



SPECTRA LUMOS ENCRYPTION GUIDE

SpectraLogic.com

TABLE OF CONTENTS

Contacting Spectra Logic	9
Related Information	10
About This Guide	12
Intended Audience	12
Chapter 1 - Encryption Overview and Strategies	13
Encryption Overview	14
Best Practices	16
People	16
Processes	16
Passwords and Other Identifiers	18
Site Security	20
Low Security Site Example	20
Medium Security Site Example	21
High Security Site Example	22
BlueScale Encryption Key Management Overview	24
Understanding the Components	24
Standard Edition vs. Professional Edition	24
KMIP using HP ESKM Overview	27
Chapter 2 - BlueScale Encryption Standard	28
Configuring BlueScale Encryption Standard Edition	29
Log In to the Encryption Feature	30
Configure Secure Initialization, Password, and Authorization Settings	31
Creating an Encryption Key	33
Assigning an Encryption Key to a Partition	35
Restoring Encrypted Data	37
Use the Key Stored in the Library	37
Import the Required Key Into the Library	37
Exporting and Protecting Encryption Keys	39
Export the Encryption Key	39
Protect the Encryption Key	41
Deleting an Encryption Key from the Library	43
Disabling Encryption in a Partition	45

Chapter 3 - BlueScale Encryption Professional	46
Configuring BlueScale Encryption Professional Edition	47
Log In to the Encryption Feature	47
Configuring Secure Initialization, Password, and Authorization Settings	49
Creating an Encryption Key	51
Assigning an Encryption Key to a Partition	53
Restoring Encrypted Data	55
Use the Key Stored in the Library	55
Import the Required Key Into the Library	55
Exporting and Protecting Encryption Keys	58
Export the Encryption Key	58
Protect the Encryption Key	60
Deleting an Encryption Key from the Library	62
Disabling Encryption in a Partition	64
Chapter 4 - KMIP Encryption Key Management	65
KMIP Encryption Key Management	66
Configuring KMIP Encryption	67
Configure a DNS Server	67
Create a Certificate Signing Request (CSR)	67
Sign the Certificate Request Using HPE ESKM	70
Add a New Local User to HPE ESKM	72
Import Artifacts for HPE ESKM	73
Sign the Certificate using Fortanix	76
Configure KMIP Servers	78
Add KMIP Server	78
Edit a KMIP Server	79
Delete a KMIP Server	80
Configuring a Partition to Use a KMIP Server	81
Disabling Encryption in a Partition	82
Chapter 5 - Encryption Troubleshooting	83
Troubleshooting Encryption Issues	84

COPYRIGHT

Copyright © 2025 Spectra Logic Corporation. All rights reserved. This item and the information contained herein are the property of Spectra Logic Corporation.

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

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

PART NUMBER

90940181 Revision B

REVISION HISTORY

Revision	Date	Description
A	May 2025	Initial Release
B	August 2025	Added Fortanix

Note: 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/>.

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, or licensee of, all right, title and interest to the Software Product, regardless of the media or form of the original download, whether by the World Wide Web, disk or otherwise. You, as licensee ("Licensee") through your downloading, installing, copying or use of this product do not acquire any ownership rights to the Software Product.

3. GENERAL

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

4. SOFTWARE PRODUCT

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

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

5. GRANT OF LICENSE AND RESTRICTIONS

- A. Spectra grants you a non-exclusive, non-transferable End-User license right to install the Software Product solely for the purpose for which it was created.
- B. Unless provided otherwise in the Documentation or by prior express written consent of Spectra, you shall not display, modify, reproduce and distribute any Art Work, or portion(s) thereof, included with or relating to the Software Product, if any. Any such authorized display, modification, reproduction and distribution shall be in full accord with this EULA. Under no circumstances will your use, display, modification, reproduction and distribution of the Art Work give you any Intellectual Property or Proprietary Rights of the Art Work. All rights, title, and interest belong solely to Spectra.
- C. Except for the initial loading of the Software Product, you shall not, without Spectra's express written consent:
 - Copy or reproduce the Software Product; or
 - Modify, adapt, or create derivative works based on the Software Product or any accompanying materials.

6. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

- A. Spectra will provide you with support services related to the Software Product ("Support"). Such Support will be provided in accordance with the Spectra Master Support Agreement, available for download and viewing on the Spectra Corporate Web site. Use of Support is governed by this EULA and Spectra's Master Support Agreement.
- B. Any supplemental software, code, content, or media provided to you in the course of Support shall be considered part of the Software Product and subject to the terms and conditions of this EULA.
- C. Spectra retains all right, title, and interest in and to the Software Product, and any rights not granted to you herein are reserved by Spectra. You hereby expressly agree not to extract information, reverse engineer, disassemble, decompile, or translate the Software Product, or otherwise attempt to derive the source code of the Software, except to the extent allowed under any applicable law. In the event that such activities are permitted by applicable law, any information you, or your authorized agent, discover shall be promptly disclosed to Spectra and shall be deemed the confidential information of Spectra.
- D. You shall not modify, sublicense, assign, or transfer the Software Product or any rights under this EULA, except as expressly provided in this EULA. Any attempt to sublicense, assign, or transfer any of the rights, duties, or obligations will be void.
- E. You may permanently transfer all of your rights under this EULA, provided you retain no copies. The other party must agree to accept the terms and conditions of the EULA.

7. ALL RESERVED

All rights not expressly granted herein are reserved by Spectra.

8. TERM

- A. This License is effective until terminated. Licensee may terminate it at any time by destroying the Software Product with all copies, full or partial, and removing all of its component parts.
- B. Your rights under this EULA will terminate automatically without notice from Spectra if you fail to comply with any term(s) or condition(s) of this EULA. In such event, no notice shall be required by Spectra to effect such termination.
- C. Upon termination of this EULA, you shall cease all use of the Software Product and destroy all copies, full or partial, together with all backup copies, modifications, printed or written materials, and merged portions in any form and remove all component parts of the Software Product.

9. INTELLECTUAL PROPERTY RIGHTS

- A. Spectra shall retain all right, title, and interest in the Software Product and to any modifications or improvements made thereto, and any upgrades, updates or Documentation provided to End User. End User will not obtain any rights in the Software Product, its updates, upgrades, and Documentation, as a result of its responsibilities hereunder.
- B. End User acknowledges Spectra's exclusive rights in the Software Product and that the Software Product is unique and original to Spectra and that Spectra is owner thereof. Unless otherwise permitted by law, End User shall not, at any time during or after the effective Term of the Agreement, dispute or contest, directly or indirectly, Spectra's exclusive right and title to the Software Product or the validity thereof.

10. U.S. GOVERNMENT END USERS

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

11. EXPORT LAW ASSURANCES

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

12. DISCLAIMER OF WARRANTIES

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

13. LIMITATION OF LIABILITY

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

14. CONTROLLING LAW AND SEVERABILITY

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

CONTACTING SPECTRA LOGIC

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

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 Support Portal 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>.

KMIP Software

See the documentation specific to your KMIP software.

LTO Ultrium Tape Drives

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

- [*IBM Tape Device Drivers Installation and User's Guide*](#)
Note: This guide also provides information about using the IBM Tape Diagnostic Tool (ITDT) to troubleshoot drive problems.
- [*IBM TotalStorage LTO Ultrium Tape Drive: SCSI Reference*](#)

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

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.

LumOS User Interface Screens

The LumOS 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 that helps 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 hardware or losing data.

ABOUT THIS GUIDE

This guide contains information about Spectra® BlueScale® Encryption key management, and KMIP encryption key management, for Spectra tape libraries using the LumOS operating system.

Note: If you are using a BlueScale operating system tape library, see the [Spectra TSeries Encryption Guide](#).

Note: If you are using a Spectra Stack tape library, see the [Spectra Stack User Guide](#).

BlueScale Encryption Key Management

- **Standard Edition** — Included as a standard feature of the LumOS operating system software. See [BlueScale Encryption Standard on page 28](#) for more information.
- **Professional Edition** — Requires a purchased option key to activate and provides additional security and flexibility features. See [BlueScale Encryption Professional on page 46](#) for more information.

KMIP Encryption Key Management

- Requires a purchased option key to activate, which enables library access to a KMIP server. See [KMIP Encryption Key Management on page 65](#) for more information.

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.

CHAPTER 1 - ENCRYPTION OVERVIEW AND STRATEGIES

Encryption Overview	14
Best Practices	16
People	16
Processes	16
Passwords and Other Identifiers	18
Site Security	20
Low Security Site Example	20
Medium Security Site Example	21
High Security Site Example	22
BlueScale Encryption Key Management Overview	24
Understanding the Components	24
Standard Edition vs. Professional Edition	24
KMIP using HP ESKM Overview	27

ENCRYPTION OVERVIEW

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



IMPORTANT

If you are using a BlueScale operating system tape library, see the [Spectra TSeries Encryption Guide](#).

For information on encryption in Spectra Stack tape libraries, see the [Spectra Stack User Guide](#).

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

Feature	BlueScale	KMIP with HPE ESKM
Library Integrated Server	✓	
Stand-alone Server		✓
Supports Spectra Cube and TFinity Plus Libraries	✓	✓
Multi-vendor Support (dual vendor shops)		✓
Graphical User Interface	✓	✓
Command Line Interface		✓
LTO-6 through LTO-10 Drive Support	✓	✓
TS11xx Technology Drive Support (TFinity Plus, T950)	✓	✓
Multi-library/ Multi-site Support		✓
AES-256 Bit Encryption	✓	✓
Secure Initialization Mode	✓	
Maximum Number of Encryption Keys	30	1,000,000+
MLM PostScan Media Verification	✓	
Key per Tape		✓

Feature	BlueScale	KMIP with HPE ESKM
Symmetric Shares	✓	✓
Asymmetric Shares		✓
Role-based Access Control	✓	✓
Key Grouping		✓
Device Grouping		✓
Key Group and Rotation Policies		✓
Key Lifecycle Status		✓
Audit Verified Key Deletion		✓
Certificates of Authority		✓
Audit Trail		✓
FIPS Certification		✓
IKEv2-SCSI Compliance		
Configuration, Policies, & Keystore Backup		✓
LDAP Support		✓

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 “Understanding User Groups and 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 18](#) 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.

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.
- 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 cannot be recreated or recovered. 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.

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.

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.

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.

Security Consideration	Strategy
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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.

Security Considerations	Strategy
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	<ul style="list-style-type: none"> • 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.

Security Considerations	Strategy
Level of security to implement	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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

BLUESCALE ENCRYPTION KEY MANAGEMENT OVERVIEW

BlueScale Encryption key management is tightly integrated into your Spectra library. Encryption is handled through encryption-enabled LTO- and later generation drives. BlueScale Encryption key management is provided through the library's user interface.

Understanding the Components

The BlueScale Encryption key management system 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 LumOS 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 below](#)).
- **The Encryption Chip in the LTO-6 or Later Generation Drives** — 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:**
- 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.
 - BlueScale Encryption key management is not compatible with KMIP encryption key management. Data encrypted using one 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 16](#) 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 20](#) for an example of setting up encryption using BlueScale Encryption Standard Edition.

For information about configuring and using BlueScale Encryption Standard Edition, see [BlueScale Encryption Standard on page 28](#).

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 21](#) and [High Security Site Example on page 22](#) for examples of setting up encryption using BlueScale Encryption Professional Edition.

For information about configuring and using BlueScale Professional Edition, see [BlueScale Encryption Professional](#) .

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

Feature		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: <ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • Single encryption key stored on the library at a time. • The same key is used for all partitions configured to use encryption. 	<ul style="list-style-type: none"> • 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.	
Compression	Drive-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.	

KMIP USING HP ESKM OVERVIEW

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 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
- TS1170 technology drives must use firmware version 6495 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.
 - **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 BlueScale encryption key management, because they cannot share encryption keys. Data encrypted using one type of encryption key management cannot be decrypted using a different type of encryption key management.

