, you can assign it to one or more partitions. The encryption choices available for a partition depend on the hardware assigned to the partition.

Notes:

- Depending on the version of BlueScale software, the Encryption screen does not display, or displays with all options grayed out, unless you are logged into the library as an encryption user and have either created one or more BlueScale encryption keys, or configured a Spectra SKLM or KMIP server. See Create an Encryption Key on page 62 for more information.
- F-QIPs are no longer available for purchase. If your library does not already contain an encryption-capable F-QIP, you must use drive-based encryption.
- By default, LTO drives are configured to compress data. If necessary, use your storage management software to modify the drive property settings to turn off compression.
- The encryption performed by encryption-enabled drives is not compatible with the encryption performed by an encryption-enabled F-QIP.
- Spectra SKLM is not compatible with BlueScale Encryption Key Management, because they cannot share encryption keys. Data encrypted using Spectra SKLM key management cannot be decrypted using BlueScale encryption key management, and vice versa.
- If a partition uses both an encryption-enabled F-QIP and encryption-enabled drives, you must choose one type of encryption or the other. You cannot use both types in the same partition.

Use the following steps to assign a key to a partition and encrypt all data sent to the partition:

1. Access the encryption feature (see Log Into the Encryption Feature on page 31).
2. Select **Configuration ⇢ Partitions**. The Shared Library Services screen displays.
3. Click **New** to create a partition, or click **Edit** to modify the settings for an existing partition (see “Creating a Storage Partition” in your *Tape Library User Guide*).
4. Proceed through the partition wizard until you reach the Encryption screen.



Encryption

NOTE: Use caution when changing the encryption mode on an existing partition. Some changes can make existing encrypted tapes unusable or unreadable.

● **No Encryption** Do not use encryption.

If KMIP encryption is enabled, this partition uses encryption keys managed by one or more of the KMIP servers configured for this library.

KMIP Encryption - Reuse Enable KMIP encryption. The library reuses KMIP encryption keys when tapes are overwritten.

NOTE: You must use **KMIP Encryption - Reuse** for media using tape partitioning (e.g. LTFS). If you use **KMIP Encryption - No Reuse** with media using tape partitioning, all read/write operations fail with encryption errors.

KMIP Encryption - No Reuse Enable KMIP encryption. The library does not reuse KMIP encryption keys when tapes are overwritten.

If BlueScale encryption is enabled, this partition uses the chosen 256-bit encryption key.

QIP-based Encryption Using QIP-based encryption is not possible for this partition because the partition contains direct attach fibre drives.

Drive-based Encryption Enable drive-based encryption

If BlueScale encryption is enabled, this partition uses the 'Laila' AES-256 256-bit encryption key.

Figure 38 Select whether to use encryption in the partition.

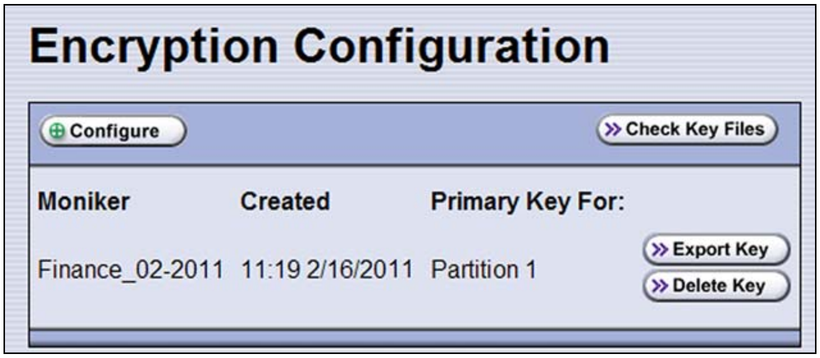
5. Select the type of encryption you would like to enable:

Encryption Option	Description
No Encryption	Turns off encryption. All subsequent data written to tapes in this partition is not encrypted. Any tapes previously written using encryption remain encrypted.
Spectra SKLM Encryption or KMIP Encryption	Only displays if a Spectra SKLM or KMIP encryption server is configured. **Note:** See Using Spectra SKLM Encryption Key Management on page 35 or Using KMIP Encryption Key Management on page 44 for more information.
BlueScale Encryption: QIP-based	Turns on BlueScale encryption using F-QIP-attached, SCSI LTO-2, LTO-3, or LTO-4 drives. The F-QIP encrypts data using the specified encryption key before it is sent to the drive. If you select QIP-based Encryption, you can optionally select **Enable Clear File at BOT**. If you choose this option, the tape headers are unencrypted so that any compatible drive can read the header information on an encrypted tape including the moniker assigned to the encryption key. Using unencrypted headers facilitates key management for sites with a large number of encrypted tapes.
BlueScale Encryption: Drive-based	Turns on BlueScale encryption using direct-attached LTO-4 and later generation drives. The encryption-enabled drives encrypt data using the specified encryption key.

6. Click **Next**.

7. Proceed through the partition wizard until you reach the Save Partition screen, and click **Save**. All data sent to this partition is encrypted using the key you selected.

8. Access the encryption feature (Accessing the Encryption Feature on page 31) and confirm that the listed key reflects the assignment you just completed.


Encryption Configuration

Moniker	Created	Primary Key For:
Finance_02-2011	11:19 2/16/2011	Partition 1

Figure 39 Confirm that the encryption key is correctly assigned to the partition.

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.

⚠ **Caution** Data cannot be recovered without the encryption key used to encrypt the data, so protecting encryption keys is extremely important to data decryption and recovery. To decrypt and restore encrypted data, you need the data, the encryption key, and the encryption key password used to protect the exported key and data.

⚠ **Important** Backup files of the library configuration include any encryption keys that are stored in the library at the time the file is created.

Best Practice Spectra Logic recommends that you export each encryption key to at least two different USB devices and store them in separate locations. Remember, lost encryption keys cannot be recreated; keep them as secure (and as backed up) as your data.

⚠ **Caution** As a matter of best practice, Spectra Logic recommends exporting encryption keys to a USB device instead of using email.

Although emailing encryption keys is supported by the library, using email presents security issues, including the following:

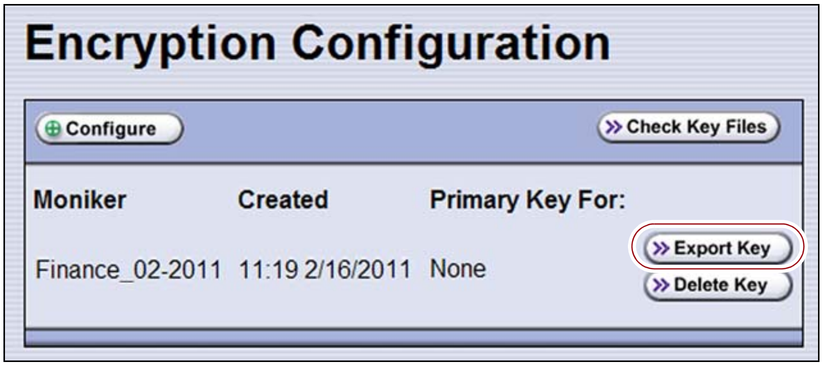
- Copies of encryption keys may be left on the email servers used for sending and receiving email and are thus subject to compromise.
- The difficulty in verifying where all of the copies of emailed encryption keys may be located can make security audits more challenging.

Export the Encryption Key

Use the following steps to export the current encryption key:

1. Access the encryption feature (see Log Into the Encryption Feature on page 31).
2. If you want to export the encryption key to a USB device, plug a USB device into a USB port on the LCM before continuing.

3. From the Encryption Configuration screen, click **Export Key**. The Export Type screen displays.

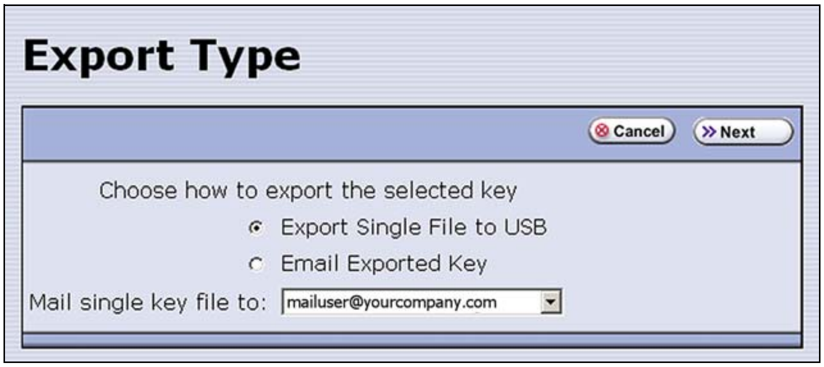


Encryption Configuration

Moniker	Created	Primary Key For:
Finance_02-2011	11:19 2/16/2011	None

Figure 40 Click **Export Key** to begin the key export process.

4. On the Export Type screen, select the desired export option.



Export Type

Choose how to export the selected key

● Export Single File to USB

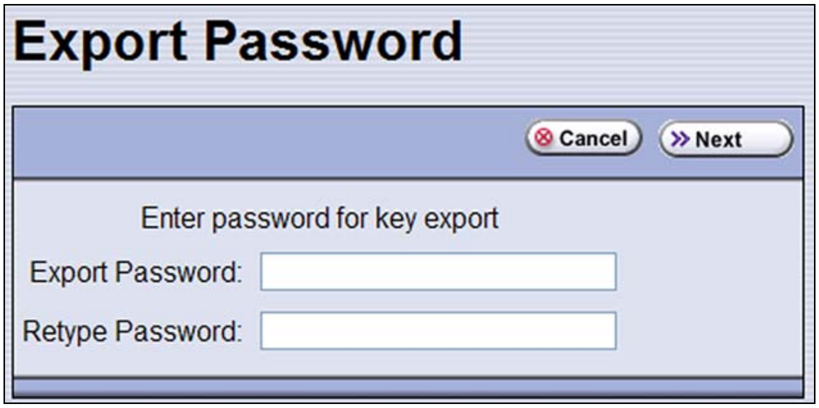
○ Email Exported Key

Mail single key file to: mailuser@yourcompany.com

Figure 41 Choose where the exported key is saved.

Export Type	Description
Export Single File to USB	Saves the exported encryption key to the USB device connected to the LCM.
Email Exported Key	Sends the encryption key as an email attachment to a previously configured mail recipient (see Configure Mail Users in your *Tape Library User Guide*). Use the **Mail single key file to:** drop-down list to select the desired recipient. **Note:** Do not use the default autosupport@spectralogic.com email recipient. Spectra Logic does not save emailed files unless they are specifically requested for troubleshooting.

5. Click **Next**. The Export Password screen displays.



Export Password

Enter password for key export

Export Password:

Retype Password:

Figure 42 Enter and confirm a password for the exported encryption key.

