HITACHI
Inspire the Next

Hitachi Virtual Storage Platform
Encryption License Key User Guide

FASTFIND LINKS

MK-90RD7015-10

Hitachi Data Systems

Contents

Preface

This guide describes and provides instructions for Encryption License Key (DAR), a feature of Storage Navigator (SN) for the Hitachi Virtual Storage Platform (VSP) storage system. You configure Encryption License Key within SN for the Hitachi Virtual Storage Platform storage system.

Read this document carefully to understand how to use this product, and maintain a copy for reference purposes.

Intended audience

This document is intended for system administrators, HDS representatives, and authorized service providers who install, configure, and operate the Hitachi Virtual Storage Platform storage system.

This document is for users who:

- Have a background in data processing and RAID storage systems.
- Are familiar with the Hitachi Virtual Storage Platform storage system and Storage Navigator.
- Are familiar with the use of encryption in a storage environment.

Product version

This document revision applies to VSP microcode 70-06-1*x* or later.

Document revision level

Revision	Date	Description
MK-90RD7015-00	October 2010	Initial release.
MK-90RD7015-01	December 2010	Supersedes and replaces MK-90RD7015-00.
MK-90RD7015-02	April 2011	Supersedes and replaces MK-90RD7015-01.
MK-90RD7015-03	August 2011	Supersedes and replaces MK-90RD7015-02.
MK-90RD7015-04	November 2011	Supersedes and replaces MK-90RD7015-03.
MK-90RD7015-05	February 2012	Supersedes and replaces MK-90RD7015-04.
MK-90RD7015-06	June 2012	Supersedes and replaces MK-90RD7015-05.
MK-90RD7015-07	August 2012	Supersedes and replaces MK-90RD7015-06.
MK-90RD7015-08	November 2012	Supersedes and replaces MK-90RD7015-07.
MK-90RD7015-09	July 2013	Supersedes and replaces MK-90RD7015-08.
MK-90RD7015-10	April 2014	Supersedes and replaces MK-90RD7015-09.

Changes in this revision

- Added information about the permissions required to format volumes while enabling and disabling data encryption at the parity-group level. Enabling data encryption at the parity group-level on page 4-5 and Disabling data encryption at the parity-group level on page 4-7.

Document organization

The following table provides an overview of the contents and organization of this document. Click the chapter title in the Chapter column to go to that chapter. The first page of each chapter provides links to the sections in that chapter.

Chapter	Description
Chapter 1, Encryption License Key Overview	Describes Encryption License Key features.
Chapter 2, Encryption License Key Installation	Lists the system and administrator requirements.
Chapter 3, Key Management Server Connections	Lists instructions for creating certificates and connection settings for a key management server.
Chapter 4, Managing data encryption license keys	Lists instructions for performing Encryption License Key operations.
Chapter 5, Troubleshooting	Contains troubleshooting information for Encryption License Key operations.
Appendix A, Encryption License Key GUI Reference	Describes the SN windows and dialog boxes for Encryption License Key operations.

Referenced documents

Hitachi Virtual Storage Platform documents:

- *Hitachi Virtual Storage Platform User and Reference Guide*, MK-90RD7042
- *Hitachi Storage Navigator User Guide*, MK-90RD7027
- *Hitachi Audit Log User Guide*, MK-90RD7007

Document conventions

This document uses the following typographic conventions.

Convention	Description
Bold	Indicates text on a window, such as menus, menu options, buttons, text boxes, and labels. **Example:** Click **OK**.
Italic	Indicates a variable, which is a placeholder for actual text provided by the user or system. **Example:** copy *source-filetarget-file* **Note:** Angled brackets (< >) also indicate variables.
`screen/code`	Indicates text that is displayed on screen or typed by the user. **Example:** `# pairdisplay -g oradb`
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. **Example:** `# pairdisplay -g <group>` **Note:** Italic font also indicates variables.

Convention	Description
[ ] square brackets	Indicates optional values. **Example:** [a | b] means that you can choose a, b, or nothing.
{ } braces	Indicates required values. **Example:** { a | b } means that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. **Example:**[a | b] means that you can choose a, b, or nothing.
Underline	Indicates the default value. **Example:** [a | b]

This document uses the following icons to draw attention to information.

Icon	Meaning	Description
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Note	Calls attention to important and/or additional information.
	Caution	Warns the user of adverse conditions and/or consequences (e.g., disruptive operations).
	WARNING	Warns the user of severe conditions and/or consequences (e.g., destructive operations).

Accessing product documentation

The Virtual Storage Platform storage system user documentation is available on the HDS Portal: https://portal.hds.com. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

The HDS customer support staff is available 24 hours a day, seven days a week. If you need technical support, log on to the HDS Portal for contact information: https://portal.hds.com.

Comments

Please send us your comments on this document: doc.comments@hds.com. Include the document title and number, including the revision level (for example, -05), and refer to specific sections and paragraphs whenever possible. All comments become the property of HDS.

Thank you!

1

Encryption License Key Overview

To guarantee the security of the data, use the Encryption License Key (DAR) feature to store encrypted data in an LDEV and encrypt them. The Encryption License Key feature provides redundant backup and restore capabilities to ensure data availability.

Encryption License Key benefits

Encrypting data can prevent information loss or leaks if a disk drive is physically removed from the system. Failure, loss, or theft are the most common reasons for information loss.

The following lists the benefits of using the Encryption License Key feature:

- Hardware-based AES 256 encryption in XTS mode for open and mainframe systems.
- You can apply encryption to some or all of the internal drives without throughput or latency impacts for data I/O and little to no disruption to existing applications and infrastructure.
- Simplified and integrated key management that does note require specialized key management infrastructure.
- Data-center friendliness. The Encryption License Key feature:
  - Uses little additional power (equivalent of one 25 watt light bulb).
  - Produces negligible amounts of additional heat.
  - Does not require additional rack space.

Encryption License Key support specifications

The following table lists the Encryption License Key feature's support specifications.

Item		Specification
Hardware specifications	Encryption algorithm	Advanced Encryption Standard (AES) 256 bit.
	Encryption mode	XTS mode.
LDEVs that you can encrypt	Volume type	Open, mainframe, multiplatform
	Emulation type	All emulation types including OPEN-V and 3390-x.
	Internal/external LDEVs	Internal LDEVs only.
	LDEV with existing data	Supported. Requires data migration.
Managing data encryption license keys	Creating data encryption license keys	Use Storage Navigator (SN) to create the data encryption license key.
	Deleting data encryption license keys	Use SN to delete data encryption license keys.
	Scope of data encryption license keys	32 data encryption license keys per storage system.
	Unit of encryption/decryption	Parity group.
	Backup/Restore functionality	Redundant (P-VOL and S-VOL) backup/restore copies.

Primary and secondary data encryption license keys

The Virtual Storage Platform (VSP) storage system uses the Encryption License Key feature to set up the data encryption license keys to encrypt and decrypt data.

You can use the Encryption License Key feature to back up data encryption license keys. The VSP storage system automatically creates a primary backup of the data encryption license key, and stores this backup on each MP package.

You can create a secondary backup data encryption license key. The secondary backup is required to restore the key if the primary backup is unavailable.

For more information about backing up secondary data encryption license keys, see Workflow for backing up secondary data encryption license keys on page 4-2.

KMIP key management server support

Using the VSP storage system, you can create backup and restore data encryption license keys on a key management server that supports Key Management Interoperability Protocol (KMIP).

For more information about backing up data encryption license keys to a key management server, see Backing up keys to a key management server on page 4-4.

Data encryption workflow

The Encryption License Key feature provides data encryption at the parity-group level to protect the data on LDEVs. Use the following process to set up for and enable data encryption:

1. A secondary data encryption license key is backed up.
2. Data encryption is enabled at the parity-group level.
3. The logical devices (LDEVs) in the parity group are formatted.
4. If V-VOLs are used, the V-VOLs are also formatted.

For more information about enabling data encryption, see Enabling data encryption at the parity group-level on page 4-5.

Data encryption on existing data workflow

Use the following process to encrypt existing data:

1. A new parity group is created. Your service representative creates parity groups using the SVP.
2. Data encryption is enabled on the parity group.
3. The LDEVs in the encrypted parity group are formatted.
4. The existing data is migrated to the new LDEVs in the encrypted parity group.

For more information about moving unencrypted data to an encrypted environment, see Workflow for moving unencrypted data to an encrypted environment on page 4-9.

Disable encrypted data workflow

Use the following process to disable encryption:

1. Data in the parity group is backed up.
2. Data encryption is disabled at the parity-group level.
3. The LDEVs in the parity group are formatted.
4. If V-VOLs are used, the V-VOLs are also formatted.
5. The LDEVs are unblocked.

For more information about disabling encryption, see Disabling data encryption at the parity-group level on page 4-7.

Change data encryption license key workflow

You must migrate data to encrypt data with a different data encryption license key on the VSP storage system.

For more information about migration practices with encryption, see Migration practices with encryption on page 1-4.

Use the following process to change encryption license keys:

1. A new parity group is created.
2. Encryption is enabled with a new data encryption license key.
3. The LDEVs in the encrypted parity group are formatted.
4. The source data is migrated to the new target LDEVs in the encrypted parity group.
5. The data is encrypted with the new data encryption license key on the VSP storage system.

Migration practices with encryption

Migrate encrypted source data by encrypting the target LDEV. Migrate data on a per-LDEV basis. As a best practice, match encrypted areas with other encrypted areas. Do not mix encrypted and unencrypted areas.

Note: When migrating an encrypted LUSE LDEV, migrate all LDEVs within the LUSE volume so that you do not have encrypted and non-encrypted areas.

For more information about encrypting an LDEV, see Workflow for enabling data encryption on parity groups on page 4-4.

Audit logging of encryption events

The VSP storage system Audit Log feature provides audit logging of events that happen in the system. The audit log records events related to data encryption and data encryption license keys.

For more information about audit logging, audit log events, and the Audit Log feature, see the *Hitachi Storage Navigator User Guide* and the *Hitachi Audit Log User Guide*.

Encryption states and protection

Match the encryption states of the primary (P-VOL) and secondary (S-VOL), pool (pool-VOL), journal, or virtual volume (V-VOL). The encryption states must match to copy data or differential data and to protect the data. If the state of the P-VOL is "Encrypt", then the state of all other LDEVs referenced by or associated with the P-VOL should also be "Encrypt".

This practice also applies to migration situations.

For more information about migration and encryption, see Migration practices with encryption on page 1-4.

Interoperability with other software applications

Use the following table to determine the interoperability of software applications with data encryption.

Software application	Interoperability notes
ShadowImage, TrueCopy, Compatible FlashCopy® V2, and Compatible XRC	Encrypt the P-VOL and S-VOLs to ensure data security.
Copy-on-Write Snapshot and Thin Image	Match the encryption states of the P-VOL and pool-VOL. If the P-VOL is encrypted, encrypt all of the pool-VOLs. If the data pool contains non-encrypted pool-VOL, the differential data of the P-VOL is not encrypted.
Universal Replicator	Match the encryption states of a P-VOL and S-VOL. If you encrypt the P-VOL only, the data copied on the S-VOL is not encrypted is not protected. When you encrypt a P-VOL or S-VOL, use a journal to which only encrypted LDEVs are registered as journal volumes. If the encryption states of the P-VOL, S-VOL, and journal volumes do not match, the journal data in the P-VOL is not encrypted, and the security of the data cannot be guaranteed.
LUN Expansion (LUSE)	Encrypt all LDEVs to ensure all areas are encrypted. For more information about LUSE LDEVs and migration practices, see Migration practices with encryption on page 1-4.

Software application	Interoperability notes
Dynamic Provisioning, Dynamic Tiering, Dynamic Provisioning for Mainframe, and Dynamic Tiering for Mainframe	When enabling encryption for data written to a data pool with a V-VOL, use a data pool that consists of encrypted volumes. **Note:** If encryption is set, encryption formatting for pool volumes and V-VOLs is also required.
Cross-system Copy	Encrypt the source LDEV and the target LDEV. The encryption states of the source and target LDEVs must match for the DAR feature to encrypt and guarantee the security of the data on the target LDEV.

2

Encryption License Key Installation

This chapter discusses how to install the DAR feature.

- ☐ Encryption License Key installation workflow
- ☐ System requirements
- ☐ Enabling the Encryption License Key feature

Encryption License Key installation workflow

Use the following workflow to install the DAR feature:

1. Ensure your system meets the system requirements.

   For more information about the system requirements, see System requirements on page 2-2.
2. Ensure your product suite interoperates the way you want it to with the DAR feature.
3. Enable the DAR feature.

   For more information about enabling the DAR feature, see Enabling the Encryption License Key feature on page 2-2.
4. Assign the Security Administrator (View & Modify) role to the administrator who creates, backs up, and restores data encryption license keys.

   For more information about assigning roles, see the *Hitachi Storage Navigator User Guide*.

System requirements

The following table lists the system requirements for using the DAR feature.

Item	Requirement
Hitachi Virtual Storage Platform	• Microcode 70-01-0x and later. • Microcode 70-04-0x and later if you backup and restore data encryption license keys on a key management server.
Hitachi Storage Navigator	• Encryption License Key software license. • Virtual LVI/LUN Manager software. • Security Administrator (View & Modify) role to enable or disable data encryption and to back up or restore keys.
SVP (Web server)	To connect to the key management server by specifying the host name instead of IP address, you need the DNS server settings. For SVP configuration, give your service representative the IP address of the DNS server.
Host platforms	All open-systems and mainframe host platforms are supported.
Data volumes	All volume types and emulations are supported: open-systems, mainframe, and multiplatform. Supported volumes: Internal

Enabling the Encryption License Key feature

Enable the DAR feature in Storage Navigator.

1. Log onto SN.
2. Type the software license key.

3

Key Management Server Connections

You can use an optional key management server with VSP storage systems. This chapter provides information on how to set up the key management server.

- ☐ Key management server requirements
- ☐ Key management server settings workflow

Key management server requirements

If you are using a key management server, it must meet the following requirements:

- Protocol: Key Management Interoperability Protocol 1.0 (KMIP1.0)
- Software: SafeNet KeySecure k460 6.1.0
- Certificates:
  - Root certificate of the key management server (X.509)
  - Client certificate in PKCS#12 format

Root and client certificates

Root and client certificates are required to connect to KMIP servers and to ensure that the network access is good. You upload the certificates to the SVP.

To access the key management server, the client certificate must be current and not have expired.

For more information about the client certificate password in PKCS#12 format:

- Contact the key management server administrator.
- See Client certificate password on page 3-2.

To get copies of the root and client certificates, contact the key management server administrator.

For more information about uploading the client certificates, see Converting the client certificate to the PKCS#12 format on page 3-4.

Root certificate on the key management server

If you use SafeNet KeySecure on the key management server, create and put the root certificate on the server.

For more information about SafeNet KeySecure, see the SafeNet KeySecure k460 6.1.0 documentation.

The root certificate of the key management server must be in X.509 format.

Client certificate password

The password is a string of characters that can be zero up to 128 characters in length. Valid characters are:

- Numbers (0 to 9)
- Upper case (A-Z)
- Lower case (a-z)
- Symbols: ! # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

For more information about converting the client certificate to PKCS#12 format, see Converting the client certificate to the PKCS#12 format on page 3-4.

For more information about client certificates, see Root and client certificates on page 3-2.

Preparing the client certificate workflow

Use the following process to prepare the client certificate, which includes setting the client certificate expiration date and password:

1. Download and install `openssl.exe` from http://www.openssl.org/ to the `C:\openssl` folder.
2. Create the key file. You can create the following types of key files:
   - Private key file.

     For more information about creating a private key file, see Creating a private SSL key file on page 3-3.
   - Public key file.

     For more information about creating a public key file, see Creating a public SSL key file on page 3-4.
3. Convert the client certificate to PKCS#12 format.

   For more information about converting the client certificate, see Converting the client certificate to the PKCS#12 format on page 3-4.
4. Upload the root and client certificates to the SVP.

   For more information uploading the root and client certificate, see Converting the client certificate to the PKCS#12 format on page 3-4.

Private key file creation workflow

(Windows Vista) Prepare private and public SSL key files to use with the DAR feature.

1. If the read-only attribute is set, release it from the `c:\key` folder.
2. Create the private key file.

   For more information about creating a private key file, see Creating a private SSL key file on page 3-3.
3. Create the public key file.

   For more information about creating public key files, see Creating a public SSL key file on page 3-4.

Creating a private SSL key file

Create a private SSL key file to use with the DAR feature. A private key file has the extension (.key).

1. Open a command prompt.
2. Move the current directory to the folder where you have saved the key file (for example, `c:\key`).

3. From a command prompt, run the following command:

   c:\key > c:\openssl\bin\openssl genrsa -out server.key 1024

Creating a public SSL key file

Create a public SSL key file to use with the DAR feature. A public key file has the extension (.csr).