CHAPTER 2 - BLUESCALE ENCRYPTION STANDARD

Configuring BlueScale Encryption Standard Edition	29
Log In to the Encryption Feature	30
Configure Secure Initialization, Password, and Authorization Settings	31
Creating an Encryption Key	33
Assigning an Encryption Key to a Partition	35
Restoring Encrypted Data	37
Use the Key Stored in the Library	37
Import the Required Key Into the Library	37
Exporting and Protecting Encryption Keys	39
Export the Encryption Key	39
Protect the Encryption Key	41
Deleting an Encryption Key from the Library	43
Disabling Encryption in a Partition	45

CONFIGURING BLUESCALE ENCRYPTION STANDARD EDITION

Overview

BlueScale Encryption Standard 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. After encryption is enabled, data is automatically encrypted as it is stored in any partition that is encryption-enabled.

- Notes:**
- See [Standard Edition vs. Professional Edition on page 24](#) for a description of the differences between BlueScale Encryption Key Management Standard Edition and Professional Edition.
 - BlueScale Encryption Key Management is not compatible with KMIP encryption key management, because they cannot share encryption keys. Data encrypted using BlueScale encryption key management cannot be decrypted using KMIP encryption key management, and vice versa.

User Privilege Requirements

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

Authorization Password

The encryption password, or Authorization Password, lets a superuser access the encryption features.



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.

Log In to the Encryption Feature

1. In the LumOS user interface, select **Configuration > Encryption**.
2. Enter the **Authorization Password** and click **Submit**. The Encryption screen displays.

Note: The default password is blank.

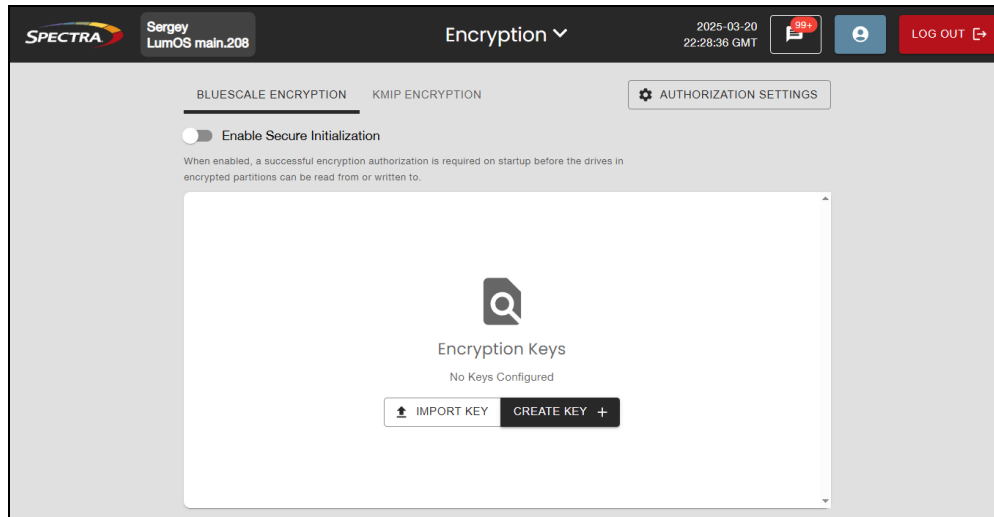


Figure 1 The Encryption screen.

CONFIGURE SECURE INITIALIZATION, PASSWORD, AND AUTHORIZATION SETTINGS

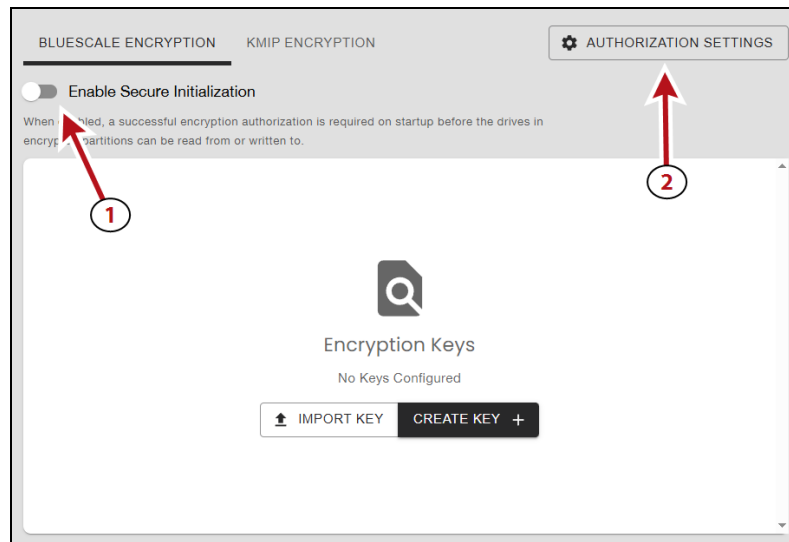


Figure 2 The Encryption screen.

1. Toggle the selector for **Enable Secure Initialization** if desired. When Secure Initialization is enabled, the encryption password must be entered when the library initializes before the library can read or write encrypted data.
2. Click **Authorization Settings** to open the Authorization Settings window.

The screenshot shows a web form titled "Authorization Settings" with a close button (X) in the top right corner. The form contains the following elements:

- A text input field labeled "Current Password" with a red circle containing the number 3 next to it.
- A dropdown menu labeled "User Mode" with "Single User" selected and a red circle containing the number 4 next to it.
- A red-bordered box containing:
 - A text input field labeled "New Password" with a red circle containing the number 5 next to it. Below this field is a note: "Use any combination of alphanumeric characters (including . @ - _). Leave the field blank to set an empty string as the password".
 - A text input field labeled "Confirm New Password".
- A black "SUBMIT" button at the bottom with a red circle containing the number 6 above it.

Figure 3 The Authorization Settings screen.

3. In the **Current Password** entry field, enter the current encryption password.

Note: The default password is blank.

4. Select the **User Mode** from the drop-down menu.

Note: Multi User mode requires a BlueScale Encryption Pro license.

5. Enter and confirm the **New Password** in the entry fields.

A password 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.

6. Click **Submit**.

CREATING AN ENCRYPTION KEY

1. In the LumOS user interface, select **Configuration > Encryption**.
2. Enter the encryption **Authorization Password** and click **Submit**.
3. On the Encryption screen, click **Create Key**. The New Encryption Key screen displays.

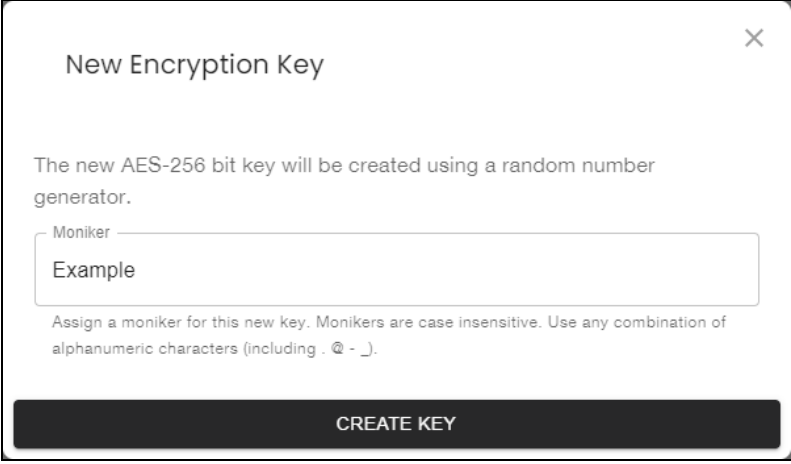


Figure 4 The New Encryption Key screen.

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

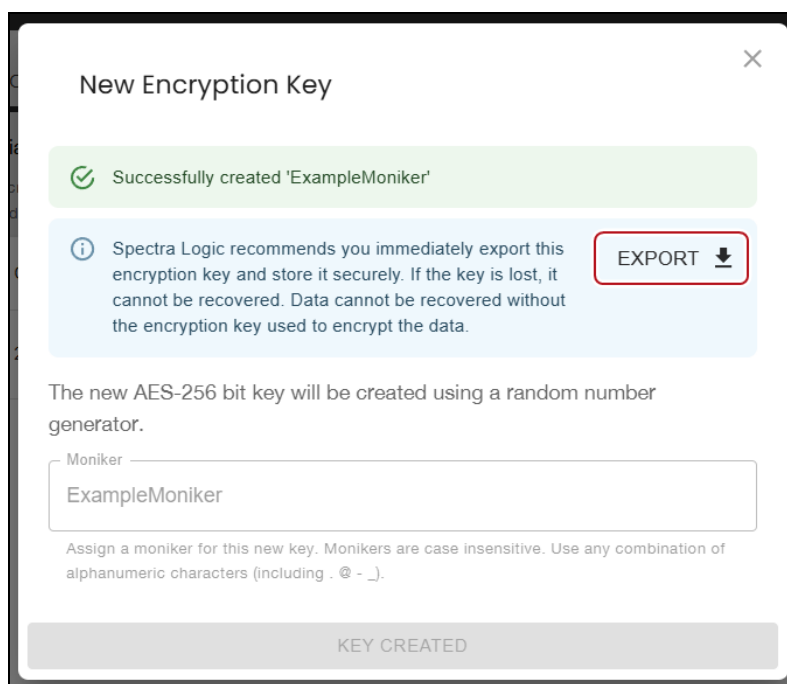


Figure 5 The New Encryption Key screen.

6. Click **Export** to export the newly created encryption key and save it to a secure location.



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 is extremely important to data decryption and recovery. See [Exporting and Protecting Encryption Keys](#) on page 39 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. Use the following steps to assign a key to a partition and encrypt all data sent to the partition:

1. In the LumOS user interface, select **Configuration > Partitions**. The Partitions screen displays.

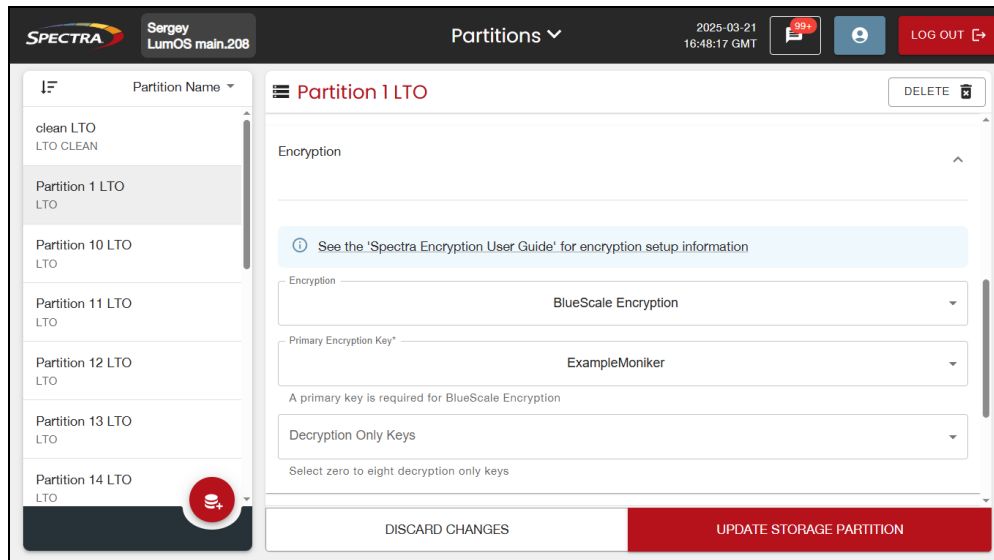


Figure 6 The Partitions screen.

2. In the left-hand pane, select the partition to which you want to add the encryption key. The configuration options for the partition display in the right-hand main window.
3. Expand the Encryption pane.
4. Using the **Encryption** drop-down menu, select **BlueScale Encryption**.
5. Using the **Primary Encryption Key** drop-down menu, select the desired encryption key.
6. Click **Update Storage Partition**.
7. Select **Configuration > Encryption**.
8. Enter the **Authorization Password** and click **Submit**. The Encryption screen displays.