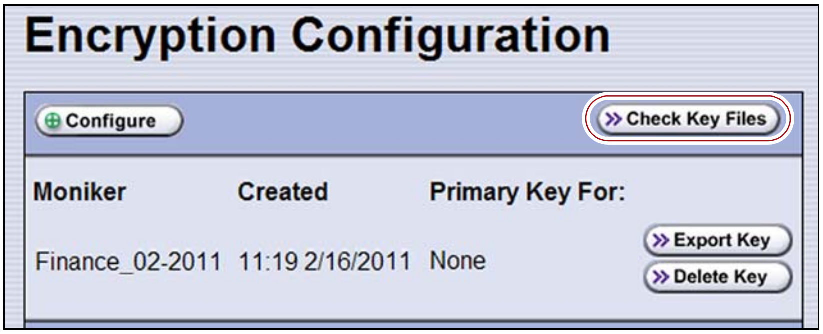
6. Type and retype an export password using any combination of the numbers **0–9**, lower and upper case alphabetic characters (**a–z** and **A-Z**), and the at symbol (**@**), dash (**–**), underscore (**_**), and period (**.**) characters. This key is used to encrypt the exported key.
7. Make a record of the encryption key password; you need it in order to import the key back into the library. Without the password, you cannot import the key, and the data encrypted using the key is inaccessible.

Caution Do not lose the encryption key password. Without it, you cannot reimport an encryption key after it is deleted from the library, and the data encrypted using the key is inaccessible.

8. Click **Next** to export the key to the selected location.

9. Confirm that the encryption key was correctly exported.

   - **If you exported the encryption key to a USB device**—Immediately confirm that the encrypted key copied correctly by clicking **Check Key Files** and following any prompts. If desired, save or print the Check Key Files report for an audit record showing that the USB device was readable, and that the destination key matched the source key. Use the steps in Verify the Exported Encryption Key on page 70 to provide a second confirmation.

Moniker	Created	Primary Key For:
Finance_02-2011	11:19 2/16/2011	None

     Figure 43 Use **Check Key Files** to confirm successful export.

     If the confirmation indicates the key did not copy correctly, delete all data from the USB device so that no trace of the failed export file remains, and then export the key again using a different USB device, beginning with Step 2 on page 67.

   - **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.

Verify the Exported Encryption Key

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

When Saved to a USB Device

1. Plug the USB device into a computer.
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 67 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 at least one 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 67.
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 67).

⚠ **Caution** As a matter of best practice, Spectra Logic recommends exporting encryption keys to a USB device instead of using email.

Although emailing encryption keys is supported by the library, doing so presents security issues, including the following:

- Copies of encryption keys may be left on the email servers used for sending and receiving email and are thus subject to compromise.
- The difficulty in verifying where all the copies of emailed encryption keys may be located can make security audits more challenging.

- If you choose to store only a single copy of an encryption key, make sure that you keep the copy secure. If something happens to the device where you stored the exported key and the key was deleted from the library, both the key and all data encrypted using the key are unrecoverable.

⚠ **Caution** **To emphasize:** If you lose the encryption key or the password for the exported file, your data is **unrecoverable** if the key was deleted from the library. You need to balance the number of copies of the key to store to guarantee access to the encrypted data against the security risk associated with storing multiple keys. Make sure that the key 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 74.

  You may want to make two copies of a key, storing each in a secure location. Keep a record of each key's location so that you can easily find the key when you need to restore or delete data.

- Maintain a list of every password associated with each key and securely store the list. Never keep this list as cleartext (unencrypted text) on a networked computer, or send it through email as cleartext. For added security, encrypt the file containing the list of passwords.

- Track every copy of each key. This tracking is critical in order to meet requirements that may govern data retention and data destruction. Destroying all exported copies of keys associated with encrypted data AND deleting the keys from the library is sufficient to satisfy data destruction requirements, since encrypted data cannot be accessed without the key used to encrypt it.

  Spectra Logic recommends tracking the information listed in the following table for every key that you create. For added security, encrypt the file containing the tracking information.

Key moniker:	
Number of shares (if any):	
Number of key copies:	
Location of each copy:	
Password(s) associated with exported copy of the moniker:	
Location of cartridges containing data encrypted using this moniker:	
Moniker creation date:	
Planned expiration date:	

RESTORING ENCRYPTED DATA

Overview Restoring encrypted data from a cartridge follows the standard data restore processes that you use with your storage management software. The only difference is that the key used to encrypt the data being restored needs to be stored in the library and assigned to the partition in which the encrypted cartridge is loaded. If the key is already stored on the library, the data is automatically decrypted as it is read from tape; if the encryption key is not currently stored on the library, it must be imported before the data can be decrypted. Once the required encryption key is assigned to the partition, standard restore procedures are unchanged.

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 Assigning an Encryption Key to a Partition on page 64. If the encryption key is assigned to a partition, continue with the following steps.

1. If you selected Secure Initialization (see Configure Secure Initialization Mode (BlueScale Encryption Only) on page 33), and no encryption user logged in since the last time the library was initialized, access the encryption feature (see Accessing the Encryption Feature on page 31).
2. If necessary, import the cartridges containing the data to be restored into the library partition to which the encryption key is assigned.
3. 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 78. You can then import another key.

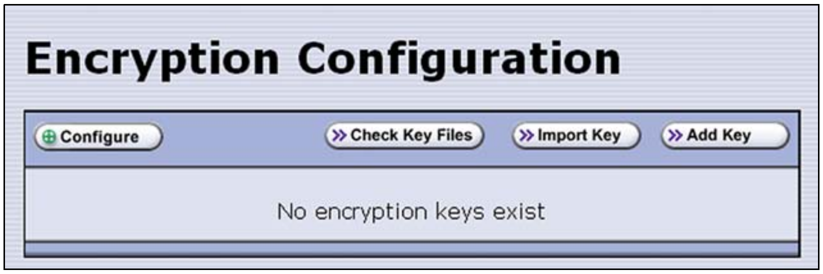
You can import the encryption key from a USB device or from a remote computer through the library's BlueScale web interface, as described in the following sections.

- Import the Key from a USB Device
- Import the Key Using a Remote Connection to the Library on page 76

Import the Key from a USB Device

Use the following steps to import a key stored on a USB device:

1. Plug the USB device containing the exported encryption key you want to import into a USB port on the LCM.
2. Access the encryption feature (see Log Into the Encryption Feature on page 31). The Encryption Configuration screen displays.



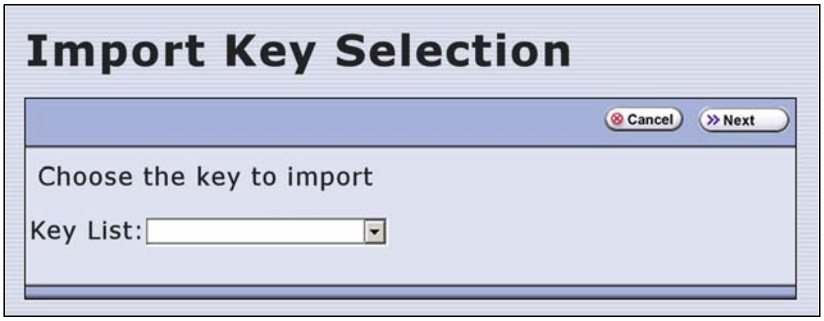
Encryption Configuration

No encryption keys exist

Figure 44 The Encryption Configuration screen.

3. From the Encryption Configuration screen, click **Import Key**. The Import Key Selection screen displays.

   Note: If you are accessing the library through the RLC, the Encryption Key Files Source screen displays instead of the Import Key Selection screen. Select **Import key from USB** and then click **Next**.



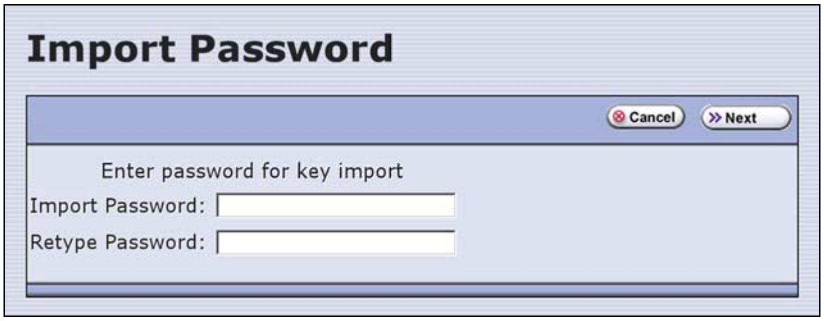
Import Key Selection

Choose the key to import

Key List:

Figure 45 The Import Key Selection screen.

4. Choose the key to import from the **Key List** drop-down list and then click **Next**. The Import Password screen displays.



Enter password for key import

Import Password:

Retype Password:

Figure 46 The Import Password screen.

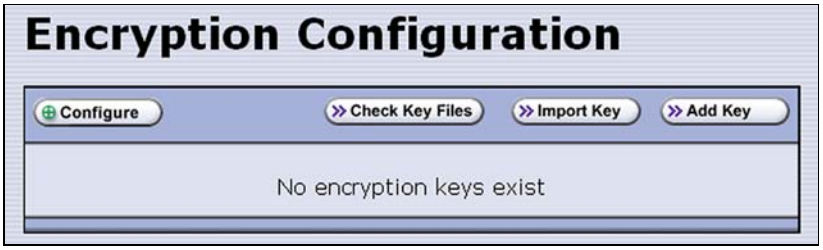
5. Type and retype the password that was used to encrypt the key file when it was exported (see Export the Encryption Key on page 67) and click **Next**.
6. When the key import is complete, the Encryption Configuration screen displays, showing the moniker of the newly imported key (see Figure 37 on page 63).
7. Assign the imported key to the partition which contains the encrypted cartridge (see Assigning an Encryption Key to a Partition on page 64).
8. Use your storage management software to restore the data.

Import the Key Using a Remote Connection to the Library

Use the following steps to import a key from a remote computer using the library's BlueScale web interface (RLC).

Notes:
- The option to import a key from a remote computer is only available if you are accessing the library using the BlueScale web interface.
- The key must be accessible to the computer you are using to access the library's BlueScale web interface.

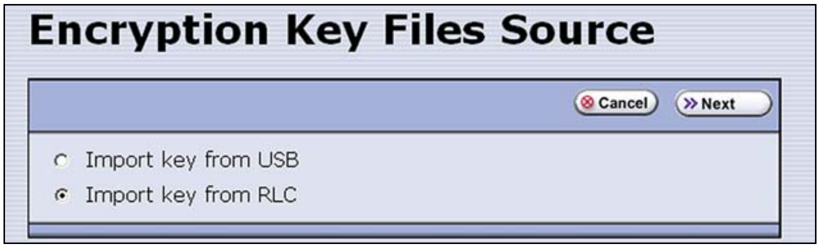
1. Access the encryption feature (see Log Into the Encryption Feature on page 31). The Encryption Configuration screen displays.