1. Open a command prompt.
2. Move the current directory to the folder where you have saved the key file (for example, `c:\key`).
3. From a command prompt, run the following command:

   c:\key > c:\openssl req -sha256 -new -key server.key -config c:\openssl\bin\openssl.cfg -out server.csr

4. Complete the following information:
   - Country Name (two-letter code)
   - Email Address
   - (Optional) Challenge password
   - (Optional) Common name - To obtain a signed and trusted certificate, ensure that the server name is the same as the host name of the storage device.
   - State or Province Name
   - Locality Name
   - Organization Name
   - Organization Unit Name
   - Common Name
5. Send the public key to the Certificate Authority (CA) of the key management server, and request that the CA issue a signed certificate. Use the signed certificate as the client certificate.

   For more information, see the SafeNet KeySecure k460 6.1.0 documentation.

Converting the client certificate to the PKCS#12 format

Convert the client certificate to the PKCS#12 format, which includes uploading the client certificate in the PKCS#12 format to the 200 Storage Virtualization System (SVP).

1. From an open command prompt, change the current directory to the folder where you want to save the client certificate in the PKCS#12 format.
2. Move the private SSL key file (.key) and the client certificate to the folder in the current directory, and run the command.

   The following is an example for an output folder of `c:\key`, private key file (`client.key`), and a client certificate file (`client.crt`:

   ```
   C:\key>c:\openssl\bin\openssl pkcs12 -export -in client.crt -
   inkey client.key -out client.p12
   ```

3. Upload the client certificate in the PKCS#12 format to the SVP and type the client certificate password.

   For more information about uploading the client certificate, see Converting the client certificate to the PKCS#12 format on page 3-4.

Configuring the connection settings to the key management server

Configure the connection settings to the key management server, which includes uploading the root certificate of the key management server and the client certificate in the PKCS#12 format to the SVP.

1. On the menu bar, click **Settings > Environmental Setting > View Key Management Server Properties**.
2. In the **View Key Management Server Properties** window, click **Setup Key Management Server**.

   If you have not set the connection to the key management server, a message is displayed. Click **OK**.
3. In the **Setup Key Management Server** window, upload the root certificate of the key management server and the client certificate in the PKCS#12 format to the SVP.

Key management server settings workflow

To use a key management server, you must configure the connection and network settings.

For more information about the appropriate connection settings, contact the key management server administrator. For more information about the network settings, contact your network administrator.

Backing up connection settings to the key management server does not back up the client certificate. Use the following process to back up the connection settings to the key management server:

Note: When you back up the connection settings to the key management server, the system does not back up the client certificate. Make sure that you back up a copy of the connection settings to the key management server and save a copy of the client certificate separately.

1. Ensure the client and root certificates are uploaded to the key management server. If the certificates are not uploaded:
   - Contact the key management server administrator.
   - See Converting the client certificate to the PKCS#12 format on page 3-4.
2. Configure the connection settings to the key management server.

   For more information about configuring these settings, see Configuring the connection settings to the key management server on page 3-5.
3. Back up the connection settings to the key management server.

   For more information about the tasks related to backing up the connection settings, see your corporate security policy.
4. Confirm that you can connect to the key management server.

5. Check with the key management server administrator, then save a back up copy of the client certificate.
6. Save a copy of the configuration files.

   For more information on how to save a configuration file, see the *Hitachi Storage Navigator User Guide*.

Viewing the key management server connection settings

View the key management server connection settings.

1. On the menu bar, click **Settings > Environmental Setting > View Key Management Server Properties**.
2. In the **View Key Management Server Properties** window, view the connection settings.

Configuring the connection settings to the key management server

Configure the connection settings to the key management server to set up the key management server and to back up the data encryption license keys to the key management server.

To connect to the key management server by host name instead of IP address, send the IP address of the DNS server to your service representative and request that the service representative configure the SVP.

If the key management server is unavailable after you complete this task, the settings may be incorrect. Contact the server or network administrator.

1. View the key management server connection settings.
2. In the **View Key Management Server Properties** window, click **Setup Key Management Server**.
3. In the displayed message, if you have not set the connection to the key management server, click **OK**.
4. In the **Setup Key Management Server** window, complete the following:
   - Specify the options to connect to the key management server.
   - If the key management server is already in use, click **Check** to test the connection. Otherwise, click **Finish**.

     Error messages appear if the server configuration test fails.
5. In the **Confirm** window, to backup data encryption license keys to the key management server, click **Next**. Otherwise, complete the following and then click **Apply**:
   - Confirm the settings.
   - For **Task Name**, type a name or description for this task.
   - Select **Go to tasks window for status** to open the **Tasks** window.

The connection to the key management server is set up.

4

Managing data encryption license keys

This chapter provides information on how to manage data encryption license keys. Managing the keys includes ensuring availability of keys and accessibility to the encrypted or decrypted data. Manage data encryption license keys using the DAR feature in the VSP storage system.

You must have the Security Administrator (View & Modify) role to manage data encryption license keys.

Workflow for creating data encryption license keys

Create a data encryption license key to use with the DAR feature.

Use the following process to create a data encryption license key:

1. Create the data encryption license key or group of keys.

   For more information about creating keys, see Creating data encryption license keys on page 4-2.

2. Back up a secondary data encryption license key.

   Schedule regular backups of all of your data encryption license keys at the same time one time every week to ensure data availability.

   For more information about backing up secondary keys, see Workflow for backing up secondary data encryption license keys on page 4-2.

Creating data encryption license keys

If you need to change a data encryption license key, create a new data encryption license key. You can create up to 32 data encryption license keys per storage system. Keep at least two keys unused at all times so that you can change an existing key.

1. In the **Administration** tree, click **Encryption Keys**.
2. In the top window, click the **Encryption Keys** tab.
3. In the **Encryption Keys** table, select an unused key ID to use as the new data encryption license key and then complete one of the following:
   - Click **Create Keys**.
   - Click **Settings > Security > Encryption Keys > Create Keys**.
4. In the **Create Keys** window of the **Create Keys** wizard, click **Finish**.
5. In the **Confirm** window of the **Create Keys** wizard, complete the following and then click **Apply**:
   - Confirm the settings.
   - For **Task Name**, type the task name.
   - (Optional) Select **Go to tasks window for status** to open the **Tasks** window.

   The new data encryption license key is created.

Workflow for backing up secondary data encryption license keys

The VSP storage system automatically creates a primary backup of the data encryption license key. Back up a secondary data encryption license key.

Caution: Securely store the secondary backup data encryption license key. Include this process in your corporate security policy.

If the primary data encryption license key becomes unavailable and a secondary backup data encryption license key does not exists, the system cannot decrypt encrypted data.

You must have the Security Administrator (View & Modify) role to back up secondary data encryption license keys.

Use the following process to back up the secondary data encryption license key:

1. Confirm that SN is not processing other tasks. You cannot back up the keys while SN is processing other tasks.
2. Use one of the following methods to back up a secondary data encryption license key:
   - Back up the secondary data encryption license key as a file on the SN computer.

     For more information about backing up secondary data encryption license keys as files, see Backing up keys as a file on page 4-3.
   - Back up data encryption license key to a key management server.

     For more information about backing up keys on key management servers, see Backing up keys to a key management server on page 4-4.

Backing up keys as a file

Back up a secondary data encryption license keys as a file on the SN computer. Back up the file and the password since the file and password are not automatically backed up.

1. In the **Administration** tree, click **Encryption Keys**.
2. In the top window, click the **Encryption Keys** tab.
3. In the **Encryption Keys** table, select the key ID for the data encryption license key you want to back up and complete one of the following:
   - Click **Settings > Security > Encryption Keys > Backup Keys to File**.
   - Click **Backup Keys > To File**.
4. In the **Backup Keys to File** window, complete the following and then click **Finish**:
   - For **Password**, type the key restoration password.

     Case sensitive: Yes
   - For **Re-enter Password**, retype the password.
5. In the **Confirm** window, complete the following and then click **Apply**:
   - Confirm the settings.
   - For **Task Name**, type a task name.
   - (Optional) Select **Go to tasks window for status** to open the **Tasks** window.
6. In the message that appears, click **OK**.
7. Select the location to which to save the backup file, and then type the backup file name using the extension `.ekf`.
8. Click **Save**.

The data encryption license key is backed up as a file on the SN computer.

Backing up keys to a key management server

Back up data encryption license keys to a key management server. The data encryption license keys that you back up to a key management server are managed with the client certificate. You can backup up to 256 data encryption license keys to a key management server.

When you back up to a key management server, the server uses another data encryption license key to encrypt the original keys. Both keys reside on the server.

1. In the **Administration** tree, click **Encryption Keys**.
2. In the top window, click the **Encryption Keys** tab.
3. In the **Encryption Keys** table, select the key ID for the data encryption license key you want to back up to a key management server and then complete one of the following:
   - Click **Settings > Security > Encryption Keys > Backup Keys to Server**.
   - Click **Backup Keys > To Server**.
   - Click **Backup Keys to Server**.
4. (Optional) In the **Backup Keys to Server** window, for **Description**, type a description and then click **Finish**.
5. In the **Confirm** window, complete the following and then click **Apply**:
   - Confirm the settings.
   - For **Task Name**, type the task name.
   - (Optional) Select **Go to tasks window for status** to open the **Tasks** window.

   A secondary backup data encryption license keys is saved.

Viewing backup data encryption license keys

View a list of the data encryption license keys that you have backed up on the key management server, which are shown in a list in the **View Backup Keys on Server** window.

1. In the **Administration** tree, click **Encryption Keys**.
2. In the top window, on the right side of the window, click **View Backup Keys on Server**.

   The **View Backup Keys on Server** window opens.

Workflow for enabling data encryption on parity groups

The Encryption License Key feature provides data encryption at the parity-group level to protect data on LDEVs.

Use the following process to set up for data encryption and enable data encryption on parity groups:

1. Back up the secondary data encryption license key.

   For more information about backing up secondary keys, see Workflow for backing up secondary data encryption license keys on page 4-2.
2. Block the LDEVs at the parity-group level. Do one of the following:
   - Block the LDEV using a file on the SN computer.

     For more information about blocking LDEVs using a file, see Blocking LDEVs using a file on page 4-10.
   - Block the LDEV on the key management server.

     For more information about blocking LDEVs on the key management server, see Blocking LDEVs on the key management server on page 4-11.
3. Enable data encryption on the parity group.

   For more information about enabling data encryption on parity groups, see Enabling data encryption at the parity group-level on page 4-5.
4. Format the LDEVs at the parity-group level.

   For more information about formatting LDEVs in the parity group, see Encryption formatting at the parity-group level on page 4-9.
5. If V-VOLs are used, format the V-VOLs.

   For details about formatting a V-VOL, see Formatting a V-VOL for encryption on page 4-6.

Enabling data encryption at the parity group-level

Enable data encryption at the parity-group level. The Security Administrator (View & Modify) role is required to enable encryption. If you want to format volumes at the same time, the Storage Administrator (Provisioning) role is also required.

1. In the **Storage Systems** tree, click **Parity Groups**.

   In the tree that is shown, **Internal** or **External** is displayed.
2. To select an internal LDEV, select **Internal**. Otherwise, click the **Parity Groups** tab.
3. In the **Parity Groups** table, select a specific parity group on which you want to enable encryption and then click **Actions > Parity Group > Edit Encryption**.

Note: If you do not select a specific parity group, data encryption is enabled on all of the parity groups in the list.

4. In the **Edit Encryption** window of the **Edit Encryption** wizard, complete the following and then click **Add**:
   - For **Available Groups**, select the parity group for which you want to enable data encryption.
   - For **Encryption Key**, select the key ID of which to enable data encryption or select **Disable** to disable data encryption at the parity-group level.
   - For **Format Type**, select the format type.

Values: Quick Format, Normal Format, or No Format

Default: Quick Format

The parity group you selected from the **Available Parity Groups** table is added to the **Selected Parity Groups** list.

5. Click **Finish**.
6. In the **Confirm** window, complete the following and then click **Apply**:
   - Confirm the settings.
   - For **Task Name**, type the task name.
   - (Optional) Select **Go to tasks window for status** to open the **Tasks** window.
7. In the message that appears, click **OK**.

   Data encryption is enabled on the parity group.

Formatting a V-VOL for encryption

If you use a V-VOL, encryption formatting for the V-VOL is required. For details about formatting LDEVs, including V-VOLs, see the Provisioning Guide for Open Systems or the Provisioning Guide for Mainframe Systems.

1. In the **Storage System** tree, select a resource to show one of the following tabs:
   - **LDEVs** tab when you select a parity group in **Parity Groups**
   - **LDEVs** tab when you select **Logical Devices**
   - **Virtual Volumes** tab when you select a pool in **Pools**
2. Select the LDEV, and click **Format LDEVs**.

   The **Format LDEVs** window is displayed.
3. Select the **Normal** format type (required for V-VOLs), and click **Finish**.

   The Confirmation window is displayed.
4. Confirm the settings and click **Apply**.

   If you select **Go to tasks window for status**, the **Tasks** window is displayed.

Workflow for disabling data encryption at the parity-group level

Disable encryption, or decrypt data, at the parity-group level.

1. Back up the secondary data encryption license key.

   For more information about backing up a secondary key, see Workflow for backing up secondary data encryption license keys on page 4-2.
2. Block the LDEV at the parity-group level.

   For more information about blocking LDEVs, see Blocking LDEVs at the parity-group level on page 4-7.
3. Disable data encryption at the parity-group level.

For more information about disabling data encryption, see Disabling data encryption at the parity-group level on page 4-7.

4. Format the LDEVs in the parity group for encryption.

   For more information about formatting LDEVs, see Encryption formatting at the parity-group level on page 4-9.

5. If V-VOLs were used, the V-VOLs are also formatted.

   For more information about formatting a V-VOL, see Formatting V-VOLs for unencryption on page 4-8.

6. Unblock the LDEVs.

   For more information about unblocking LDEVs, see Unblocking LDEVs at the parity-group level on page 4-9.

Blocking LDEVs at the parity-group level

Block the LDEVs at the parity-group level so that you can disable data encryption and format LDEVs. Blocked LDEVs in the parity group have a status of "Blocked."

Note: You cannot write to a blocked LDEV.

1. From the SN main window, click **Explorer > Storage System > volume (resource)**.
2. On the **LDEVs** tab, complete one of the following and then click **Block LDEVs**:
   - For **Parity Group**, select the parity group to which the LDEV is associated.
   - For **Logical Device**, select the LDEV you want to block.
3. In the confirmation message that appears, click **Apply**.

   The LDEV is blocked.

Disabling data encryption at the parity-group level

Disable data encryption at the parity-group level to perform (normal) formatting options on encrypted data, such as writing to or overwriting an LDEV. You must have Security Administrator (View & Modify) role to disable encryption. If you want to format volumes at the same time, the Storage Administrator (Provisioning) role is also required.

1. In the **Storage Systems** tree, click **Parity Groups**.

   In the tree, **Internal** or **External** is displayed.

2. To select an internal LDEV, select **Internal**. Otherwise, select the **Parity Groups** tab.
3. On the **Encryption Keys** tab, select the name for the parity group name you want to disable encryption and then complete one of the following:
   - Click **Actions > Parity Group > Edit Encryption**.
   - Click **More Actions > Edit Encryption**.

4. In the **Edit Encryption** window, complete the following and then click **Add**:
   - For **Available Parity Groups**, choose the parity group on which you want to disable data encryption.
   - For **Encryption Key**, select **Disable**.
   - For **Format Type**, choose the format type.

   The parity group you selected from the **Available Parity Groups** list is added to the **Selected Parity Groups** list.

Note: If an LDEV is listed in the **Selected Parity Groups** list, format the LDEVs.

For more information about formatting LDEVs, see Encryption formatting at the parity-group level on page 4-9.

The format type in the **Selected Parity Groups** list changes to No Format regardless of the status of for format type.

5. In the **Edit Encryption** window, click **Finish**.
6. In the **Confirm** window, complete the following and then click **Apply**:
   - Confirm the settings.
   - For **Task Name**, type the task name.
   - (Optional) Select **Go to tasks window for status** to open the **Tasks** window.
7. In the confirmation message that appears asking whether to apply the setting to the storage system, click **OK**.

   Encryption is disabled for the parity group.

Formatting V-VOLs for unencryption

If you use a V-VOL, unencryption formatting for the V-VOL is required.

1. In the **Storage System** tree, select a resource to show one of the following tabs:
   - **LDEVs** tab when you select a parity group in **Parity Groups**
   - **LDEVs** tab when you select **Logical Devices**
   - **Virtual Volumes** tab when you select a pool in **Pools**
2. Select the LDEV and click **Format LDEVs**.

   The **Format LDEVs** window is displayed.
3. Select the **Normal** format type (required for V-VOLs), and click **Finish**.

