HITACHI
Inspire the Next

Hitachi Virtual Storage Platform G1000
Encryption License Key User Guide

FASTFIND LINKS

MK-92RD8009-02

Hitachi Data Systems

Contents

Preface

This document describes and provides instructions for installing and using the Encryption License Key feature of the Hitachi Virtual Storage Platform G1000 storage system.

Please 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, Hitachi Data Systems representatives, and authorized service providers who install, configure, and operate the Hitachi Virtual Storage Platform G1000.

Readers of this document should be familiar with the following:

- Data processing and RAID storage systems and their basic functions.
- The Hitachi Virtual Storage Platform G1000 and the *Hitachi Virtual Storage Platform G1000 Product Guide*.
- The Hitachi storage management software for the Hitachi Virtual Storage Platform G1000 (Hitachi Command Suite or Hitachi Device Manager - Storage Navigator) and the software user manual (*Hitachi Command Suite User Guide* or *Hitachi Virtual Storage Platform G1000 Mainframe System Administrator Guide*).
- The use of data encryption in a storage environment.

Product version

This document revision applies to Hitachi Virtual Storage Platform G1000 microcode 80-02-0*x* or later.

Document revision level

Revision	Date	Description
MK-92RD8009-00	April 2014	Initial release
MK-92RD8009-01	August 2014	Supersedes and replaces MK-92RD8009-00
MK-92RD8009-02	October 2014	Supersedes and replaces MK-92RD8009-01

Changes in this revision

- Revised navigation steps in procedures.

Referenced documents

Hitachi Virtual Storage Platform G1000 documents:

- *Hitachi Virtual Storage Platform G1000 Hardware Guide*, MK-92RD8007
- *Hitachi Virtual Storage Platform G1000 Mainframe System Administrator Guide*, MK-92RD8016
- *Hitachi Command Suite User Guide*, MK-90HC172
- *Hitachi Command Suite Audit Log Reference Guide*, MK-92HC213
- *Hitachi Virtual Storage Platform G1000 Provisioning Guide for Mainframe Systems*, MK-92RD8013
- *Hitachi Virtual Storage Platform G1000 Provisioning Guide for Open Systems*, MK-92RD8014
- *Hitachi Command Suite Messages*, MK-90HC178

Document conventions

This document uses the following terminology conventions:

Convention	Description
Hitachi storage management software	Refers to all supported software products for the Hitachi Virtual Storage Platform G1000 unless otherwise noted: • Hitachi Command Suite • Hitachi Device Manager - Storage Navigator

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.

Icon	Meaning	Description
	Caution	Warns the user of adverse conditions and/or consequences (e.g., disruptive operations).
	WARNING	Warns the user of severe conditions and/or consequences (e.g., destructive operations).

Accessing product documentation

The Hitachi Virtual Storage Platform G1000 user documentation is available on the Hitachi Data Systems Portal: https://portal.hds.com. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

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

Comments

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

Thank you!

1

Encryption License Key Overview

The chapter describes the Encryption License Key feature of the Hitachi Virtual Storage Platform G1000 storage system.

- ☐ Encryption License Key benefits
- ☐ Encryption License Key support specifications
- ☐ When are data encryption license keys needed
- ☐ Primary and secondary data encryption license keys
- ☐ KMIP key management server support
- ☐ Audit logging of encryption events
- ☐ Interoperability requirements and considerations
- ☐ Workflow for enabling data encryption
- ☐ Workflow for encrypting existing data
- ☐ Workflow for disabling encryption
- ☐ Workflow for changing the encryption license key

Encryption License Key benefits

To guarantee the security of data, use the Encryption License Key feature to encrypt the data stored on the Hitachi Virtual Storage Platform G1000. Encrypting data can prevent information loss and leaks, for example, when a drive is physically removed from the storage system due to failure or theft.

The Encryption License Key feature provides the following benefits:

- Hardware-based AES 256 encryption in XTS mode for open and mainframe systems.
- You can apply encryption to some or all of the internal drives without throughput or latency impacts for data I/O and little to no disruption to existing applications and infrastructure.
- Simplified and integrated key management that does note require specialized key management infrastructure.

Encryption License Key support specifications

The following table lists the support specifications for Encryption License Key.

Item		Specification
Hardware specifications	Encryption algorithm	Advanced Encryption Standard (AES) 256 bit.
	Encryption mode	XTS mode.
LDEVs that you can encrypt	Volume type	Open, mainframe, multiplatform.
	Emulation type	All emulation types.
	Internal/external LDEVs	Internal LDEVs only.
	LDEV with existing data	Supported. Requires data migration.

Item		Specification
Managing data encryption license keys	Creating data encryption license keys	Use the Hitachi storage management software to create data encryption license keys.
	Deleting data encryption license keys	Use the Hitachi storage management software 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 license keys are used per HDD.
	Scope of data encryption license keys	4,096 data encryption license keys per storage system. You can create 4,096 Free keys or DEK keys. You can create 32 CEK keys and one KEK key. Therefore, the total number of data encryption license keys will be 4,129 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 perform the following operations:

- Adding 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.
- Adding or replacing disk adapters

  Six Free keys are needed for each disk adapter to create four CEK keys and two keys to register CEK keys.
- Updating CEK keys

Four Free keys for each disk adapter (32 Free keys per storage system) are needed to change CEK keys.

If a problem occurs during an operation, extra keys might be needed to recover from the problem.

Primary and secondary data encryption license keys

The Hitachi Virtual Storage Platform G1000 automatically creates a primary backup of each data encryption license key and stores this backup on each MP package. The Encryption License Key feature enables you to create secondary backups of the data encryption license keys for the Hitachi Virtual Storage Platform G1000. If the primary backup key is unavailable, the secondary backup is required to restore the key.

WARNING: If the primary backup key becomes unavailable and no secondary backup key exists, the system cannot decrypt the encrypted data.

It is strongly recommended that you back up each key or group of keys immediately after you create them and schedule regular weekly backups of all keys to ensure data availability. You are responsible for storing the secondary backup keys securely.

It is also recommended that you back up each key after you perform any of the following operations:

- Adding, removing, or replacing drives
- Adding, removing, or replacing disk adapters
- Updating CEK keys
- Updating KEK keys

Note: The creation and secure storage of secondary backup encryption license keys must be included as part of your corporate security policy.

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

KMIP key management server support

Using the Encryption License Key feature, 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 details about backing up data encryption license keys to a key management server, see Backing up keys to a key management server on page 4-4.

Audit logging of encryption events

The Audit Log feature of the Hitachi Virtual Storage Platform G1000 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 details about audit logging and audit log events, see the *Hitachi Command Suite Audit Log Reference Guide*.

Interoperability requirements and considerations

The following table provides the interoperability requirements and considerations for Encryption License Key operations.

Functions	Interoperability requirements and considerations
ShadowImage, TrueCopy, Compatible FlashCopy® V2, and Compatible XRC	Encrypt both the P-VOL and S-VOLs (S-VOL and T-VOLs for Compatible FlashCopy® V2) of pairs 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 and therefore 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, Dynamic Provisioning for Mainframe, and Dynamic Tiering for Mainframe	When enabling encryption for data written to a data pool with a V-VOL, use a data pool that consists of encrypted volumes.

Workflow for enabling data encryption

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

1. Create a secondary backup of the data encryption license key. For details, see Workflow for backing up secondary data encryption license keys on page 4-3.
2. Enable data encryption at the parity-group level. For details, see Enabling data encryption at the parity group-level on page 4-7.
3. Format the LDEVs in the encrypted parity group. The data to be stored on these new LDEVs will be encrypted.

   For instructions on formatting LDEVs, see the *Hitachi Virtual Storage Platform G1000 Provisioning Guide for Open Systems*.

Workflow for encrypting existing data

To encrypt existing data, you must migrate the data to an encrypted parity group.

Use the following process to encrypt existing data:

1. Create a new parity group.
2. Enable data encryption on the parity group. For details, see Enabling data encryption at the parity group-level on page 4-7.
3. Format the LDEVs in the encrypted parity group. For instructions, see the *Hitachi Virtual Storage Platform G1000 Provisioning Guide for Open Systems*.
4. Migrate the existing data to the LDEVs in the encrypted parity group. For details about data migration, contact your Hitachi Data Systems account team.

Workflow for disabling encryption

Use the following process to disable encryption:

1. Back up the data in the parity group.
2. Disable data encryption at the parity-group level. For details, see Workflow for disabling data encryption at the parity-group level on page 4-8.
3. Format the LDEVs in the parity group. For instructions, see the *Hitachi Virtual Storage Platform G1000 Provisioning Guide for Open Systems*.

Workflow for changing the encryption license key

To change the encryption license key for existing encrypted data, you must migrate the data to an encrypted parity group that has a different encryption license key.

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

1. Create a new parity group.
2. Enable encryption with a new data encryption license key. For details, see Enabling data encryption at the parity group-level on page 4-7.
3. Format the LDEVs in the encrypted parity group. For instructions, see the *Hitachi Virtual Storage Platform G1000 Provisioning Guide for Open Systems*.
4. Migrate the source data to the new target LDEVs in the encrypted parity group.

When a drive is replaced, the data encryption license keys that are allocated to that drive are deleted, and new data encryption license keys are allocated when the new drive is added.

2

Encryption License Key Installation

This chapter describes how to install the Encryption License Key feature.

- ☐ Workflow for Encryption License Key installation
- ☐ System requirements
- ☐ Enabling the Encryption License Key feature
- ☐ Disabling the Encryption License Key feature

Workflow for Encryption License Key installation

Use the following process to install the Encryption License Key feature:

1. Verify that your system meets the system requirements.

   For details, see System requirements on page 2-2.

2. Enable the Encryption License Key feature.

   For details, see Enabling the Encryption License Key feature on page 2-2.

3. Assign the Security Administrator (View & Modify) role to the administrator who creates, backs up, and restores data encryption license keys.

   For details, see Enabling the Encryption License Key feature on page 2-2.

System requirements

The following table lists the system requirements for the Encryption License Key feature.

Item	Requirement
Hitachi Virtual Storage Platform G1000	• Microcode 80-01-2x and later.
Hitachi Command Suite Hitachi Device Manager - Storage Navigator	• Encryption License Key software license • Security Administrator (View & Modify) role to enable or disable data encryption and to back up or restore keys • Storage Administrator (provisioning) role to format volumes
SVP (Web server)	To connect to the key management server by specifying the host name instead of IP address, you need the DNS server settings. For SVP configuration, give your service representative the IP address of the DNS server.
Host platforms	All open-systems and mainframe host platforms are supported.
Data volumes	All volume types and emulations are supported: open-systems, mainframe, and multiplatform. Supported volumes: Internal
Disk adapter	A disk adapter that provides data encryption.

Enabling the Encryption License Key feature

To enable the Encryption License Key feature:

1. Enable the software license key for the Encryption License Key feature. For instructions, see the *Hitachi Command Suite User Guide* or the *Hitachi Virtual Storage Platform G1000 Mainframe System Administrator Guide*.

If the Encryption License Key software license expires or is missing, you cannot delete the encryption key.

2. Assign the Security Administrator (View & Modify) role to the user who will be enabling or disabling data encryption and back up or restoring keys.

   For details about assigning roles, see the *Hitachi Command Suite User Guide* or the *Hitachi Virtual Storage Platform G1000 Mainframe System Administrator Guide*.

Disabling the Encryption License Key feature

Caution: You must perform steps 1 and 2 in the following procedure before you delete the software license key.

1. Disable data encryption at the parity-group level. For instructions, see Disabling data encryption at the parity-group level on page 4-9.
2. Initialize the connection settings to the key management server. For instructions, see Initialize the connection settings to the key management server on page 4-17.
3. Disable the software license key. For instructions, see the *Hitachi Command Suite User Guide* or the *Hitachi Virtual Storage Platform G1000 Mainframe System Administrator Guide*.

3

Key Management Server Connections

You can use an optional key management server with the Hitachi Virtual Storage Platform G1000. This chapter provides information on setting up the key management server.

- ☐ Key management server requirements
- ☐ Workflow for edit encryption environmental settings

Key management server requirements

The key management server 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

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 expired.

For details 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 details about uploading the client certificates, see Uploading the root and client certificate on page 3-3.

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 details about SafeNet KeySecure, see the SafeNet KeySecure k460 documentation. For details 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 can be from 0 to 128 characters in length. The valid characters for the password are:

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

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

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

Workflow for preparing the client certificate

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 details, 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 details, see Uploading the root and client certificate on page 3-3.

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 details about the client certificate password, see Client certificate password on page 3-2.

Uploading the root and client certificate

Before you configure the connection settings to the key management server, you must 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 (mainframe-only environment):

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.

Workflow for edit encryption environmental settings

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 3-3.
2. Configure the connection settings to the key management server.

   For details, 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 instructions, see the *Hitachi Command Suite User Guide* or the *Hitachi Virtual Storage Platform G1000 Mainframe System Administrator 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 4-4.

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 (mainframe-only environment):
   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 **Task** window to open after you click **Apply**, select **Go to tasks window for status**.

   Click **Apply**.

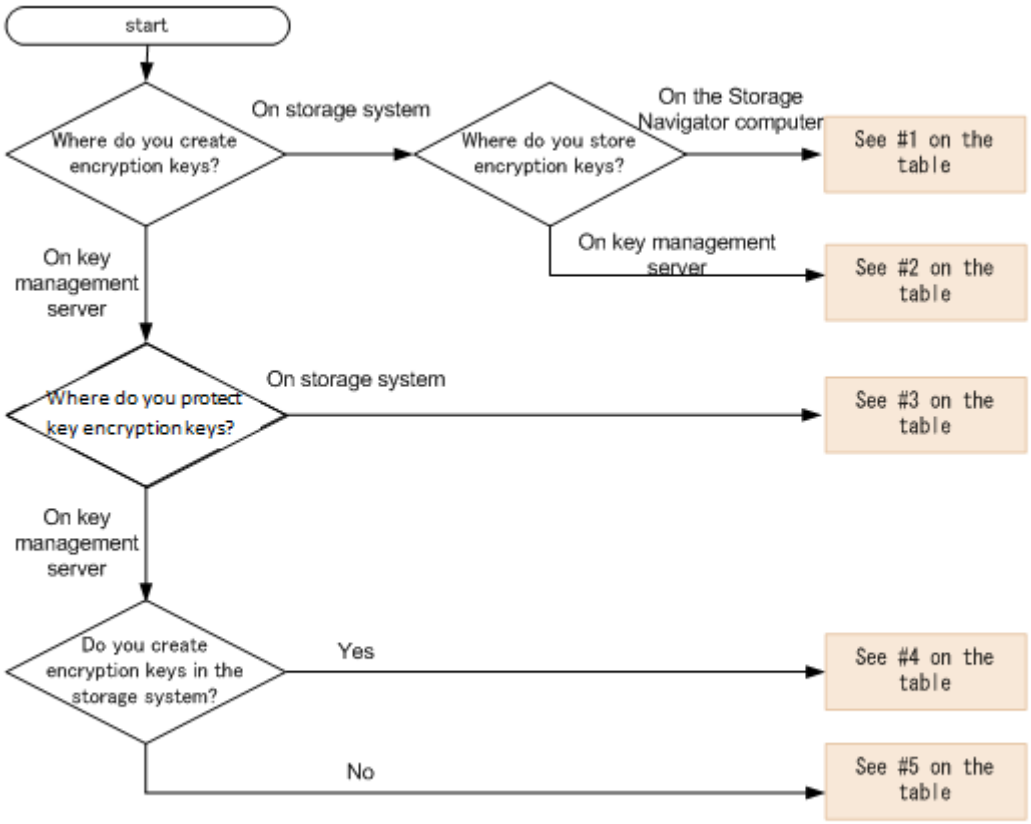
   The connection to the key management server is set up.