No encryption keys exist

Figure 47 The Encryption Configuration screen.

2. From the Encryption Configuration screen, click **Import Key**. The Encryption Key Files Source screen displays.



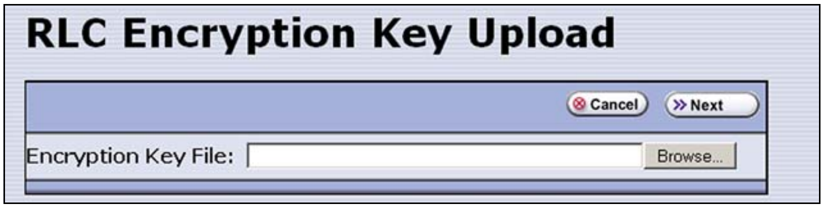
Encryption Key Files Source

○ Import key from USB

● Import key from RLC

Figure 48 The Encryption Key Files Source screen.

3. Select **Import key from RLC** and then click **Next**. The RLC Encryption Key Upload screen displays.



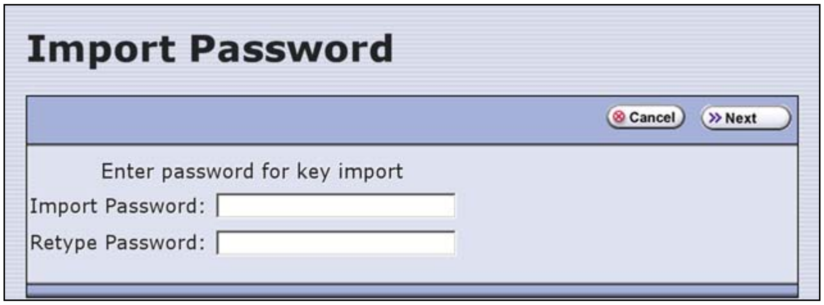
RLC Encryption Key Upload

Encryption Key File:

Figure 49 The RLC Encryption Key Upload screen.

4. To enter the name of the key file to import:
   - Type in the full path and file name in the **Encryption Key File** field.

     —OR—
   - Click **Browse**. In the File Upload screen, browse to the location where the key is stored, select the key file and then click **Open**. The path and filename for the key display in the **Encryption Key File** field.
5. Click **Next**. The Import Password screen displays.



Import Password

Enter password for key import

Import Password:

Retype Password:

Figure 50 The Import Password screen.

6. Type and retype the password used to encrypt the key file when it was exported (see Export the Encryption Key on page 67). Click **Next**. The Encryption Configuration screen displays, showing the moniker of the newly imported key (see Figure 37 on page 63).
7. Assign the imported key to the partition containing the encrypted cartridge (see Assigning an Encryption Key to a Partition on page 64).
8. Use your storage management software to restore the data.

Deleting an Encryption Key from the Library

Overview BlueScale Encryption Standard Edition only supports storing a single encryption key in the library. You must first delete the key currently stored in the library before you can create or import a new key and assign it to one or more partitions.

Caution Make sure that you export a copy of the existing key before you delete it. You need a copy of the exported key and its password to import the key back into the library and restore data that was encrypted with the key.

Important Backup files of the library configuration include any encryption keys that were stored in the library at the time the file was created.

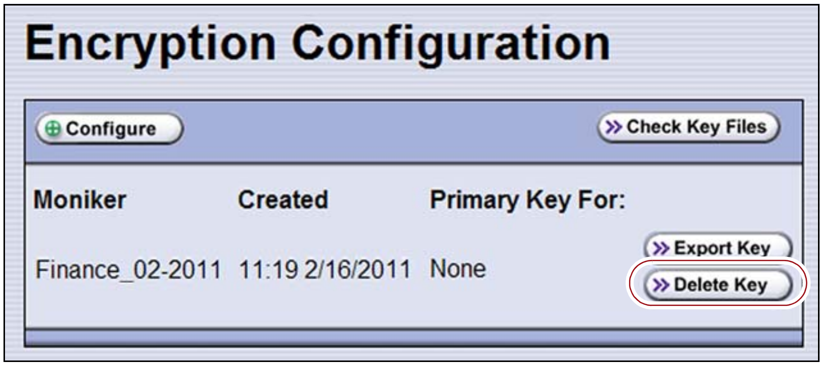
Use the following steps to delete a key:

1. Access the encryption feature (see Log Into the Encryption Feature on page 31).
2. Export at least one copy of the key and store it in a safe location (see Export the Encryption Key on page 67).
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 page 79).

   Note: If you delete an encryption key that is assigned to a partition you are not able to encrypt or decrypt data in that partition until you reimport the key.

4. From the Encryption Configuration screen, click **Delete Key** next to the key you want to remove from the library.

   Note: There is no confirmation screen. As soon as you click **Delete Key**, the library deletes the key.



Moniker	Created	Primary Key For:
Finance_02-2011	11:19 2/16/2011	None

Figure 51 Click **Delete Key** to remove the key from the library.

5. The Encryption Configuration screen redisplays with a message indicating that the key was successfully deleted. The moniker is no longer listed on the screen.

Disabling Encryption in a Partition

Use the following steps to disable encryption in a partition:

Note: If you are not already logged in as an encryption user, you must enter the encryption password before you create or edit a partition using the BlueScale partition wizard.

1. Access the encryption feature (see Log Into the Encryption Feature on page 31).
2. Select **Configuration ⇢ Partitions**. The Shared Library Services screen displays.
3. Select the partition for which you want to disable encryption and click **Edit**.
4. Click **Next** to navigate through the partition wizard screens until you reach the Encryption screen (see Figure 38 on page 65).
5. Select the **No Encryption** radio button.
6. Click **Next** to navigate through the remaining partition configuration screens.
7. When you reach the Save Partition screen, click **Save**.

Note: Any tapes in the partition that contain encrypted data cannot be read or used for new data unless encryption is re-enabled or the tapes are recycled. See Recycling Encrypted Media on page 104.

CHAPTER 5

Using BlueScale Encryption Professional Edition

This chapter describes configuring and using BlueScale Encryption Key Management — Professional Edition.

- If you are using Spectra SKLM Encryption Key Management, see Chapter 2 – Using Spectra SKLM Encryption Key Management, beginning on page 35.
- If you are using KMIP Encryption Key Management, see Chapter 3 – Using KMIP Encryption Key Management, beginning on page 44.
- If you are using BlueScale Encryption — Standard Edition, see Chapter 4 – Using BlueScale Encryption Standard Edition, beginning on page 61.

CONFIGURING BLUESCALE ENCRYPTION PROFESSIONAL EDITION

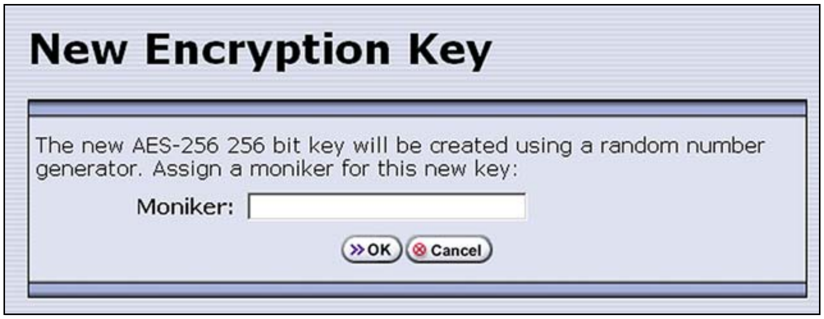
Overview BlueScale encryption key management configuration entails selecting an encryption startup mode, creating an encryption password, creating and using encryption keys, and designating one or more partitions as encryption-enabled. The encryption passwords let superusers access the encryption features. After encryption is enabled, data is automatically encrypted as it is written to tape in any partition that is encryption-enabled. See Standard Edition vs. Professional Edition on page 20 for a description of the differences between BlueScale Encryption Standard Edition and Professional Edition.

⚠ **Caution** The BlueScale encryption feature password is separate from the password used to log into the library. Make sure you keep a record of this password. If you lose this password, you are not able to configure encryption nor are you able to import/ export encryption keys that were already assigned and used on encrypted tapes.

User Privilege Requirements Only users with superuser privileges can access and use the BlueScale encryption features.

Create an Encryption Key

1. Access the encryption feature (see Log Into the Encryption Feature on page 31).
2. On the Encryption Configuration screen, click **Add Key**. The New Encryption Key screen displays.



New Encryption Key

The new AES-256 256 bit key will be created using a random number generator. Assign a moniker for this new key:

Moniker:

Figure 52 Enter a unique moniker to create a new encryption key.

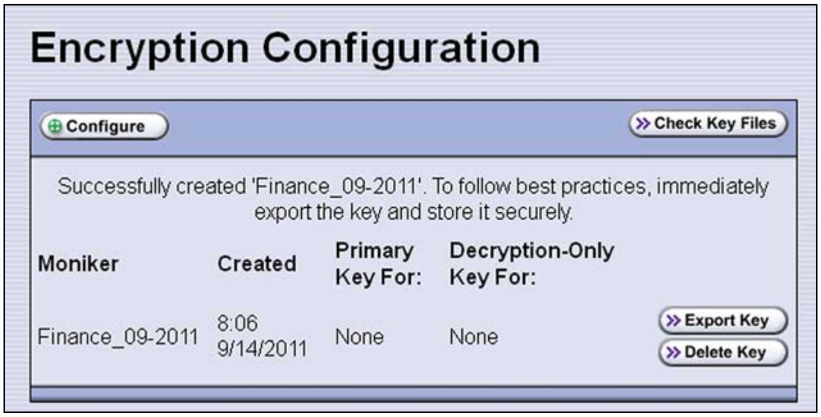
3. Enter a name for the encryption key in the **Moniker** field. Make sure that the moniker meets the following requirements:
   - A moniker can be any combination of the numbers **0–9**, lower and upper case alphabetic characters (**a–z** and **A–Z**), and the at symbol (**@**), dash (**–**), underscore (**_**), and period (**.**) characters. 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.

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

4. Click **OK**. The Encryption Configuration screen displays with a confirmation showing the moniker for the newly created encryption key and a message reminding you to create a copy of the key for safekeeping.

   Note: If the key is not yet assigned to a partition, **None** displays in the **Primary Key For** column.



Encryption Configuration

Successfully created 'Finance_09-2011'. To follow best practices, immediately export the key and store it securely.

Moniker	Created	Primary Key For:	Decryption-Only Key For:	
Finance_09-2011	8:06 9/14/2011	None	None	Export Key Delete Key

Figure 53 The encryption key currently stored in the library.

