HITACHI
Inspire the Next

Encryption License Key

User Guide

Htachi Virtual Storage Platform G1000 and G1500

Hitachi Virtual Storage Platform F1500

Hitachi Virtual Storage Platform G200, G400, G600, G800

Hitachi Virtual Storage Platform F400, F600, F800

Hitachi Data Systems

MK-92RD8009-10

October 2016

© 2014, 2016 Hitachi, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Data Systems Corporation (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

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

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

By using this software, you agree that you are responsible for:

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals to access relevant data; and
2. Verifying that data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

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

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

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, IBM, Lotus, MVS, OS/390, PowerPC, RS/6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, the Microsoft Corporate Logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

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

Contents

Preface....7
Intended audience....8
Product version....8
Release notes....8
Changes made in this revision....8
Related documents....8
Document conventions....9
Conventions for storage capacity values....11
Accessing product documentation....11
Getting help....12
Comments....12

1 Encryption License Key Overview....13
Encryption License Key benefits....14
Encryption License Key support specifications....14
When are data encryption keys needed....16
Primary and secondary data encryption keys....16
KMIP key management server support....17
Implementing data encryption....17
How to encrypt existing data....18
Workflow for disabling encryption....18
Workflow for changing the encryption key....18
Audit logging of encryption events....19

2 Encryption License Key installation....21
System requirements....22
Interoperability requirements and considerations....22
Workflow for Encryption License Key installation....23
Enabling the Encryption License Key feature....23
Disabling the Encryption License Key feature....24

3 Key Management Server Connections..... 25
Key management server requirements..... 26
Root and client certificates..... 26
Root certificate on the key management server..... 26
Client certificate password..... 26
Workflow for preparing the client certificate..... 27
Converting the client certificate to the PKCS#12 format..... 27
Uploading the root and client certificate..... 28
Workflow for editing encryption environmental settings..... 28
Configuring the connection settings to the key management server..... 29
Restoring the key management server connection after SVP replacement..... 31
Settings in the Edit Encryption Environmental Settings window..... 31

4 Managing data encryption keys..... 33
Workflow for creating data encryption keys..... 34
Creating data encryption keys..... 34
Workflow for creating secondary backups of the data encryption keys..... 35
Backing up the keys as a file..... 36
Backing up the keys to a key management server..... 37
Changing the password requirements for the backup encryption keys..... 38
Opening the Backup Keys to Server window using the Encryption window..... 39
Opening the Backup Keys to Server window using the View Backup Keys on Server window..... 39
Viewing encryption keys backed up on the key management server..... 39
Workflow for enabling data encryption..... 40
Enabling data encryption..... 40
Workflow for disabling data encryption..... 42
Disabling data encryption..... 42
Formatting V-VOLs for unencryption..... 43
Encryption formatting at the parity-group level 44
Workflow for restoring data encryption keys..... 44
Restoring keys from a file..... 45
Restoring keys from a key management server..... 46
Workflow for deleting data encryption keys..... 47
Deleting data encryption keys..... 47
Deleting backup data encryption keys from the server..... 48
Exporting encryption key table information..... 49
Rekeying key encryption keys..... 49
Rekeying certificate encryption keys..... 50
Retrying Key Encryption Key Acquisition..... 51
Initializing the encryption environment settings..... 52

5 Troubleshooting..... 53
Encryption events in the audit log..... 54
Troubleshooting for Encryption License Key..... 54
Contacting customer support..... 56

A Encryption License Key GUI Reference..... 57
Encryption Keys window..... 58

Edit Encryption Environmental Settings wizard....60
Edit Encryption Environmental Settings window....60
Edit Encryption Environmental Settings confirmation window....63
Create Keys wizard....64
Create Keys window....65
Create Keys confirmation window....65
Edit Password Policy (Backup Encryption Keys) wizard....66
Edit Password Policy (Backup Encryption Keys) window....66
Edit Password Policy (Backup Encryption Keys) confirmation window....68
Backup Keys to File wizard....70
Backup Keys to File window....70
Backup Keys to File confirmation window....71
Backup Keys to Server wizard....72
Backup Keys to Server window....72
Backup Keys to Server confirmation window....73
Restore Keys from File wizard....74
Restore Keys from File window....74
Restore Keys confirmation window....75
Restore Keys from Server wizard....76
Restore Keys from Server window....76
Restore Keys from Server confirmation window....77
Delete Keys wizard....78
Delete Keys window....78
Delete Keys confirmation window....79
Delete Backup Keys on Server window....80
View Backup Keys on Server window....81
Edit Encryption wizard....83
Edit Encryption window....83
Edit Encryption confirmation window....86
Rekey Certificate Encryption Keys window....87
Rekey Key Encryption Key window....88
Retry Key Encryption Key Acquisition window....88

Glossary....91

Index....113

Preface

This document describes and provides instructions for Encryption License Key, a feature of the VSP G series or VSP F series systems.

Please read this document carefully to understand how to use these products, and maintain a copy for your reference.

- ☐ Intended audience
- ☐ Product version
- ☐ Release notes
- ☐ Changes made in this revision
- ☐ Related documents
- ☐ Document conventions
- ☐ Conventions for storage capacity values
- ☐ Accessing product documentation
- ☐ Getting help
- ☐ Comments

Intended audience

This document is intended for system administrators, Hitachi Data Systems representatives, and authorized service providers who install, configure, and operate Hitachi Virtual Storage Platform G200, G400, G600, G800, Hitachi Virtual Storage Platform F400, F600, F800, or VSP G1000, G1500, and VSP F1500 storage systems.

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 G200, G400, G600, G800, Hitachi Virtual Storage Platform F400, F600, F800, and VSP G1000, G1500, and VSP F1500 storage systems and the *Product Overview*.
- The Hitachi Device Manager - Storage Navigator software and the *Hitachi Command Suite User Guide*.
- The concepts and functionality of storage provisioning operations.

Product version

This document revision applies to:

- VSP G200, G400, G600, G800, VSP F400, F600, F800 firmware 83-04-0*x* or later
- VSP G1000, G1500, and VSP F1500 microcode 80-05-0*x* or later
- SVOS 7.0 or later

Release notes

Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document. Release notes are available on Hitachi Data Systems Support Connect: https://knowledge.hds.com/Documents.

Changes made in this revision

- Added support for VSP G1500and VSP F1500.

Related documents

Hitachi VSP G series and VSP F series documents:

- *Product Overview*, MK-94HM8013

- *Hitachi Virtual Storage Platform G200 Hardware Reference Guide*, MK-94HM8020
- *Hitachi Virtual Storage Platform G400, G600 Hardware Reference Guide*, MK-94HM8022
- *Hitachi Virtual Storage Platform G800 Hardware Reference Guide*, MK-94HM8026
- *Hitachi Virtual Storage Platform F400, F600 Hardware Reference Guide*, MK-94HM8045
- *Hitachi Virtual Storage Platform F800 Hardware Reference Guide*, MK-94HM8046
- *Performance Guide*, MK-94HM8012
- *Provisioning Guide*, MK-94HM8014
- *System Administrator Guide*, MK-94HM8016
- *Hitachi TrueCopy® User Guide*, MK-94HM8019
- *Hitachi ShadowImage® User Guide*, MK-94HM8021
- *Hitachi Audit Log User Guide*, MK-94HM8028
- *Hitachi Universal Replicator User Guide*, MK-94HM8023

VSP G1000, G1500, and VSP F1500 documents:

- *Product Overview*, MK-92RD8051
- *Hardware Guide for Hitachi Virtual Storage Platform G1000, G1500, and F1500*, MK-92RD8007
- *Performance Guide*, MK-92RD8012
- *Provisioning Guide for Mainframe Systems*, MK-92RD8013
- *Provisioning Guide for Open Systems*, MK-92RD8014
- *System Administrator Guide*, MK-92RD8016
- *Hitachi Audit Log User Guide*, MK-94HM8028

Hitachi Command Suite documents:

- *Hitachi Command Suite User Guide*, MK-90HC172
- *Hitachi Command Suite Messages*, MK-90HC178

Document conventions

This document uses the following terminology conventions:

Convention	Description
VSP family	Refers to all models of the Hitachi Virtual Storage Platform family.
VSP Gx00 models	Refers to all of the following storage systems: • Hitachi Virtual Storage Platform G200 • Hitachi Virtual Storage Platform G400 • Hitachi Virtual Storage Platform G600 • Hitachi Virtual Storage Platform G800
VSP G series	Refers to all of the following storage systems: • VSP G1000, G1500, and VSP F1500

Convention	Description
	• VSP Gx00 models
• VSP Fx00 models • VSP F series	Refers to all of the following storage systems: • Hitachi Virtual Storage Platform F400 • Hitachi Virtual Storage Platform F600 • Hitachi Virtual Storage Platform F800

This document uses the following typographic conventions:

Convention	Description
Bold	• Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click **OK**. • Indicates emphasized words in list items.
Italic	• Indicates a document title or emphasized words in text. • Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: `pairdisplay -g group` (For exceptions to this convention for variables, see the entry for angle brackets.)
`Monospace`	Indicates text that is displayed on screen or entered by the user. Example: `pairdisplay -g oradb`
< > angle brackets	Indicates variables in the following scenarios: • Variables are not clearly separated from the surrounding text or from other variables. Example: `Status-<report-name><file-version>.csv` • Variables in headings.
[ ] square brackets	Indicates optional values. Example: [a | b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a | b } indicates that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a | b] indicates that you can choose a, b, or nothing. { a | b } indicates that you must choose either a or b.

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

Icon	Label	Description
	Note	Calls attention to important or additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.

Icon	Label	Description
	Caution	Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash).
	WARNING	Warns the user of a hazardous situation which, if not avoided, could result in death or serious injury.

Conventions for storage capacity values

Physical storage capacity values (for example, disk drive capacity) are calculated based on the following values:

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10^3) bytes
1 megabyte (MB)	1,000 KB or $1{,}000^2$ bytes
1 gigabyte (GB)	1,000 MB or $1{,}000^3$ bytes
1 terabyte (TB)	1,000 GB or $1{,}000^4$ bytes
1 petabyte (PB)	1,000 TB or $1{,}000^5$ bytes
1 exabyte (EB)	1,000 PB or $1{,}000^6$ bytes

Logical capacity values (for example, logical device capacity) are calculated based on the following values:

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KB Open-systems: • OPEN-V: 960 KB • Others: 720 KB
1 KB	1,024 (2^{10}) bytes
1 MB	1,024 KB or $1{,}024^2$ bytes
1 GB	1,024 MB or $1{,}024^3$ bytes
1 TB	1,024 GB or $1{,}024^4$ bytes
1 PB	1,024 TB or $1{,}024^5$ bytes
1 EB	1,024 PB or $1{,}024^6$ bytes

Accessing product documentation

Product user documentation is available on Hitachi Data Systems Support Connect: https://knowledge.hds.com/Documents. Check this site for the

most current documentation, including important updates that may have been made after the release of the product.

Getting help

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

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

Comments

Please send us your comments on this document to doc.comments@hds.com. Include the document title and number, including the revision level (for example, -07), 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 VSP G series or VSP F series storage systems.

- ☐ Encryption License Key benefits
- ☐ Encryption License Key support specifications
- ☐ When are data encryption keys needed
- ☐ Primary and secondary data encryption keys
- ☐ KMIP key management server support
- ☐ Implementing data encryption
- ☐ How to encrypt existing data
- ☐ Workflow for disabling encryption
- ☐ Workflow for changing the encryption key
- ☐ Audit logging of encryption events

Encryption License Key benefits

To guarantee the security of data, use the Encryption License Key feature to encrypt the data stored on VSP G series or VSP F series storage systems. 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
- Encryption can be applied to some or all internal drives.
- Encryption does not impact I/O throughput or latency.
- Encryption requires little to no disruption of 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
	Encryption module standard	VSP G200: Compliant to FIPS 140-2 Level 1[1] VSP G400, G600, G800, VSP F400, F600, F800: Compliant to FIPS 140-2 Level 2 VSP G1000, VSP G1500, and VSP F1500: Compliant to FIPS 140-2 Level 1 and Level 2[2,3]
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.
Managing data encryption keys	Creating data encryption keys	Use your system's storage management software to create data encryption keys.
	Deleting data encryption keys	Use your system's storage management software to delete data encryption keys. However, you cannot delete data encryption keys that are allocated to implemented drives.
	Unit of encryption/decryption	Parity group. Data encryption key is used per HDD.
	Scope of data encryption keys	• For VSP G200:

Item		Specification
		512 data encryption keys per storage system. You can create 512 Free keys or DEK keys. You can create 4 CEK keys and one KEK key. Therefore, the total number of data encryption keys will be 517 at the maximum when including CEK keys and KEK keys. • For VSP G400, G600 and VSP F400, F600: 1,024 data encryption keys per storage system. You can create 1,024 Free keys or DEK keys. You can create 4 CEK keys and one KEK key. Therefore, the total number of data encryption keys will be 1,029 at the maximum when including CEK keys and KEK keys. • For VSP G800 and VSP F800: 2,048 data encryption keys per storage system. You can create 2,048 Free keys or DEK keys. You can create 16 CEK keys and one KEK key. Therefore, the total number of data encryption keys will be 2,065 at the maximum when including CEK keys and KEK keys. • For VSP G1000, G1500, and VSP F1500: 4,096 data encryption 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 keys will be 4,129 at the maximum when including CEK keys and KEK keys.
	Attribute of encryption keys	The following attributes will be set for the encryption keys: Free: The unused key before allocating the encryption key. DEK: The encryption 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

Notes:

1. FIPS 140-2 Level 1 is in the process of certification as of Jun. 2016.
2. FIPS 140-2 Level 2 is in the process of certification as of Jun. 2016.
3. To use encryption modules compliant to FIPS 140-2 Level 2, contact customer support.

When are data encryption keys needed

After you setup the encryption environment, you will need data encryption 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 encrypting back-end directors (EBEDs)
  Six Free keys are needed for each EBED to create four CEK keys and two keys to register CEK keys.
- Updating CEK keys
  For VSP G200, VSP G400, G600, and VSP F400, F600: Two Free keys for each disk board (Four Free keys per storage system) are needed to change CEK keys.
  For VSP G800 and VSP F800:
  Two Free keys for each disk board (16 free keys per storage system) are needed to change CEK keys.
  For VSP G1000, G1500, and VSP F1500:
  Four Free keys for each EBED (32 Free keys per storage system) are needed to change CEK keys.

For information about the availability of Virtual Storage Platform F1500, contact your HDS representative.

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

Primary and secondary data encryption keys

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

Caution: 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:

- Creating encryption keys
- Adding, removing, or replacing drives
- Adding, removing, or replacing EBEDs for VSP G400, G600, G800 or VSP F400, F600, F800
- Replacing controllers for VSP G200
- Updating CEK keys
- Updating KEK keys

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

Related references

- Workflow for creating secondary backups of the data encryption keys on page 35

KMIP key management server support

Using the Encryption License Key feature, you can create backup and restore data encryption 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.

Related tasks

- Backing up the keys to a key management server on page 37

Implementing data encryption

Use the following process to implement data encryption:

1. Install the Encryption License Key feature. For details, see Workflow for Encryption License Key installation on page 23.
2. If you use a key management server, prepare the client certificate and configure the encryption environmental settings. For details, see Workflow for preparing the client certificate on page 27 and Workflow for editing encryption environmental settings on page 28.
3. Create and back up the encryption keys. For details, see Workflow for creating data encryption keys on page 34 and Workflow for creating secondary backups of the data encryption keys on page 35.
4. Enable encryption on the desired parity groups. For details, see Enabling data encryption on page 40.

How to encrypt 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 on page 40.
3. Format the LDEVs in the encrypted parity group. For instructions, see the *Provisioning Guide* for your storage system.
4. Migrate the existing data to the LDEVs in the encrypted parity group. For details about data migration, contact your account team.
5. After migrating the existing data to the encrypted parity group, shred the unencrypted data (migration source volumes) to prevent the data from being leaked. For details about shredding volumes, see the *Hitachi Volume Shredder User Guide*.