Related topics

- Edit Encryption Environmental Settings window on page A-4

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 instructions for managing data encryption license keys using the Encryption License Key feature of the Hitachi Virtual Storage Platform G1000 storage system.

Workflow for creating data encryption license keys

Create a data encryption license key to use with the Encryption License Key feature.

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

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

   For details, see Creating data encryption license keys on page 4-2.
2. Back up the secondary data encryption license key.

   For details, see Workflow for backing up secondary data encryption license keys on page 4-3.
3. Schedule regular weekly backups of all of your data encryption license keys to ensure data availability.

Creating data encryption license keys

If you need to change a data encryption license key, create a new data encryption license key. 4,048 Free keys or DEK keys are created when you configure encryption environmental settings on the **Edit Encryption Environmental Settings** window for the first time (this differs from the configuration. 4,048 keys are created if maximum disk adapters are installed). After that, you can create 4,096 Free keys or DEK keys. You can create up to 4,096 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 strongly 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 (mainframe-only environment):
   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 **Create Keys**.

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 **Task** 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

The Hitachi Virtual Storage Platform G1000 automatically creates a primary backup of the data encryption license key. You can also back up a secondary data encryption license.

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.
- Adding, removing, or replacing drives.
- Adding, removing, or replacing disk adapters.
- Updating CEK keys.
- Updating KEK keys.

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

1. Confirm that the Virtual Storage Platform G1000 is not processing other tasks. You cannot back up a key while the Virtual Storage Platform G1000 is processing other tasks.
2. Use one of the following methods to back up the secondary data encryption license key:
   - Back up the secondary data encryption license key as a file on the HCS management server or HDvM - SN computer.

     For details, see Backing up keys as a file on page 4-4.
   - Back up the secondary data encryption license key to a key management server.

     For details, see Backing up keys to a key management server on page 4-4.

Backing up keys as a file

Back up a secondary data encryption license keys as a file on the 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 (mainframe-only environment):
   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 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 **Task** 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 secondary backup encryption license key is saved.

Related topics

- Encryption Keys window on page A-2
- Backup Keys to File window on page A-15

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 is 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 (mainframe-only environment):
   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 open the **Backup Keys to Server** window.
3. (Optional) In the **Backup Keys to Server** window, for **Description**, type a description and then click **Finish**.
4. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.

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

   Click **Apply**.

   The secondary backup encryption license key is saved.

Related topics

- Encryption Keys window on page A-2
- Backup Keys to Server window on page A-19

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 (mainframe-only environment):
   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 you want to back up from the **Encryption Keys** table, and 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 (mainframe-only environment):
   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. 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 (mainframe-only environment):
   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. In Hitachi Command Suite, you can click **OK**.

   In Device Manager - Storage Navigator, you can click **Finish**.
3. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.

   If you want the **Task** 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-12

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 details, see Workflow for backing up secondary data encryption license keys on page 4-3.
2. Block the LDEVs at the parity-group level.

   For details, see the *Hitachi Virtual Storage Platform G1000 Provisioning Guide for Mainframe Systems* or *Hitachi Virtual Storage Platform G1000 Provisioning Guide for Open Systems*.
3. Enable data encryption on the parity group.

   For details, see Enabling data encryption at the parity group-level on page 4-7.
4. Format the LDEVs at the parity-group level.

   For details, see Workflow for enabling data encryption on parity groups on page 4-7.

Enabling data encryption at the parity group-level

Data encryption is enabled at the parity-group level.

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 (mainframe-only environment):
   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, 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 **Task** 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-30

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 details, see Workflow for backing up secondary data encryption license keys on page 4-3.

2. Block the LDEVs at the parity-group level.

   For details, see the *Hitachi Virtual Storage Platform G1000 Provisioning Guide for Mainframe Systems* or *Hitachi Virtual Storage Platform G1000 Provisioning Guide for Open Systems*.

3. Disable data encryption at the parity-group level.

   For details, see Disabling data encryption at the parity-group level on page 4-9.

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

   For details, see Encryption formatting at the parity-group level on page 4-10.

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.

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 (mainframe-only environment):
   a. Display the Device Manager - Storage Navigator main window.
   b. Select **Storage Systems** in **Explorer**, and select **Parity Groups**.
   c. In the tree that is shown, **Internal** or **External** are displayed.
2. Select the name for the parity group name you want to disable encryption and then click **Edit Encryption**.
3. 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**.

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

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

   Click **Apply**.
6. 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-30

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 cannot be used (for example, due to a system failure).

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 adapters 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.

For details, see the *Hitachi Virtual Storage Platform G1000 Provisioning Guide for Open Systems* or the *Hitachi Virtual Storage Platform G1000 Provisioning Guide for Mainframe Systems*.

2. Restore the data encryption license key from a primary or secondary backup copy. Do one of the following:
   - Restore the data encryption license key from a file backed up on the HCS management server or HDvM - SN computer.

     For details, see Restoring keys from a file on page 4-11.
   - Restore the data encryption license key from the key management server.

     For details, 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 (mainframe-only environment):
   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 **Task** 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 File window on page A-21

Restoring keys from a key management server

Restore a data encryption license key from the key management server. You can restore up to 4,128 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 (mainframe-only environment):
   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 **Task** 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-23

Workflow for deleting data encryption license keys

Delete a data encryption license key from a file on the HCS management server or 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 details, 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-2 and check the key allocation.

3. Delete the data encryption license key using one of the following methods:

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

     For details, see Deleting data encryption license keys on page 4-13.

   - Delete the backup key from the key management server.

     For details, 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 HCS management server or 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 (mainframe-only environment):
   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 key you want to delete from the **Encryption Keys** table, and click **More Actions > Delete Keys**.
3. To back up 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 4-4.
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 **Task** 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.

Related topics

- Delete Keys window on page A-25

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 (mainframe-only environment):
   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, confirm the settings, and enter your task name in **Task Name**.

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

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

   The data encryption license key is deleted.

Related topics

- View Backup Keys on Server window on page A-27
- Delete Backup Keys on Server window on page A-26

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 (mainframe-only environment):
   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-2
- View Backup Keys on Server window on page A-27

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 (mainframe-only environment):
   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**.

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 (mainframe-only environment):
   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 > Rekey Key Encryption Keys**.
4. In the **Rekey Key Encryption Key** window, confirm the settings, and enter your task name in **Task Name**.

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

   Click **Apply**.

Related topics

- Rekey Key Encryption Key window on page A-36

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 (mainframe-only environment):
   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 **Rekey Certificate Encryption Keys**.
3. In the **Rekey Certificate Encryption Keys** window, confirm the settings, and enter your task name in **Task Name**.

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

Click **Apply**.

Related topics

- Rekey Certificate Encryption Keys window on page A-35

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 (mainframe-only environment):
   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 **More Actions > Retry Key Encryption Key Acquisition**.
3. In the **Retry Key Encryption Key Acquisition** window, confirm the settings, and enter your task name in **Task Name**.

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

   Click **Apply**.

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

Related topics

- Retry Key Encryption Key Acquisition window on page A-37

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.

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 (mainframe-only environment):
   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 **Task** 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-4

5

Troubleshooting

This chapter provides troubleshooting information for Encryption License Key.

Troubleshooting for Encryption License Key

For troubleshooting information for the Hitachi Virtual Storage Platform G1000, see the *Hitachi Virtual Storage Platform G1000 Hardware Guide*.

For troubleshooting information for Hitachi Command Suite, see the *Hitachi Command Suite Administrator Guide*. For details about HCS error messages, see *Hitachi Command Suite Messages*.

For troubleshooting information for Device Manager - Storage Navigator, see the *Hitachi Virtual Storage Platform G1000 Mainframe System Administrator Guide*. For details about HDvM - SN error messages, see *Hitachi Command Suite Messages*.

The following table provides general troubleshooting information for Encryption License Key. If you need technical assistance, see Contacting the Hitachi Data Systems Support Center on page 5-3.

Problem	Action
Cannot use the Encryption License Key feature to back up or restore a key.	Verify the following: • 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. • 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.

Problem	Action
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: • Restore the connection to the key management server. • Retry key encryption key acquisition. • Contact the Hitachi Data Systems Support Center to restore the disk adapter and blocked drives or blocked volumes.
Editing encryption environmental settings has failed with the error (00002-058578).	If it is the first time you are configuring encryption environmental settings in the **Edit Encryption Environmental Settings** window and it fails (error message 00002-058578), complete the following tasks: 1. Wait a few minutes, then click **File > Refresh All** to reread the configuration information. 2. Initialize the connection settings to the key management server. 3. Configure the encryption environmental settings again. If it is *not* the first time you are configuring encryption environmental settings in the **Edit Encryption Environmental Settings** window and it fails (error message 00002-058578), complete the following tasks: 1. Wait a few minutes, then click **File > Refresh All** to reread the configuration information. 2. Configure the encryption environmental settings again.

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 messages displayed on the host systems.
- The content of any error messages displayed on Device Manager - Storage Navigator.
- The Device Manager - Storage Navigator configuration information (use the FD Dump Tool).

- The service information messages (SIMs), including reference codes and severity levels, displayed by Device Manager - Storage Navigator.

The Hitachi Data Systems Support Center is available 24 hours a day, seven days a week. If you need technical support, log on to the Hitachi Data Systems Support Portal for contact information: https://portal.hds.com

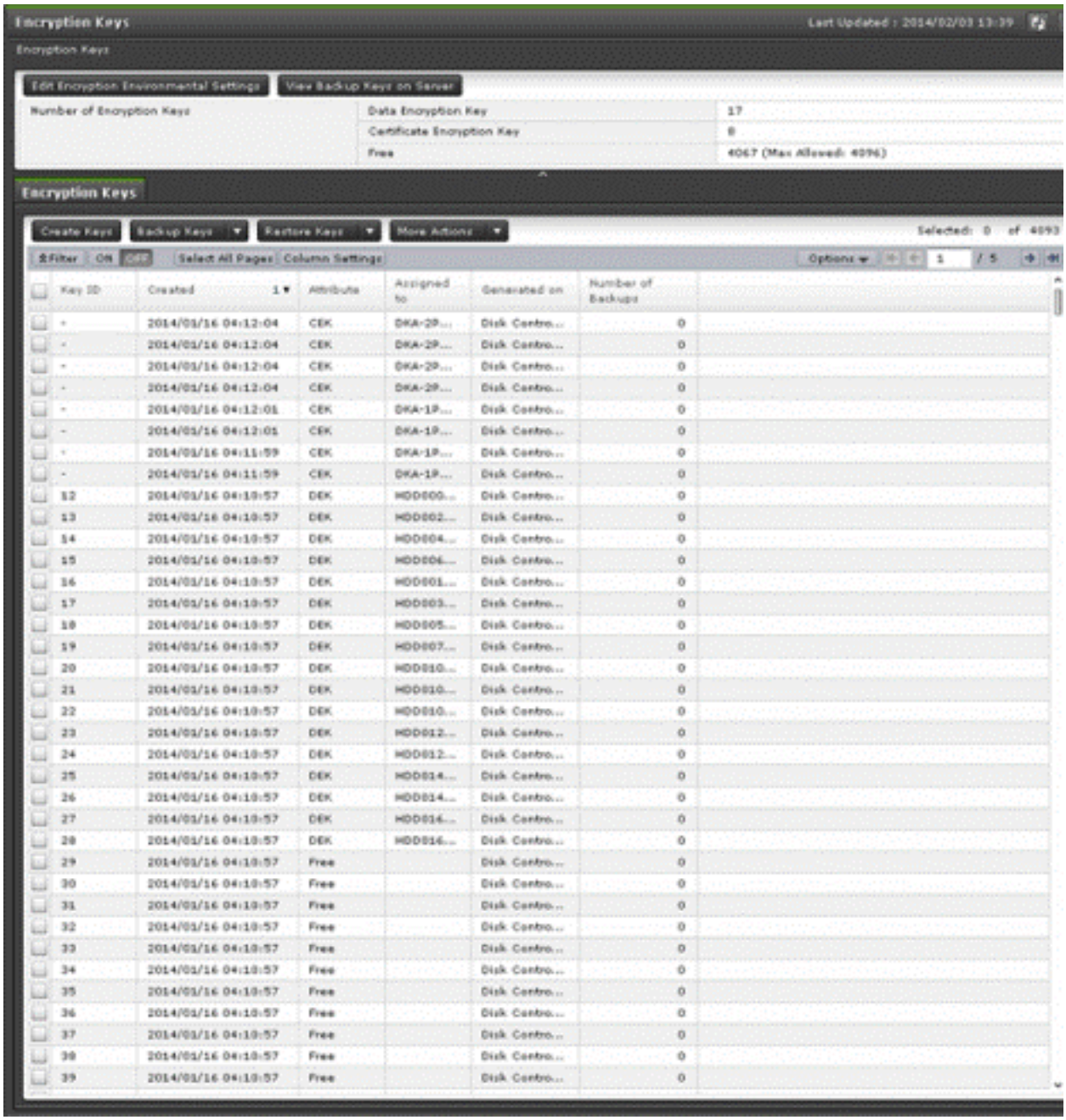
Encryption License Key GUI Reference

This chapter provides descriptions of the Device Manager - Storage Navigator windows and dialog boxes for the Encryption License Key feature.

- ☐ Encryption Keys window
- ☐ Edit Encryption Environmental Settings wizard
- ☐ Create Keys wizard
- ☐ Edit Password Policy (Backup Encryption Keys) wizard
- ☐ Backup Keys to File wizard
- ☐ Backup Keys to Server wizard
- ☐ Restore Keys from file wizard
- ☐ Restore Keys from Server wizard
- ☐ Delete Keys wizard
- ☐ Delete Backup Keys on Server window
- ☐ View Backup Keys on Server window
- ☐ Edit Encryption wizard
- ☐ Rekey Certificate Encryption Keys window
- ☐ 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-2
- Encryption Keys tab on page A-3

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.
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.