   The Confirmation window is displayed.
4. Confirm the settings and click **Apply**.

   If you select **Go to tasks window for status**, the **Tasks** window is displayed.

Encryption formatting at the parity-group level

The LDEV formatting operation writes zero data to the entire area of all drives in the parity group, or overwrites an LDEV. This process is also referred to as encryption formatting. If you use a V-VOL, encryption/unencryption formatting for the V-VOL is required.

Unblocking LDEVs at the parity-group level

Unblock LDEVs at the parity-group level to protect the data after you format an LDEV at the parity-group level. Unblocked LDEVs in the parity group have a status of "Unblocked".

1. From the SN main window, click **Explorer > Storage System > volume (resource)**.
2. On the **LDEVs** tab, complete the following and then click **Unblock LDEVs**:
   - For **Parity Group**, select the parity group to which the LDEV is associated.
   - For **Logical Device**, select the LDEV you want to unblock.
3. In the confirmation message that appears, click **Apply**.

   The LDEV is unblocked.

Workflow for moving unencrypted data to an encrypted environment

Migrate existing data to new LDEVs in an encrypted parity group.

If you are migrating existing unencrypted data to an environment with encryption, the process includes the following additional steps:

1. Move the unencrypted data from the VSP storage system to another storage system.

   For more information about moving unencrypted data, call the Support Center.
2. Create a new parity group. Your service representative creates parity groups using the SVP.
3. Enable data encryption on the parity group.

   For more information about enabling data encryption on parity groups, see Enabling data encryption at the parity group-level on page 4-5.
4. Format the LDEVs in the encrypted parity group.

   For more information about formatting LDEVs, see Encryption formatting at the parity-group level on page 4-9.
5. Migrate the existing data to the new LDEVs in the encrypted parity group.

   For more information about migration practices with encryption, see Migration practices with encryption on page 1-4.

For more information about data migration services, call the Support Center.

Workflow for restoring data encryption license keys

Restore a data encryption license key from the primary or secondary backup copy when all the LDEVs belonging to an encrypted parity group are blocked or if an existing data encryption license key becomes unavailable or you cannot use it. For example, a system failure occurred.

The system automatically restores data encryption license keys from the primary backup. You must have Security Administrator (View & Modify) role to restore the data encryption license key from a secondary backup data encryption license key.

Use the following process to restore a data encryption license key:

1. Block the LDEVs associated to the encrypted parity group. Do one of the following:
   - Block the LDEV using a file on the SN computer.

     For more information about blocking LDEVs using a file, see Blocking LDEVs using a file on page 4-10.
   - Block the LDEV on the key management server.

     For more information about blocking LDEVs on the key management server, see Blocking LDEVs on the key management server on page 4-11.
2. Restore an data encryption license key from a primary or secondary backup copy. Do one of the following:
   - Restore the data encryption license keys from a file backed up on the SN computer.

     For more information about restoring keys from a file, see Restoring keys from a file on page 4-11.
   - Restoring data encryption license keys from the key management server.

     For more information about restoring keys from the key management server, see Restoring keys from a key management server on page 4-12.

Blocking LDEVs using a file

Block LDEVs at the parity-group level from a file on the SN computer.

1. From the SN main window, click **Explorer > Storage System > volume (resource)**.
2. On the **LDEVs** tab, complete one of the following and then click **Block LDEVs**:
   - For **Parity Group**, select the parity group to which the LDEV is associated.
   - For **Logical Device**, select the LDEV you want to block.

3. In the confirmation message that appears, click **Apply**.

   The LDEV is blocked.

Blocking LDEVs on the key management server

Block LDEVs at the parity-group level from the key management server.

1. From the SN main window, click **Explorer > Storage System > volume (resource)**.
2. On the **LDEVs** tab, complete one of the following and then click **Block LDEVs**:
   - For **Parity Group**, select the parity group associated to the LDEV you want to block.
   - For **Logical Device**, select the LDEV you want to block.
3. In the confirmation message that appears, click **Apply**.

   The LDEVs is blocked.

Restoring keys from a file

Restore the data encryption license keys from a file backed up on the SN computer.

1. In the **Administration** tree, click **Encryption Keys**.
2. In the top window, click the **Encryption Keys** tab.
3. Complete one of the following:
   - Click **Settings > Security > Encryption Keys > Restore Keys from File**.
   - Click **Restore Keys > From File**.
4. In the **Restore Keys from File** window, click **Browse** and then click **OK**.
5. In the **Open** dialog box, select the backup file and click **Open**.
6. In the **Restore Keys from File** window, complete the following item and then click **Finish**:
   - For **File Name**, shows the name of the selected file.

     View-only: Yes
   - For **Password**, type the password for the data encryption license key that you typed when you backed up the selected data encryption license key.
7. In the **Confirm** window, complete the following and then click **Apply**:
   - Confirm the settings.
   - For **Task Name**, type the task name.
   - (Optional) Select **Go to tasks window for status** to open the **Tasks** window.

   The data encryption license key is restored.

Restoring keys from a key management server

Restore a data encryption license key from the key management server. You can restore up to 32 data encryption license keys at a time.

The client certificate is required to restore backed up data encryption license keys from a key management server.

Caution: If you do not have the client certificate, and the system administrator replaces the SVP due to a failure, you cannot restore the backed up data encryption license keys.

1. In the **Administration** tree, click **Encryption Keys**.
2. In the top window, click the **Encryption Keys** tab and complete one of the following:
   - Click **Settings > Security > Encryption Keys > Restore Keys from Server**.
   - Click **Restore Keys > From Server**.
   - Click **Restore Keys from Server**.
3. In the **Restore Keys from Server** window, select the data encryption license key you want to restore and then click **Finish**.
4. In the **Confirm** window, complete the following and then click **Apply**:
   - Confirm the settings.
   - For **Task Name**, type a task name.
   - (Optional) Select **Go to tasks window for status** to open the **Tasks** window.

   The backup data encryption license key is restored.

Workflow for changing data encryption license keys

Encrypt data with a different data encryption license key.

Use the following process to change the data encryption license key:

1. Create a new parity group.
2. Enable encryption with the new data encryption license key.

   For more information about enabling data encryption at the parity-group level, see Enabling data encryption at the parity group-level on page 4-5.
3. Format the LDEVs in the encrypted parity group.

   For more information about formatting LDEVs in the encrypted parity groups, see Encryption formatting at the parity-group level on page 4-9.
4. Migrate the existing data to the new LDEVs in the encrypted parity group.

   For more information about data migration services, call the Support Center.

   For more information about migration practices with encryption, see Migration practices with encryption on page 1-4.

5. Encrypt the data with the new data encryption license key on the VSP storage system.

Workflow for deleting data encryption license keys

Delete a data encryption license key from a file on the SN computer or from a key management server.

Use the following process to delete a data encryption license key:

1. Back up the secondary data encryption license key.

   For more information about backing up secondary data encryption license keys, see Workflow for backing up secondary data encryption license keys on page 4-2.

2. Ensure the key is not allocated to the parity group.

   For more information about checking the key allocation, see Creating data encryption license keys on page 4-2.

3. Delete the data encryption license key using one of the following methods:
   - Delete the key from a file on the SN computer.

     For more information about deleting keys from the SN computer, see Deleting data encryption license keys on page 4-13.
   - Delete the backup key from the key management server.

     For more information about deleting backup keys from a key management server, see Deleting backup data encryption license keys from the server on page 4-14.

Deleting data encryption license keys

Delete data encryption license keys from a file on the SN computer.

You cannot delete data encryption license keys that you have not created or keys that are allocated to the parity group.

1. In the **Administration** tree, click **Encryption Keys**.
2. In the top window, click the **Encryption Keys** tab.
3. From the **Encryption Keys** table, select the key ID for the data encryption license key you want to delete and then complete one of the following:
   - Click **Settings > Security > Encryption Keys > Delete Keys**.
   - Click **More Actions > Delete Keys**.
4. In the **Delete Keys** window, click **Finish**.
5. In the **Confirm** window, complete the following and then click **Apply**:
   - Confirm the settings.
   - For **Task Name**, type a task name.
   - (Optional) Select **Go to tasks window for status** to open the **Tasks** window.

The data encryption license key is deleted from the file on the SN computer.

6. In the message that appears asking whether to apply the setting to the storage system, click **OK**.

Deleting backup data encryption license keys from the server

Delete a backup data encryption license key from the key management server.

Caution: Before deleting a primary or secondary backup data encryption license key from the key management server, ensure that you have backed up another data encryption license key.

1. View the backup data encryption license keys on the key management server.
2. In the **View Backup Keys on Server** window, select the key ID for the backup data encryption license key you want to delete and then complete one of the following:
   - Click **Settings > Security > Encryption Keys > Delete Keys**.
   - Click **Delete Backup Keys on Server**.
   - Click **More Actions > Delete Keys**.
3. In the **Delete Backup Keys on Server** window, complete the following and then click **Apply**:
   - Confirm the settings.
   - For **Task Name**, type the task name.
   - (Optional) Select **Go to tasks window for status** to open the **Tasks** window.
4. In the message that appears asking whether to apply the setting to the storage system, click **OK**.

   The system deletes the backup data encryption license key.

Exporting encryption license key table information

You can output encryption license key table information.

1. In the **Administration** tree, click **Encryption Keys**.
2. In the top window, click the **Encryption Keys** tab.
3. From the **Encryption Keys** table, select the key ID for the data encryption license key information you want to output and then complete one of the following:
   - Click **Settings > Security > Encryption Keys > Export**.
   - Click **More Actions > Export**.

5

Troubleshooting

Common problems using DAR include connection problems, license problems, and administrator permission problems. Managing or changing encryption settings is not possible if you cannot connect, write to, or run the storage system.

- ☐ Encryption events in the audit log
- ☐ Problems and solutions
- ☐ Contacting the Hitachi Data Systems Support Center

Encryption events in the audit log

The VSP storage system audit log records events related to the DAR feature, including data encryption and DAR processes. You can export an audit log that contains encryption events in near real-time to an external syslog server.

For more information about the audit log and how to export log events, see the *Hitachi Storage Navigator User Guide* and the *Hitachi Audit Log User Guide*.

Encryption License Key processes that the audit log records

The audit log records all of the tasks that you do using the DAR feature. The tasks are recorded as audit log notations.

The following table lists the audit log notations and their meaning.

Log notation	Meaning
Backup Keys	The system created a backup of a data encryption license key.
Backup Keys to File	The system created a backup of a data encryption license key to a file.
Backup Keys to Serv	The system created a backup of a data encryption license key to a key management server.
Create Keys	The system created one or more data encryption license keys.
Delete Keys	The system deleted one or more data encryption license keys.
Delete Keys on Serv	The system deleted one or more data encryption license keys on a key management server.
Edit Encryption	The system enabled or disabled encryption at the parity group level.
Restore Keys	The system restored one or more data encryption license keys.
Restore Keys fr File	The system restored one or more data encryption license keys from a file.
Restore Keys fr Serv	The system restored one or more data encryption license keys from a key management server.
Setup Key Mng Serv	The system set up a key management server.

Problems and solutions

For troubleshooting information about the VSP storage system, see the *Hitachi Virtual Storage Platform User and Reference Guide*.

For troubleshooting information about SN, see the *Hitachi Storage Navigator User Guide* and *Hitachi Storage Navigator Messages*.

The following table lists common problems and solutions for encryption features.

Problem	Action
Cannot use the DAR feature to back up or restore a key.	Make sure that: • The Encryption License Key software license is valid and installed. • You have the Security Administrator (View & Modify) role. • If you backup and restore data encryption license keys with a key management server, the connection to the key management server is available.
Cannot create or delete data encryption license keys.	Make sure that: • The Encryption License Key software license is valid and installed. • You have the Security Administrator (View & Modify) role.
Cannot enable encryption for a parity group.	Make sure that: • The Encryption License Key software license is valid and installed. • All LDEVs in the parity group are in the blocked status.
Cannot disable encryption for a parity group.	Make sure that all LDEVs in the parity group are in the blocked status.
Cannot restore a data encryption license key.	Make sure that: • The Encryption License Key software license is valid and installed. • You have the Security Administrator (View & Modify) role. • If you backup and restore data encryption license keys with a key management server, the connection to the key management server is available.
Server configuration test failed.	Check the following key management server connection settings: • Host name • Port number • Client certificate file • Root certificate file If the communication failure is due to the length of time to connect to the server, try changing these settings: • Timeout • Retry interval • Number of retries

Contacting the Hitachi Data Systems Support Center

When contacting the Hitachi Data Systems Support Center, provide as much information about the problem as possible, including:

- The circumstances surrounding the error or failure.
- The content of any error message(s) displayed on the host system(s).
- The content of any error message(s) displayed on SN.
- The SN configuration information (use the FD Dump Tool).
- The service information messages (SIMs), including reference codes and severity levels, that SN displays.

The HDS customer support staff is available 24 hours a day, seven days a week. If you need technical support, log on to the HDS Support Portal for contact information: https://hdssupport.hds.com

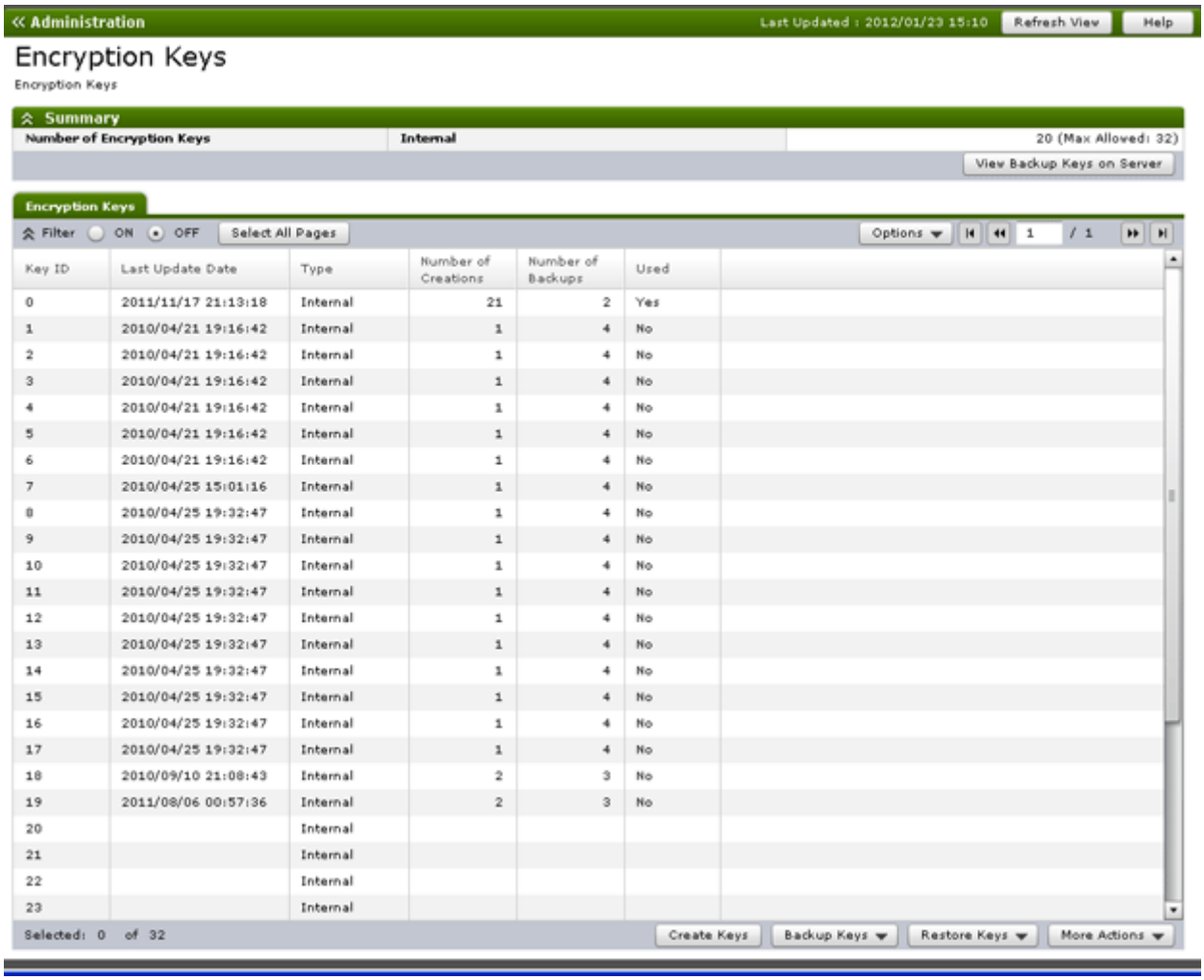
Encryption License Key GUI Reference

This chapter includes descriptions of encryption-related SN windows and dialog boxes for the DAR feature.

For more information about other SN windows and dialog boxes, see the *Hitachi Storage Navigator User Guide*.