5. Export the newly created encryption key and save it to a secure location (see Exporting and Protecting Encryption Keys on page 86).

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 86 for additional information.

Assigning an Encryption Key to a Partition

Overview After creating an encryption key, you can assign it to one or more partitions. The encryption choices available for a partition depend on the hardware assigned to the partition.

Notes:

- The Encryption screen in the partition wizard lets you enable the encryption features for the partition. Depending on the version of BlueScale software, the Encryption screen does not display, or displays with all options grayed out, unless you are logged into the library as an encryption user and have either created one or more BlueScale encryption keys, or configured a Spectra SKLM or KMIP server. See Create an Encryption Key on page 62 for more information.
- F-QIPs are no longer available for purchase. If your library does not already contain an encryption-capable F-QIP, you must use drive-based encryption.
- By default, LTO drives are configured to compress data. If necessary, use your storage management software to modify the drive property settings to turn off compression.
- The encryption performed by encryption-enabled drives is not compatible with the encryption performed by an encryption-enabled F-QIP.
- Spectra SKLM key management is not compatible with BlueScale Encryption key management. Data encrypted using Spectra SKLM key management cannot be decrypted using BlueScale Encryption key management, and vice versa.
- If a partition uses both an encryption-enabled F-QIP and encryption-enabled drives, you must choose one type of encryption or the other. You cannot use both types in the same partition.

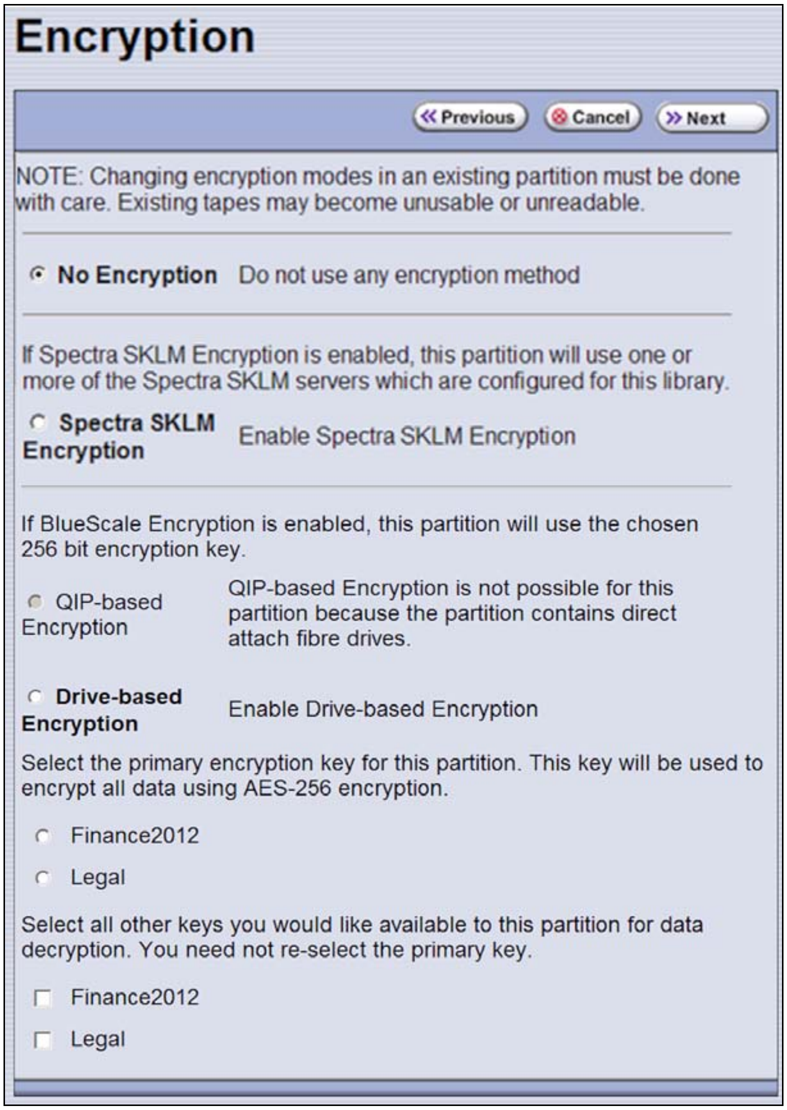
Use the following steps to assign a key to a partition and encrypt all data sent to the partition:

1. Access the encryption feature (see Log Into the Encryption Feature on page 31).

   Note: If you are not already logged in as an encryption user, you must enter the encryption password before you create or edit a partition using the BlueScale partition wizard.

2. Select **Configuration** ···› **Partitions**. The Shared Library Services screen displays.
3. Click **New** to create a partition, or click **Edit** to modify the settings for an existing partition (see “Creating a Storage Partition” in your *Tape Library User Guide* for more information about creating or editing partitions).

4. Proceed through the partition wizard until you reach the Encryption screen.



NOTE: Changing encryption modes in an existing partition must be done with care. Existing tapes may become unusable or unreadable.

● **No Encryption** Do not use any encryption method

If Spectra SKLM Encryption is enabled, this partition will use one or more of the Spectra SKLM servers which are configured for this library.

○ **Spectra SKLM Encryption** Enable Spectra SKLM Encryption

If BlueScale Encryption is enabled, this partition will use the chosen 256 bit encryption key.

○ QIP-based Encryption QIP-based Encryption is not possible for this partition because the partition contains direct attach fibre drives.

○ **Drive-based Encryption** Enable Drive-based Encryption

Select the primary encryption key for this partition. This key will be used to encrypt all data using AES-256 encryption.

○ Finance2012

○ Legal

Select all other keys you would like available to this partition for data decryption. You need not re-select the primary key.

□ Finance2012

□ Legal

Figure 54 The Encryption screen.

5. Choose the type of encryption to use.

Encryption Option	Description
No Encryption	Turns off encryption. All subsequent data written to tapes in this partition is not encrypted. Any tapes previously written using encryption remain encrypted.
Spectra SKLM Encryption or KMIP Encryption	Only displays if a Spectra SKLM or KMIP encryption server is configured. **Note:** See Using Spectra SKLM Encryption Key Management on page 35 or Using KMIP Encryption Key Management on page 44 for more information.

Encryption Option	Description
BlueScale Encryption: QIP-based	Turns on BlueScale encryption using F-QIP-attached, SCSI LTO-2, LTO-3, or LTO-4 drives. The F-QIP encrypts data using the specified encryption key before it is sent to the drive. If you select QIP-based Encryption, optionally select **Enable Clear File at BOT**. If you choose this option, the tape headers are unencrypted so that any compatible drive can read the header information on an encrypted tape including the moniker assigned to the encryption key. Using unencrypted headers facilitates key management for sites with a large number of encrypted tapes.
BlueScale Encryption: Drive-based	Turns on BlueScale encryption using direct-attached LTO-4 and later generation drives. The encryption-enabled drives encrypt data using the specified encryption key. If only one key is present, it is selected automatically. If multiple keys are listed, select the key you want to use.

6. If there is only one key in the library, skip to Step 7.

   If there are multiple encryption keys in the library, use the following steps to configure encryption and decryption for the partition.

   a. Select the primary key for the partition. This key is used when encrypting and decrypting data.

   Notes:
   - Only one key can be assigned as the primary encryption key.
   - With drive-based encryption, only one encryption key is allowed per tape. If you associate a different encryption key with a partition, you must first recycle tapes encrypted with the previous key to re-use them. Refer to Chapter 6 – Recycling Encrypted Media, beginning on page 104 for more information.

   b. Select none, one, or multiple additional keys to be associated with this partition for decrypting data.

   Notes:
   - The additional keys are only used for decrypting data. Having additional keys associated with the partition makes it possible to decrypt data encrypted with those keys even if the primary key for the partition is different.
   - You do not need to reselect the primary key.
   - A single partition can have a maximum of eight decryption keys assigned to it.

7. Click **Next** to move to the next partition configuration screen. Proceed through the remaining partition configuration screens.

8. When you reach the Save Partition screen, click **Save**. All data sent to this partition is encrypted using the key you selected.

9. Access the encryption feature (Accessing the Encryption Feature on page 31) and confirm that the listed keys reflect the assignments you just completed.

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.

Caution Data cannot be recovered without the encryption key used to encrypt the data, so protecting encryption keys is extremely important to data decryption and recovery. To decrypt and restore encrypted data, you need the data, the encryption key, and the encryption key password used to protect the exported key and data.

Important Backup files of the library configuration include any encryption keys that were stored in the library at the time the file was created.

Best Practice Spectra Logic recommends that you export each encryption key to at least two different USB devices and store them in separate locations. Remember, lost encryption keys cannot be recreated; keep them as secure (and as backed up) as your data.

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

Although emailing encryption keys is supported by the library, using email presents security issues, including the following:

- Copies of encryption keys may be left on the email servers used for sending and receiving email and are thus subject to compromise.
- The difficulty in verifying where all of the copies of emailed encryption keys may be located can make security audits more challenging.

Key Protection Features of Encryption Professional

Three Passwords to Access Export and Import Key Functions If you enabled Multi-User mode when you configured the encryption feature, you must enter two of the three encryption passwords in order to export keys from the library. See Configure the User Mode (BlueScale Encryption Professional Only) on page 32 for information about enabling Multi-User mode and configuring the library to support multiple encryption passwords.

Export as M-of-N Shares If desired, you can choose to split an encryption key into multiple files (M-of-N shares) when you export it. During the export process, you choose the a total number of shares (N) to split the key into and the subset of those shares (M) required to import the encrypted key file into the library. Depending on your site requirement, you can choose one of the following options for your M-of-N shares:

- 2-of-3
- 2-of-4
- 3-of-4
- 2-of-5
- 3-of-5
- 4-of-5

Each of the shares is then copied to a separate USB device or sent to a separate mail recipient. See Step 4 on page 89 for information on how to enable the M-of-N shares option when exporting a key.

Requirements for Exporting Keys as M-of-N Shares If you want to export the encryption key as M-of-N shares, you must meet the following requirements.

- If you choose to export the key to USB, you need a separate USB device for each share. The shares are copied to the USB devices one after the other.
- If you choose to email the key, you must select different, previously configured mail users to receive the shares. Each recipient receives one share as an email attachment.
- Although you can email shares when exporting the key, the only way to import shares of a key is to use USB devices.

