P3AG-3762-02ENZ0

FUJITSU Storage
ETERNUS LT140 Tape Library
Key Management Function Option

User's Guide

FUJITSU

This page is intentionally left blank.

Preface

Fujitsu would like to thank you for purchasing our Key Management Function Option for the FUJITSU Storage ETERNUS LT140 tape library (hereinafter referred to as "LT140").

This manual describes the setup methods and the operation procedures that are required to use the Key Management Function Option as well as notes and other information.

For information on handling the tape libraries (hereinafter referred to as "tape library", "library", or "device"), refer to the respective tape library user's guides. For information on console messages and commands of the backup software used, refer to the manual provided with the backup software.

Second Edition
December 2019

Acknowledgments

- LTO, Linear Tape-Open, and Ultrium are registered trademarks of Hewlett Packard Enterprise, IBM Corporation, and Quantum Corporation.
- Oracle and Java are registered trademarks of Oracle and/or its affiliates.
- Internet Explorer is a trademark or registered trademark of Microsoft Corporation in the United States and other countries.
- The company names and product names mentioned in this document are registered trademarks or trademarks of their respective companies.

Microsoft product screen shot(s) reprinted with permission from Microsoft Corporation.

Copyright 2019 FUJITSU LIMITED

About This Manual

Organization

This manual is composed of the following four chapters and an appendix:

- Chapter 1 Overview

  This chapter provides a functional overview of the Key Management Function Option.

- Chapter 2 Setup and Operation Procedures

  This chapter explains the setup and operation procedures of the key management function.

- Chapter 3 Setup Methods for Different Operations

  This chapter explains the setup methods for different operations.

- Chapter 4 Considerations

  This chapter provides notes on the Key Management Function Option.

Additional information on "Appendix A Logs Related to the Key Management Function" is provided as an appendix.

Copyright 2019 FUJITSU LIMITED

Warning Notations

Before using the Key Management Function Option, carefully read the contents of this manual to ensure the safe use of this product. Follow the directions in this manual correctly in order to prevent injury to the user and/or material damage. After reading, store this manual in a safe place for quick reference.

Warning signs are shown throughout this manual in order to prevent injury to the user and/or material damage. Carefully check the written descriptions indicated by these signs when reading this manual.

CAUTION	This symbol indicates the possibility of personal injury or material damage when this product is not used properly.

To ensure the safe use of this product, the following symbol (caution symbol) as well as related information is provided.

	This marks indicates instructions for general use.

Symbols Used in This Manual

- In this manual, a button or menu that is referred to is indicated as, for example, [OK].
- The following marks are used in this manual.

Caution	This symbol indicates important points to note when using this product.
Note	This mark indicates additional information regarding things such as convenient functions and procedures while performing operations and settings with this product.

Copyright 2019 FUJITSU LIMITED

Table of Contents

Copyright 2019 FUJITSU LIMITED

Copyright 2019 FUJITSU LIMITED

List of Figures

Copyright 2019 FUJITSU LIMITED

Copyright 2019 FUJITSU LIMITED

List of Tables

Copyright 2019 FUJITSU LIMITED

Chapter 1
Overview

1.1 Overview of the Data Encryption Function of LTO Ultrium Tape Drives

LTO Ultrium tape drives that are installed in the LT140 tape library have the function to write data to data cartridges (*2) with AES (*1) (256 bit) .

With this function, data is assigned an arbitrary key when written to a data cartridge (*2), and the data can be read only if the same key is assigned again at the data read time. (*3)

The function can thus prevent leakage of information on the tape cartridge, even if the tape cartridge is left unattended when taken out or is missing, because its data cannot be read without the key.

Also, the tape cartridge can be disposed of without deleting the data.

*1: Advanced Encryption Standard (AES): Encryption system authorized by the National Institute of Standards and Technology (NIST)
*2: Excludes Ultrium3 or earlier generation data cartridges that do not support the data encryption function.
*3: The data cartridge generations that can be read and written varies depending on the generation of the LTO Ultrium tape drive that is being used. For details, refer to "A.1.2 Tape Drive Compatibility with Tape Cartridges" in "FUJITSU Storage ETERNUS LT140 Tape Library User's Guide -Installation & Operation-".

1.2 Features of the Data Encryption Function of LTO Ultrium Tape Drives

The data encryption function of LTO Ultrium tape drives has the following features:

- The function conforms to the high security requirements specified in FIPS 140-2 (*1).
- A key can be delivered through the host interface and the interface between a library and tape drive.
- The encryption logic is implemented by hardware, which means that encryption has less effect on read-write performance.

*1: FIPS 140-2 defines the U.S. government's security requirements for cryptographic modules used for data.

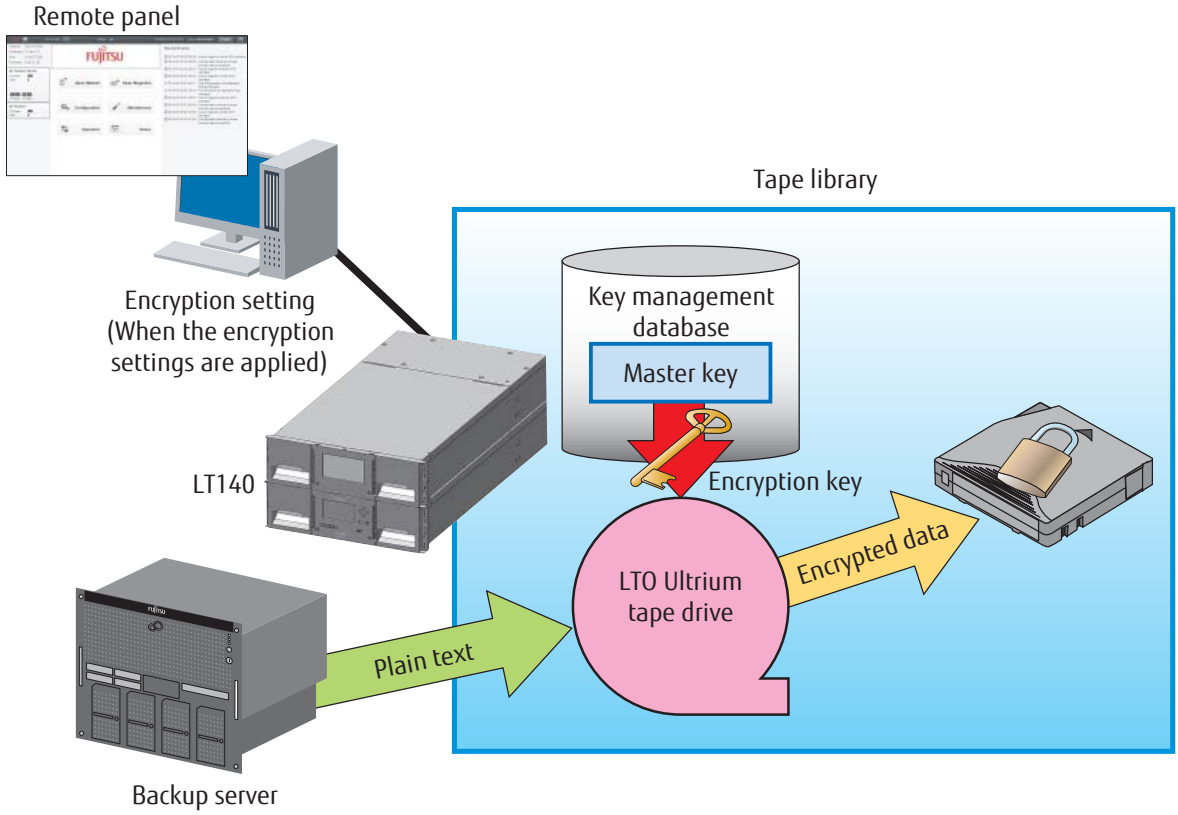
Copyright 2019 FUJITSU LIMITED

1.3 Functional Overview of the Key Management Function Option

The Key Management Function Option allows the use of the encryption function provided by Ultrium tape drives to manage encryption keys on the tape library.

Figure 1.1 shows how the Key Management Function Option works.

Figure 1.1 How the Key Management Function Option works



The Key Management Function Option applies the encryption settings from the remote panel to the tape library and assigns one key called the master key. The encryption key that is automatically generated for each data cartridge by the tape library is based on the master key, and this information is stored in a database in the tape library.

During a data backup from a backup server, the tape library automatically assigns an encryption key to the specified data cartridge, encrypts the data (plain text), and saves the data. The encryption process is performed transparently during this time.

Copyright 2019 FUJITSU LIMITED

Caution

The following tape drives and tape cartridges are required to use the Key Management Function Option:

- LTO Ultrium6 (G6) or later tape drives
- LTO Ultrium4 (G4) or later tape cartridges (G4 is for reading only)

For other required optional products, refer to "FUJITSU Storage ETERNUS LT140 Tape Library Product List". For more details about tape cartridges, refer to "A.1 Ultrium Tape Cartridge" in "FUJITSU Storage ETERNUS LT140 Tape Library User's Guide -Installation & Operation-".

Note

To use the key management function, purchasing the Key Management Function Option is required.

1.4 Features of the Key Management Function Option

The Key Management Function Option has the following features:

- It enables easy construction of a secure backup system that is independent of the OS and backup software, since the tape library will automatically handle encryption. (*1)
- Because encryption keys are set for the tape library from a Web browser terminal, the library manager alone can ensure the security of the library, with no need for a backup operator to intervene.
- One master key is set for each tape library, and encryption keys based on the master key are automatically assigned to all data cartridges in the tape library. Thus, the library manager need not manage any of the encryption keys of the data cartridges. (*2)
- Setting the same master key as the common master key for the ETERNUS LT140, LT220, LT230, LT250, LT260, LT270, and LT270 S2 (*3) will facilitate the use of encrypted tape cartridge data among all these tape libraries.
- To share data among multiple tape libraries, Fujitsu recommends operation with a common master key. In the event of a disaster, a data cartridge stored at an external location may need to be read with a tape library having a different master key. This different tape library can read the data on the data cartridge only if the encryption key had been exported in advance using the encryption key export or import function (*4).

*1: The Key Management Function Option cannot be used together with the encryption function of backup software.

*2: For information on master keys, refer to "1.5.1 Master Key" (page 14). For information on encryption keys, refer to "1.5.2 Encryption Key" (page 15).

*3: The ETERNUS LT20, LT20 S2, LT40, LT40 S2, LT60, LT60 S2, LT200, and LT210 do not support the key management function. The ETERNUS LT220, LT230, LT250, and LT270 have been discontinued.

*4: For information on the encryption key export or import function, refer to "2.1.5 Encryption Key Export and Import Functions" (page 45).

Copyright 2019 FUJITSU LIMITED

1.5 Types of Keys

The Key Management Function Option uses two types of keys for encryption: the master key that must have been set for each LT140 tape library, and the encryption key assigned to each tape cartridge in the tape library.

This section describes these keys.

1.5.1 Master Key

A master key is set for each tape library.

The tape library must have a master key set in order for the Key Management Function Option to work.

The functions of a master key are listed below.

- The encryption key for a data cartridge is automatically generated from a master key. (*1)
- The same master key can be set for multiple tape libraries. This function enables these multiple tape libraries to share data cartridges containing encrypted data.
- The tape library manager can make the settings to set a master key.
- In a logical library (or partition) configuration, a master key can also be assigned for reach logical library (or partition).

*1: Since automatically generated master keys are managed only by the tape library, their values are invisible to users.

The two methods of creating a master key are as follows: automatic generation using the tape library and manual creation using arbitrary characters.

For automatic generation with a tape library, each tape library automatically generates a master key based on data unique to the tape library. For this reason, other tape libraries cannot generate the same master key. Once a master key is created, the master key can no longer be decrypted even by a maintenance engineer.

Although the master key is stored redundantly in the database of the tape library, it may be lost in the rare event that the tape library fails. The encrypted data can no longer be read in such a case. Therefore, after setting the master key, be sure to export it (to a binary file) and keep it in a safe place.

Note

For information on setting a master key, refer to "2.1.4 Setting the Master Key" (page 35).
For information on exporting the master key, refer to "2.1.4.2 Exporting the Master Key" (page 37).

Copyright 2019 FUJITSU LIMITED

1.5.2 Encryption Key

An encryption key is assigned to each data cartridge.

Different data cartridges never have the same encryption key because the tape library automatically generates an encryption key based on the master key and data unique to each data cartridge.

If different tape libraries have the same master key and same data unique to the data cartridge, the libraries will generate the same encryption key for the cartridge.

Only one encryption key is assigned to each data cartridge.

During normal operations, because the tape library performs the encryption key operations, the user is not involved.

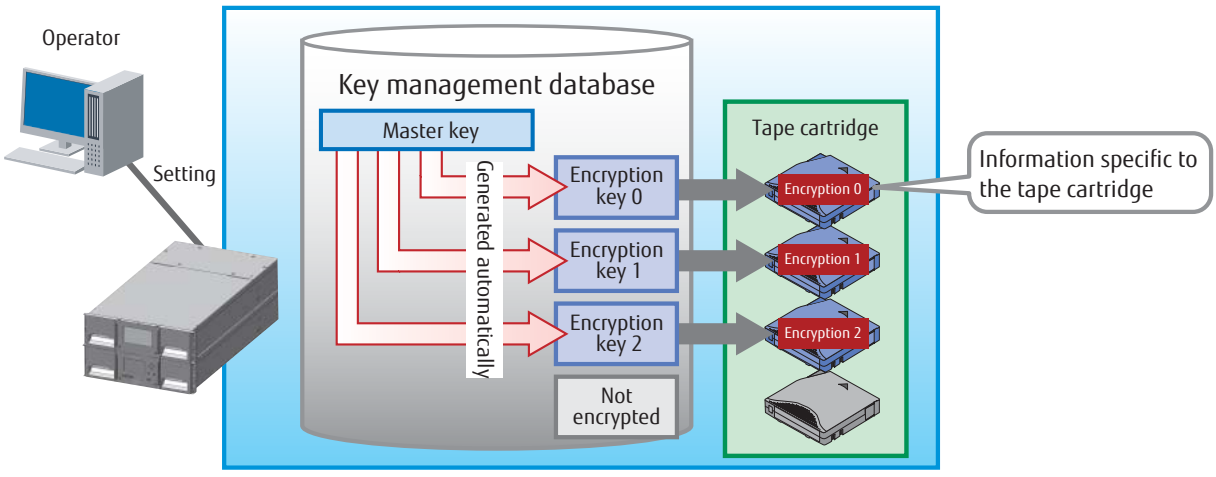
Caution

The encryption key export or import function can be used to export or import only an encryption key (a password and encrypted binary file) for data sharing between tape libraries with different master keys. However, note that if the encryption key is lost, the data can no longer be restored.
To share data among tape libraries, Fujitsu recommends operation with a common master key.

Note

- An encryption key is generated and assigned when a data write process is performed to the data cartridge.
- For information on the encryption key export or import function, refer to "2.1.5 Encryption Key Export and Import Functions" (page 45).

Figure 1.2 Automatic generation of encryption keys



Copyright 2019 FUJITSU LIMITED

1.5.3 Management of Key Information and Encryption Setting Information

Although key information and encryption setting information are stored in a redundant manner in the tape library, encryption keys may be lost in the rare event that the tape library fails. The encrypted data saved on data cartridges can no longer be decrypted in such a case. Therefore, after registering a master key or setting an encryption key for a data cartridge, be sure to export the encryption key and keep it in a safe place.

For information on exporting a master key, refer to "2.1.4.2 Exporting the Master Key" (page 37). For information on backing up encryption setting information, refer to "2.2 Backing Up the Setting Information" (page 58).

1.6 Operational Examples

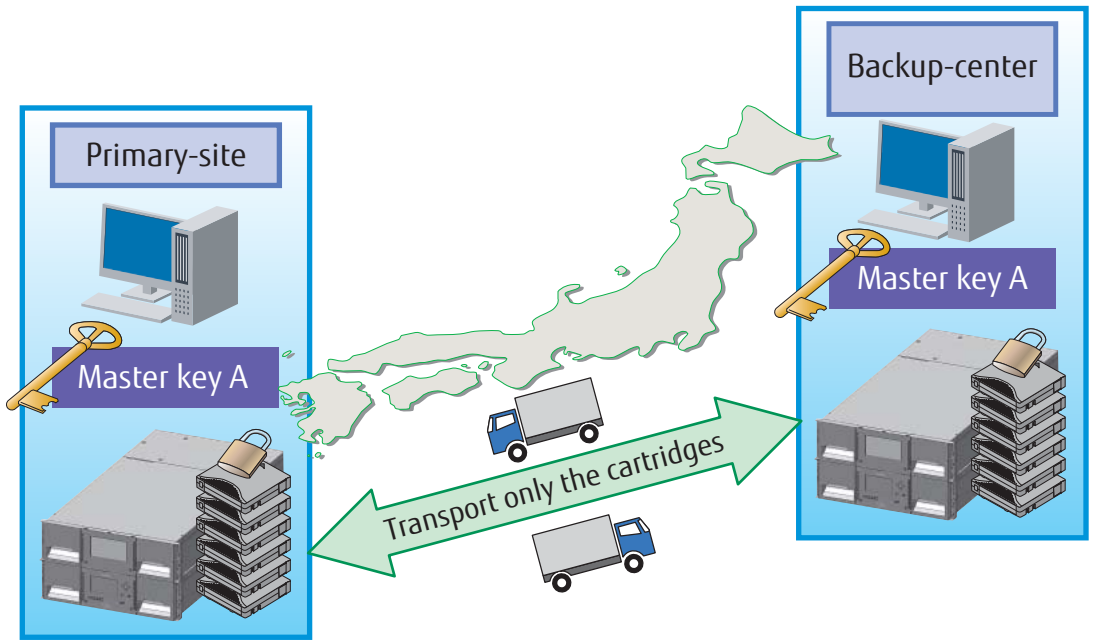
It is not necessary to make any change to existing operations in order to use data encryption using the Key Management Function Option.

This section describes operational examples of sharing data on encrypted data cartridges among multiple tape libraries and external storage of encrypted data cartridges.

1.6.1 Data Sharing between Centers

Setting the same master key for multiple tape libraries installed in the same center or separate centers enables these libraries to share data cartridges with encryption keys hidden from view.

Figure 1.3 Data cartridge sharing using one master key



Copyright 2019 FUJITSU LIMITED

1.6.2 Encryption of Data Cartridges Stored at an External Location

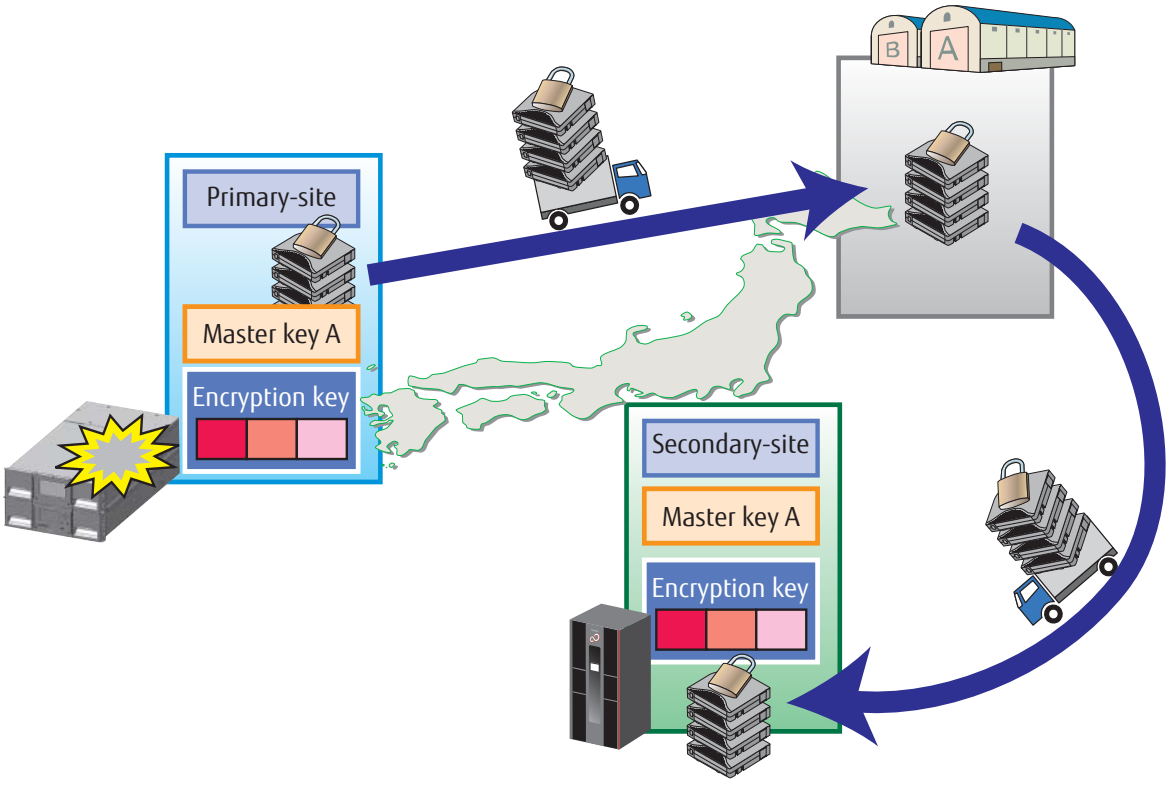
For disaster recovery, encrypted data cartridges can be stored at an external location and, when needed, brought back to read the data on them. Even if a data cartridge in storage is lost or stolen, the encryption can prevent data leakage.