Workflow for disabling encryption

Use the following process to disable encryption:

1. Back up the data in the parity group to be decrypted.
2. Disable data encryption on the parity group. For details, see Workflow for disabling data encryption on page 42.
3. Format the LDEVs in the parity group. For instructions, see the *Provisioning Guide* for your storage system.

Workflow for changing the encryption key

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

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

1. Create a new parity group.
2. Enable encryption with a new data encryption key. For details, see Enabling data encryption on page 40.
3. Format the LDEVs in the encrypted parity group. For instructions, see the *Provisioning Guide* for your storage system.
4. Migrate the source data to the new target LDEVs in the encrypted parity group.

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

Audit logging of encryption events

The Audit Log feature of the VSP G series or VSP F series storage systems provides audit logging of events that happen in the system. The audit log records events related to data encryption and data encryption keys and is the only feature that records the interaction between the SVP and the KMIP key manager when configured. It can be used in checking and troubleshooting key back and generation.

For details about audit logging and audit log events, see the *Hitachi Audit Log User Guide*.

2

Encryption License Key installation

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

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

System requirements

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

Item	Requirement
VSP G1000 and G1500, and VSP F1500	Microcode 80-01-2x and later. For information about the availability of Virtual Storage Platform F1500, contact your HDS representative.
VSP G200, VSP G400, G600, G800 / VSP F400, F600, F800	• For VSP G200: Firmware 83-03-0x and later. • For VSP G400, G600, G800 or VSP F400, F600, F800: Firmware 83-01-0x 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
Encrypting back-end director (EBED)	A special BED that provides data encryption. A BED can also be called a disk adapter (DKA). For both EBEDs and standard BEDs, spare disks must be installed. The spare disk of an EBED cannot be used as a spare disk of a standard BED, and the spare disk of a standard BED cannot be used as a spare of an EBED.

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

Functions	Interoperability requirements and considerations
	contains an unencrypted 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 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 22.
2. Enable the Encryption License Key feature.
   For details, see Enabling the Encryption License Key feature on page 23.
3. Assign the Security Administrator (View & Modify) role to the administrator who creates, backs up, and restores data encryption keys.
   For details, see Enabling the Encryption License Key feature on page 23.

Enabling the Encryption License Key feature

Procedure

1. Enable the Encryption License Key license on the storage system. For VSP G1000, G1500, and VSP F1500, see the *Hitachi Command Suite User Guide* or *System Administrator Guide* for your storage system. For VSP Gx00 models and VSP Fx00 models, see the *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 backing up or restoring keys.

   For details about assigning roles, see the *Hitachi Command Suite User Guide* or *System Administrator Guide*.

Disabling the Encryption License Key feature

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

Procedure

1. Disable data encryption on all encrypted parity groups. For instructions, see Disabling data encryption on page 42.
2. Initialize the encryption environmental settings. For instructions, see Initializing the encryption environment settings on page 52.
3. Disable the software license key. For instructions, see the *Provisioning Guide* for your storage system.

3

Key Management Server Connections

You can use an optional key management server with the VSP G series or VSP F series storage systems. This chapter provides information on setting up the key management server.

- ☐ Key management server requirements
- ☐ Workflow for editing 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 8.2.0 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 26.

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

Related tasks

- Uploading the root and client certificate on page 28

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 27.

Related references

- Root and client certificates on page 26

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 27.
4. Upload the root and client certificates to the SVP.
   For details, see Uploading the root and client certificate on page 28.

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 service processor (SVP).

Procedure

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 26.

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.

Before you begin

- You must have the Security Administrator (View & Modify) role.

Procedure

1. Open the **Encryption Keys** window.
   In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.
   In Device Manager - Storage Navigator:
   a. Display the Device Manager - Storage Navigator main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. Click **Edit Encryption Environmental Settings**.
3. Upload the certificates in the **Edit Encryption Environmental Settings** window.

Workflow for editing 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 the storage system.

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 27 and Uploading the root and client certificate on page 28.

2. Configure the connection settings to the key management server.
   For details, see Configuring the connection settings to the key management server on page 29.
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 *System Administrator Guide* for your storage system.

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 keys to the key management server.

For more information, see Settings in the Edit Encryption Environmental Settings window on page 31 and Backing up the keys to a key management server on page 37.

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.

Note: If you use a V-VOL, you will need encryption/unencryption formatting for the V-VOL.

Before you begin

- You must have the Security Administrator (View & Modify) role.

Procedure

1. Open the **Encryption Keys** window.
   In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.
   In Device Manager - Storage Navigator:
   a. Display the Device Manager - Storage Navigator main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. Select the **Encryption Keys** tab.
3. Click **Edit Encryption Environmental Settings**.

4. In the **Edit Encryption Environmental Settings** window, select **Enable** or **Disable** on the **Key Management Server**.
5. If you connect to the Key Management Server, specify the primary server and the secondary server.
6. If the key management server is already in use, select **Check** to test the connection. Error messages appear if the server configuration test fails.
7. Create an encryption key:
   - To generate an encryption key on the key management server, select **Generate Encryption Keys on Key Management Server**. To store the encryption key on the key management server, select **Protect the Key Encryption Key on the Key Management Server**, then **I Agree**.

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

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

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

8. To backup data encryption 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 references

- Edit Encryption Environmental Settings window on page 60

Restoring the key management server connection after SVP replacement

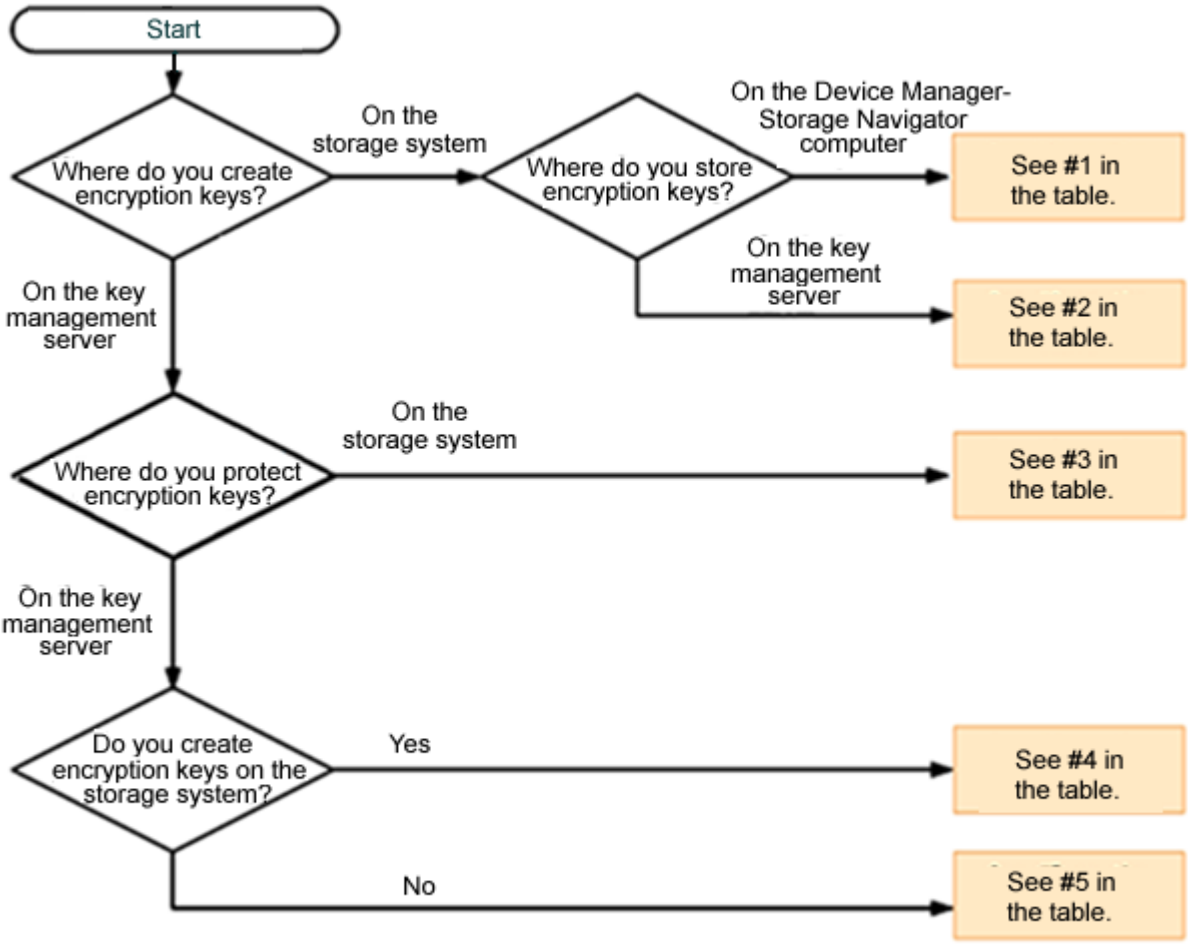
If you are restoring the key management server connection after the SVP replacement, restore the connection setting of the key management server which is already backed up. After doing so, if the setting in the **Edit Encryption Environmental Settings** window before the SVP replacement is a value other than #1 in the table in Settings in the Edit Encryption Environmental Settings window on page 31, set the client certificate and root certificate of the key management server again.

If you have not backed up the connection setting of the key management server, set the connection for the key management server again. If you have not stored the client certificate, create a new client certificate. Then, set the client certificate and root certificate of the key management server that you have just created.

If the setting in the **Edit Encryption Environmental Settings** window before the SVP replacement is #4 or #5 in the table in Settings in the Edit Encryption Environmental Settings window on page 31 and you have already created a new client certificate after the SVP replacement, update the key encryption key after you set the connection for the key management server. When you do this, the key deletion key encryption fails because you cannot delete the key encryption key before the update; however, the key encryption key is already updated.

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 keys

This chapter provides instructions for managing data encryption keys using the VSP G series or VSP F series storage systems.

- ☐ Workflow for creating data encryption keys
- ☐ Workflow for creating secondary backups of the data encryption keys
- ☐ Workflow for enabling data encryption
- ☐ Workflow for disabling data encryption
- ☐ Workflow for restoring data encryption keys
- ☐ Workflow for deleting data encryption keys
- ☐ Exporting encryption key table information
- ☐ Rekeying key encryption keys
- ☐ Rekeying certificate encryption keys
- ☐ Retrying Key Encryption Key Acquisition
- ☐ Initializing the encryption environment settings

Workflow for creating data encryption keys

Create data encryption keys to use with the Encryption License Key feature.

Use the following process to create data encryption keys:

1. Create the data encryption key or group of keys.
   For details, see Creating data encryption keys on page 34.
2. Create the secondary backups of the data encryption keys.
   For details, see Workflow for creating secondary backups of the data encryption keys on page 35.
3. Schedule regular weekly backups of all of your data encryption keys to ensure data availability.

Creating data encryption keys

If you need to change a data encryption key, create a new data encryption 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 depends on the number of EBEDs and drives setup in the configuration. 4,048 keys are created if maximum EBEDs are installed). After that, you can create 4,096 Free keys or DEK keys. You can create a maximum of 4,096 encryption keys per system.

For VSP G200, when you configure encryption environmental settings on the **Edit Encryption Environmental Settings** window for the first time, 506 free keys or DEK keys are created. (This differs from the configuration. 506 keys are created if maximum EBEDs are installed). After that, you can create 512 free keys or DEK keys.

For VSP G400, G600 and VSP F400, F600, when you configure encryption environmental settings on the **Edit Encryption Environmental Settings** window for the first time, 1,018 Free keys or DEK keys are created. (This differs from the configuration. 1,018 keys are created if maximum EBEDs are installed). After that, you can create 1,024 Free keys or DEK keys. You can create up to 1,024 encryption keys per storage system.

For VSP G800 and VSP F800, when you configure encryption environmental settings on the **Edit Encryption Environmental Settings** window for the first time, 2,024 Free keys or DEK keys are created. (This differs from the configuration. 2,024 keys are created if maximum EBEDs are installed). After that, you can create 2,048 free keys or DEK keys.

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 keys, it is strongly recommended that you back up all keys.

Before you begin

- You must have the Security Administrator (View & Modify) role.

Procedure

1. Open the **Encryption Keys** window.

   In Hitachi Command Suite:

   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.

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

   In Device Manager - Storage Navigator:

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

   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. Select the **Encryption Keys** tab.
3. Click **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 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 key is created.

Related references

- Create Keys window on page 65

Workflow for creating secondary backups of the data encryption keys

The VSP G series or VSP F series storage systems automatically create a primary backup of the data encryption keys. You can also create secondary backups of the data encryption keys.

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

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

- Creating encryption keys
- Adding, removing, or replacing drives
- Adding, removing, or replacing EBEDs
- Updating CEK keys
- Updating KEK keys

Use the following process to create secondary backups of the data encryption keys:

1. Confirm that the VSP G series or VSP F series storage systems are not processing other tasks. You cannot back up the keys while your storage system is processing other tasks.
2. Use one of the following methods to create secondary backups of the data encryption keys:
   - Back up the data encryption keys as a file on the HCS management server or HDvM - SN computer.
     For details, see Backing up the keys as a file on page 36.
   - Back up the data encryption keys to a key management server.
     For details, see Backing up the keys to a key management server on page 37.

Backing up the keys as a file

You can create the secondary backups of the data encryption keys as a file on the computer. Back up the file and the password since the file and password are not automatically backed up.

Before you begin

- You must have the Security Administrator (View & Modify) role

Procedure

1. Open the **Encryption Keys** window.
   In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.
   In Device Manager - Storage Navigator:
   a. Display the Device Manager - Storage Navigator main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. Select the **Encryption Keys** tab.
3. In the **Encryption Keys** table, select the key ID for the data encryption 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 key is saved.

Related references

- Encryption Keys window on page 58
- Backup Keys to File window on page 70

Backing up the keys to a key management server

You can create the secondary backups of the data encryption keys on a key management server. The data encryption 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 key to encrypt the original keys. Both keys reside on the server.

Before you begin

- You must have the Security Administrator (View & Modify) role

Procedure

1. Open the **Encryption Keys** window.

   In Hitachi Command Suite:

   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.

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

   In Device Manager - Storage Navigator:

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

   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. On the **Encryption Keys** tab, click **View Backup Keys on Server** to 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 key is saved.

Related references

- Encryption Keys window on page 58
- Backup Keys to Server window on page 72

Changing the password requirements for the backup encryption keys

You can set the minimum number of characters required for the password for the backup encryption keys.

Before you begin

- You must have the Security Administrator (View & Modify) role

Procedure

1. Open the **Encryption Keys** window.

   In Hitachi Command Suite:

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

   In Device Manager - Storage Navigator:

   a. Display the Device Manager - Storage Navigator main window.
   b. From the **Settings** menu, select **Security > Encryption Key > Edit Password Policy (Backup Encryption Keys)**.
   c. In the **Edit Password Policy (Backup Encryption Keys)** window, set the minimum number of characters.
2. 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 references

- Edit Password Policy (Backup Encryption Keys) window on page 66

Opening the Backup Keys to Server window using the Encryption window

Before you begin

- You must have the Security Administrator (View & Modify) role.

Procedure

1. Open the **Encryption Keys** window.
   In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.
   In Device Manager - Storage Navigator:
   a. Display the Device Manager - Storage Navigator main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. On the **Encryption Keys** tab, select the key ID for the data encryption 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

Before you begin

- You must have the Security Administrator (View & Modify) role.

Procedure

1. Open the **Encryption Keys** window.
   In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.
   In Device Manager - Storage Navigator:
   a. Display the Device Manager - Storage Navigator main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. On the **Encryption Keys** tab, click **View Backup Keys on Server**.
3. Click **Backup Keys to Server**.