Top window when selecting Encryption Keys

Use the top window to create data encryption license keys. Clicking **Encryption Keys** in the **Administration** tree opens this window.



The top window includes the following section and tab:

- Summary section on page A-2
- Encryption Keys tab on page A-3

Summary section

Use the **Summary** section to view details about the number of data encryption license keys and to open the **View Backup Keys on Server** window.

Item	Description
Number of Encryption Keys	Shows the number of data encryption license keys: • **Internal:** Number of data encryption license keys for internal LDEVs. • **External:** Number of data encryption license keys for external LDEVs.
View Backup Keys on Server button	Opens the **View Backup Keys on Server** window.

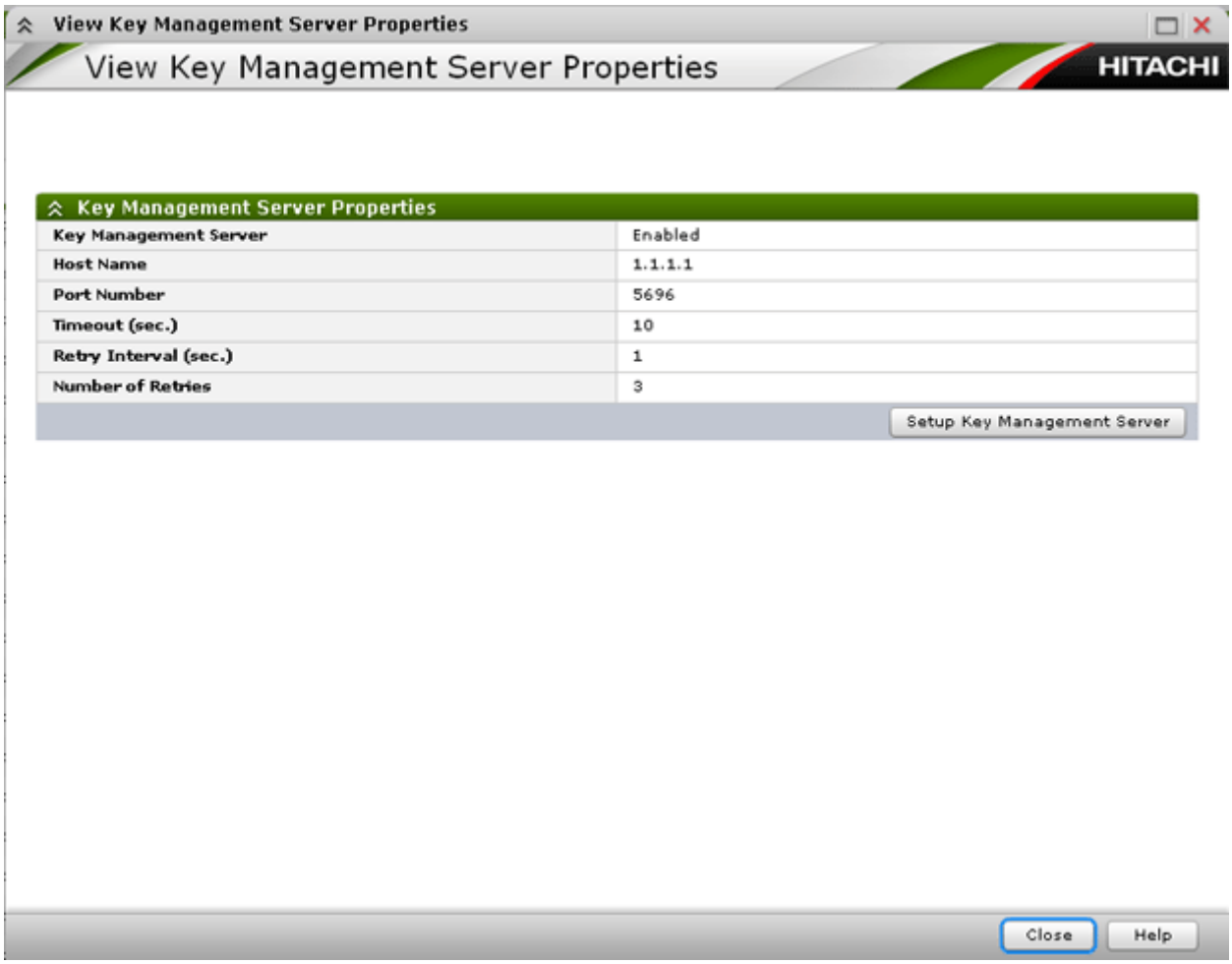
Encryption Keys tab

Use the **Encryption Keys** tab to view a list of the data encryption license key details and to select an unused data encryption license key to create.

Item	Description
Key ID	IDs of data encryption license keys.
Last Update Date	The date and time the data encryption license key was created or was last updated.
Type	The data encryption license key types. If the key ID is 0 to 31, the label **Internal** is displayed.
Number of Creations	The number of times that a data encryption license key is created.
Number of Backups	The number of times that a backup of a data encryption license key is created.
Used	Shows whether the data encryption license key is used.
Create Keys button	Click to open the **Create Keys** window.
Backup Keys drop-down list	Select **To File** to open the **Backup Keys to File** window. Select **To Server** to open the **Backup Keys to Server** window.
Restore Keys drop-down list	Select **From File** to open the **Restore Keys from File** window. Select **From Server** to open the **Restore Keys from Server** window.
More Actions drop-down list	Select **Delete Keys** from the list to delete a selected data encryption license key. Select **Export** from the list to open the window for outputting table information.

View Key Management Server Properties window

Use the **View Key Management Server Properties** window to view key management server properties.



Item	Description
Key Management Server	The key management server. Values: • Enable - shows that a key management server is used. • Disable -shows that a key management server is not used.
Host Name	Host name of the key management server.
Port Number	Port number of the key management server.
Timeout (sec.)	Shows the time (in seconds) until the connection attempt to the key management server times out.
Retry Interval (sec.)	Shows the time (in seconds) to wait before initiating a connection to the key management server.
Number of Retries	Shows the number of times to initiate a connection to the key management server.
Setup Key Management Server	Opens the **Setup Key Management Server** window.

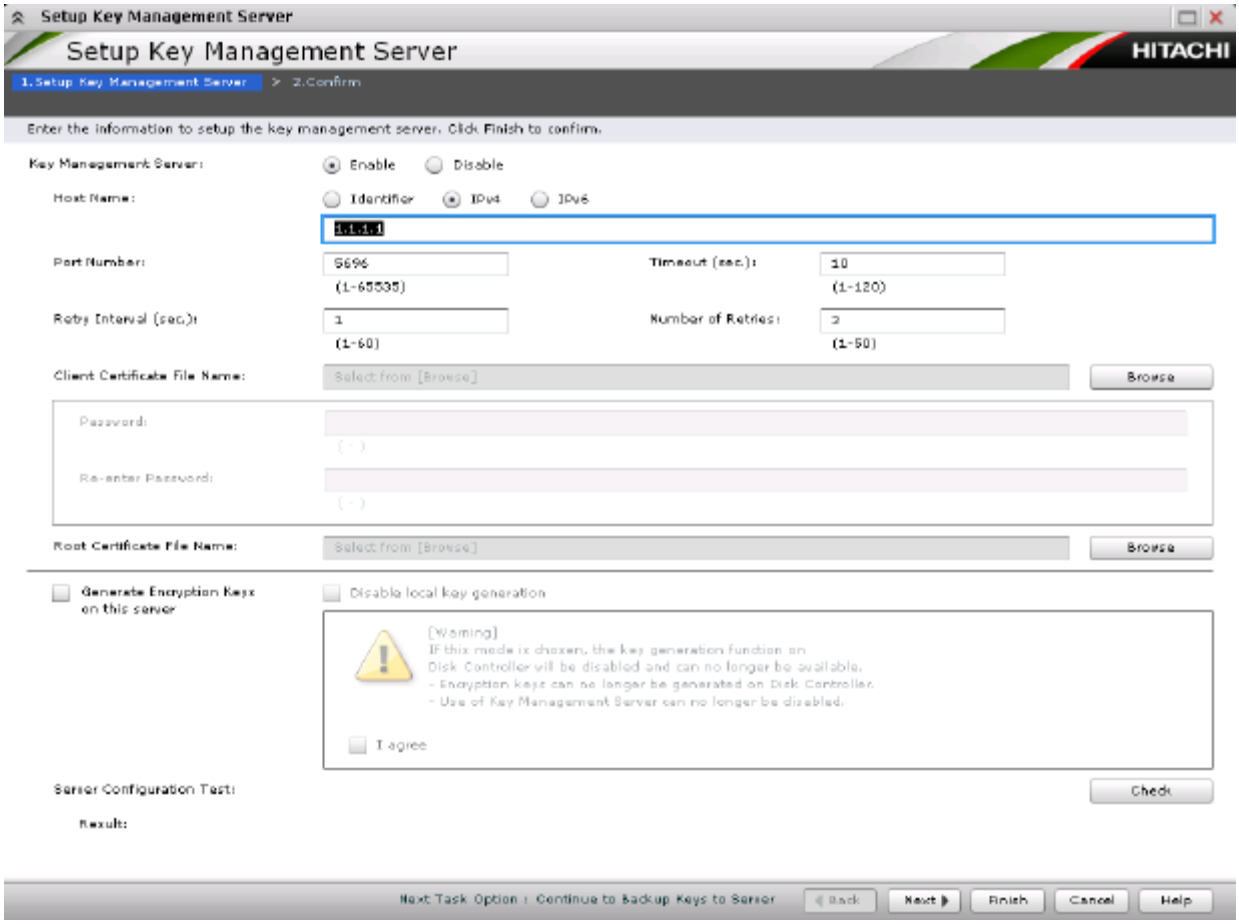
Setup Key Management Server wizard

Use the **Setup Key Management Server** wizard to set up the key management server.

The **Setup Key Management Server** wizard includes the following windows:

- **Setup Key Management Server** window
- **Confirm** window

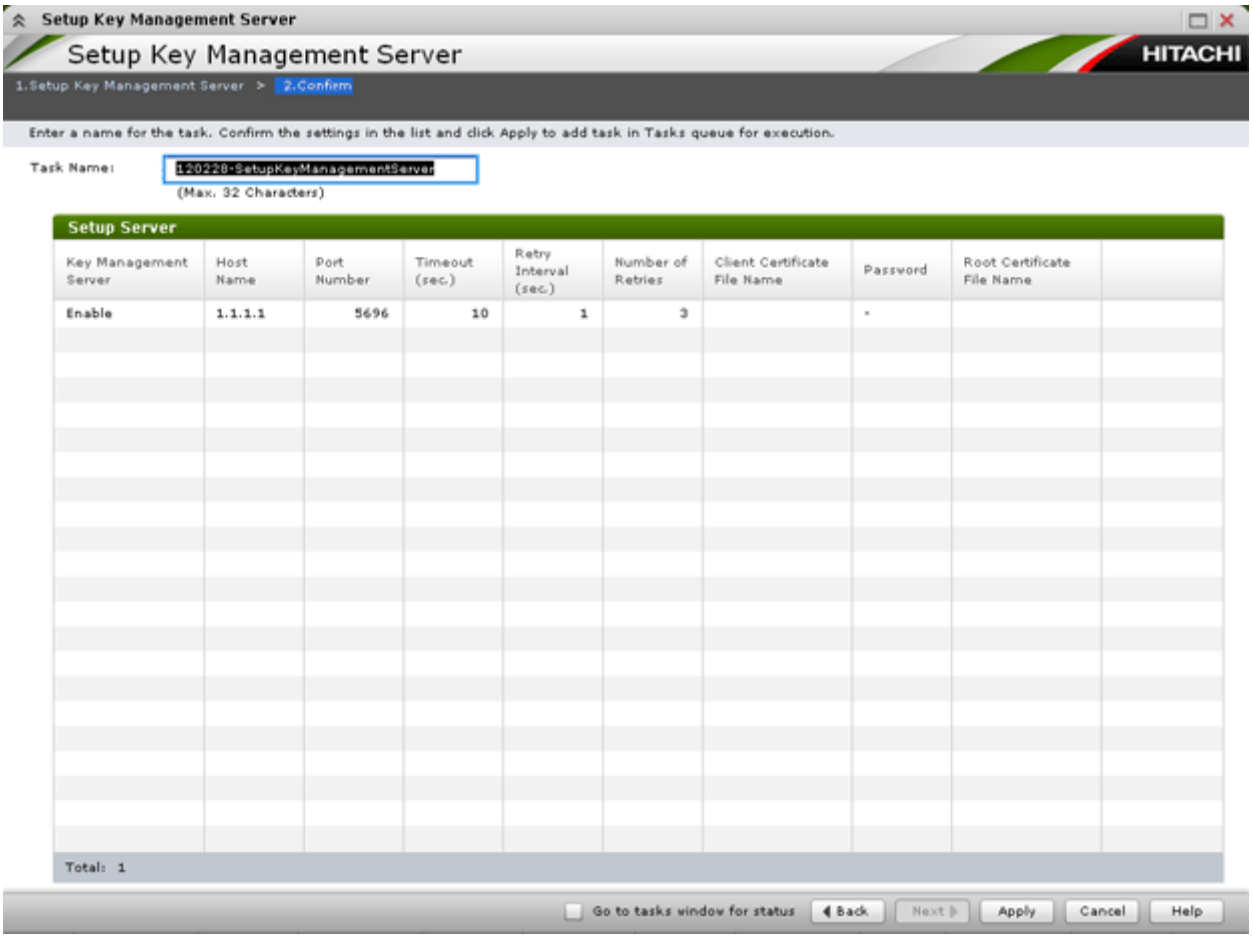
Setup Key Management Server window



Item	Description
Key Management Server	Select whether to use the key management server: • **Enable:** (default) key management server is used. • **Disable:** key management server is not used.
Host Name	The host name of the key management server: • **Identifier:** Type the identifier of the host. • **IPv4:** Type the IPv4 address of the host. • **IPv6:** Type the IPv6 address of the host.

Item	Description
Port Number	The port number of the key management server. Values: 1 to 65535 Default: 5696
Timeout (sec.)	The time until the connection attempt to the key management server times out. Values: 1 to 120 Default: 10
Retry Interval (sec.)	The interval to retry the connection to the key management server. Values: 1 to 60 Default: 1
Number of Retries	The number of times to retry the connection to the key management server. Values: 1 to 50 Default: 3
Client Certificate File Name	Shows the name of the client certificate file. Click **Browse** and select the client certificate file to connect to the key management server.
Browse	Shows a list of the client certificate file from which you can choose. For more information about the client certificate file, contact the server or network administrator.
Password	The password for the client certificate. Character limits: 0 to 128 Valid characters: • Numbers (0 to 9) • Upper case (A-Z) • Lower case (a-z) • Symbols: ! # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
Re-enter Password	Type the password again for confirmation.
Root Certificate File Name	Displays the name of the selected file. Select the root certificate file for connecting to the key management server. Click **Browse** and select the file.
Browse	Select the root certificate file. The form of the client certificate is X.509. For more information about the root certificate file, contact the server administrator or the network administrator.
Server Configuration Test	Click **Check** to start a server connection test for the key management server based on the specified settings.
Check	Start a server connection test for the key management server based on the specified settings.
Result	Shows the result of the server connection test for the key management server.

Confirm window in the Setup Key Management Server wizard



Item	Description
Key Management Server	Shows whether the key management server is used. • **Enable:** key management server is used. • **Disable:** key management server is not used.
Host Name	Host name of the key management server.
Port Number	Port number of the key management server.
Timeout (sec.)	Shows the time until the connection attempt to the key management server times out.
Retry Interval (sec.)	Shows the interval to retry the connection to the key management server.
Number of Retries	Shows the number of times to retry the connection to the key management server.
Client Certificate File Name	Shows the name of the client certificate file used to connect to the key management server.
Password	Shows the password for the client certificate as ****** (six asterisks).
Root Certificate File Name	Shows the root certificate file for connecting to the key management server.