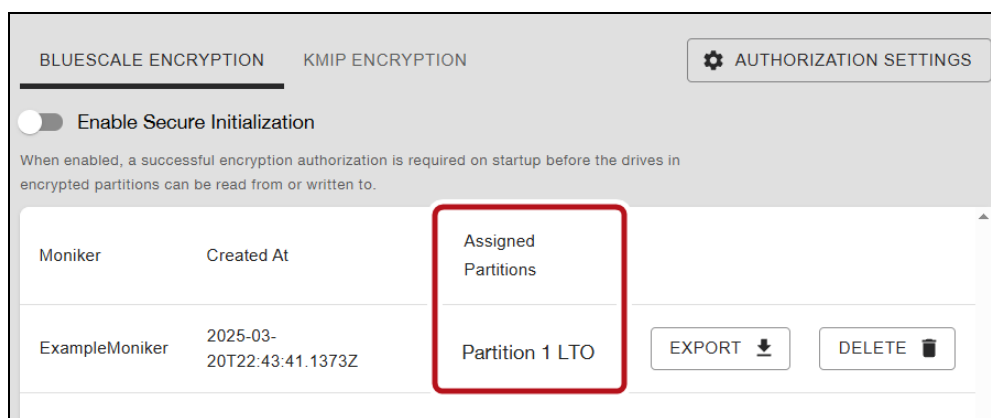


Figure 7 The Encryption screen.

9. Confirm the partition you to which you just assigned the key is listed in the **Assigned Partitions** column.

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.

1. If the encryption key is not currently assigned to the partition, modify the partition as described in [Assigning an Encryption Key to a Partition](#).
2. If you enabled Secure Initialization and no encryption user logged in since the last time the library initialized, enter the Authorization Password on the Encryption screen.
3. If necessary, import the cartridges containing the data to be restored into the library partition to which the encryption key is assigned.
4. Use your storage management software to restore the data. The data is automatically decrypted using the stored key.

Import the Required Key Into the Library

If the encryption key required for a specific set of encrypted data 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.

1. In the LumOS user interface, select **Configuration > Encryption**.
2. Enter the encryption **Authorization Password** and click **Submit**. The Encryption screen displays.

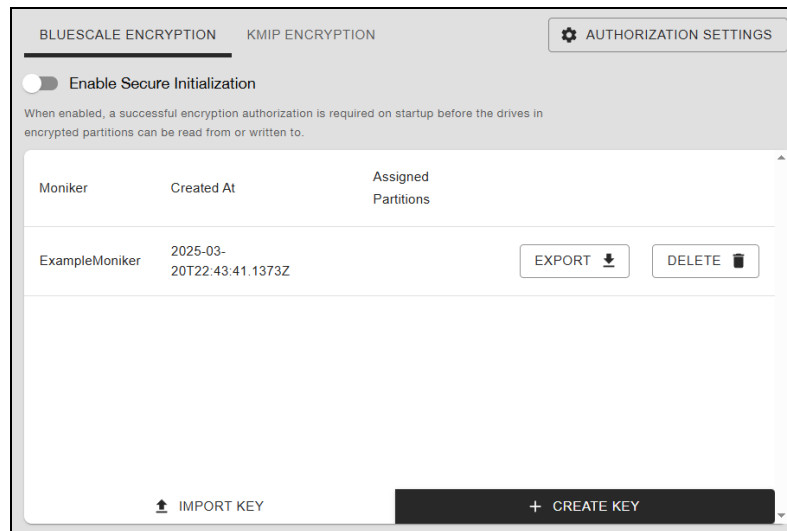


Figure 8 The Encryption screen.

3. Click **Import Key**. The Import Encryption Key screen displays.

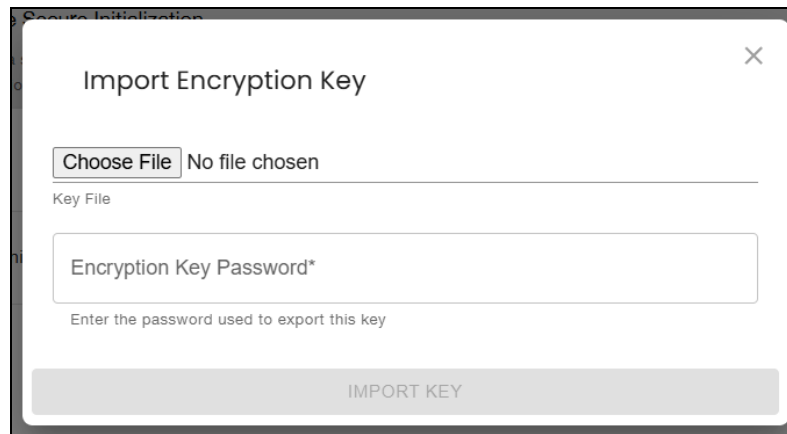


Figure 9 The Import Encryption Key screen.

4. Click **Chose File** and browse the location of the key you want to import.
5. Enter the **Encryption Key Password**. This is the password entered when the key was exported.
6. Click **Import Key**. The imported key displays on the Encryption screen.
7. Assign the imported key to the partition containing the encrypted cartridge (see [Assigning an Encryption Key to a Partition on page 35](#)).
8. Use your storage management software to restore the data.

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 that displays immediately after creating a key, or use the method described in this section to export encryption keys when needed.



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 and copy it 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.

Export the Encryption Key

Here is how to export the current encryption key:

1. In the LumOS user interface, select **Configuration > Encryption**.
2. Enter the encryption **Authorization Password** and click **Submit**. The Encryption screen displays.



Figure 10 The Encryption screen.

3. Click **Export** next to the encryption key you want to export. The Export *moniker name* screen displays.

Figure 11 The Export *moniker name* screen.

4. Enter and confirm the **Password** for the selected key. Use 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. The password is required when you import the key.
5. Click **Export Key**.

6. 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.

7. Confirm that the encryption key was correctly exported by browsing to the directory where you exported the key and locating key file. The file name is the name of the moniker with a .bsk extension.
8. Make sure that the file is more than 0 bytes in size. If the file meets this requirement, the encryption key was successfully exported and is usable.

Protect the Encryption Key

In conformance with your security plan, track the location of each USB device containing the exported key or, if you email the encryption key, 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.

**CAUTION**

As a matter of best practice, Spectra Logic recommends storing encryption keys to a USB device instead of using email to share encryption keys. 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.
-

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 39](#)).
- 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.



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 using multiple keys. Make sure that the key was successfully exported prior to deleting the 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 [Restoring Encrypted Data on page 37](#).

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:	

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. Export at least one copy of the encryption key and store it in a safe location (see [Export the Encryption Key on page 39](#)).
2. 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 82](#)).



Figure 12 The Encryption screen.

3. From the Encryption screen, click **Delete** on the row of the key you want to delete.

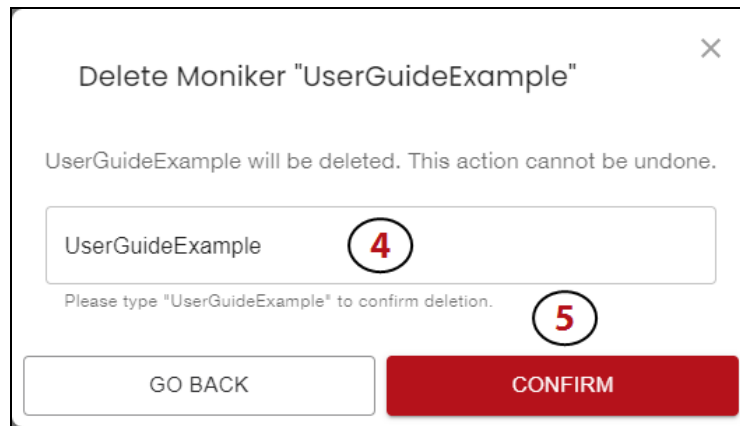


Figure 13 The Delete Moniker screen.

4. In the confirmation window, enter the **Moniker** of the key into the text field.
5. Click **Confirm** to delete the encryption key.

DISABLING ENCRYPTION IN A PARTITION

Use the following steps to disable encryption in a partition.

1. In the LumOS user interface, select **Configuration > Partitions**. The Partitions screen displays.

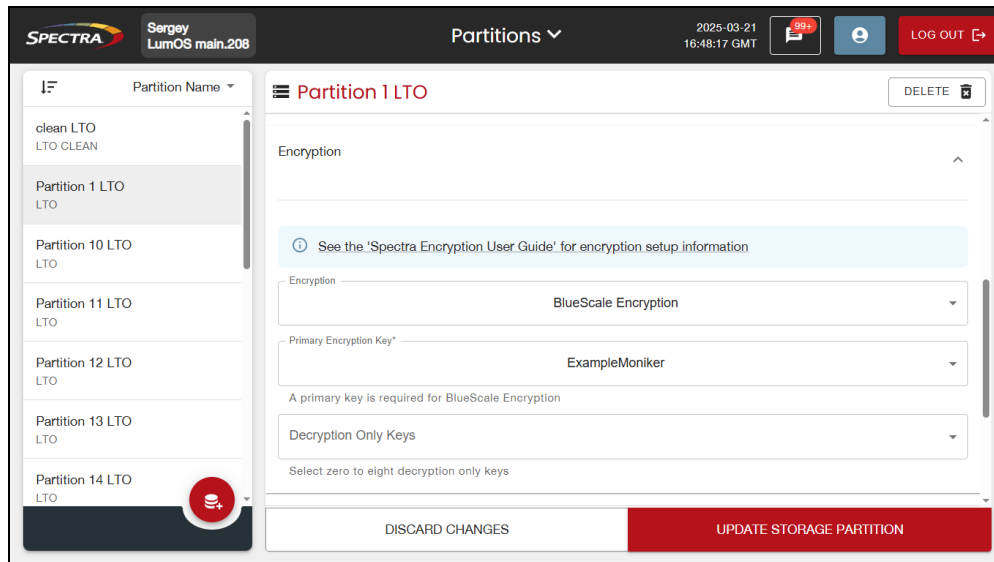


Figure 14 The Partitions screen.

2. In the left-hand pane, select the partition to which you want to disable encryption. The configuration options for the partition display in the right-hand main window.
3. Expand the Encryption pane.
4. Using the **Encryption** drop-down menu, select **Disabled**.
5. Click **Update Storage Partition**.

CHAPTER 3 - BLUESCALE ENCRYPTION PROFESSIONAL

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

Configuring BlueScale Encryption Professional Edition	47
Log In to the Encryption Feature	47
Configuring Secure Initialization, Password, and Authorization Settings	49
Creating an Encryption Key	51
Assigning an Encryption Key to a Partition	53
Restoring Encrypted Data	55
Use the Key Stored in the Library	55
Import the Required Key Into the Library	55
Exporting and Protecting Encryption Keys	58
Export the Encryption Key	58
Protect the Encryption Key	60
Deleting an Encryption Key from the Library	62
Disabling Encryption in a Partition	64

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. After encryption is enabled, data is automatically encrypted as it is written to tape in any partition that is encryption-enabled.

- Notes:**
- See [Standard Edition vs. Professional Edition on page 24](#) for a description of the differences between BlueScale Encryption Key Management Standard Edition and Professional Edition.
 - BlueScale Encryption Key Management is not compatible with KMIP encryption key management, because they cannot share encryption keys. Data encrypted using BlueScale encryption key management cannot be decrypted using KMIP encryption key management, and vice versa.

User Privilege Requirements

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

Authorization Password

The encryption password, or Authorization Password, lets a superuser access the encryption features.



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.

Log In to the Encryption Feature

1. In the LumOS user interface, select **Configuration > Encryption**.
2. Enter the **Authorization Password** and click **Submit**. The Encryption screen displays.

Note: The default password is blank.

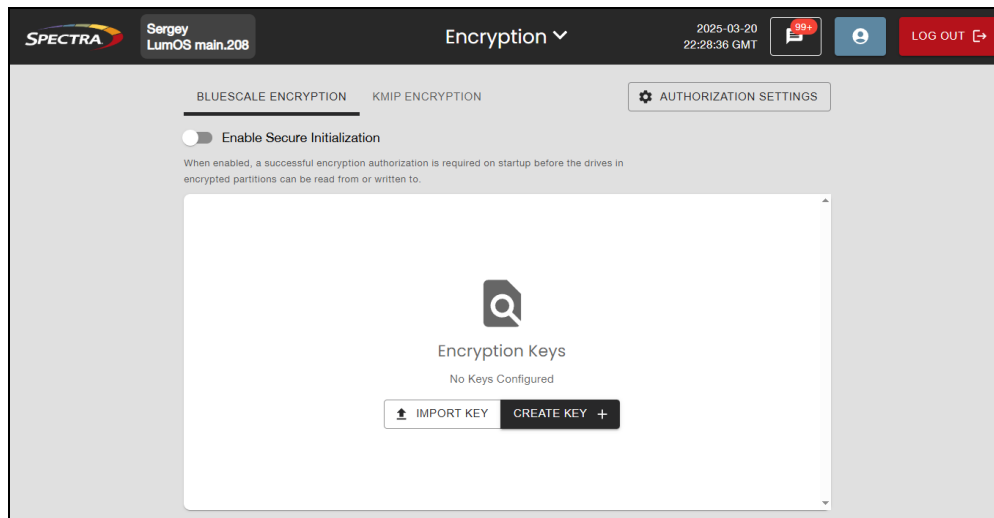


Figure 15 The Encryption screen.