Viewing encryption keys backed up on the key management server

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

Before you begin

- You must have the Security Administrator (View & Modify) role.

Procedure

1. Open the **Encryption Keys** window.
   In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.
   In Device Manager - Storage Navigator:
   a. Display the Device Manager - Storage Navigator main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. On the **Encryption Keys** tab, click **View Backup Keys on Server** to view the backup keys on the key management server.

Related references

- Encryption Keys window on page 58
- View Backup Keys on Server window on page 81

Workflow for enabling data encryption

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

Use the following process to enable data encryption on a parity group:

1. Create the secondary backups of the data encryption keys.
   For details, see Workflow for creating secondary backups of the data encryption keys on page 35.
2. Block the LDEVs in the parity group to be encrypted.
   For details, see the *Provisioning Guide* for your storage system.
3. Enable data encryption on the parity group.
   For details, see Enabling data encryption on page 40.
4. Format the LDEVs at the parity-group level.

Enabling data encryption

Data encryption is enabled at the parity-group level.

Before you begin

- You must have the Security Administrator (View & Modify) role.
- You must have the Storage Administrator (Provisioning) role to format volumes.
- The accelerated compression feature of the parity group must be disabled.

Procedure

1. Open the **Encryption Keys** window.
   In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Parity Groups**.
   In Device Manager - Storage Navigator:
   a. Display the Device Manager - Storage Navigator main window.
   b. Select **Storage Systems** in **Explorer**, and select **Parity Groups**.
2. In the **Parity Groups** table, select a specific parity group on which you want to enable encryption and then click **Edit Encryption**.
   In the tree that is shown, **Internal** or **External** is displayed.
3. To select an internal LDEV, select **Internal**. Otherwise, click the **Parity Groups** tab.
4. In the **Parity Groups** table, select a specific parity group on which you want to enable encryption and then click **Actions > Parity Group > Edit Encryption**.

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

5. In the **Edit Encryption** window, 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 for the selected parity group.
   - For **Format Type**, select the format type.
     Values: Quick Format (default), Normal Format, or No Format

   Caution: If accelerated compression of the parity group is enabled, do not select **Enable** for **Encryption**. If you select **Enable** for **Encryption**, an error occurs when performing the task.

   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 are no volumes in the selected 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 references

- Edit Encryption window on page 83

Workflow for disabling data encryption

Encryption is disabled at the parity-group level.

1. Create the secondary backups of the data encryption keys.

   For details, see Workflow for creating secondary backups of the data encryption keys on page 35.
2. Block the LDEVs in the parity group to be decrypted.

   For details, see the *Provisioning Guide* for your storage system.
3. Disable data encryption on the parity group.

   For details, see *Provisioning Guide* for your storage system.
4. Format the LDEVs in the decrypted parity group.

   For details, see Encryption formatting at the parity-group level on page 44.

Disabling data encryption

Disable data encryption at the parity-group level to perform (normal) formatting options on encrypted data, such as writing to or overwriting an LDEV.

Before you begin

- You must have the Security Administrator (View & Modify) role.
- You must have the Storage Administrator (Provisioning) role to format volumes.

Procedure

1. Open the **Encryption Keys** window.

   In Hitachi Command Suite:

   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.

b. Expand the target storage system, and then select **Parity Groups**.
c. In the table that is shown, **Internal** or **External** are displayed.

In Device Manager - Storage Navigator:

a. Display the Device Manager - Storage Navigator main window.
b. Select **Storage Systems** in **Explorer**, and select **Parity Groups**.
c. In the 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 references

- Edit Encryption window on page 83

Formatting V-VOLs for unencryption

If you use a V-VOL, unencryption formatting for the V-VOL is required. For details about formatting volumes, see the *Provisioning Guide* for your storage system.

Procedure

1. In the **Storage System** tree, select a resource to show one of the following tabs:
   - **LDEVs** tab when you select a parity group in **Parity Groups**
   - **LDEVs** tab when you select **Logical Devices**
   - **Virtual Volumes** tab when you select a pool in **Pools**
2. Select the LDEV, and go to **Actions > Logical Device > Format LDEVs** or select **Format LDEVs** on the bottom right-hand corner of the window.
3. In the **Format LDEVs**, select the **Normal** format type (required for V-VOLs), and 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**.

Encryption formatting at the parity-group level

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

Workflow for restoring data encryption keys

Restore a data encryption 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 key becomes unavailable or cannot be used (for example, due to a system failure).

Restoration is performed in a batch for the backed up data encryption keys (including free keys, DEK, and CEK): 516 keys for VSP G200 models, 1,028 keys for VSP G400, G600 models and VSP F400, F600 models, and 2,064 keys for VSP G800 and VSP F800 models where key information is lost or deleted.

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

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

To restore the data encryption key, the volumes belonging to the parity group for which the key is set must be blocked. In addition, after the restoration of the key, the volumes belonging to the parity group for which encryption key is set must be restored.

Procedure

1. Block the LDEVs associated to the encrypted parity group.
   For details, see the *Provisioning Guide* for your storage system.
2. Restore the data encryption key from a primary or secondary backup copy. Do one of the following:
   - Restore the data encryption 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 45.
   - Restore the data encryption key from the key management server.
     For details, see Restoring keys from a key management server on page 46.

Restoring keys from a file

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

Before you begin

- You must have the Security Administrator (View & Modify) role.

Procedure

1. Open the **Encryption Keys** window.
   In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.
   In Device Manager - Storage Navigator:
   a. Display the Device Manager - Storage Navigator main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. On the **Encryption Keys** tab, click **Restore Keys > From File**.
3. In the **Restore Keys from File** window, click **Browse** and then click **OK**.
4. In the **Open** dialog box, select the backup file and click **Open**.
5. In the **Restore Keys from File** window, complete the following item and then click **Finish**:
   - For **File Name**, shows the name of the selected file.
     View-only: Yes
   - For **Password**, type the password for the data encryption key that you typed when you backed up the selected data encryption 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 key is restored.

Related references

- Restore Keys from File window on page 74

Restoring keys from a key management server

Restore a data encryption key from the key management server. You can restore up to 4,128 data encryption keys at a time.

The client certificate is required to restore backed up data encryption 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 keys.

Before you begin

- You must have the Security Administrator (View & Modify) role.

Procedure

1. Open the **Encryption Keys** window.
   In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.
   In Device Manager - Storage Navigator:
   a. Display the Device Manager - Storage Navigator main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. On the **Encryption Keys** tab, click **Restore Keys > From Server**.
3. In the **Restore Keys from Server** window, select the data encryption 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 key is restored.

Related references

- Restore Keys from Server window on page 76

Workflow for deleting data encryption keys

Delete a data encryption 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 key:

1. Back up the secondary data encryption key.
   For details, see Workflow for creating secondary backups of the data encryption keys on page 35.
2. Ensure the key is not allocated to the parity group.
   See the Encryption Keys window on page 58 and check the key allocation.
3. Delete the data encryption key using one of the following methods:
   - Delete the data encryption key from a file on the HCS management server or HDvM - SN computer.
     For details, see Deleting data encryption keys on page 47.
   - Delete the backup key from the key management server.
     For details, see Deleting backup data encryption keys from the server on page 48.

Deleting data encryption keys

Delete data encryption 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.

Before you begin

- You must have the Security Administrator (View & Modify) role.

Procedure

1. Open the **Encryption Keys** window.
   In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.
   In Device Manager - Storage Navigator:
   a. Display the Device Manager - Storage Navigator main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.

2. On the **Encryption Keys** tab, select the key ID for the 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 the keys to a key management server on page 37.
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 key is deleted.

Related references

- Delete Keys window on page 78

Deleting backup data encryption keys from the server

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

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

Before you begin

- You must have the Security Administrator (View & Modify) role.

Procedure

1. Open the **Encryption Keys** window.

   In Hitachi Command Suite:

   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.

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

   In Device Manager - Storage Navigator:

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

   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. On the **Encryption Keys** tab, click **View Backup Keys on Server**.
3. In the **View Backup Keys on Server** window, select the key ID for the backup data encryption 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 key is deleted.

Related references

- View Backup Keys on Server window on page 81
- Delete Backup Keys on Server window on page 80

Exporting encryption key table information

You can output encryption key table information.

Before you begin

- You must have the Security Administrator (View & Modify) role.

Procedure

1. Open the **Encryption Keys** window.

   In Hitachi Command Suite:

   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.

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

   In Device Manager - Storage Navigator:

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

   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. On the **Encryption Keys** tab, select the key ID for the data encryption 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 keys, it is recommended that you back up each key.

Use the following procedure to rekey key encryption keys.

Before you begin

- You must have the Security Administrator (View & Modify) role.

Procedure

1. Open the **Encryption Keys** window.
   In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.
   In Device Manager - Storage Navigator:
   a. Display the Device Manager - Storage Navigator main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. On the **Encryption Keys** tab, select the key ID for the data encryption 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 references

- Rekey Key Encryption Key window on page 88

Rekeying certificate encryption keys

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

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

Before you begin

- You must have the Security Administrator (View & Modify) role.

Procedure

1. Open the **Encryption Keys** window.
   In Hitachi Command Suite:
   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.
   b. Expand the target storage system, and then select **Encryption Keys**.
   In Device Manager - Storage Navigator:
   a. Display the Device Manager - Storage Navigator main window.
   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. On the **Encryption Keys** tab, select **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 references

- Rekey Certificate Encryption Keys window on page 87

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.

Before you begin

- You must have the Security Administrator (View & Modify) role.

Procedure

1. Open the **Encryption Keys** window.

   In Hitachi Command Suite:

   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.

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

   In Device Manager - Storage Navigator:

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

   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. On the **Encryption Keys** tab, select **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**.

Result

You need to restore the EBEDs and blocked drives or blocked volumes after retrying key encryption key acquisition. Contact customer support to restore the EBEDs and blocked drives or blocked volumes.

Related references

- Retry Key Encryption Key Acquisition window on page 88

Initializing the encryption environment settings

Disable data encryption at the parity-group level before initializing the encryption environment settings.

Before you begin

- You must have the Security Administrator (View & Modify) role.

Procedure

1. Open the **Encryption Keys** window.

   In Hitachi Command Suite:

   a. On the **Resources** tab, click **Storage Systems**, and then expand **All Storage Systems**.

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

   In Device Manager - Storage Navigator:

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

   b. Select **Administration** in **Explorer**, and select **Encryption Keys**.
2. On the **Encryption Keys** tab, select **Edit Encryption Environmental Settings**.
3. In the **Edit Encryption Environmental Settings** window, select **Initialize Encryption Environmental Settings**.
4. Select **Finish** to display the **Confirm** window.
5. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.

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

   Click **Apply**.

Related references

- Edit Encryption Environmental Settings window on page 60

5

Troubleshooting

This chapter provides troubleshooting information for Encryption License Key.

- Encryption events in the audit log
- Troubleshooting for Encryption License Key
- Contacting customer support

Encryption events in the audit log

The audit log of VSP G200, VSP G400, G600, G800, or VSP F400, F600, F800 records events related to Encryption License Key, including data encryption and Encryption License Key processes. You can export an audit log that contains encryption events in near real-time to an external syslog server.

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

Troubleshooting for Encryption License Key

For troubleshooting information for VSP G1000, G1500, and VSP F1500, see the *Hardware Guide for Hitachi Virtual Storage Platform G1000, G1500, and F1500*.

For troubleshooting information for your VSP G series or VSP F series storage system, see the *Hardware Guide* for your storage system. For details about HCS error messages, see *Hitachi Command Suite Messages*.

For troubleshooting information for Device Manager - Storage Navigator, see the *System Administrator Guide* for your storage system. For details about HDvM - SN error messages, see *Hitachi Device Manager - Storage Navigator Messages*.

The following table provides general troubleshooting information for Encryption License Key. If you need technical assistance, contact customer support.

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 keys with a key management server, the connection to the key management server is available. • If you backup and restore data encryption 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 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 keys.	Make sure that: • The Encryption License Key software license is valid and installed. • You have the Security Administrator (View & Modify) role.

Problem	Action
	• If you have backed up and restored data encryption keys with a key management server, that the connection to the key management server is available.
Cannot enable encryption for a parity group.	Make sure that: • The Encryption License Key software license is valid and installed. • All LDEVs in the parity group are in the blocked status.
Cannot disable encryption for a parity group.	Make sure that all LDEVs in the parity group are in the blocked status.
Server configuration test failed.	Check the following key management server connection settings: • Host name • Port number • Client certificate file • Root certificate file If the communication failure is due to the length of time to connect to the server, try changing these settings: • Timeout • Retry interval • Number of retries
The Edit Encryption wizard operation failed, but the status of encryption (enable or disable) has changed.	The change of the status succeeds, but the format of the volume fails. Confirm the message, remove the error, and format volumes again.
The storage system failed to get encryption keys backed up on the key management server and all volumes are blocked when the storage system is turned on. The SIM code 661000 is returned.	Complete the following tasks: • Restore the connection to the key management server. • Retry key encryption key acquisition. • Contact customer support to restore the EBEDs 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 encryption environmental settings. **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.
Server configuration test has succeeded, but the following error is displayed: 10126-105022 The connected key management server does not support the required functions.	A required function for the setting of the key management server is not supported with the connected key management server. See Key management server requirements on page 26 and update the software of the key management server to the latest version.
The Edit Encryption Wizard operation failed though the free key (Encryption key with the free attribute) exists. The error below is displayed. 03005-108104 There are not enough free keys.	The **Edit Encryption Environmental Settings** wizard executed prior to the **Edit Encryption** wizard might have failed because of disk board failure. Confirm in the **Task** window that the **Edit Encryption Environmental Settings wizard** failed and if so, move the cause of error. Then retry the **Edit Encryption Environmental Settings** wizard and the **Edit Encryption** wizard after initializing the **Encryption Environmental Setting**.