Once a data cartridge in storage is inserted into its original tape library or one with the same master key, the data can be read from the library without setting the key again.

Note

Once encryption keys are exported, even if the tape library becomes unavailable such as in the event of a disaster, data on the data cartridge can be read by importing the encryption key to a tape library with a different master key.

Figure 1.4 External storage of data cartridges

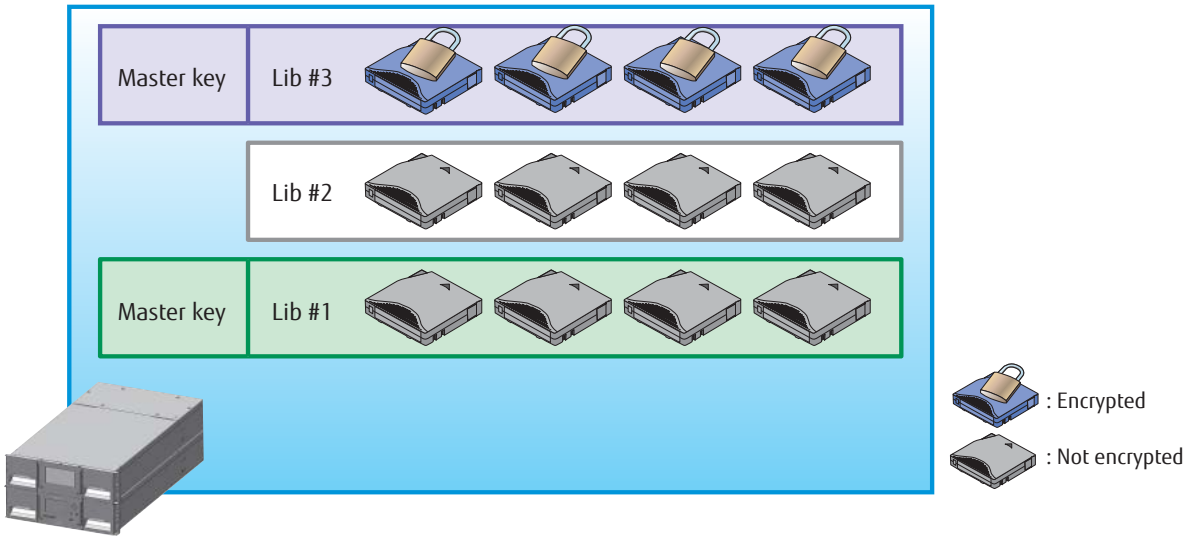


Copyright 2019 FUJITSU LIMITED

1.6.3 Encryption of Each Logical Library (or Partition)

In a logical library (or partition) configuration, the master key can be assigned individually to each logical library (or partition).

Figure 1.5 Encryption of each logical library



Copyright 2019 FUJITSU LIMITED

1.6.4 Interoperation among LT-series Models

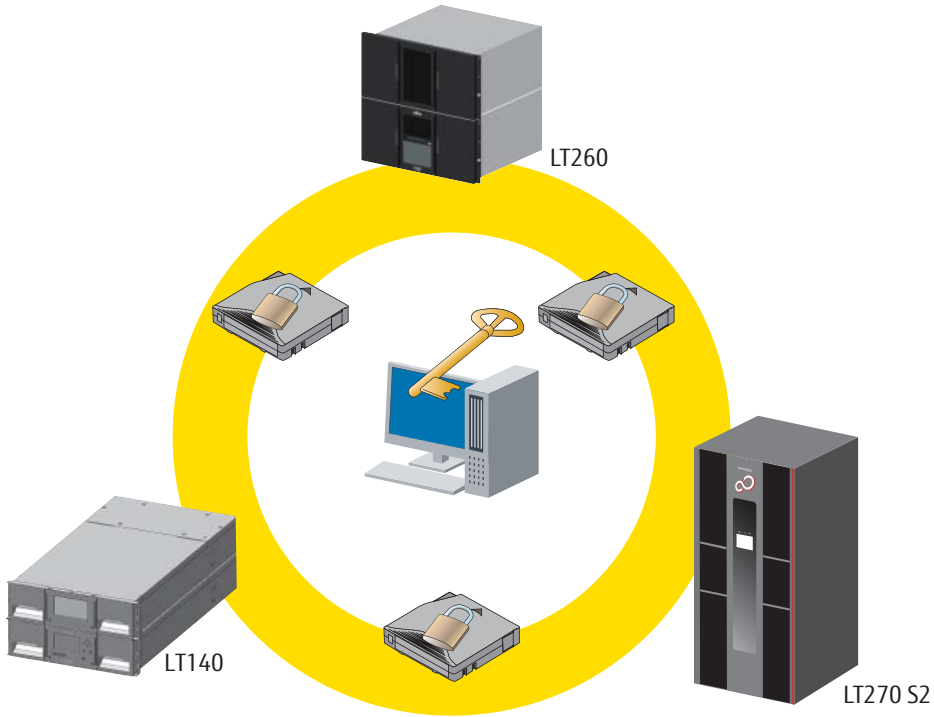
The ETERNUS LT140, LT220, LT230, LT250, LT260, LT270, and LT270 S2 tape libraries (LT-series) share compatible master keys and encryption keys, so keys and encrypted data cartridges can be shared among these LT-series.

Setting a common master key for these tape libraries facilitates data sharing and data migration between the tape libraries.

Caution

- The Key Management Function Option does not support interoperability with the tape libraries, encryption devices, software encryption functions, and other related hardware or software manufactured by other companies.
- Sales of the ETERNUS LT220, LT230, LT250, and LT270 tape libraries have been discontinued.

Figure 1.6 Interoperation among LT-series models



Copyright 2019 FUJITSU LIMITED

1.7 Security Functions

This section describes the security functions that are used for the Key Management Function Option.

1.7.1 Security Account

The security account is used from the remote panel for operations and settings related to the key management function.

To log in to the remote panel, the security administrator account, "security", is used for operations and settings of the key management function.

The security administrator logs in with this dedicated account to make all the relevant settings. Anyone who logs in with another account cannot modify the settings of the key management function.

For information on how to log in with the security account, refer to "2.1.2.2 Logging in to the Remote Panel" (page 24).

1.7.2 Network Security

The protocol for the connection to the remote panel via a LAN can be set to "https," which encrypts the data that is the transmitted information.

For information on the https setting, refer to "2.1.2.3 Enabling SSL" (page 26).

1.7.3 Security-Related Logs

A history of key management function operations or settings is automatically recorded in a log. This enables the tracking of unauthorized access and operations.

For information on the storage and contents of the security-related logs, refer to "Appendix A Logs Related to the Key Management Function" (page 76).

Copyright 2019 FUJITSU LIMITED

Chapter 2

Setup and Operation Procedures

This chapter explains the settings that are related to the key management function.

The setup and operations for each function are performed from the remote panel. For details about the setup and operations, refer to "FUJITSU Storage ETERNUS LT140 Tape Library User's Guide -Panel Operation-".

CAUTION

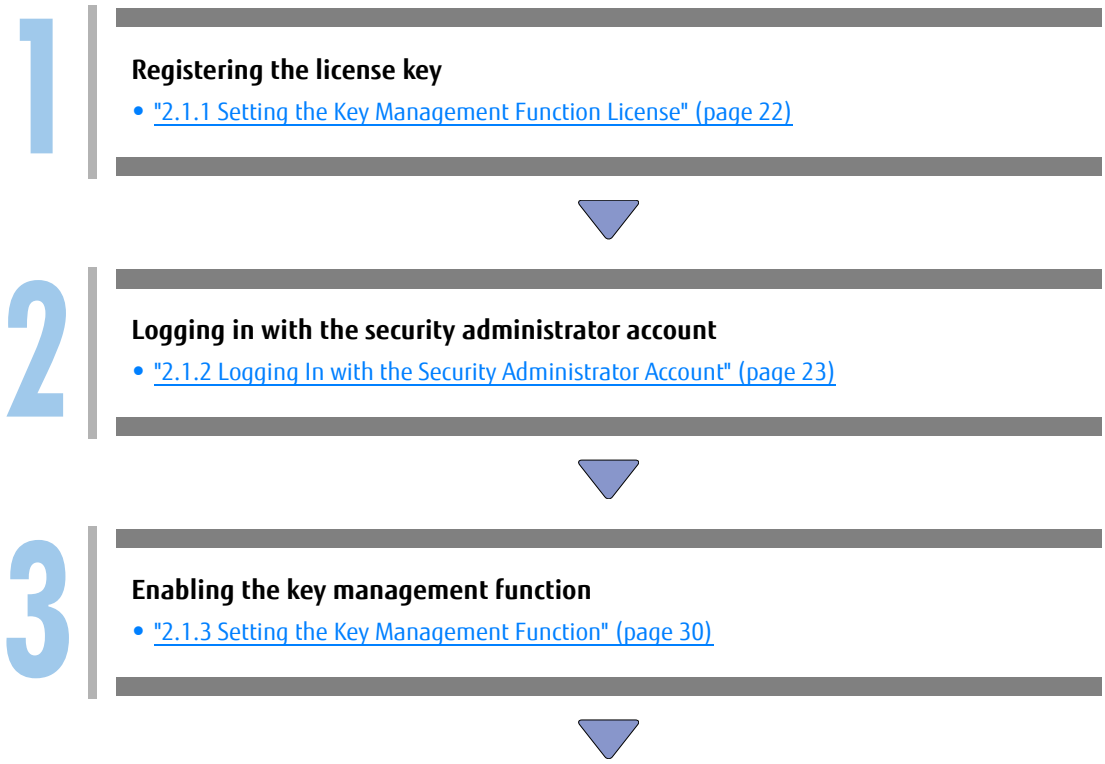
Do

- Perform the setup while the tape library is not in operation. Otherwise, data may be lost.

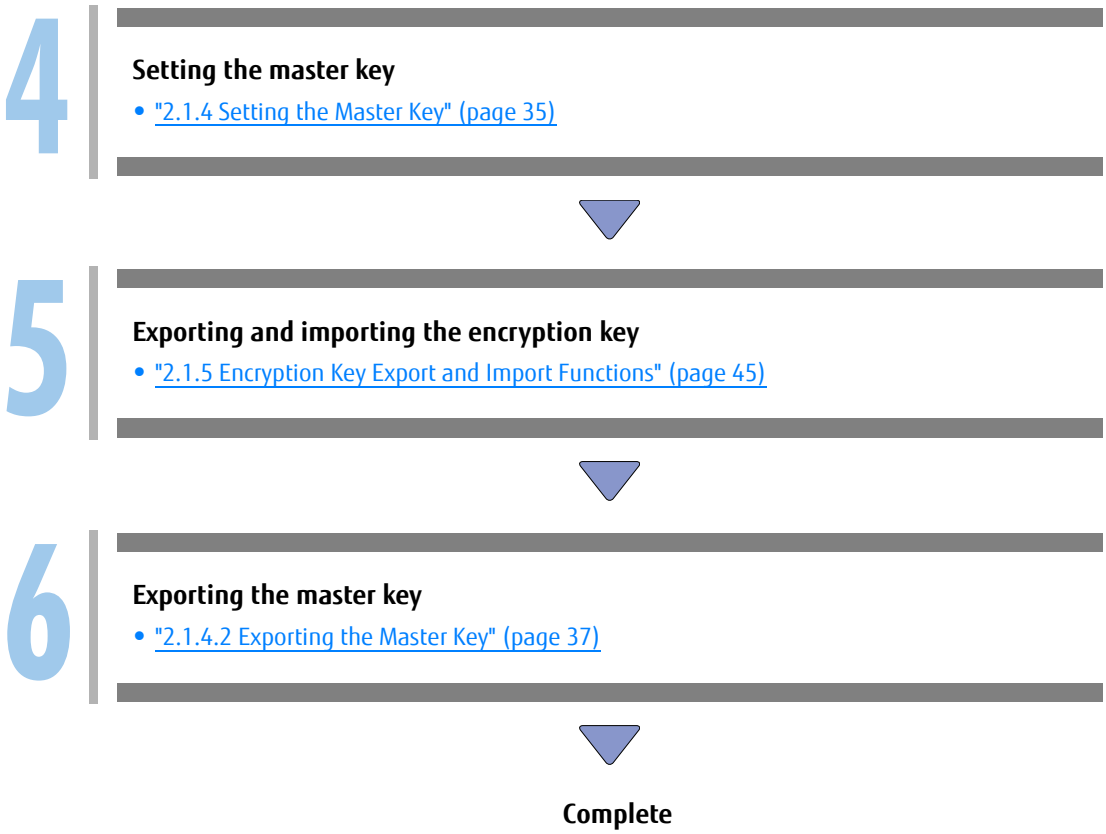
2.1 Basic Setup

This section provides the procedure for the basic setup of the key management function.

Figure 2.1 Basic setup procedure



Copyright 2019 FUJITSU LIMITED



2.1.1 Setting the Key Management Function License

Once the license key on the license sheet that is provided with the Key Management Function Option is entered, the key management function can be set.

Ask a maintenance engineer to perform this setting.

Caution

- If the tape library and the Key Management Function Option are purchased together, the license is already set and does not need to be set again.
- The license key for the Key Management Function Option cannot be used with a tape library that has a different serial number. Since the license sheet that has the license key may be required for maintenance work, be sure to keep it in a safe place.

Copyright 2019 FUJITSU LIMITED

2.1.2 Logging In with the Security Administrator Account

To use the key management function, you must log in to the remote panel using the security administrator account with Secure Socket Layer (SSL) enabled.

The following describes the initial settings for logging in to the remote panel with the security administrator account and the procedure for enabling SSL.

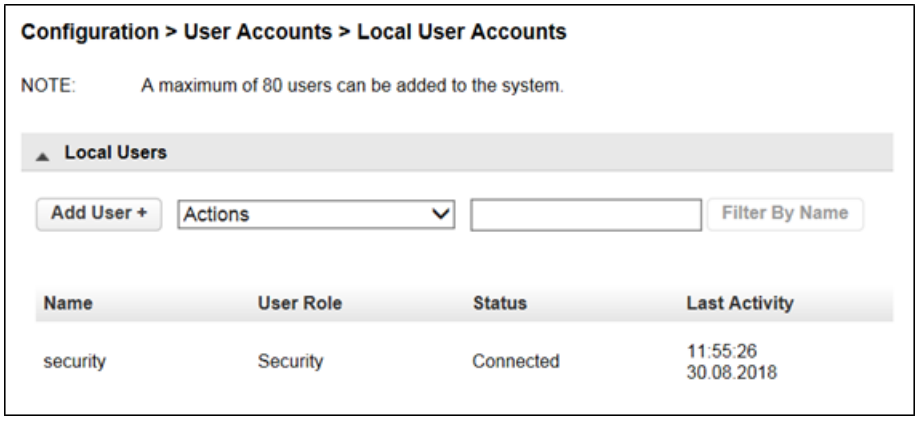
2.1.2.1 Changing the Initial Password of the Security Administrator Account

Change the password of the security administrator account with the [Configuration > User Accounts > Local User Accounts] screen on the remote panel.

Note

If the initial password has been changed, this procedure is not required.

Figure 2.2 Account setting screen



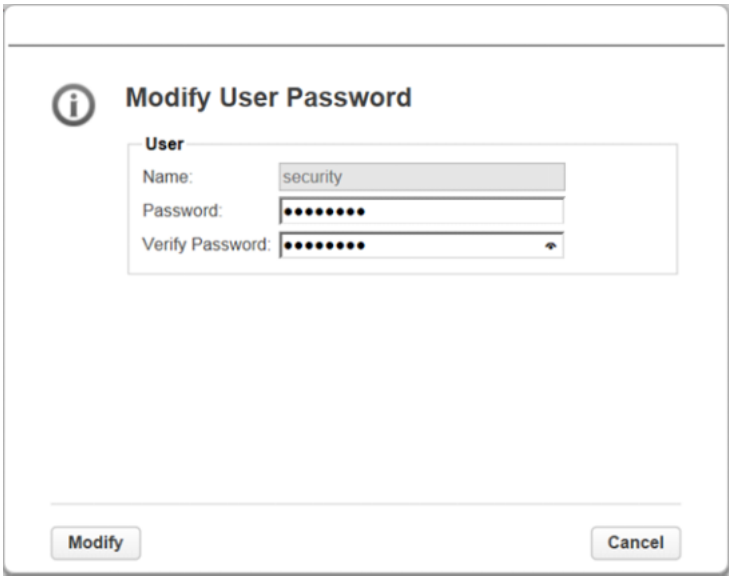
Procedure

1. Click "security" from the account list displayed on the lower part of the screen.
2. Select [Modify User Password] from [Actions].

Copyright 2019 FUJITSU LIMITED

3 When the [Modify User Password] screen appears, enter the new password in both boxes.

Figure 2.3 Changing passwords



4 Click [Modify].

End of procedure

Note

For password settings, passwords must satisfy the requirements. If the password setting does not succeed, check the setting requirements from [Configuration > User Accounts > User Accounts Settings]. For details about the setting items, refer to "3.4.16 Configuring Password Setting Requirements" in "FUJITSU Storage ETERNUS LT140 Tape Library User's Guide -Panel Operation-".

2.1.2.2 Logging in to the Remote Panel

The procedure for logging in to the remote panel with the security administrator account is described below.

The security administrator has the following account name and initial password.

User (account name)	security (alphabetical characters)
Password (initial password)	security (alphabetical characters)

Caution

- For security purposes, changing the initial password after starting the library is recommended.
  For details about how to change passwords, refer to "2.1.2.1 Changing the Initial Password of the Security Administrator Account" (page 23).
- When connecting to the remote panel, use Internet Explorer 10 or later.

Copyright 2019 FUJITSU LIMITED

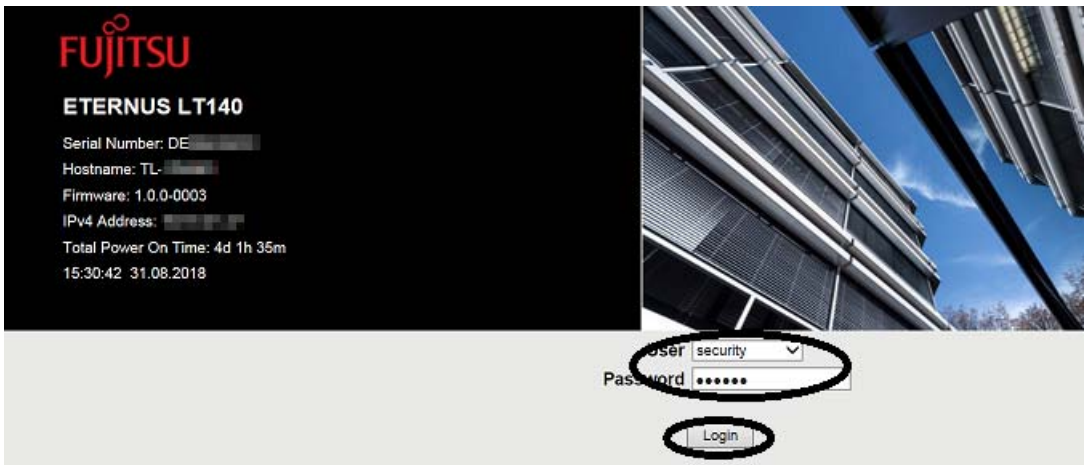
Procedure

1. Enter "http://(IP address of the tape library)" in the address bar on the web browser to access the remote panel.
2. Select [security] from the [User] pull-down menu.
3. For [Password], enter the security administrator account password that was set and click [Login].

Note

The initial password of the security administrator account is "security".
If the initial password is not changed, change it immediately after logging in to the remote panel.
For details about how to change passwords, refer to "2.1.2.1 Changing the Initial Password of the Security Administrator Account" (page 23).

