HITACHI
Inspire the Next

Encryption License Key User Guide

Hitachi Virtual Storage Platform G200, G400, G600, G800
Hitachi Virtual Storage Platform F400, F600, F800

FASTFIND LINKS

Hitachi Data Systems

MK-94HM8029-02

November, 2015

© 2015 Hitachi, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written permission of Hitachi, Ltd.

Hitachi, Ltd., reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. This document contains the most current information available at the time of publication. When new or revised information becomes available, this entire document will be updated and distributed to all registered users.

Some of the features described in this document might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Data Systems Corporation at https://support.hds.com/en_us/contact-us.html.

Notice: Hitachi, Ltd., products and services can be ordered only under the terms and conditions of the applicable Hitachi Data Systems Corporation agreements. The use of Hitachi, Ltd., products is governed by the terms of your agreements with Hitachi Data Systems Corporation.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

Hitachi is a registered trademark of Hitachi, Ltd., in the United States and other countries. Hitachi Data Systems is a registered trademark and service mark of Hitachi, Ltd., in the United States and other countries.

Archivas, Essential NAS Platform, HiCommand, Hi-Track, ShadowImage, Tagmaserve, Tagmasoft, Tagmasolve, Tagmastore, TrueCopy, Universal Star Network, and Universal Storage Platform are registered trademarks of Hitachi Data Systems Corporation.

AIX, AS/400, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, ESCON, FICON, FlashCopy, IBM, Lotus, MVS, OS/390, RS/6000, S/390, System z9, System z10, Tivoli, VM/ESA, z/OS, z9, z10, zSeries, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

Contents

Preface

This guide describes and provides instructions for Encryption License Key (DAR), a feature of Device Manager - Storage Navigator (HDvM - SN) for the Hitachi Virtual Storage Platform G400, G600, G800 and Hitachi Virtual Storage Platform F400, F600, F800 storage systems. You configure Encryption License Key within HDvM - SN for the Hitachi Virtual Storage Platform G400, G600, G800 and Hitachi Virtual Storage Platform F400, F600, F800 storage systems.

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 G400, G600, G800 and Hitachi Virtual Storage Platform F400, F600, F800 systems.

This document is for users who:

- Have a background in data processing and RAID storage systems
- Are familiar with the Hitachi Virtual Storage Platform G400, G600, G800 and Hitachi Virtual Storage Platform F400, F600, F800 systems and Device Manager - Storage Navigator
- Are familiar with the use of encryption in a storage environment

Product version

This document revision applies to firmware 83-02-0*x* or later.

Release notes

The release notes for this product are available on Hitachi Data Systems Support Connect: https://support.hds.com/en_us/contact-us.html. Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document.

Changes in this revision

- Added a table column in section Problems and solutions on page 5-2
- Added support for Hitachi Virtual Storage Platform F400, F600, F800 storage systems

Referenced documents

Hitachi Virtual Storage Platform G400, G600, G800 and Hitachi Virtual Storage Platform F400, F600, F800 documents:

- *Hitachi Command Suite User Guide*, MK-90HC172
- *Hitachi Virtual Storage Platform Audit Log User Guide*, MK-94HM8028.
- *Hitachi Virtual Storage Platform G400, G600 Hardware Reference Guide*, MK-94HM8022
- *Provisioning Guide for Hitachi Virtual Storage Platform Gx00 and Fx00 Models*, MK-94HM8014
- *Hitachi Virtual Storage Platform G800 Hardware Reference Guide*, MK-94HM8026

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-file target-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.
[ ] 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

Product documentation is available on Hitachi Data Systems Support Connect: https://support.hds.com/en_us/documents.html. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

Hitachi Data Systems Support Connect is the destination for technical support of products and solutions sold by Hitachi Data Systems. To contact technical support, log on to Hitachi Data Systems Support Connect for contact information: https://support.hds.com/en_us/contact-us.html.

Hitachi Data Systems Community is a new global online community for HDS customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hds.com, register, and complete your profile.

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 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.

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.
	Emulation type	OPEN-V
	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 Device Manager - Storage Navigator (HDvM - SN) to create the data encryption license key.
	Deleting data encryption license keys	Use HDvM - SN to delete data encryption license keys. However, you cannot delete data encryption license keys that are allocated to implemented drives.
	Unit of encryption/decryption	Parity group. Data encryption licence keys are used per HDD.
	Scope of data encryption license keys	1,024 data encryption license keys per storage system. You can create 1,024 Free keys or DEK keys. You can create 4 CEK keys and one KEK key. Therefore, the total number of data encryption license keys will be 1,029 at the

Item		Specification
		maximum when including CEK keys and KEK keys.
	Attribute of encryption license keys	The following attributes will be set for the encryption license keys: **Free**: The unused key before allocating the encryption license key. **DEK**: The encryption license key. The key for the encryption of the stored data. **CEK**: The certificate encryption key. The key for the encryption of the certificate and the key for the encryption of DEK per HDD. **KEK**: Key Encryption Key. The key for the encryption of the CEK.
	Backup/Restore functionality	Redundant (primary and secondary) backup/restore copies.

When are data encryption license keys needed

After you have completed the encryption environmental settings, you will need data encryption license keys to work on the following operations:

- Increasing drives
  A Free key is needed for each drive to allocate a DEK key.
- Replacing drives
  A Free key is needed for each drive to change a DEK key.
- Increasing or replacing disk boards.
  3 Free keys are needed for each disk board to create 2 CEK keys and a key to register CEK keys.
- Updating CEK keys
  2 Free keys for each disk board (4 free keys per storage system) are needed to change CEK keys.
  If a problem occurs in the middle of an operation, extra keys might be needed to recover from it.

Primary and secondary data encryption license keys

VSP G400, G600, G800 and VSP F400, F600, F800 systems use the Encryption License Key feature to set up the data encryption license keys to encrypt and decrypt data.

Note: VSP G200 cannot use the Encryption License Key feature.

You can use the Encryption License Key feature to back up data encryption license keys. Your storage system automatically creates a primary backup of the data encryption license key, and stores this backup in cache flash memory.

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.

It is recommended that you back up each key or group of keys immediately after you create them. You are responsible for storing the secondary backup securely. Schedule regular backups for all keys at the same time one time every week to ensure data availability.

In addition, it is recommended that you back up each key after you perform any of the following operations:

- Creating encryption license keys.
- Increasing, decreasing, or replacing drives.
- Increasing, decreasing, or replacing disk boards.
- Updating CEK keys.
- Updating KEK keys.

For more information about backing up secondary data encryption license keys, see Workflow for backing up secondary data encryption license keys on page 4-3.

Caution: You must add storing secondary backup encryption license keys securely as part of your corporate security policy.
If the primary backup key becomes unavailable and no secondary backup key exists, the system cannot decrypt encrypted data.

KMIP key management server support

Using VSP G400, G600, G800 or VSP F400, F600, F800, you can create backup and restore data encryption license keys on a key management server that supports Key Management Interoperability Protocol (KMIP).

There are a limited number of keys you can back up on the key management server. Therefore, it is recommended that you delete unnecessary keys when possible.

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 4-5.

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.

For more information about enabling data encryption, see Enabling data encryption at the parity group-level on page 4-8.

Data encryption on existing data workflow

Use the following process to encrypt existing data:

1. A new parity group is created.
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 data migration services, call the Support Center.

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.

For more information about disabling encryption, see Workflow for disabling data encryption at the parity-group level on page 4-9.

Change data encryption license key workflow

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

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.

When you exchange a drive, data encryption license keys that are allocated to that drive will be deleted; new data encryption license keys will be allocated when a new drive is implemented.

Audit logging of encryption events

The audit Log feature of VSP G400, G600, G800 and VSP F400, F600, F800 systems 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 Virtual Storage Platform Audit Log User Guide*.

Interoperability with other software applications

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

Software application	Interoperability notes
ShadowImage and TrueCopy	Encrypt the P-VOL and S-VOLs to ensure data security.
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.
Dynamic Provisioning, Dynamic Tiering, and active flash	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 is also required.

2

Encryption License Key Installation

This chapter discusses how to install the DAR 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 Command Suite User Guide*.

System requirements

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

Item	Requirement
VSP G400, G600, G800 and VSP F400, F600, F800	• DKCMAIN firmware 83-01-0x and later.
SVP	• Encryption License Key software license. • Security Administrator (View & Modify) role to enable or disable data encryption and to back up or restore keys • SVP must always be activated if you want to protect key encryption keys at the key management server.
DNS server	To connect to the key management server by specifying the host name instead of IP address, you need the DNS server settings. For DNS server configuration, configure the IP address of the DNS server in SVP.
Host platforms	All open-systems platforms are supported.
Data volumes	Volumes for open systems (OPEN-V emulation type) are supported.
Disk board	A disk board that enables the data encrypting.

Enabling the Encryption License Key feature

To enable the DAR feature please refer *Hitachi Command Suite User Guide* for more details.

Disabling the Encryption License Key feature

You can disable the DAR feature in Device Manager - Storage Navigator.

Caution: Perform Step 1 and 2 before you delete the software license key.

1. 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 4-9.
2. Initialize the connection settings to the key management server. For more information about initializing the connection settings to the key management server, see Initialize the connection settings to the key management server on page 4-18.
3. Delete the software license key.

3

Key Management Server Connections

You can use an optional key management server with VSP G400, G600, G800 and VSP F400, F600, F800. This chapter provides information on how to set up the key management server.

- ☐ Key management server requirements
- ☐ Edit encryption environmental 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 6.4.1 or Thales keyAuthority 4.0.2
- Certificates:
  - Root certificate of the key management server (X.509)
  - Client certificate in PKCS#12 format
- Configuration: Two clustered servers, if you want to protect key encryption keys.

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 Uploading the root and client certificate on page 3-4.

Root certificate on the key management server

If you use SafeNet KeySecure or Thales keyAuthority 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 documentation. For more information about Thales keyAuthority, see the Thales keyAuthority 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 3-3.

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.
   - Public key file.
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 3-3.
4. Upload the root and client certificates to the SVP.
   For more information uploading the root and client certificate, see Uploading the root and client certificate on page 3-4.

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. Type the client certificate password.
   For more information about the client certificate password, see Client certificate password on page 3-2.

Uploading the root and client certificate

As part of configuring the connection settings to the key management server, you'll need to upload the root certificate and the client certificate.

Prerequisites

- Required role: Security Administrator (View & Modify)

1. In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.

   In Device Manager - Storage Navigator:
   a. Display the **Device Manager - Storage Navigator** main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. Click **Edit Encryption Environmental Settings**.
3. Upload the certificates in the **Edit Encryption Environmental Settings** window.

Edit encryption environmental settings workflow

To use a key management server, you must configure the connection and network settings. You can also set the encryption settings such as disabling the local key generations and storing key encryption key to DKC.

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.

Caution: Encryption keys backed up on the key management server are managed with the client certificate. If the client certificate is lost, and the SVP is replaced due to a failure, you cannot restore the encryption keys that were backed up before the replacement.
When the connection settings are backed up 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. Refer to your corporate security policy for procedures related to backups.

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 3-3 and Uploading the root and client certificate 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. Confirm that you can connect to the key management server.
4. Check with the key management server administrator, then save a back up copy of the client certificate.
5. Back up the connection settings to the key management server.

   For more information on how to save the connection settings, see the Storage Systems Settings section of the *Hitachi Command Suite User Guide*.

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.

For more information, see Settings in the Edit Encryption Environmental Settings window on page 3-6 and Backing up keys to a key management server on page 4-5.

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.

Prerequisites

- Required role: Security Administrator (View & Modify)

1. In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.

   In Device Manager - Storage Navigator:
   a. Display the **Device Manager - Storage Navigator** main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. Select the **Encryption Keys** tab.
3. Click **Edit Encryption Environmental Settings**.
4. In the **Edit Encryption Environmental Settings** window, select **Enable** or **Disable** on the **Key Management Server**.
5. If you connect to the Key Management Server, specify the primary server and the secondary server.
6. If the key management server is already in use, select **Check** to test the connection. Error messages appear if the server configuration test fails.
7. Create an encryption key:
   - To generate an encryption key on the key management server, select **Generate Encryption Keys on Key Management Server**. To store the encryption key on the key management server, select **Protect**

the Key Encryption Key on the Key Management Server, then **I Agree**.

Caution: If you have selected **Protect the Key Encryption Key on the Key Management Server** in **Generate Encryption Keys on Key Management Server**, the storage system will try to get encryption keys backed up on the key management server once the storage system is turned on. Therefore, it is recommended that you confirm that the SVP is connected to the key management server properly before turning the storage system on.

- To generate an encryption key on the key management server without creating an encryption key in the storage system, select **Disable Local Key Generation**. Confirm the Warning that displays and select **I Agree**.

Caution: When you select the **Disable local key generation** and **I Agree** check-boxes in **Generate Encryption Keys on Key Management Server** and finished the settings, you cannot undo this action.

8. To backup data encryption license keys to the key management server, click **Next**. Otherwise, click **Finish**.
9. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.

   If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.

   Click **Apply**.