Contacting customer support

When contacting customer support, 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

customer support is available 24 hours a day, seven days a week. If you need technical support, log on to customer support for contact information: https://support.hds.com/en_us/contact-us.html

A

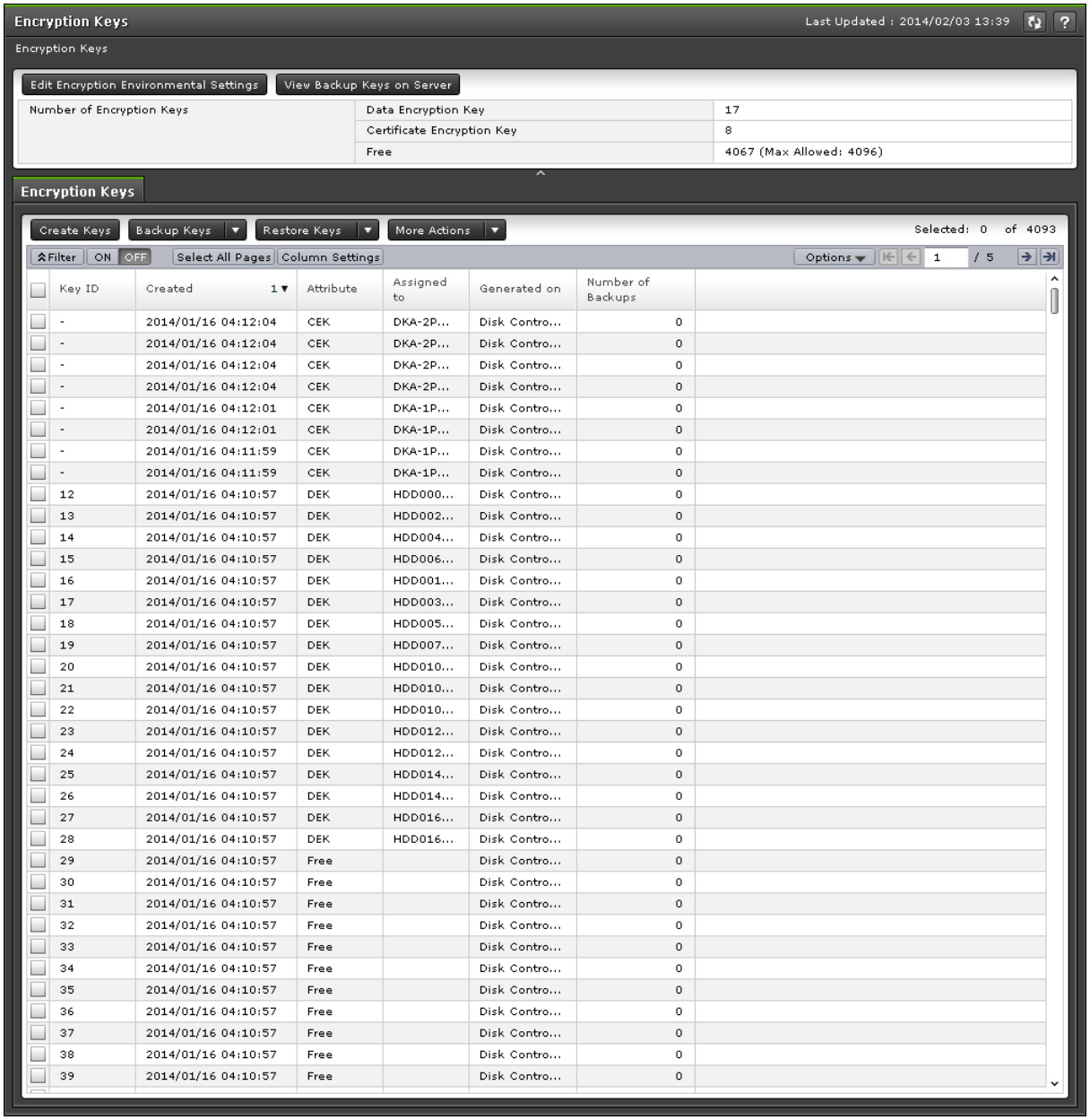
Encryption License Key GUI Reference

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 keys. Clicking Encryption Keys in the Administration tree opens this window.



Summary

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

Item	Description
Number of Encryption Keys	Shows the number of data encryption 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 key details and to select an unused data encryption 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 keys A hyphen (-) is displayed when the encryption key is CEK or KEK.
Created	The date and time the data encryption 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 key is created When the attribute is KEK, a hyphen (-) is displayed.
Create Keys	Click to open the **Create Keys** window
Backup Keys	Select To File to open the **Backup Keys to File** window. Select To Server to open the **Backup Keys to Server** window.
Restore Keys	Select From File to open the **Restore Keys from File** window. Select From Server to open the **Restore Keys from Server** window.
More Actions	Select Rekey Key Encryption Keys to display the **Rekey Key Encryption Keys** window.

Item	Description
	Select Delete Keys from the list to delete a selected data encryption 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 tasks

- Creating data encryption keys on page 34
- Backing up the keys as a file on page 36
- Backing up the keys to a key management server on page 37
- Restoring keys from a file on page 45
- Restoring keys from a key management server on page 46
- Deleting data encryption keys on page 47
- Deleting backup data encryption keys from the server on page 48
- Viewing encryption keys backed up on the key management server on page 39

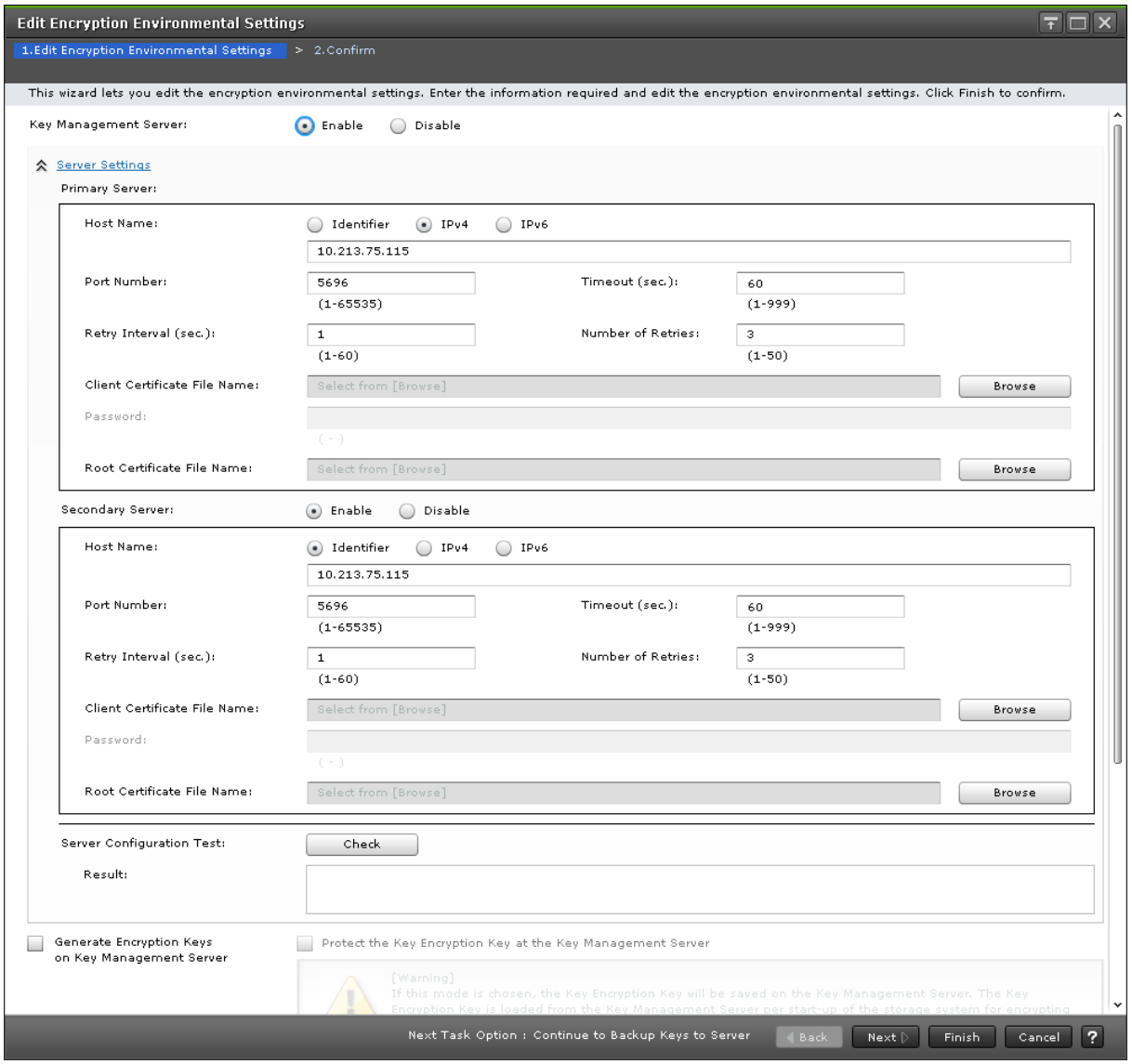
Edit Encryption Environmental Settings wizard

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

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 the storage system.

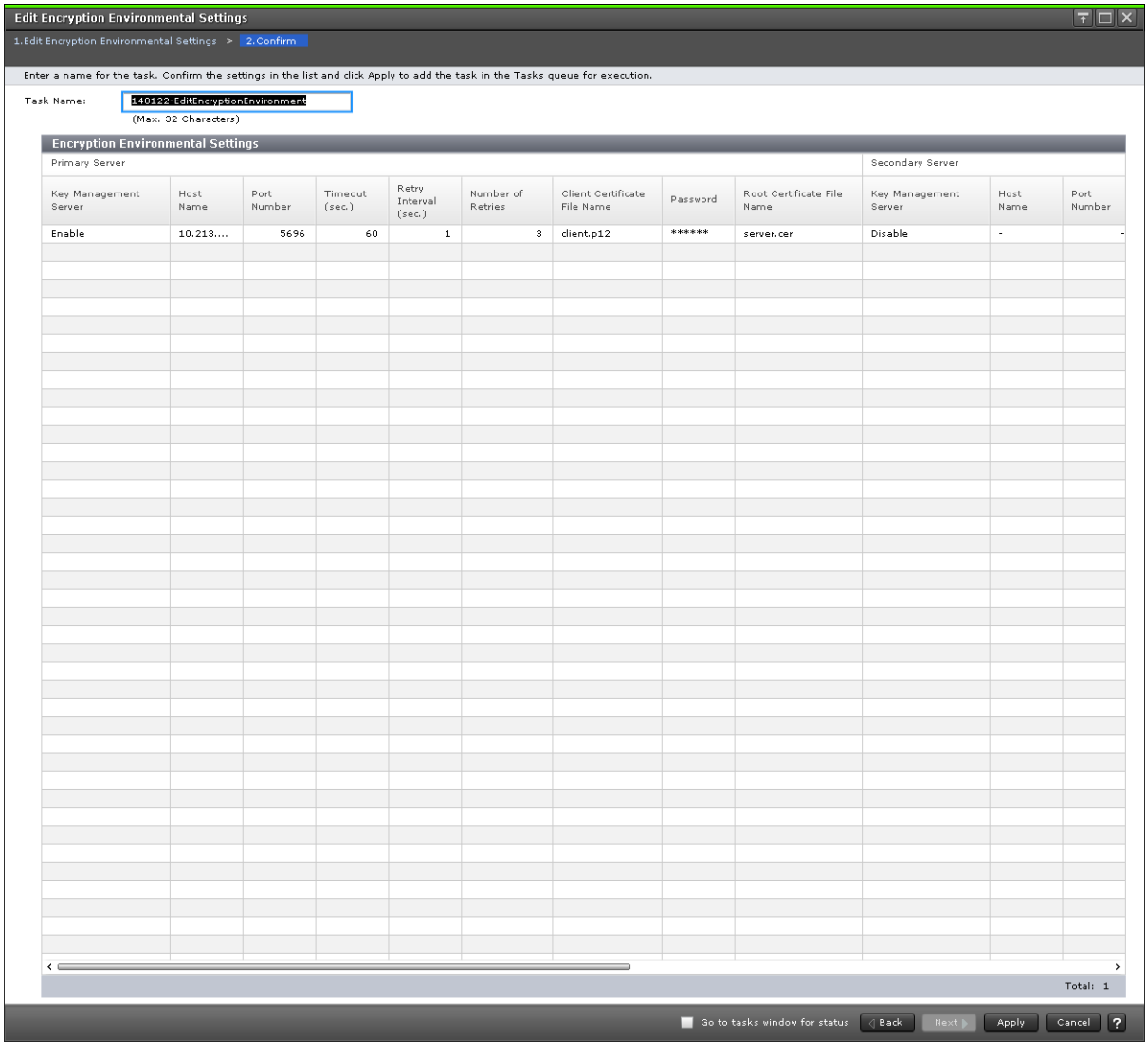


Item	Description
Key Management Server	Select whether to use the key management server: • Enable: (default) key management server is used • Disable: key management server is not used
Server Setting	When you use the key management server, the following items display: • Primary server • Secondary server • Server Configuration test
Primary Server	Specify the primary server information. • Host Name: Enter the host name of the key management server. Identifier: Enter the host identifier. IPv4: Enter the host IPv4 address. IPv6: Enter the host IPv6 address.

Item	Description
	• 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.
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.

Item	Description
	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 encryption environmental settings

Edit Encryption Environmental Settings confirmation window



Item	Description
Primary Server	Displays the primary server information.

Item	Description
	• Key Management Server: Shows whether the key management server is used Enable: key management server is used Disable: key management server is not used Not Set: Initialize the encryption environmental settings • 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

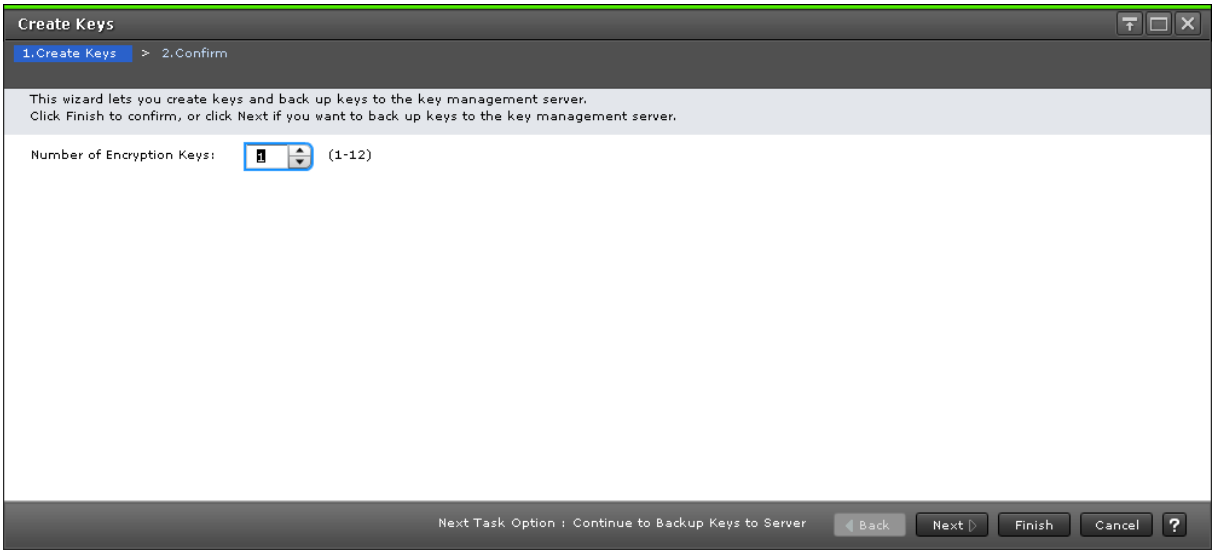
Use the Create Keys wizard to create keys and to backup keys to the key management server.

This wizard includes the following windows:

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

Create Keys window

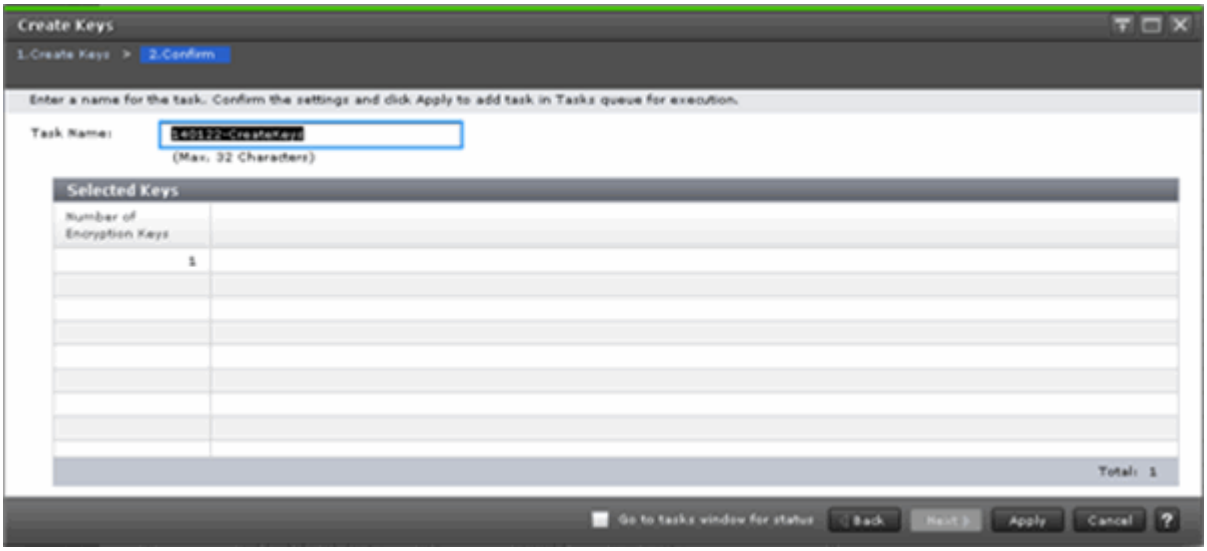
Use the **Create Keys** window to create a data encryption key. This window includes the Selected Keys table.