Figure 2.4 Logging in to the remote panel



End of procedure

Copyright 2019 FUJITSU LIMITED

2.1.2.3 Enabling SSL

Before the key management function is used, Secure Socket Layer (SSL) must be enabled to access the remote panel securely.

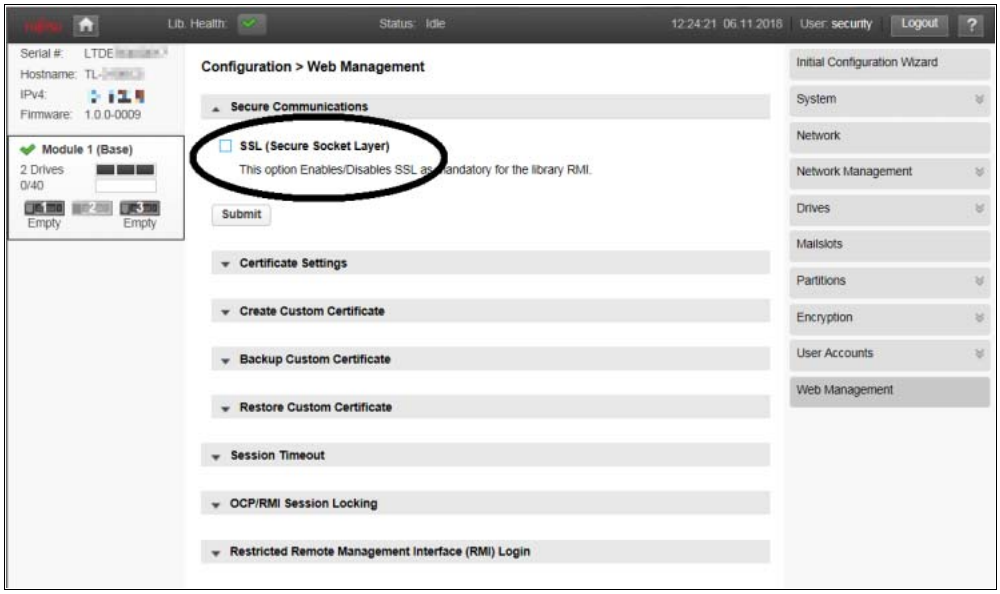
When SSL is enabled, https must be used to connect to the remote panel.

SSL is disabled by default.

Procedure

1 Move to the [Configuration > Web Management] screen.

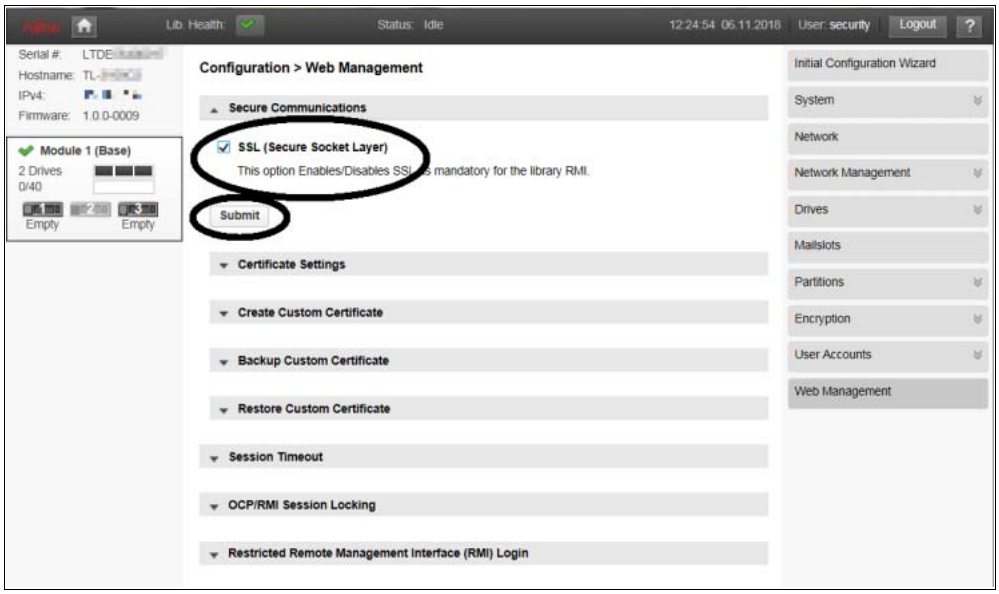
Figure 2.5 Initial value of SSL (disabled)



Copyright 2019 FUJITSU LIMITED

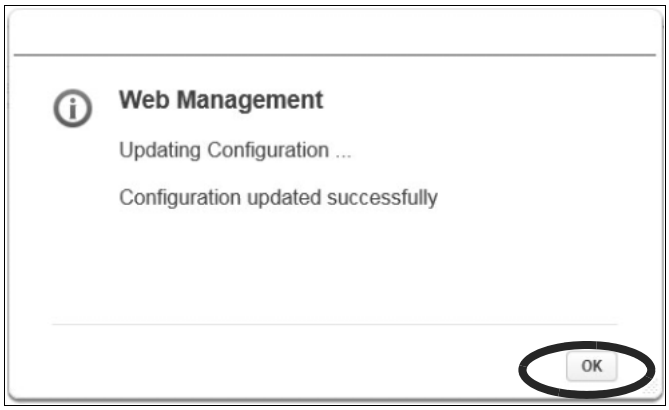
2 Select the [SSL (Secure Socket Layer)] checkbox to enable SSL.
Click [Submit] to update the setting.

Figure 2.6 SSL setting (enabled)



3 When the SSL confirmation screen for the change appears, click [OK].

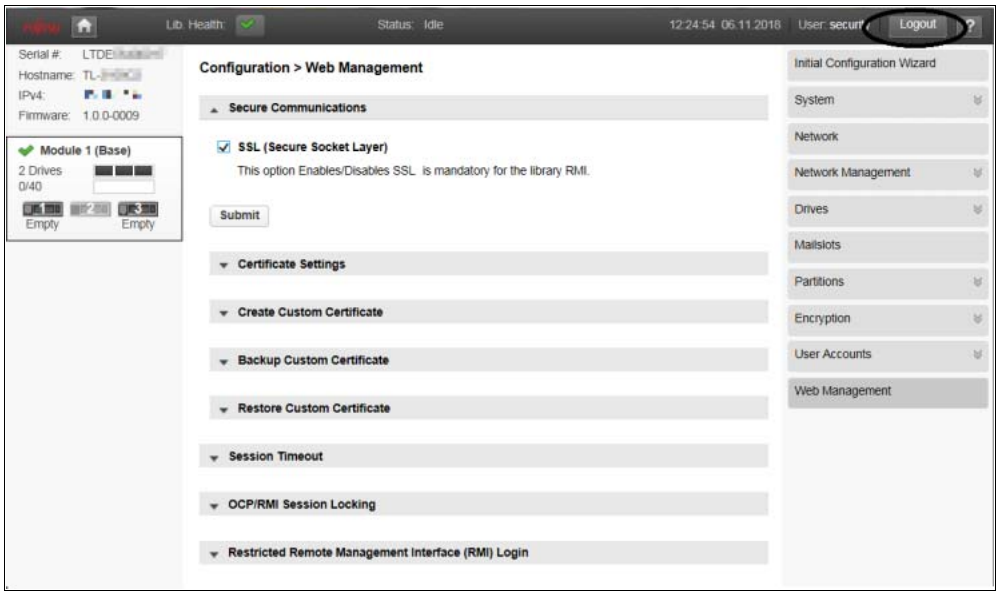
Figure 2.7 Confirming the SSL setting change



Copyright 2019 FUJITSU LIMITED

4 To update the changed SSL setting, log out of the remote panel. Use the LOGOUT icon on the upper of the screen to log out.

Figure 2.8 Logging out of the remote panel



End of procedure

Caution

After SSL is enabled, the method for connecting to the remote panel changes.
For the connection method, refer to "2.1.2.4 Connecting to the Remote Panel after Enabling SSL" (page 29).

Copyright 2019 FUJITSU LIMITED

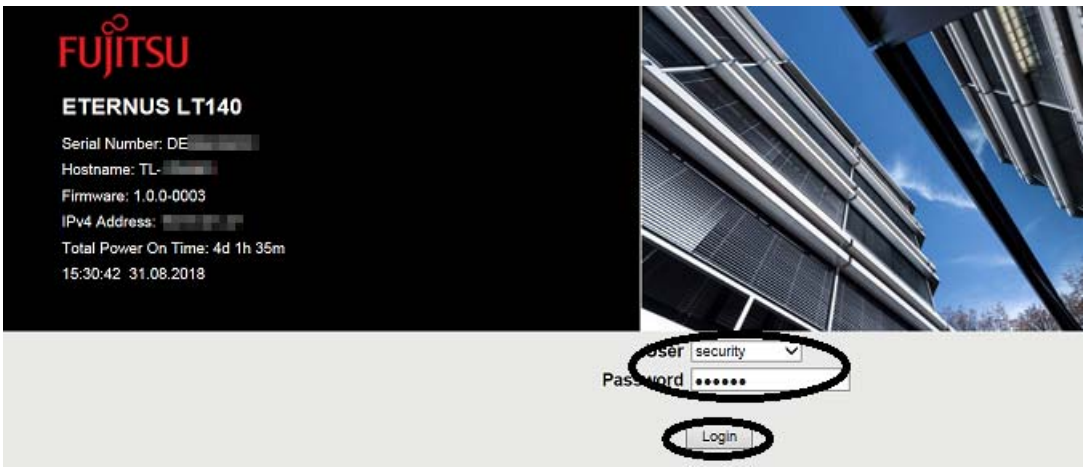
2.1.2.4 Connecting to the Remote Panel after Enabling SSL

The method for connecting to the remote panel after SSL is enabled is provided below.

Procedure

1. Enter "https://(IP address of the tape library)" in the address bar on the web browser.
2. Any attempt to connect to a web service that is not registered as an approved site causes a security certificate warning to appear.
3. Click [Continue to this website (not recommended)].
   The remote panel is connected while SSL is enabled.
   "Certificate Error" is displayed in the login screen. This does not cause any problems to the remote panel operations.
4. Select [security] from the [User] pull-down menu.
5. For [Password], enter the security administrator account password and click [Login].

Figure 2.9 Logging in to the security administrator account



End of procedure

Copyright 2019 FUJITSU LIMITED

2.1.3 Setting the Key Management Function

This setting sets the key management function. The methods that are available for setting this function are to set all the related settings at once or to enable/disable the encryption key management function only.
For logical library (or partition) configurations, regardless of the method used, the key management function can be enabled/disabled for each logical library (or partition).

Caution

- Even when this setting is performed, data that is already written in a data cartridge is not encrypted. After deleting existing data and enabling the key management function, write the data to the data cartridge again.
- To perform this setting, the key management function license must be set in advance. For details, refer to "2.1.1 Setting the Key Management Function License" (page 22).
- When changing the logical library (or partition) configuration or when changing the setting to enable or disable the key management function, back up the encryption key in advance.

Note

To set the key management function, you must log in to the remote panel using the security administrator account. For details about how to log in, refer to "2.1.2 Logging In with the Security Administrator Account" (page 23).

Copyright 2019 FUJITSU LIMITED

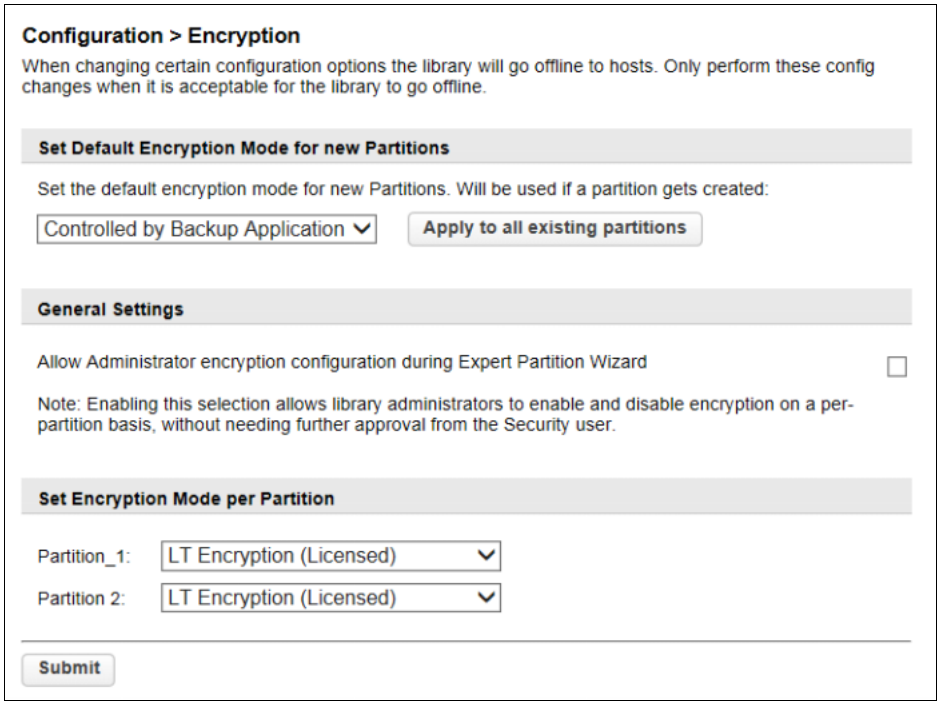
2.1.3.1 Basic Setup of the Key Management Function

This setting sets the key management function.

Procedure

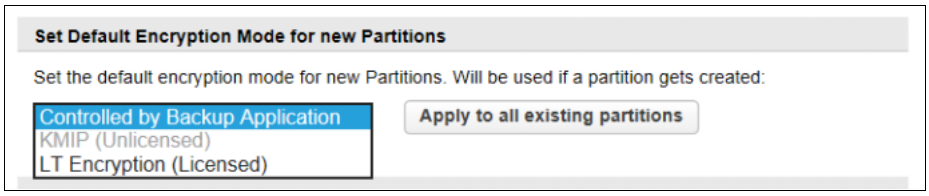
1 Move to the [Configuration > Encryption] screen.

Figure 2.10 Setting the key management function



2 Apply the default settings of the key management function (for a new partition).
Select [LT Encryption (Licensed)] from the [Set Default Encryption Mode for new Partitions] pull-down menu.

Figure 2.11 Default setting of the key management function



Copyright 2019 FUJITSU LIMITED

Note

After the default settings of the key management function are changed by using this step, the setting to enable or disable the key management function is automatically selected based on the default settings when a new partition is created.
If the default settings are not changed, omit this step and proceed to Step 4.

3 Apply the default settings of the key management function to all existing partitions.

Click [Apply to all existing partitions]. Confirm that [LT Encryption (Licensed)] is selected for all the partitions displayed in [Set Encryption Mode per Partition].

Note

If the default settings are not applied to the existing partitions, omit this step and proceed to Step 4.

4 Allow the administrator account permission to set the key management function.

Select the checkbox in [General Settings] to allow the administrator account permission to enable or disable the settings for the key management function in the Expert Partition Wizard.
For details about the Expert Partition Wizard, refer to "3.4.13.2 Using the Expert Partition Wizard" in "FUJITSU Storage ETERNUS LT140 Tape Library Use's Guide -Panel Operation-".

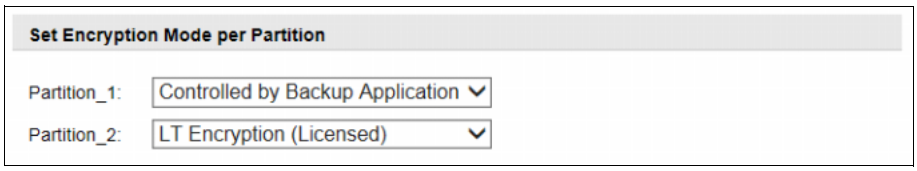
Note

When the Expert Partition Wizard is used with the security administrator account, the setting for the key management function can be enabled or disabled at any time.

5 Enable or disable the key management function for each logical library (or partition).

From the pull-down menu of [Set Encryption Mode per Partition] for each partition, select [LT Encryption (Licensed)] to enable the key management function or [Controlled by Backup Application] to disable it.

Figure 2.12 Setting the key management function per partition



Note

If the default settings are applied to all partitions in Step 3 without any changes, this step is not required.

6 Click [Submit].

Copyright 2019 FUJITSU LIMITED

Note

- After the default settings of the key management function are changed, the setting to enable or disable the key management function is automatically selected based on the default settings when a new partition is created.
- When the Expert Partition Wizard is used to edit the partition, the setting for the key management function can be enabled or disabled. For details, refer to "3.4.13.2 Using the Expert Partition Wizard" in "FUJITSU Storage ETERNUS LT140 Tape Library User's Guide -Panel Operation-".
- When the key management function is disabled, data encryption depends on the backup software setting.

End of procedure

Copyright 2019 FUJITSU LIMITED

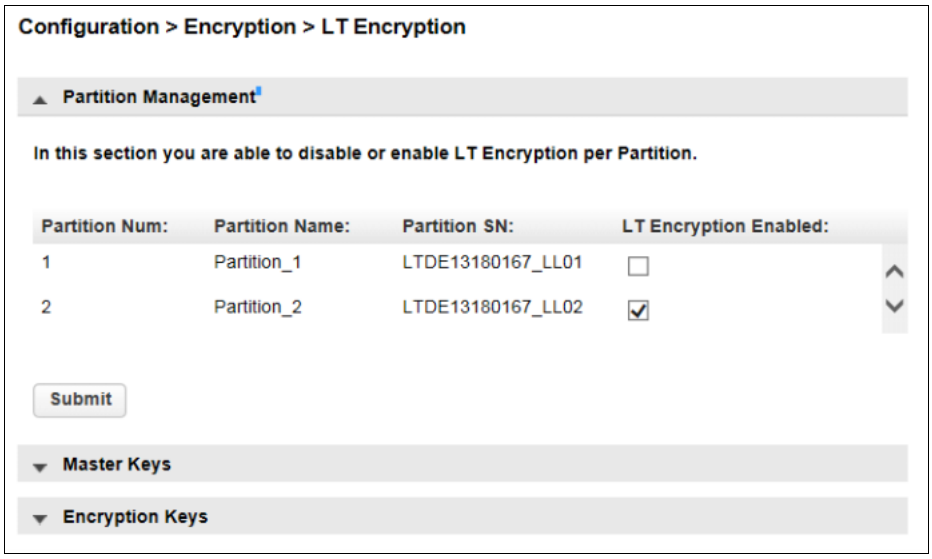
2.1.3.2 Setting the Key Management Function for Each Logical Library (Partition)

This setting enables or disables the key management function for the existing partitions. Refer to "2.1.3.1 Basic Setup of the Key Management Function" (page 31) to perform basic setup other than enabling or disabling the key management function.

Procedure

1. Move to the [Configuration > Encryption > LT Encryption] screen.
2. Select whether to enable or disable the key management function for each partition.
3. Click [Submit].

Figure 2.13 Example setting of the key management function for each partition



Note

- The settings related to the key management function conform to the basic setup when a partition is edited or created. Refer to "2.1.3.1 Basic Setup of the Key Management Function" (page 31) to perform basic setup.
- When the key management function is disabled, data encryption depends on the backup software setting.

End of procedure

Copyright 2019 FUJITSU LIMITED

2.1.4 Setting the Master Key

This section provides the procedure for setting a master key in the tape library to use the key management function.

Caution

If a master key is already set, the old master key is overwritten with a new master key. Data that was encrypted using the old master key cannot be read. Back up the old master key in advance so that the master key can be changed back to the old master key to read the data as required. In addition, by exporting and importing the encryption key for the required data cartridge, changing back the master key is not required even if the master key is changed. For details about backing up the master key, refer to "2.1.4.2 Exporting the Master Key" (page 37).

2.1.4.1 Setting the Master Key

This section provides the procedure for setting a master key in the partition where the key management function is enabled.

Procedure

1. Move to the [Configuration > Encryption > LT Encryption] screen.
2. Select [Master Keys] > [Set Manual Key] on the center pane.
3. Enter a new master key in both boxes.
   The master key must be specified within 8 to 16 characters. Uppercase and lowercase alphanumeric characters and special characters can be used.
4. Select the partition where the master key is to be set.