Create Keys wizard

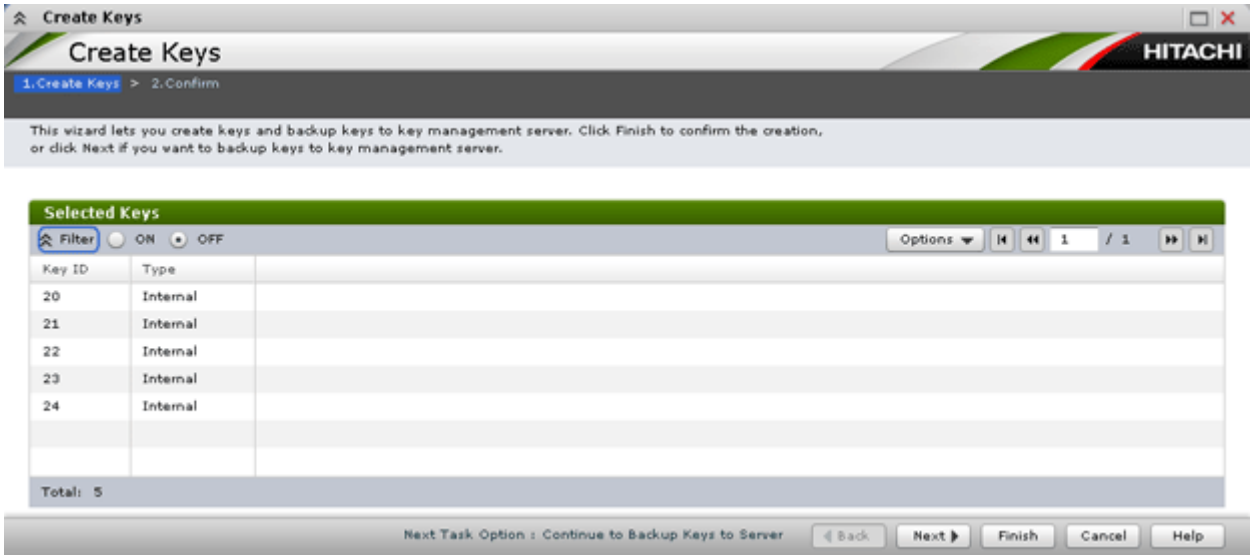
Use the **Create Keys** wizard to create keys and to backup keys to the key management server.

This wizard includes the following windows:

- **Create Keys** window
- **Confirm** window

Create Keys window

Use the **Create Keys** window to create a data encryption license key. This window includes the **Selected Keys** table.

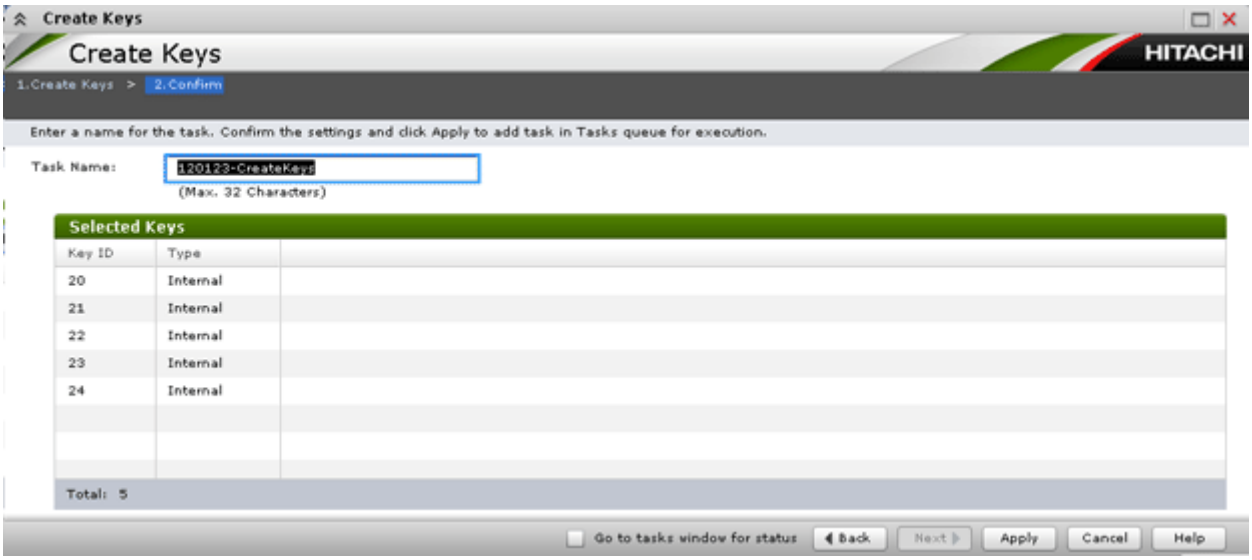


Selected Keys table on Create Keys window

The following table lists descriptions of the items in the **Selected Keys** table on the **Create Keys** window.

Item	Description
Key ID	The identifiers for the data encryption license keys.
Type	The data encryption license key types. If the Key ID is 0 to 31, the label **Internal** is displayed.
Finish	Click to create the data encryption license key.
Next	Click to continue to add a task name to the data encryption license key.

Confirm window in the Create Keys wizard



Selected Keys table on Confirm window

The following table lists descriptions of the items in the **Selected Keys** table on the **Confirm** window.

Item	Description
Key ID	The identifiers for the backup data encryption license keys.
Type	The data encryption license key types. If the Key ID is 0 to 31, the label **Internal** is displayed.

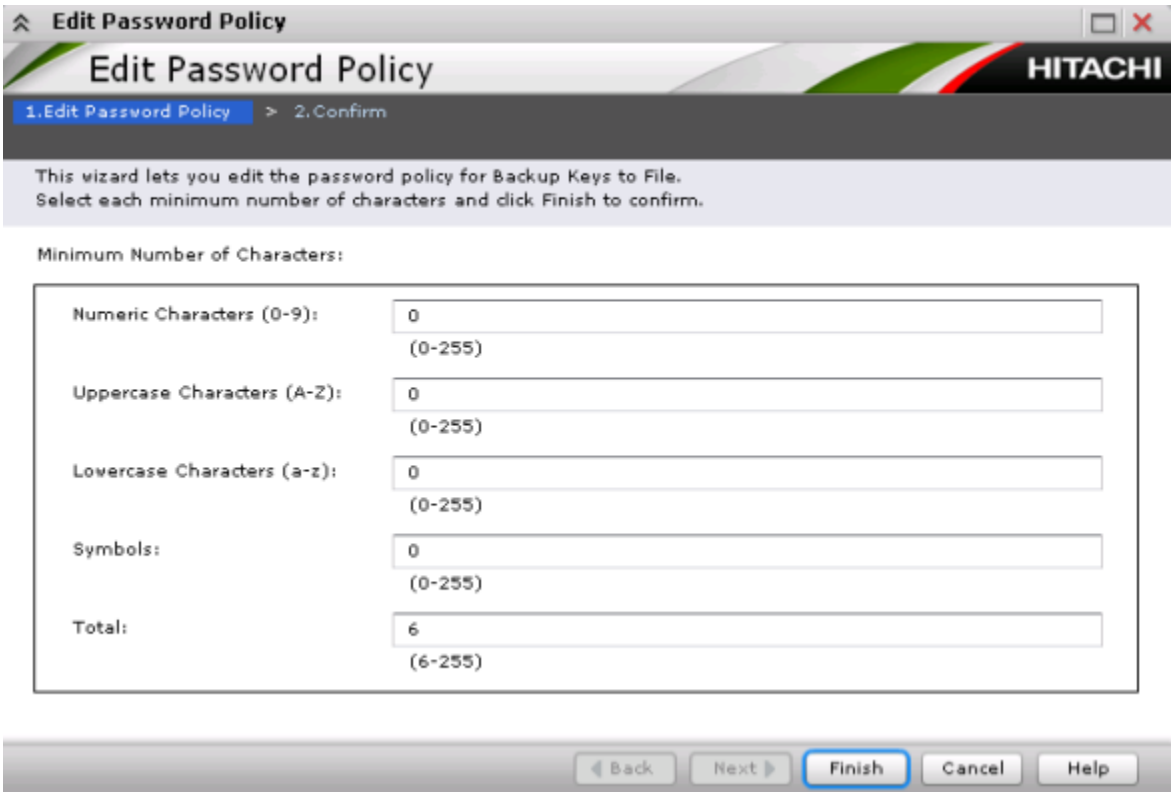
Edit Password Policy wizard

Use the **Edit Password Policy** wizard to edit the password policy for backup keys.

This wizard includes the following windows:

- **Edit Password Policy** window
- **Confirm** window

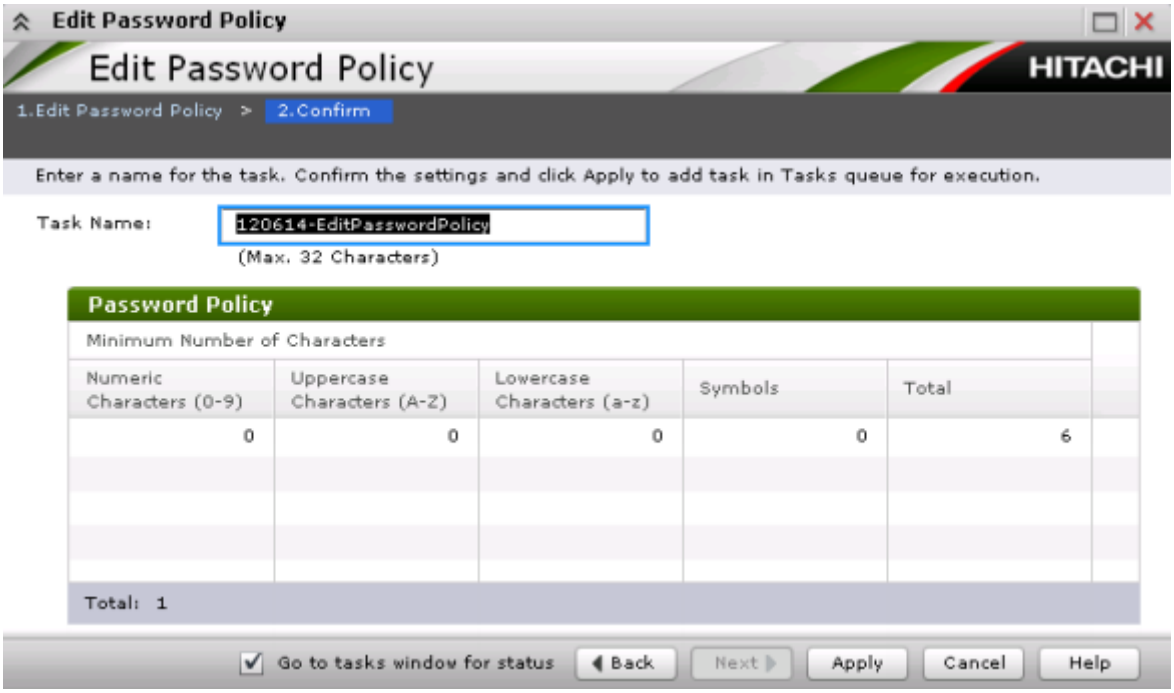
Edit Password Policy window



Item	Description
Numeric Characters (0-9)	The minimum number of numeric characters that should be used for this password. Values: 0 to 255 Default: 0
Uppercase Characters (A-Z)	The minimum number of alphabetical upper case characters that should be used for this password. Values: 0 to 255 Default: 0
Lowercase Characters (a-z)	The minimum number of alphabetical lower case characters that should be used for this password. Values: 0 to 255 Default: 0
Symbols	The minimum number of symbols that should be used for this password. Values: 0 to 255 Default: 0
Total	The minimum number of characters for this password. Values: 6 to 255 Default: 6

Confirm window in the Edit Password Policy wizard

Use the **Confirm** window in the **Edit Password Policy** wizard to confirm the changes to the password policy.



Item	Description
Numeric Characters (0-9)	Displays the minimum number of numeric characters that should be used for this password.
Uppercase Characters (A-Z)	Displays the minimum number of alphabetical upper case characters that should be used for this password.
Lowercase Characters (a-z)	Displays the minimum number of alphabetical lower case characters that should be used for this password.
Symbols	Displays the minimum number of symbols that should be used for this password.
Total	Displays the minimum number of characters for this password.

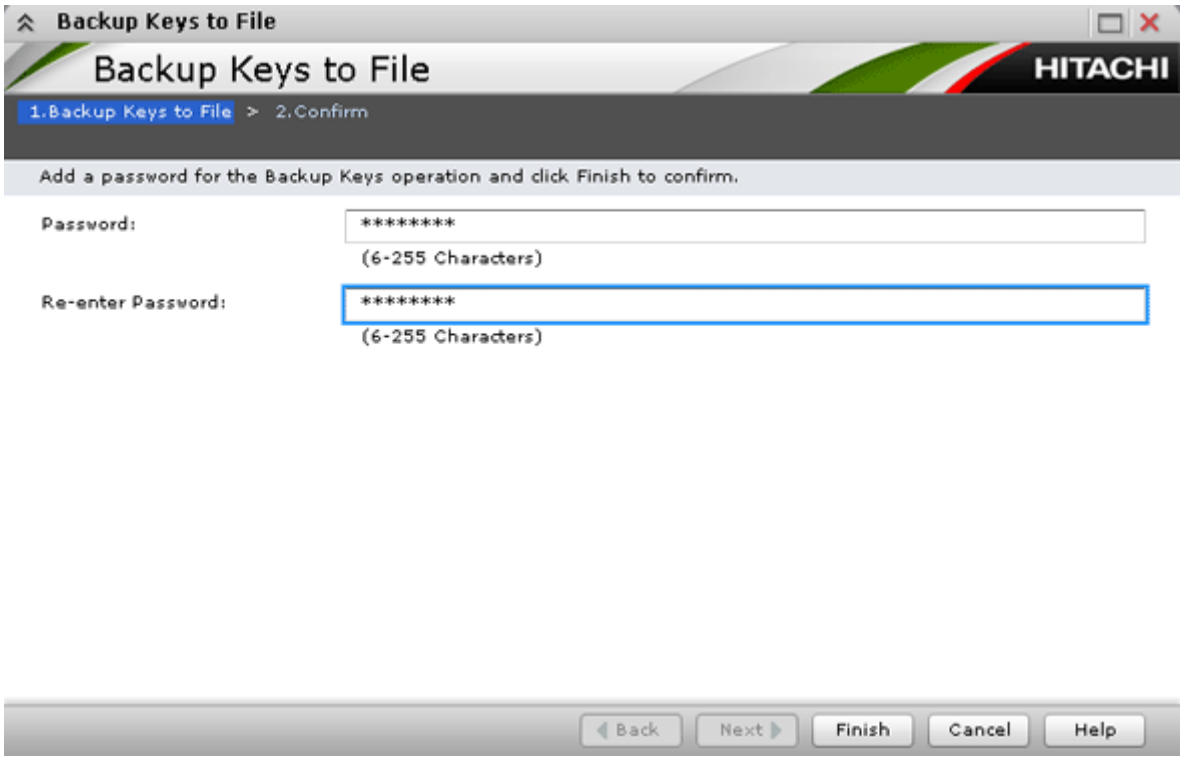
Backup Keys to File wizard

Use the **Backup Keys to File** wizard to create backup data encryption license keys as files on SN.

This wizard includes the following windows:

- **Backup Keys to File** window
- **Confirm** window

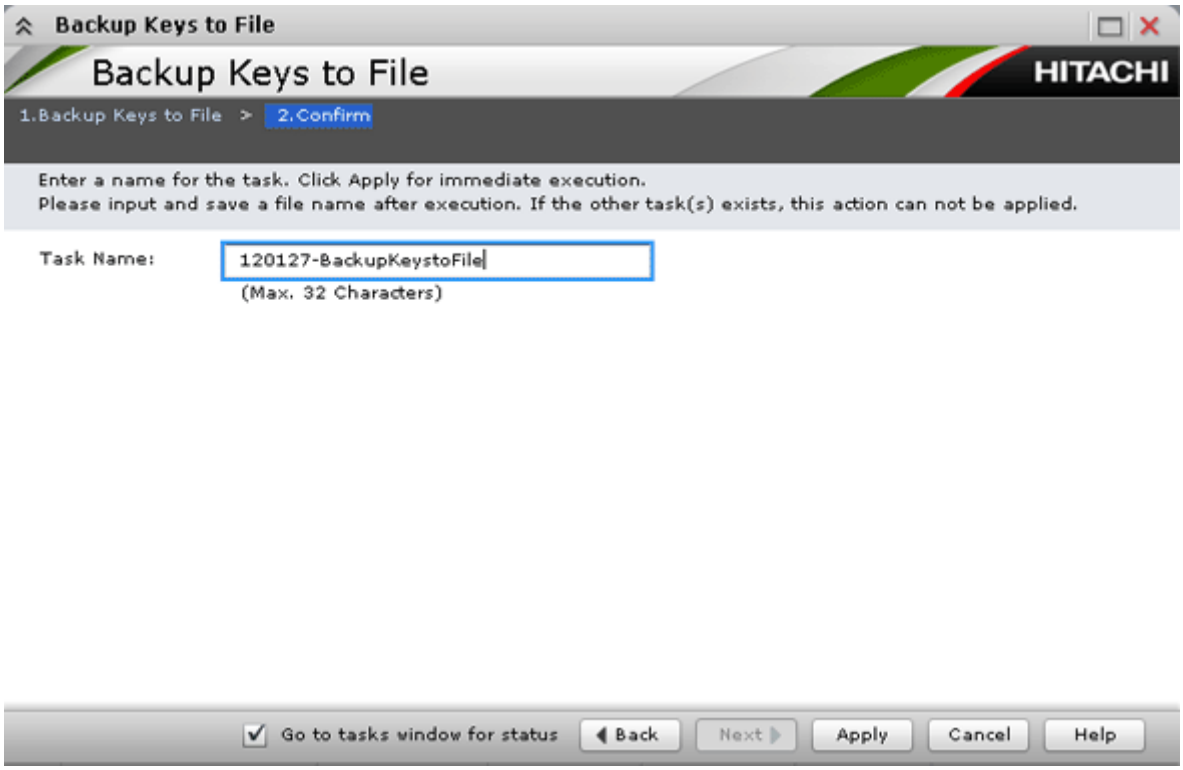
Backup Keys to File window



Item	Description
Password	The password for the backup data encryption license key. Character limits: 6 to 255 Valid characters: • Numbers (0 to 9) • Upper case (A-Z) • Lower case (a-z) • Symbols: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
Re-enter Password	Type the password again for confirmation.
Finish	Click to save the password for the backup data encryption license key.