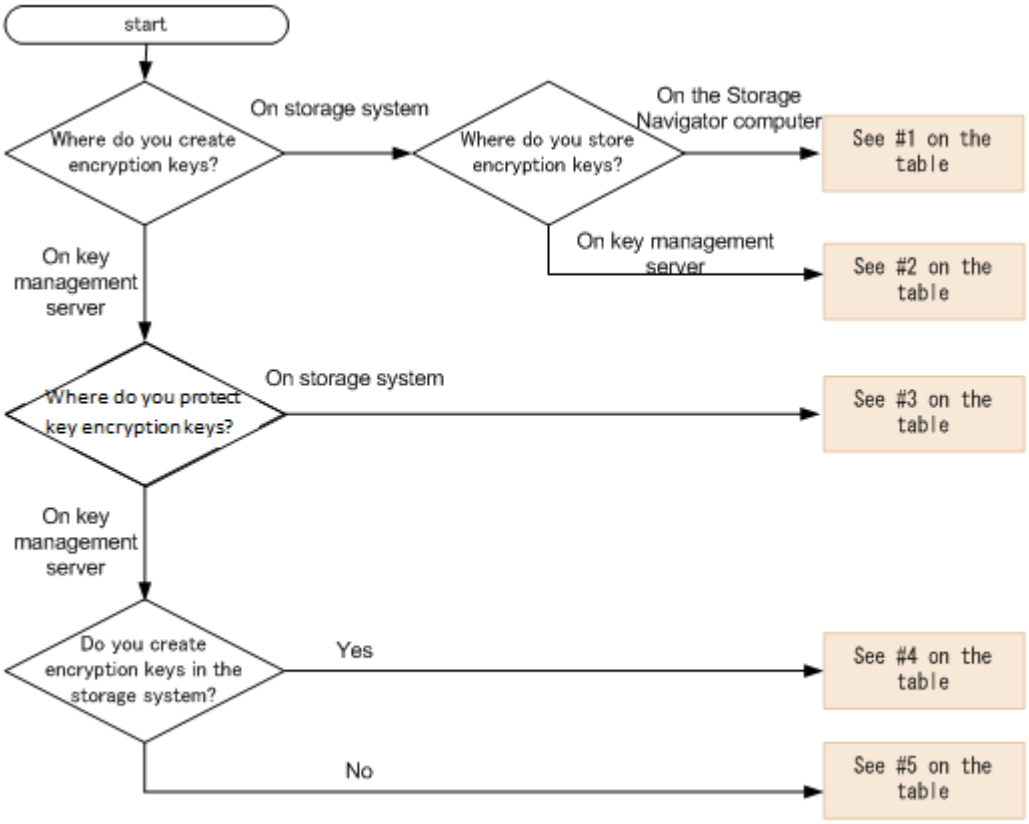
The connection to the key management server is set up.

Related topics

- Edit Encryption Environmental Settings window on page A-5

Settings in the Edit Encryption Environmental Settings window

To manage encryption keys properly, refer to the following flow chart and table and choose settings for the Edit Encryption Environmental Settings window accordingly.



	Settings in the Edit Encryption Environmental Settings window			
	Key Management Server	**Generate Encryption Keys on Key Management Server**	**Protect the Key Encryption Key at the Key Management Server**	**Disable local key generation**
#1	Select Disable	Do not check	Do not check	Do not check
#2	Select Enable	Do not check	Do not check	Do not check
#3	Select Enable	Check	Do not check	Do not check
#4	Select Enable	Check	Check	Do not check
#5	Select Enable	Check	Check	Check

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 your VSP G400, G600, G800 or VSP F400, F600, F800 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 4-3.

Creating data encryption license keys

If you need to change a data encryption license key, create a new data encryption license key.

When you configure encryption environmental settings on the **Edit Encryption Environmental Settings** window for the first time, 1,018 Free keys or DEK keys are created. (This differs from the configuration. 1,018 keys are created if maximum disk adapters are installed). After that, you can create 1,024 Free keys or DEK keys. You can create up to 1,024 encryption keys per storage system.

When you configure encryption environmental settings on the **Edit Encryption Environmental Settings** window again, Free Keys are not created, and DEK keys and CEK keys are not updated. Keys that were created previously will be used.

Encryption keys are commonly created in the storage system. However, when the key management server is in use, and **Generate Encryption Keys on Key Management Server** is checked in the **Edit Encryption Environmental Settings** window, encryption keys will be created on the key management server, and used in the storage system.

After creating data encryption license keys, it is recommended that you back up each key.

Prerequisites

- Required role: Security Administrator (View & Modify)

1. In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.

   In Device Manager - Storage Navigator:
   a. Display the **Device Manager - Storage Navigator** main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.

2. Select the **Encryption Keys** tab.
3. From the **Settings** menu, select **Security > Encryption Keys > Key Generation**.
4. In the **Create Keys** window, specify the number of encryption keys you want to create. The encryption keys with the attribute of **Free** will be set. The key IDs will be automatically assigned.
5. To backup data encryption license keys to the key management server, click **Next**. Otherwise, click **Finish**.
6. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.

   If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.

   Click **Apply**.

The new data encryption license key is created.

Related topics

- Create Keys window on page A-10

Workflow for backing up secondary data encryption license keys

VSP G400, G600, G800 and VSP F400, F600, F800 systems automatically create a primary backup of the data encryption license key. You can also back up a secondary data encryption license.

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

The backup of the encryption key is performed to the existing DEK keys and CEK keys at the same time.

In addition, it is recommended that you back up each key after you perform any of the following operations:

- Creating encryption license keys.
- Increasing, decreasing, or replacing drives.
- Increasing, decreasing, or replacing disk boards.
- Updating CEK keys.
- Updating KEK keys.

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

1. Confirm that HDvM - SN is not processing other tasks. You cannot back up the keys while HDvM - 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 HDvM - SN computer.

For more information about backing up secondary data encryption license keys as files, see Backing up keys as a file on page 4-4.

- 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 4-5.

Backing up keys as a file

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

Prerequisites

- Required role: Security Administrator (View & Modify)

1. In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.

   In Device Manager - Storage Navigator:
   a. Display the **Device Manager - Storage Navigator** main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. Select 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, confirm the settings, and enter your task name in **Task Name**.

   If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.

   Click **Apply**.
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 HDvM - SN computer.

Related topics

- Encryption Keys window on page A-3
- Backup Keys to File window on page A-14

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.

There are a limited number of keys you can back up on the key management server. Therefore, it is recommended that you delete unnecessary keys when possible.

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.

Prerequisites

- Required role: Security Administrator (View & Modify)

1. In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.

   In Device Manager - Storage Navigator:
   a. Display the **Device Manager - Storage Navigator** main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. In the **Encryption Keys** window, click the **Encryption Keys** tab.
3. Open the **Backup Keys to Server** window using one of the two following methods:
   - Use the **Encryption** window to open the **Backup Keys to Server** window.
   - Use the **View Backup Keys on Server** window to open the **Backup Keys to Server** window.
4. (Optional) In the **Backup Keys to Server** window, for **Description**, type a description and then click **Finish**.
5. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.

   If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.

   Click **Apply**.

A secondary backup data encryption license keys is saved.

Related topics

- Encryption Keys window on page A-3
- Backup Keys to Server window on page A-16

Opening the Backup Keys to Server window using the Encryption window

Prerequisites

- Required role: Security Administrator (View & Modify)

1. In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.

   In Device Manager - Storage Navigator:
   a. Display the **Device Manager - Storage Navigator** main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. Complete one of the following in the **Encryption Keys** window:
   - Click **Settings > Security > Encryption Keys > Backup Keys to Server**.
   - Click **Backup Keys > To Server**.

Opening the Backup Keys to Server window using the View Backup Keys on Server window

Prerequisites

- Required role: Security Administrator (View & Modify)

1. In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.

   In Device Manager - Storage Navigator:
   a. Display the **Device Manager - Storage Navigator** main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. Complete one of the following in the **Encryption Keys** window:
   - Click **Settings > Security > Encryption Keys > View Backup Keys on Server**.
   - Click **View Backup Keys on Server**.
3. Click **Backup Keys to Server**.

Editing the password policy

You can set the minimum number of characters required for passwords.

Prerequisites

- Required role: Security Administrator (View & Modify)

1. In Hitachi Command Suite:
   a. On the **Administration** tab, click **Security**, and then **Password**.
   b. In the **Password** window, click **Edit Settings**.
   c. In the **Password Policy** window, set the minimum number of characters.

   In Device Manager - Storage Navigator:
   a. Display the **Device Manager - Storage Navigator** main window.
   b. From the **Settings** menu, select **Security > Encryption Key > Edit Password Policy (Backup Encryption Keys)**.
   c. In the **Edit Password Policy (Backup Encryption Keys)** window, set the minimum number of characters.
2. Click **Finish**.
3. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.
   If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.
   Click **Apply**.

Related topics

- Edit Password Policy (Backup Encryption Keys) window on page A-11

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 4-3.
2. Block the LDEVs at the parity-group level, using a file on the HDvM - SN computer.
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 4-8.
4. Format the LDEVs at the parity-group level.

For more information about formatting LDEVs in the parity group, see Workflow for enabling data encryption on parity groups on page 4-7.

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. The Storage Administrator (provisioning) role is also required if you want to format volumes at the same time.

Prerequisites

- Required role: Security Administrator (View & Modify)
- Required role to format volumes: Storage Administrator (Provisioning)

1. In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Parity Groups**.

   In Device Manager - Storage Navigator:
   a. Display the **Device Manager - Storage Navigator** main window.
   b. Select **Storage Systems** in **Explorer**, and select **Parity Groups**.
2. In the **Parity Groups** table, select a specific parity group on which you want to enable encryption and then click **Edit Encryption**.
   In the tree that is shown, **Internal** or **External** is displayed.
3. To select an internal LDEV, select **Internal**. Otherwise, click the **Parity Groups** tab.
4. 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.

5. 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**, select **Enable** 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.
   When you click **Add**, **Format Type** becomes inactive and you cannot select the format type. If you want to change the format type, delete all

parity groups in the **Selected Parity Groups** list and then select the format type again.

You do not need to format volumes when there is no volume selected in the parity group. Therefore, the format type in the **Selected Parity Groups** list becomes a hyphen (-) regardless of the status of the format type.

6. Click **Finish**.
7. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.

   If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.

   Click **Apply**.
8. In the message that appears, click **OK**.

   Data encryption is enabled on the parity group.

Related topics

- Edit Encryption window on page A-24

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 4-3.
2. Block the LDEV at the parity-group level.
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 4-9.
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 4-11.

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. The Storage Administrator (provisioning) role is also required if you want to format volumes at the same time.

Prerequisites

- Required role: Security Administrator (View & Modify)
- Required role to format volumes: Storage Administrator (Provisioning)

1. In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Parity Groups**.
   c. In the table that is shown, **Internal** or **External** are displayed.

   In Device Manager - Storage Navigator:
   a. Display the **Device Manager - Storage Navigator** main window.
   b. Select **Storage Systems** in **Explorer**, and select **Parity Groups**.
   c. In the table that is shown, **Internal** or **External** are displayed.
2. To select an internal LDEV, select **Internal**. Otherwise, select the **Parity Groups** tab.
3. On the **Parity Groups** 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 **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**, 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: When you click **Add**, **Format Type** becomes inactive and you cannot select the format type. If you want to change the format type, delete all parity groups in the **Selected Parity Groups** list and then select the format type again. You do not need to format volumes when there is no volume in the selected parity group. Therefore, the format type in the **Selected Parity Groups** list becomes "-" (a hyphen) regardless of the status of **Format Type**.

5. In the **Edit Encryption** window, click **Finish**.
6. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.

   If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.

   Click **Apply**.
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.

Related topics

- Edit Encryption window on page A-24

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.

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.

Caution: When you restore the data encryption license key, always restore the latest key. If a data encryption license key is updated after a secondary backup is performed, and the restored key is not the latest key, drives and disk boards will be blocked and will not be able to read data.

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

1. Block the LDEVs associated to the encrypted parity group by blocking the LDEV using a file on the HDvM - SN computer.

   For more information about blocking LDEVs using a file, see the *Hitachi Command Suite User Guide*.
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 HDvM - SN computer.

     For more information about \ 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.

Restoring keys from a file

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

Prerequisites

- Required role: Security Administrator (View & Modify)

1. In Hitachi Command Suite:

a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
b. Expand the target storage system, and then select **Encryption Keys**.

In Device Manager - Storage Navigator:

a. Display the **Device Manager - Storage Navigator** main window.
b. Select **Administration** in **Explorer**, and select **Encryption Keys**.

2. On the **Encryption Keys** tab, click **Restore Keys > From File**.
3. In the **Restore Keys from File** window, click **Browse** and then click **OK**.
4. In the **Open** dialog box, select the backup file and click **Open**.
5. 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.
6. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.
   If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.
   Click **Apply**.

The data encryption license key is restored.

Related topics

- Restore Keys from File window on page A-17

Restoring keys from a key management server

Restore a data encryption license key from the key management server. You can restore up to 1,028 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.

Prerequisites

- Required role: Security Administrator (View & Modify)

1. In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.

b. Expand the target storage system, and then select **Encryption Keys**.

In Device Manager - Storage Navigator:

a. Display the **Device Manager - Storage Navigator** main window.

b. Select **Administration** in **Explorer**, and select **Encryption Keys**.