CONFIGURING SECURE INITIALIZATION, PASSWORD, AND AUTHORIZATION SETTINGS

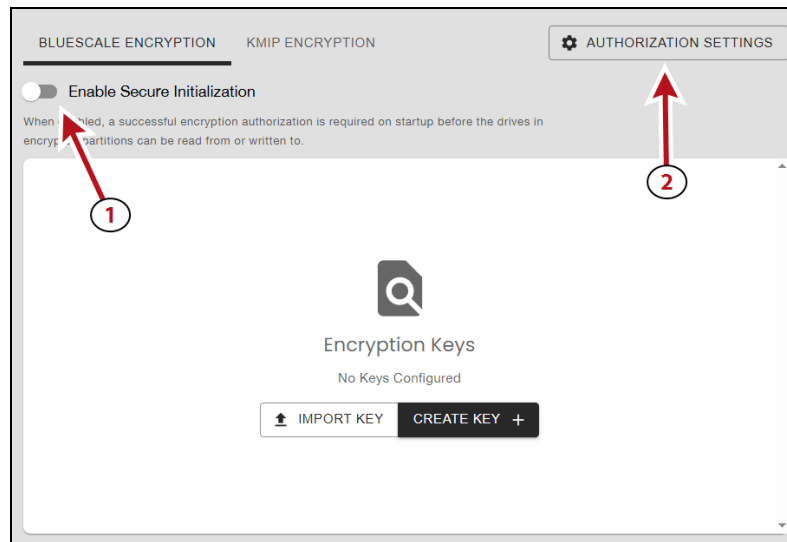


Figure 16 The Encryption screen.

1. Toggle the selector for **Enable Secure Initialization** if desired. When Secure Initialization is enabled, the encryption password must be entered when the library initializes before the library can read or write encrypted data.
2. Click **Authorization Settings** to open the Authorization Settings window.

Figure 17 The Authorization Settings screen - Single User

3. In the **Current Password** entry field, enter the current encryption password.

Note: The default password is blank.

4. Using the **User Mode** drop-down menu, select Single User or Multi User mode. This setting determines how many passwords are required to access the encryption screen, import and export keys, and enable the library after initialization if Secure Initialization is enabled.

- **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 configure the three users and passwords, they are used as follows:
 - Enter any one of the three passwords to access the Encryption screen, and to initialize encryption on a library using Secure Initialization mode.
 - Enter any two of the three passwords when importing or exporting an encryption key.

5. Enter and confirm the **New Password** in the entry fields. If you are configuring multi-user mode, enter 3 unique passwords.

A password 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.

6. Click **Submit**.

CREATING AN ENCRYPTION KEY

1. In the LumOS user interface, select **Configuration > Encryption**.
2. Enter the encryption **Authorization Password** and click **Submit**.
3. On the Encryption screen, click **Create Key**. The New Encryption Key screen displays.

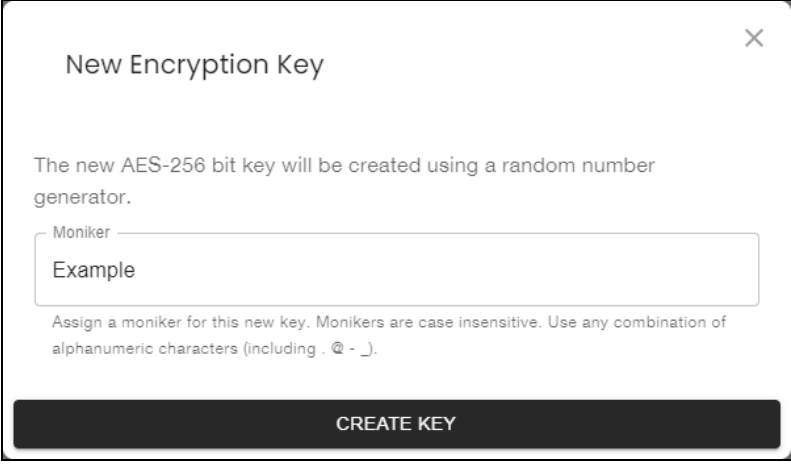


Figure 18 The New Encryption Key screen.

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

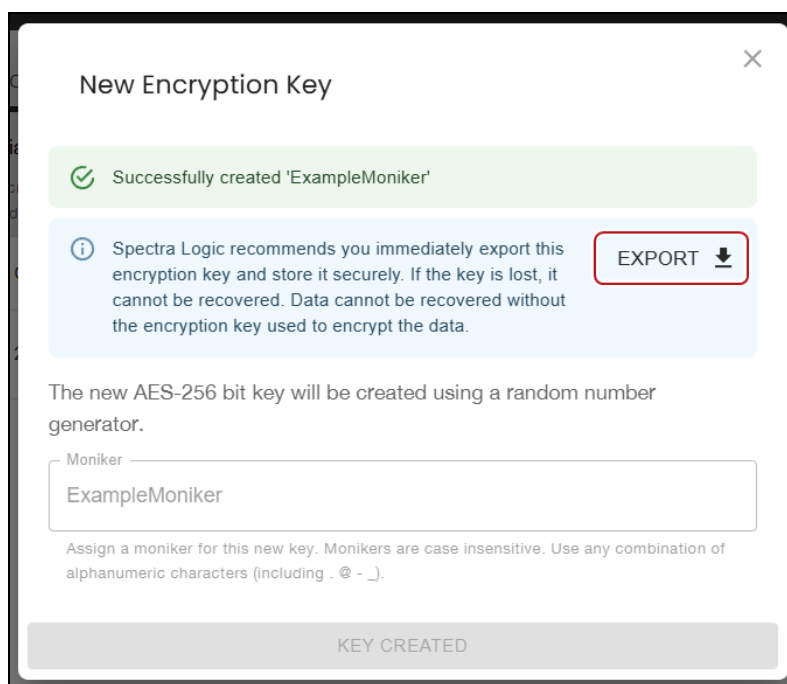


Figure 19 The New Encryption Key screen.

6. Click **Export** to export the newly created encryption key and save it to a secure location.



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 is extremely important to data decryption and recovery. See [Exporting and Protecting Encryption Keys](#) on page 39 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. Use the following steps to assign a key to a partition and encrypt all data sent to the partition:

1. In the LumOS user interface, select **Configuration > Partitions**. The Partitions screen displays.

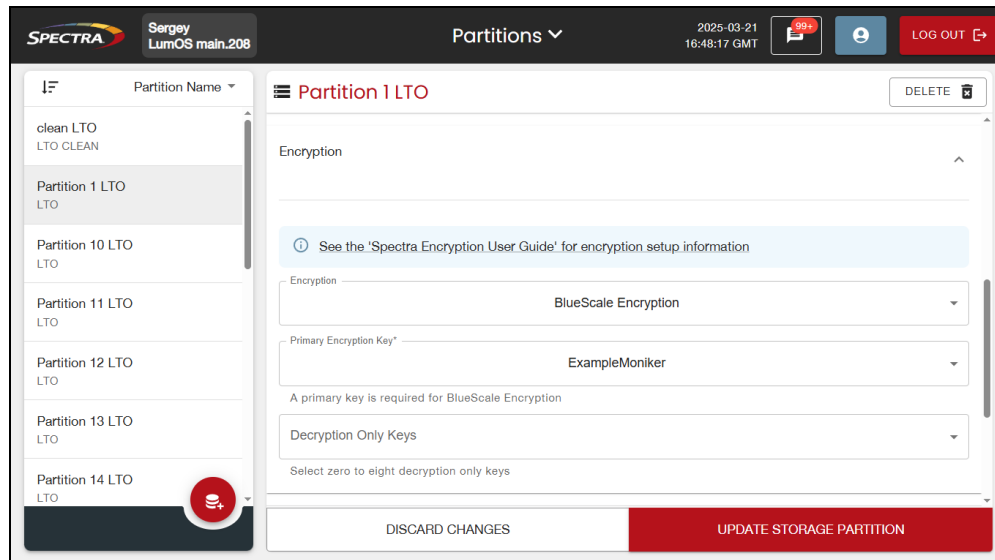


Figure 20 The Partitions screen.

2. In the left-hand pane, select the partition to which you want to add the encryption key. The configuration options for the partition display in the right-hand main window.
3. Expand the Encryption pane.
4. Using the **Encryption** drop-down menu, select **BlueScale Encryption**.
5. Using the **Primary Encryption Key** drop-down menu, select the desired encryption key. This key is used to both encrypt and decrypt data written to tape media.

Note: Only one key can be assigned as the primary encryption key.

6. If desired, use the **Decryption Only Keys** drop-down menu to select one or more keys used to decrypt data written by the Primary Encryption Key.
7. Click **Update Storage Partition**.
8. Select **Configuration > Encryption**.
9. Enter the **Authorization Password** and click **Submit**. The Encryption screen displays.

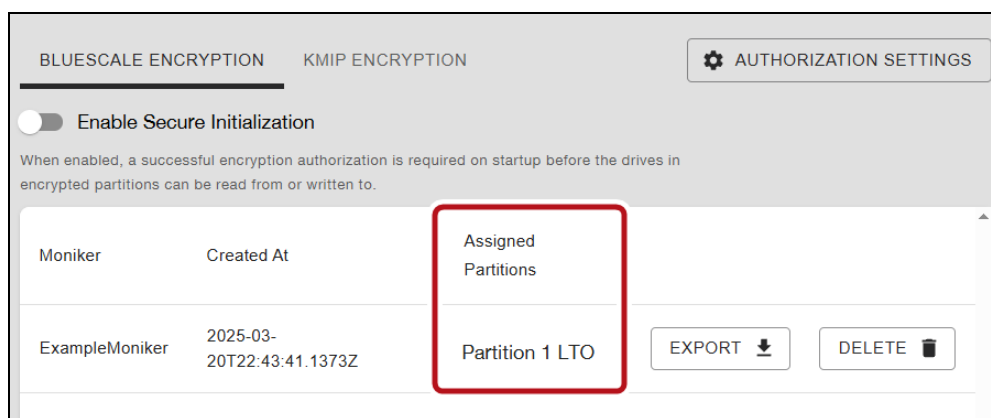


Figure 21 The Encryption screen.

10. Confirm the partition to which you just assigned encryption key(s) is listed in the **Assigned Partitions** column for each of the key(s) assigned to the partition.

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.

Multiple 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.

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.

1. 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 53](#).
2. If you enabled Secure Initialization and no encryption user logged in since the last time the library initialized, enter the Authorization Password on the Encryption screen.
3. If necessary, import the cartridges containing the data to be restored into the library partition to which the encryption key is assigned.
4. Use your storage management software to restore the data. The data is automatically decrypted using the stored key.

Import the Required Key Into the Library

If the encryption key required for a specific set of encrypted data 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.

1. In the LumOS user interface, select **Configuration > Encryption**.
2. Enter the encryption **Authorization Password** and click **Submit**. The Encryption screen displays.

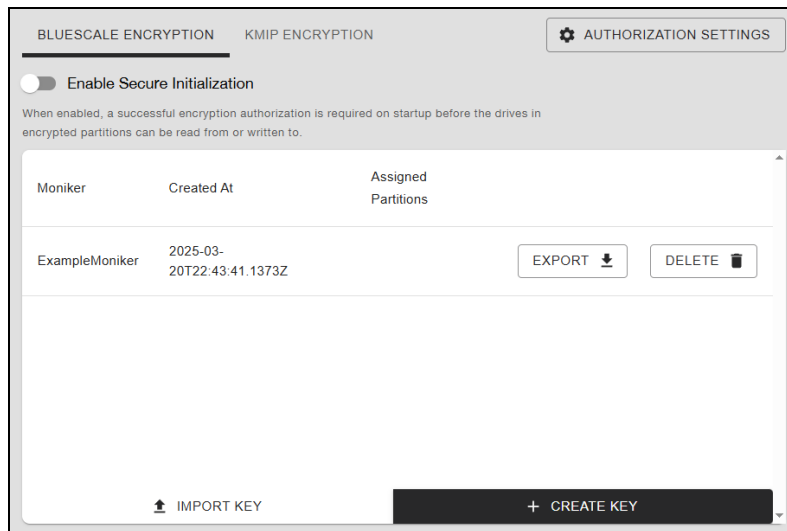


Figure 22 The Encryption screen.