Item	Description
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 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 4-4
- 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 4-13
- 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 4-14

Edit Encryption Environmental Settings wizard

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

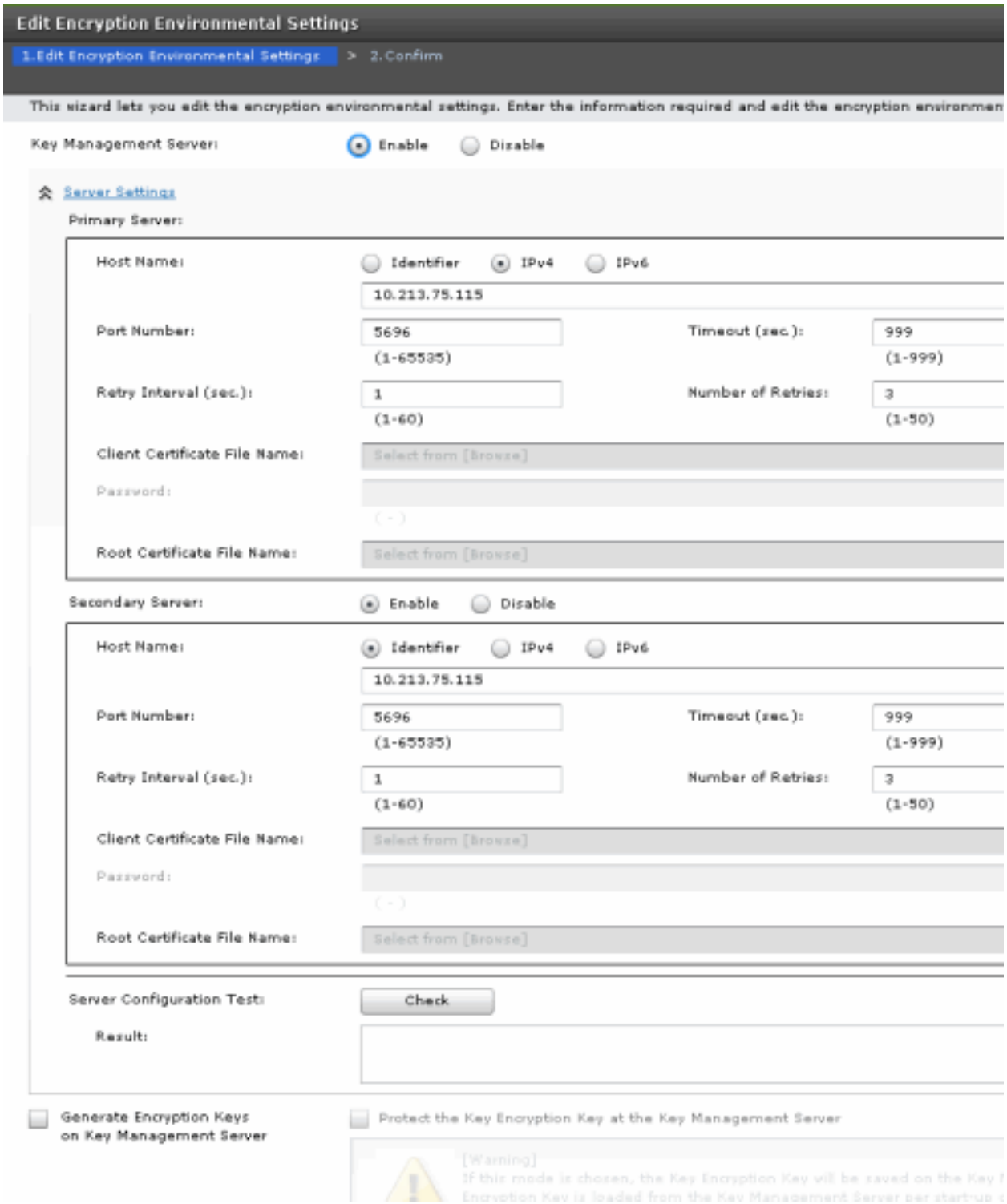
The **Edit Encryption Environmental Settings** wizard includes the following windows:

- Edit Encryption Environmental Settings window on page A-4
- Edit Encryption Environmental Settings confirmation window on page A-8

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.

Item	Description
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. • **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.

Item	Description
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 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.

Edit Encryption Environmental Settings confirmation window

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

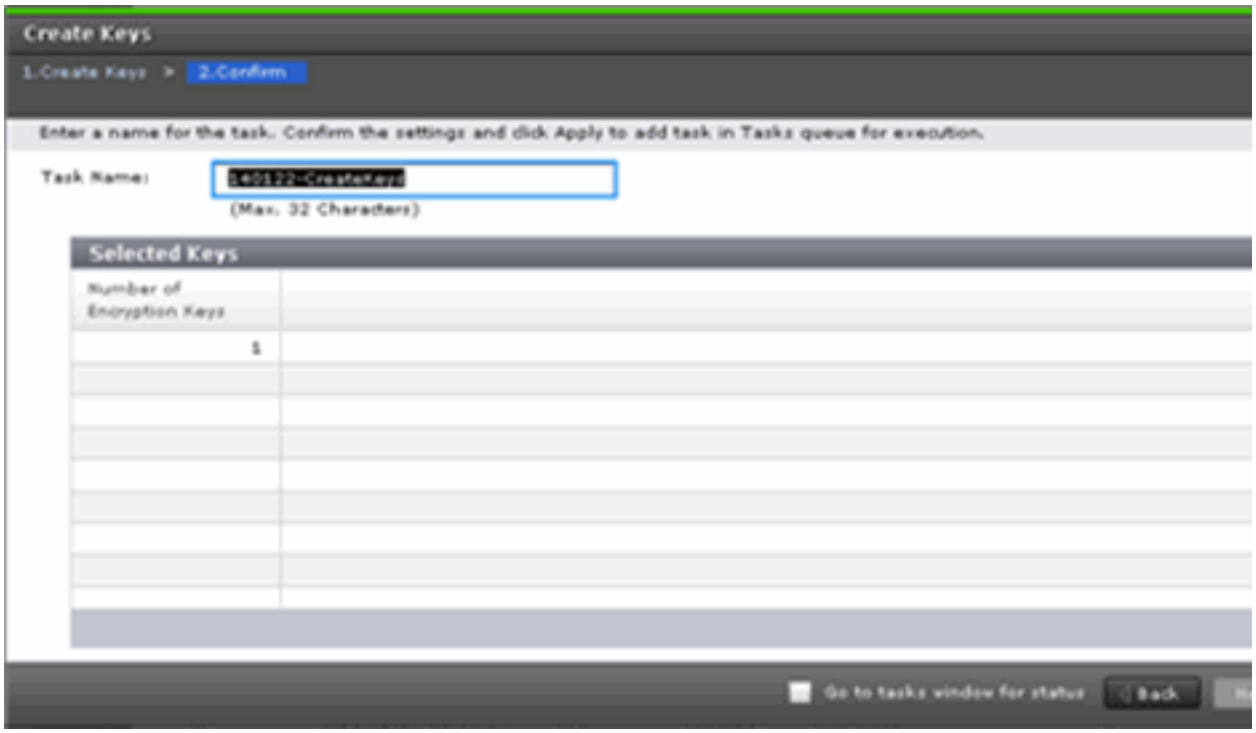
Create Keys window

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 (1-4,096). 4,096 is the maximum number of encryption keys. This window shows the value that subtracted the number of created DEK and Free keys from 4,096.

Create Keys confirmation window

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

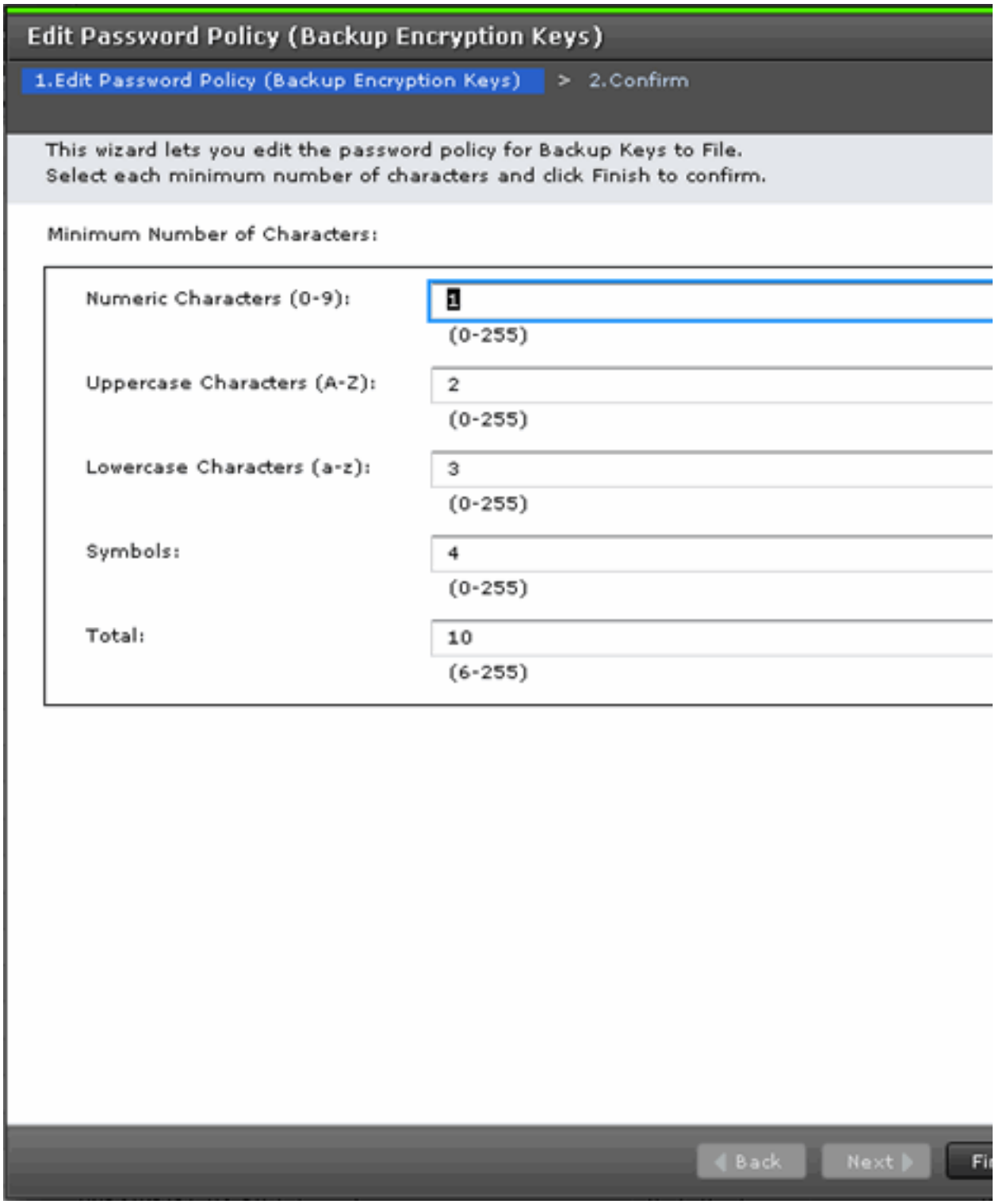
Edit Password Policy (Backup Encryption Keys) wizard

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

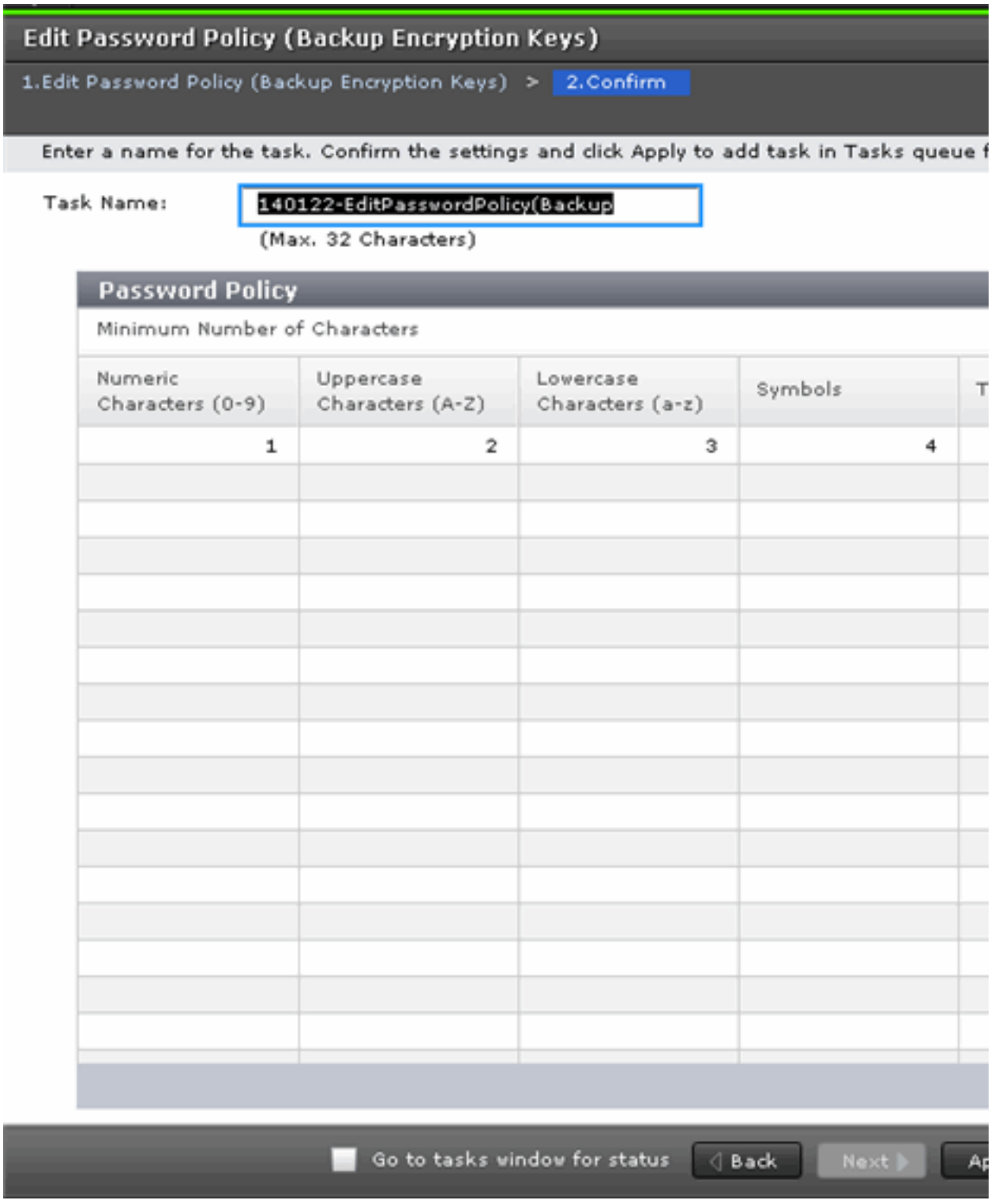
Edit Password Policy (Backup Encryption Keys) window



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

Edit Password Policy (Backup Encryption Keys) confirmation window

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.