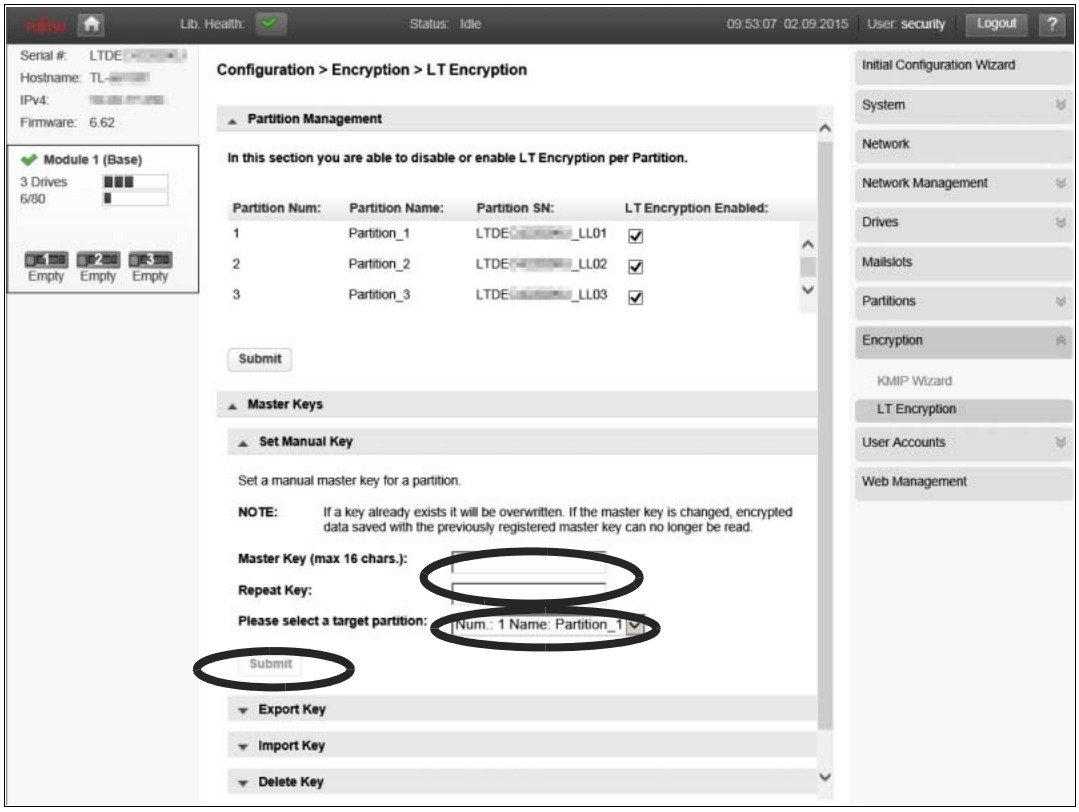
   Note

   If no logical libraries (or partitions) are configured, only "Partition_1" is displayed in the drop down list.

Copyright 2019 FUJITSU LIMITED

5 Click [Submit].

Figure 2.14 Setting the master key



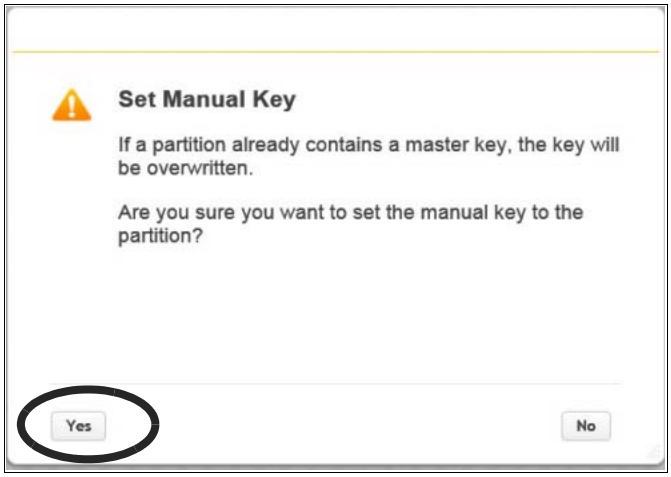
Copyright 2019 FUJITSU LIMITED

6 On the confirmation screen, click [Yes] to confirm the setting.

Caution

If a master key is already set, the old master key is overwritten with a new master key. Data that was encrypted using the old master key cannot be read. For details about backing up the master key, refer to "2.1.4.2 Exporting the Master Key" (page 37).

Figure 2.15 Confirmation screen for the master key setting



End of procedure

2.1.4.2 Exporting the Master Key

The purposes for exporting the master key are as follows.

- Backing up the master key
  By exporting the generated master key, backups are saved externally.
- Sharing the master key with other tape libraries
  When the encrypted data is shared between multiple tape libraries, the master key is shared by importing the exported master key to other tape libraries.

Note

For the LT140, if a maintenance part must be replaced due to a failure, the master key and encryption keys may need to be exported and imported by the user.

When exported, the master key is created as a binary file that is protected by a password. There is no risk of decrypting the master key.

Caution

If a master key is not set and the imported master key does not exist, a master key is automatically created when the data is first written to the data cartridge in each partition.

Copyright 2019 FUJITSU LIMITED

Procedure

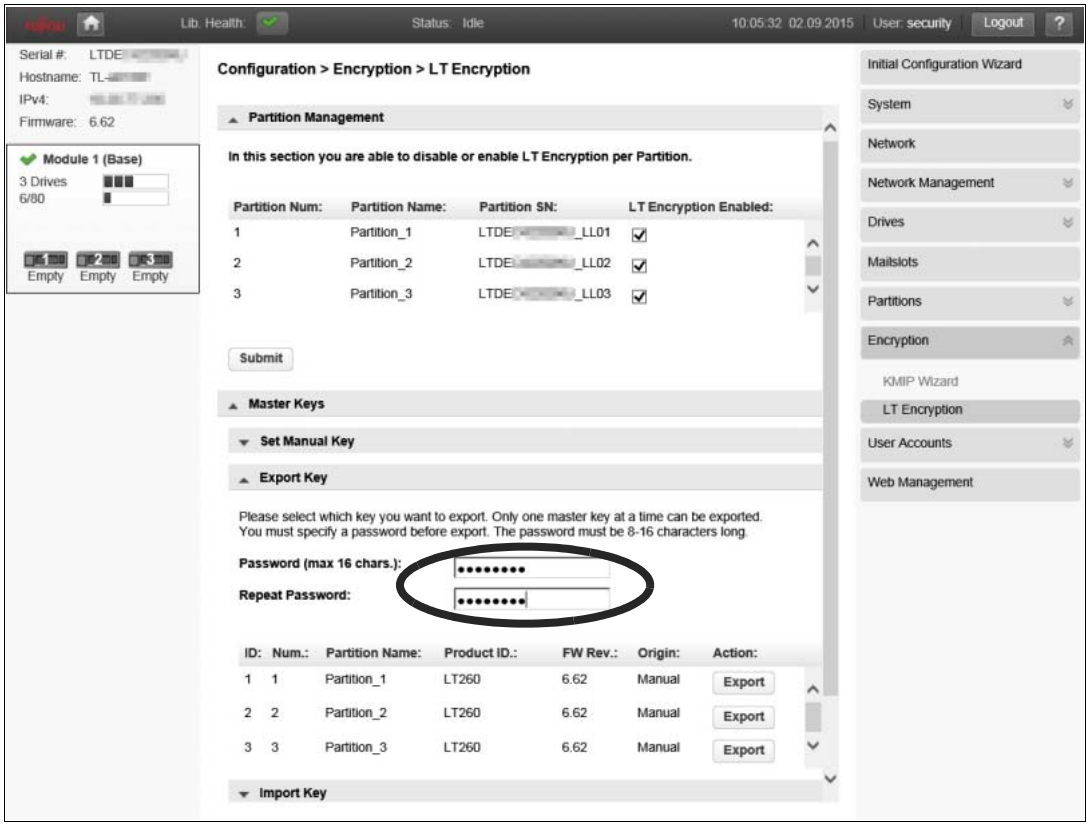
1. Move to the [Configuration > Encryption > LT Encryption] screen.
2. Select [Master Keys] > [Export Key] on the center pane.
3. Enter the password in both boxes.

   The password must be specified within 8 to 16 characters. Uppercase and lowercase alphanumeric characters and special characters can be used.

Caution

The password is required to import the master key. Keep the password in a safe place.

Figure 2.16 Setting a password for the master key



Copyright 2019 FUJITSU LIMITED

4 Click [Export] for the partition where the master key that is to be exported exists.

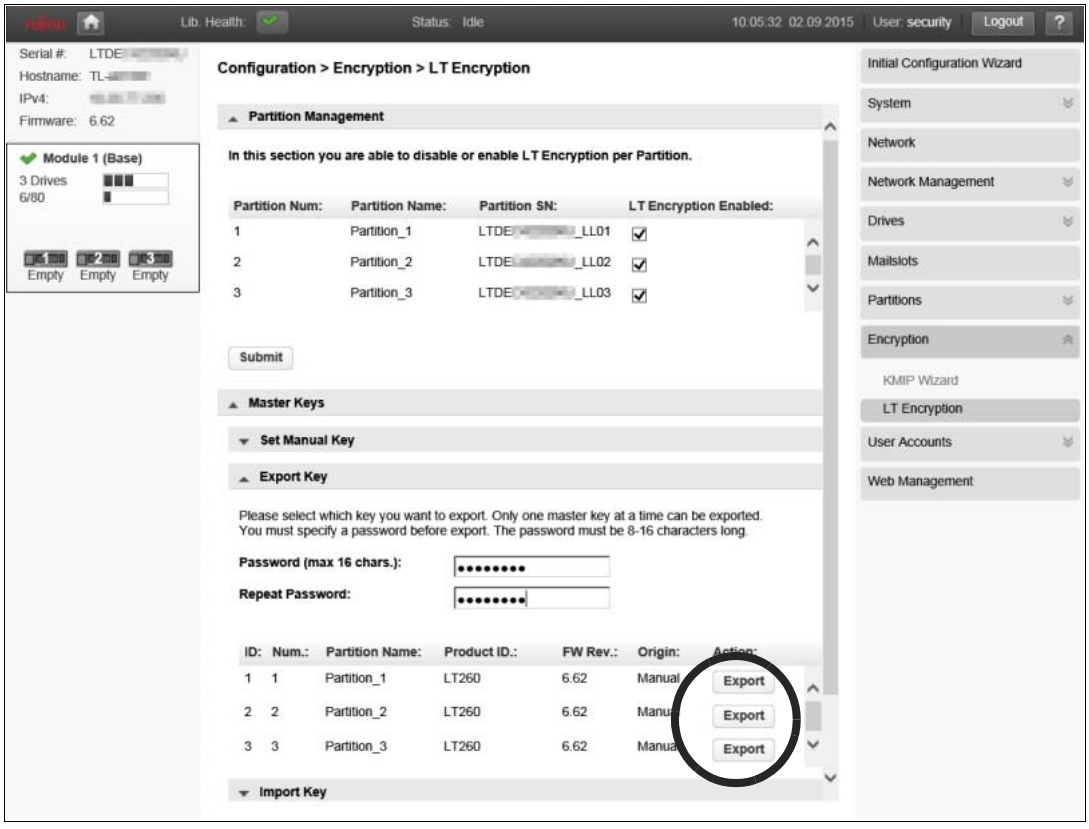
Note

If no logical libraries (or partitions) are configured, only "Partition_1" is displayed in the partition list.

Caution

Only a single master key can be exported at a time. When exporting the master keys of multiple partitions, repeat the procedure from Step 4 and onward. Partitions cannot be selected if the master key is not set.

Figure 2.17 Exporting the master key



Copyright 2019 FUJITSU LIMITED

5 Specify the destination to which the master key is exported.

Caution

The operation for saving the master key differs depending on the OS.

The default file name for the exported master key is determined by the "ID_x_MasterKey_yyyymmdd_xxxxxxxxxx.key" format. The file size is 128 bytes.

Figure 2.18 Saving the master key to export

End of procedure

2.1.4.3 Importing the Master Key

Caution

If the master key is already set, the old master key is overwritten with a new master key. Data that was encrypted using the old master key cannot be read. Back up the old master key in advance so that the master key can be changed back to the old master key to read the data as required. In addition, by exporting and importing the encryption key for the required data cartridge, changing back the master key is not required even if the master key is changed. For details about backing up the master key, refer to "2.1.4.2 Exporting the Master Key" (page 37).

Procedure

1 Move to the [Configuration > Encryption > LT Encryption] screen.

2 Select [Master Keys] > [Import Key] on the center pane.

3 Select the master key file to be imported.

Copyright 2019 FUJITSU LIMITED

4 Select the destination partition where the master key is to be imported.

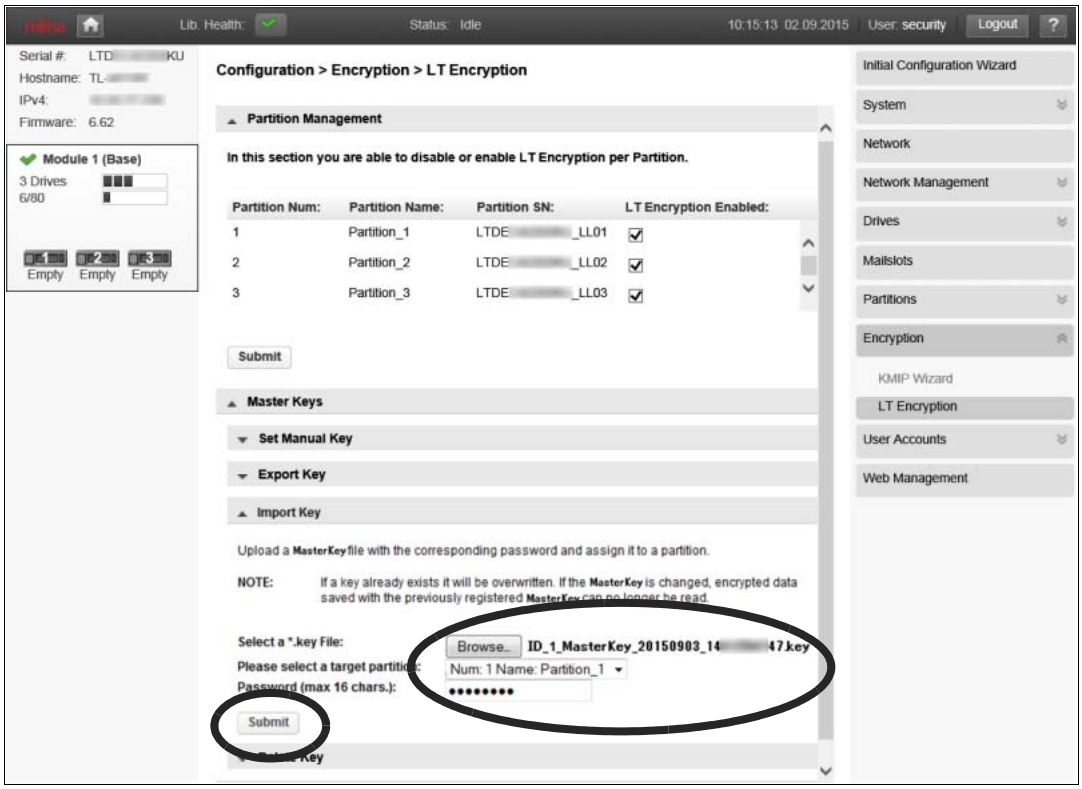
Note

If no logical libraries (or partitions) are configured, only "Partition_1" is displayed in the drop down list.

5 Enter the password that was set when the master key was exported.
For details, refer to "2.1.4.2 Exporting the Master Key" (page 37).

6 Click [Submit].

Figure 2.19 Importing the master key



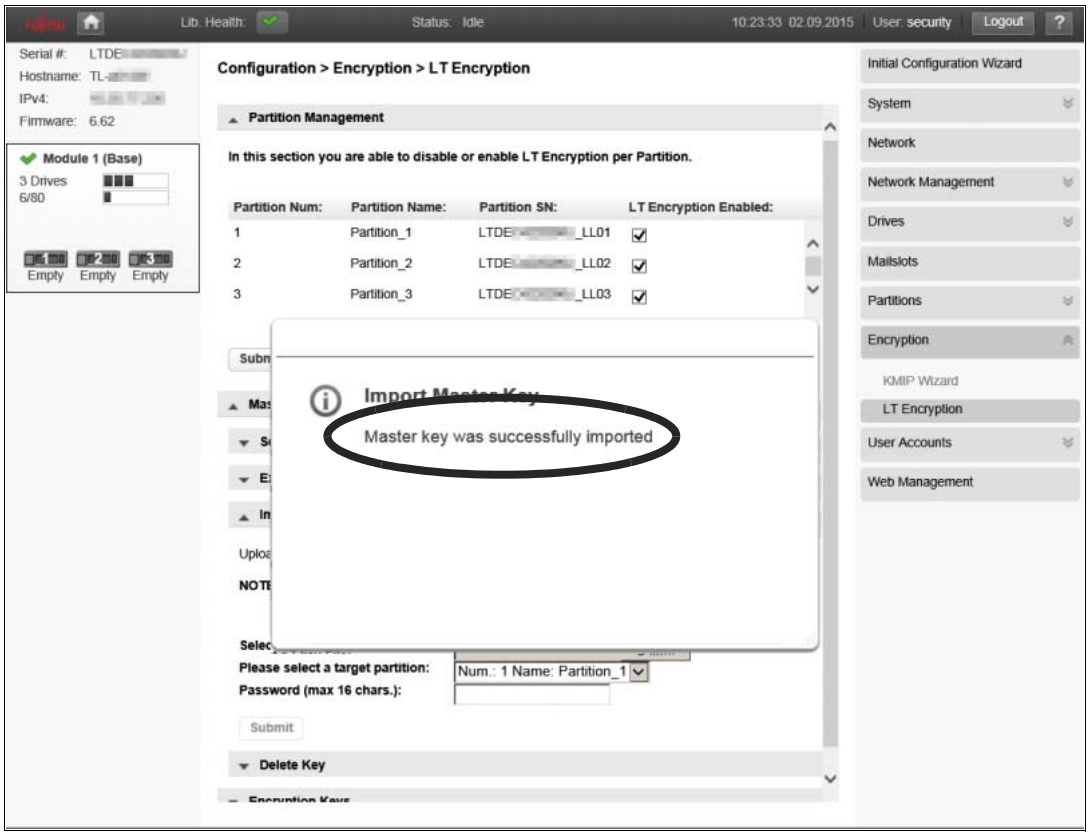
Copyright 2019 FUJITSU LIMITED

7 On the confirmation screen, click [Yes] to import the master key.

Figure 2.20 Confirmation screen for importing the master key

If the "Master key was successfully imported" message disappears, the master key has been imported.

Figure 2.21 Status of importing the master key



End of procedure

Copyright 2019 FUJITSU LIMITED

2.1.4.4 Deleting the Master Key

This function can delete any unnecessary master key.

Procedure

1. Move to the [Configuration > Encryption > LT Encryption] screen.
2. Select [Master Keys] > [Delete Key] on the center pane.
3. Click [Delete] for the partition where the master key that is to be deleted exists.

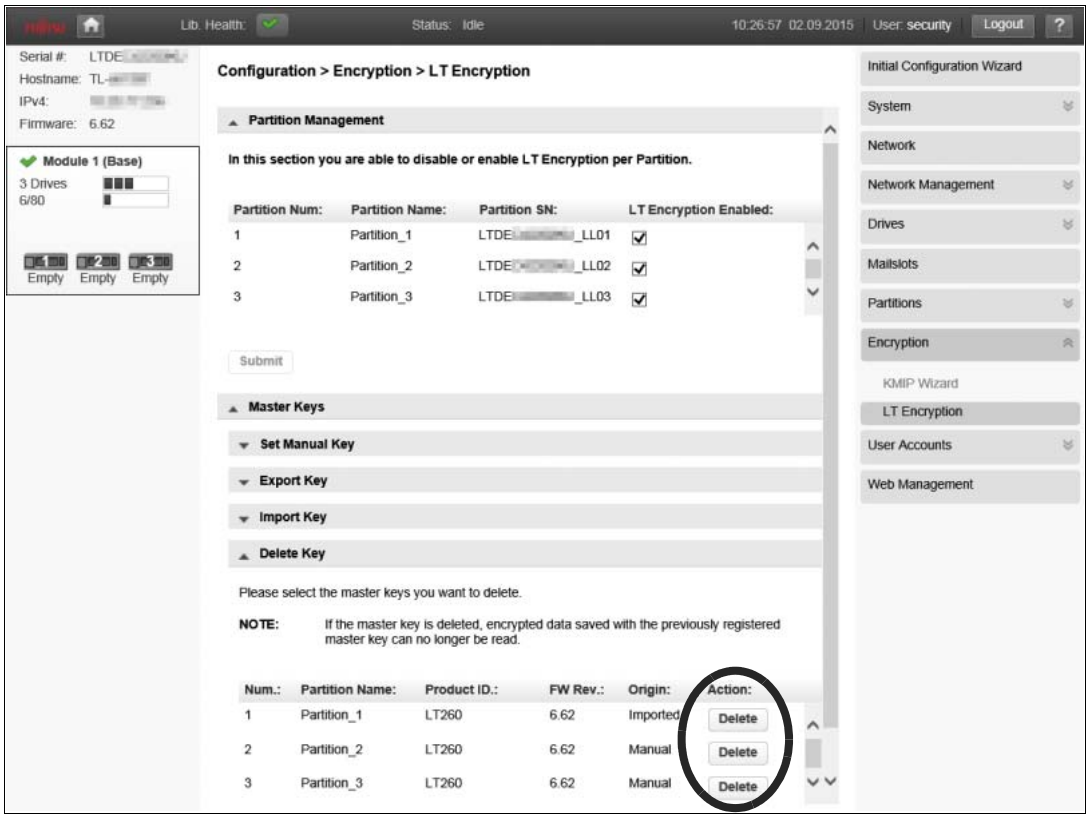
Note

If no logical libraries (or partitions) are configured, only "Partition_1" is displayed in the partition list.