3. Click **Import Key**. The Import Encryption Key screen displays.

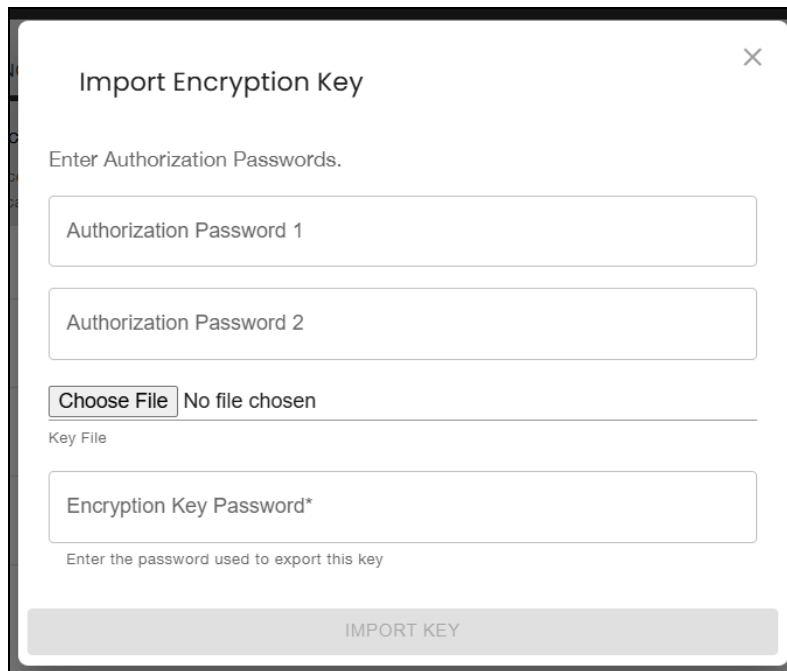


Figure 23 The Import Encryption Key screen.

4. Enter the two of the three configured **Authorization Passwords**.
5. Click **Chose File** and browse the location of the key you want to import.
6. Enter the **Encryption Key Password**. This is the password entered when the key was exported.

7. Click **Import Key**. The imported key displays on the Encryption screen.
8. Assign the imported key to the partition containing the encrypted cartridge (see [Assigning an Encryption Key to a Partition on page 53](#)).
9. Use your storage management software to restore the data.

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 that displays immediately after creating a key, or use the method described in this section to export encryption keys when needed.



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 and copy it 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.

Export the Encryption Key

Here is how to export the current encryption key:

1. In the LumOS user interface, select **Configuration > Encryption**.
2. Enter the encryption **Authorization Password** and click **Submit**. The Encryption screen displays.



Figure 24 The Encryption screen.

3. Click **Export** next to the encryption key you want to export. The Export *moniker name* screen displays.

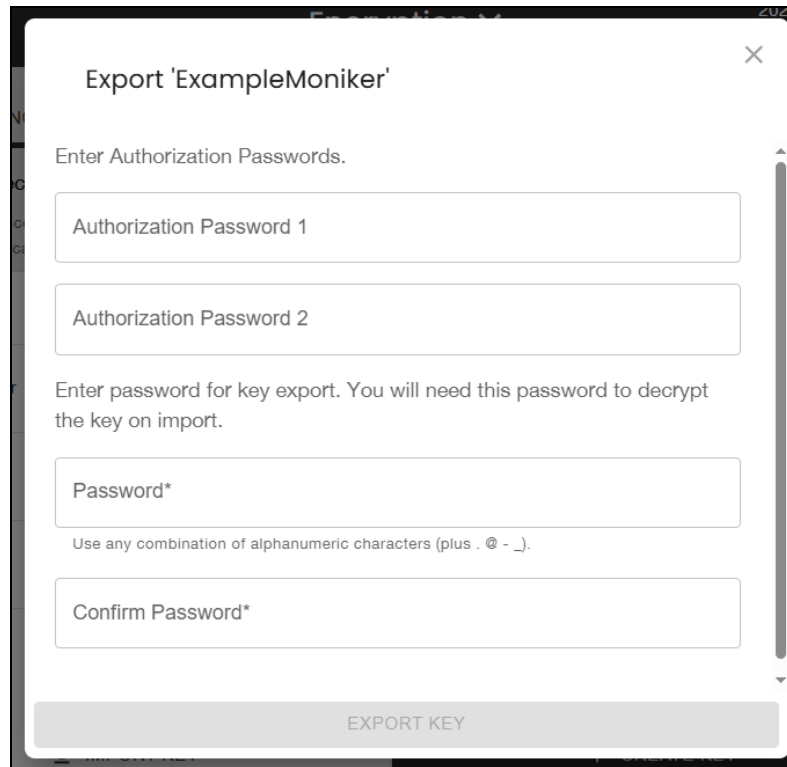


Figure 25 The Export *moniker name* screen.

4. Enter the two of the three configured **Authorization Passwords**.
5. Enter and confirm the **Password** for the selected key. Use 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. The password is required when you import the key.
6. Click **Export 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. Confirm that the encryption key was correctly exported by browsing to the directory where you exported the key and locating key file. The file name is the name of the moniker with a .bsk extension.
9. Make sure that the file is more than 0 bytes in size. If the file meets this requirement, the encryption key was successfully exported and is usable.

Protect the Encryption Key

In conformance with your security plan, track the location of each USB device containing the exported key or, if you email the encryption key, 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.

**CAUTION**

As a matter of best practice, Spectra Logic recommends storing encryption keys to a USB device instead of using email to share encryption keys. 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.
-

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 58](#)).
- 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 using multiple keys. Make sure that the key was successfully exported prior to deleting the 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 55](#).

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:	

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. Export at least one copy of the encryption key and store it in a safe location (see [Export the Encryption Key on page 39](#)).
2. 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 82](#)).



Figure 26 The Encryption screen.

3. From the Encryption screen, click **Delete** on the row of the key you want to delete.

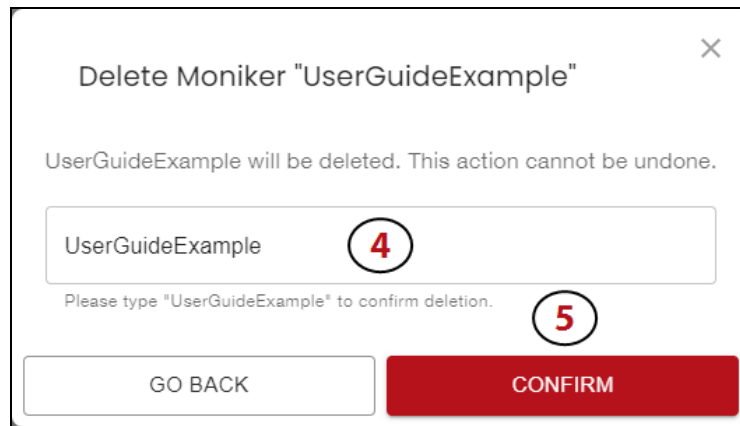


Figure 27 The Delete Moniker screen.

4. In the confirmation window, enter the **Moniker** of the key into the text field.
5. Click **Confirm** to delete the encryption key.

DISABLING ENCRYPTION IN A PARTITION

Use the following steps to disable encryption in a partition.

1. In the LumOS user interface, select **Configuration > Partitions**. The Partitions screen displays.

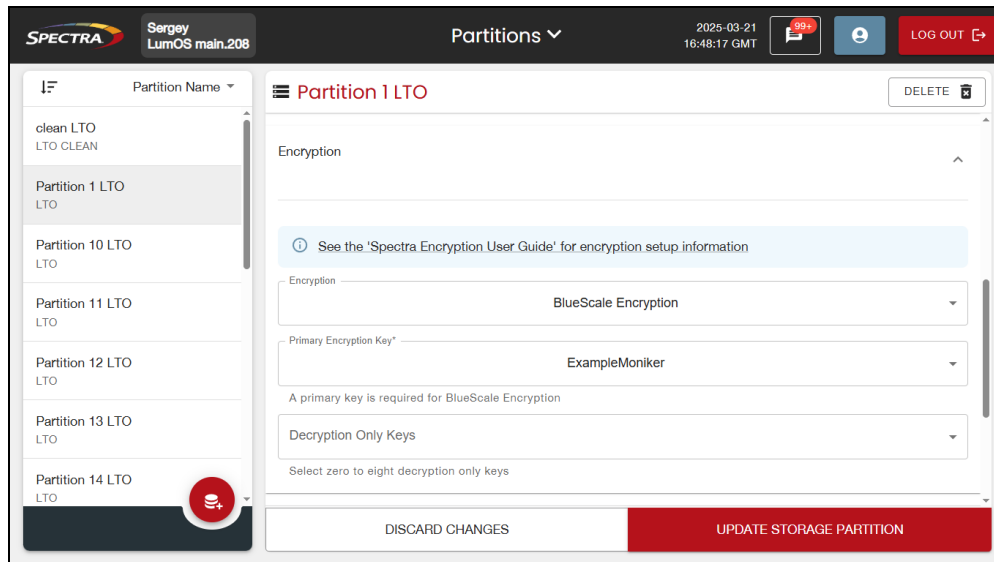


Figure 28 The Partitions screen.

2. In the left-hand pane, select the partition to which you want to disable encryption. The configuration options for the partition display in the right-hand main window.
3. Expand the Encryption pane.
4. Using the **Encryption** drop-down menu, select **Disabled**.
5. Click **Update Storage Partition**.

CHAPTER 4 - KMIP ENCRYPTION KEY MANAGEMENT

KMIP Encryption Key Management	66
Configuring KMIP Encryption	67
Configure a DNS Server	67
Create a Certificate Signing Request (CSR)	67
Sign the Certificate Request Using HPE ESKM	70
Add a New Local User to HPE ESKM	72
Import Artifacts for HPE ESKM	73
Sign the Certificate using Fortanix	76
Configure KMIP Servers	78
Add KMIP Server	78
Edit a KMIP Server	79
Delete a KMIP Server	80
Configuring a Partition to Use a KMIP Server	81
Disabling Encryption in a Partition	82

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 drives must have the following firmware:

- LTO-6 drives must use firmware version G352 or later
- LTO-7 drives must use firmware version G552 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
- TS1170 technology drives must use firmware version 6495 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.
 - **KMIP Server** — Install and configure KMIP on your server.

- Notes:**
- The library supports connections to Hewlett Packard Enterprise (HPE) Enterprise Secure Key Manager (ESKM) servers and Fortanix Data Security Manager servers.
 - KMIP encryption key management is not compatible with BlueScale encryption key management, because they cannot share encryption keys. Data encrypted using KMIP key management cannot be decrypted using BlueScale encryption key management, and vice versa.

CONFIGURING KMIP ENCRYPTION

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

User Privilege Requirements

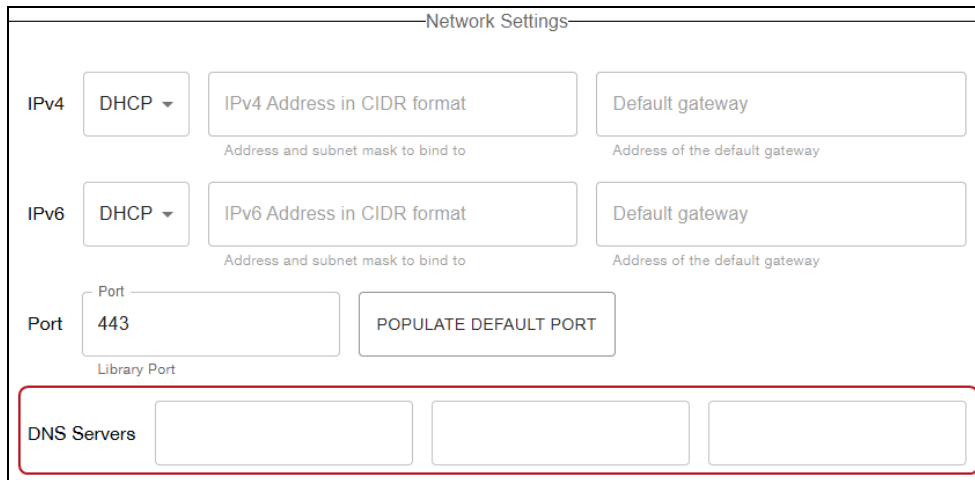
Only users with superuser privileges can configure the encryption features.