Item	Description
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

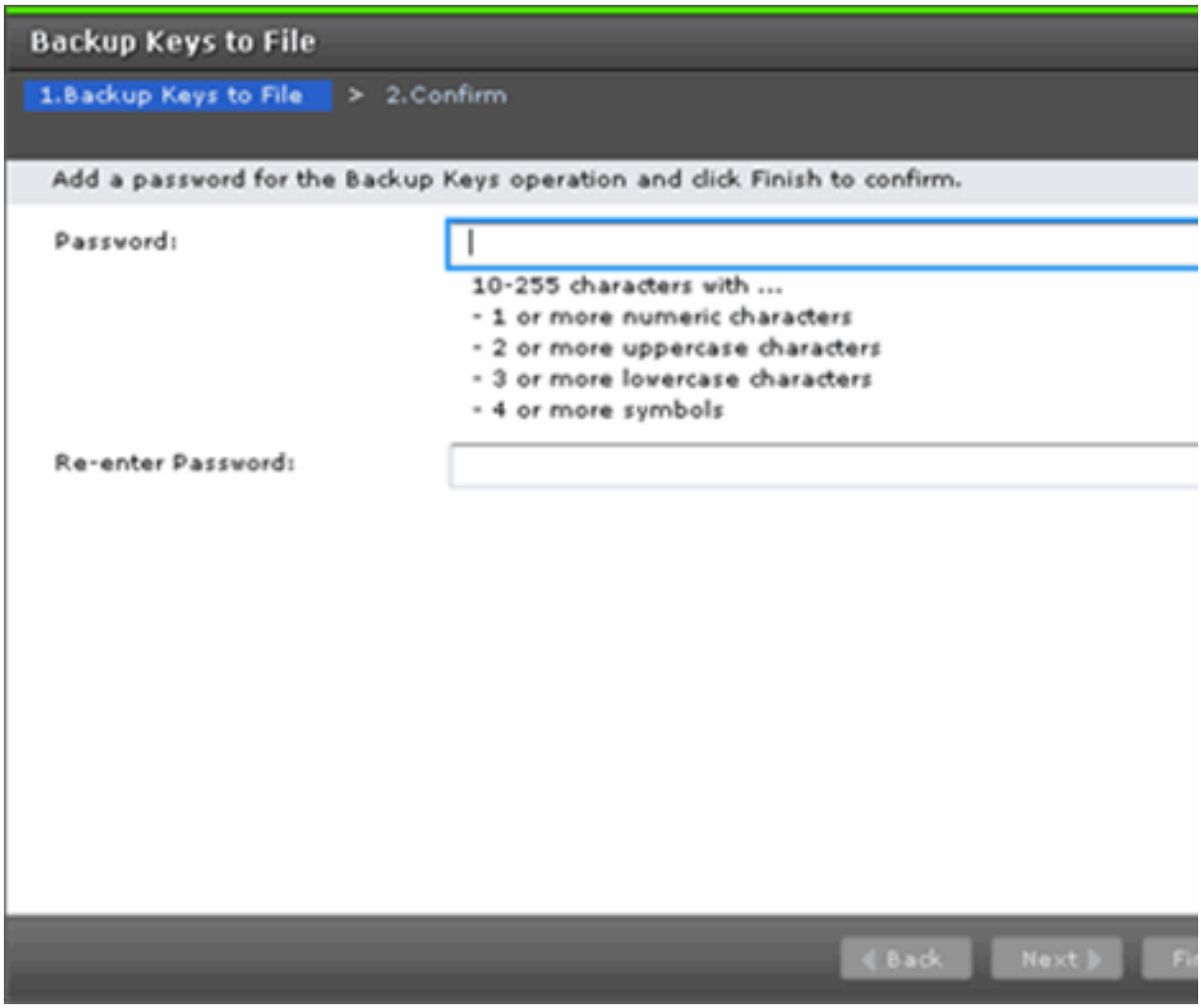
Use the **Backup Keys to File** wizard to create backup data encryption license keys as files on the HCS management server or HDvM - SN computer.

This wizard includes the following windows:

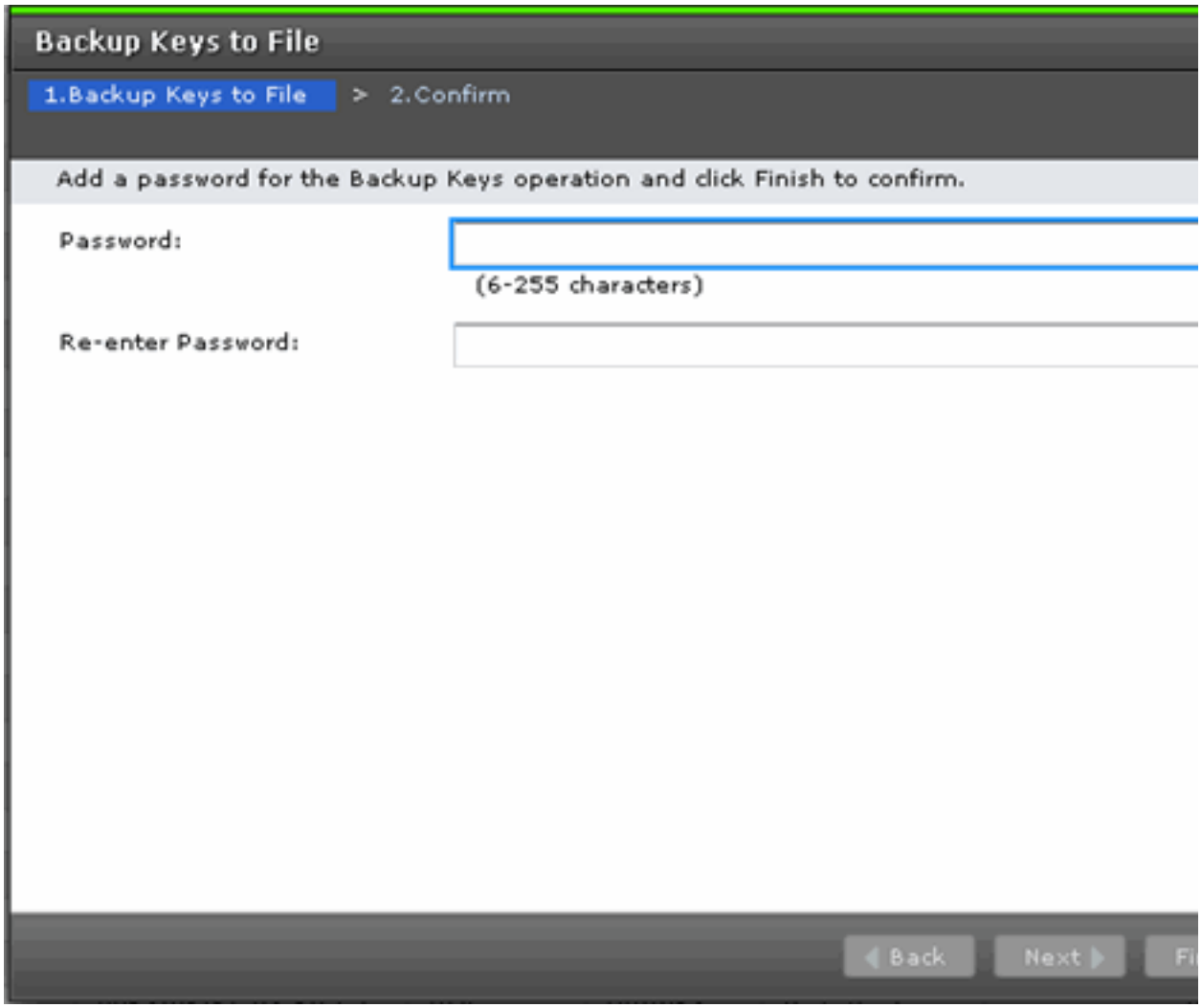
- **Backup Keys to File** window
- **Confirm** window

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.

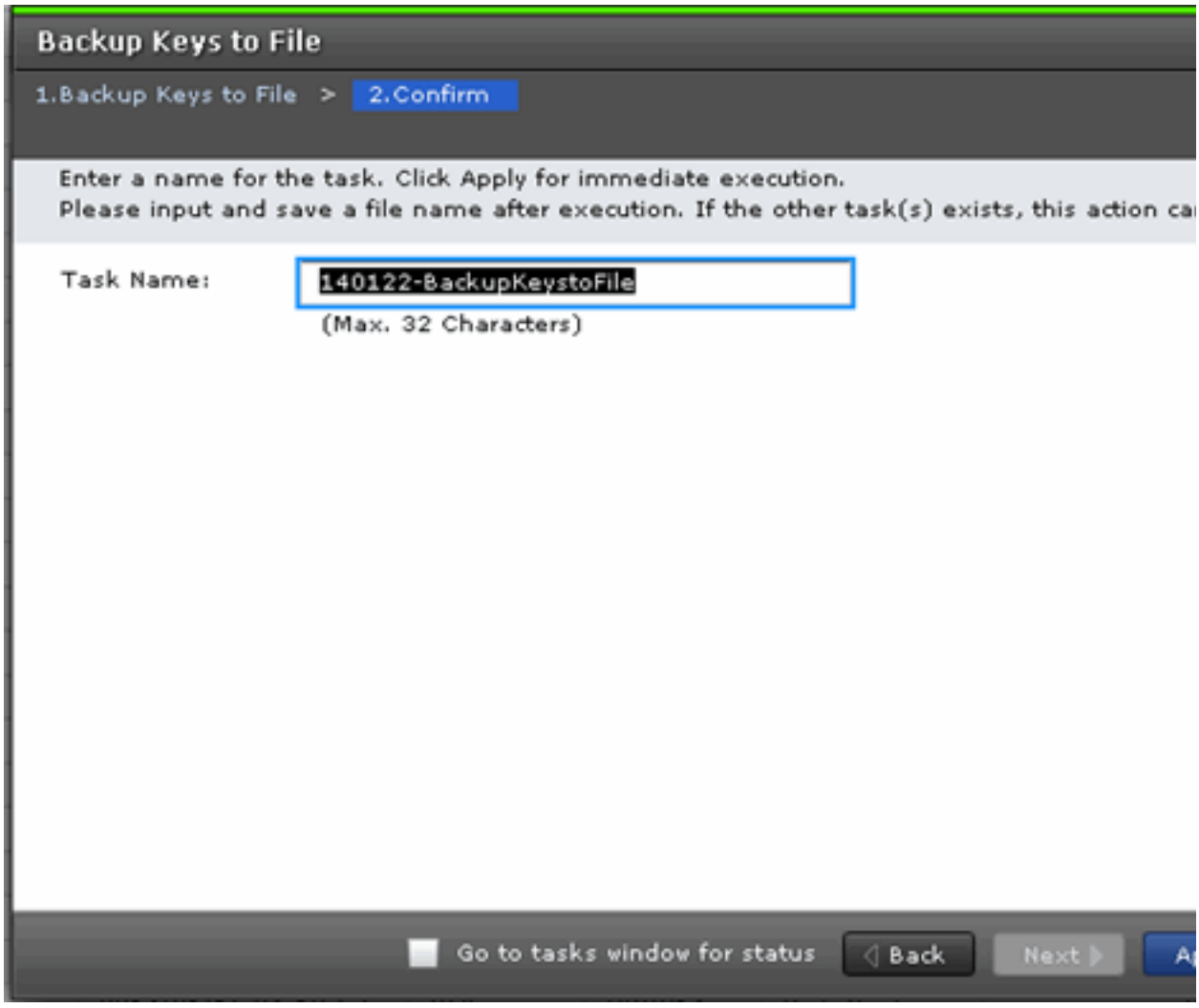


When the password policy is not edited in the **Edit Password Policy (Backup Encryption Keys)** window, you will see the following figure.



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

Backup Keys to File confirmation window



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.

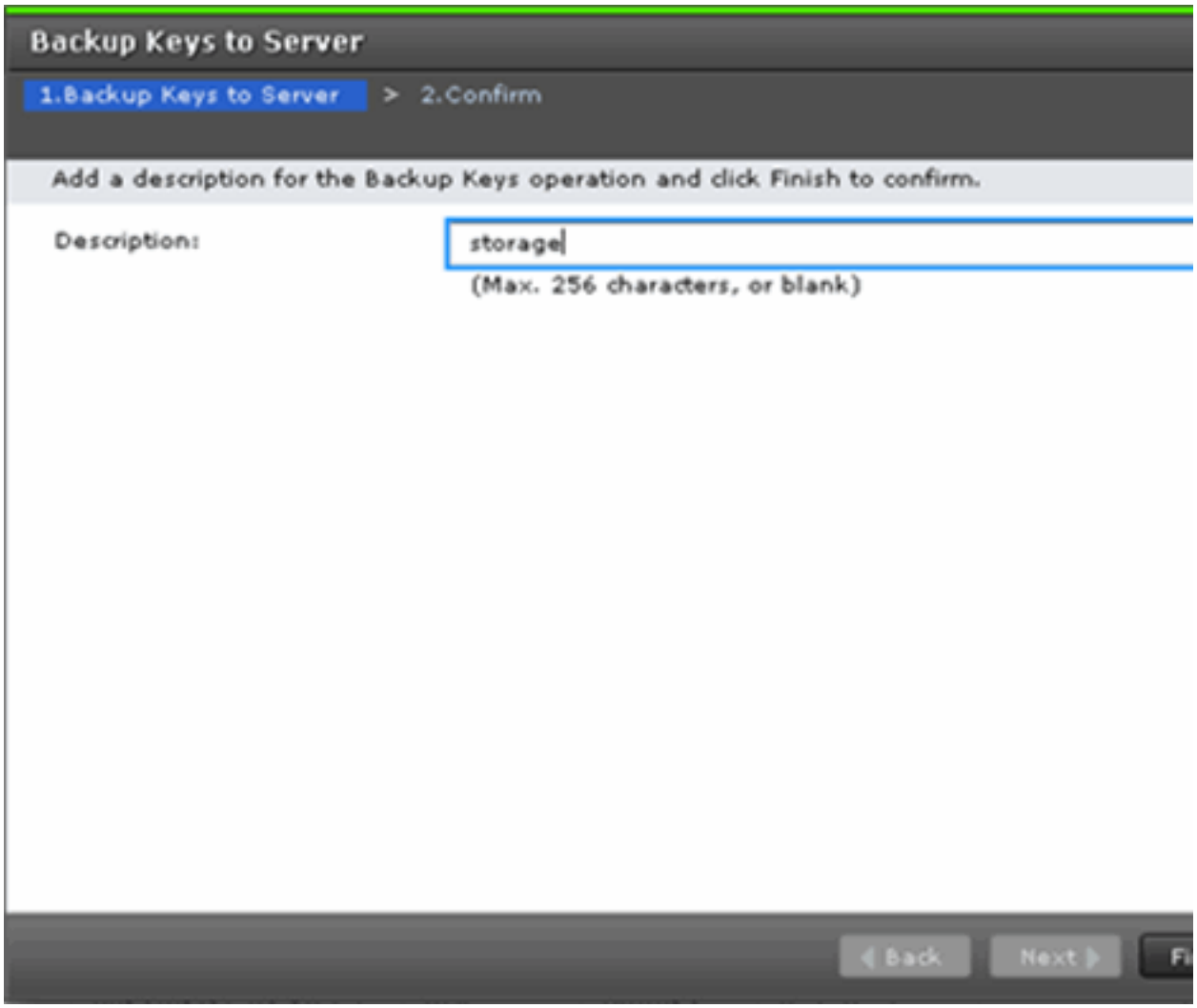
Backup Keys to Server wizard

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

This wizard includes the following windows:

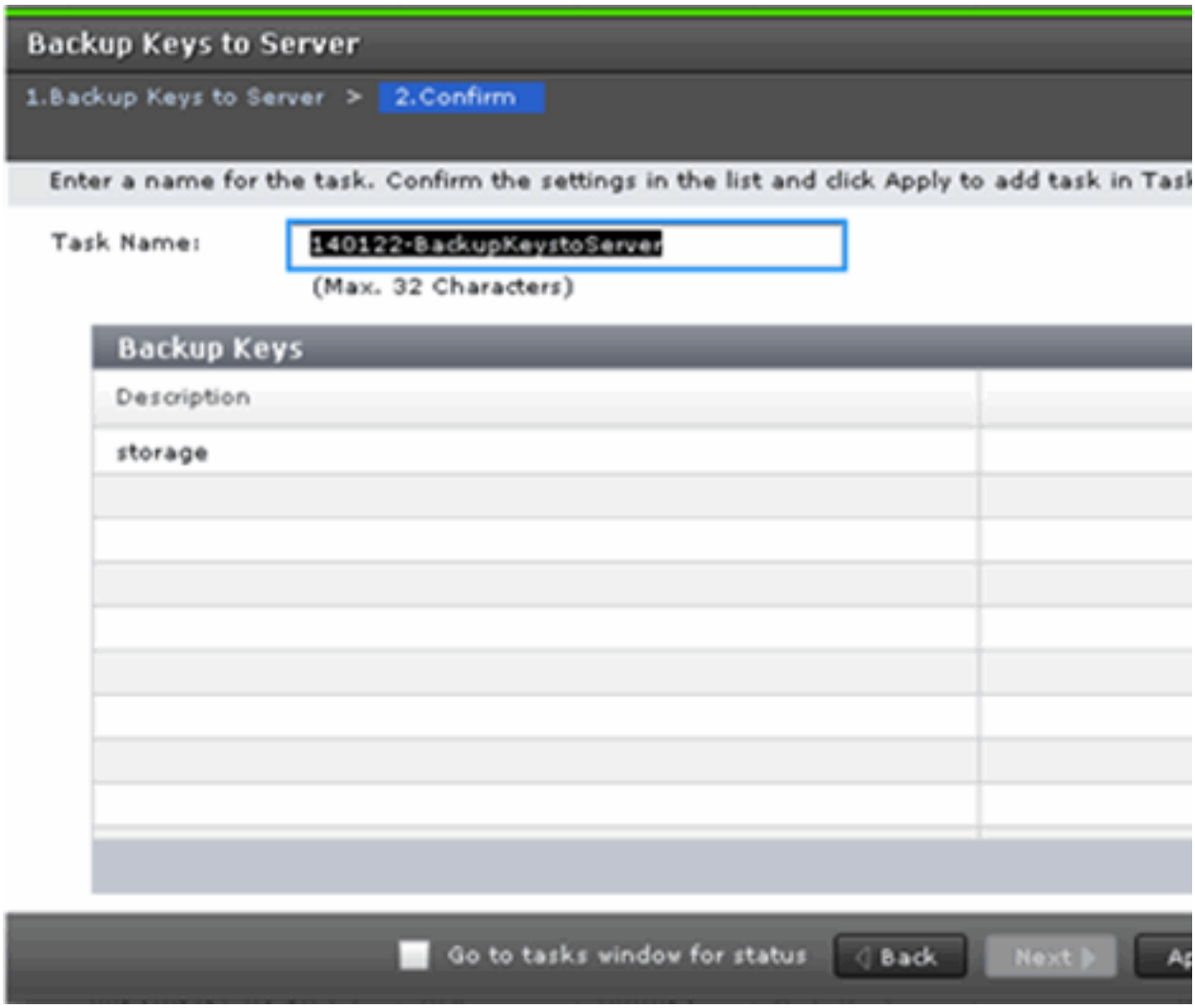
- **Backup Keys to Server** window
- **Confirm** window

Backup Keys to Server window



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

Backup Keys to Server confirmation window



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

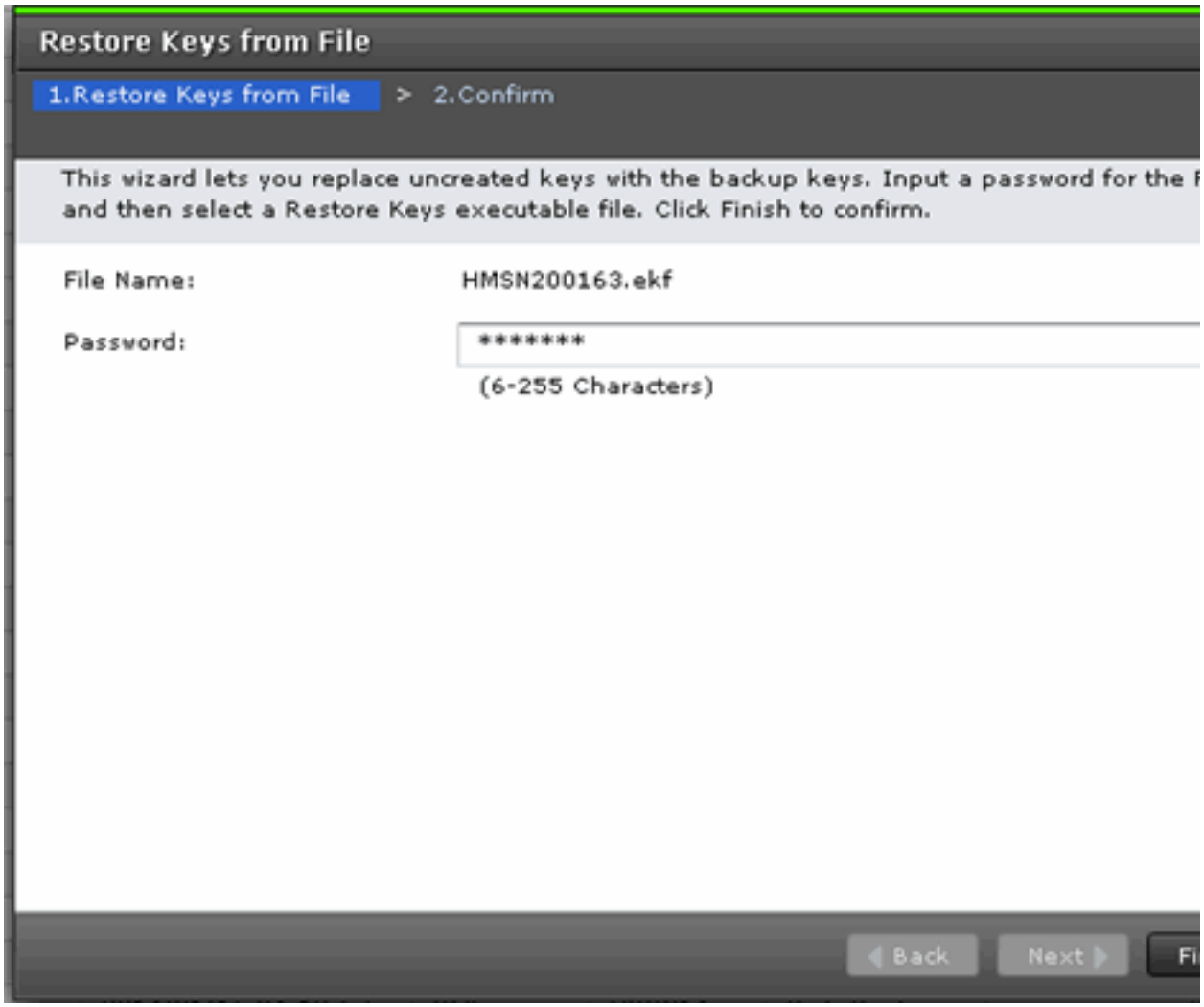
Restore Keys from file wizard

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

This wizard includes the following windows:

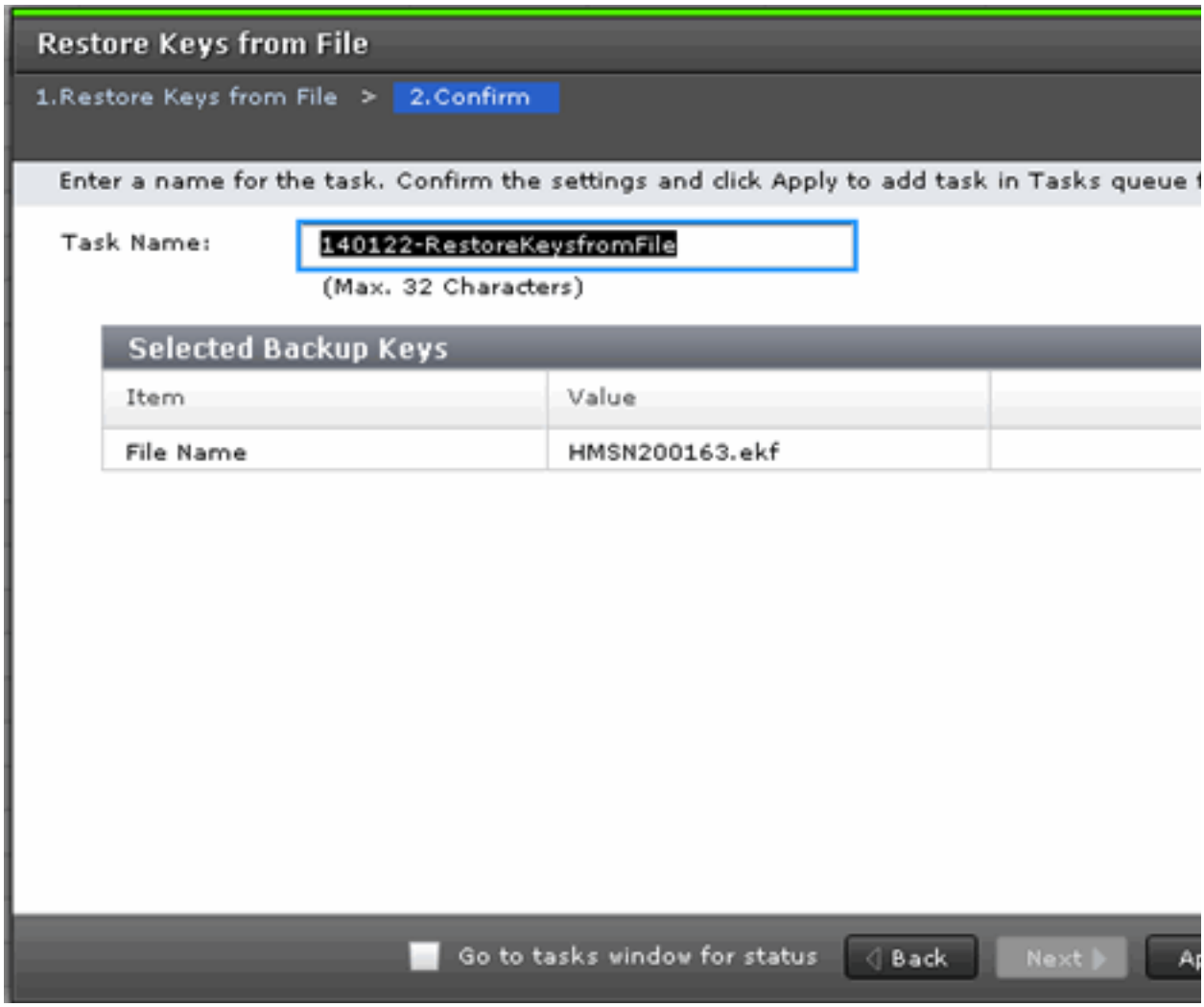
- **Restore Keys from File** window
- **Confirm** window

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.

Restore Keys confirmation window



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

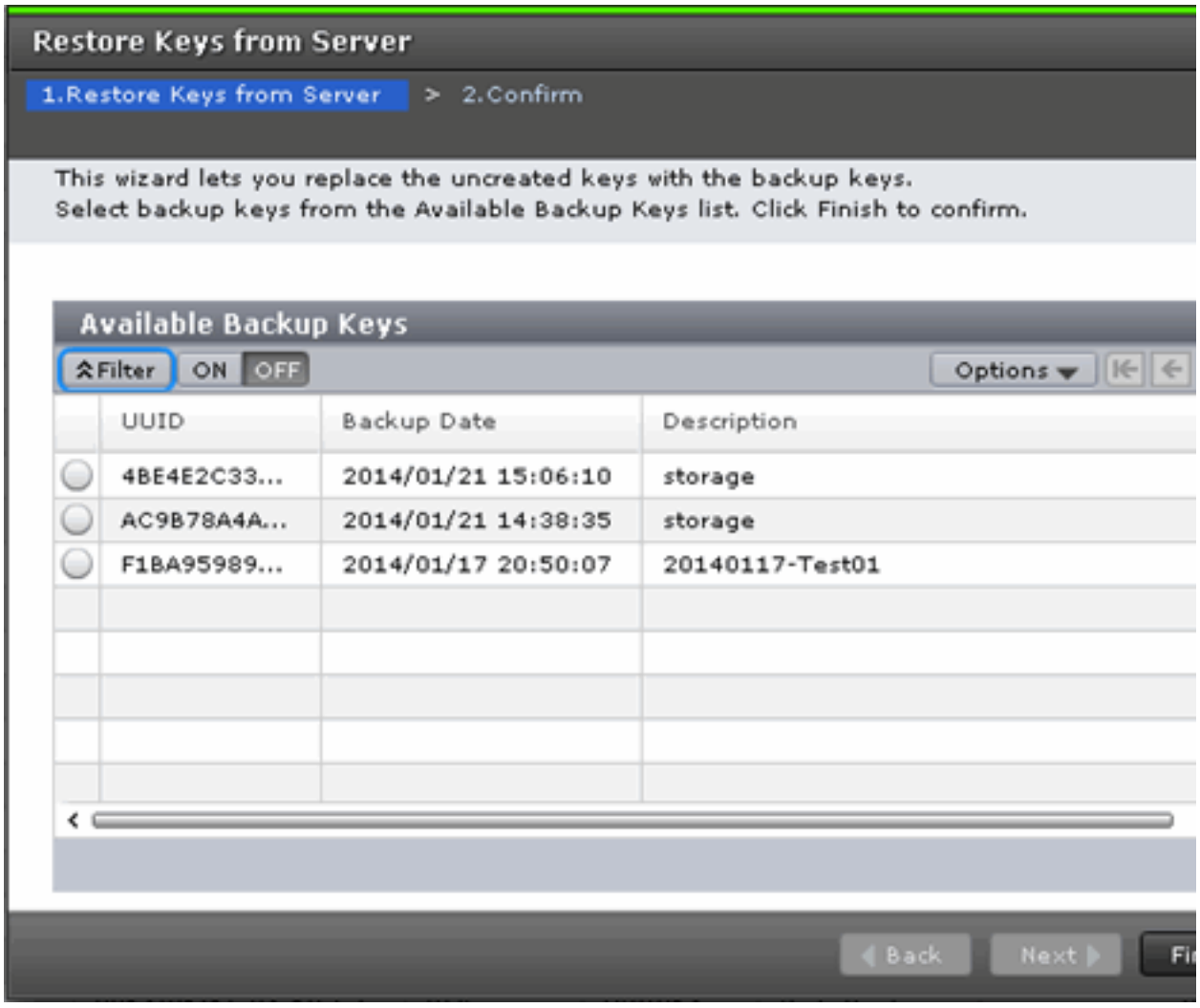
Restore Keys from Server wizard

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

This wizard includes the following windows:

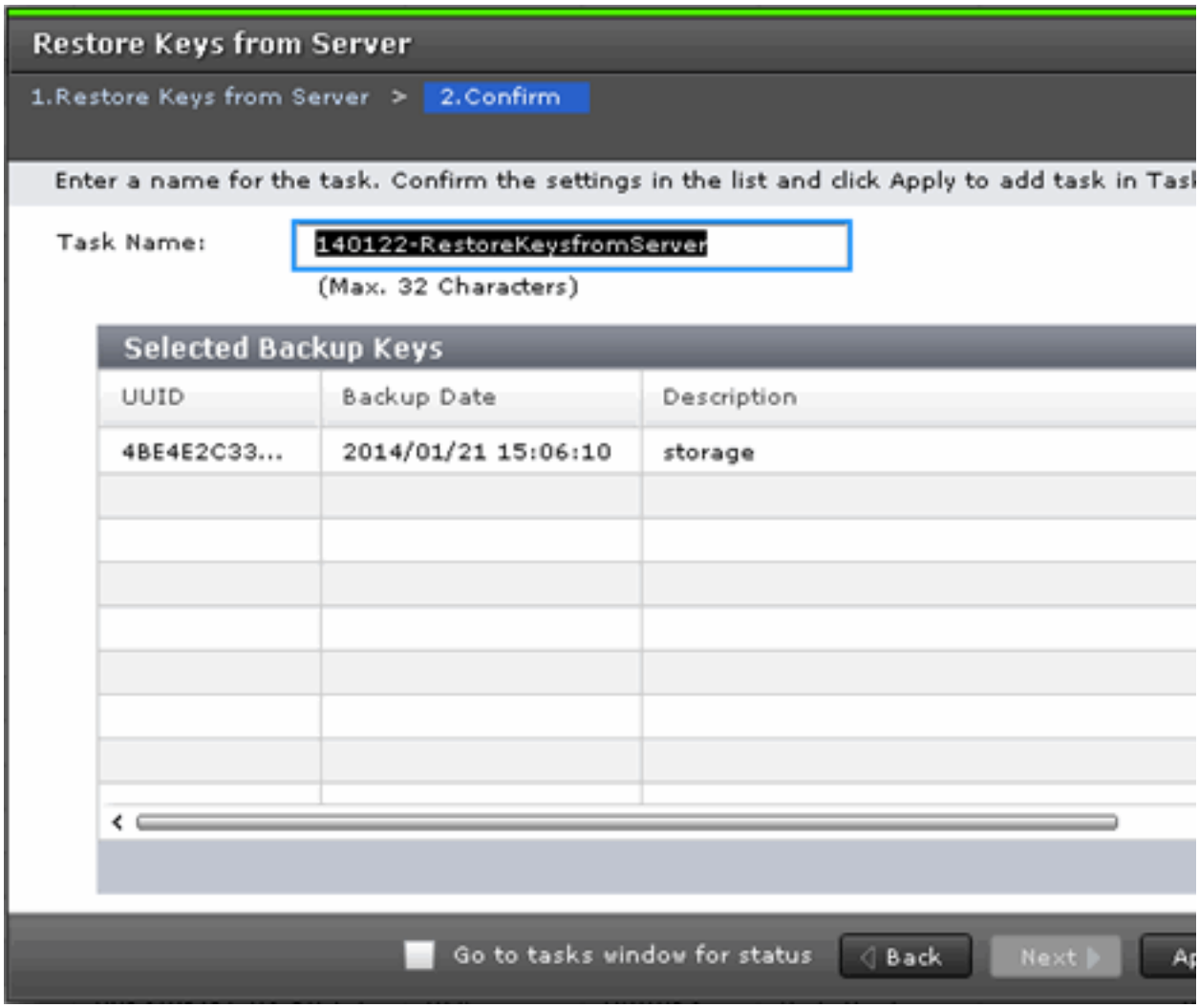
- **Restore Keys from Server** window
- **Confirm** window

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.

Restore Keys from Server confirmation window



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.

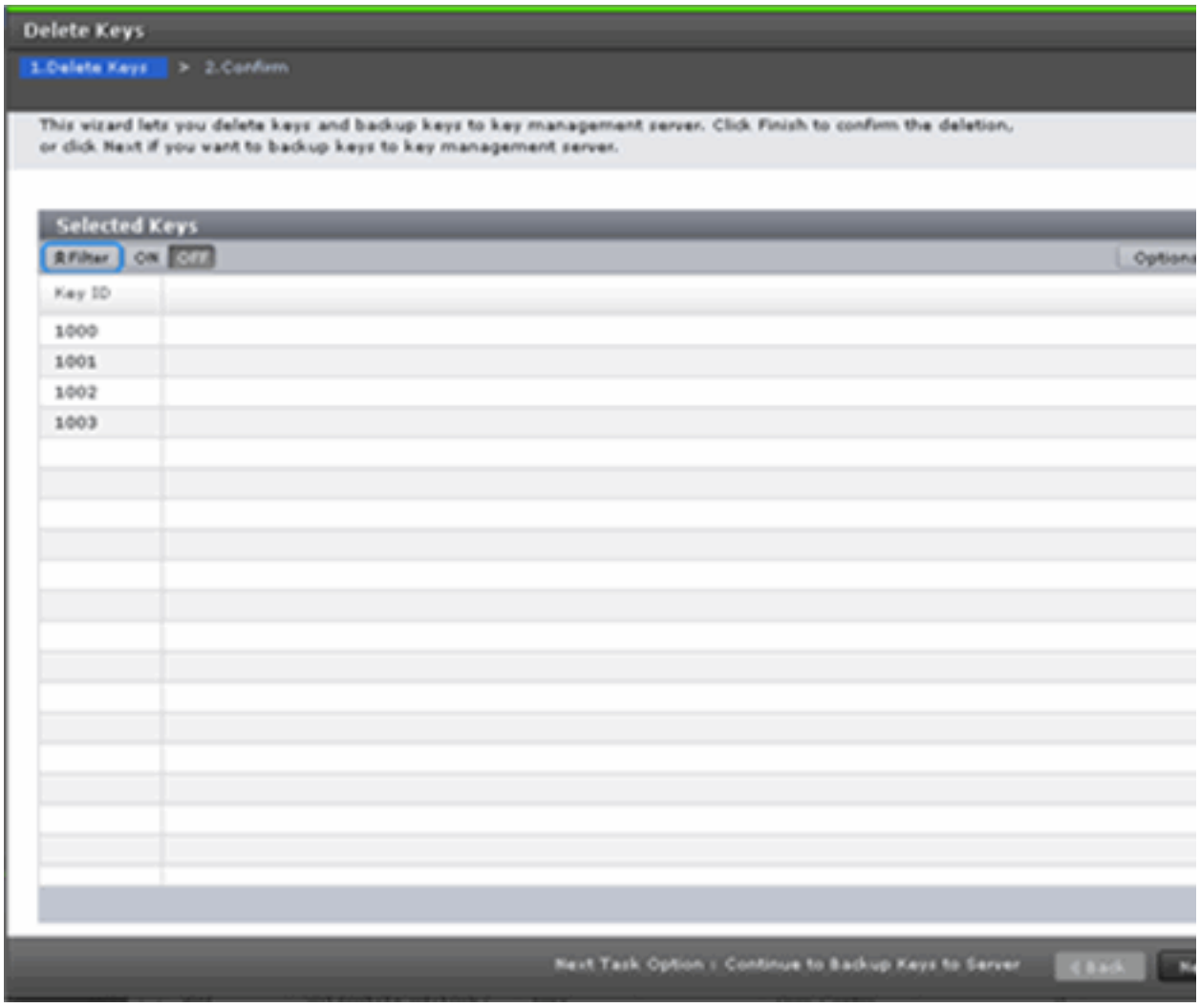
Delete Keys wizard

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

This wizard includes the following windows:

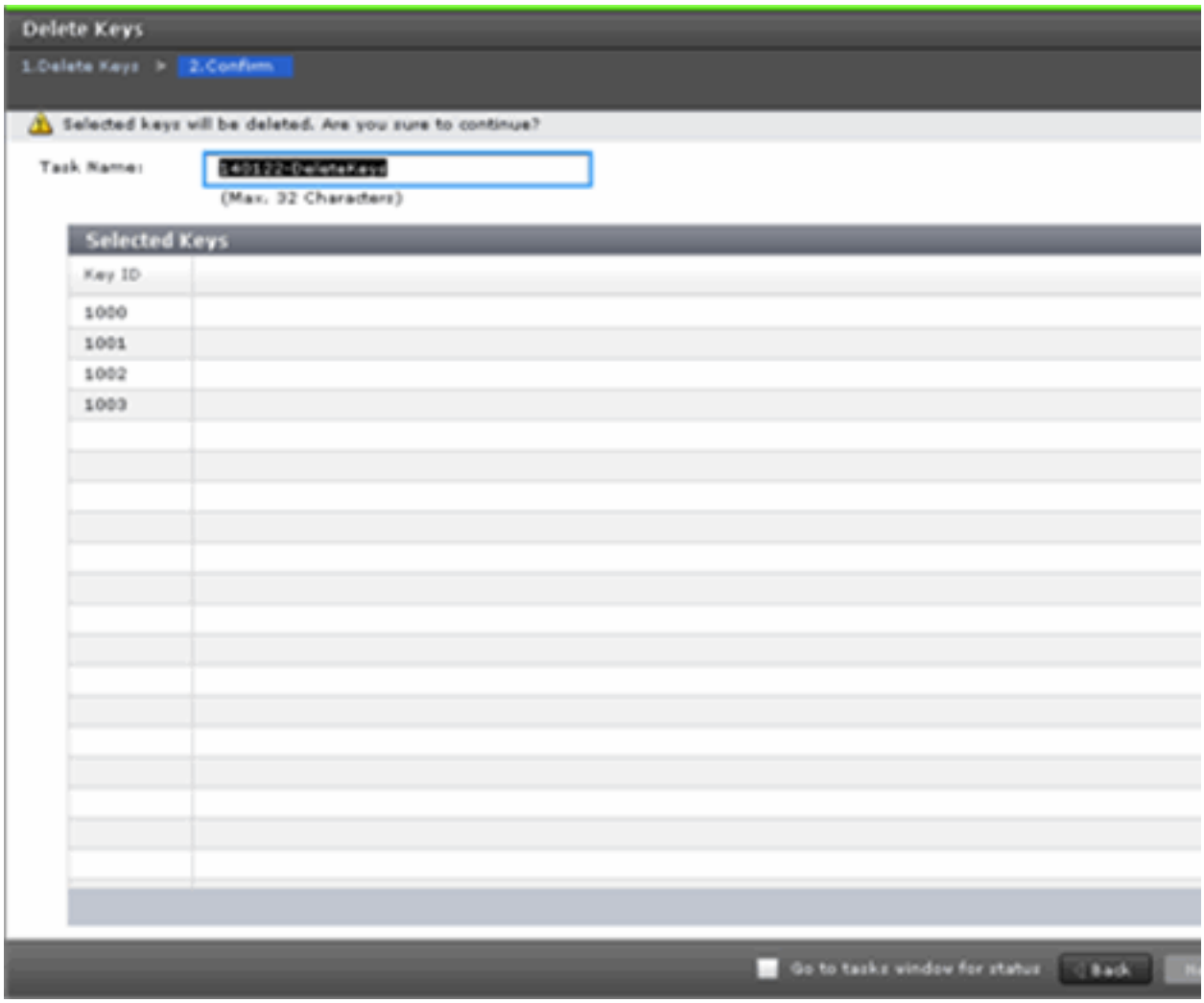
- **Delete Keys** window
- **Confirm** window

Delete Keys window



Item	Description
Key ID	IDs of data encryption license keys.

Delete Keys confirmation window

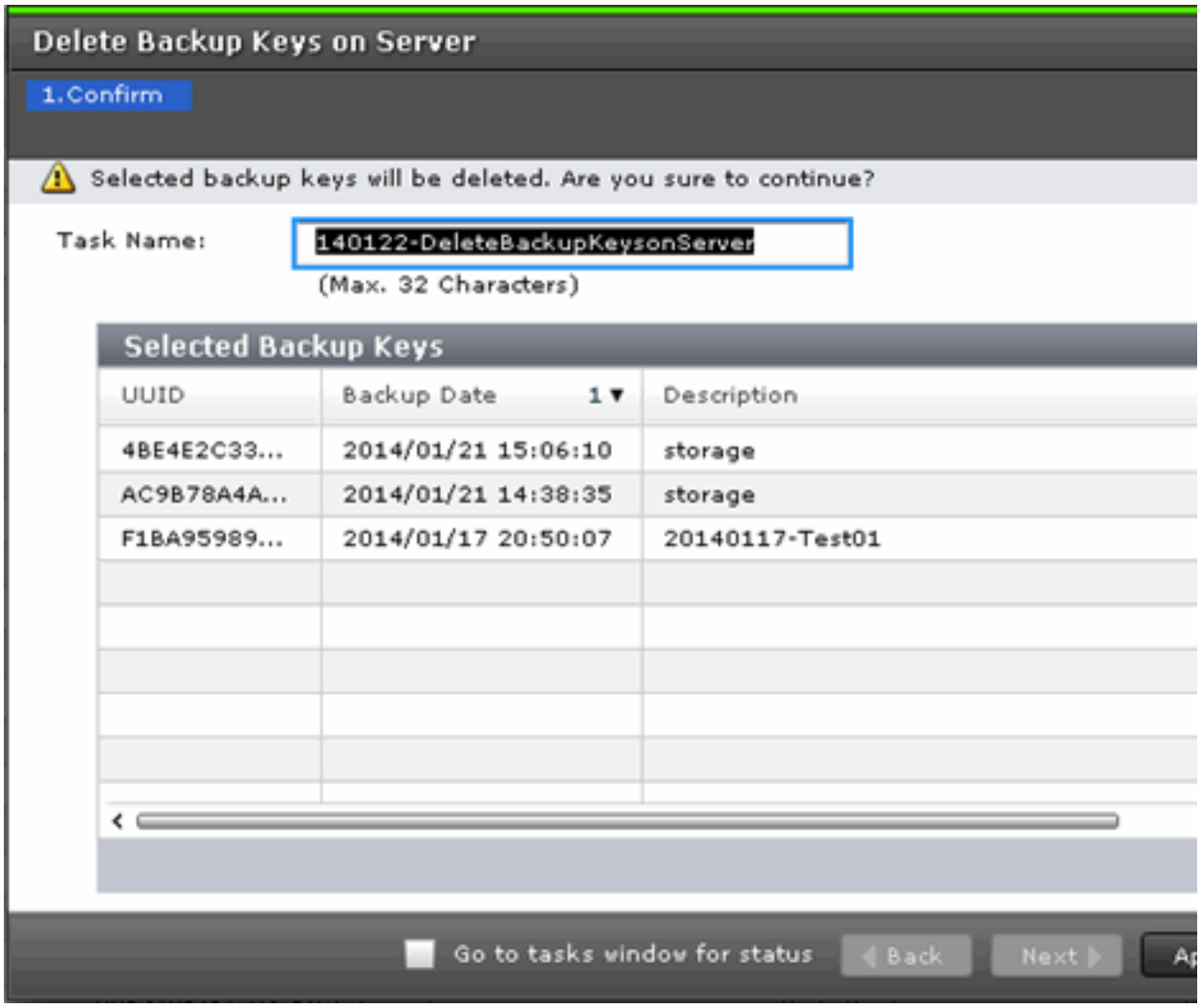


Item	Description
Key ID	The identifiers for the data encryption license keys.