Item	Description
Number of Encryption Keys	• For VSP G200, this specifies the number of encryption keys (1-512). The maximum number of encryption keys is 512. This window shows the value obtained by subtracting the number of created DEK and free keys from 512. • For VSP G400, G600 or VSP F400, F600, this specifies the number of encryption keys (1-1,024). 1,024 is the maximum number of encryption keys. This window shows the value that subtracted the number of created DEK and Free keys from 1,024. • For VSP G800 and VSP F800, this specifies the number of encryption keys (1-2,048). The maximum number of encryption keys is 2,048. This window shows the value obtained by subtracting the number of created DEK and free keys from 2,048. • For VSP G1000, G1500, and VSP F1500, this specifies the number of encryption keys (1-4,096). 4,096 is the maximum number of encryption keys. This window shows the value obtained by subtracting 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 tasks

- Creating data encryption keys on page 34

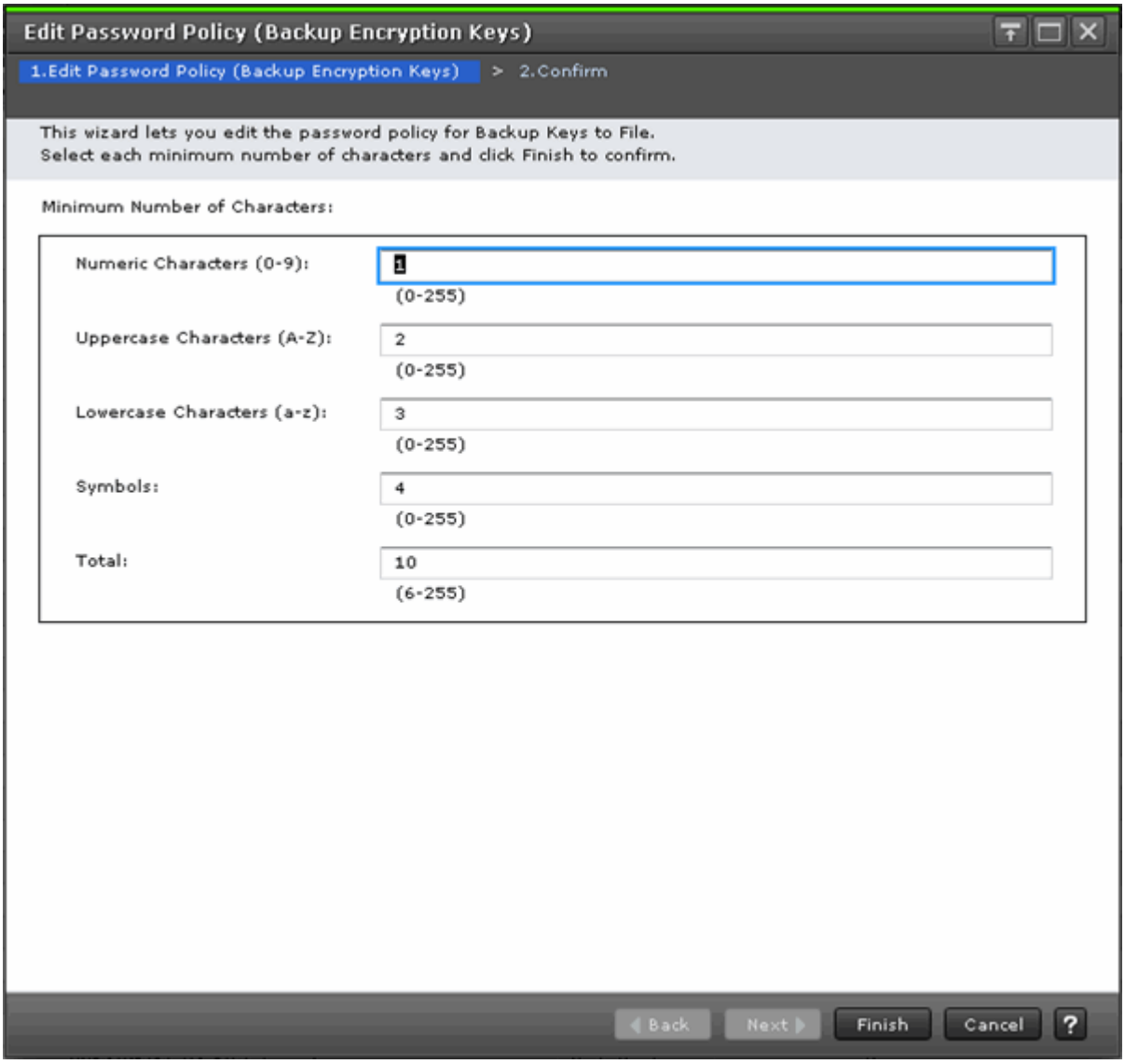
Edit Password Policy (Backup Encryption Keys) wizard

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

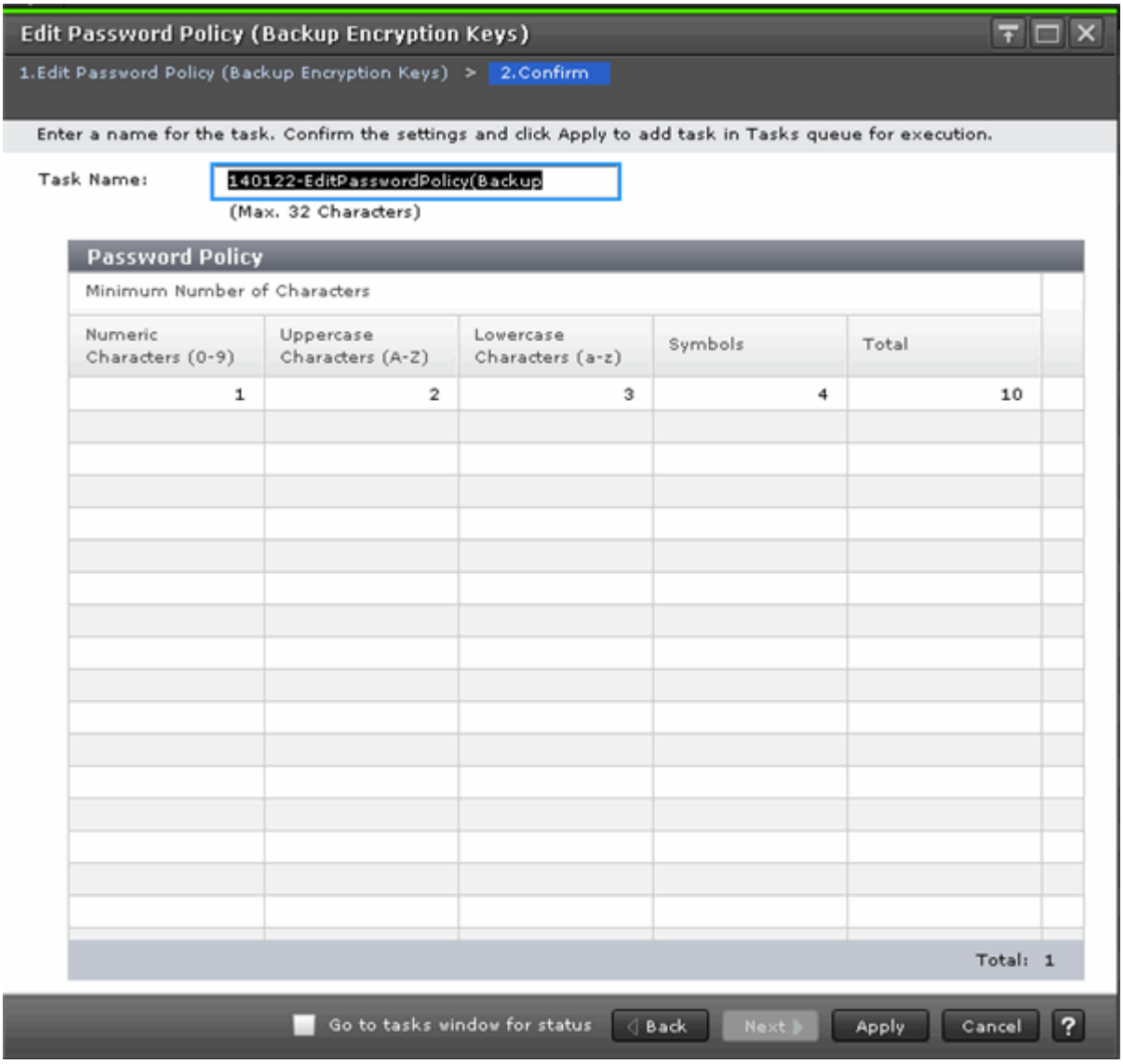


Item	Description
Numeric Characters (0-9)	The minimum number of numeric characters that should be used for this password Values: 0 to 255 Default: 0
Uppercase Characters (A-Z)	The minimum number of alphabetical upper case characters that should be used for this password Values: 0 to 255 Default: 0
Lowercase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

Item	Description
	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
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

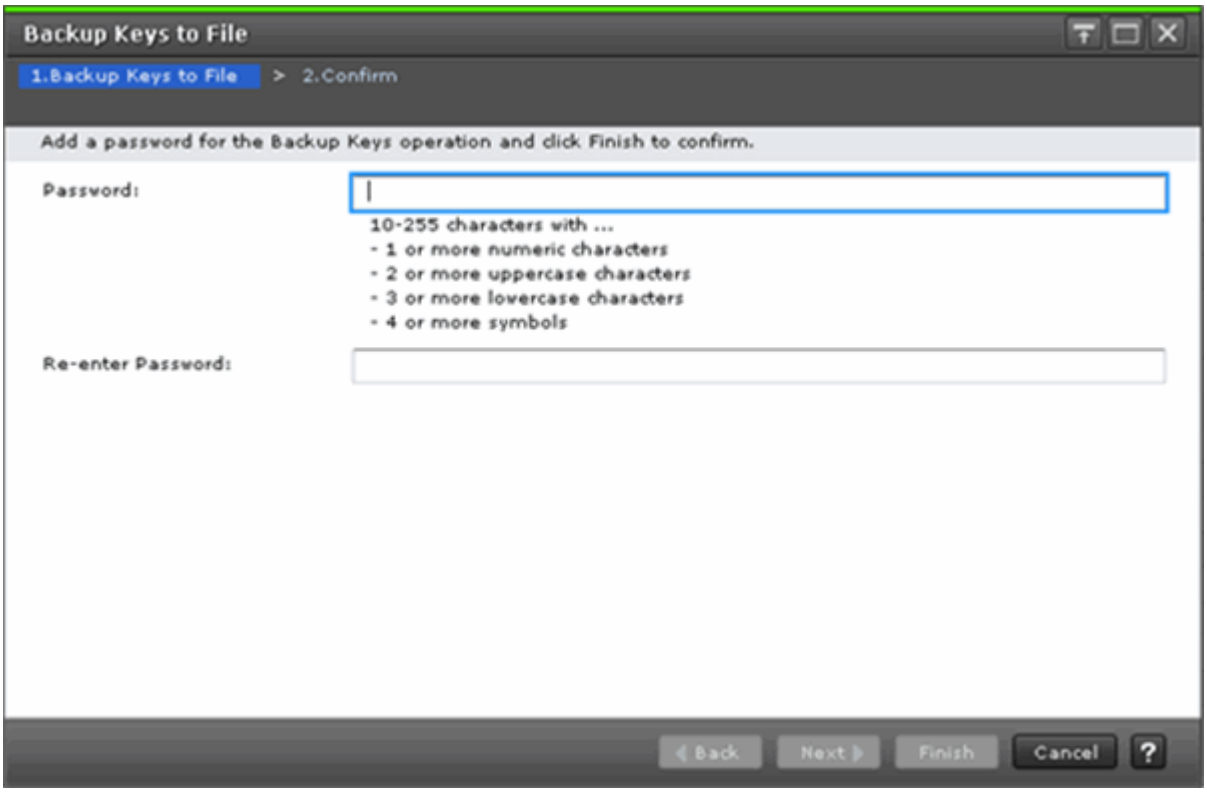
Use the Backup Keys to File wizard to create backup data encryption keys as files on the HCS management server or HDvM - SN computer.

This wizard includes the following windows:

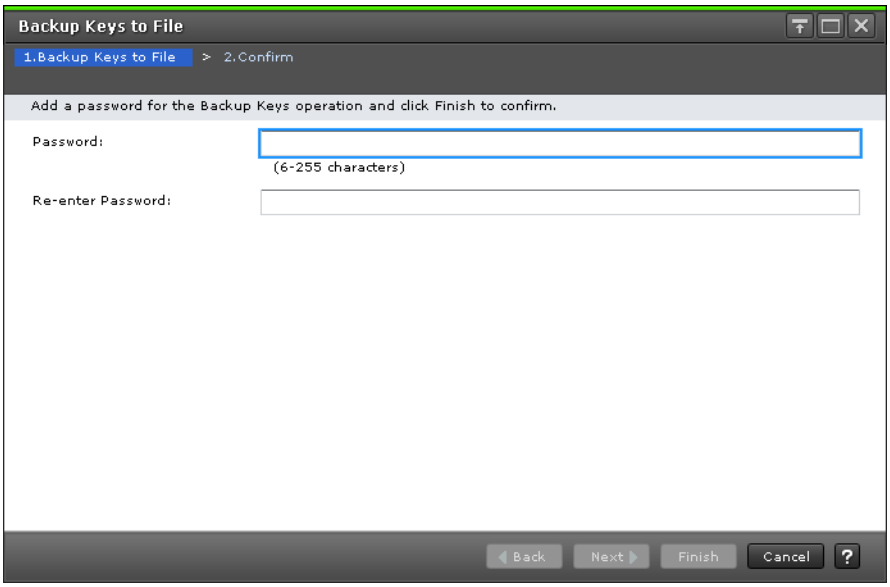
- **Backup Keys to File** window
- **Confirm** window

Backup Keys to File window

When the password policy is edited in the **Edit Password Policy (Backup Encryption Keys)** window, the screen appears as follows:

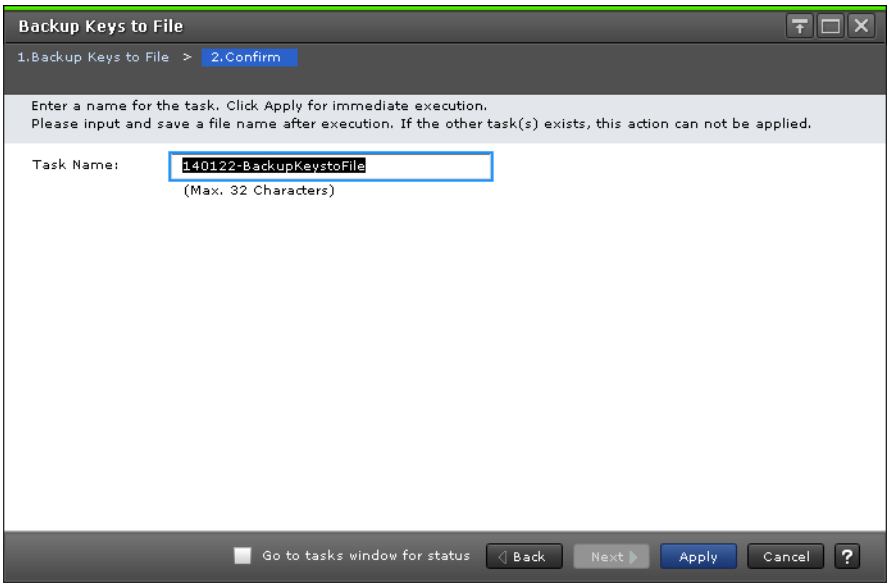


When the password policy is not edited in the **Edit Password Policy (Backup Encryption Keys)** window, the screen appears as follows:



Item	Description
Password	The password for the backup data encryption 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.