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, you must configure at least one DNS server for the library.

Note: If you plan to use an IP address, skip to [Create a Certificate Signing Request \(CSR\)](#) below.

1. In the LumOS user interface, select **Configuration > Settings**. The System Settings screen displays.
2. Scroll down to the Network Settings pane.



The screenshot shows the 'Network Settings' pane. It includes sections for IPv4 and IPv6, each with a DHCP dropdown, an address field, and a default gateway field. Below these is a 'Port' section with a 'Port' dropdown set to '443' and a 'POPULATE DEFAULT PORT' button. At the bottom, the 'DNS Servers' section is highlighted with a red border, showing three empty input fields.

Figure 29 The Network Settings pane of the System Settings screen.

3. Enter an IP address for a DNS server, and then click **Save Changes** (not pictured).

Create a Certificate Signing Request (CSR)

1. In the LumOS user interface, select **Configuration > Encryption**.
2. Enter the encryption **Authorization Password** and click **Submit**.
3. On the Encryption screen, click the **KMIP Encryption** tab. The KMIP Encryption screen displays.

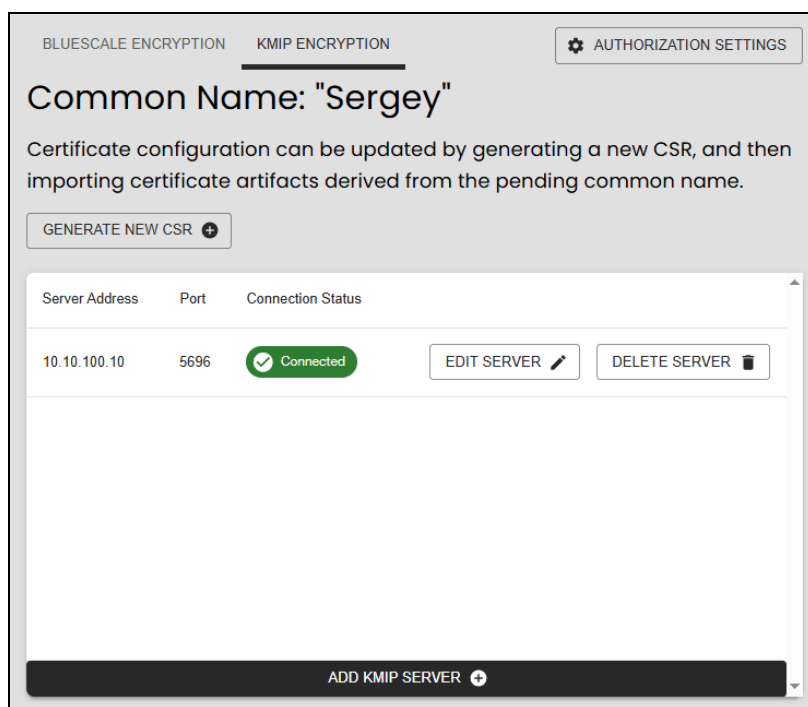


Figure 30 The KMIP Encryption Screen.

4. Click **Generate New CSR**. The New Certificate Signing Request screen displays.

The screenshot shows the 'New Certificate Signing Request' dialog box. It has a title bar with a close button. Below the title is a section titled 'Certificate Characteristics'. This section contains several text input fields: 'Common Name*' (with the value 'User Guide Example'), 'Country', 'State', 'Locality', 'Organization', and 'Organizational Unit'. At the bottom of the dialog is a 'GENERATE CSR' button.

Figure 31 The New Certificate Signing Request screen.

5. In the **Common Name** text field, enter a 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.
6. Optionally, fill out the **Country**, **State**, **Locality**, **Organization**, and **Organization Unit** text fields.
- 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.
7. Click **Generate CSR**. The library generates a key pair, and presents the CSR.

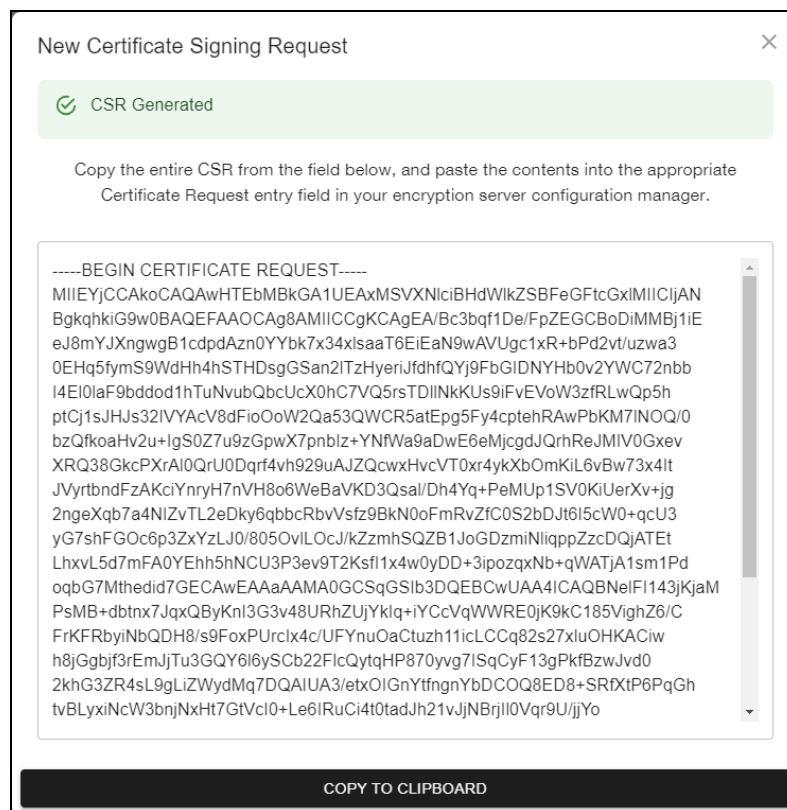


Figure 32 The New Certification Signing Request screen.

8. Click **Copy To Clipboard** to copy the new certification signing request.
9. The next steps depend on which KMIP software package you are using. For HPE ESKM, see ["Sign the Certificate Request Using HPE ESKM" on the next page](#). For Fortanix, see ["Sign the Certificate using Fortanix" on page 76](#)

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.

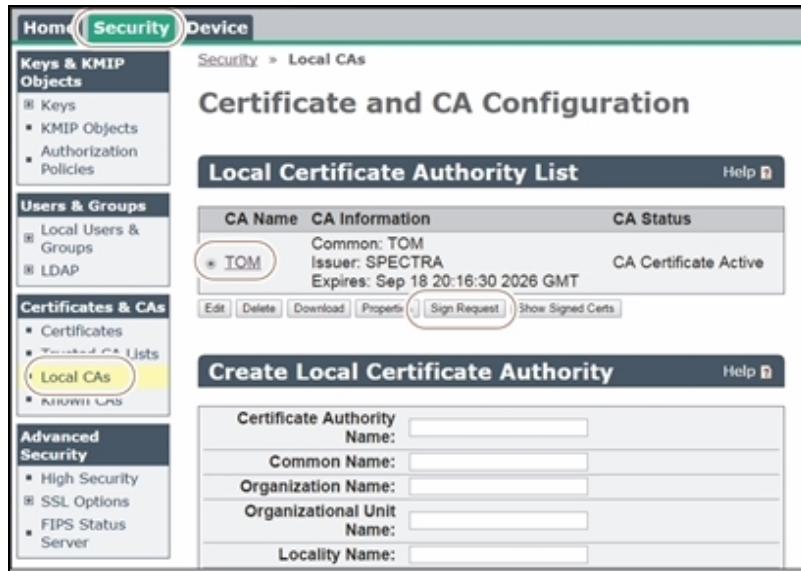


Figure 33 Navigate to the Certificate and CA Configuration screen.

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.



Figure 34 The Sign Certificate Request section of the Certificate and CA Configuration screen.

5. Paste the CSR text from the library New Certificate Signing Request (Step 8 on page 69) 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.

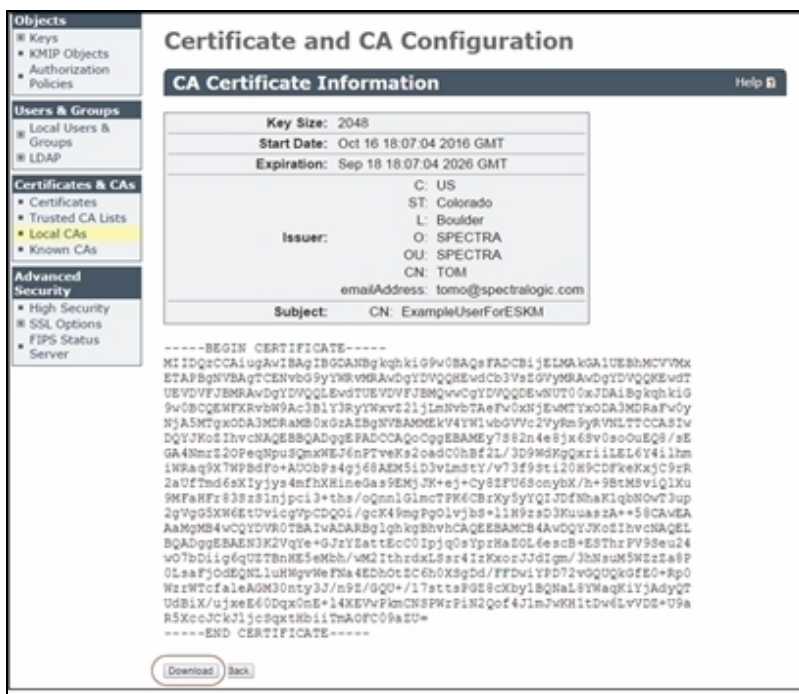


Figure 35 Copy or download the signed certificate.

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.

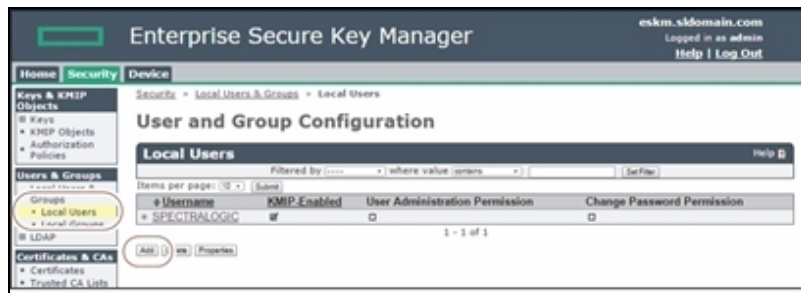


Figure 36 The Users and Group Configuration screen.

2. Click **Add** to display the Create Local User screen.
3. For Username, enter the name you configured as the Common Name in [Step 5](#) on [page 68](#).

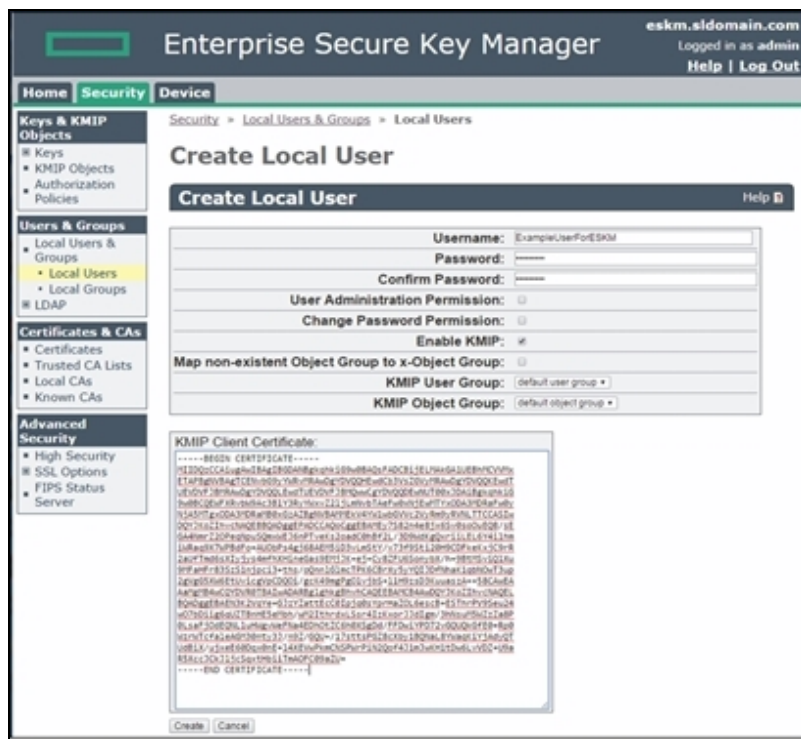


Figure 37 Enter the information to create a local user.