2. On the **Encryption Keys** tab, click **Restore Keys > From Server**.
3. In the **Restore Keys from Server** window, select the data encryption license key you want to restore.
4. Click **Finish**.
5. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.

   If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.

   Click **Apply**.

The backup data encryption license key is restored.

Related topics

- Restore Keys from Server window on page A-19

Workflow for deleting data encryption license keys

Delete a data encryption license key from a file on the HDvM - 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 4-3.
2. Ensure the key is not allocated to the parity group.

   See the Encryption Keys window on page A-3 and check the key allocation.
3. Delete the data encryption license key using one of the following methods:

   - Delete the key from a file on the HDvM - SN computer.

     For more information about deleting keys from the HDvM - SN computer, see Deleting data encryption license keys on page 4-14.
   - 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 HDvM - SN computer.

You can only delete encryption keys with a **Free** attribute can be deleted. Encryption keys with the other attributes cannot be deleted.

Prerequisites

- Required role: Security Administrator (View & Modify)

1. In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.

   In Device Manager - Storage Navigator:
   a. Display the **Device Manager - Storage Navigator** main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. On the **Encryption Keys** tab, click **More Actions > Delete Keys**.
3. To backup encryption keys to the key management server, click **Next**. To back up encryption keys to the server, see Backing up keys to a key management server on page 4-5.
4. In the **Delete Keys** window, click **Finish**.
5. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.
   If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.
   Click **Apply**.
6. In the message that appears asking whether to apply the setting to the storage system, click **OK**.

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

Related topics

- Delete Keys window on page A-20

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.

Prerequisites

- Required role: Security Administrator (View & Modify)

1. In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.

   In Device Manager - Storage Navigator:
   a. Display the **Device Manager - Storage Navigator** main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. On the **Encryption Keys** tab, click **View Backup Keys on Server**.
3. 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 click **Delete Backup Keys on Server**.
4. 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.
5. 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.

Related topics

- View Backup Keys on Server window on page A-22
- Delete Backup Keys on Server window on page A-21

Viewing encryption keys backed up on the key management server

You can view encryption keys that are backed up on the key management server.

Prerequisites

- Required role: Security Administrator (View & Modify)

1. In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.

   In Device Manager - Storage Navigator:
   a. Display the **Device Manager - Storage Navigator** main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.

2. On the **Encryption Keys** tab, click **View Backup Keys on Server** to view the backup keys on the key management server.

Related topics

- Encryption Keys window on page A-3
- View Backup Keys on Server window on page A-22

Exporting encryption license key table information

You can output encryption license key table information.

Prerequisites

- Required role: Security Administrator (View & Modify)

1. In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.

   In Device Manager - Storage Navigator:
   a. Display the **Device Manager - Storage Navigator** main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. On the **Encryption Keys** tab, select the key ID for the data encryption license key information you want to output from the **Encryption Keys** table.
3. Click **More Actions > Export**.
4. When the **Ready to Download** message appears, click **OK**.
5. Select the location to save the export file.
   The default filename format is `YYMMDD-Encryption_KeysExport.tsv`. If you change the filename, keep the `.tsv` extension.
6. Click **Save**.
   The encryption license key table information file is saved on your computer.

Rekeying key encryption keys

If you create key encryption keys on the key management server, use the following procedure to rekey key encryption keys.

After rekeying key encryption license keys, it is recommended that you back up each key.

Use the following procedure to rekey key encryption keys.

Prerequisites

- Required role: Security Administrator (View & Modify)

1. In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.

   In Device Manager - Storage Navigator:
   a. Display the **Device Manager - Storage Navigator** main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. In the **Encryption Keys** window, select the **Encryption Keys** tab.
3. Select **Settings > Security > Encryption Keys > Rekey Key Encryption Keys** or select **More Actions > Rekey Key Encryption Keys**.
4. Confirm the settings and enter the task name in the **Task Name** field.
5. Click **Apply** in the **Confirm** window to save the settings to the system.
   If you selected the **Go to tasks window for status** check box, the **Task** window will appear.

Related topics

- Rekey Key Encryption Key window on page A-29

Rekeying certificate encryption keys

If you change certificate encryption keys, use the following procedure to rekey the keys.

After rekeying certificate encryption license keys, it is recommended that you back up each key.

Prerequisites

- Required role: Security Administrator (View & Modify)

1. In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.

   In Device Manager - Storage Navigator:
   a. Display the **Device Manager - Storage Navigator** main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. In the **Encryption Keys** window, select the **Encryption Keys** tab.
3. Select **Settings > Security > Encryption Keys > Rekey Certificate Encryption Keys** or select **More Actions > Rekey Certificate Encryption Keys**.
4. Confirm the settings and enter the task name in the **Task Name** field.

5. Click **Apply** in the **Confirm** window to save the settings to the system.

Related topics

- Rekey Certificate Encryption Keys window on page A-28

Retrying Key Encryption Key Acquisition

If you acquire the key encryption keys from the key management server when the storage device starts, retry key encryption key acquisition.

Prerequisites

- Required role: Security Administrator (View & Modify)

1. In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.

   In Device Manager - Storage Navigator:
   a. Display the **Device Manager - Storage Navigator** main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. In the **Encryption Keys** window, select the **Encryption Keys** tab.
3. Select **Settings > Security > Encryption Keys > Retry Key Encryption Key Acquisition** or select **More Actions > Retry Key Encryption Key Acquisition**.
4. Confirm the settings and enter the task name in the **Task Name** field.
5. Click **Apply** in the **Confirm** window to save the settings to the system.
   If you selected the **Go to tasks window for status** check box, the **Task** window will appear.

You need to restore the disk board and blocked drives or volumes after retrying key encryption key acquisition. Contact the Hitachi Data Systems Support Center to restore the disk board or blocked drives or volumes.

Related topics

- Retry Key Encryption Key Acquisition window on page A-29

Initialize the connection settings to the key management server

Disable data encryption at the parity-group level before initializing the connection settings to the key management server.

To initialize the connection settings to the key management server, use this procedure.

Prerequisites

- Required role: Security Administrator (View & Modify)

1. In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.

   In Device Manager - Storage Navigator:
   a. Display the **Device Manager - Storage Navigator** main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. On the **Encryption Keys** tab, select **Edit Encryption Environmental Settings**.
3. In the **Edit Encryption Environmental Settings** window, select **Initialize Encryption Environmental Settings**.
4. Select **Finish** to display the **Confirm** window.
5. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.
   If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.
   Click **Apply**.

Related topics

- Edit Encryption Environmental Settings window on page A-5

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 audit log of VSP G400, G600, G800 or VSP F400, F600, F800 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 Virtual Storage Platform Audit Log User Guide*.

Problems and solutions

For troubleshooting information about your storage system, see the reference guide for your storage system.

For troubleshooting information about HDvM - SN, see the *Hitachi Command Suite 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. • If you backup and restore data encryption license keys with a key management server, the number of keys which you can back up on the key management server is not exceeded. • If you backup and restore data encryption license keys with a key management server, a time-out has not occurred due to the increase in the number of keys on the key management server. • The latest key is restored (the key will not be updated after a secondary backup has been performed).
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.

Problem	Action
	• If you have backed up and restored data encryption license keys with a key management server, that the connection to the key management server is available.
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.
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
The **Edit Encryption** wizard operation failed, but the status of encryption (enable or disable) has changed.	The change of the status succeeds, but the format of the volume fails. Confirm the message, remove the error, and format volumes again.
The storage system failed to get encryption keys backed up on the key management server and all volumes are blocked when the storage system is turned on. The SIM code 661000 is returned.	Complete the following tasks: • Make sure SVP is activated. • Restore the connection to the key management server. • Retry key encryption key acquisition. • Contact the the Hitachi Data Systems Support Center to restore the disk board and blocked drives or blocked volumes.
Server configuration test succeeded, but the following error was displayed: **10126-105022 The connected key management server does not support the required functions.**	A required function for the setting of the key management server is not supported with the connected key management server. See Key management server requirements on page 3-2 and update the software of the key management server to the latest version.

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 HDvM - SN.
- The HDvM - SN configuration information (use the FD Dump Tool).
- The service information messages (SIMs), including reference codes and severity levels, that HDvM - SN displays.

The the Hitachi Data Systems Support Center support staff is available 24 hours a day, seven days a week. If you need technical support, log on to HDS Support Connect for contact information: https://support.hds.com/en_us/contact-us.html

A

Encryption License Key GUI Reference

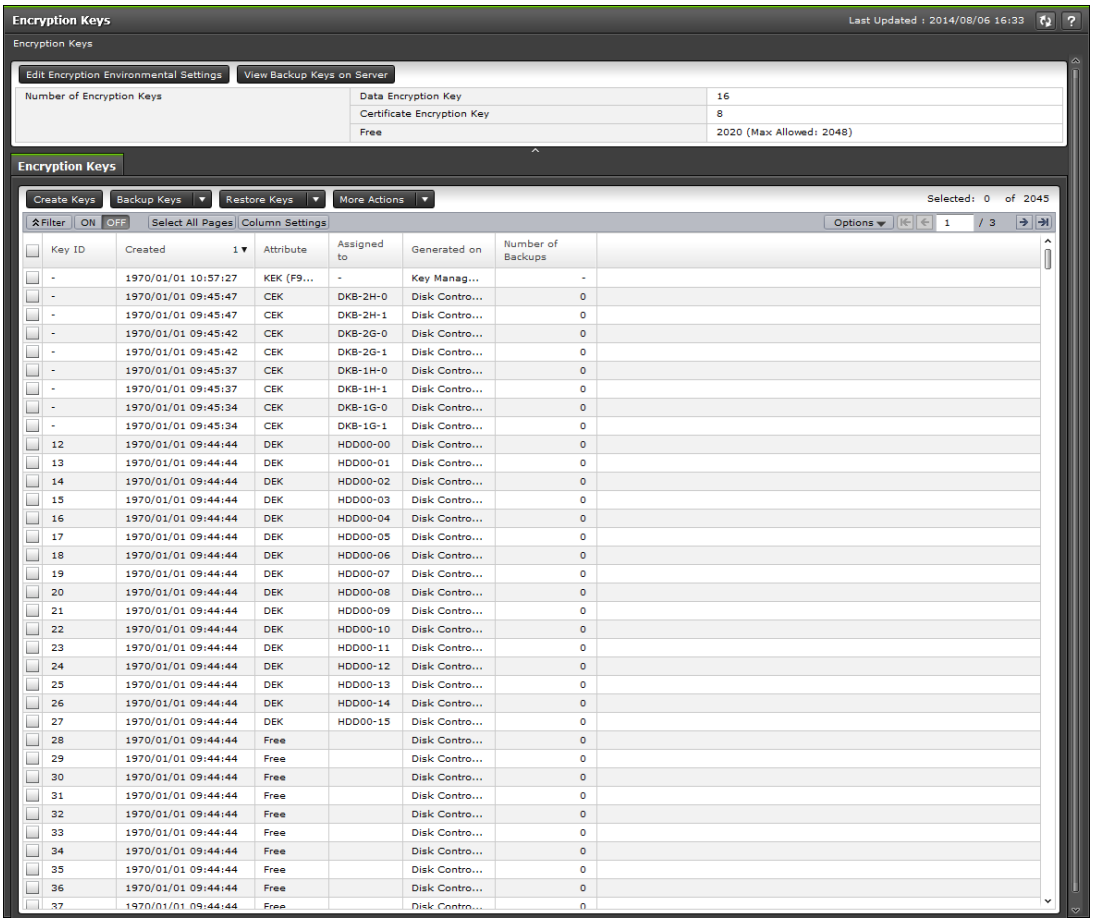
This chapter includes descriptions of encryption-related HDvM - SN windows and dialog boxes for the DAR feature.

For more information about other HDvM - SN windows and dialog boxes, see the *Hitachi Command Suite User Guide*.

- Rekey Key Encryption Key window
- Retry Key Encryption Key Acquisition window

Encryption Keys window

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



- Summary on page A-3
- Encryption Keys tab on page A-4

Summary

Use the **Summary** 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: • **Data Encryption Key**: Number of data encryption keys. • **Certificate Encryption Key**: Number of certificate encryption keys. • **Free**: Number of free keys (Number of keys that can be created). The number of key encryption keys are not included.

Item	Description
Edit Encryption Environmental Settings	Shows the **Edit Encryption Environmental Settings** window.
View Backup Keys on Server	Shows 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.

The **Encryption Keys** tab displays only the created encryption keys and in descending order of the **Last Update Date**. It also displays **Perform the Edit Environmental Settings** in the center of the window when the initialized settings are not performed, and displays **Perform the Retry Key Encryption Key Acquisition** in the center of the window when the Key Encryption Key Acquisition operation has failed.