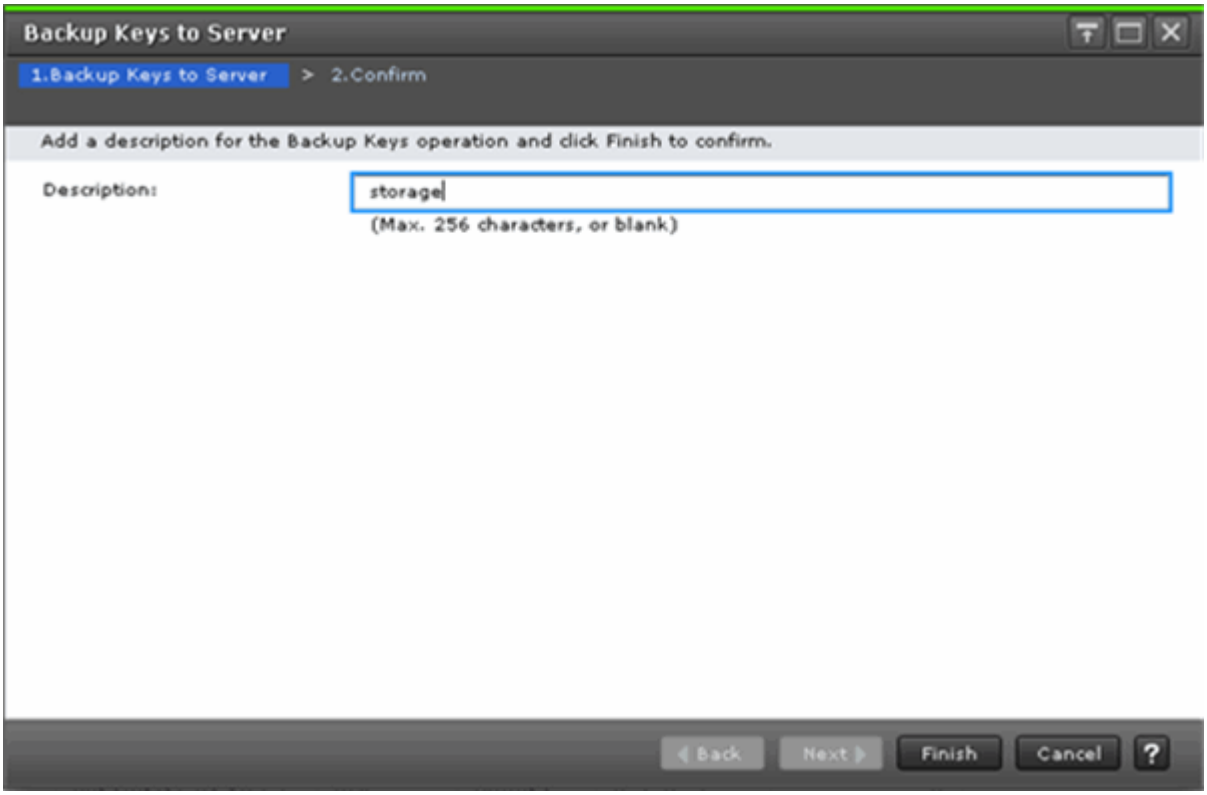
Backup Keys to Server wizard

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

This wizard includes the following windows:

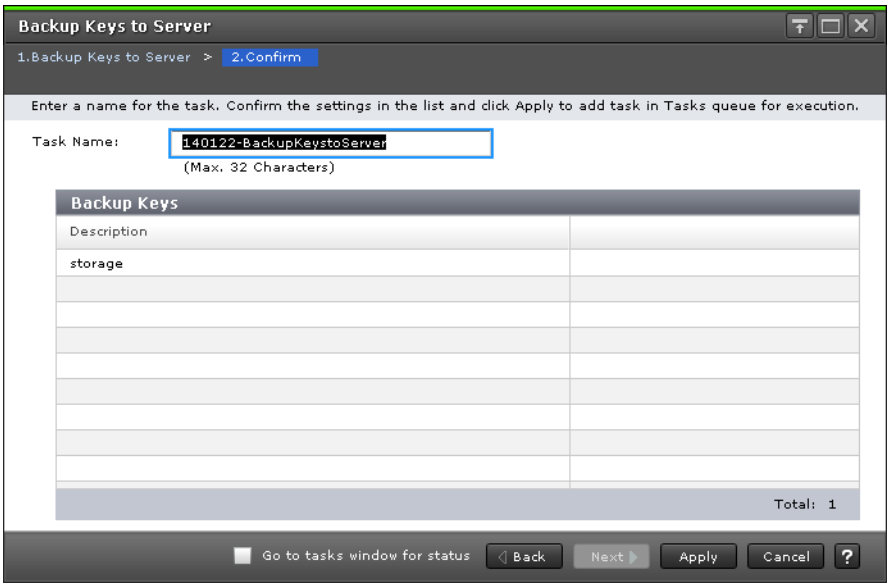
- **Backup Keys to Server** window
- **Confirm** window

Backup Keys to Server window



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

Backup Keys to Server confirmation window



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

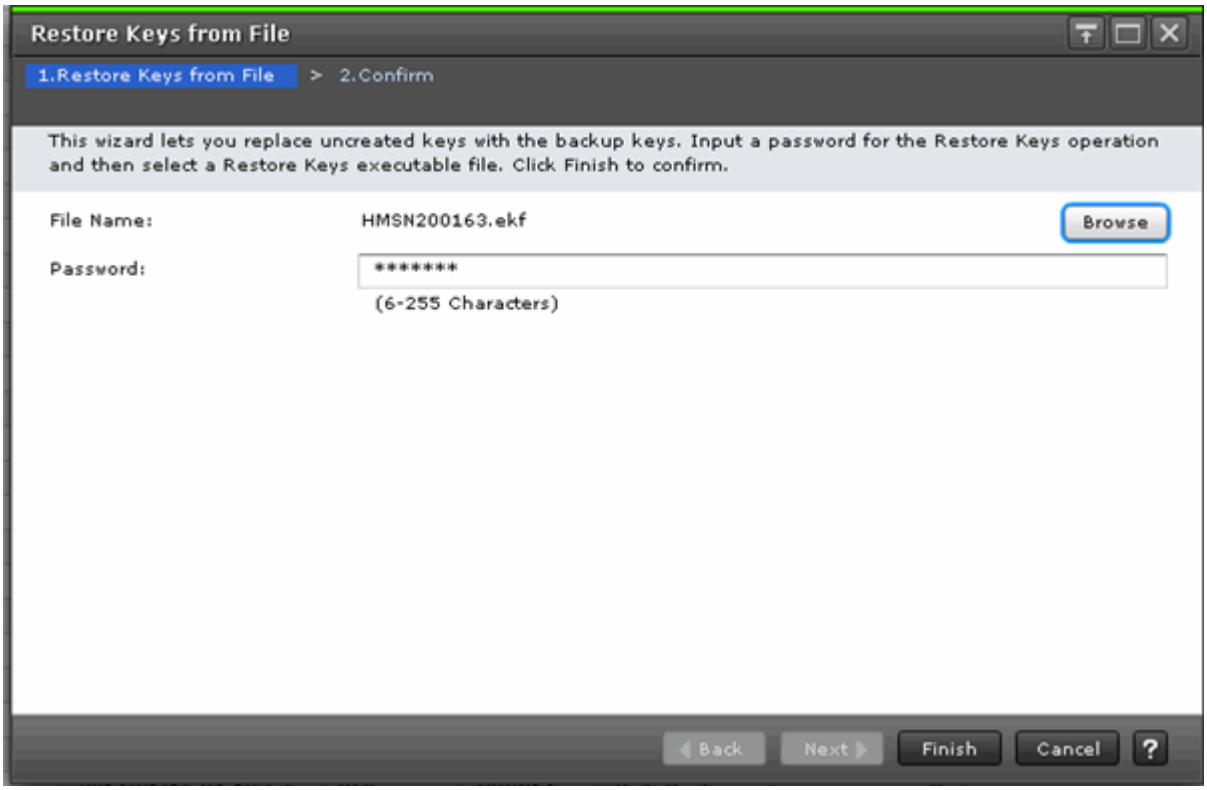
Restore Keys from File wizard

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

This wizard includes the following windows:

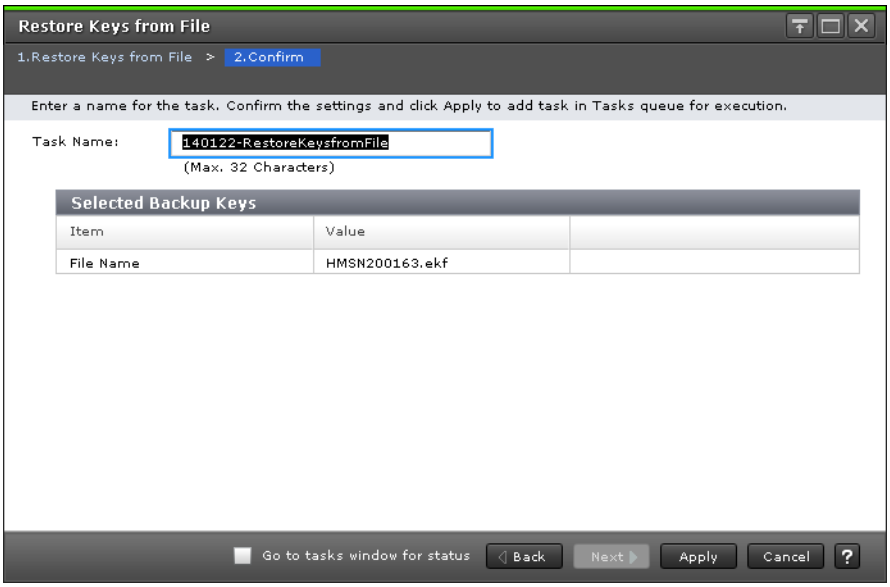
- **Restore Keys from File** window
- **Confirm** window

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 key

Restore Keys confirmation window



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

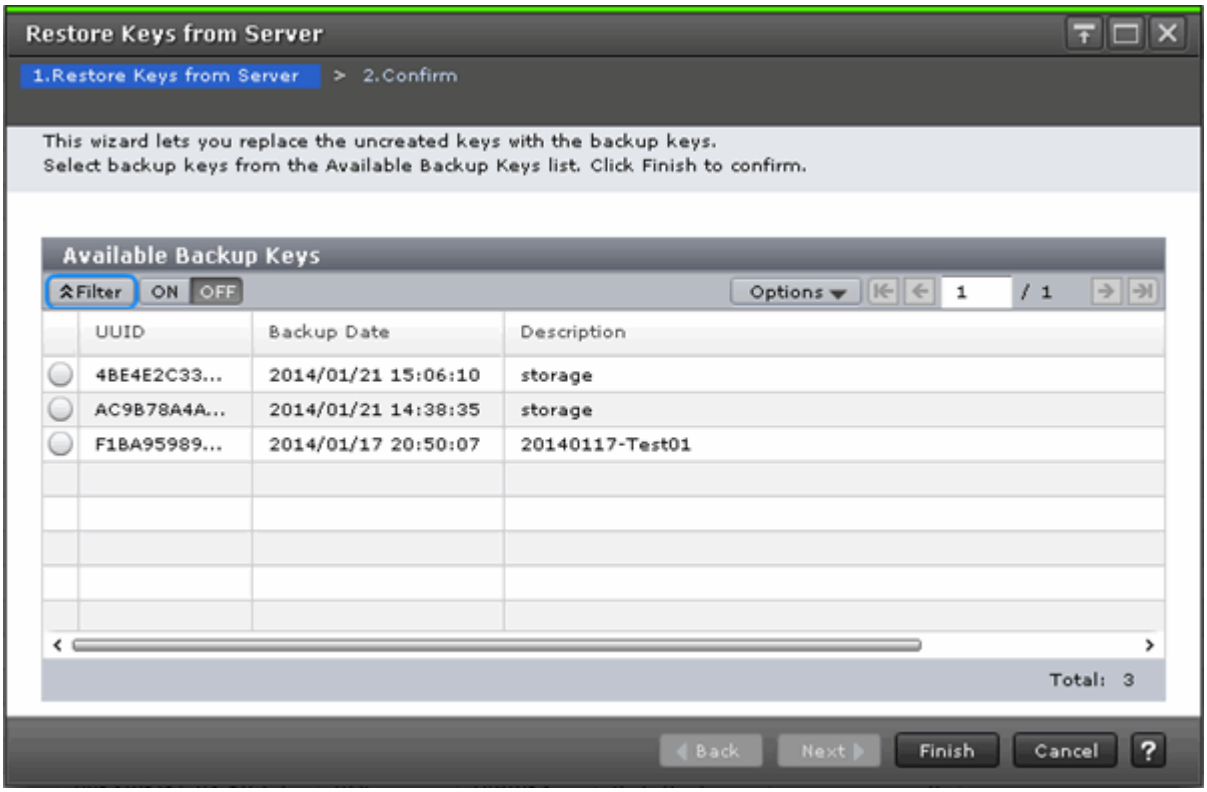
Restore Keys from Server wizard

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

This wizard includes the following windows:

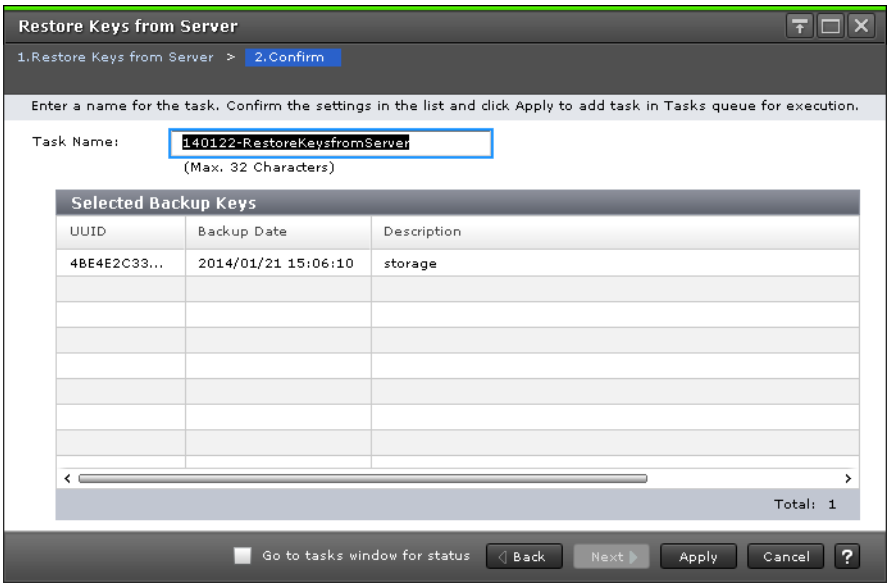
- **Restore Keys from Server** window
- **Confirm** window