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 71](#) into the KMIP Client Certificate field.
 6. Click **Create**.

Import Artifacts for HPE ESKM

1. On the KMIP Encryption screen in the library LumOS interface, click **Import Certificate Artifacts**.

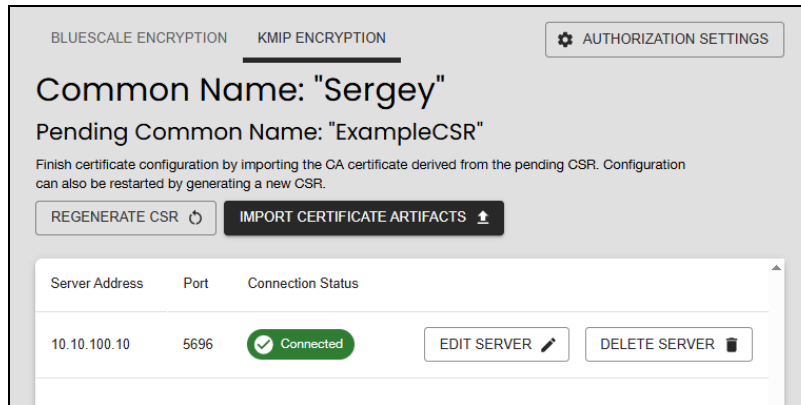


Figure 38 Click **Import Certificate Artifacts**.

The Import Certificate Artifacts screen displays.

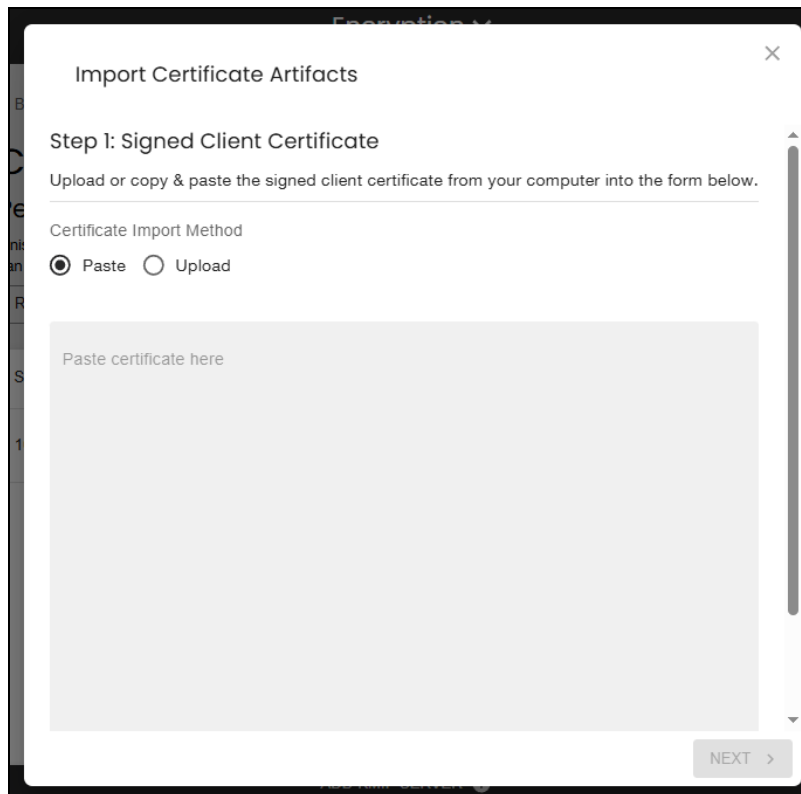
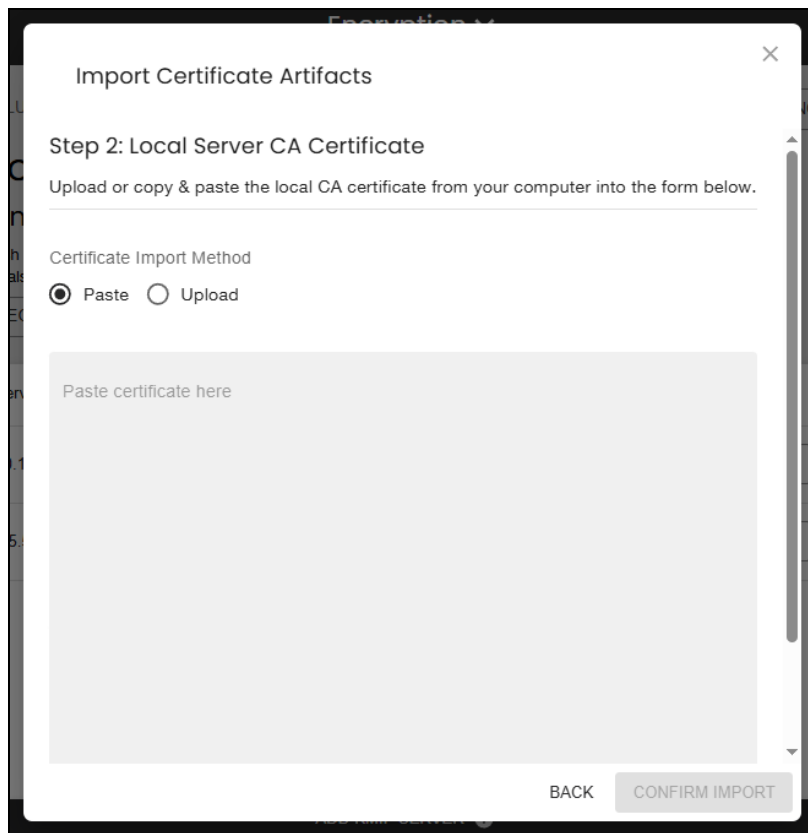


Figure 39 The Import Certificate Artifacts - Signed Client Certificate screen.

2. Paste the signed client certificate copied in [Step on page 67](#) 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 Local Server CA Certificate screen of the Import Certificate Artifacts wizard displays.



Import Certificate Artifacts

Step 2: Local Server CA Certificate

Upload or copy & paste the local CA certificate from your computer into the form below.

Certificate Import Method

☒ Paste ☐ Upload

Paste certificate here

BACK CONFIRM IMPORT

Figure 40 The Import Certificate Artifacts - Local Server CA Certificate screen.

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

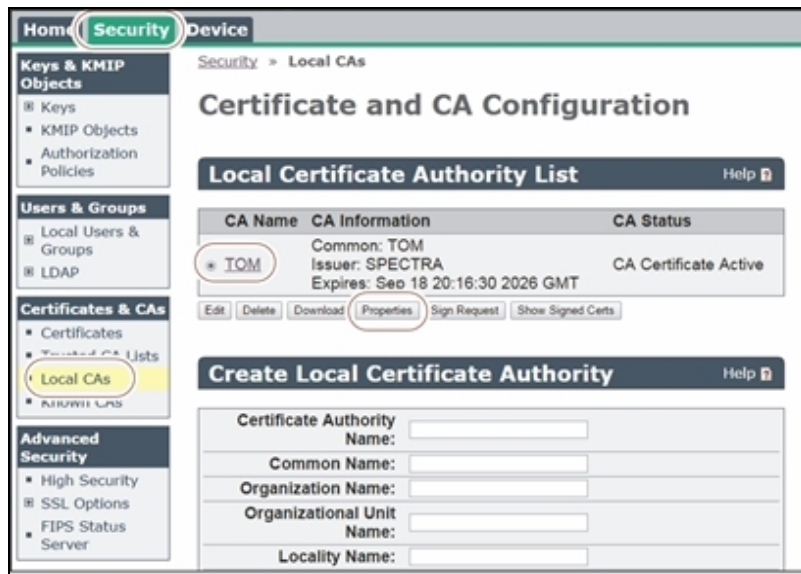


Figure 41 Navigate to the Certificate and CA Configuration screen.

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.

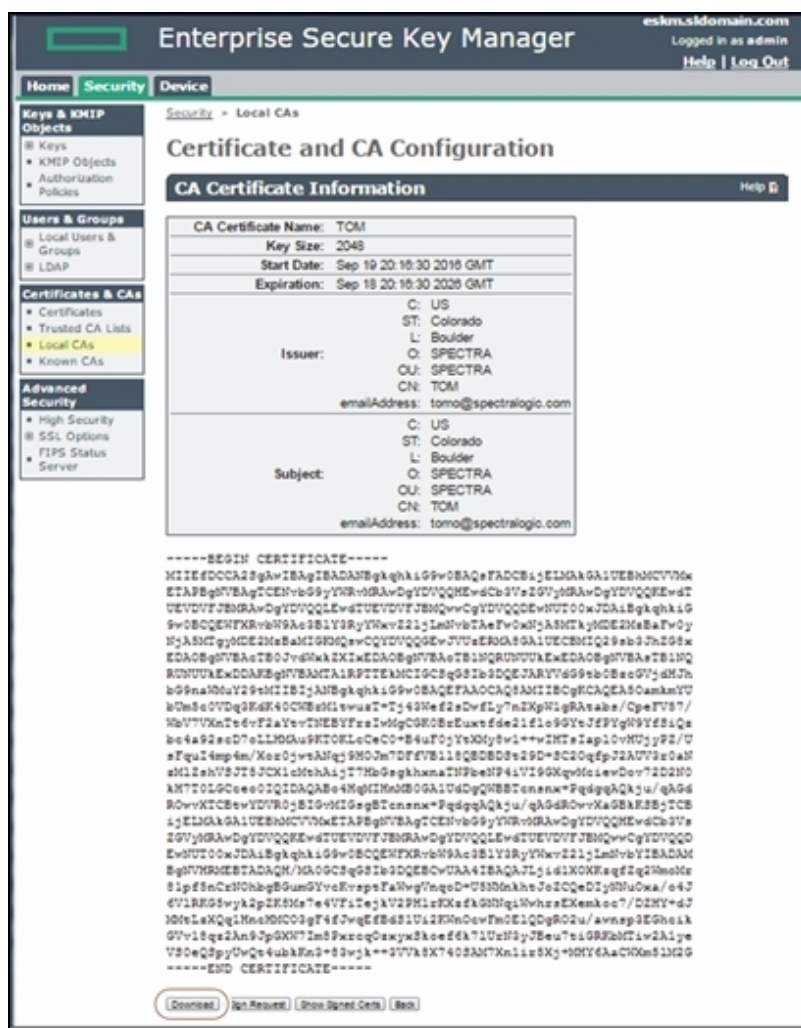


Figure 42 The CA Certificate Information screen.

6. In the LumOS user interface, paste the CA certificate copied in [Step 5 on page 75](#) into the entry field on the Local Server CA Certificate screen of the Import Certificate Artifacts wizard (see [Figure 40 on page 74](#)). 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 **Confirm Import**.

Sign the Certificate using Fortanix

1. Log into the Fortanix server using the Fortanix DSM application.

Update a certificate for LarrytheLibrary

Current certificate subject: CN=a7004f82-622f-451e-bb23-9f78dd1966fe

UPLOAD NEW CERTIFICATE

Upload certificate

Previous authentication method:
Certificate

Expiration Setting:
Expire previous authentication immediately **EDIT**

I understand that

☐ This action will replace existing authentication with the new authentication.

☐ Clients using previous authentication will no longer work after the specified time period.

CANCEL **UPDATE**

Figure 43 The Update Certificate screen.