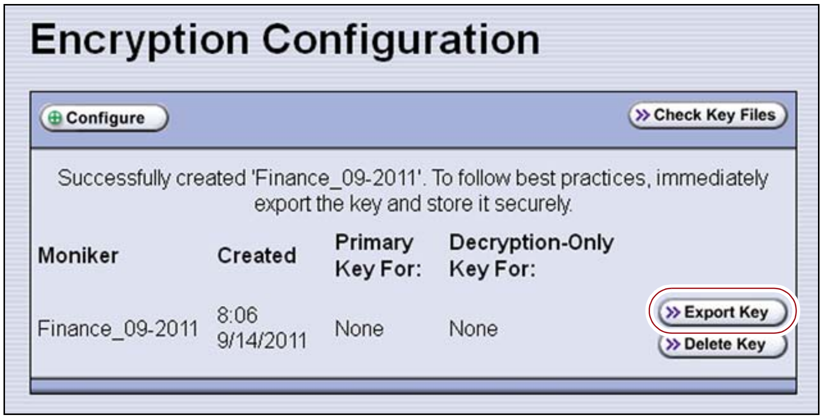
For example, if you choose the 2-of-3 option, then the encrypted key, which is further protected by a key-specific password, is split into three shares. Each share is then copied to a separate USB device or sent as an email attachment.

Keys that are split into shares can only be imported from USB devices; they cannot be uploaded through the BlueScale web interface. If the shares were sent as email attachments, they must be copied to separate USB devices in order to import the key. Building on the previous example, this means that two of the three USB devices, along with the encryption key password, are needed to import the key.

Export an Encryption Key

Use the following steps to export the current encryption key:

1. Access the encryption feature (see Log Into the Encryption Feature on page 31).
2. If you want to export the encryption key to one or more USB devices, plug a USB device into a USB port on the LCM before continuing.
3. From the Encryption Configuration screen, click **Export Key**.



Encryption Configuration

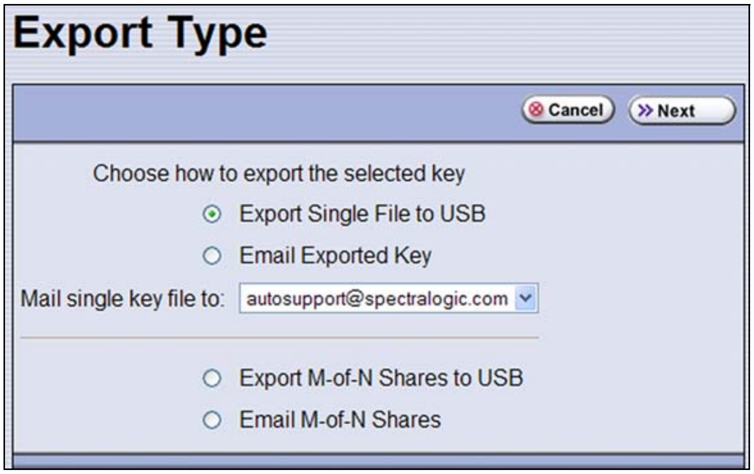
Successfully created 'Finance_09-2011'. To follow best practices, immediately export the key and store it securely.

Moniker	Created	Primary Key For:	Decryption-Only Key For:
Finance_09-2011	8:06 9/14/2011	None	None

Figure 55 Click **Export Key** to begin the key export process.

- If you selected Multi-User mode and you did not previously enter a second encryption user password, you are prompted to enter another password. Enter one of the encryption user passwords that you did not use during the initial login and then click **Next**. The Export Type screen displays.

4. On the Export Type screen, select the desired export option.



Export Type

Choose how to export the selected key

● Export Single File to USB

○ Email Exported Key

Mail single key file to: autosupport@spectralogic.com

○ Export M-of-N Shares to USB

○ Email M-of-N Shares

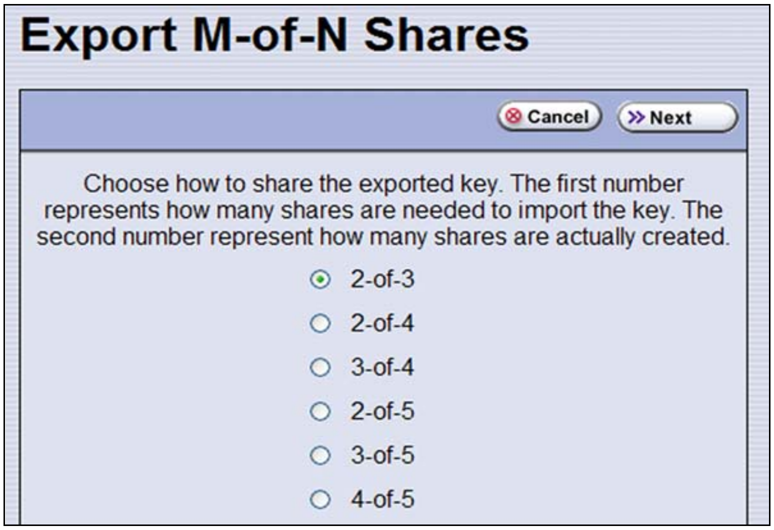
Figure 56 Choose the method for exporting the key.

Export Type	Description
Export Single File to USB	Saves the exported encryption key to the USB device connected to the LCM.
Email Exported Key	Sends the encryption key as an email attachment to a previously configured mail recipient (see Configure Mail Users in your *Tape Library User Guide*). Use the **Mail single key file to:** drop-down list to select the desired recipient. **Note:** Do not use the default autosupport@spectralogic.com email recipient. Spectra Logic does not save emailed files unless they are specifically requested for troubleshooting.
Export M-of-N Shares to USB	Divides the exported key into multiple shares, with each share saved to a separate USB device. When you select this option, you need a separate USB device for each share (N). **Note:** Refer to Export as M-of-N Shares on page 87 for more information about using this option.
Email M-of-N Shares	Divides the exported key into multiple shares, with each share sent as an email attachment to a separate, previously configured mail recipient. **Note:** Refer to Export as M-of-N Shares on page 87 for more information about using this option.

5. If you did not select one of the M-of-N options, continue with Step 6.

   If you selected one of the M-of-N options, use the following steps to configure the shares.

   a. Click **Next**. The Export M-of-N Shares screen displays.



Export M-of-N Shares

Choose how to share the exported key. The first number represents how many shares are needed to import the key. The second number represent how many shares are actually created.

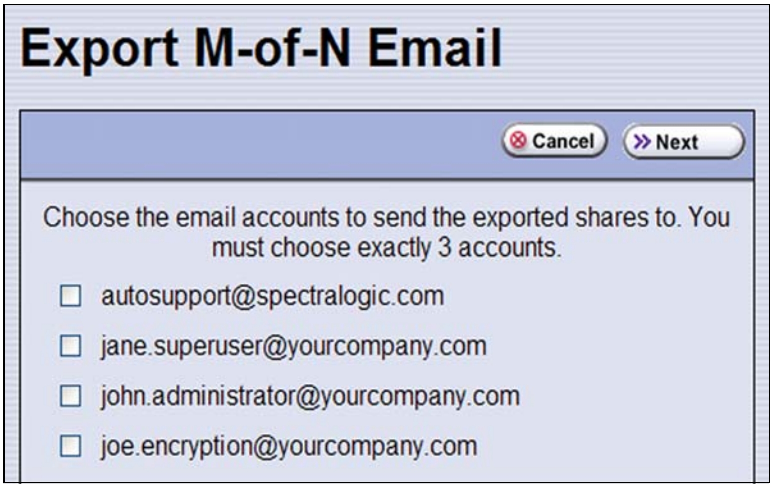
● 2-of-3
○ 2-of-4
○ 3-of-4
○ 2-of-5
○ 3-of-5
○ 4-of-5

Figure 57 Select the desired M-of-N option.

   b. Select the desired M-of-N option, where **M** is the minimum number of shares required to import the encryption key and **N** is the total number of shares to be created.

   c. If you chose to export the shares to USB, continue with Step 6.

   If you chose to email the shares, click **Next**. The Export M-of-N Email screen displays.



Export M-of-N Email

Choose the email accounts to send the exported shares to. You must choose exactly 3 accounts.

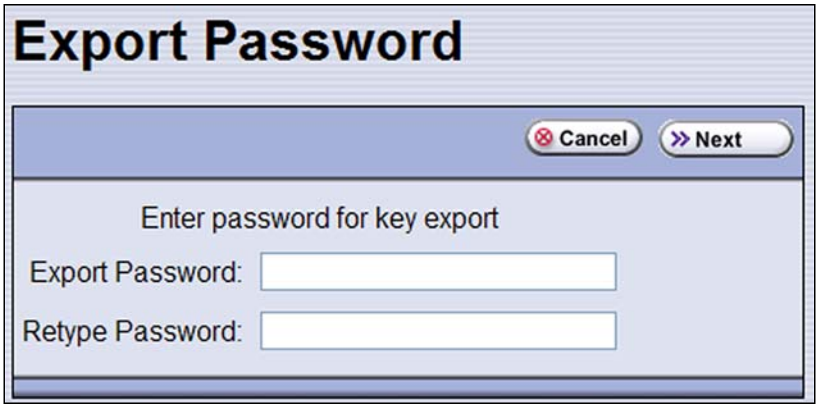
□ autosupport@spectralogic.com
□ jane.superuser@yourcompany.com
□ john.administrator@yourcompany.com
□ joe.encryption@yourcompany.com

Figure 58 Select the mail recipients.

   d. Select from the list of mail recipients; you must select the same number of email users as the total number of shares (N).

Note: Do not use the default autosupport@spectralogic.com email recipient. Spectra Logic does not save emailed files unless they are specifically requested for troubleshooting.

6. Click **Next**. The Export Password screen displays.



Export Password

Enter password for key export

Export Password:

Retype Password:

Figure 59 Enter and confirm a password for the exported encryption key.

7. Type and retype an export password using any combination of the numbers **0–9**, lower and upper case alphabetic characters (**a–z** and **A–Z**), and the at symbol (**@**), dash (**–**), underscore (**_**), and period (**.**) characters. This key is used to encrypt the exported key.

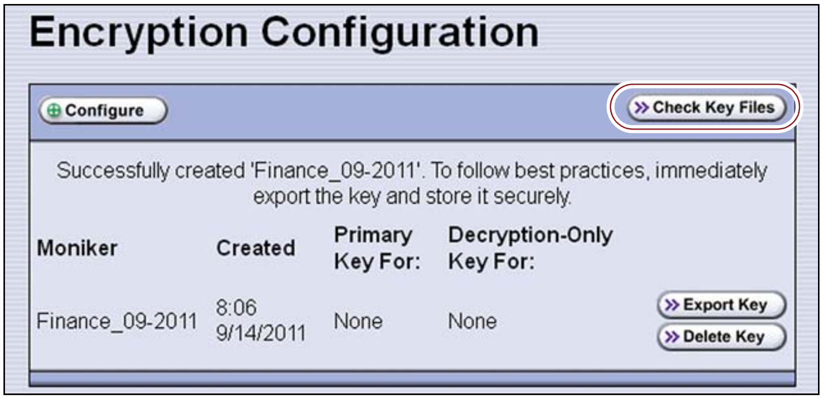
8. Make a record of the encryption key password; you need it in order to import the key back into the library. Without the password, you cannot import the key, and the data encrypted using the key is inaccessible.