Confirm window in the Backup Keys to File wizard

When you click **Apply** in the **Confirm** window, a confirmation message will appear. After you click **OK**, a window for saving the file for encryption keys will appear. Enter the backup file name with the extension of ".ekf" and save the file.



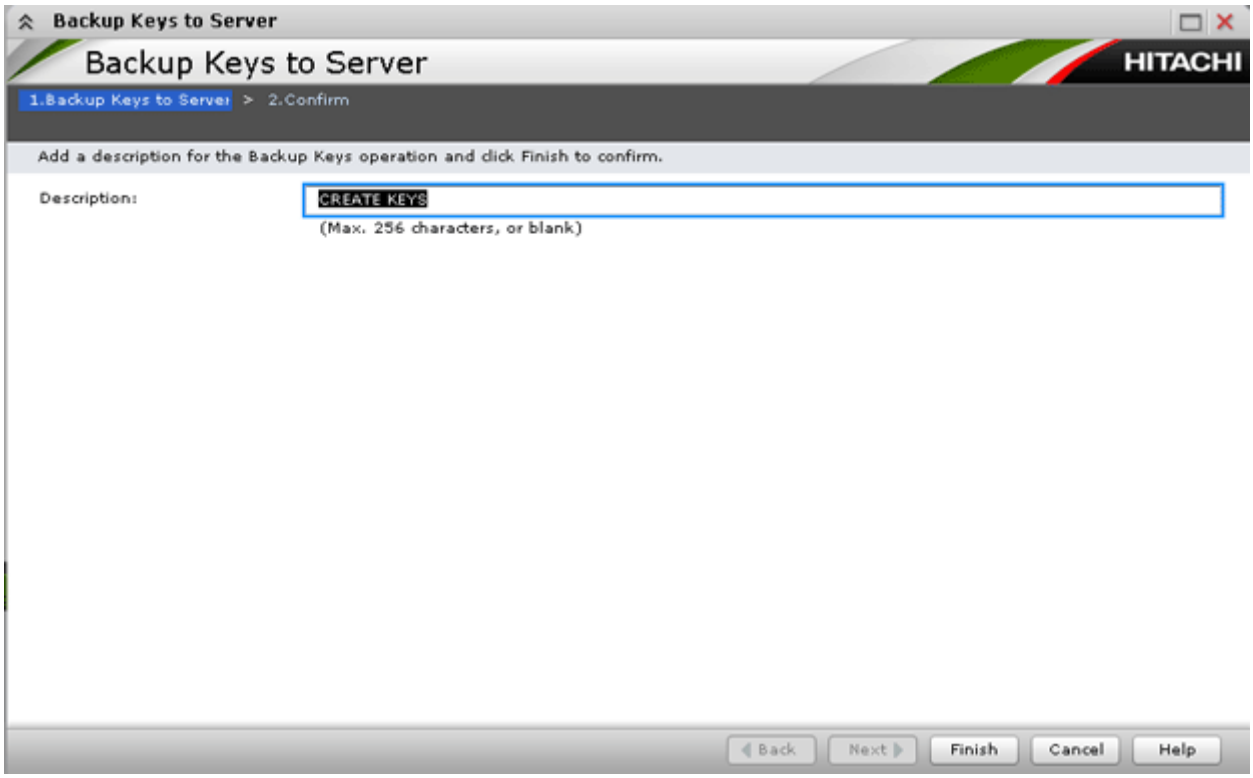
Backup Keys to Server wizard

Use the **Backup Keys to Server** wizard to backup data encryption license keys on the key management server.

This wizard includes the following windows:

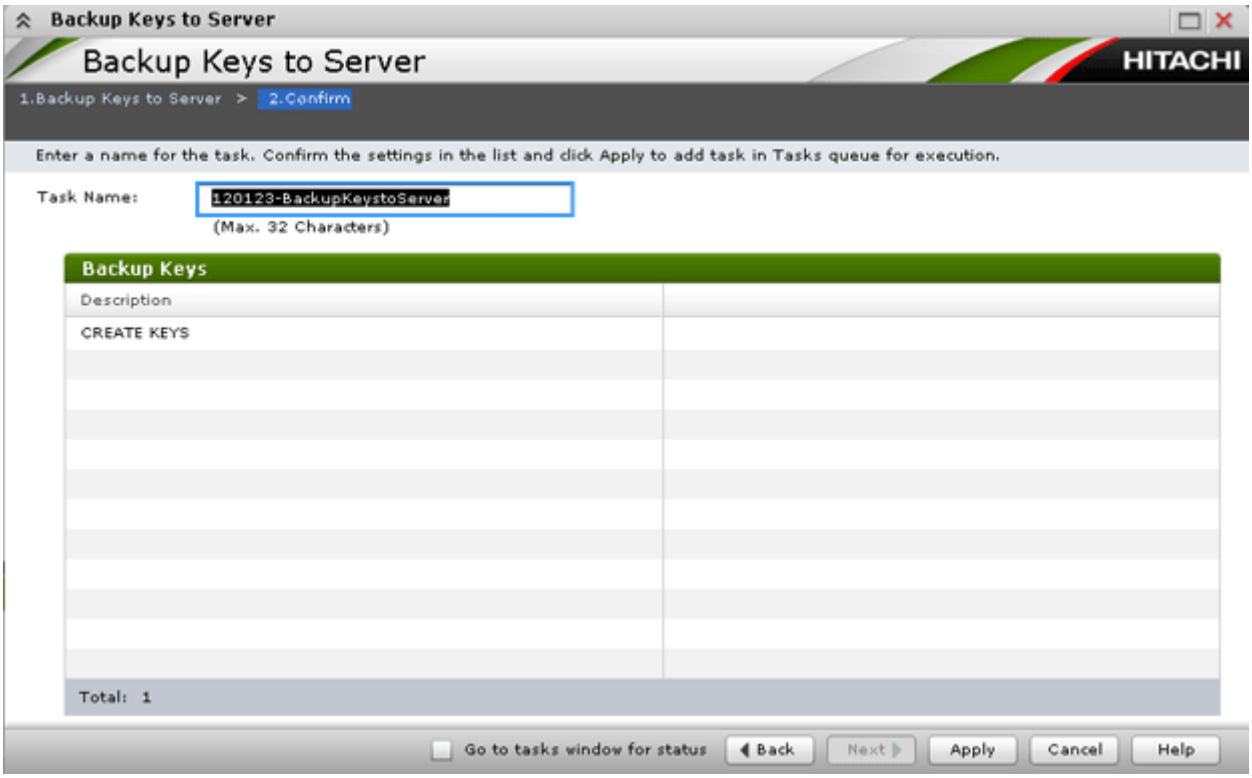
- **Backup Keys to Server** window
- **Confirm** window

Backup Keys to Server window



Item	Description
Description	Optionally, enter a description for the backup data encryption license key. Character limits: 256

Confirm window in the Backup Keys to Server wizard



Item	Description
Description	Shows the description for the backup data encryption license key.

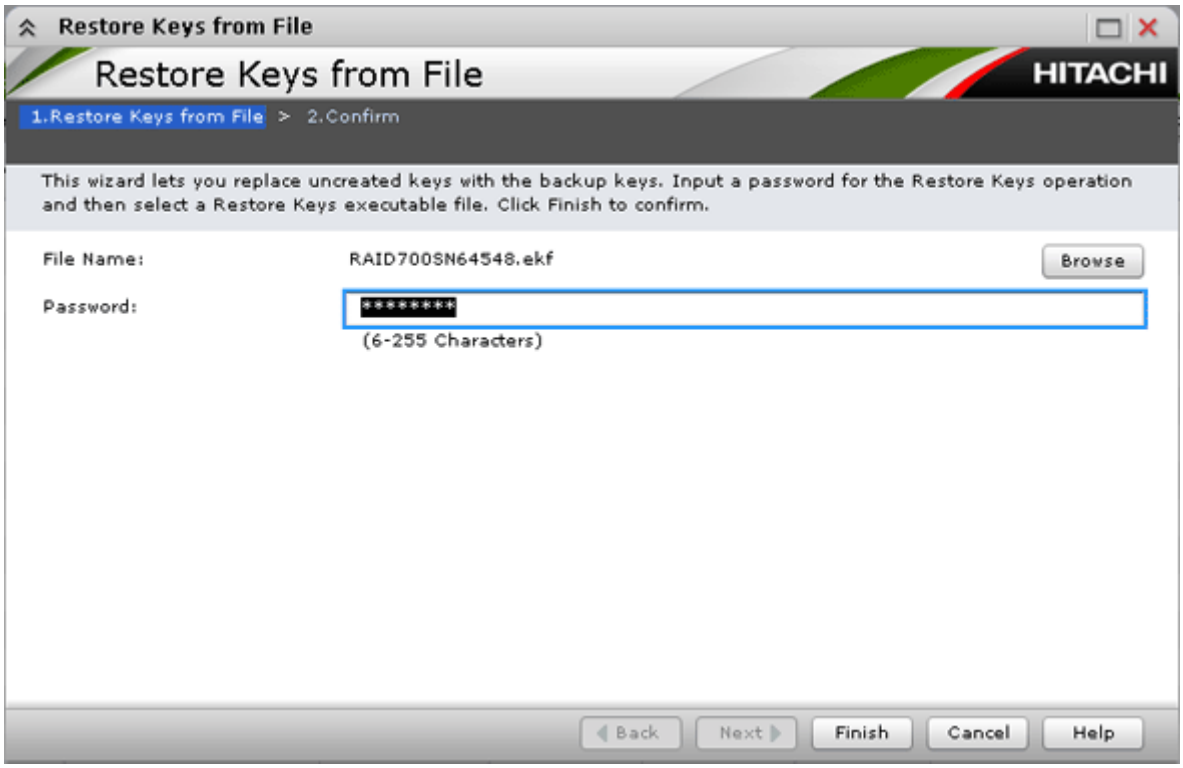
Restore Keys from file wizard

Use the **Restore Keys** wizard to restore data encryption license keys from a file you backed up on the SN computer.

This wizard includes the following windows:

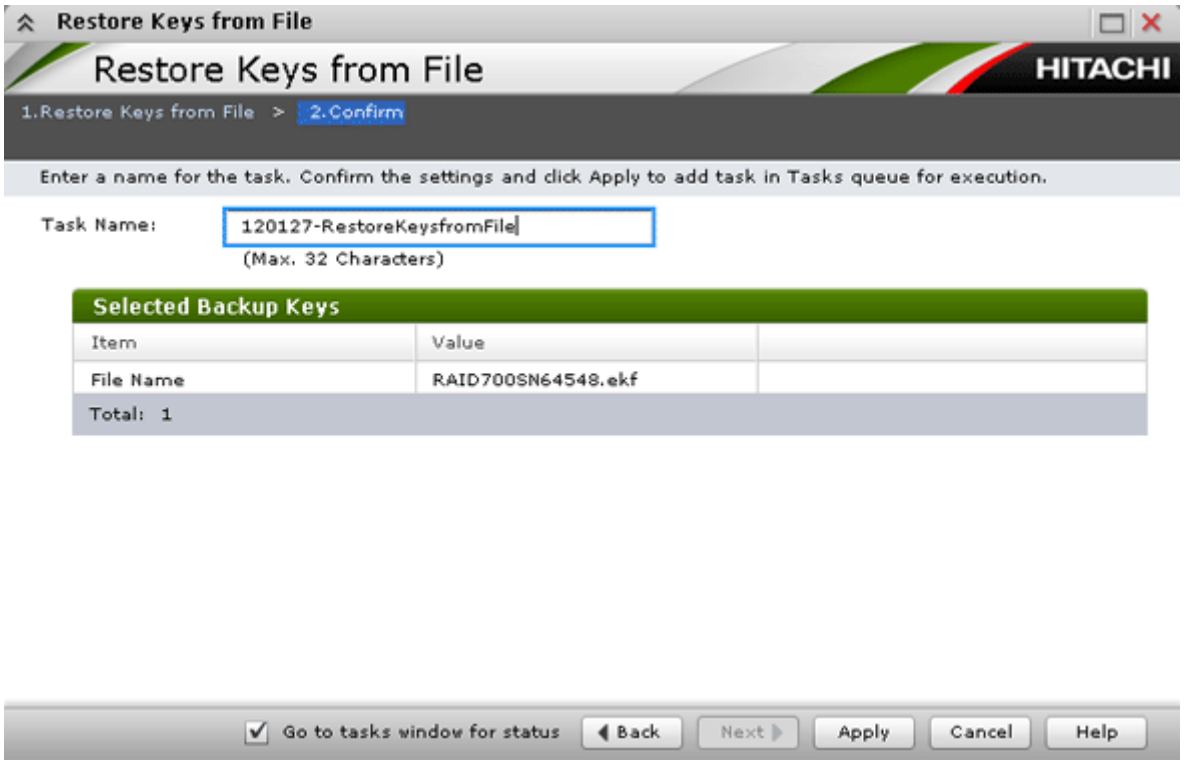
- **Restore Keys from File** window
- **Confirm** window

Restore Keys from File window



Item	Description
File Name	File name of the selected backup file.
Browse	Select the backup file (.ekf). The name of the selected file is shown for **File Name**.
Password	The password that you typed when you created the backup data encryption license key.

Confirm window in the Restore Keys wizard



Item	Description
Item	Item of the data encryption license key to restore.
Value	Value of the data encryption license key to restore.

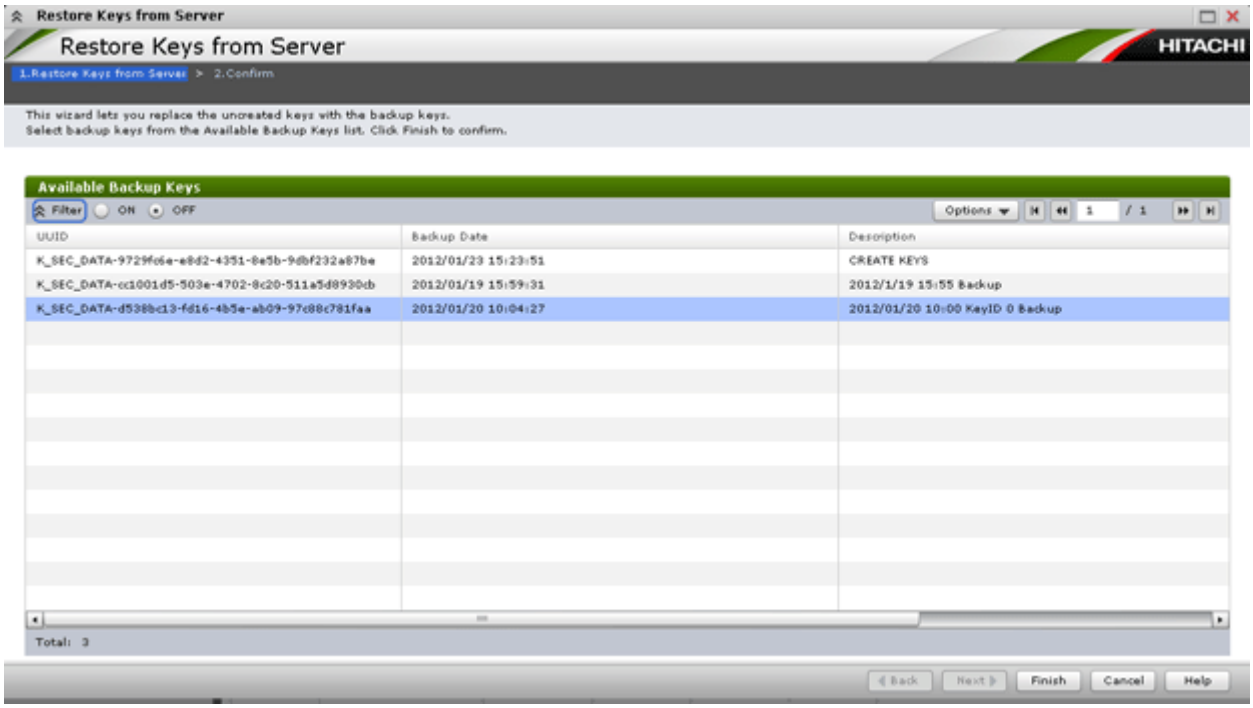
Restore Keys from Server wizard

Use the **Restore Keys from Server** wizard to restore data encryption license keys from the key management server.