Item	Description
Key ID	IDs of data encryption license keys. A hyphen (-) is displayed when the encryption key is CEK or KEK.
Created	The date and time the data encryption license key was created or was last updated.
Attribute	Displays the attribute (CEK, DEK, KEK or Free) of the encryption key. When KEK for the key management server is displayed, the format of "KEK (UUID)" is displayed with UUID.
Assigned to	The resource to which the encryption key is assigned is displayed. When the attribute is KEK, a hyphen (-) is displayed.
Generated on	The path in which the encryption key is created.
Number of Backups	The number of times that a backup of a data encryption license key is created. When the attribute is KEK, a hyphen (-) is displayed.
Create Keys	Click to open the **Create Keys** window.
Backup Keys	Select **To File** to open the **Backup Keys to File** window. Select **To Server** to open the **Backup Keys to Server** window.
Restore Keys	Select **From File** to open the **Restore Keys from File** window. Select **From Server** to open the **Restore Keys from Server** window.
More Actions	Select **Rekey Certificate Encryption Keys** to display the **Rekey Certificate Encryption Keys** window.

Item	Description
	Select **Rekey Key Encryption Keys** to display the **Rekey Key Encryption Keys** window. Select **Delete Keys** from the list to delete a selected data encryption license key. Select **Retry Key Encryption Key Acquisition** to display the **Retry Key Encryption Key Acquisition** window. Select **Export** from the list to open the window for outputting table information.

Related topics

- Creating data encryption license keys on page 4-2
- Backing up keys as a file on page 4-4
- Backing up keys to a key management server on page 4-5
- Restoring keys from a file on page 4-11
- Restoring keys from a key management server on page 4-12
- Deleting data encryption license keys on page 4-14
- Deleting backup data encryption license keys from the server on page 4-14
- Viewing encryption keys backed up on the key management server on page 4-15

Edit Encryption Environmental Settings wizard

Use the **Edit Encryption Environmental Settings** wizard to edit the encryption environmental settings.

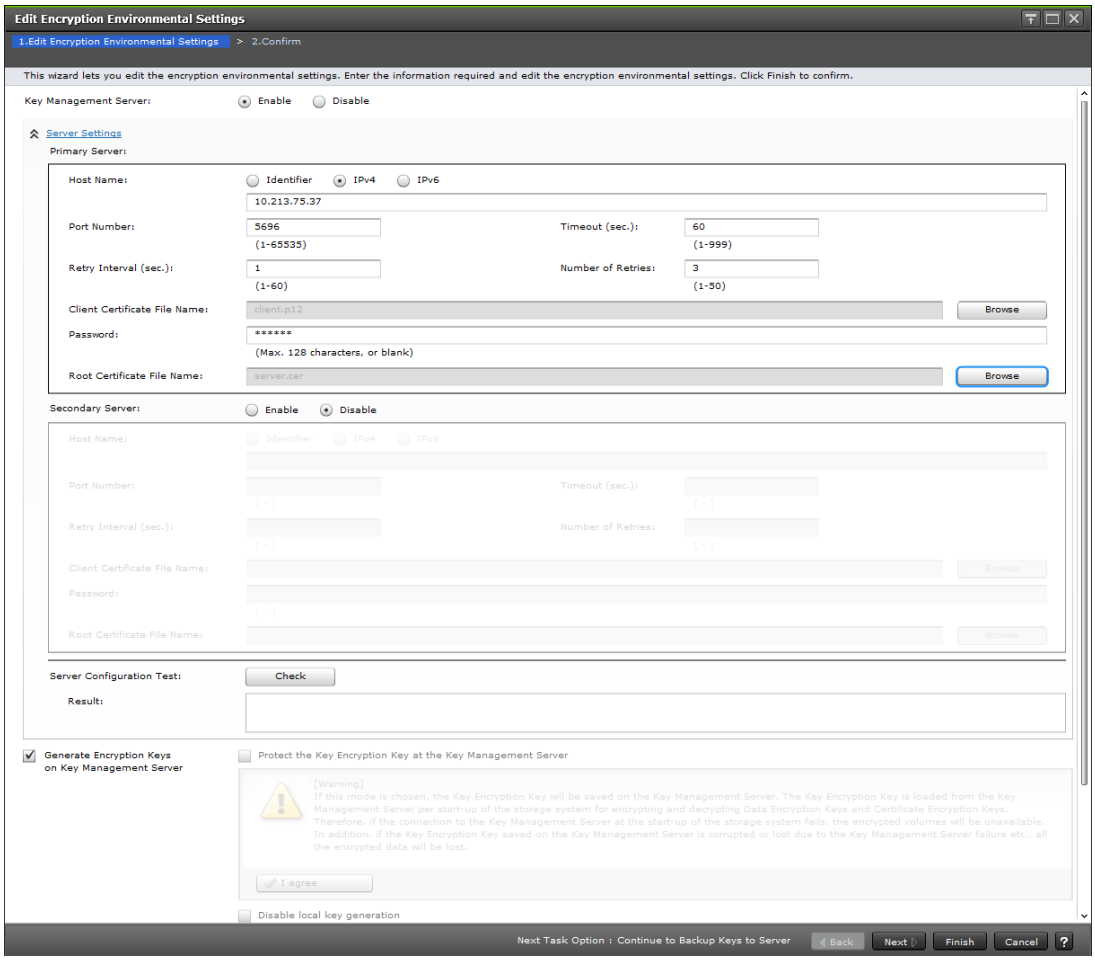
The **Edit Encryption Environmental Settings** wizard includes the following windows:

- **Edit Encryption Environmental Settings** window
- **Confirm** window

Edit Encryption Environmental Settings window

Items to be configured in the **Edit Encryption Environmental Settings** window can be changed under the following conditions:

- When the key management server is not in use
- When local key generation is disabled.
- When the key encryption key for the key management server is stored on DKC.

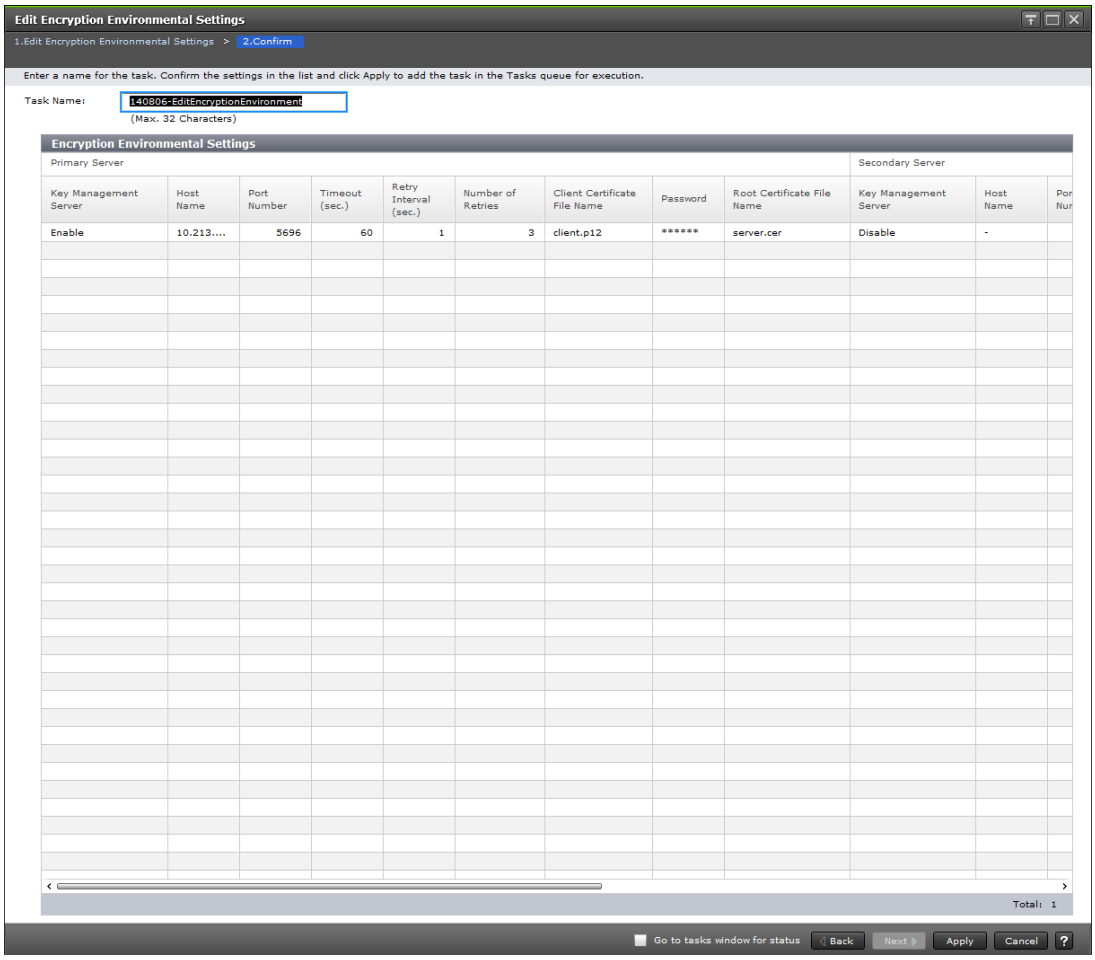


Item	Description
Key Management Server	Select whether to use the key management server: • **Enable:** (default) key management server is used. • **Disable:** key management server is not used.
Server Setting	When you use the key management server, the following items display: • Primary server • Secondary server • Server Configuration test
Primary Server	Specify the primary server information. • **Host Name**: Enter the host name of the key management server. **Identifier**: Enter the host identifier. **IPv4**: Enter the host IPv4 address. **IPv6**: Enter the host IPv6 address. • **Port number**: Enter the port number of the key management server. **Values**: 1 to 65535. **Default**: 5696. • **Timeout (sec.)**: Enter the time until the connection attempt to the key management server times out. **Values**: 1 to 999. **Default**: 60.

Item	Description
	• **Retry Interval (sec.)**: Enter the interval to retry the connection to the key management server. **Values**: 1 to 60. **Default**: 1. • **Number of Retries**: Enter the number of times to retry the connection to the key management server. **Values**: 1 to 50. **Default**: 3. • **Client Certificate File Name**: Select the client certificate file for connecting to the key management server. Click **Browse** and select the file. • **Browse**: Select the client certificate file. The form of the client certificate is PKCS#12. For information about the client certificate file, contact the server or network administrator. The file name appears in the **Client Certificate File Name** field. • **Password**: Enter 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: ! # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ • **Root Certificate File Name**: 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. If you do not know about the root certificate file, contact the server administrator or the network administrator. The name of the selected file appears in the **Root Certificate File Name** field.
Secondary Server	When the secondary server is set to **Enable**, the same items can be set as the items of the primary server.
Server Configuration Test	Select **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.
Generate Encryption Keys on Key Management Server	Checks when encryption keys are created on a key management server.
Protect the Key Encryption Key at the Key Management Server	Specifies when key encryption keys are saved on key management servers. If **Warning** is displayed, confirm the content of the warning, and select **I Agree**.
Disable local key generation	Checks when encryption keys are saved on key management servers and encryption keys cannot be

Item	Description
	created on the storage system. If **Warning** is displayed, confirm the content of the warning, and select **I Agree**. **Caution**: If you finish the setting, you cannot restore the setting, so it is recommended that you confirm there are no problems before selecting **I Agree**.
Initialize Encryption Environmental Settings	Select to initialize the connection settings to the key management server.

Confirm window in the Edit Encryption Environmental Settings wizard



Item	Description
Primary Server	Displays the primary server information. • **Key Management Server**: Shows whether the key management server is used. • **Disable**: key management server is not used. • **Not Set**: Initialize the connection settings to the key management server.

Item	Description
	• **Host Name**: The host name of the key management server. • **Port number**: The port number of the key management server. • **Timeout (sec.)**: The time until the connection attempt to the key management server times out. • **Retry Interval (sec.)**: The interval to retry the connection to the key management server. • **Number of Retries**: The number of times to retry the connection to the key management server. • **Client Certificate File Name**: The client certificate file for connecting to the key management server. • **Password**: The password for the client certificate is displayed as ****** (six asterisks). • **Root Certificate File Name**: The root certificate file for connecting to the key management server.
Secondary Server	When the secondary server exists, displays items same as the primary server.
Generate Encryption Keys on Key Management Server	Displays whether encryption keys are created on a key management server or not. • **Yes**: Encryption keys are created on a key management server. • **No**: Encryption keys are not created on a key management server.
Protect the Key Encryption Key at the Key Management Server	Displays whether key encryption keys are saved on key management servers or not. • **Yes**: Encryption keys are saved on key management servers. • **No**: Encryption keys are not saved on key management servers.
Disable local key generation	Displays whether encryption keys are saved on key management servers and encryption keys cannot be created on the storage system. • **Yes**: Encryption keys are created on key management servers and encryption keys cannot be created on the storage system. • **No**: Encryption keys are not created on key management servers. Encryption keys are created on storage systems.