Caution Do not lose the encryption key password. Without it, you cannot reimport an encryption key after it is deleted from the library, and the data encrypted using the key is inaccessible.

9. Click **Next** to export the key to the selected location. If you selected the option to split the key across M-of-N shares on multiple USB devices, remove the USB device from the LCM when you are prompted to do so and insert another USB device.

10. Confirm that the encryption key was correctly exported.

- **If you exported the encryption key to a USB device**—Immediately confirm that the encrypted key copied correctly by clicking **Check Key Files** and following any prompts. If desired, save or print the Check Key Files report for an audit record showing that the USB device was readable, and that the destination key matched the source key. Use the steps in Verify the Exported Encryption Key to provide a second confirmation.



Encryption Configuration

Successfully created 'Finance_09-2011'. To follow best practices, immediately export the key and store it securely.

Moniker	Created	Primary Key For:	Decryption-Only Key For:	
Finance_09-2011	8:06 9/14/2011	None	None	Export Key Delete Key

Figure 60 Use **Check Key Files** to confirm successful export.

If the confirmation indicates the key did not copy correctly, delete all data from the USB device(s) so that no trace of the failed export file remains. Then, export the key again using a different USB device or set of USB devices, beginning with Step 3 on page 88.

- **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 page 93.

Verify the Exported Encryption Key

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

When Saved to a USB Device

1. Plug the USB device into a computer and verify the following:
   - That it contains a file called `name.bsk` if you exported the key as a single file, or `name.bss` if you exported the key as a share, where `name` is the moniker you assigned to the key when it was created
   - That the file is more than 0 bytes in size

   If the file meets these requirements, the encryption key or share was successfully exported and is usable.

   If the file does not exist or is 0 bytes in size, the encryption key or share did not copy correctly. Delete all data from the USB device (all USB devices if a share did not copy correctly) so that no trace of the failed export file remains. Then, export the key again beginning with Step 3 on page 88. Do not use the USB device that failed the verification.
2. 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.
3. Store the USB device in a safe location.
4. If you exported the key as M-of-N shares, repeat Step 1 through Step 3 for each additional USB device.

When Sent as an Email Attachment

1. Open the email attachment and verify the following:
   - That it contains a file called `name.bsk` if you exported the key as a single file, or `name.bss` if you exported the key as a share, where `name` is the moniker you assigned to the key when it was created
   - That the file is more than 0 bytes in size.

   If the file meets these requirements, the encryption key or share was successfully exported and is usable.

   If the file does not exist or is 0 bytes in size, the encryption key or share did not copy correctly. Export the key again beginning with Export an Encryption Key on page 88.
2. 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.
3. Save the email attachment to a safe location from which you can copy it to a USB device, if needed.
4. If you exported the key as M-of-N shares, each share recipient must perform Step 1 through Step 3 for each emailed share.

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 need 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 cannot import the encryption key.

Important Backup files of the library configuration include any encryption keys that were stored in the library at the time the file was created.

The following guidelines outline the essential tasks required to protect encryption keys:

- Save one or more copies of every key using the Key Export option on the Encryption Configuration screen (see Export an Encryption Key on page 88).

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

Although emailing encryption keys is supported by the library, doing so presents security issues, including the following:

- Copies of encryption keys may be left on the email servers used for sending and receiving email and are thus subject to compromise.
- The difficulty in verifying where all the copies of emailed encryption keys may be located can make security audits more challenging.

- If you choose to store only a single copy of an encryption key make sure that you keep the copy secure. If something happens to the device where you stored the exported key and the key was deleted from the library, both the key and all data encrypted using the key are unrecoverable.

Caution **To emphasize:** If you lose the encryption key or the password for the exported file, your data is **unrecoverable** if the key was deleted from the library. You need to balance the number of copies of the key to store to guarantee access to the encrypted data against the security risk associated with storing multiple keys. Make sure that the key 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 97.

  You may want to make two copies of a key, storing each in a secure location. Keep a record of each key's location so that you can easily find the key when you need to restore or delete data.
- Maintain a list of every password associated with each key and securely store the list. Never keep this list as cleartext (unencrypted text) on a networked computer, or send it through email as cleartext. For added security, encrypt the file containing the list of passwords.
- Track every copy of each key. This tracking is critical in order to meet requirements that may govern data retention and data destruction. Destroying all exported copies of keys associated with encrypted data AND deleting the keys from the library is sufficient to satisfy data destruction requirements, since encrypted data cannot be accessed without the key used to encrypt it.

  Spectra Logic recommends tracking the information listed in the following table for every key that you create. For added security, encrypt the file containing the tracking information.

Key moniker:	
Number of shares (if any):	
Number of key copies:	
Location of each copy:	
Password(s) associated with exported copy of the moniker:	
Location of cartridges containing data 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 data partition containing the encrypted tape, the data is automatically decrypted as it is read from tape; if the encryption key is not currently stored on the library, it must be imported before the data can be decrypted. Once the required encryption key is assigned to the partition, standard restore procedures are unchanged.

Three Passwords to Access Import Key Functions If you enabled Multi-User mode, two of the three encryption passwords are required to access the import key function. See Configure the User Mode (BlueScale Encryption Professional Only) on page 32 for information about enabling Multi-User mode and configuring the library to support multiple encryption passwords.

Requirements for Importing Keys Split into M-of-N Shares If you exported the encryption key as M-of-N shares, then M shares are required to import the encryption key into the library. See Export as M-of-N Shares on page 87 for information about using the M-of-N shares option.

Keys that were split into shares can only be imported from USB devices; they cannot be uploaded through the BlueScale web interface. If the shares were sent as email attachments, each share must be copied to a separate USB device in order to import the key.

For example, if you chose the 2-of-3 option and exported the key to USB devices, two of the three USB devices, along with the encryption key password, are needed to import the key.

Use a Key Stored in the Library

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 key currently stored in the library, the library prompts you with the moniker of the key that is required to decrypt the data. You must import the key as described in Import the Required Key Into the Library on page 97 before the data can be restored.

If the encryption key is not currently assigned to the partition, modify the partition as described in Assigning an Encryption Key to a Partition on page 83. If the encryption key is assigned to a partition, continue with the following steps.

1. If you selected Secure Initialization (see Configure Secure Initialization Mode (BlueScale Encryption Only) on page 33), and no encryption user logged in since the last time the library was initialized, access the encryption feature (see Log Into the Encryption Feature on page 31).
2. If necessary, import the cartridges containing the data to be restored into the library partition to which the encryption key is assigned.

   Note: If you assigned the required key to the partition as an additional key, you do not need to modify the partition to make the key primary.
3. 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.

As described in the following sections, you can import the encryption key from a USB device or from a remote computer through the library's BlueScale web interface.

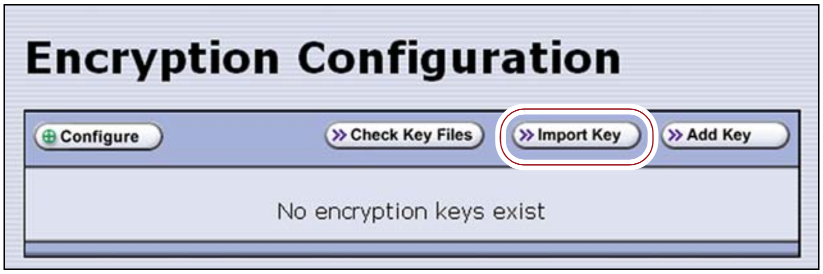
Important You cannot import a key that was exported using M-of-N shares using the BlueScale web interface. You must use multiple USB devices to import the key. If the shares of the encrypted key were distributed as email attachments, the required number of shares (M) must be copied to separate USB devices before the key can be imported and used to decrypt and restore data.

- Import the Key from a USB Device on page 98
- Import the Key Using a Remote Connection to the Library on page 100

Import the Key from a USB Device

Use the following steps to import a key stored on a USB device:

1. Access the encryption feature (see Log Into the Encryption Feature on page 31). The Encryption Configuration screen displays.



Encryption Configuration

No encryption keys exist

Figure 61 The Encryption Configuration screen.

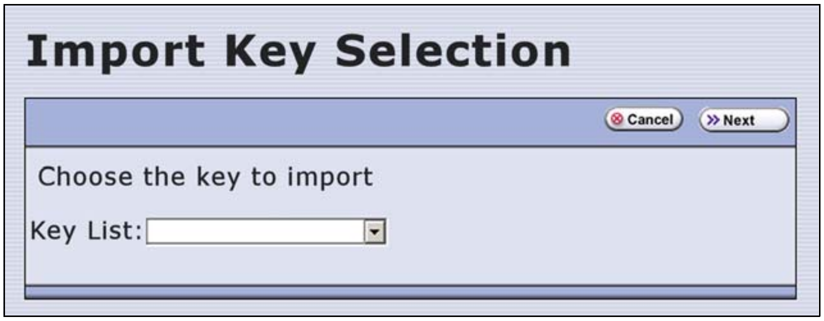
2. Plug the USB device containing the exported encryption key you want to import into a USB port on the LCM.

   Note: If you exported the key as M-of-N shares, you need the required number shares (M) available on separate USB devices. Plug in only one USB device.

3. From the Encryption Configuration screen, click **Import Key**.

   - If you selected Multi-User mode and you did not previously enter a second encryption user password, you are prompted to enter another password. Enter one of the encryption user passwords that you did not use during the initial login and then click **Next**. The Import Key Selection screen displays.
   - Otherwise, the Import Key Selection screen displays immediately.

   Note: If you are accessing the library through the RLC, the Encryption Key Files Source screen displays instead of the Import Key Selection screen (see Figure 65 on page 100). Select **Import key from USB** and then click **Next**.



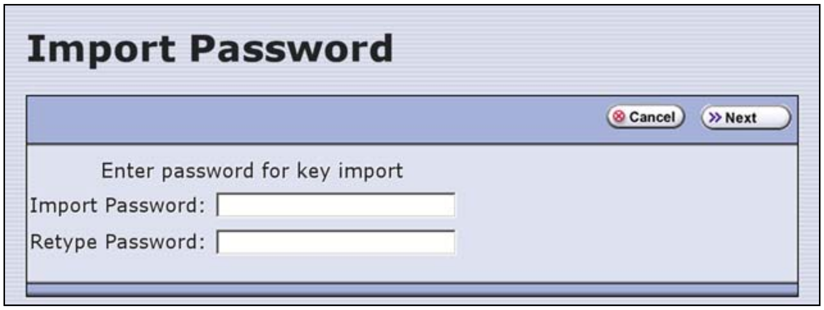
Import Key Selection

Choose the key to import

Key List:

Figure 62 The Import Key Selection screen.