Caution

Only a single master key can be deleted at a time. When deleting the master keys of multiple partitions, repeat the procedure from Step 3 and onward.

Figure 2.22 Deleting the master key



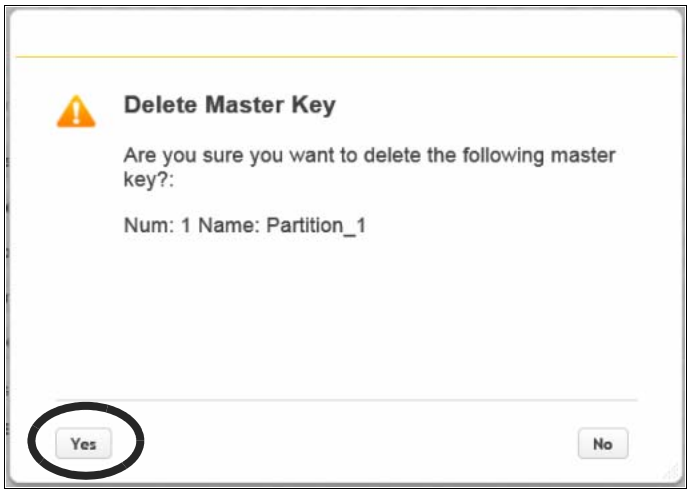
Copyright 2019 FUJITSU LIMITED

4 On the confirmation screen, click [Yes] to delete the master key.

Caution

- If the master key is deleted, data that was encrypted using the deleted master key cannot be read. For details about backing up the master key, refer to "2.1.4.2 Exporting the Master Key" (page 37).
- Deleted master keys cannot be restored even by a maintenance engineer or the manufacturing plant. Carefully consider whether to delete the master key.

Figure 2.23 Confirmation screen for deleting the master key



End of procedure

Copyright 2019 FUJITSU LIMITED

2.1.5 Encryption Key Export and Import Functions

Caution

- An encryption key file that is created by exporting encryption keys from multiple data cartridges at the same time can only be imported to the LT140. To import the encryption keys that were exported from the LT140 to tape libraries that support a key management function (*1) different from the LT140, export one encryption key per data cartridge.
- Regardless of the number of selected data cartridges, only one encryption key file is created when encryption keys are exported from multiple data cartridges.

*1: ETERNUS LT220, LT230, LT250, LT260, LT270, and LT270 S2

Note

- An encryption key is generated and assigned when a data write process is performed to the data cartridge.
- For the LT140, if a maintenance part must be replaced due to a failure, the master key and encryption keys may need to be exported and imported by the user.

2.1.5.1 Exporting the Encryption Key

Procedure

1. Move to the [Configuration > Encryption > LT Encryption] screen.
2. Select [Encryption Keys] > [Export Key] on the center pane.

Copyright 2019 FUJITSU LIMITED

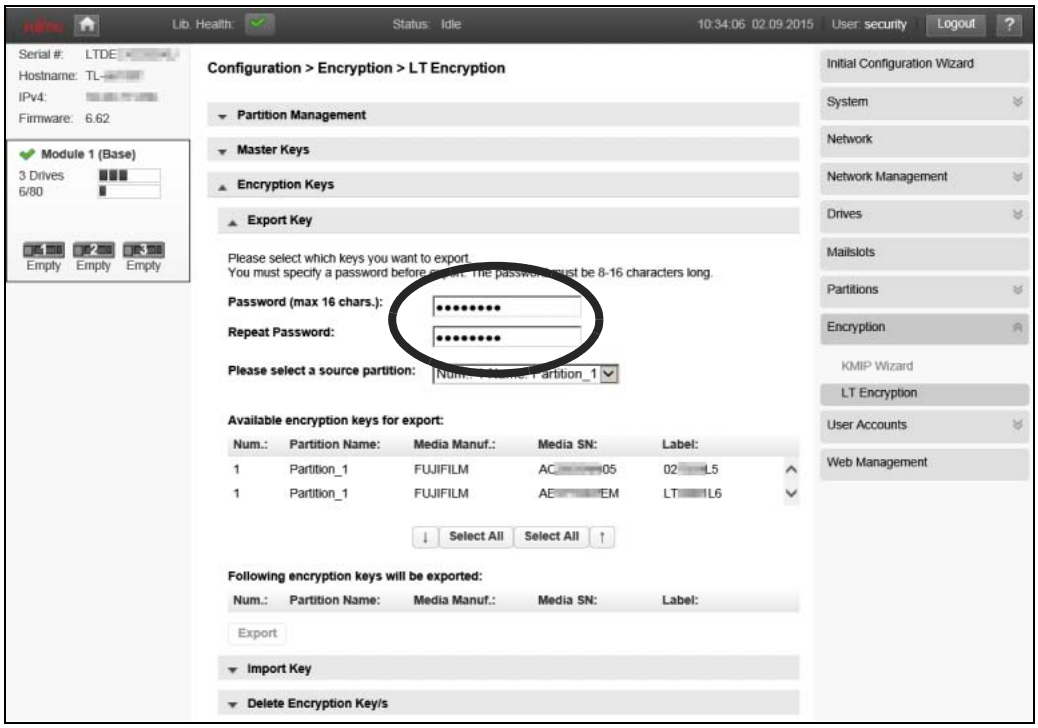
3 Enter the password in both boxes.

The password must be specified within 8 to 16 characters. Uppercase and lowercase alphanumeric characters and special characters can be used.

Caution

The password is required to import the encryption key. Keep the password in a safe place.

Figure 2.24 Encryption key password settings



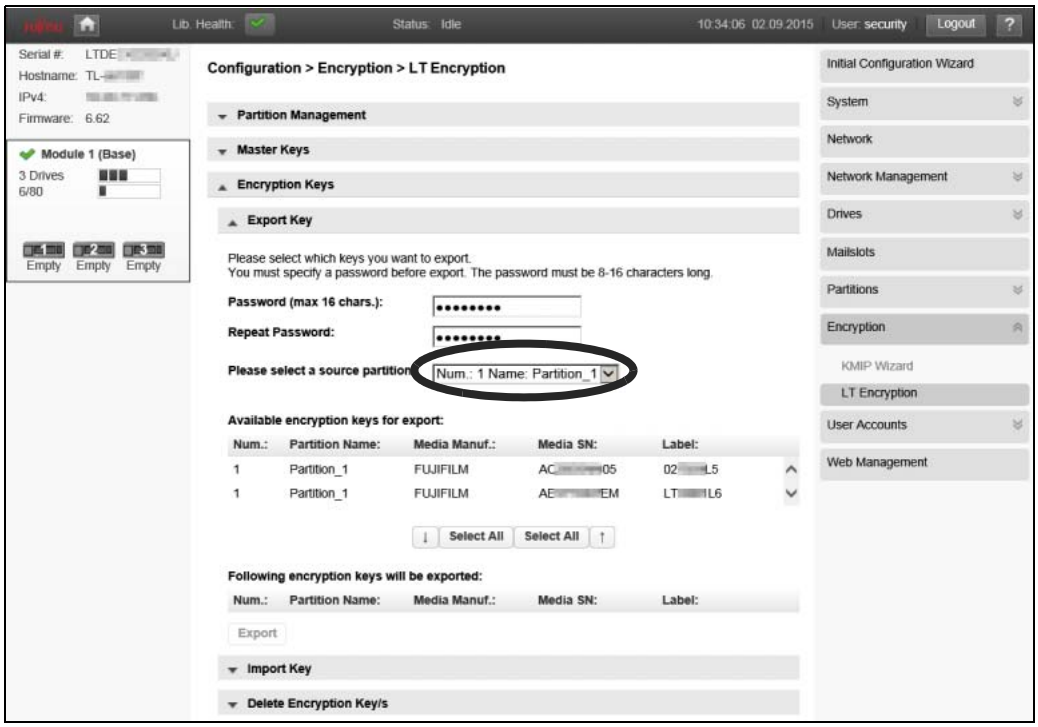
Copyright 2019 FUJITSU LIMITED

4 Select the partition where the data cartridges to export the encryption keys are stored.

Note

If no logical libraries (or partitions) are configured, only "Partition_1" is displayed in the drop down list.

Figure 2.25 Selecting the partition to export the target data cartridges

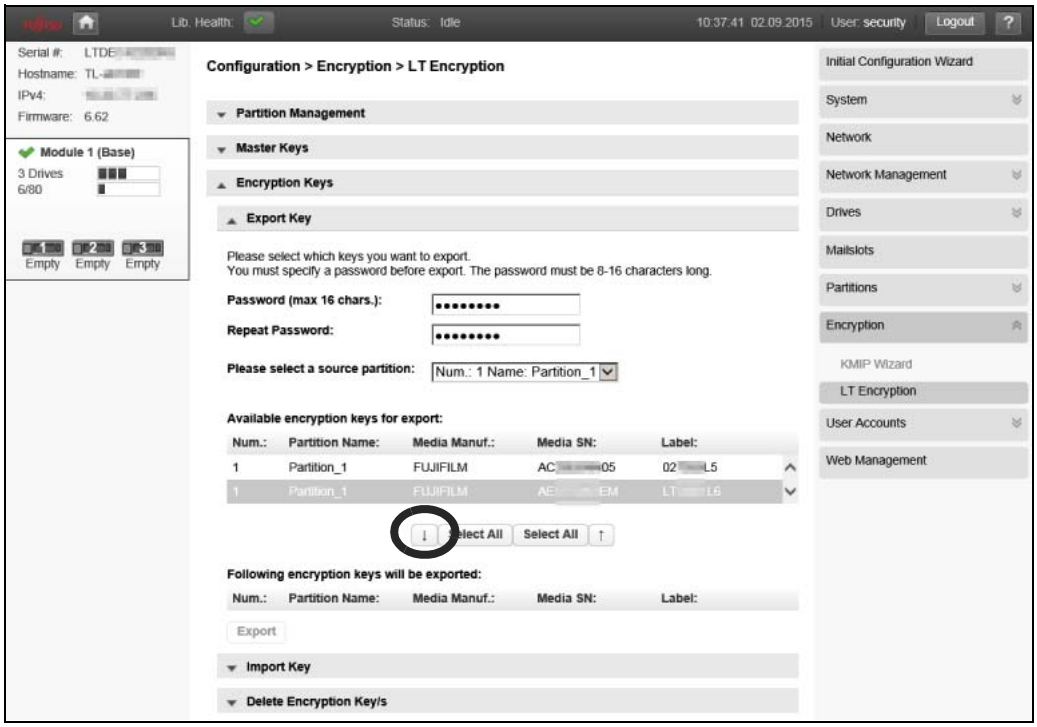


Copyright 2019 FUJITSU LIMITED

5 Select the data cartridges to export the encryption keys.

The color of the selected data cartridges changes. Click [↓] to move the data cartridge to a dedicated field for storing export target data cartridges. Multiple data cartridges can be moved at the same time.

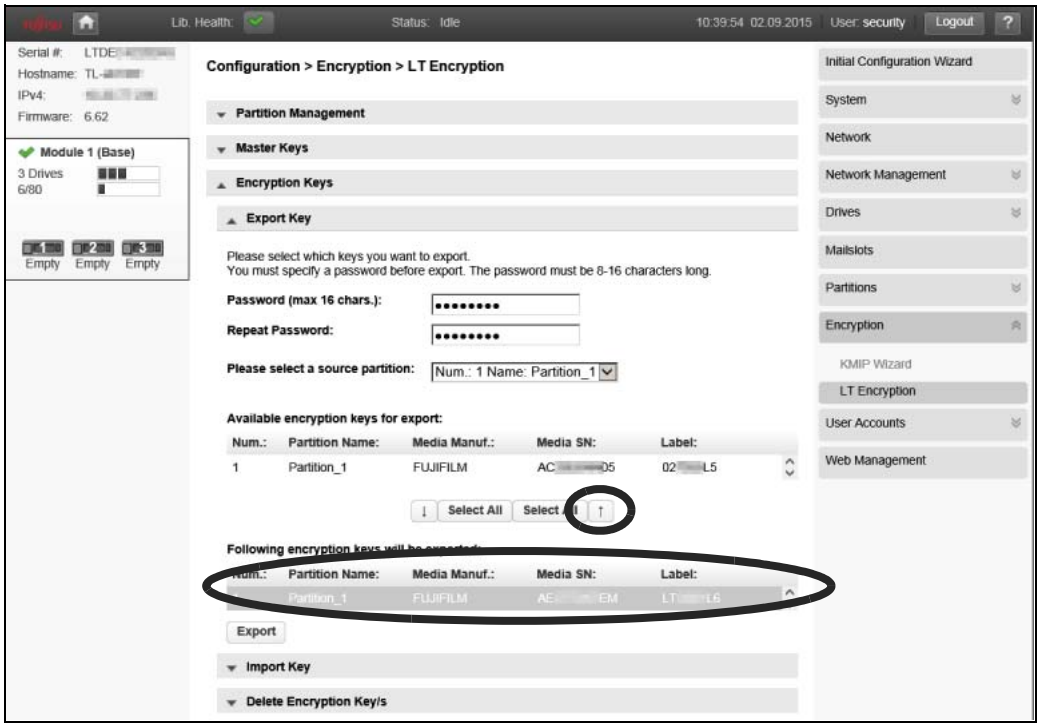
Figure 2.26 Selecting the data cartridges that are to be exported



Copyright 2019 FUJITSU LIMITED

To remove the data cartridges from the export target field, select the relevant data cartridge. The color of the selected data cartridge changes. Click [↑] to remove the selected data cartridge.

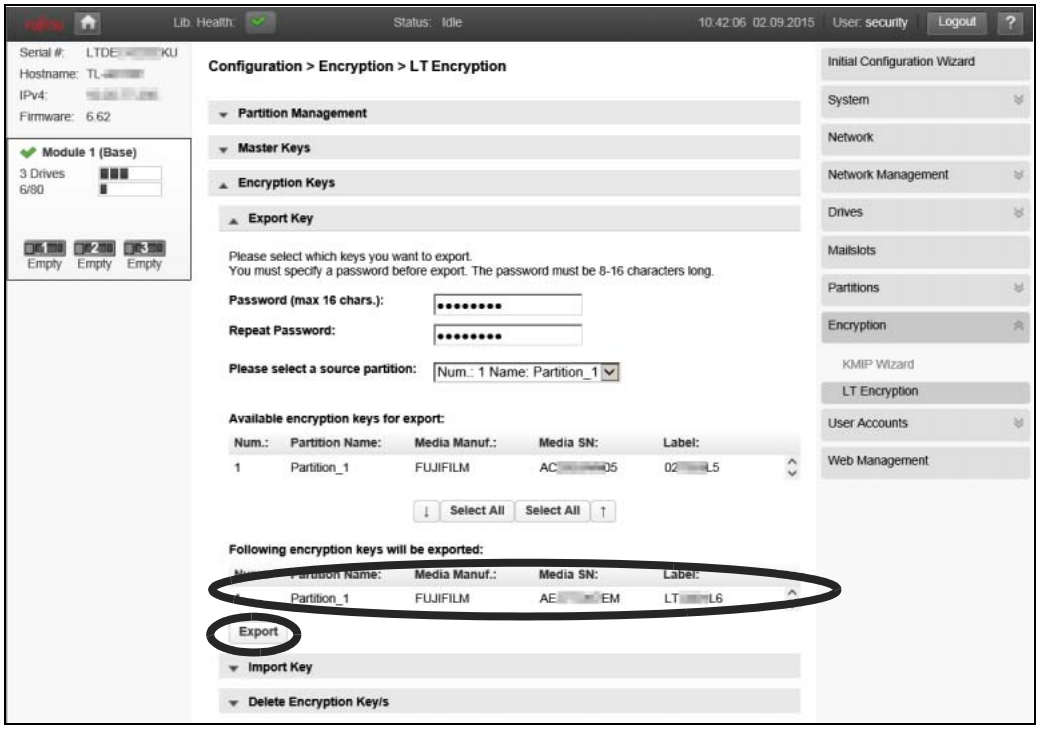
Figure 2.27 Removing the export target data cartridges



Copyright 2019 FUJITSU LIMITED

6 Click [Export] to export the encryption keys from the selected data cartridges.

Figure 2.28 Exporting the encryption key



Copyright 2019 FUJITSU LIMITED

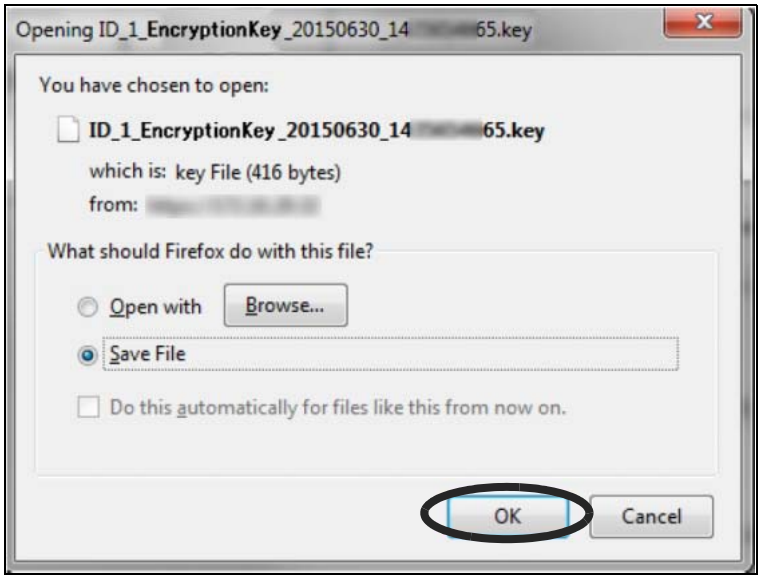
7 Specify the destination to which the encryption key is exported.

Caution

The operation for saving the encryption key differs depending on the OS.

The default file name for the exported encryption key is determined by the "ID_x_EncryptionKey_yyyymmdd_xxxxxxxxxx.key" format. The file size is 128 bytes.

Figure 2.29 Saving the encryption key to export



End of procedure

Copyright 2019 FUJITSU LIMITED

2.1.5.2 Importing the Encryption Key

Caution

- To use an encrypted data cartridge brought in from outside in the LT140 with a different master key, import the encryption key for that data cartridge before mounting in the LT140. If the encryption key was not imported, data writing is not allowed.
- If the encrypted data cartridge brought in from the outside is mounted in the LT140 with a different master key before the encryption key has been imported, a new encryption key may be assigned to the data cartridge. The new encryption key can be overwritten by importing the encryption key that was exported in advance.

Procedure

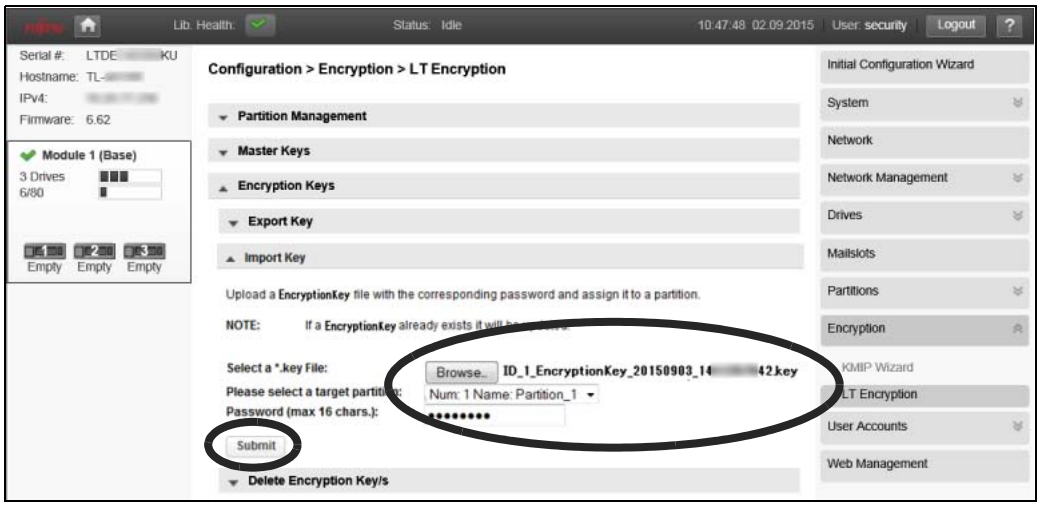
1. Move to the [Configuration > Encryption > LT Encryption] screen.
2. Select [Encryption Keys] > [Import Key] on the center pane.
3. Select the encryption key file that is to be imported.
4. Select the partition where the encryption key is to be imported.