Create Keys wizard

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

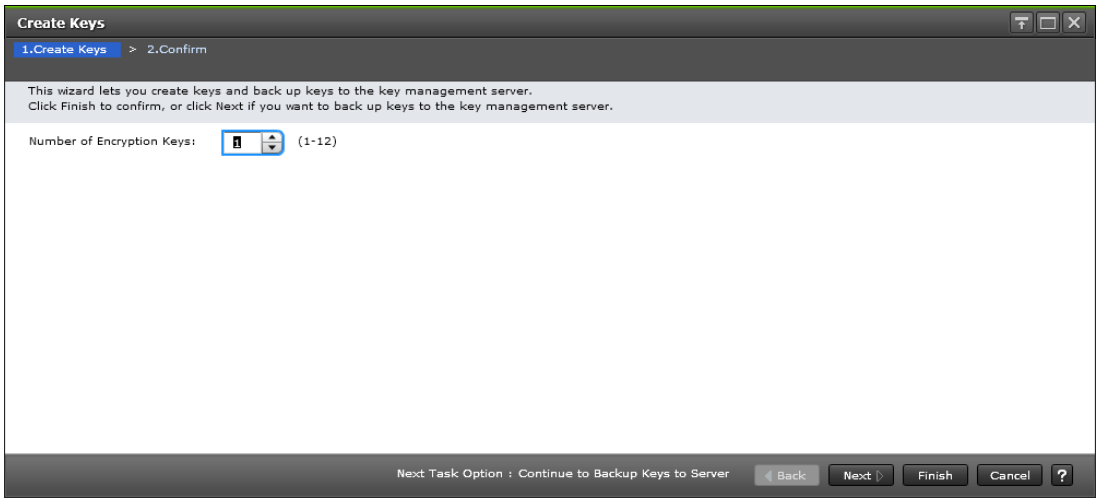
This wizard includes the following windows:

- **Create Keys** window

- **Confirm** window

Create Keys window

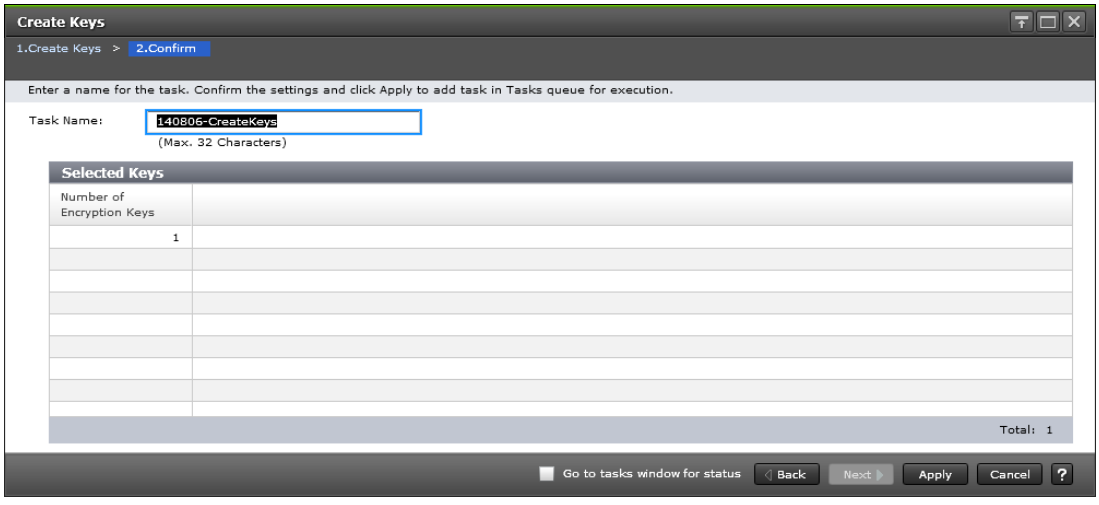
Use the **Create Keys** window to create a data encryption license key. This window includes the **Selected Keys** table.



Item	Description
Number of Encryption Keys	Specifies the number of encryption keys (1-1,024). The maximum number of encryption keys is 1,024. This window shows the value obtained by subtracting the number of created DEK and Free keys from 1,024.

Confirm window in the Create Keys wizard

The following is the **Confirm** window in the **Create Keys** wizard.



Item	Description
Number of Encryption Keys	Displays the number of encryption keys.

Related topics

- Workflow for creating data encryption license keys on page 4-2
- Creating data encryption license keys on page 4-2

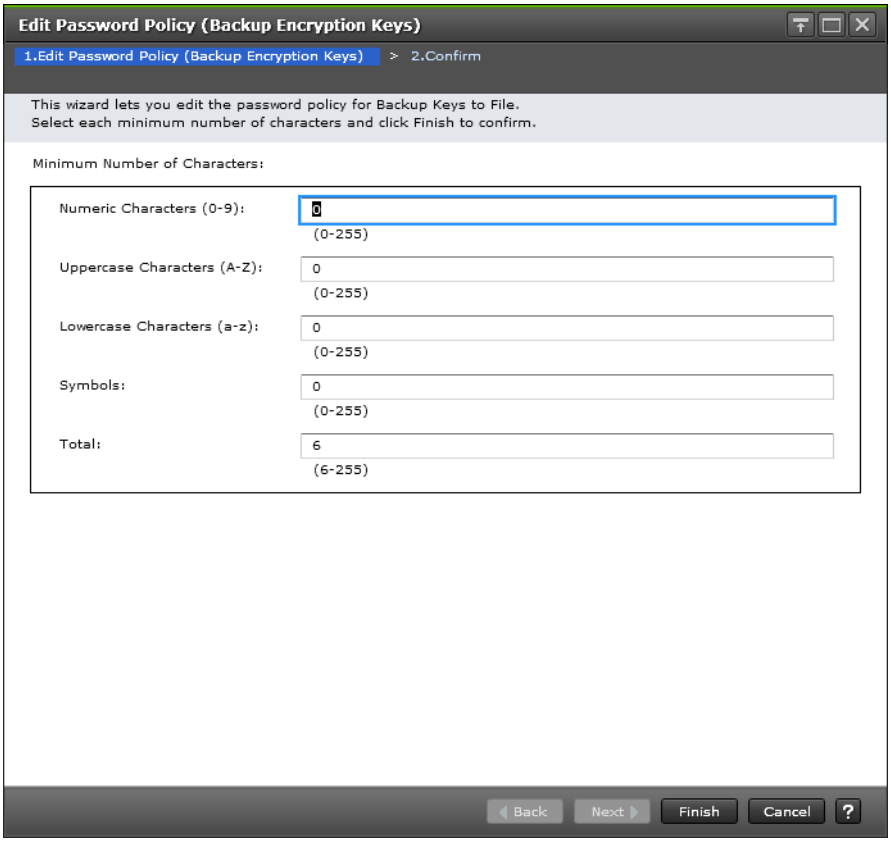
Edit Password Policy (Backup Encryption Keys) wizard

Use the **Edit Password Policy (Backup Encryption Keys)** wizard to edit the password policy for backup keys.

This wizard includes the following windows:

- **Edit Password Policy (Backup Encryption Keys)** window
- **Confirm** window

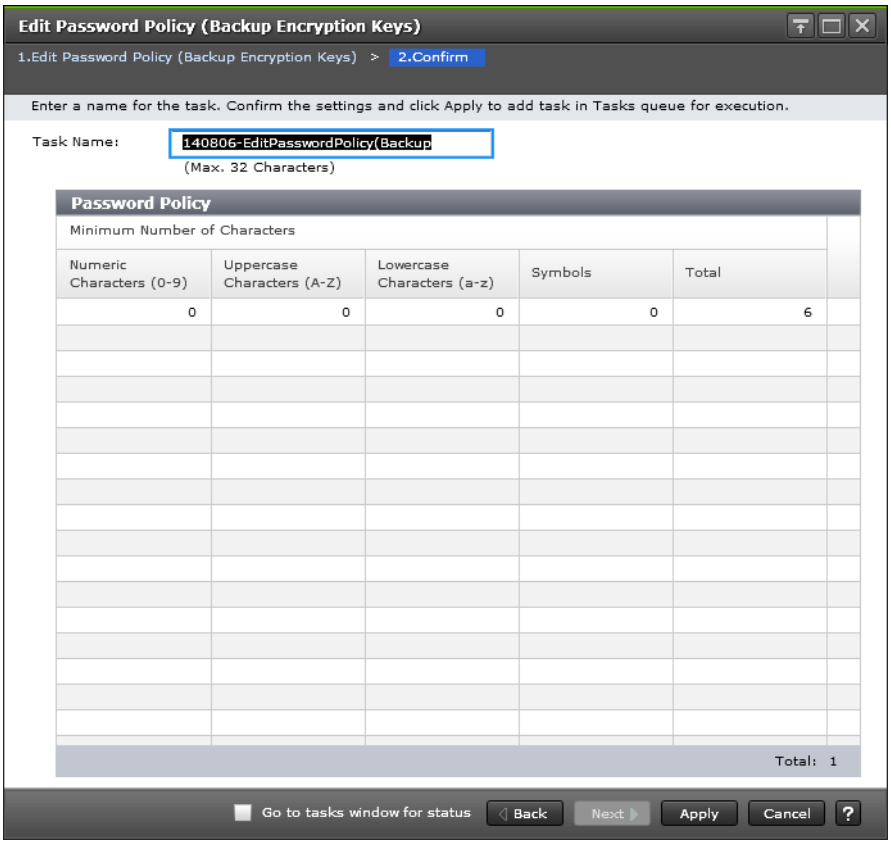
Edit Password Policy (Backup Encryption Keys) window



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 (Backup Encryption Keys) wizard

Use the **Confirm** window in the **Edit Password Policy (Backup Encryption Keys)** 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

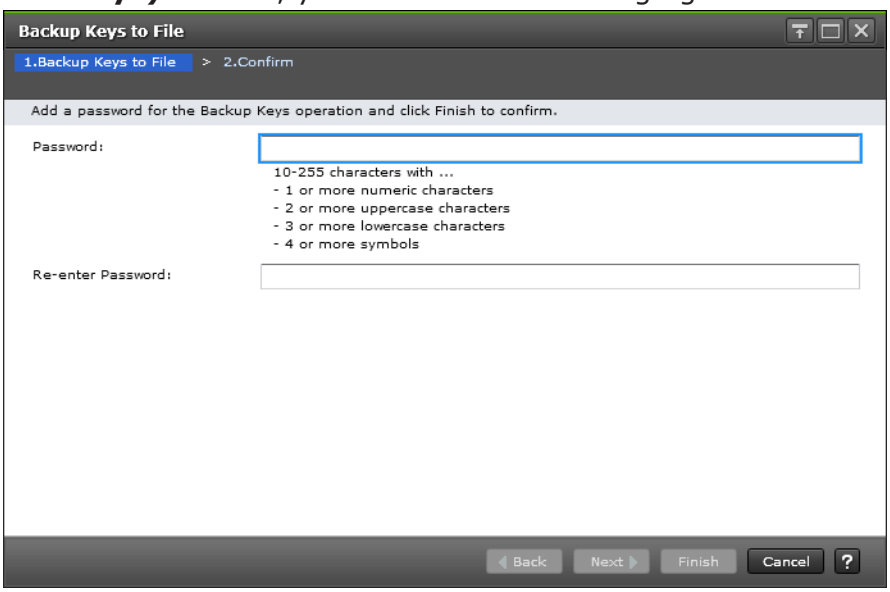
Use the **Backup Keys to File** wizard to create backup data encryption license keys as files on HDvM - SN.

This wizard includes the following windows:

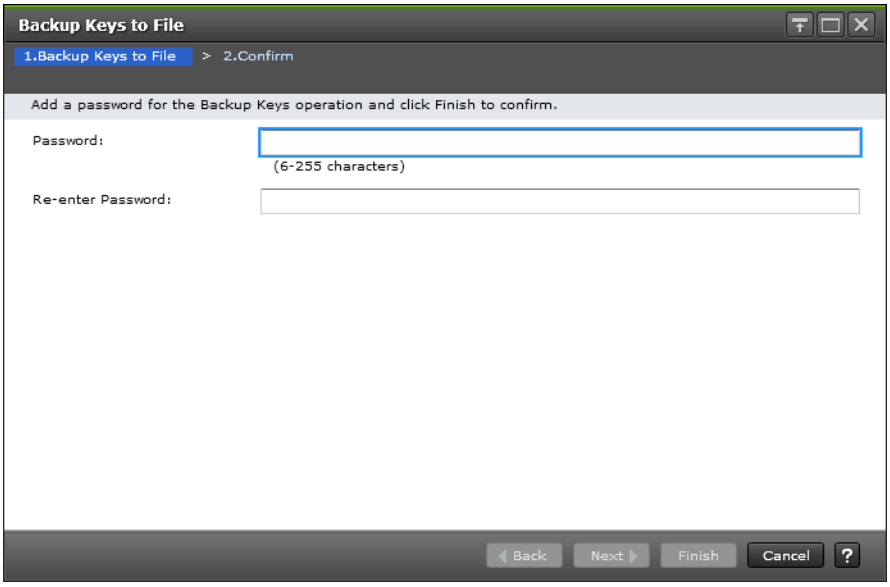
- **Backup Keys to File** window
- **Confirm** window

Backup Keys to File window

When the password policy is edited in the **Edit Password Policy (Backup Encryption Keys)** window, you will see the following figure.