4. Choose the key to import from the **Key List** drop-down list and then click **Next**. The Import Password screen displays.



Import Password

Enter password for key import

Import Password:

Retype Password:

Figure 63 The Import Password screen.

5. Type and retype the password that was used to encrypt the key file when it was exported (see Export an Encryption Key on page 88) and click **Next**.

   If you are importing a key that was exported as M-of-N shares, connect each of the required UBS drives, one after the other, when prompted. For each share, type and retype the password that was used to encrypt the key file when it was exported.

6. When the key import is complete, the Encryption Configuration screen displays, showing the moniker of the newly imported key (see Figure 53 on page 82).

7. Assign the imported key to the partition which contains the encrypted cartridge (see Assigning an Encryption Key to a Partition on page 83).

8. Use your storage management software to restore the data.

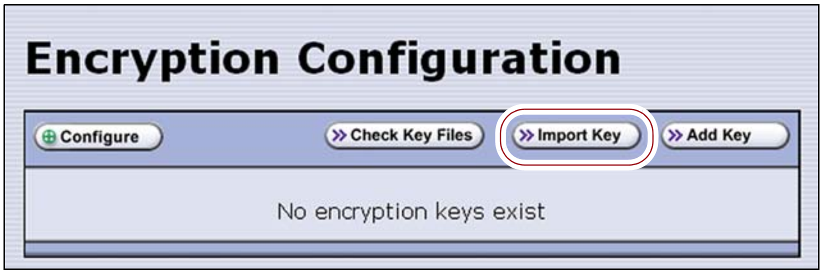
Import the Key Using a Remote Connection to the Library

Use the following steps to import a key from a remote computer using the library's BlueScale web interface (RLC).

Notes:

- The option to import a key from a remote computer is only available if you are accessing the library using the BlueScale web interface.
- The key must be accessible to the computer you are using to access the library's BlueScale web interface.
- Importing a key from a remote computer is not supported for keys that were split into M-of-N shares.

1. Access the encryption feature (see Log Into the Encryption Feature on page 31). The Encryption Configuration screen displays.

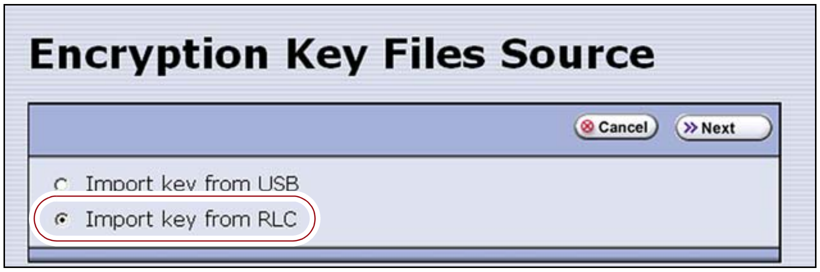


Encryption Configuration

No encryption keys exist

Figure 64 The Encryption Configuration screen.

2. From the Encryption Configuration screen, click **Import Key**.
   - If you selected Multi-User mode and you did not previously enter a second encryption user password, you are prompted to enter another password. Enter one of the encryption user passwords that you did not use during the initial login and then click **Next**. The Encryption Key Files Source screen displays.
   - Otherwise, the Encryption Key Files Source screen displays immediately.



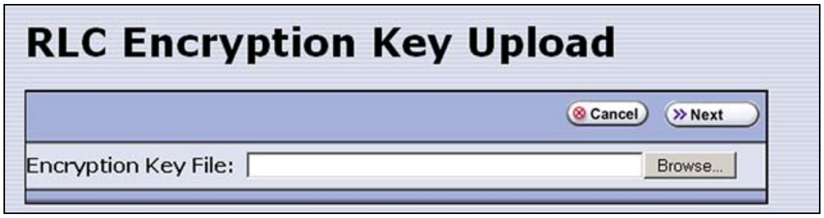
Encryption Key Files Source

○ Import key from USB

● Import key from RLC

Figure 65 The Encryption Key Files Source screen.

3. Select **Import key from RLC** and then click **Next**. The RLC Encryption Key Upload screen displays.



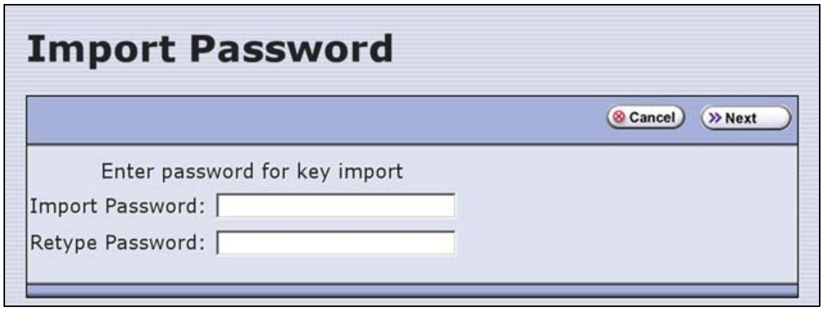
RLC Encryption Key Upload

Encryption Key File:

Figure 66 The RLC Encryption Key Upload screen.

4. To enter the name of the key file to import:
   - Type in the full path and file name in the **Encryption Key File** field.

     —OR—
   - Click **Browse**. In the File Upload screen, browse to the location where the key is stored, select the key file and then click **Open**. The path and filename for the key display in the **Encryption Key File** field.
5. Click **Next**. The Import Password screen displays.



Import Password

Enter password for key import

Import Password:

Retype Password:

Figure 67 The Import Password screen.

6. Type and retype the password used to encrypt the key file when it was exported (see Export an Encryption Key on page 88). Click **Next**. The Encryption Configuration screen displays, showing the moniker of the newly imported key (see Figure 53 on page 82).
7. Assign the imported key to the partition containing the encrypted cartridge (see Assigning an Encryption Key to a Partition on page 83).
8. Use your storage management software to restore the data.

Deleting an Encryption Key from the Library

Overview BlueScale Encryption Professional Edition supports storing up to 30 encryption keys in the library. If, in accordance with your key retirement policies, an encryption key can no longer be used, you can delete the key from the library.

Caution Make sure that you export a copy of the existing key before you delete it. You need a copy of the exported key and its password to import the key back into the library and restore data that was encrypted with the key.

Important Backup files of the library configuration include any encryption keys that were stored in the library at the time the file was created.

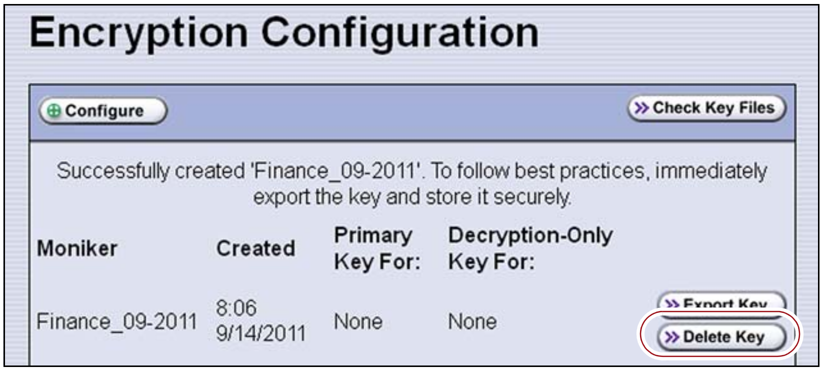
Use the following steps to delete a key:

1. Access the encryption feature (see Log Into the Encryption Feature on page 31).
2. Export at least one copy of the key and store it in a safe location (see Export an Encryption Key on page 88).
3. If the encryption key you plan to delete is assigned to a partition, either as the primary key or as a decryption-only key, edit the partition to disable encryption (see Disabling Encryption in a Partition on page 103 or assign a different key (see Assigning an Encryption Key to a Partition on page 83).

   Note: If you delete an encryption key that is assigned to a partition you are not able to encrypt or decrypt data in that partition until you reimport the key.

4. From the Encryption Configuration screen, click **Delete Key** next to the key you want to remove from the library.

   Note: There is no confirmation screen. As soon as you click **Delete Key**, the library deletes the key.



Successfully created 'Finance_09-2011'. To follow best practices, immediately export the key and store it securely.

Moniker	Created	Primary Key For:	Decryption-Only Key For:
Finance_09-2011	8:06 9/14/2011	None	None

Figure 68 Click **Delete Key** to remove the key from the library.

5. The Encryption Configuration screen redisplays with a message indicating that the key was successfully deleted. The moniker is no longer listed on the screen.

Disabling Encryption in a Partition

Use the following steps to disable encryption in a partition:

Note: If you are not logged in as an encryption user, you must enter the encryption password before you create or edit a partition using the BlueScale partition wizard.

1. Access the encryption feature (see Accessing the Encryption Feature on page 31).
2. Select **Configuration ⇢ Partitions**. The Shared Library Services screen displays.
3. Select the partition for which you want to disable encryption and click **Edit**.
4. Click **Next** to navigate through the partition wizard screens until you reach the Encryption screen (see Figure 54 on page 84).
5. Select the **No Encryption** radio button.
6. Click **Next** to navigate through the remaining partition configuration screens.
7. When you reach the Save Partition screen, click **Save**.

Note: Any tapes in the partition that contain encrypted data cannot be read or used for new data unless encryption is re-enabled or the tapes are recycled. See Recycling Encrypted Media on page 104.

CHAPTER 6

Recycling Encrypted Media

Overview Encryption-enabled LTO and TS11xx technology drives require that all data encrypted and written to a single cartridge use the same encryption key — that is, a single key is associated with all the encrypted data on an individual cartridge. If you want to change the encryption key associated with a cartridge that was encrypted using BlueScale Encryption or use the cartridge for non-encrypted data, you must first recycle the cartridge using the BlueScale Recycle Encryption Media feature. In addition, you must recycle the cartridge before you can re-use it if you lose the encryption key for the cartridge.

Recycle Encryption Media can also be used to erase the MAM attributes added to a cartridges by KMIP encryption. However, this is not necessary to reuse the tape.

⚠ **Caution** Any data on media selected for recycle is inaccessible and unrecoverable after Recycle Encrypted Media completes.

Notes:

- If you plan to use the same key that was used to encrypt the data already on the cartridge, you do not need to recycle the cartridge using the process described in this section.
- Make sure that the storage management software cannot access the drive you plan to use for recycling the encrypted media.
- The recycle media operation can only be performed from the library operator panel. You cannot access the Import/Export screen when using the BlueScale web interface from a remote computer.
- This feature is required for cartridges encrypted using BlueScale encryption and can be used to clear MAM attributes added to cartridges encrypted using KMIP encryption. It has no affect on cartridges encrypted using Spectra SKLM encryption.
- After recycling the tape, Spectra Logic recommends using your host software to erase the tape. MLM Health will show that the tape contains “Encrypted Data” until the tape is erased or overwritten.