Note

If no logical libraries (or partitions) are configured, only "Partition_1" is displayed in the drop down list.

5. Enter the password that was set when the encryption key was exported.
   For details about the password, refer to "2.1.5.1 Exporting the Encryption Key" (page 45).
6. Click [Submit].

Figure 2.30 Importing the encryption key



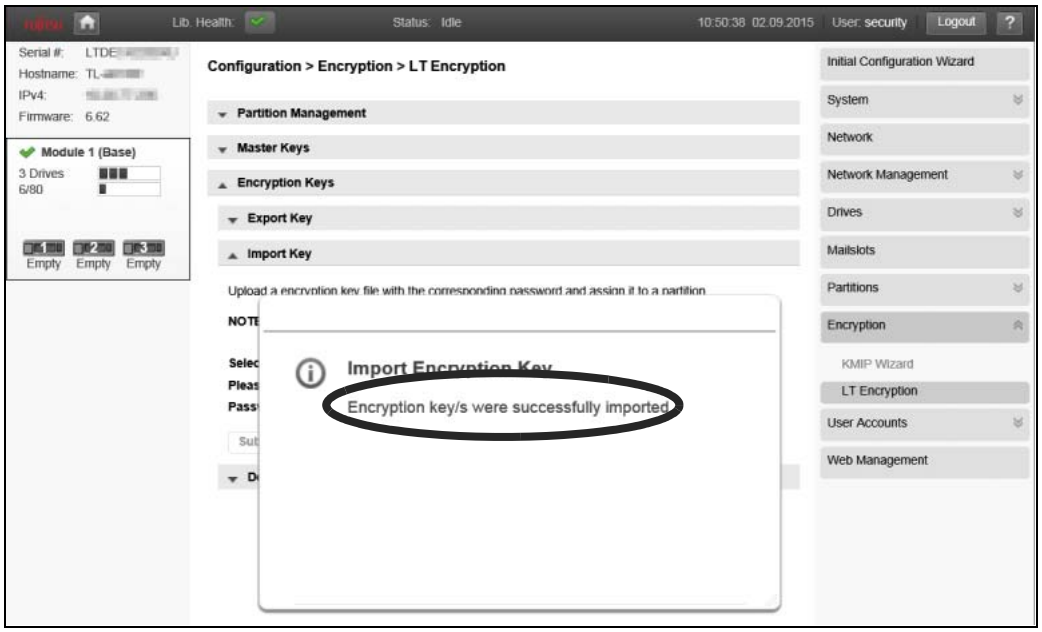
Copyright 2019 FUJITSU LIMITED

7 When a confirmation screen appears, click [Yes] to import the encryption key.

Figure 2.31 Confirmation screen for importing the encryption key

If the "Encryption key/s were successfully imported" message disappears, the encryption key has been imported.

Figure 2.32 Progress status screen for importing the encryption key



End of procedure

Copyright 2019 FUJITSU LIMITED

2.1.5.3 Deleting the Encryption Key

This function deletes the imported encryption key. Use this function to delete the unnecessary encryption key after using the encrypted data cartridge that was brought in from outside.

Caution

This function is used to delete the imported encryption key that is used for encrypted data cartridges that were brought in from the outside. Note that this function cannot be used for deleting encryption keys that are automatically assigned to the data cartridge from the tape library.

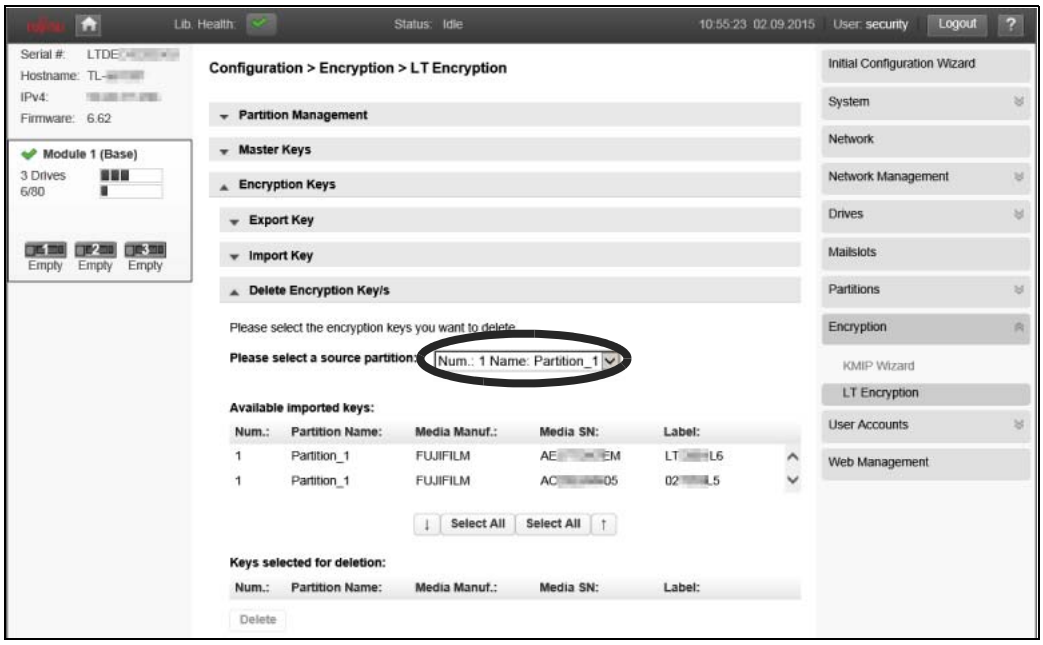
Procedure

1. Move to the [Configuration > Encryption > LT Encryption] screen.
2. Select [Encryption keys] from the menu.
3. Select [Delete Encryption Key/s] from the menu.
4. Select the partition that stores the data cartridge for deleting the encryption key.

Note

If no logical libraries (or partitions) are configured, only "Partition_1" is displayed in the drop down list.

Figure 2.33 Selecting the partition where the deletion target encryption key exists



Copyright 2019 FUJITSU LIMITED

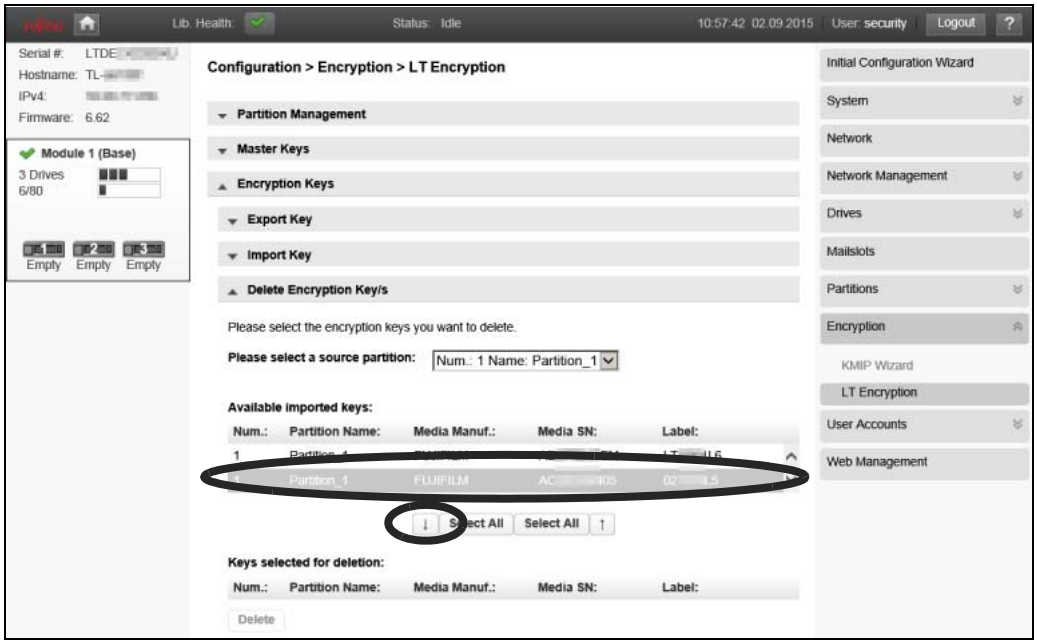
5 Select the data cartridge that corresponds to the deletion target encryption key.

The color of the selected data cartridge changes. Click [↓] to move the data cartridge to a dedicated field for storing deletion target data cartridges. Multiple data cartridges can be moved at the same time.

Caution

In this screen, only the data cartridges with an imported encryption key are displayed.

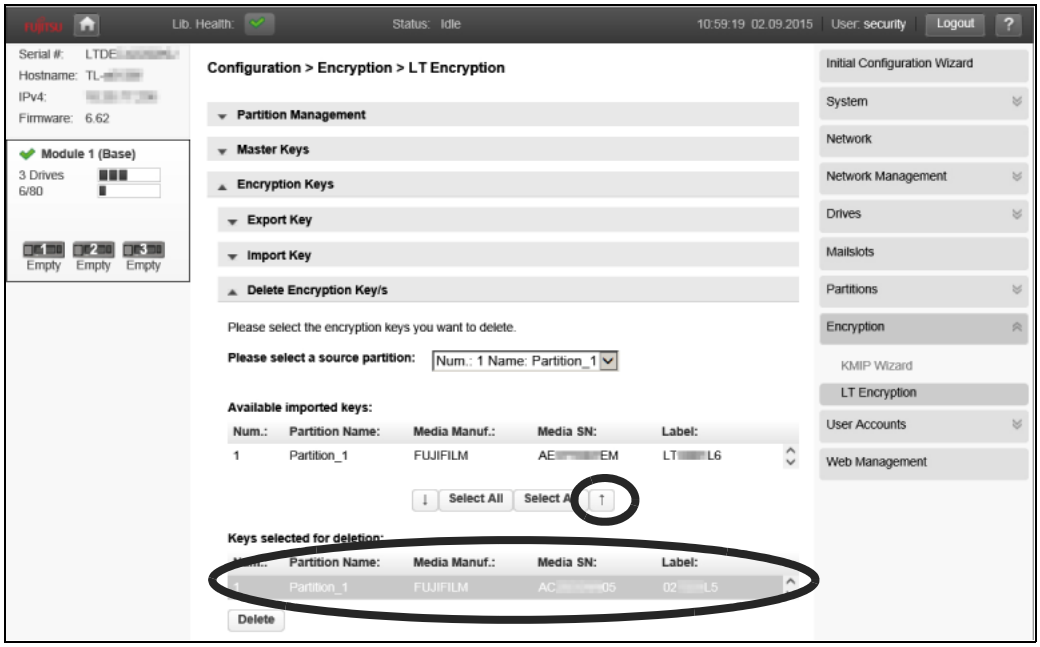
Figure 2.34 Selecting data cartridges with deletion target encryption keys



Copyright 2019 FUJITSU LIMITED

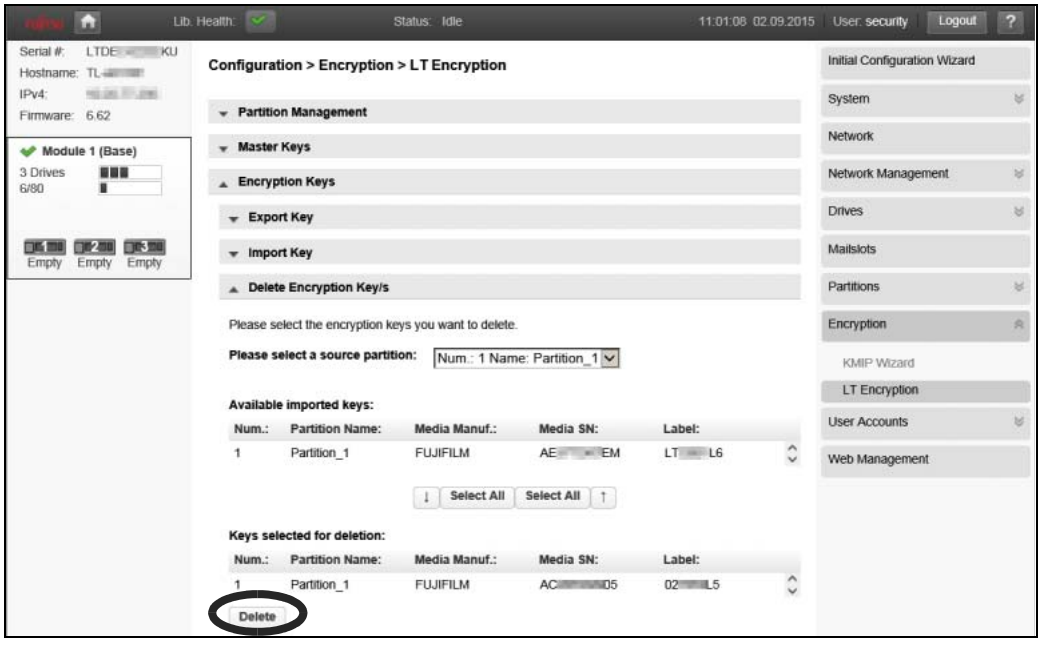
To exclude a data cartridge from the deletion target field, select the target data cartridge and click [↑].

Figure 2.35 Excluding data cartridges with deletion target encryption keys



6 Click [Delete].

Figure 2.36 Selecting imported encryption keys that are to be deleted



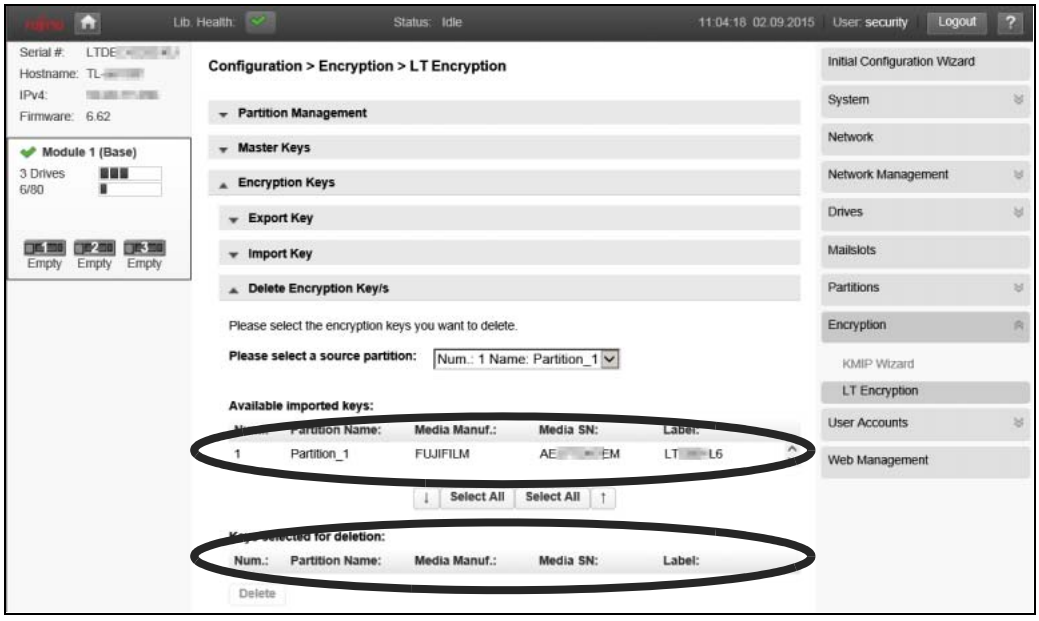
Copyright 2019 FUJITSU LIMITED

7 When a confirmation screen appears, click [Yes] to delete the imported encryption key.

Figure 2.37 Deleting the imported encryption keys

Information of the data cartridge disappears. The deletion of the imported encryption keys is complete.

Figure 2.38 Deletion confirmation of the imported encryption key



End of procedure

Copyright 2019 FUJITSU LIMITED

2.2 Backing Up the Setting Information

For the LT140, by saving the library configuration settings as a file, the saved settings can be restored in the tape library.

For the procedure to back up the setting information, refer to "Saving the library configuration to a file" of "3.4.2 Saving, Restoring and Resetting the Library Configuration" in "FUJITSU Storage ETERNUS LT140 Tape Library User's Guide -Panel Operation-".

While the Key Management Function Option is being used, if the file that is saved with the library configuration settings is restored to the tape library, the master key and encryption keys must be saved externally (or exported) in advance.
If an attempt at restoring the settings file for the library configuration in the tape library is performed, a confirmation screen to delete the master key and encryption keys is displayed (refer to "Figure 2.39").
If the [Yes] button on this confirmation screen is clicked, the master key and encryption keys that are saved in the LT140 tape library are all automatically deleted.
At this point, if the master key and encryption keys have not been exported, click the [No] button. After the master key and encryption key are exported respectively, restore the setting file for the library configuration in the tape library again. After the settings file for the library configuration is restored, import the exported master key and encryption keys if necessary.

Figure 2.39 Confirmation screen if an attempt at restoring the settings file for the library configuration is performed

Note

For the LT140, backing up only the information related to the encryption key management function from the setting information is not available. The setting information for libraries related to the encryption key management function is stored with other configurations not related to the encryption key management function such as configurations for libraries and operations.

Copyright 2019 FUJITSU LIMITED

2.3 Checking the Setting Information

This section explains how to check the setting information of the key management function.

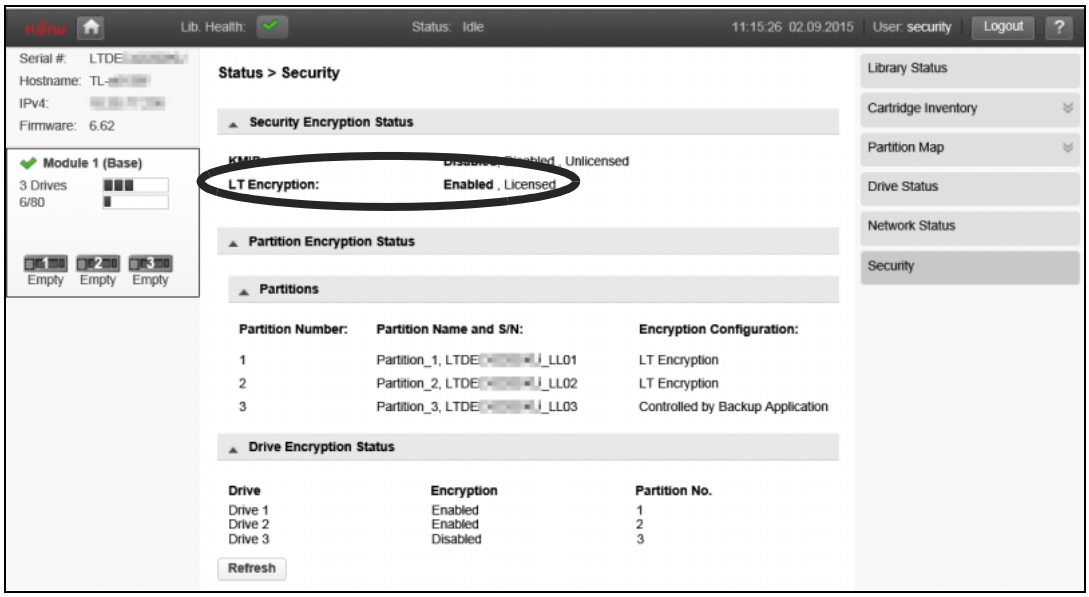
2.3.1 Setting Information of the Key Management Function

To check whether the key management function is enabled, follow the procedure below.

Procedure

1. Log in to the remote panel.
2. Move to the [Status > Security] screen.
   In [Security Encryption Status], if "Enabled" is displayed for [LT Encryption], the key management function is enabled.