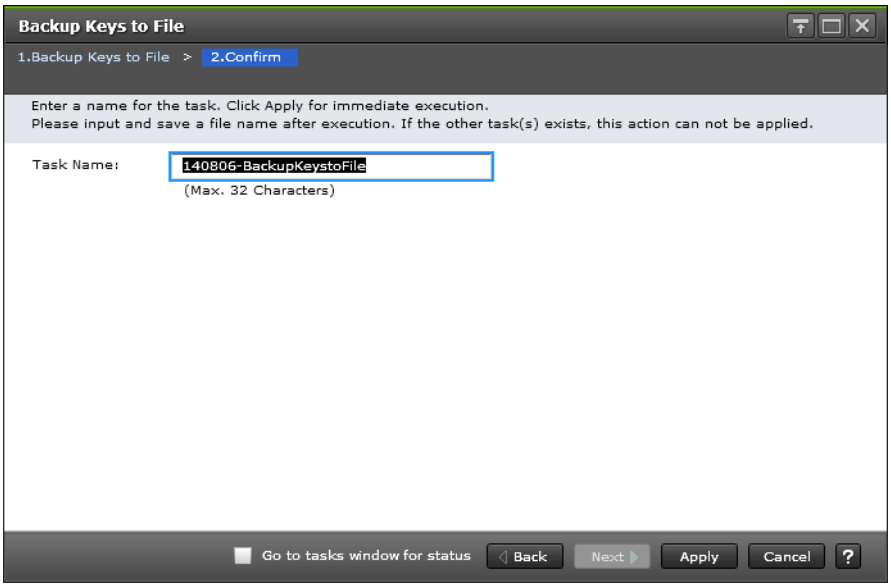
When the password policy is not edited in the **Edit Password Policy (Backup Encryption Keys)** window, you will see the following figure.



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)

Item	Description
	• Symbols: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
Re-enter Password	Type the password again for confirmation.

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.

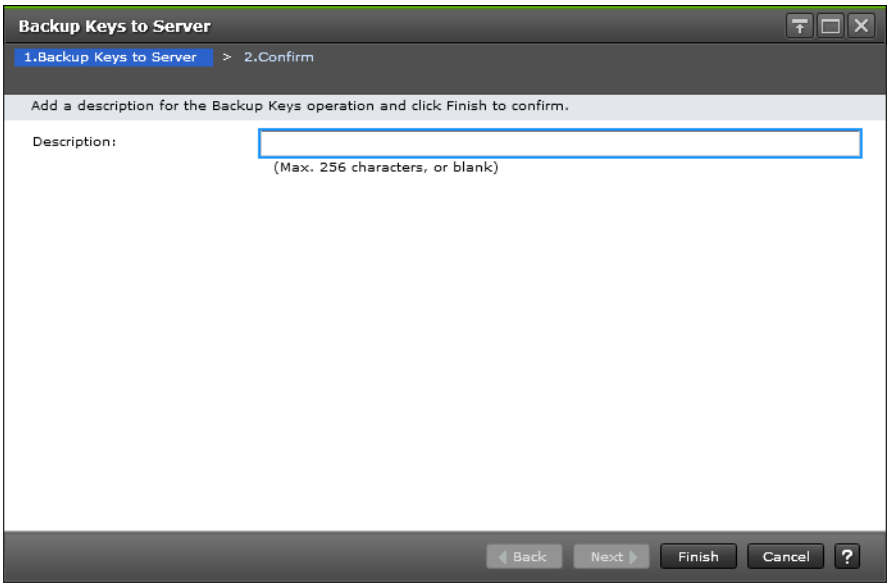
Backup Keys to Server wizard

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

This wizard includes the following windows:

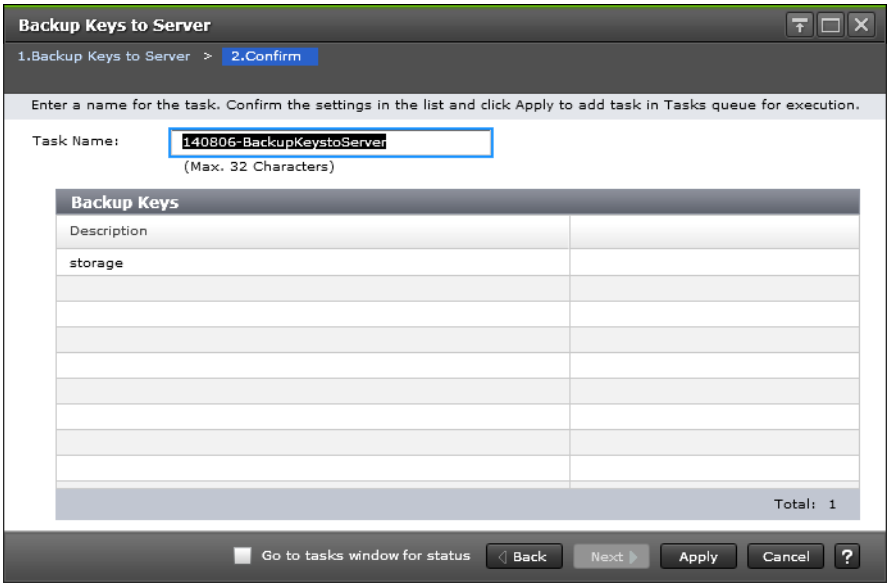
- **Backup Keys to Server** window
- **Confirm** window

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.

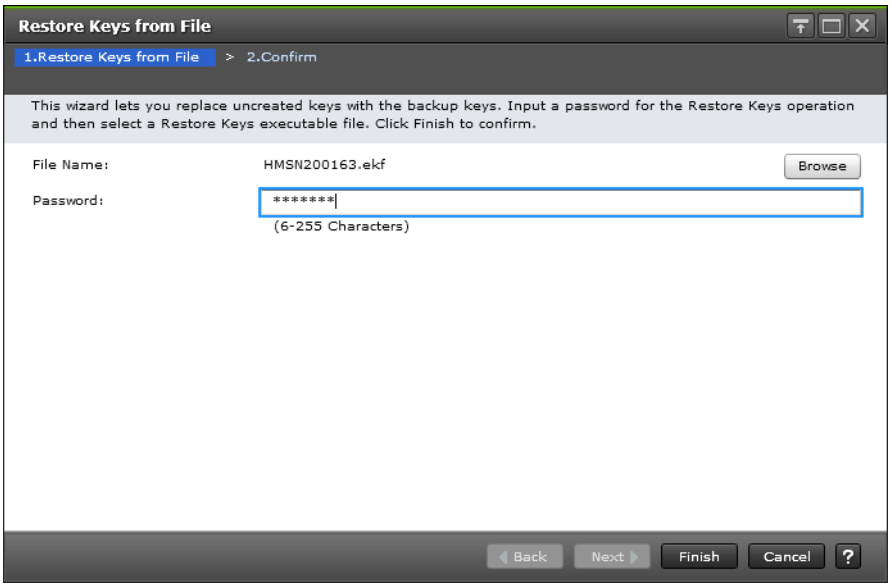
Restore Keys from file wizard

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

This wizard includes the following windows:

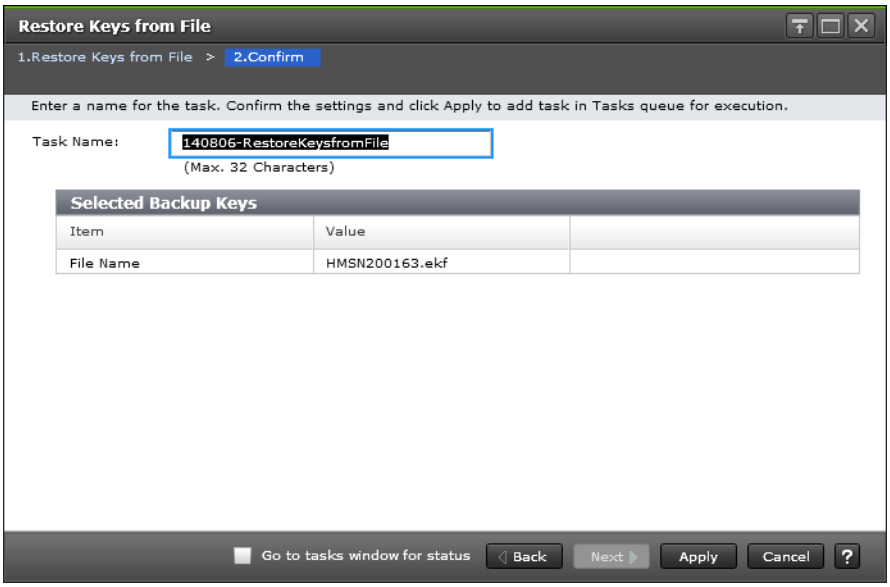
- **Restore Keys from File** window
- **Confirm** window

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.

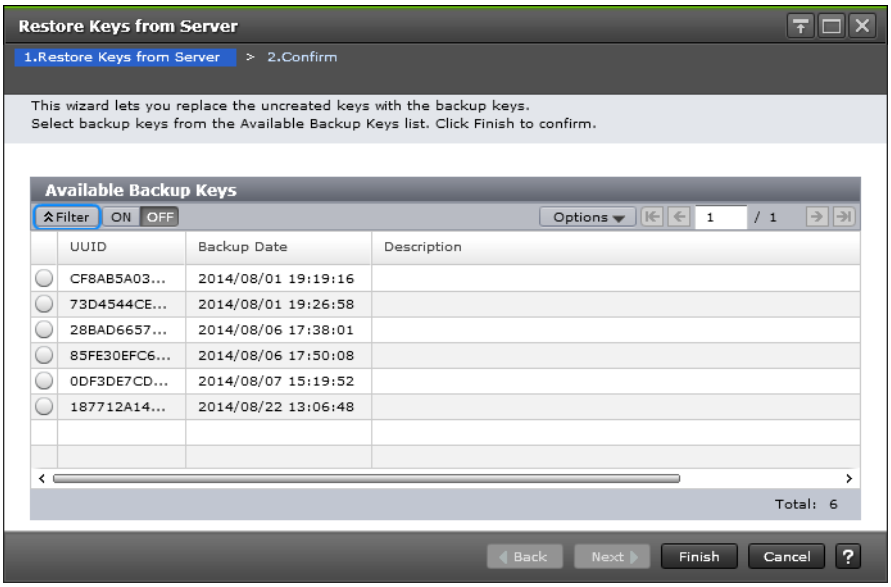
Restore Keys from Server wizard

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

This wizard includes the following windows:

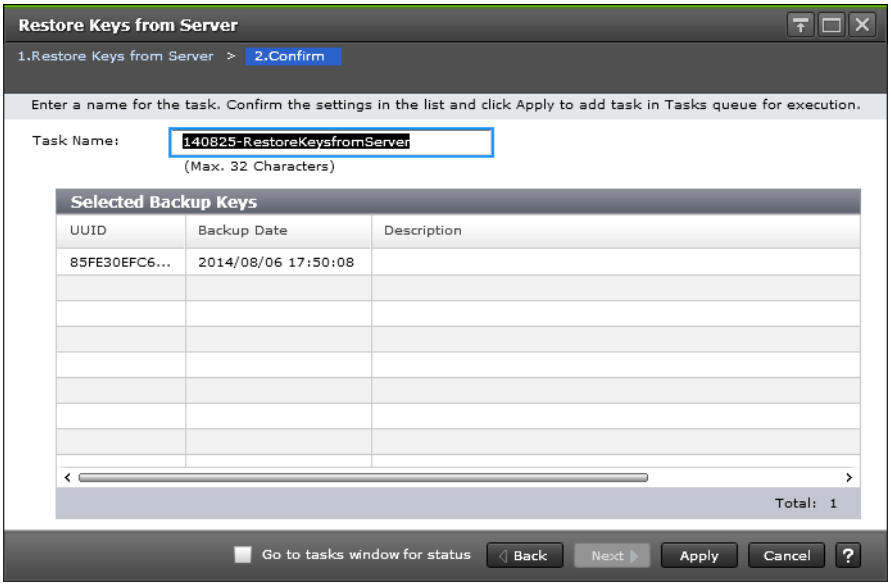
- **Restore Keys from Server** window
- **Confirm** window

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.