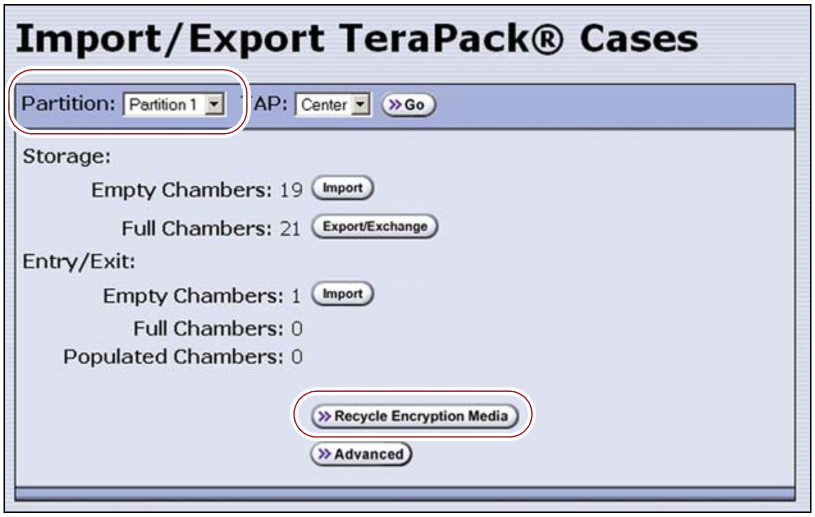
User Privilege Requirement Any user with operator privileges who is assigned to the partition and all users with superuser or administrator privileges can recycle encrypted cartridges. See your *Tape Library User Guide* for information about assigning users to a partition.

Requirements You cannot run backup or restore operations while the library is recycling encrypted cartridges. If there are a large number of cartridges to process, make sure that you wait until the library is idle.

Important For libraries that use one of the drives in the partition to provide the robotic control path, use your software to take the library off-line or stop all backup or restore operations to the partition before beginning the recycle process. Attempting to recycle media while the host is issuing commands to the library through the exporting drive may cause the backup or restore operation to fail.

Process Use the following steps to recycle one or more encrypted LTO cartridges so that they can be reused with a new encryption key.

1. From the operator panel, log into the library as a user with the appropriate privileges (see User Privilege Requirement on page 105).
2. Select **General ⇢ Import/Export**. The Import/Export screen displays showing the information for the last partition that was viewed on either the Import/Export screen or the Inventory screen.
3. Select the partition that contains the cartridges that you want to recycle from the **Partition** drop-down list and then click **Go**. The Import/Export screen refreshes to show the current status of the chambers assigned to the selected partition.



Import/Export TeraPack® Cases

Partition: Partition 1 AP: Center

Storage:

Empty Chambers: 19

Full Chambers: 21

Entry/Exit:

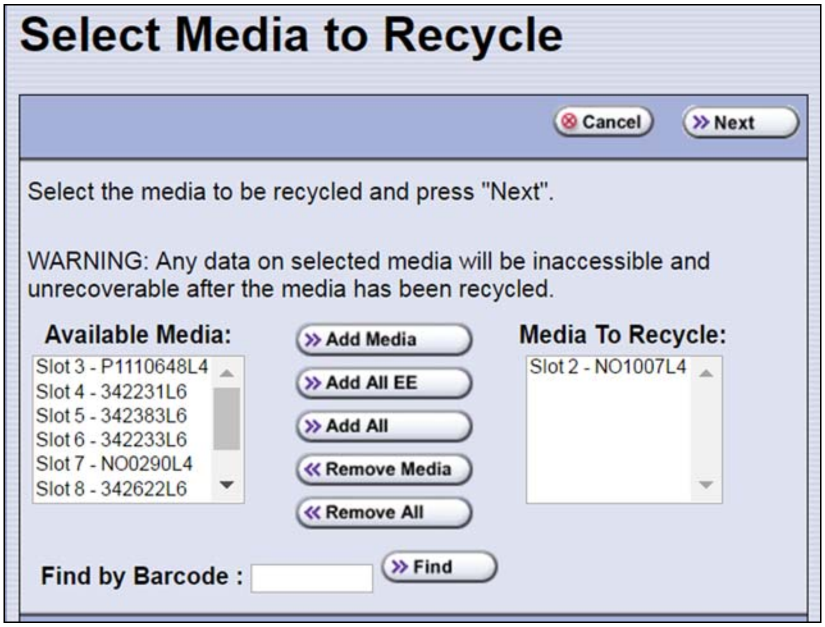
Empty Chambers: 1

Full Chambers: 0

Populated Chambers: 0

Figure 69 Choose the partition containing the cartridges to be recycled.

4. Click **Recycle Encryption Media**. The Select Media to Recycle screen displays.



Select Media to Recycle

Select the media to be recycled and press "Next".

WARNING: Any data on selected media will be inaccessible and unrecoverable after the media has been recycled.

Available Media:	Media To Recycle:
Slot 3 - P1110648L4	Slot 2 - NO1007L4
Slot 4 - 342231L6	
Slot 5 - 342383L6	
Slot 6 - 342233L6	
Slot 7 - NO0290L4	
Slot 8 - 342622L6	

Find by Barcode :

Figure 70 The Select Media to Recycle screen.

5. Select the cartridge to move into or out of the **Media To Recycle** list using the buttons described below.

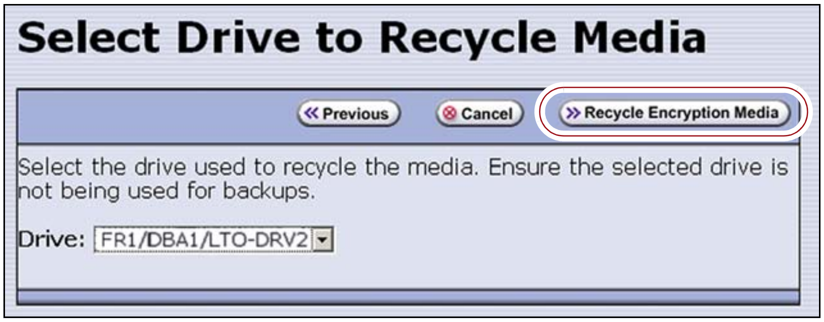
Notes:
- The **Available Media** list shows all of the cartridges currently in the partition, both encrypted and unencrypted.
- To narrow down the media choices in the **Available Media** list, enter a partial or entire barcode in the **Find by Barcode** field and select **Find**. The list displays only cartridges with barcodes that match the values that you entered.

Important

Important: When using **Find by Barcode**, the library only searches the slots below the top one displayed in the list. Scroll to the top of the source list before clicking **Find**. The search starts at the second visible slot.

Media to Recycle Button	Function
Add Media	Adds the cartridge currently selected in the **Available Media** list to the **Media To Recycle** list.
Add All EE	Adds all of the media currently in the entry/exit pool to the **Media To Recycle** list. This option is especially useful if you imported a large amount of encrypted media into the library entry/exit pool and want to recycle it before moving it into a partition.
Add All	Adds all of the cartridges in the **Available Media** list to the **Media To Recycle** list.
Remove Media	Removes the selected cartridge from the **Media To Recycle** list.
Remove All	Removes all of the cartridges from the **Media To Recycle** list.

6. Click **Next**. The Select Drive to Recycle Media screen displays.



Select Drive to Recycle Media

Select the drive used to recycle the media. Ensure the selected drive is not being used for backups.

Drive: FR1/DBA1/LTO-DRV2

Figure 71 The Select Drive to Recycle Media screen.

7. Select the drive that you want to use for recycling the cartridges from the **Drive** drop-down list and then click **Recycle Encryption Media** to begin the recycling operation.

   Note: Once the recycle operation starts, you cannot stop it and you cannot perform any other library operations until it is complete.

CHAPTER 7

Encryption Troubleshooting

This chapter describes troubleshooting steps you can take, as appropriate, to help resolve problems you might encounter while operating the library. Try these troubleshooting procedures *before* you open a support ticket with Spectra Logic Technical Support. If you are unable to resolve the problem yourself, open a support ticket. See "Opening a Support Ticket" in your *Tape Library User Guide* for instructions.

Note: The library must be under warranty or have a valid service contract in order to qualify for support.

TROUBLESHOOTING ENCRYPTION ISSUES

The information in this section may help resolve encryption-related problems.

Issue	Cause	Resolution
Library can not access the Spectra SKLM server.	The Spectra SKLM server's operating system firewall does not allow the library to access the server.	If you are setting up Spectra SKLM on a Windows server, create a firewall rule on the server to allow the library to access the server. Use the port setting assigned to the server during the BlueScale (library) portion of the Spectra SKLM server configuration. The default port setting is 3801. See Configure a Spectra SKLM Server on page 37 to determine your port setting.
System message states that "Load attempted while encryption is enabled, but no moniker or key list was sent to the DCM."	If a drive loses and regains power with a tape inside it, the drive is not able to receive encryption monikers.	Use the following steps to re-enable the encryption process: **1.** Move the cartridge out of the drive and return it to its storage location (see "Moving Cartridges Within a Partition" in your *Tape Library User Guide*). **2.** Reset the drive (see "Resetting a Drive" in your *Tape Library User Guide*).

Issue	Cause	Resolution
System message states that a tape drive requires a specific moniker.	The encryption key used to encrypt the cartridge is not currently available on the library. Or, if you are using BlueScale Professional Edition, the required encryption key is available, but is not selected as one of the partition's decryption keys.	Depending on which BlueScale Encryption edition you are using, use the following steps to enable the cartridge to be read: **BlueScale Standard Edition** **1.** Log into the library as a superuser. **2.** Log into the encryption feature. **3.** Export and then delete the encryption key currently listed on the Encryption Configuration screen (see Deleting an Encryption Key from the Library on page 78). **4.** Import the required key (see Import the Required Key Into the Library on page 74). **5.** Select **Configuration → Partitions.** **6.** Click **Edit** next to the partition containing the cartridge. **7.** Navigate through the BlueScale partition wizard to the Encryption screen. **8.** Select the encryption key to be associated with the partition. **9.** Proceed through the partition wizard until you reach the Save Partition screen, and click **Save**. **BlueScale Professional Edition** **1.** Log into the library as a superuser. **2.** Log into the encryption feature. **3.** Make sure the encryption key is listed on the Encryption Configuration screen. If it is not listed, add the key to the library (see Import the Required Key Into the Library on page 97). **4.** Select **Configuration → Partitions.** **5.** Click **Edit** next to the partition containing the cartridge. **6.** Navigate through the BlueScale partition wizard to the Encryption screen. **7.** Select the required encryption key as either the primary encryption key or as a decryption key. **8.** Proceed through the partition wizard until you reach the Save Partition screen, and click **Save**.

INDEX