Figure 2.40 [Status > Security > Security Encryption Status] screen



End of procedure

Copyright 2019 FUJITSU LIMITED

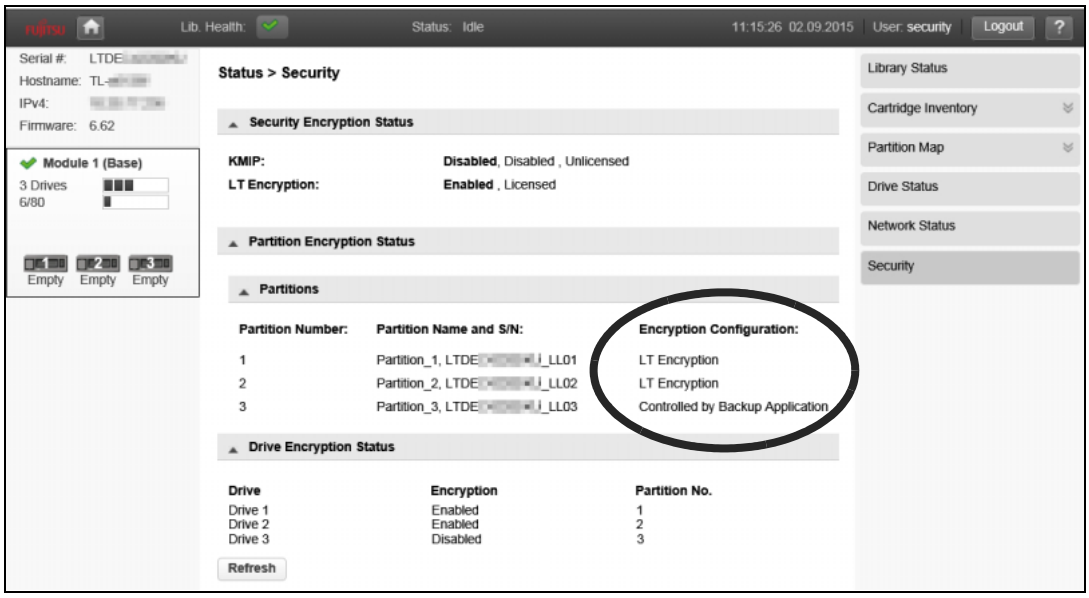
2.3.2 Setting Information of the Key Management Function for the Partition

To check the setting information of the key management function for each partition, follow the procedure below.

Procedure

1. Log in to the remote panel.
2. Move to the [Status > Security] screen.
   In [Partition Encryption Status] > [Partitions], if "LT Encryption" is displayed for [Encryption Configuration], the key management function is enabled. If "Controlled by Backup Application" is displayed for [Encryption Configuration], the key management function is disabled, and the key management function follows the backup software setting.

Figure 2.41 [Status > Security > Partition Encryption Status] screen



End of procedure

Copyright 2019 FUJITSU LIMITED

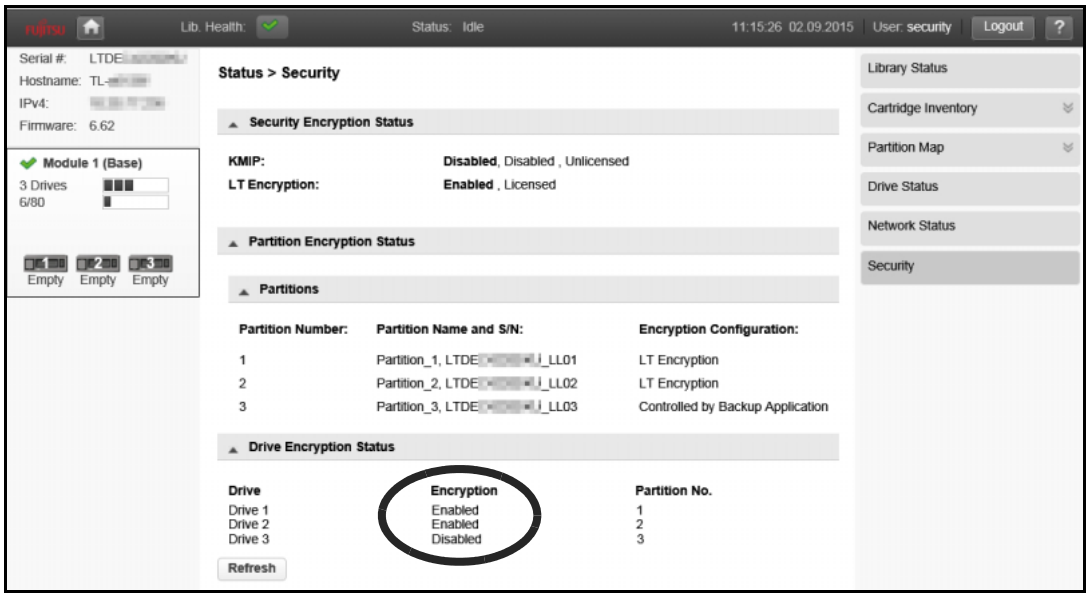
2.3.3 Setting Information of the Key Management Function for the Drive

To check the setting information of the key management function for each drive, follow the procedure below.

Procedure

1. Log in to the remote panel.
2. Move to the [Status > Security] screen.
   In [Drive Encryption Status], if "Enabled" is displayed for [Encryption], the key management function of the drive is enabled. If "Disabled" is displayed for [Encryption], the key management function is disabled, and the key management function follows the backup software setting.

Figure 2.42 [Status > Security > Drive Encryption Status] screen



End of procedure

Copyright 2019 FUJITSU LIMITED

2.3.4 Encryption Setting Information of the Data Cartridge

Check the encryption setting information of the data cartridge in the tape library.

Use either of the following methods to check.

- Using the inventory list
- Using the inventory graphical view

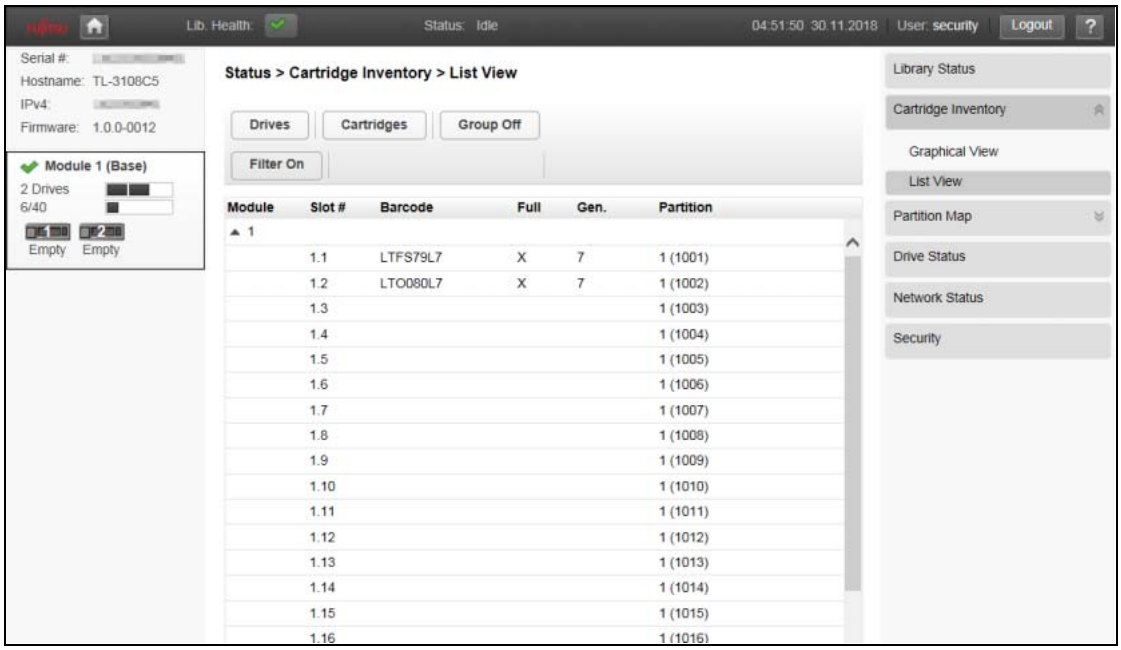
2.3.4.1 Using the Inventory List

To use the inventory list to check the encryption setting information of the data cartridge, follow the procedure below.

Procedure

1. Log in to the remote panel.
2. Move to the [Status > Cartridge Inventory > List View] screen.

Figure 2.43 [Status > Cartridge Inventory > List View] screen



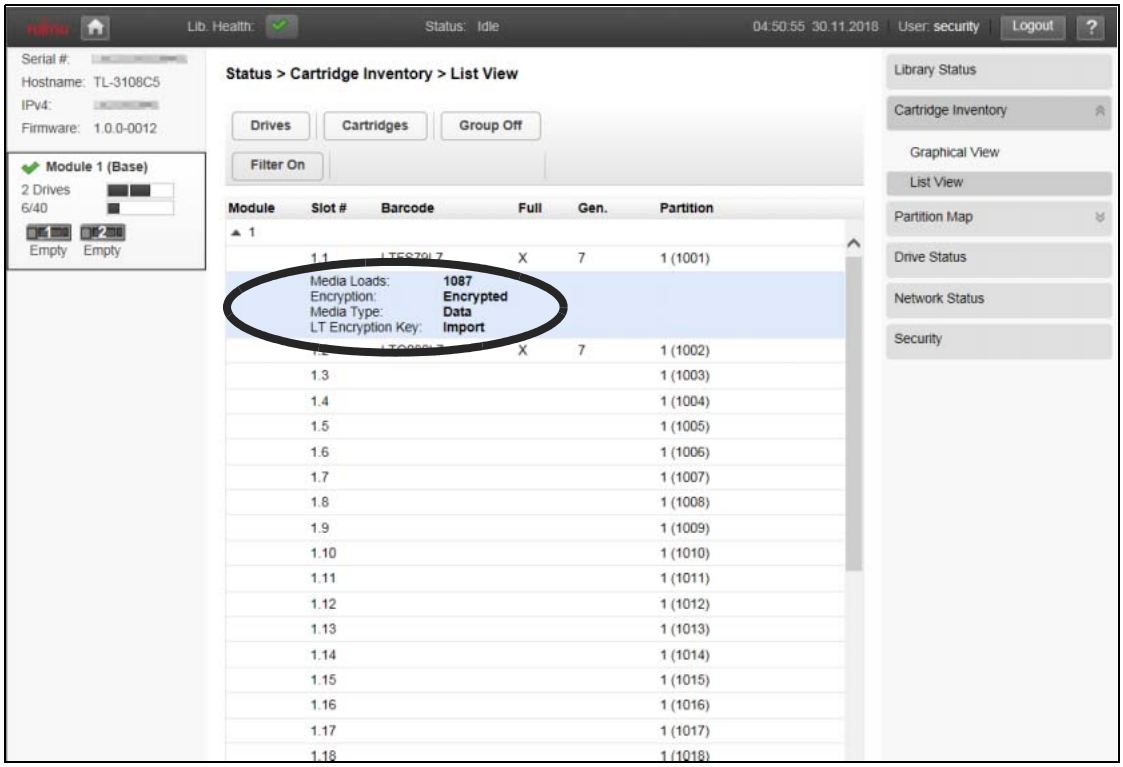
Copyright 2019 FUJITSU LIMITED

3 Click the data cartridge that is to be checked.

Additional information is displayed. The encryption setting information of the data cartridge can be checked by viewing [Encryption] and [LT Encryption Key].

- Encryption
  - Not Encrypted
    An encryption key is assigned, but there is no encrypted data.
  - Encrypted
    An encryption key is assigned and encrypted data exists.
  - N/A
    An encryption key is not assigned.
- LT Encryption Key
  - Auto
    An automatically generated encryption key is used.
  - Import
    An imported encryption key is used.
  - N/A
    An encryption key is not assigned.

Figure 2.44 [Status > Cartridge Inventory > List View (detailed)] screen



Copyright 2019 FUJITSU LIMITED

Note

For Ultrium3 or earlier data cartridges, all the items above are displayed as "N/A".

End of procedure

2.3.4.2 Using the Inventory Graphical View

To use the inventory graphical view to check the encryption setting information of the data cartridge, follow the procedure below.

Procedure

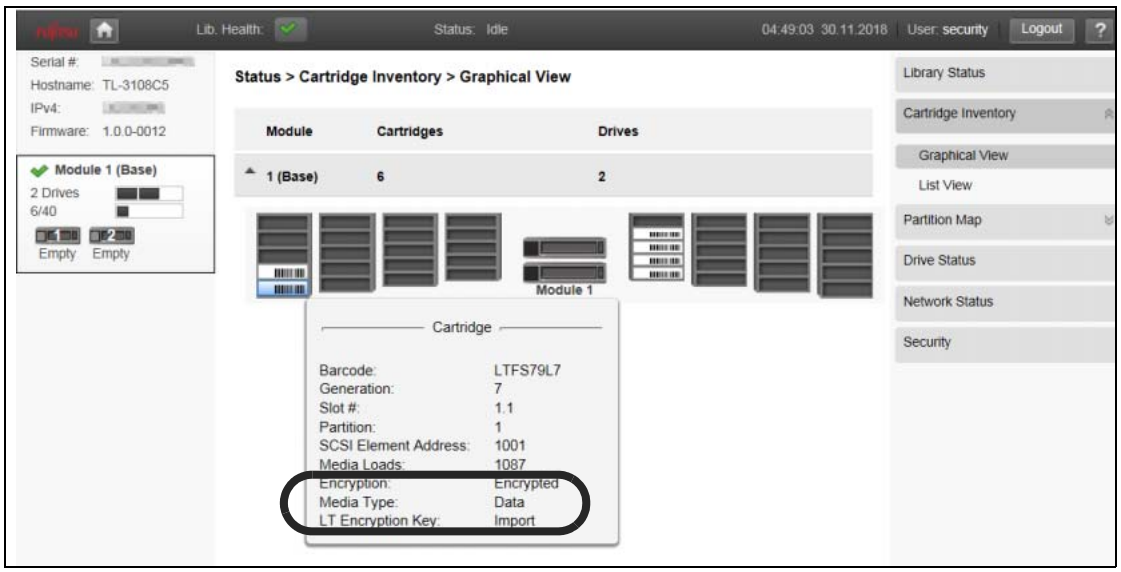
1. Log in to the remote panel.
2. Move to the [Status > Cartridge Inventory > Graphical View] screen.
3. Move the mouse over the data cartridge that is to be checked.

   Detailed information is displayed. The encryption setting information of the data cartridge can be checked by viewing [Encryption] and [LT Encryption Key].

   - Encryption
     - Not Encrypted
       An encryption key is assigned, but there is no encrypted data.
     - Encrypted
       An encryption key is assigned and encrypted data exists.
     - N/A
       An encryption key is not assigned.
   - LT Encryption Key
     - Auto
       An automatically generated encryption key is used.
     - Import
       An imported encryption key is used.
     - N/A
       An encryption key is not assigned.

Copyright 2019 FUJITSU LIMITED

Figure 2.45 [Status > Cartridge Inventory > Graphical View] screen



Note

For Ultrium3 or earlier data cartridges, all the items above are displayed as "N/A".

End of procedure

Copyright 2019 FUJITSU LIMITED

Chapter 3

Setup Methods for Different Operations

This chapter explains the setup procedures in examples of general operations with the key management function.

3.1 Sharing Data among Multiple Tape Libraries

This section explains a general setup procedure for assigning the same master key to multiple tape libraries to share data cartridges (data) among them.

Make appropriate settings by following the procedure below.

Procedure

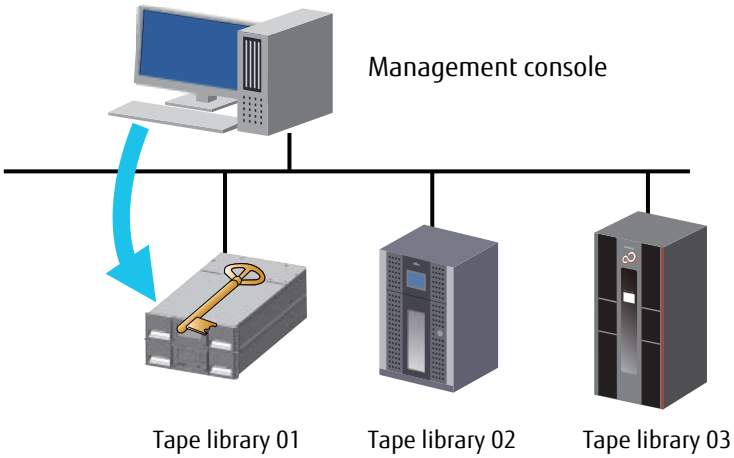
1 Set the license key of the Key Management Function Option of each tape library.

Note

One Key Management Function Option is required for each tape library.

2 Assign a master key for the main tape library.

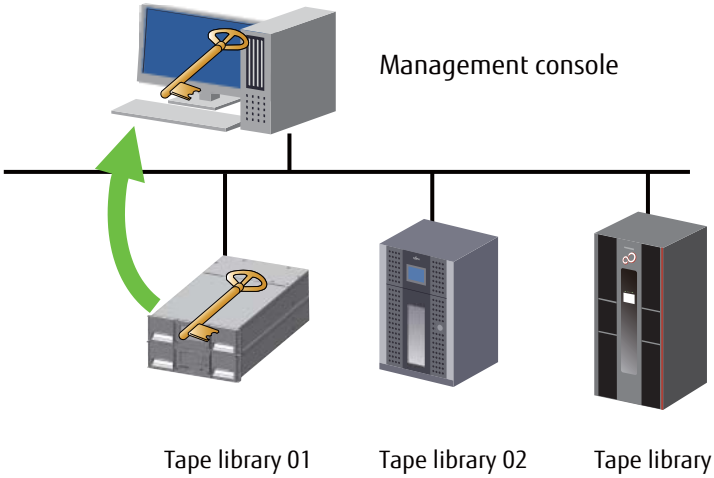
For information on how to set the master key, refer to "2.1.4 Setting the Master Key" (page 35).



Copyright 2019 FUJITSU LIMITED

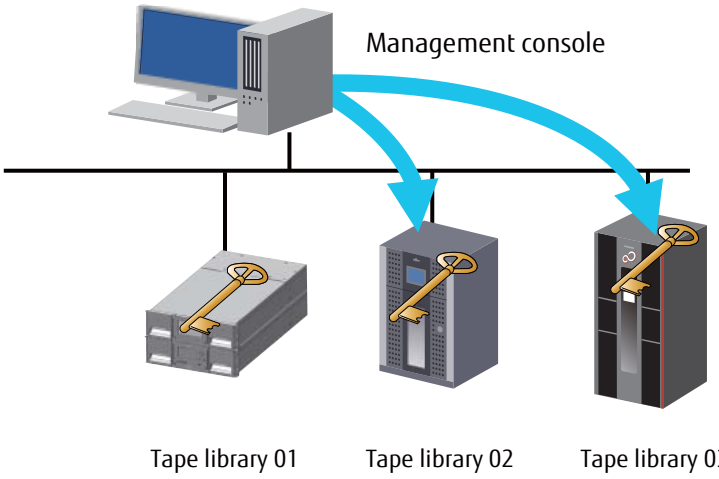
3 Export the set master key to the management console.

For information on how to export the master key, refer to "2.1.4.2 Exporting the Master Key" (page 37).



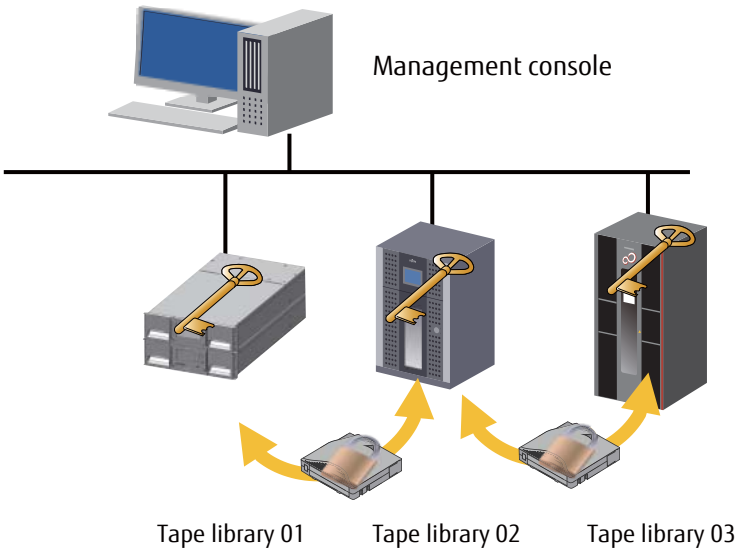
4 Import the exported master key to the other tape libraries.

For information on how to import a master key, refer to "2.1.4.3 Importing the Master Key" (page 40).
For information on how to import a master key to the ETERNUS LT250, LT270, and LT270 S2, refer to "FUJITSU Storage ETERNUS LT250/LT270/LT270 S2 Tape Library Key Management Function Option User's Guide".



Copyright 2019 FUJITSU LIMITED

5 The above setup enables the tape libraries assigned the same master key to share data cartridges without any special settings and operations.