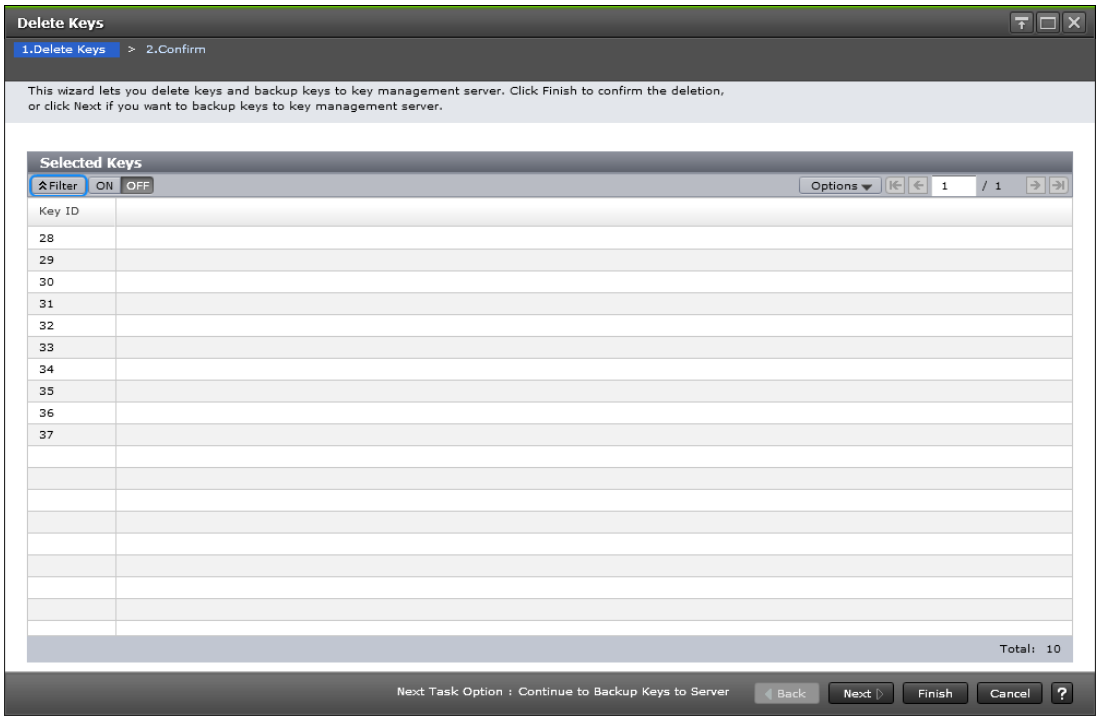
Delete Keys wizard

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

This wizard includes the following windows:

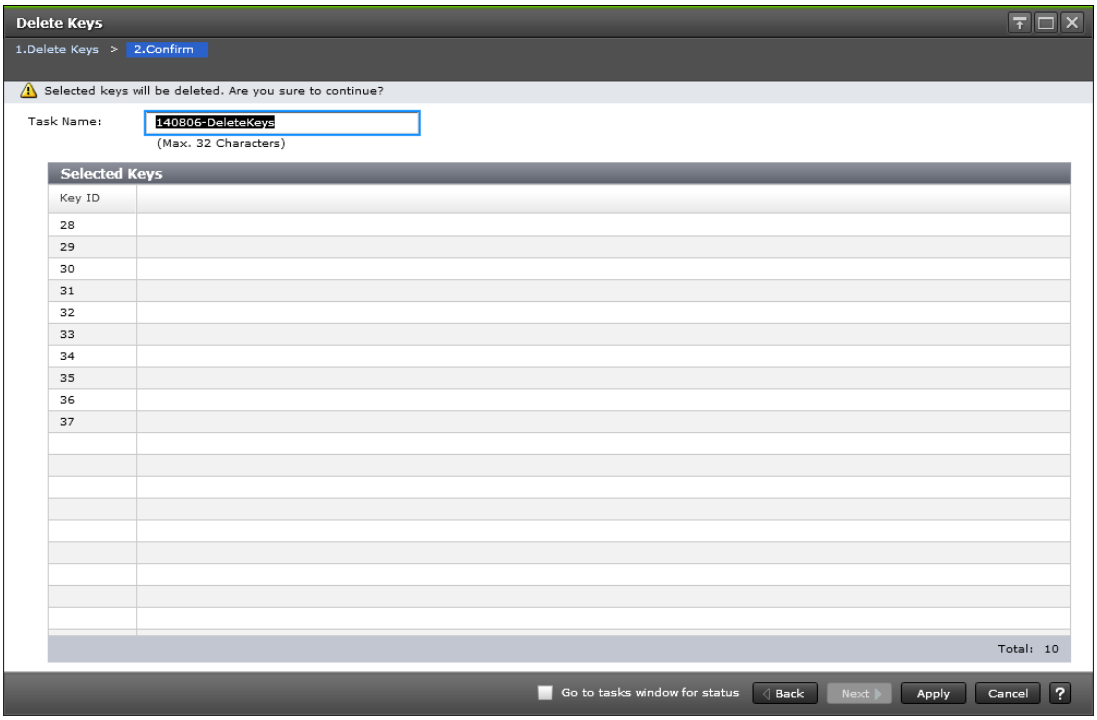
- **Delete Keys** window
- **Confirm** window

Delete Keys window



Item	Description
Key ID	IDs of data encryption license keys.

Confirm window in the Delete Keys wizard

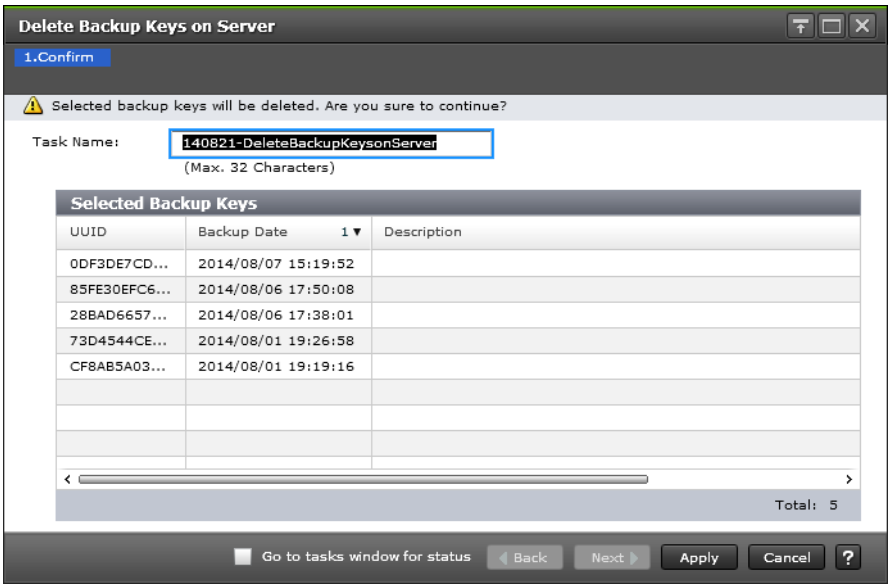


Item	Description
Key ID	The identifiers for the data encryption license keys.

Delete Backup Keys on Server window

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

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

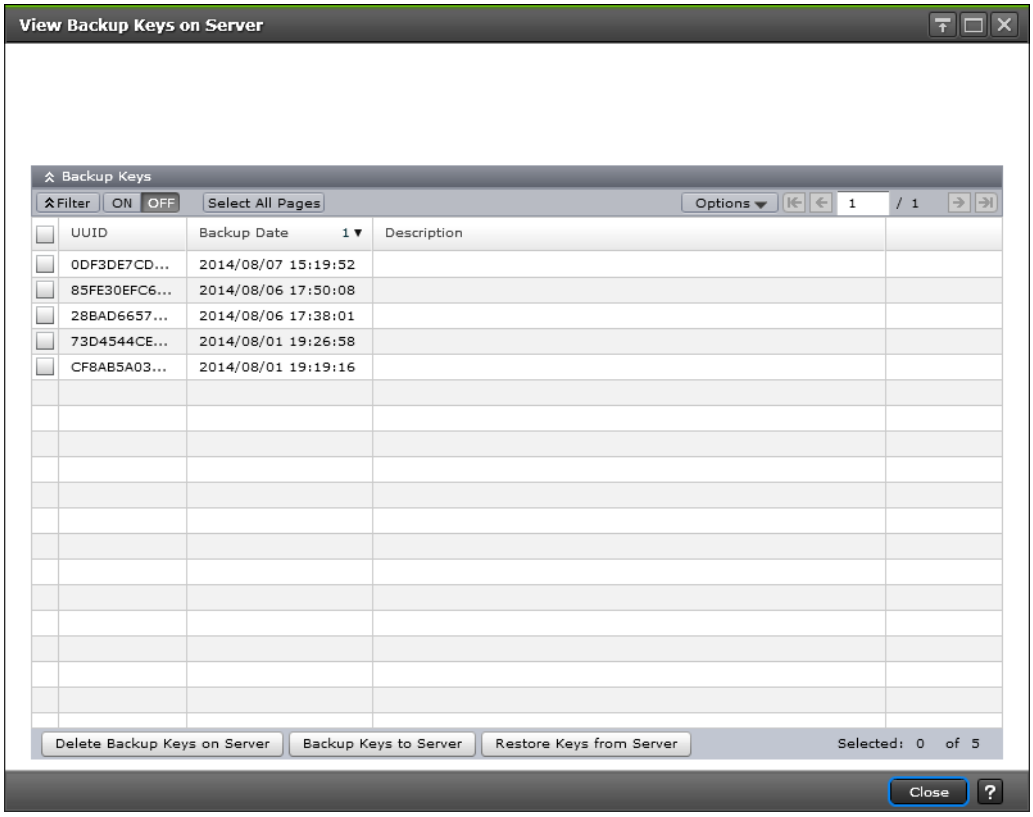


Item	Description
UUID	Shows the UUID of the data encryption license key you backed up on the key management server.
Backup Date	Shows the time when you backed up the data encryption license key on the key management server.
Description	Shows the description you typed when you backed up the data encryption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

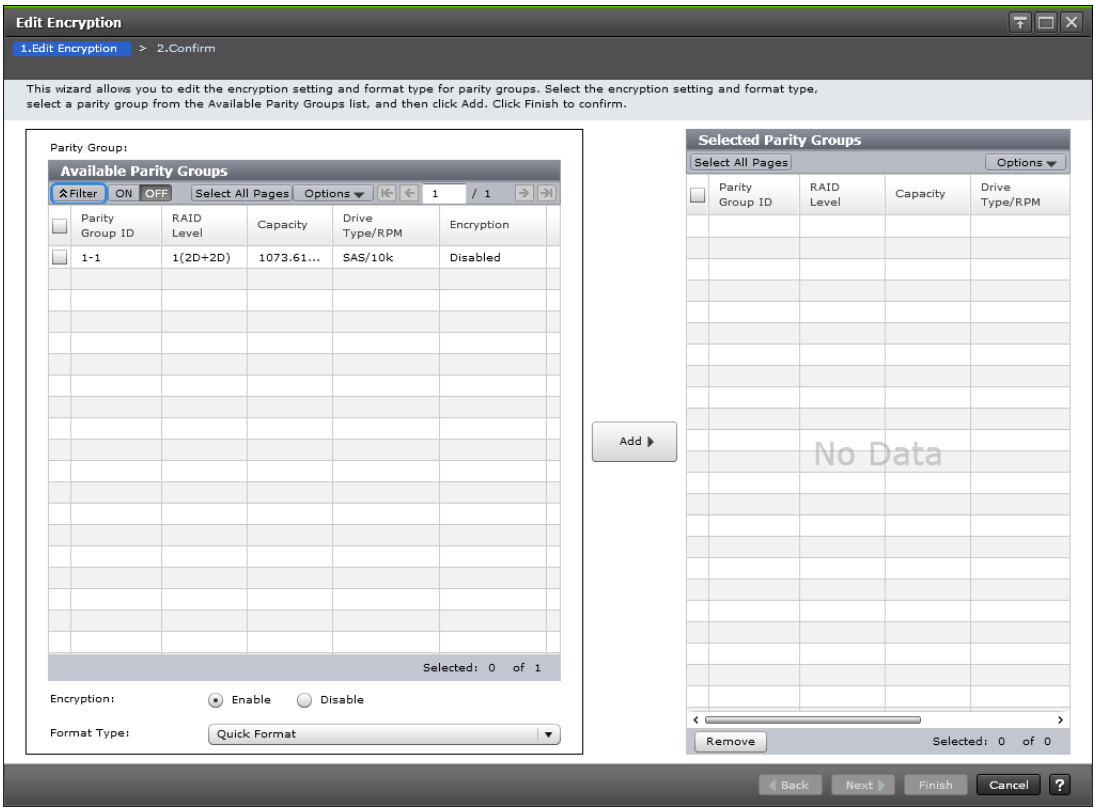
Use the **Edit Encryption** wizard to do the following:

- 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

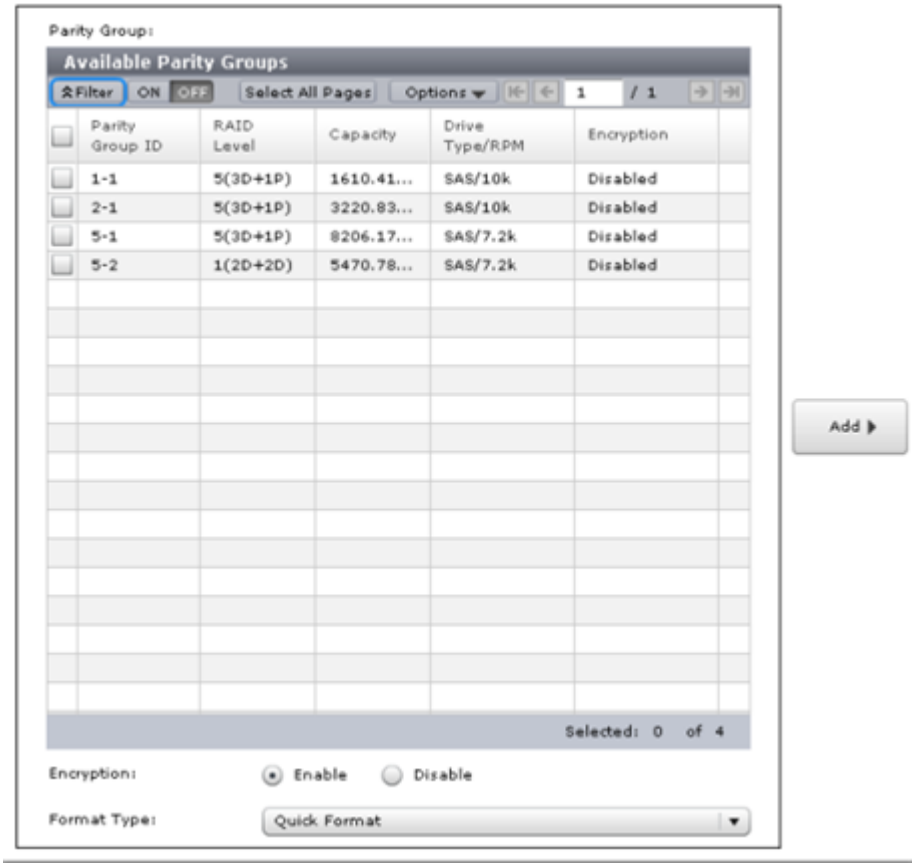


The **Edit Encryption** window includes the following items:

- **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-26.