2. Open the library and select **Upload New Certificate**.
3. Paste the signed client certificate copied from your Certificate Authority in the entry field, or if you downloaded the certificate file onto your local host, click **Upload New Certificate** and use your web browser to upload the file.
4. If desired, under Expiration Setting select **Edit** to change the expiration settings for any existing authentication, and select the boxes below.
5. Click **Update**.

CONFIGURE KMIP SERVERS

Add KMIP Server

Use the steps and figure below to add a KMIP server.

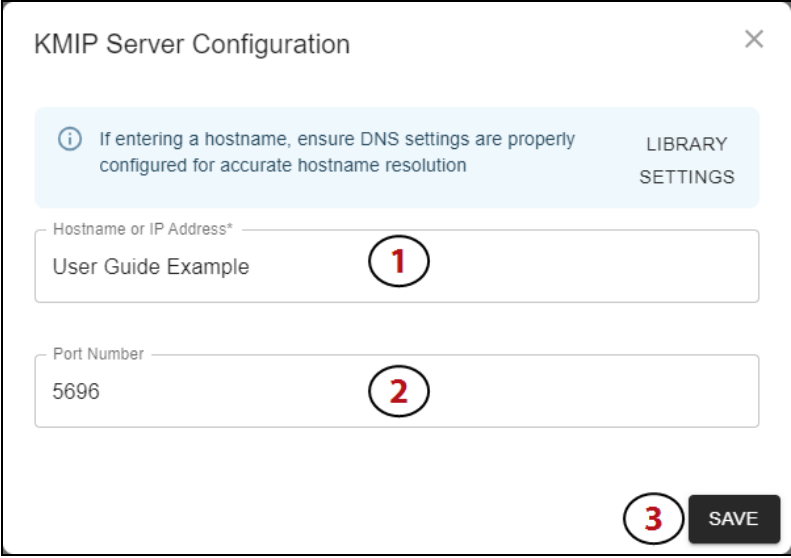
The image shows a 'KMIP Server Configuration' dialog box. At the top, there is a title bar with a close button (X). Below the title bar, there is a light blue informational banner with an 'i' icon and the text: 'If entering a hostname, ensure DNS settings are properly configured for accurate hostname resolution'. To the right of this banner is a link that says 'LIBRARY SETTINGS'. Below the banner, there are two text input fields. The first field is labeled 'Hostname or IP Address*' and contains the text 'User Guide Example'. A red circle with the number '1' is placed to the right of this field. The second field is labeled 'Port Number' and contains the text '5696'. A red circle with the number '2' is placed to the right of this field. At the bottom right of the dialog, there is a red circle with the number '3' next to a dark grey button labeled 'SAVE'.

Figure 44 The KMIP Server Configuration screen.

1. In the **Hostname or IP Address** text field, enter the KMIP server hostname or IP address.
2. Optionally, enter the KMIP server port number in the **Port Number** text field.
3. Click **Save**.
4. 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.

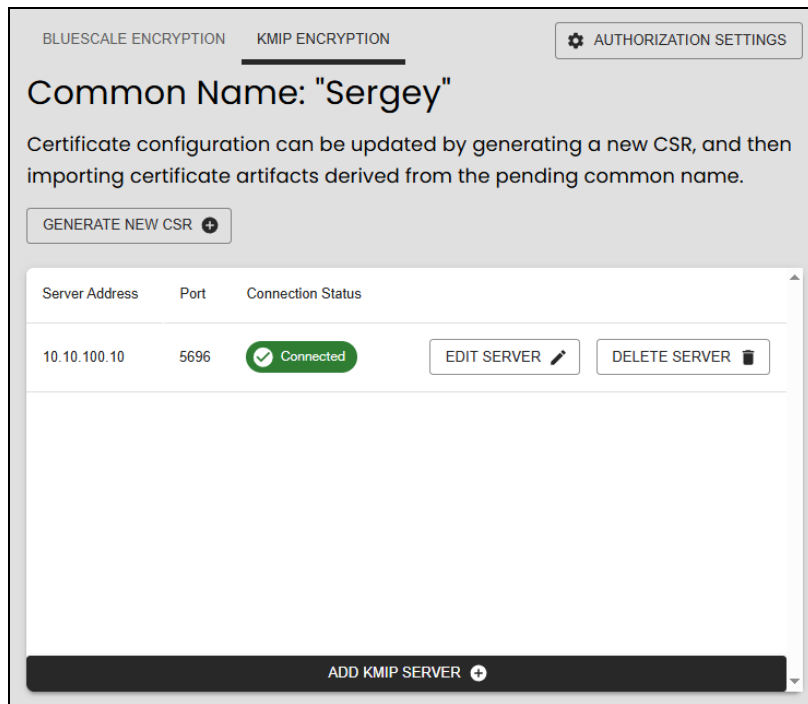


Figure 45 Access the KMIP Configuration Screen.

Note: **Connected** in a green circle appears in the Connection Status column next to servers the library can access. A red **Disconnected** in the Connection Status column indicates the library is currently unable to connect to that server.

Edit a KMIP Server

Use the steps below to edit a previously configured KMIP server.

1. In the LumOS user interface, select **Configuration > Encryption**.
2. Click **Edit Server** on the configured KMIP server you want to edit.

The screenshot shows a 'KMIP Server Configuration' dialog box. It has a title bar with a close button. Inside, there's an information icon and a note: 'If entering a hostname, ensure DNS settings are properly configured for accurate hostname resolution'. To the right of this note is a 'LIBRARY SETTINGS' link. Below the note are two input fields: 'Hostname or IP Address*' with the value '10.10.100.10' and 'Port Number' with the value '5697'. At the bottom right, there are 'RESET' and 'SAVE' buttons.

Figure 46 The KMIP Server Configuration screen.

3. Edit the **Hostname or IP Address** and **Port Number** text fields.
4. Click **Save**.

Delete a KMIP Server

Use the steps below to delete a previously configured KMIP server.

1. In the LumOS user interface, select **Configuration > Encryption**.
2. Click **Delete Server** on the configured KMIP server you want to edit.

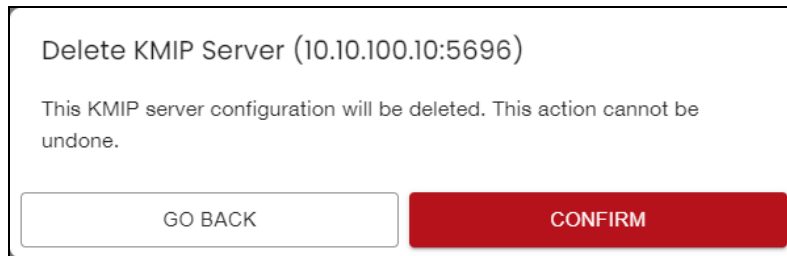


Figure 47 The Delete KMIP Server screen.

3. Click **Confirm** to delete the server.

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.

Note: You must use **KMIP Encryption - Reuse** for media using tape partitioning (for example, LTF5). 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. In the LumOS user interface, select **Configuration > Partitions**. The Partitions screen displays.

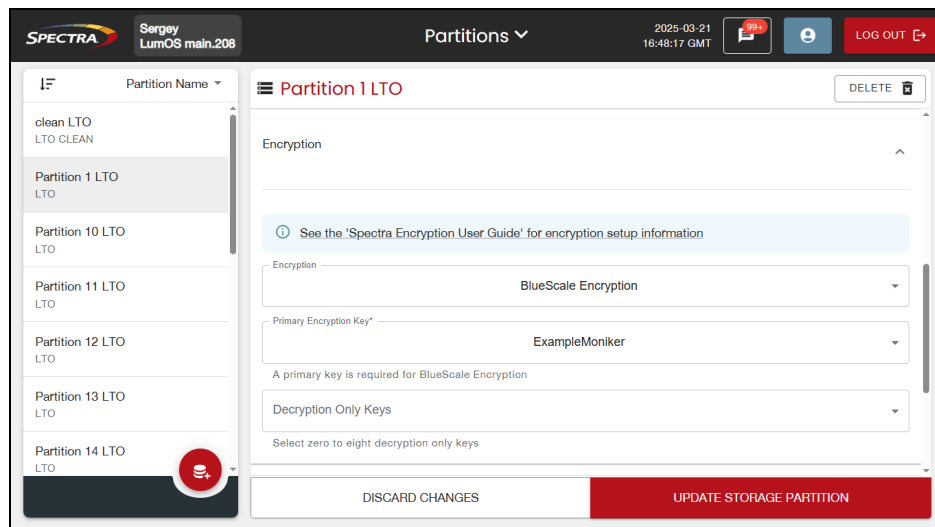


Figure 48 The Partitions screen.

2. In the left-hand pane, select the partition to which you want to use KMIP encryption. The configuration options for the partition display in the right-hand main window.
3. Choose the type of encryption to use:

Encryption Option	Description
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.

4. Click **Update Storage Partition**.

DISABLING ENCRYPTION IN A PARTITION

Use the following steps to disable encryption in a partition.

1. In the LumOS user interface, select **Configuration > Partitions**. The Partitions screen displays.

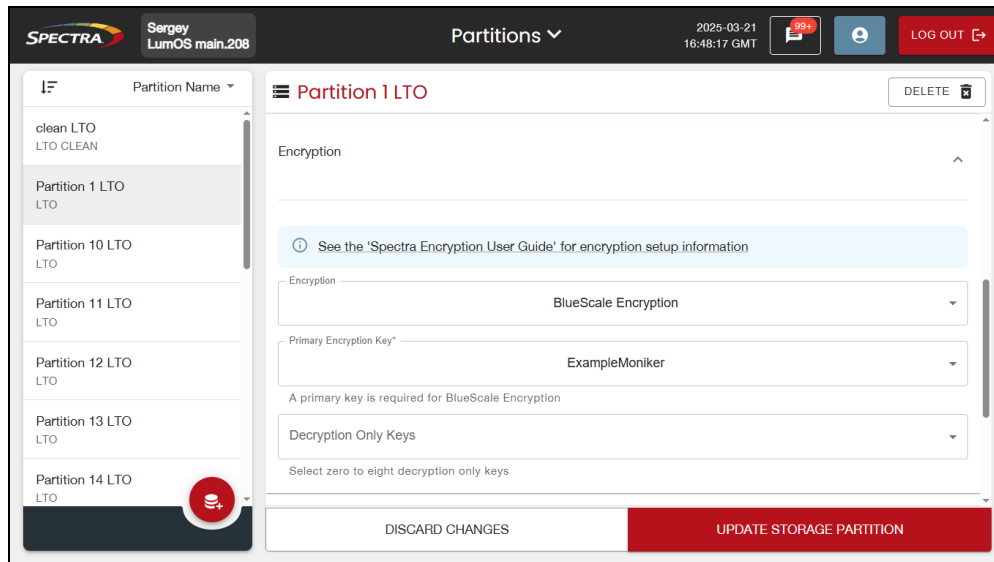


Figure 49 The Partitions screen.

2. In the left-hand pane, select the partition to which you want to disable encryption. The configuration options for the partition display in the right-hand main window.
3. Expand the Encryption pane.
4. Using the **Encryption** drop-down menu, select **Disabled**.
5. Click **Update Storage Partition**.

CHAPTER 5 - 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
System Message states that no encryption key was sent to the drive/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: <ol style="list-style-type: none"> 1. Move the cartridge out of the drive and return it to its storage location (see “Moving Media” in your Tape Library User Guide). 2. Reset the drive (see “Drive Actions” in your Tape Library User Guide).
System message states that a tape drive requires a specific moniker - BlueScale Encryption	<p>The encryption key used to encrypt the cartridge is not currently available on the library.</p> <p>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.</p>	<p>Depending on which BlueScale Encryption edition you are using, use the following steps to enable the cartridge to be read:</p> <p>BlueScale Standard Edition</p> <ol style="list-style-type: none"> 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 62). 4. Import the required key (see Import the Required Key Into the Library on page 37). 5. Select Configuration > Partitions. 6. Select the partition containing the cartridge. 7. Select the encryption key to be associated with the partition and click Save. <p>BlueScale Professional Edition</p> <ol style="list-style-type: none"> 1. Log into the library as a superuser. 2. Log into the encryption feature.

Issue	Cause	Resolution
		<ol style="list-style-type: none">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 37).4. Select Configuration > Partitions.5. Select the partition containing the cartridge.6. Select the required encryption key as either the primary encryption key or as a decryption key and click Save.