This wizard includes the following windows:

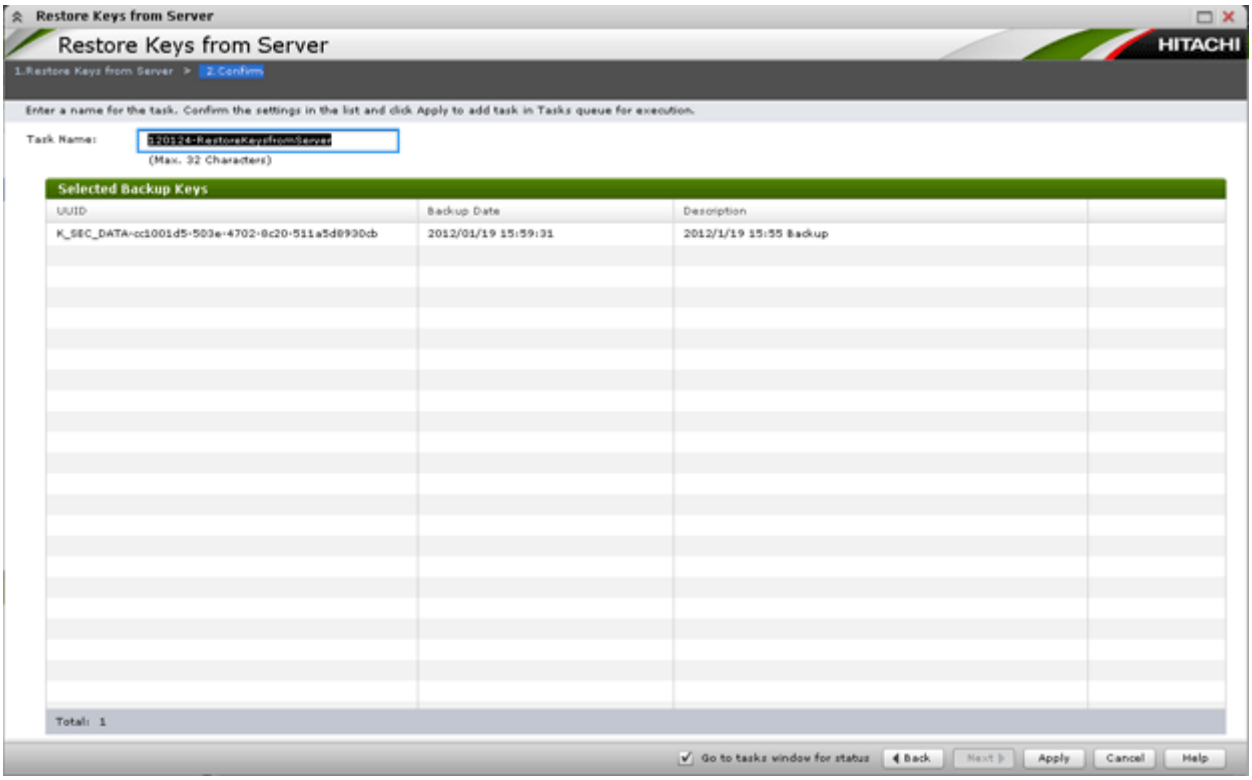
- **Restore Keys from Server** window
- **Confirm** window

Restore Keys from Server window



Item	Description
UUID	Shows the UUID of the data encryption license key that you backed up on the key management server.
Backup Date	Shows the time you backed up the data encryption license key on the key management server.
Description	Shows the description you typed when you backed up the data encryption license key on the key management server.

Confirm window in the Restore Keys from Server wizard



Item	Description
UUID	Shows the UUID of the data encryption license key you backed up on the key management server.
Backup Date	Shows the time when you backed up the data encryption license key on the key management server.
Description	Shows the description you typed when you backed up the data encryption license key on the key management server.

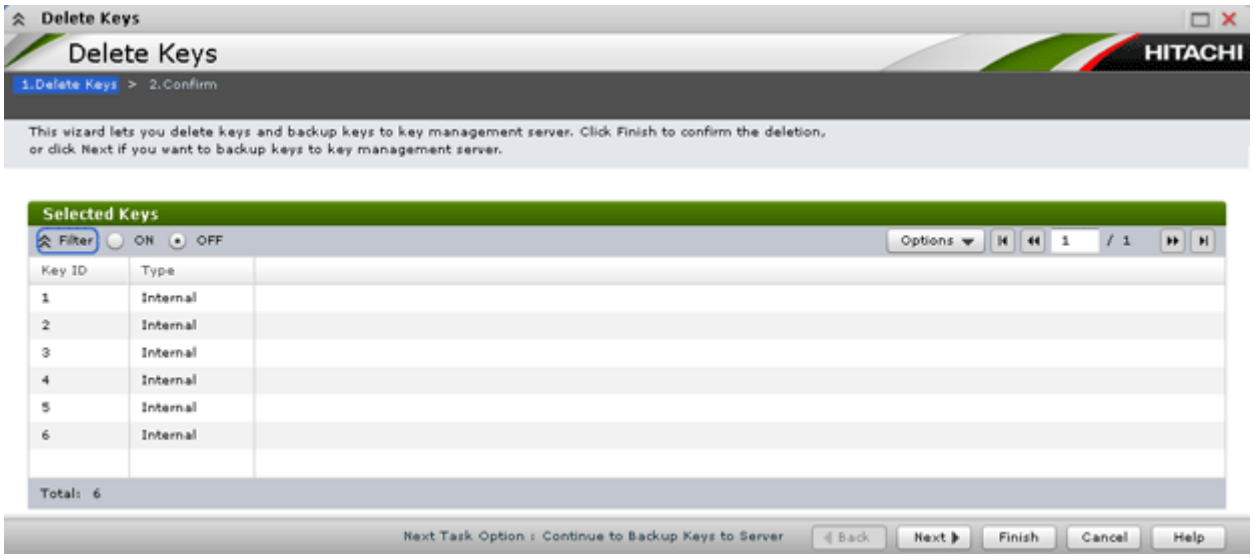
Delete Keys wizard

Use the **Delete Keys** wizard to delete keys and backup data encryption license keys in SN.

This wizard includes the following windows:

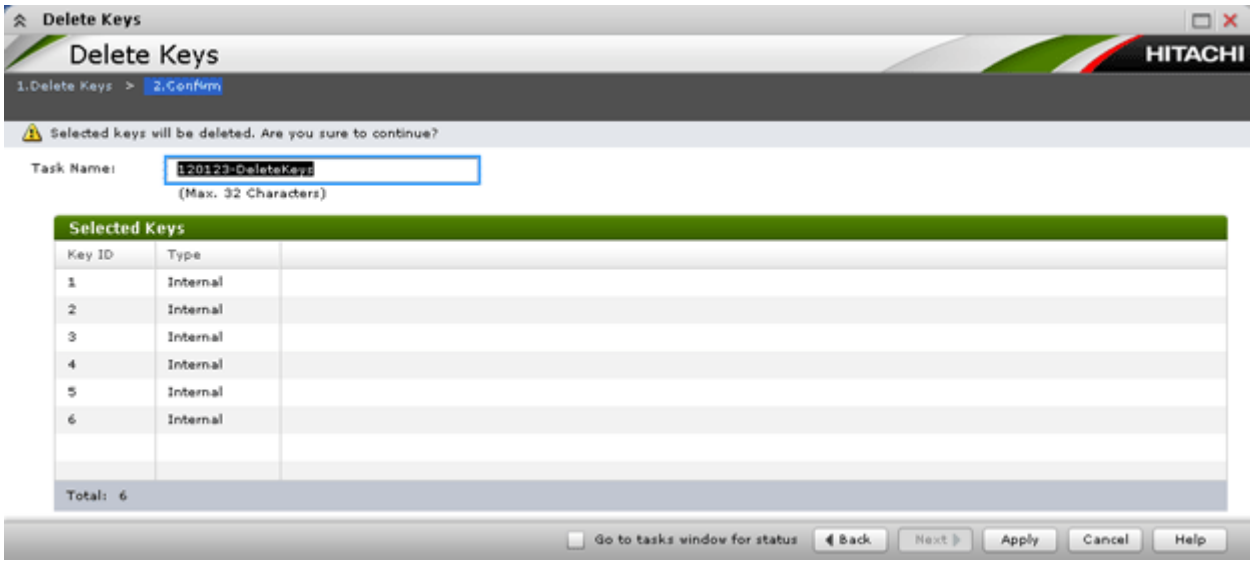
- **Delete Keys** window
- **Confirm** window

Delete Keys window



Item	Description
Key ID	IDs of data encryption license keys.
Type	Data encryption license key types. If the key ID is 0 to 31, the label **Internal** is displayed.

Confirm window in the Delete Keys wizard

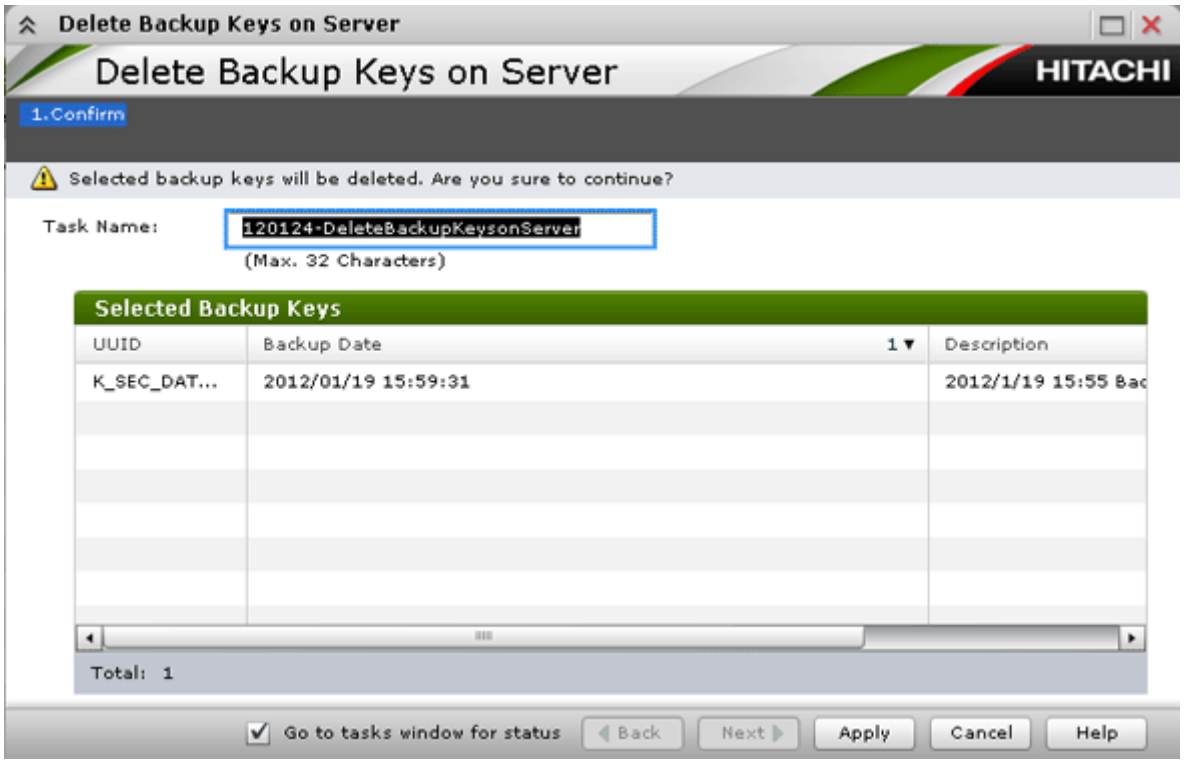


Item	Description
Key ID	The identifiers for the data encryption license keys.
Type	Data encryption license key types. If the key ID is 0 to 31, the label **Internal** is displayed.

Delete Backup Keys on Server window

Use the **Delete Backup Keys on Server** window to confirm the deletion of a backup key in SN.

This window includes the **Selected Backup Keys** table.

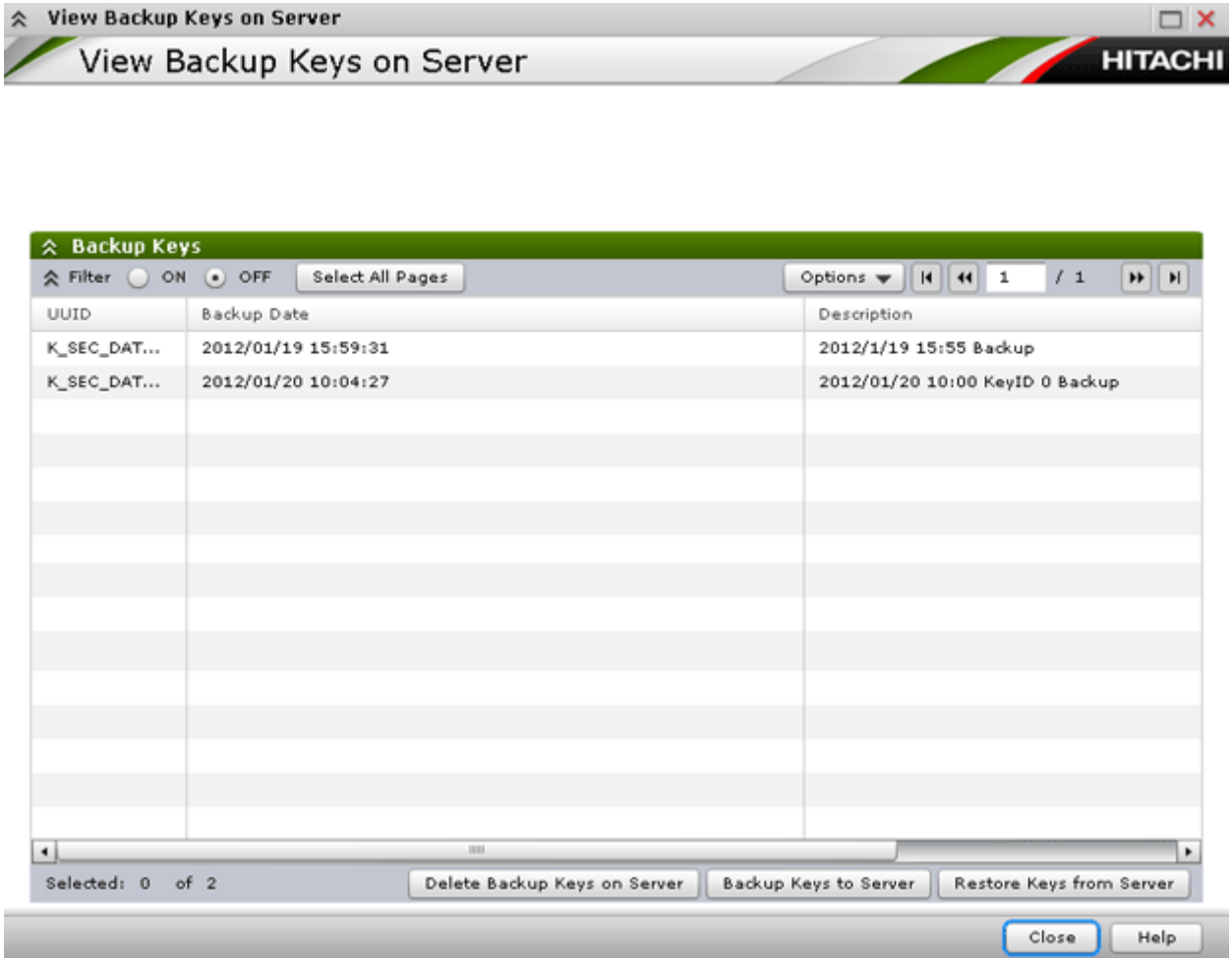


Item	Description
UUID	Shows the UUID of the data encryption license key you backed up on the key management server.
Backup Date	Shows the time when you backed up the data encryption license key on the key management server.
Description	Shows the description you typed when you backed up the data encryption license key on the key management server.

View Backup Keys on Server window

Use the **View Backup Keys on Server** window to view a list of the backup data encryption license keys on the server.

This window includes the **Backup Keys** table.



Backup Keys table

The **Backup Keys** table is shown on the **View Backup Keys on Server** window. This table lists the backup data encryption license keys.