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 drive types and RPM (rotation per minute) of the LDEV in the parity group.
Encryption	Shows the encryption setting for the parity group. **Enable**: Encryption is enabled. **Disable**: Encryption is disabled.
Encryption	Select the encryption setting for the parity group: • If you click **Enable**, data encryption, select will be enabled. • If you click **Disable**, data encryption, select will be disabled.
Format Type	Select the format types of the parity group. You do not need to format volumes when there are none selected in the parity group. Therefore, the format type

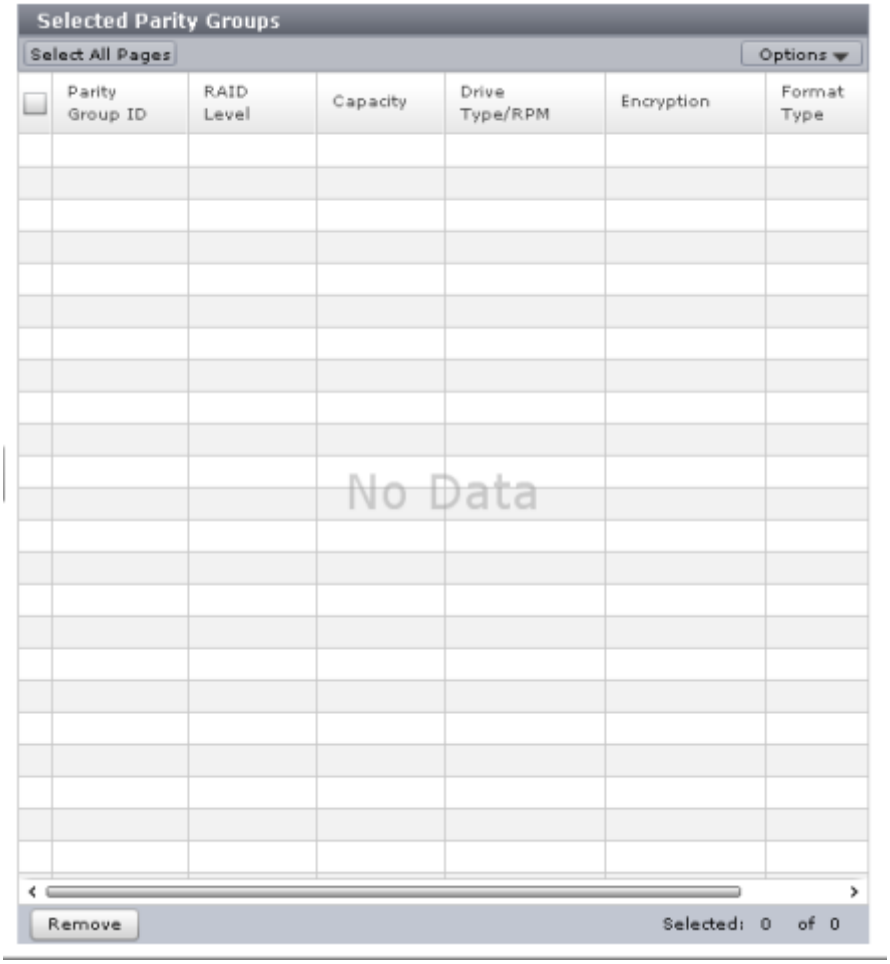
Item	Description
	in the **Selected Parity Groups** list becomes a hyphen (-) regardless of the status of the format type.

Add

Use this button to move a selected parity group in the **Available Parity Groups** table to the **Selected Parity Groups** table.

Selected Parity Groups table

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

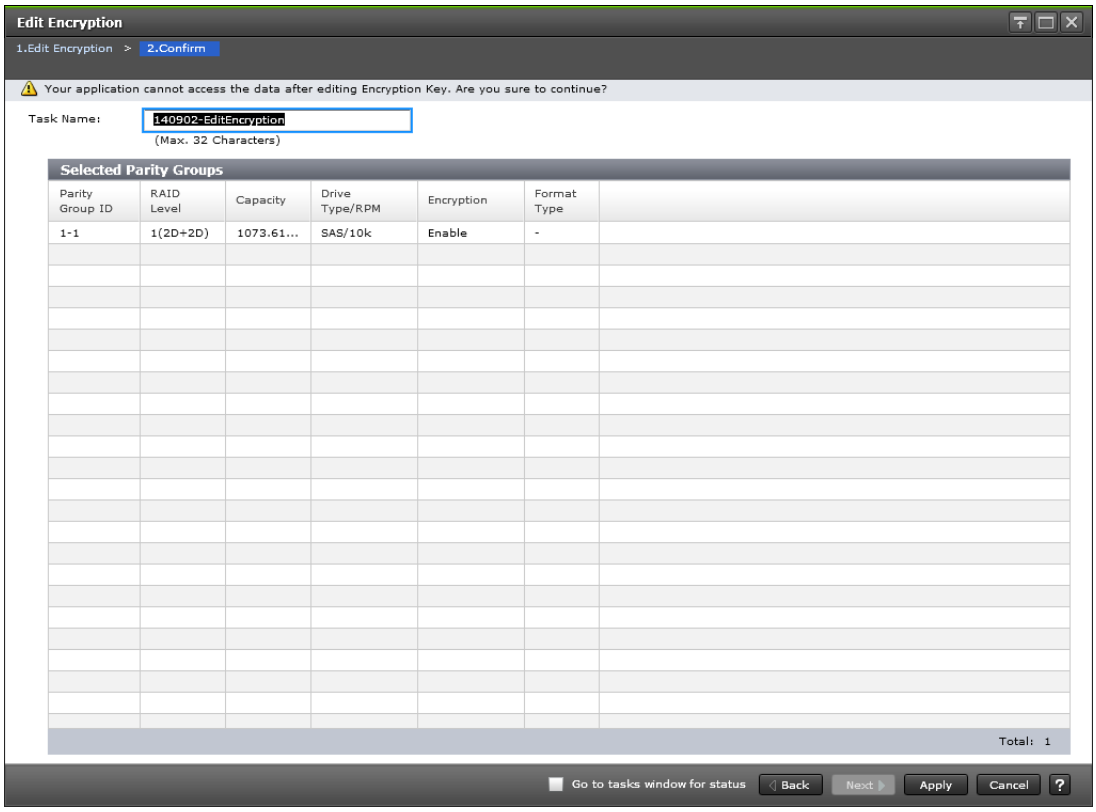


Item	Description
Parity Group ID	Shows parity group IDs.
RAID Level	Shows the RAID level of the parity group. For an interleaved parity group, the interleaved number appears after the RAID level. Example: 1(2D+2D)*2

Item	Description
Capacity	Shows the total capacity (unit) of the parity group.
Drive Type/RPM	Shows the drive types and RPM (rotation per minute) of the LDEV in the parity group.
Encryption	Shows the encryption setting for the parity group: • **Enable**: Encryption is enabled. • **Disable**: Encryption is disabled.
Format Type	Shows the format types of the parity group. You do not need to format volumes when there are none selected in the parity group. Therefore, the format type in the **Selected Parity Groups** list becomes a hyphen (-) regardless of the status of the format type.
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 drive types and RPM (rotation per minute) of the LDEV in the parity group.
Encryption	Encryption setting for the parity group: • Enable - encryption enabled • Disable - no encryption
Format Type	Shows the format types of the parity group. You do not need to format volumes when there is no volume in the selected parity group. Therefore, the format type in the **Selected Parity Groups** list becomes "-" (a hyphen) regardless of the status of **Format Type**.

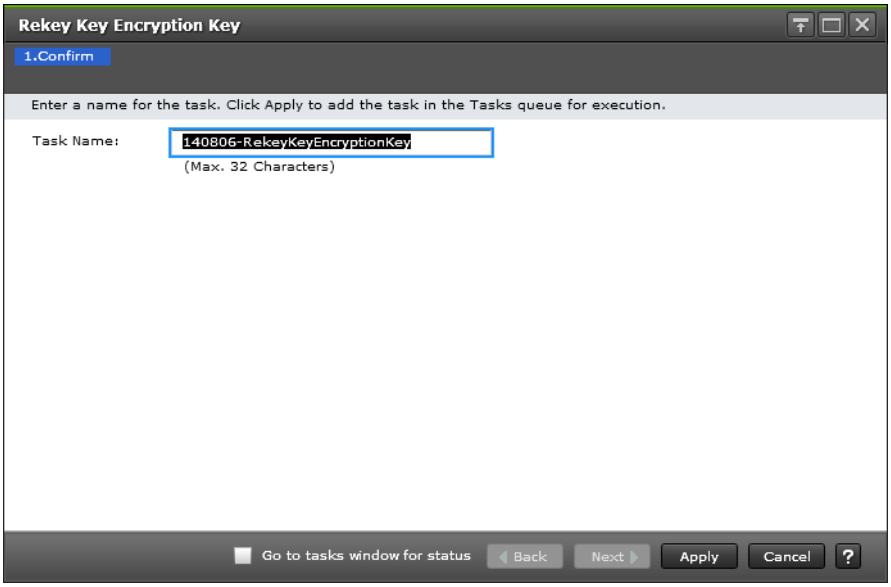
Rekey Certificate Encryption Keys window

If you change certificate encryption keys, you can use the **RekeyCertificate Encryption Keys** window to rekey certificate encryption keys.

Item	Description
Task Name	You can enter up to 32 ASCII characters (letters,numerals, and symbols) in **Task Name**. Task namesare case-sensitive.

Rekey Key Encryption Key window

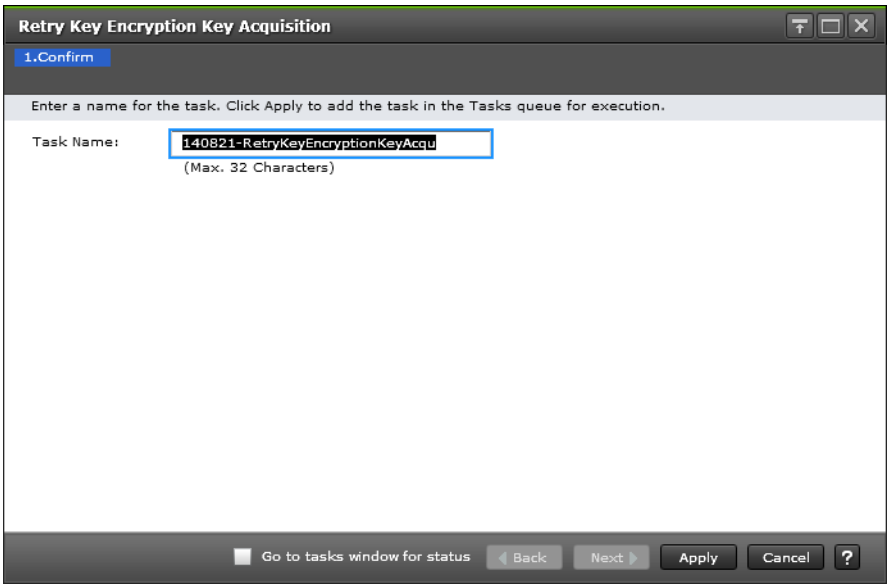
If you change key encryption keys, you can use the **Rekey key Encryption Keys** window to rekey key encryption keys.



Item	Description
Task Name	You can enter up to 32 ASCII characters (letters, numerals, and symbols) in **Task Name**. Task names are case-sensitive.

Retry Key Encryption Key Acquisition window

If you acquire the key encryption keys from the external key management server when the storage device starts, retry key encryption key acquisition unless you can acquire them by some reasons.



Item	Description
Task Name	You can enter up to 32 ASCII characters (letters, numerals, and symbols) in **Task Name**. Task names are case-sensitive.

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; open-system emulation types include OPEN-V and OPEN-3.

Encryption Administrator
User role in Device Manager - Storage Navigator with permission to perform DAR operations. Compare with *Storage Administrator*.

#	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

encryption key
The data encryption license key is used to encrypt and decrypt data on VSP G400, G600, G800 or VSP F400, F600, F800.

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 Device Manager - 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 Device Manager - 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 Device Manager - 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 Device Manager - 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

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-94HM8029-02