Delete Backup Keys on Server window

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

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

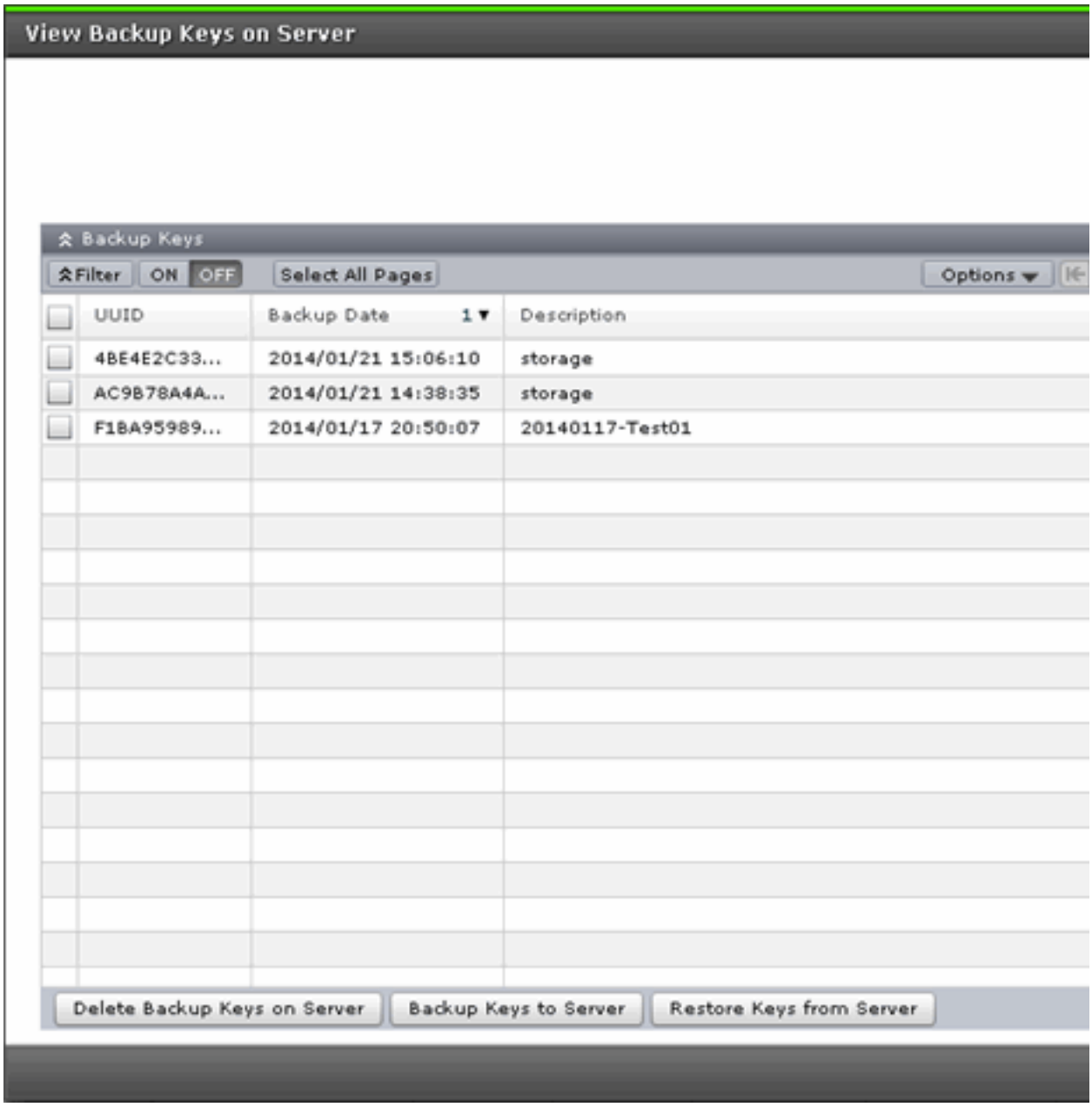


Item	Description
UUID	Shows the UUID of the data encryption license key you backed up on the key management server.
Backup Date	Shows the time when you backed up the data encryption license key on the key management server.
Description	Shows the description you typed when you backed up the data encryption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

Item	Description
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

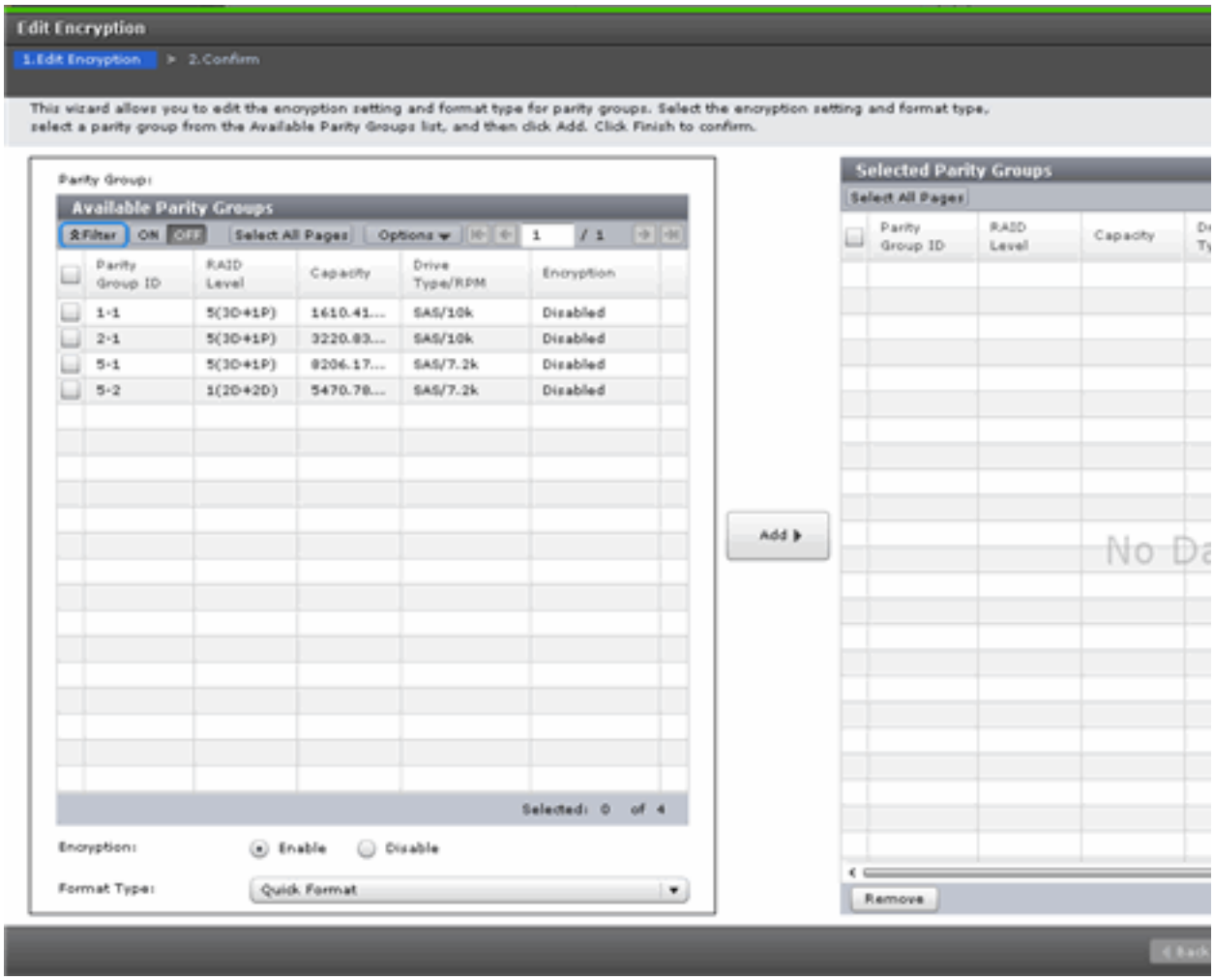
Use the **Edit Encryption** wizard to do the following:

- 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:

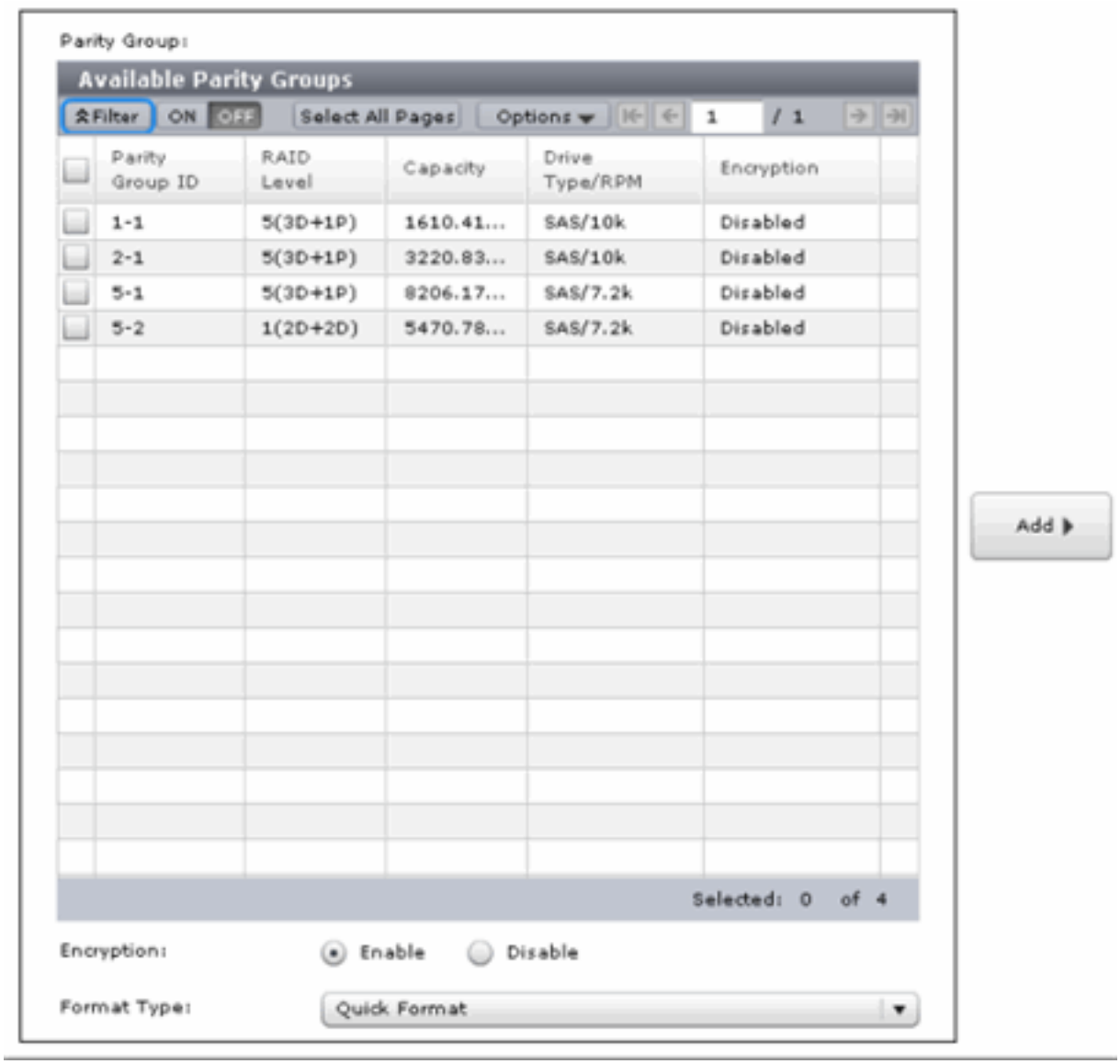
- **Available Parity Groups** table

  For details, see Available Parity Groups table on page A-30.
- **Selected Parity Groups** table

  For details, see Selected Parity Groups table on page A-32.

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.

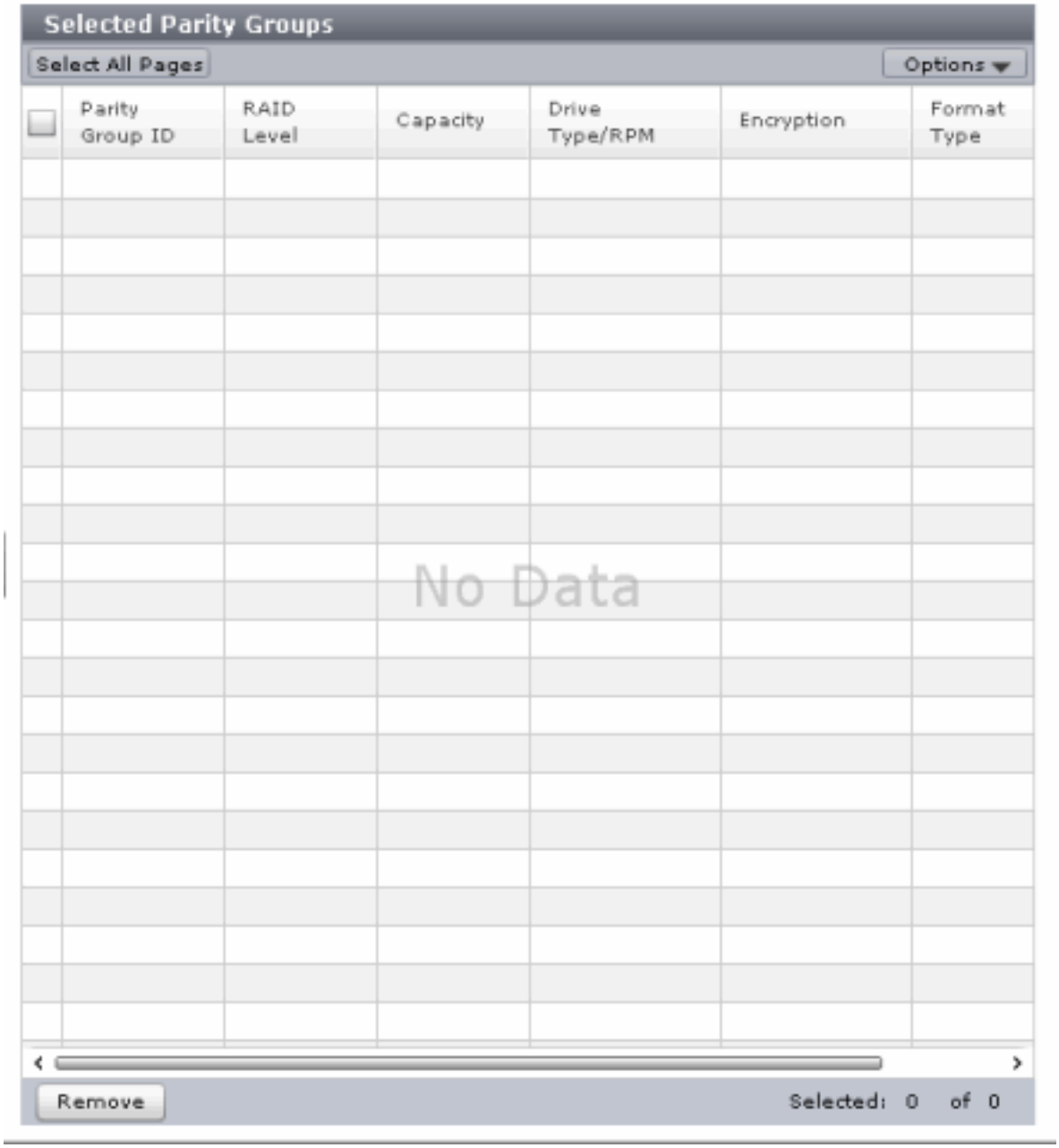
Item	Description
Encryption	Select the encryption setting for the parity group: • If you click **Enable**, data encryption, select will be enabled. • If you click **Disable**, data encryption, select will be disabled.
Format Type	Select the format types of the parity group. You do not need to format volumes when there are none selected in the parity group. Therefore, the format type 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.