End of procedure

3.2 Storing Data Cartridges at External Locations

For disaster recovery, encrypted data cartridges can be stored externally, such as at an external warehouse, and, when needed, brought back to read the data on them.

Make appropriate settings by following the procedure below.

Procedure

1 Set the license key of the Key Management Function Option of each tape library.

2 Assign a master key for the main tape library.
For information on how to set the master key, refer to "2.1.4 Setting the Master Key" (page 35).

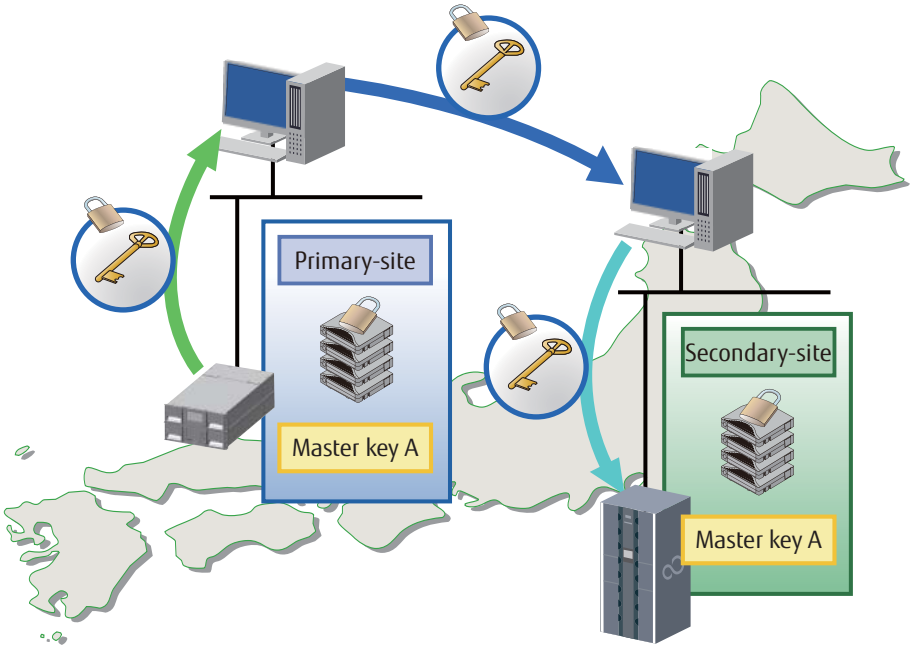
3 Export the set master key to the management console.
For information on how to export the master key, refer to "2.1.4.2 Exporting the Master Key" (page 37).

Copyright 2019 FUJITSU LIMITED

4 Import the master key to the other tape libraries that will share data, so that the tape libraries have a common master key.

Caution

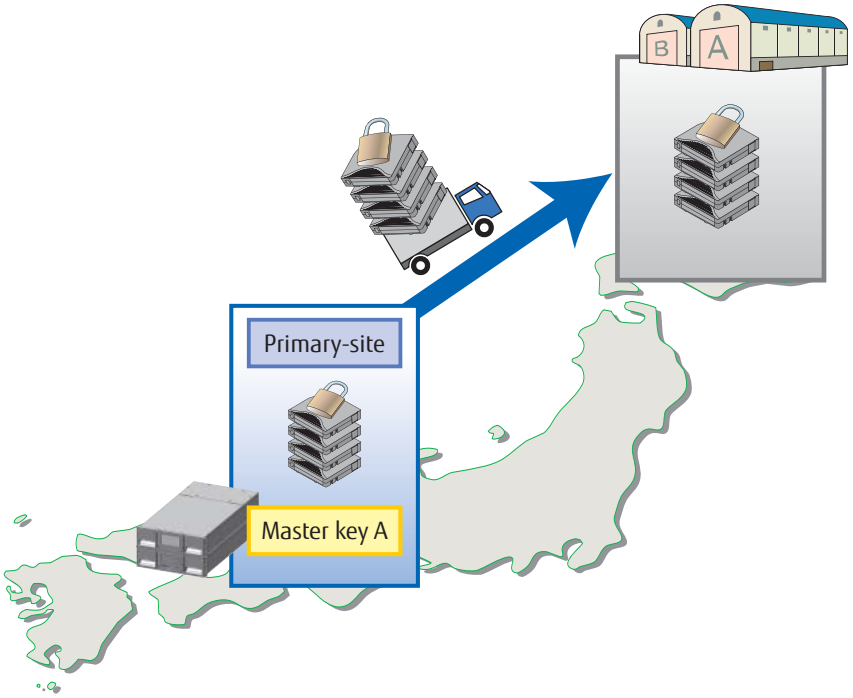
The encryption key export or import function can be used to export the encryption keys of a stored data cartridge, so that a tape library with a different master key can use the data cartridge after importing the encryption key. However, if the encryption key is deleted or lost by mistake, the data can no longer be read. Therefore, Fujitsu recommends that the same master key be set for the tape libraries sharing data. For information on the encryption key export or import function, refer to "2.1.5 Encryption Key Export and Import Functions" (page 45).



Copyright 2019 FUJITSU LIMITED

5 Eject the data cartridges for external storage.

For information on how to eject a data cartridge, refer to "3.5 Loading and Ejecting Cartridges" in "FUJITSU Storage ETERNUS LT140 Tape Library User's Guide -Installation & Operation-".



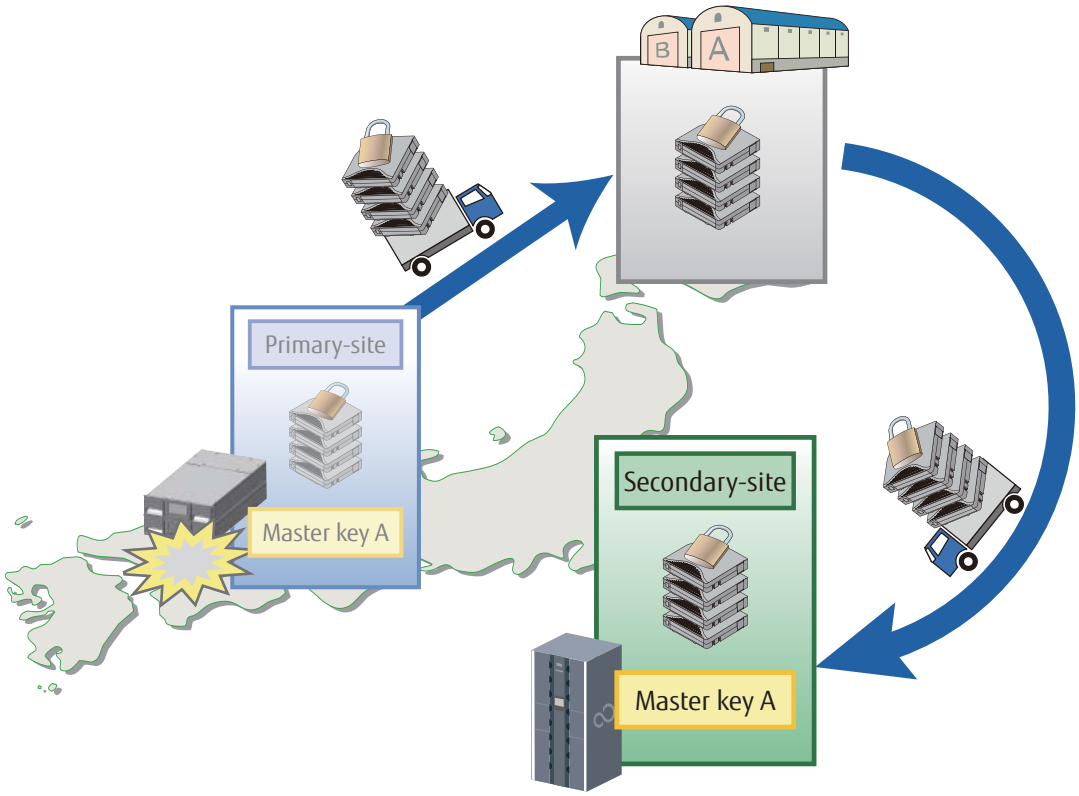
Copyright 2019 FUJITSU LIMITED

6 To use the data cartridges that were placed in external storage in case of disaster, insert these cartridges into a tape library that has the same master key as the previous tape library.

The data cartridges can be used without modification by using a tape library that has the same master key.

Note

- To use the data cartridge in a tape library with a different master key, import its exported encryption key before inserting the data cartridge into the tape library.
- For information on how to import an encryption key, refer to "2.1.5.2 Importing the Encryption Key" (page 52). For information on how to insert a data cartridge, refer to "3.5 Loading and Ejecting Cartridges" in "FUJITSU Storage ETERNUS LT140 Tape Library User's Guide -Installation & Operation-".



End of procedure

Copyright 2019 FUJITSU LIMITED

Chapter 4
Considerations

4.1 Troubleshooting

If any problem occurs with the key management function, check for the problem in Table 4.1, and review the usage and settings.

Table 4.1 Troubleshooting

Problem	Cause	Corrective action
Encryption failed.	Possible causes are: 1. Data was not recorded with an Ultrium5 or later tape drive. 2. An Ultrium3 or earlier data cartridge was used. 3. The appropriate settings for encryption have not been made.	Confirm that: 1. The data was recorded with an Ultrium5 or later tape drive. 2. No Ultrium1, Ultrium2, or Ultrium3 data cartridge was used. 3. Appropriate settings for encryption have been made. Refer "2.3.4 Encryption Setting Information of the Data Cartridge" (page 62)
An encryption key could not be exported.	The encryption key has not been assigned to a data cartridge.	An encryption key is generated and assigned when a data write process is performed to the data cartridge. Refer "2.3.4 Encryption Setting Information of the Data Cartridge" (page 62)
The menu for the [Configuration > Encryption > LT Encryption] screen could not be displayed.	An account other than the security account may have been used to log in.	Log in with the security account. Refer "2.1.3.1 Basic Setup of the Key Management Function" (page 31)

Copyright 2019 FUJITSU LIMITED

Problem	Cause	Corrective action
The following error message appeared on the [Configuration > Encryption > LT Encryption] screen. "Import Export functionality is only available using secure HTTPS connection."	Instead of an https connection, an http connection may have been used to log in.	Enable [SSL Secure Socket Layer] by selecting the checkbox on the [Configuration > Web Management] screen. After that, log out and then log back in using https. Refer • "2.1.2.3 Enabling SSL" (page 26) • "2.1.2.4 Connecting to the Remote Panel after Enabling SSL" (page 29)
The following message appeared on the [Configuration of Encryption] screen and the key management function cannot be enabled or disabled. "Note: Encryption configuration changes cannot be made while media is loaded in any drive."	The tape cartridge may have been loaded in the tape drive.	Check whether the tape cartridge is loaded in the tape drive. If the tape cartridge is loaded, move it from the tape drive to the slot. Refer • "3.6.1 Moving Media" in "FUJITSU Storage ETERNUS LT140 Tape Library User's Guide -Panel Operation-" • "3.7.2 Using Inventory Lists" in "FUJITSU Storage ETERNUS LT140 Tape Library User's Guide -Panel Operation-"

Copyright 2019 FUJITSU LIMITED

4.2 Sense Keys Related to the Key Management Function

The following table lists the sense keys displayed on the server for the occurrence of an error related to the key management function.

Table 4.2 Sense keys

Sense Key	asc	ascq	Error information	Cause
7	74	0	Security error	A drive or tape library may be faulty.
7	74	1	Unable to decrypt data	A drive or tape library may be faulty.
7	74	2	Unencrypted data encountered while Decrypting	A drive or tape library may be faulty.
7	74	3	Incorrect data encryption key	The encryption key of the data cartridge is probably different from the imported encryption key.
7	74	4	Cryptographic integrity validation failed	A drive or tape library may be faulty.
7	74	5	Key-associated data descriptors changed	A drive or tape library may be faulty.
7	74	8	Digital signature validation failure	A drive or tape library may be faulty.
7	74	9	Encryption mode mismatch on read	A drive or tape library may be faulty.
7	74	a	Encrypted block not raw read enabled	A drive or tape library may be faulty.
7	74	b	Incorrect encryption parameters	A drive or tape library may be faulty.
5	74	21	Data encryption configuration prevented	The settings cannot be changed because the encryption function is enabled in the tape library. Check the setting information.
7	74	80	KAD changed	A setting error of the encryption parameters exists. A drive, tape library, or media may be faulty.

4.3 Reuse of Data Cartridges

To reuse an encrypted data cartridge, use backup software to erase the data.

Copyright 2019 FUJITSU LIMITED

4.4 Connectivity with Backup Software

On a system using the key management function, Fujitsu recommends using verified backup software.

If unverified backup software is used, encryption may not work normally. For more information, contact your sales representative.

If your backup software supports the encryption function of Ultrium6 or later tape drives, be sure to disable the encryption function of the backup software as necessary.

4.5 Purchasing a License

To issue a license for using the Key Management Function Option, the serial number of the tape library is required. If the LT140 has already been purchased, provide the serial number of the tape library to your sales representative to obtain this license.

If the Key Management Function Option is purchased with the tape library, no action is necessary because the license has already been set.

4.6 Changing the System Firmware

The following operations are required to downgrade the system firmware from version 6.70 or later (for the LT140 in which the Key Management Function Option is being used) to version 6.56 or earlier (for which the Key Management Function Option is not supported).

- Deleting the master key
- Deleting the encryption key
- Disabling the key management function

Since the encrypted data cannot be read after the master key and the encryption key are deleted, be sure to export the master key and the encryption key in advance and keep them in a safe place.

Copyright 2019 FUJITSU LIMITED

Appendix A

Logs Related to the Key Management Function

A history of key management function operations or settings is automatically recorded in a log. This enables the tracking of unauthorized access and other operations.
The log related to the key management function is saved with the logs for the library settings and operations not related to the key management function.

A.1 How to Download Logs Related to the Key Management Function

Downloading only the log related to the key management function is not possible. Note that the log related to the key management function is saved with the logs for the library settings and operations not related to the key management function.

For information on how to download logs, refer to "3.5.6 Downloading Log and Trace Files" in "FUJITSU Storage ETERNUS LT140 Tape Library User's Guide -Panel Operation-".

A.2 Checking the Contents of the Logs Related to the Key Management Function

Download the log and trace files (compressed files in the tgz format) according to "A.1 How to Download Logs Related to the Key Management Function" (page 76) and decompress the files. The following files are then extracted in the "syslog-*hostname-library (system) firmware version_date_time*" folder.

(1) conflog.txt

(2) details.bin

(3) infolog.txt

(4) servicelog.txt

(5) system.log

(6) ticketlog.txt

For events related to the key management function that are recorded in each file, refer to "Table A.1 Events related to the key management function" (page 79)".

Copyright 2019 FUJITSU LIMITED

(1) conflog.txt

This file records the changes of the library configuration and settings.
The contents are recorded in the "EVENT: *event code - message*" format.
For events related to the key management function, refer to "Table A.1 Events related to the key management function" (page 79).

Example:

```
-------- EVENT: 8053 - LT Encryption encryption keys exported to key file --------
Message:                          EXPORT_LT_DATA_KEYS
Time:                             10/25/2018 04:51:04 PM
-------- Details --------
 PHYSICAL_PART:                    1
 PARTITION_NAME:                   Partition_0
 KEY_COUNT:                        1
 SYS_COMPONENT:                    SYSTEM
 PHY_NUM:                          1
```

(2) details.bin

This file records the detailed information of the library in the binary format.
The contents cannot be viewed.

(3) infolog.txt

This file records the library warnings.
The contents are recorded in the "EVENT: *event code - message*" format.
For events related to the key management function, refer to "Table A.1 Events related to the key management function" (page 79).

Example:

```
-------- EVENT: 9059 - LT encryption Key retrieved by tape drive --------
Message:                          ENCR_KEY_REQUEST
Time:                             10/25/2018 10:36:29 AM
-------- Details --------
 KEY_CREATE:                       FALSE
 SYS_COMPONENT:                    SYSTEM
 PHY_NUM:                          1
```

(4) servicelog.txt

This file records information that is required for maintenance.

Example:

```
-------- TYPE: SERVICE --------
Message:                        SINGULAR_TICKET
Time:                           10/25/2018 07:22:51 PM
  -------- Details --------
  ERRORCODE:                    Drive status monitoring failed (DRIVE_STATUS_FAILED)
  SEVERITY:                     WARNING
  SYS_COMPONENT:                DRIVE
  PHY_NUM:                      1 (19)
  -------------------------
  ERRORCODE:                    ADT SCSI command check condition not retryable
(DRIVE_SCSI_CMD_CHECK_CONDITION)
  CDB_DATA:                     8C 00 00 00 00 00 00 00 04 08 00 00 00 0A 00
  SENSE_DATA:                   03 11 12
  FIELD_POINTER:                CD 0, SKSV 0, FP 11458 (2CC2)
```


Copyright 2019 FUJITSU LIMITED

(5) system.log

This file records the library configuration, the status, and the settings.
The contents that are displayed in the Status menu and the encryption setting information are recorded.

Example:

```
Service Dump from: 10/25/2018 10:41:36 AM
-----------------------------------------

Library Information:
--------------------
Vendor              : FUJITSU            Product ID          : ETERNUS LT260
Serial Number       : LTDE56400017       Base FW Revision    : 1.0.0-0009
Base FW Build Date  : 10-25-2018         Base FW Checksum    : 985D
.........
.........
LT Encryption:
---------------

 Master Keys:
  ------------
  Partition |FW Rev      |Product ID      |Src. Library SN     |Src. Library Name   |UTC created         |Origin
  ----------+------------+----------------+--------------------+--------------------+--------------------
    1       |1.0.0       |LT140           |LTDE56400017        |New Partition_1     |1541381486          |Auto

  Encryption Keys:
  ----------------
   Partition |Media Manuf.              |Media SN               |Barcode Label       |FW Rev              |Product ID          |Origin
  -----------+--------------------------+-----------------------+--------------------+--------------------+--------------------+-------------------


License: TVVCNMS8UPQQSO1
Description: LT Library Encryption
Parameter: 12
Index: 1
Status: active
Expiration: never
```

(6) ticketlog.txt

This file records the library error information.
The contents are recorded in the "Event *event code* - *message*" format.
For events related to the key management function, refer to "Table A.1 Events related to the key management function" (page 79).

Example:

```
-------- Event 4059 - Drive is included to an encrypting partition but is not supporting encryption --------
Ticket-No:                    76
Time:                         10/25/2018 02:26:41 PM
State:                        Resolved
Closed:                       No
Severity:                     WARNING
Component:                    DRIVE
Component-Id:                 21
  -------------- DETAILS ---------------
  ERRORCODE_2:                Drive configuration failed (DRIVE_CONFIG_FAILED)
  SEVERITY_2:                 WARNING
  SYS_COMPONENT_2:            DRIVE
  PHY_NUM_2:                  3 (21)
  --------------------------
  ERRORCODE:                  Drive is not supporting encryption (DRIVE_NO_ENCRYPTION)
```


Copyright 2019 FUJITSU LIMITED

Table A.1 Events related to the key management function

Event code	Message	Meaning
4055	Encryption configuration failed	Configuration of the encryption setting failed.
4059	Drive configuration failed because it does not support encryption	The tape drive does not support the encryption function.
4114	LT Library encryption not licensed	The license for the Key Management Function Option is not set.
8048	LT Encryption master key created	The master key was generated by a manual setting or by automatic generation.
8049	LT Encryption master key deleted	The master key was deleted.
8050	LT Encryption master key exported to key file	The master key was exported to the library as a file.
8051	LT Encryption master key imported from key file	The master key was imported to the library as a file.
8052	LT Encryption master key changed	The master key was changed by a manual setting or the import process.
8053	LT Encryption encryption keys exported to key file	The encryption keys were exported to the library as a file.
8054	LT Encryption encryption keys imported from key file	The encryption keys were imported to the library as a file.
8055	LT Encryption encryption keys deleted	The encryption keys were deleted.
9059	LT encryption Key retrieved by tape drive	The tape drive received the encryption key.

Copyright 2019 FUJITSU LIMITED

FUJITSU Storage ETERNUS LT140 Tape Library
Key Management Function Option
User's Guide

P3AG-3762-02ENZ0

Date of issuance: December 2019
Issuance responsibility: FUJITSU LIMITED

- The content of this manual is subject to change without notice.
- This manual was prepared with the utmost attention to detail.
  However, Fujitsu shall assume no responsibility for any operational problems as the result of errors, omissions, or the use of information in this manual.
- Fujitsu assumes no liability for damages to third party copyrights or other rights arising from the use of any information in this manual.
- The content of this manual may not be reproduced or distributed in part or in its entirety without prior permission from Fujitsu.


FUJITSU