Item	Description
UUID	Shows the UUID of the backup data encryption license key on the key management server.
Backup Date	Shows the time you backed up the data encryption license key on the key management server.
Description	Shows the description you typed when you backed up the data encryption license key on the key management server.
Delete Backup Keys on Server button	Opens the **Delete Backup Keys on Server** window.
Backup Keys to Server button	Open the **Backup Keys to Server** window.
Restore Keys from Server button	Opens the **Restore Keys from Server** window.

Edit Encryption wizard

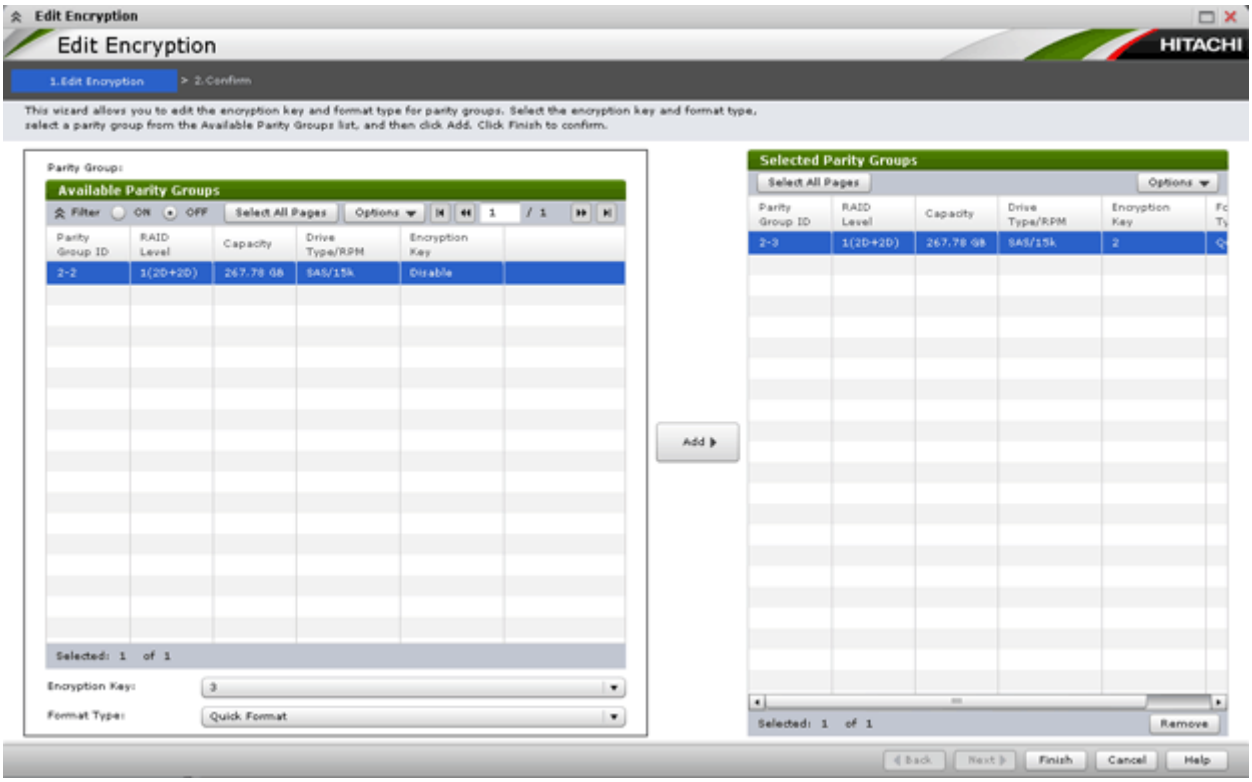
Use the **Edit Encryption** wizard to do the following:

- Enable data encryption on a parity group.
- Edit or associate the data encryption license key to the LDEV.
- Edit the format type for the parity group.

This wizard includes the following windows:

- **Edit Encryption** window
- **Confirm** window

Edit Encryption window



The **Edit Encryption** window includes the following items:

- **Available Parity Groups** table

  For more information about this table, see Available Parity Groups table on page A-24.

- **Selected Parity Groups** table

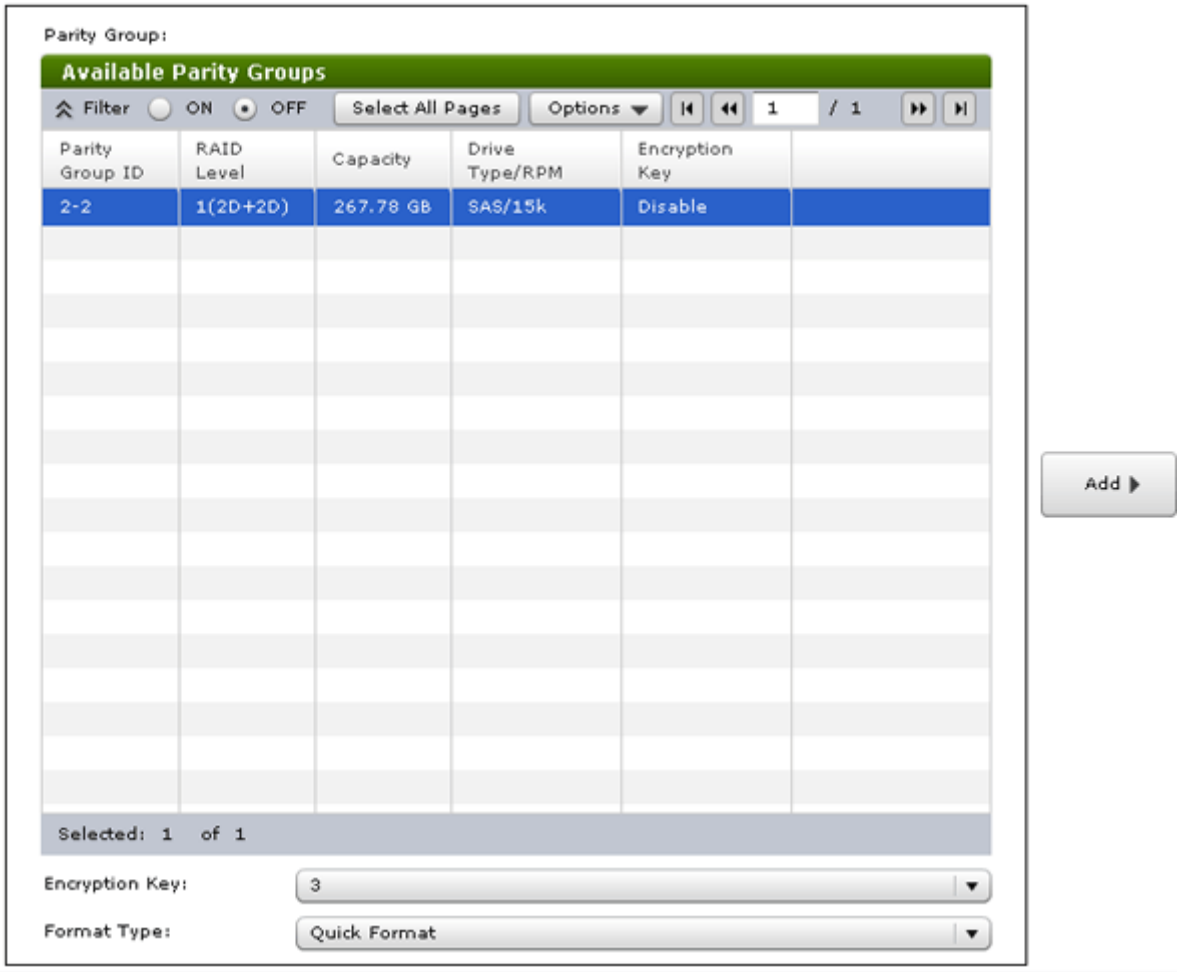
  For more information about this table, see Selected Parity Groups table on page A-25.

- **Encryption Key** drop-down list, from which you can select the key ID of which to enable data encryption or to disable data encryption at the parity-group level.
- **Format Type** drop-down list, from which you can select the parity group's format type.

- **Add** button, which you can click to move a selected parity group in the **Available Parity Groups** table to the **Selected Parity Groups** table.

Available Parity Groups table

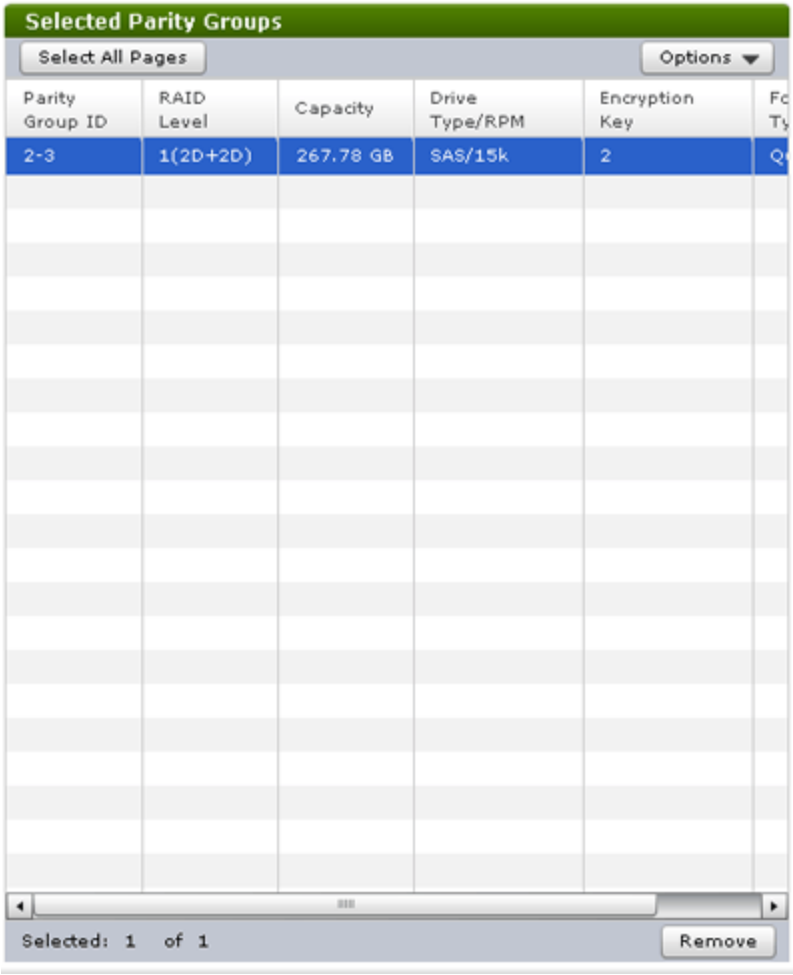
Use the **Available Parity Groups** table on the **Edit Encryption** window to view a list of the available parity groups.



Item	Description
Parity Group ID	Shows the parity group IDs.
RAID Level	Shows the RAID level of the parity group. For an interleaved parity group, the interleaved number appears after the RAID level. **Example:** 1(2D+2D)*2
Capacity	Shows the total capacity (unit) of the parity group.
Drive Type/RPM	Shows the hard disk drive types and RPM (rotation per minute) of the LDEV in the parity group.
Encryption Key	Shows the encryption setting for the parity group: • Key ID - enabled • Disable - no encryption

Selected Parity Groups table

Use the **Selected Parity Groups** table to remove the parity group from the list.



Item	Description
Parity Group ID	Shows parity group IDs.
RAID Level	Shows the RAID level of the parity group. For an interleaved parity group, the interleaved number appears after the RAID level. Example: 1(2D+2D)*2
Capacity	Shows the total capacity (unit) of the parity group.
Drive Type/RPM	Shows the hard disk drive types and RPM (rotation per minute) of the LDEV in the parity group.
Encryption Key	Encryption setting for the parity group: • Key ID - enabled • Disable - no encryption

Item	Description
Format Type	Shows the format types of the parity group. The format type shows **No Format** regardless of the status of format type you selected from the **Format Type** list.
Remove	Removes parity groups from the **Selected Parity Groups** table.

Confirm window in the Edit Encryption wizard

Use the **Confirm** window to confirm the changes to the data encryption license key and to view a list of the selected parity groups related to the data encryption license key.

Selected Parity Groups table

Use the **Selected Parity Groups** table to view a list of the selected parity groups related to the data encryption license key.

Item	Description
Parity Group ID	Shows parity group identifier.
RAID Level	Shows the RAID level of the parity group. For an interleaved parity group, the interleaved number appears after the RAID level. **Example:** 1(2D+2D)*2
Capacity	Shows the total capacity of the parity group.
Drive Type/RPM	Shows the hard disk drive types and RPM (rotation per minute) of the LDEV in the parity group.
Encryption Key	Encryption setting for the parity group: • Key ID - enabled • Disable - no encryption
Format Type	Shows the format types of the parity group.

Glossary

This glossary defines the special terms used in this document. Click the letter links below to navigate.

A

AES

Advanced Encryption Standard

C

CU

control unit

E

ECB

Electronic Code Book

emulation type

Indicates the type of LDEV: mainframe emulation types include 3390-x and 3380-x; open-system emulation types include OPEN-V and OPEN-3.

Encryption Administrator

User role in Storage Navigator with permission to perform DAR operations. Compare with *Storage Administrator*.

encryption key

The data encryption license key is used to encrypt and decrypt data on the VSP storage system.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

external volume

A volume whose data is stored on drives that are physically outside of the RAID storage system. Universal Volume Manager is used to manage external storage. Compare with *internal volume*.

I

internal volume

A volume whose data is stored on drives that are physically within the RAID storage system. Compare with *external volume*.

L

logical device (LDEV)

An individual logical device (on multiple drives in a RAID configuration) in the storage system. An LDEV may or may not contain any data and may or may not be defined to any hosts. Each LDEV has a unique identifier, or address, within the storage system composed of the LDKC number, CU number, and LDEV number.

An LDEV formatted for use by mainframe hosts is called a logical volume image (LVI). An LDEV formatted for use by open-system hosts is called a logical unit (LU).

logical unit (LU)

An LDEV that is configured for use by open-systems hosts (for example, OPEN-V).

logical volume image (LVI)

An LDEV that is configured for use by mainframe hosts (for example, 3390-3).

P

parity group

A redundant array of independent drives (RAID) that have the same capacity and are treated as one group for data storage and recovery. A parity group contains both user data and parity information, which allows the user data to be accessed in the event that one or more of the drives within the parity group are not available. The RAID level of a parity group determines the number of data drives and parity drives and how the data is "striped" across the drives.

primary volume (P-VOL)

The volume in a copy pair that contains the original data to be replicated. The data on the P-VOL is duplicated synchronously or asynchronously on the secondary volume(s) (S-VOL).

The following Hitachi products use the term P-VOL: Copy-on-Write Snapshot, ShadowImage, ShadowImage for Mainframe, TrueCopy, Universal Replicator, Universal Replicator for Mainframe, and High Availability Manager.

See also *secondary volume.*

P-VOL

See *primary volume.*

S

service information message (SIM)

Message generated by the RAID storage system when an error or service requirement is detected. SIMs are reported to hosts and displayed on Storage Navigator.

secondary volume (S-VOL)

The volume in a copy pair that is the copy of the original data on the primary volume. The following Hitachi products use the term "secondary volume": ShadowImage, ShadowImage for Mainframe, TrueCopy, Universal Replicator, Universal Replicator for Mainframe, and High Availability Manager.

See also *primary volume.*

source volume (S-VOL)

In the previous version of the Storage Navigator GUI, this is the volume containing the original data that is duplicated on the target volume (T-VOL). The following Hitachi products use the term source volume: ShadowImage for Mainframe, Dataset Replication, Compatible FlashCopy® V2.

In the latest version of the GUI, "source volume" and "S-VOL" are replaced with "primary volume".

Storage Administrator

User role in Storage Navigator with permission to perform data encryption operations. Compare with *Encryption Administrator*.

S-VOL

See *secondary volume* or *source volume (S-VOL)*.

T

target volume (T-VOL)

In the previous version of the Storage Navigator GUI, this is the copy of the original data on the source volume (S-VOL). The following Hitachi

products use the term target volume: ShadowImage for Mainframe, Dataset Replication, and Compatible FlashCopy® V2.

In the latest version of the GUI, "target volume" and "T-VOL" are replaced with "primary volume".

See also *source volume (S-VOL)*.

T-VOL

See *target volume (T-VOL).*

U

USP V/VM

Hitachi Universal Storage Platform V/VM

V

VSP

Hitachi Virtual Storage Platform

X

XRC

Extended Remote Copy

XTS

XEX-based Tweaked CodeBook mode (TCB) with CipherText Stealing (CTS)

Z

zero data

The number 0 (zero). A zero-formatting operation is a formatting operation that writes the number 0 (zero) to the entire disk area.

Index

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, California 95050-2639
U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

Europe, Middle East, and Africa
+44 (0)1753 618000
info.emea@hds.com

Asia Pacific
+852 3189 7900
hds.marketing.apac@hds.com

Hitachi Data Systems

MK-90RD7015-10