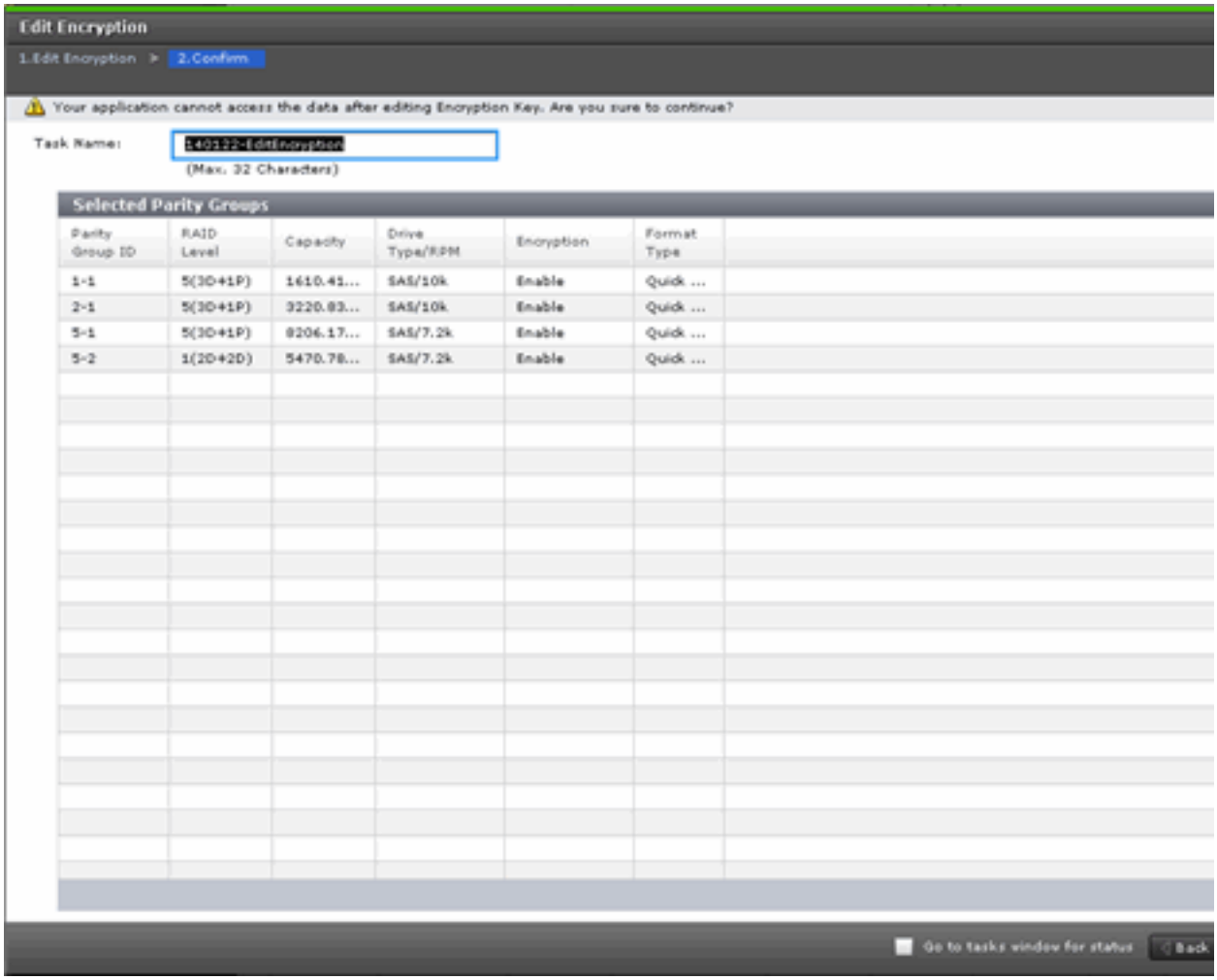


Item	Description
Parity Group ID	Shows parity group IDs.
RAID Level	Shows the RAID level of the parity group. For an interleaved parity group, the interleaved number appears after the RAID level. Example: 1(2D+2D)*2
Capacity	Shows the total capacity (unit) of the parity group.
Drive Type/RPM	Shows the drive types and RPM (rotation per minute) of the LDEV in the parity group.

Item	Description
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.

Edit Encryption confirmation window

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**.

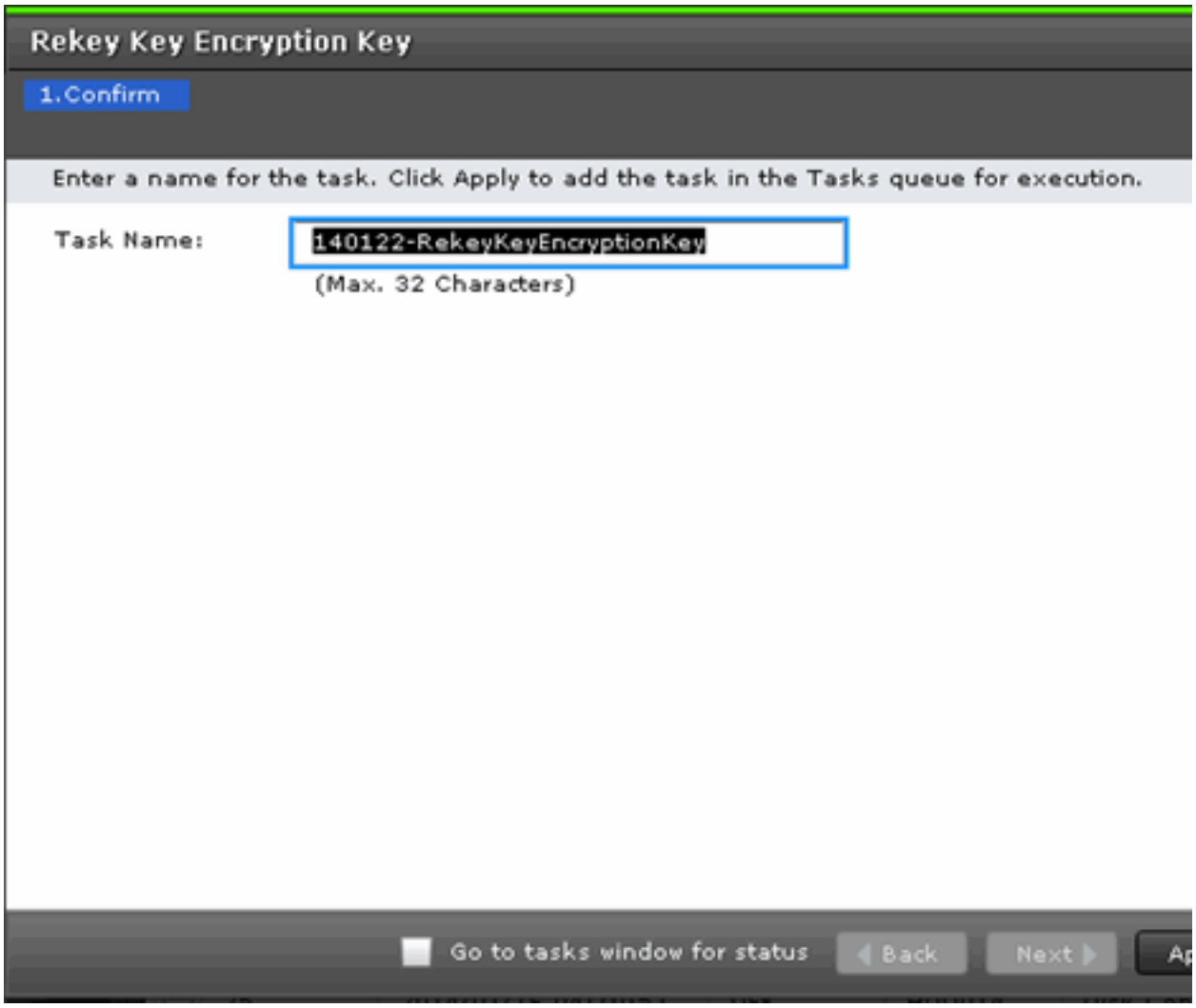
Rekey Certificate Encryption Keys window

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

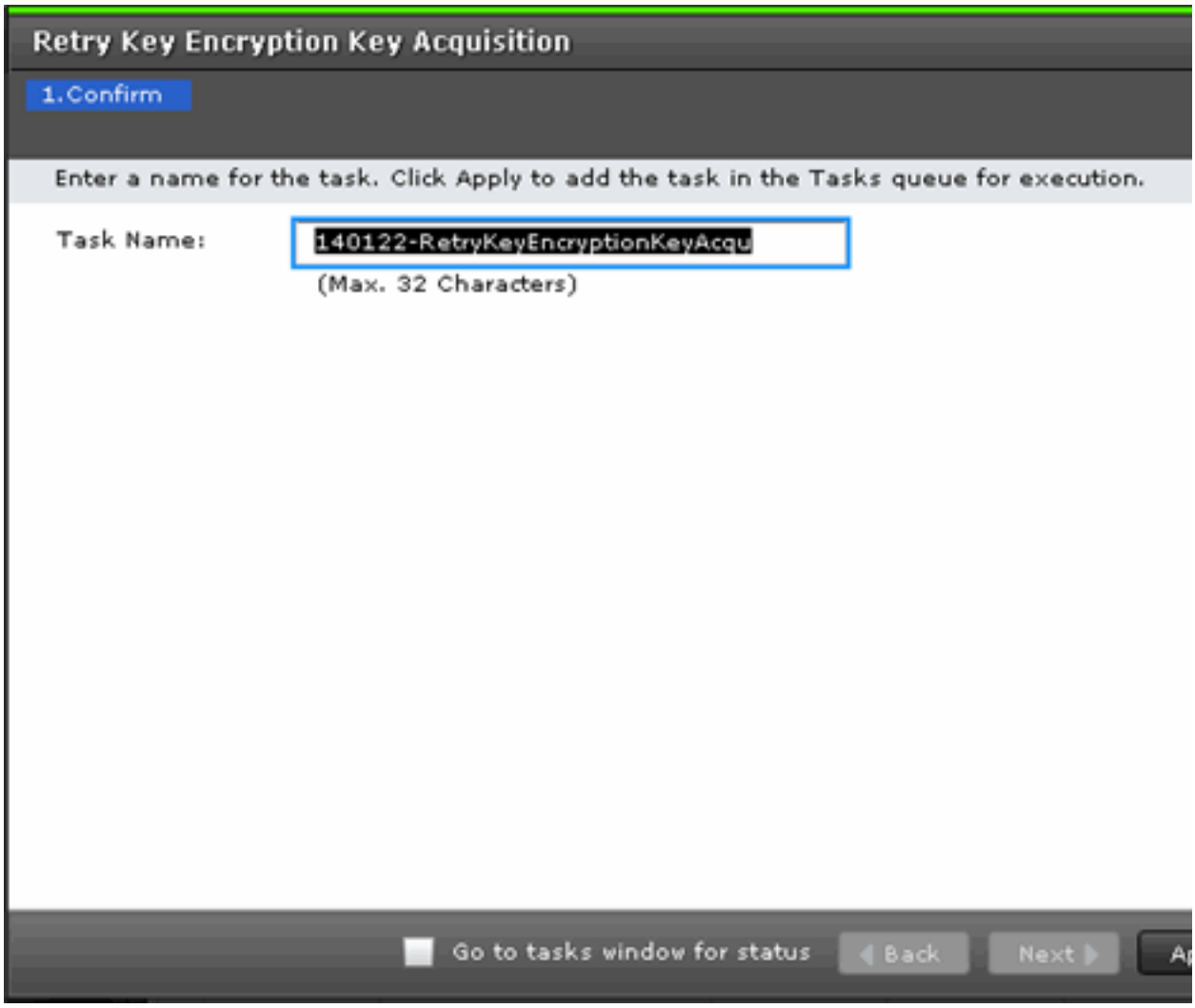
If you change key encryption keys, you can use the **Rekey key Encryption Keys** window to rekey key encryption keys.



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 (for example, OPEN-V, 3390-9).

Encryption Administrator

User role in Hitachi Command Suite and Hitachi Device Manager - Storage Navigator with permission to perform Encryption License Key operations. Compare with *Storage Administrator*.

encryption key

The data encryption license key is used to encrypt and decrypt data on the Hitachi Virtual Storage Platform G1000.

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.

P-VOL

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.

Storage Administrator

User role in Hitachi Command Suite and Hitachi Device Manager - Storage Navigator with permission to perform data encryption operations. Compare with *Encryption Administrator*.

S-VOL

secondary volume (source volume for Hitachi Compatible FlashCopy®)

T

T-VOL

target volume

U

USP V/VM

Hitachi Universal Storage Platform V/VM

V

VSP G1000

Hitachi Virtual Storage Platform G1000

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
750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: 1 408 970 1000
www.hds.com
info@hds.com

Asia Pacific and Americas
750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: 1 408 970 1000
info@hds.com

Europe Headquarters
Sefton Park
Stoke Poges
Buckinghamshire SL2 4HD
United Kingdom
Phone: + 44 (0)1753 618000
info.eu@hds.com

Hitachi Data Systems

MK-92RD8009-02