Restore Keys from Server window



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

Restore Keys from Server confirmation window



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

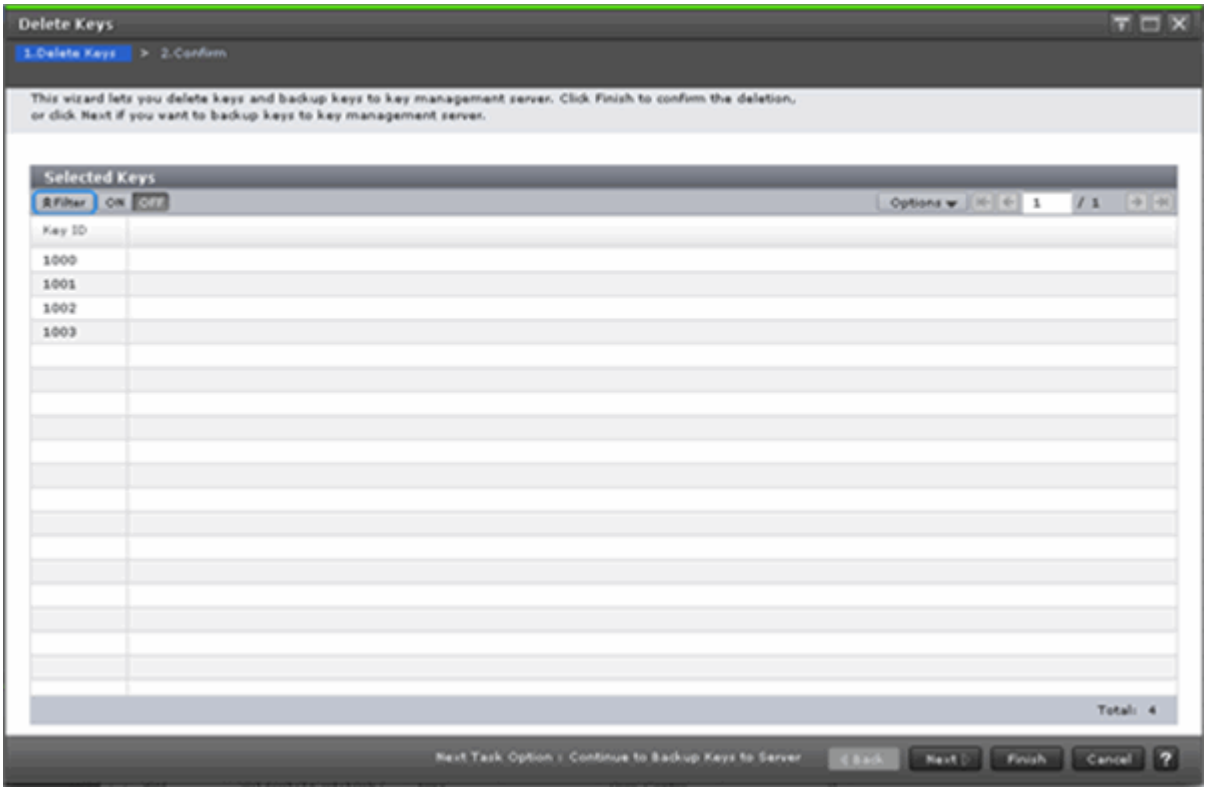
Delete Keys wizard

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

This wizard includes the following windows:

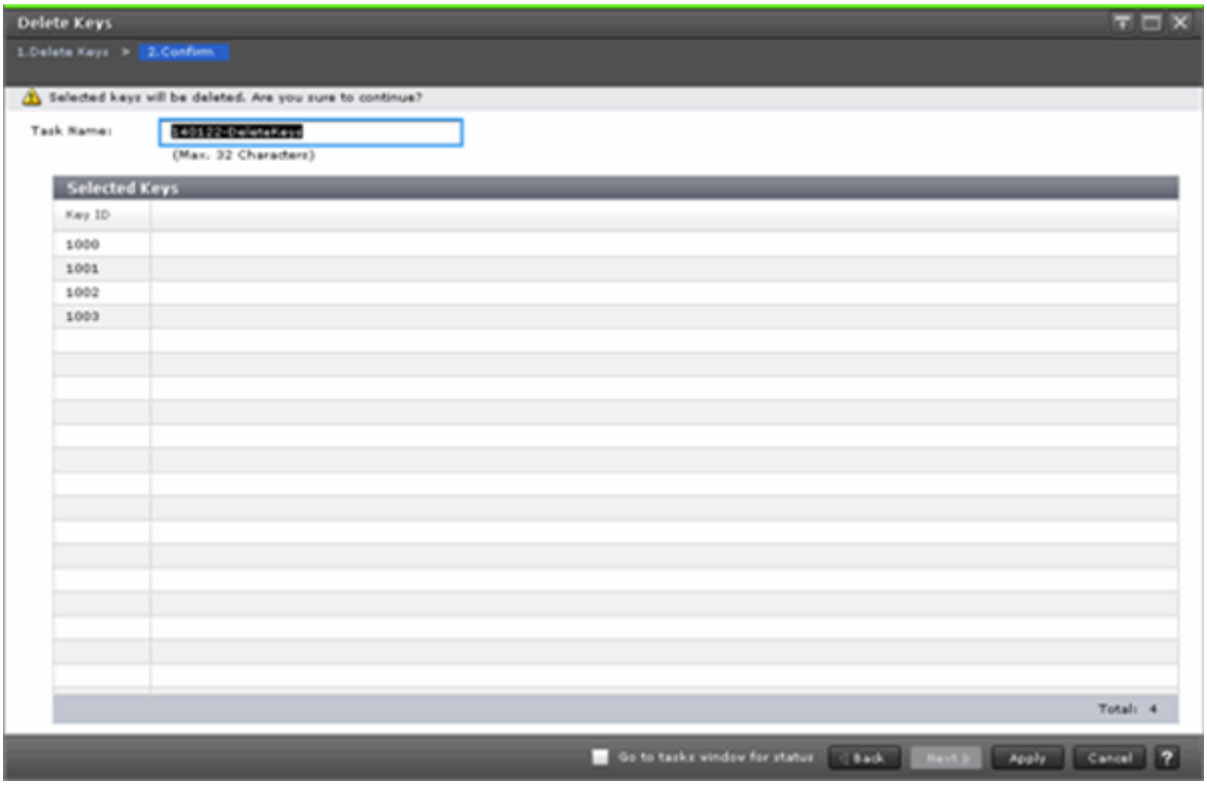
- **Delete Keys** window
- **Confirm** window

Delete Keys window



Item	Description
Key ID	IDs of data encryption keys

Delete Keys confirmation window

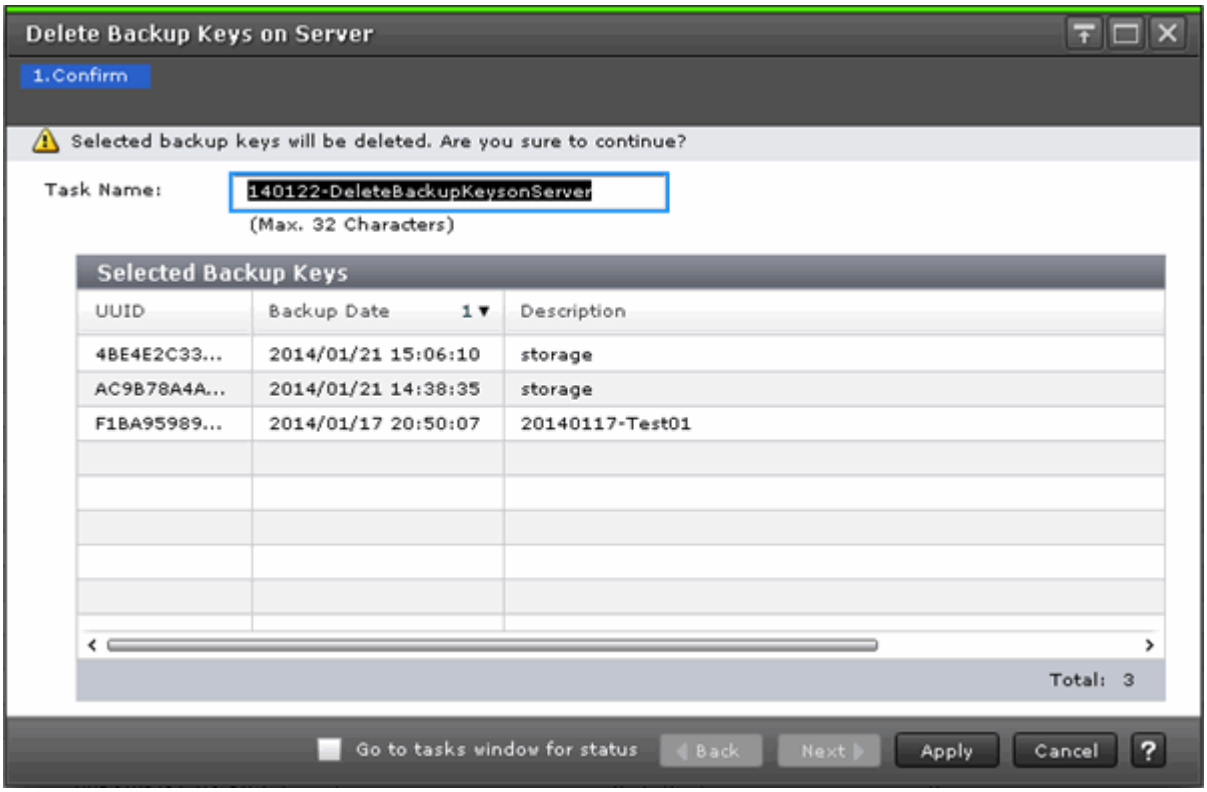


Item	Description
Key ID	The identifiers for the data encryption keys

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.

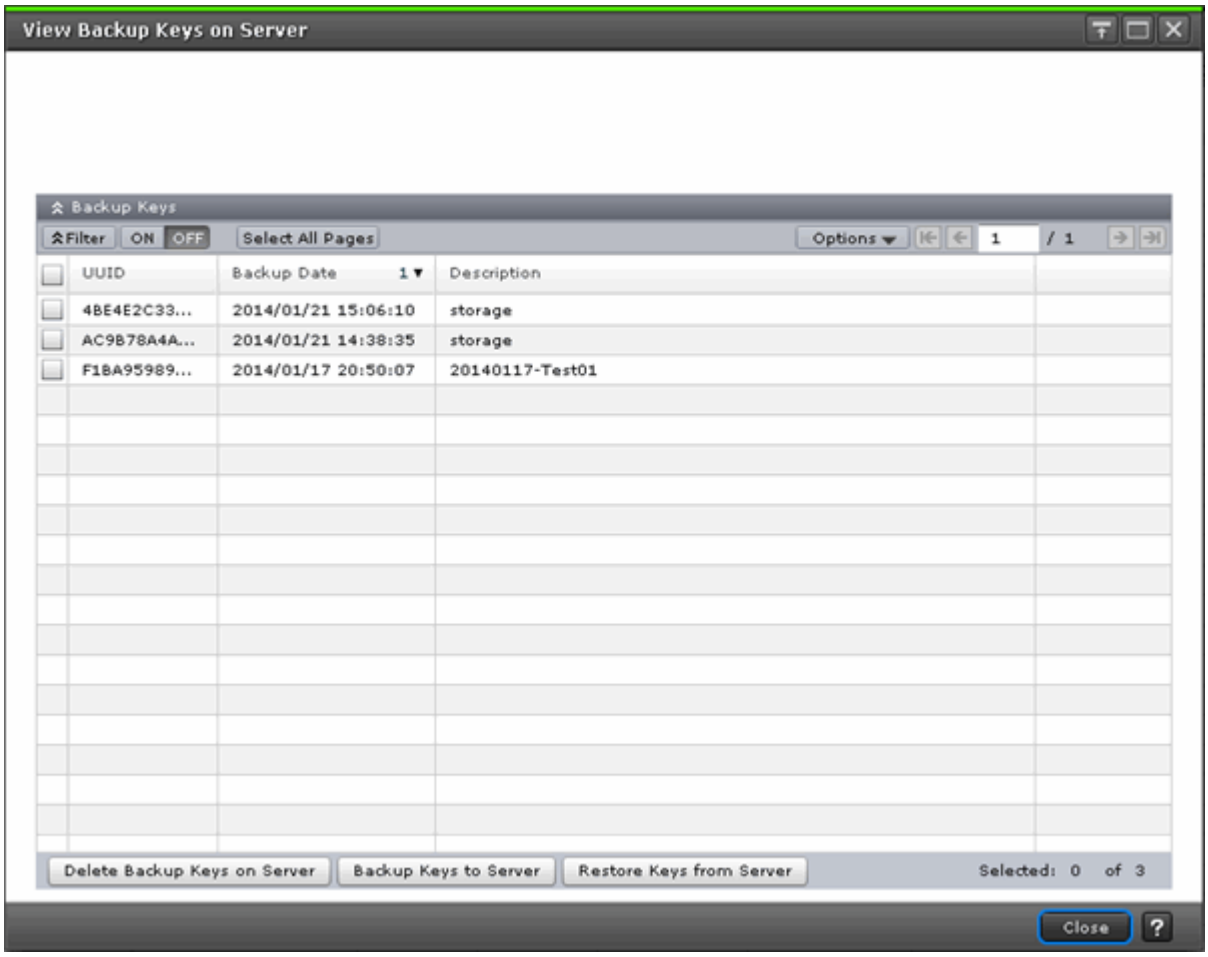


Item	Description
UUID	Shows the UUID of the data encryption key you backed up on the key management server
Backup Date	Shows the time when you backed up the data encryption key on the key management server
Description	Shows the description you typed when you backed up the data encryption key on the key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

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

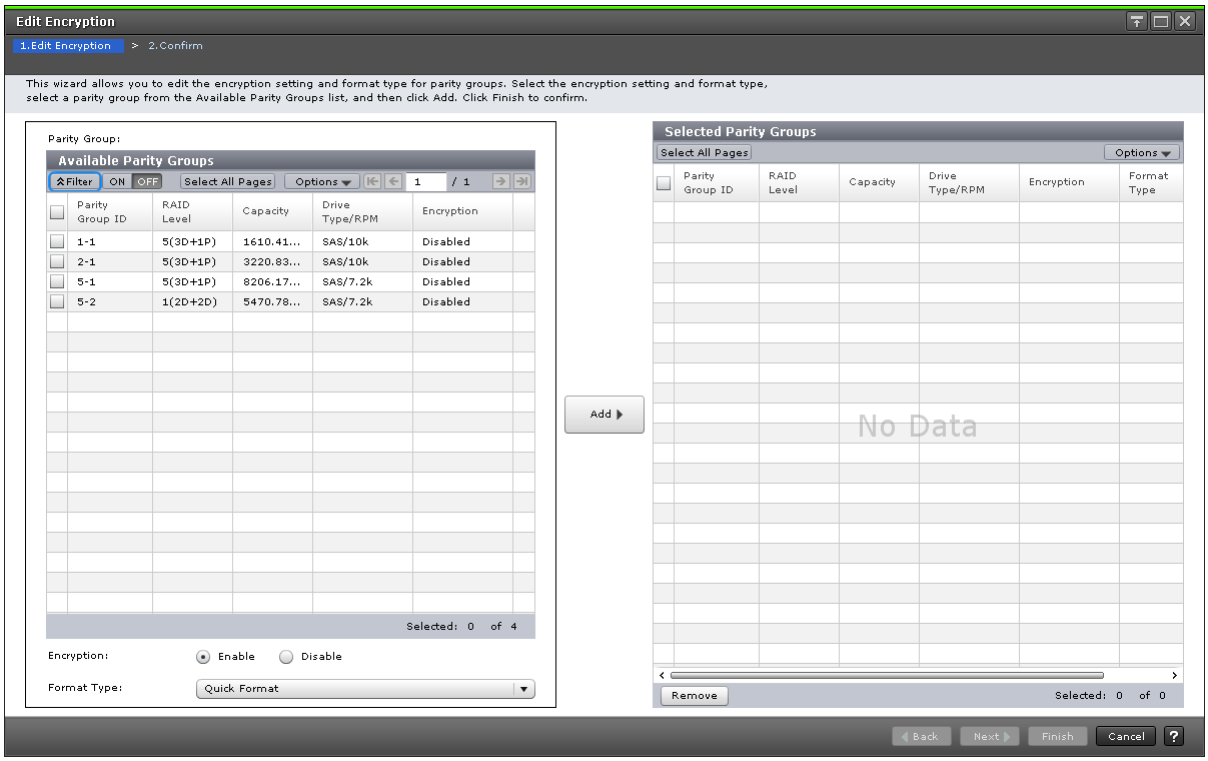
Use the Edit Encryption wizard to do the following:

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

This wizard includes the following windows:

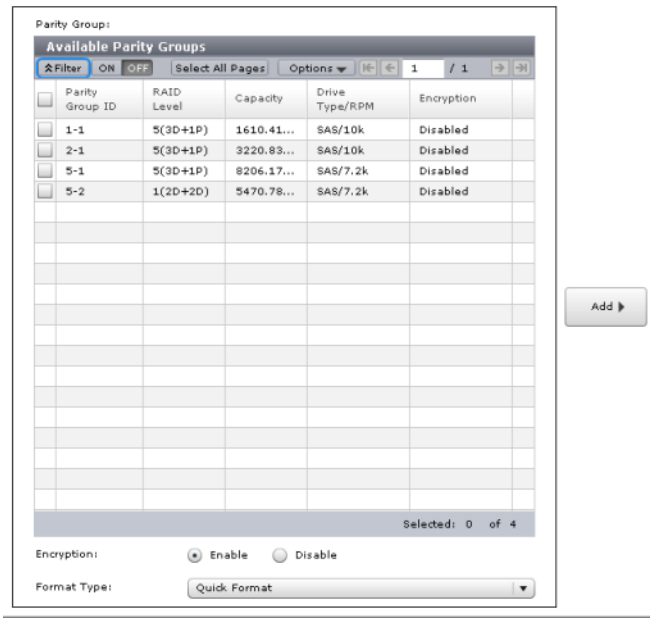
- **Edit Encryption** window
- **Confirm** window

Edit Encryption window



Available Parity Groups table

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



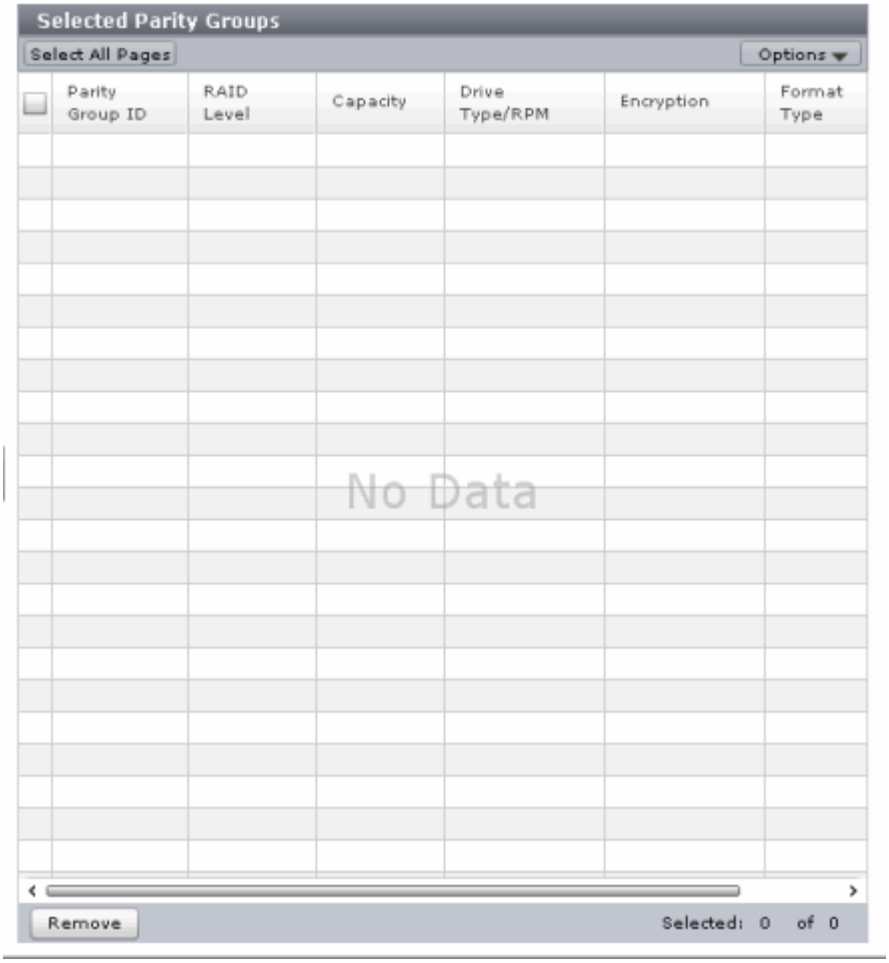
Item	Description
Parity Group ID	Shows the parity group IDs
RAID Level	Shows the RAID level of the parity group For an interleaved parity group, the interleaved number appears after the RAID level. Example: 1(2D+2D)*2
Capacity	Shows the total capacity (unit) of the parity group
Drive Type/RPM	Shows the drive types and RPM (rotation per minute) of the LDEV in the parity group
Encryption	Shows the encryption setting for the parity group. • Enabled: Encryption is enabled. • Disabled: Encryption is disabled. If accelerated compression of the parity group is enabled, do not select Enable for Encryption. If you select Enable for Encryption, an error occurs when performing the task.
Format Type	Select the format types of the parity group. You do not need to format volumes when there are none in the selected 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.

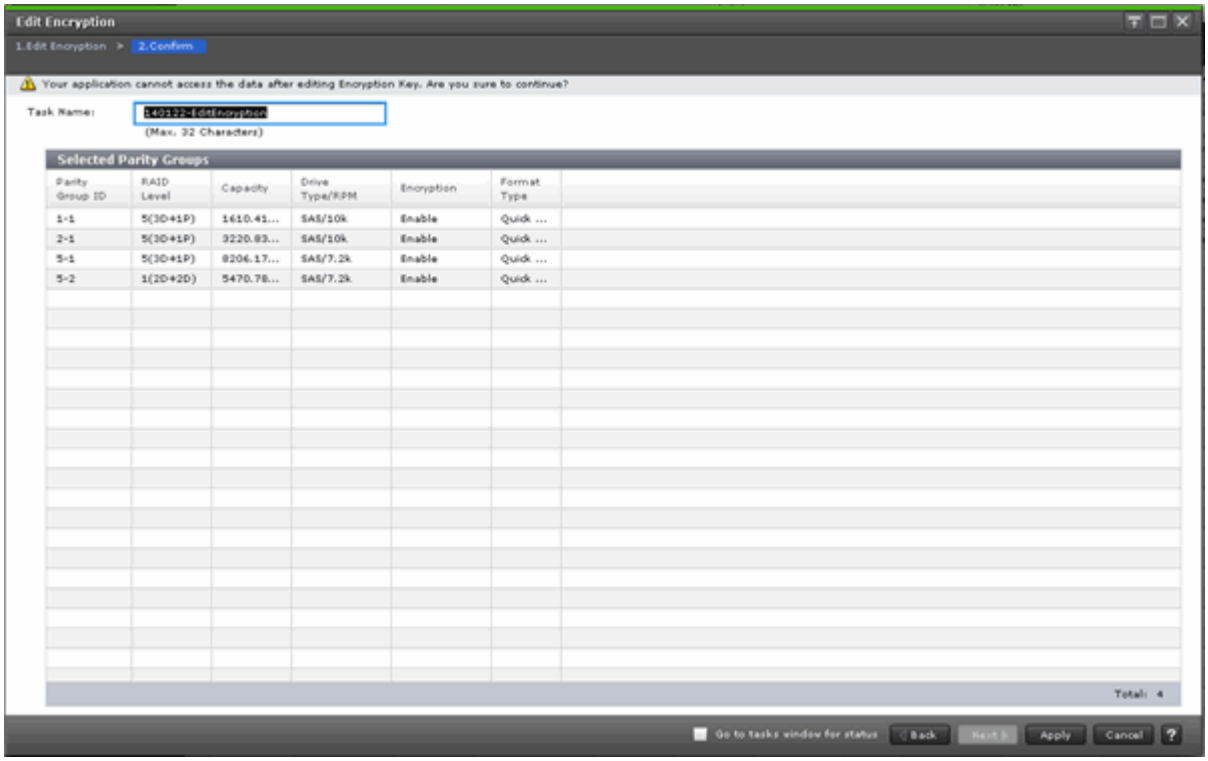


Item	Description
Parity Group ID	Shows parity group IDs
RAID Level	Shows the RAID level of the parity group For an interleaved parity group, the interleaved number appears after the RAID level. Example: 1(2D+2D)*2
Capacity	Shows the total capacity (unit) of the parity group
Drive Type/RPM	Shows the drive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

Item	Description
	You do not need to format volumes when there are none in the selected 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 key and to view a list of the selected parity groups related to the data encryption 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 key.

Item	Description
Parity Group ID	Shows parity group identifier
RAID Level	Shows the RAID level of the parity group

Item	Description
	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 are no volumes 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

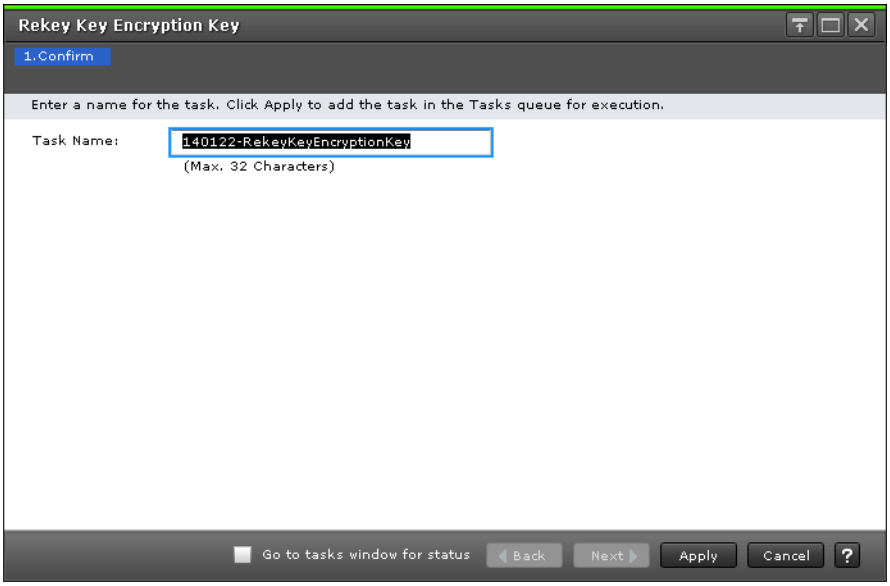
If you change certificate encryption keys, you can use the **Rekey Certificate Encryption Keys** window to rekey certificate encryption keys.



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

Rekey Key Encryption Key window

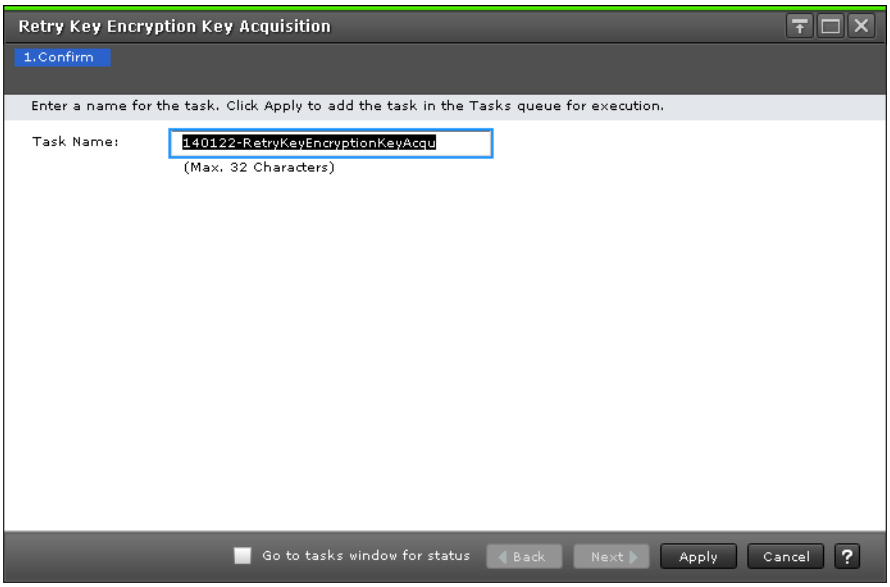
If you change key encryption keys, you can use the **Rekey key Encryption Keys** window to rekey key encryption keys.



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 other means.



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

#

2DC

two-data-center. Refers to the local and remote sites, or data centers, in which TrueCopy (TC) and Universal Replicator (UR) combine to form a remote replication configuration.

In a 2DC configuration, data is copied from a TC primary volume at the local site to the UR master journal volume at an intermediate site, then replicated to the UR secondary volume at the remote site. Since this configuration side-steps the TC secondary volume at the intermediate site, the intermediate site is not considered a data center.

3DC

three-data-center. Refers to the local, intermediate, and remote sites, or data centers, in which TrueCopy and Universal Replicator combine to form a remote replication configuration.

In a 3DC configuration, data is copied from a local site to an intermediate site and then to a remote site (3DC cascade configuration), or from a local site to two separate remote sites (3DC multi-target configuration).

A

administrative logical unit (ALU)

An LU used for the conglomerate LUN structure, a SCSI architecture model. In the conglomerate LUN structure, all host access is through the ALU, which functions as a gateway to sort the I/Os for the subsidiary logical units (SLUs) grouped under the ALU.

The host requests I/Os by using SCSI commands to specify the ALU and the SLUs grouped under the ALU. An ALU is called a Protocol Endpoint (PE) in vSphere. See also *subsidiary logical unit (SLU)*.

ALU

See *administrative logical unit (ALU)*.

ALUA

See *asymmetric logical unit access*.

array

See disk array

asymmetric access

A method of defining a preferred path for sending and receiving data when multiple alternate paths are used between a server and storage systems, such as a cross-path configuration for global-active device. To use, ALUA must be enabled.

asymmetric logical unit access (ALUA)

Asymmetric logical unit access functionality of SCSI. When multiple alternate paths are used to connect storage systems, or a server and one or more storage systems, you can define a preferred path in a storage system, and issue I/O requests from the server to storage systems. If a failure occurs in a preferred path, an alternate path is used. See also *asymmetric access*.

audit log

Files that store a history of the operations performed from Device Manager - Storage Navigator and the commands that the storage system received from hosts, and data encryption operations.

B

back end module (EBEM)

The hardware component that controls the transfer of data between the drives and cache. A BEM consists of a pair of boards. A BEM is also referred to as a *disk adapter* (DKA).

back-end director (BED)

The hardware component that controls the transfer of data between the drives and cache. A BED feature consists of a pair of boards. A BED is also referred to as a disk adapter (DKA) or disk board (DKB).

BED

See *back-end director*.

BEM

See *back end module (BEM)*.

bind mode

In bind mode the Cache Residency Manager extents are used to hold read and write data for specific extent(s) on volume(s). Data written to the Cache Residency Manager bind area is not destaged to the drives. For bind mode, all targeted read and write data is transferred at host data transfer speed.

blade

A computer module, generally a single circuit board, used mostly in servers.

C

cache logical partition (CLPR)

Consists of virtual cache memory that is set up to be allocated to different hosts in contention for cache memory.

capacity

The amount of data storage space available on a physical storage device, usually measured in bytes (MB, GB, TB, and so on).

CCI

Command Control Interface

channel board box (CHBB)

See *host port expansion chassis*.

CHAP

challenge handshake authentication protocol

CHBB

channel board box. See *host port expansion chassis*.

CLPR

See *cache logical partition (CLPR)*.

cluster

Multiple-storage servers working together to respond to multiple read and write requests.

command device

A dedicated logical volume used only by Command Control Interface and Business Continuity Manager to interface with the storage system. Can be shared by several hosts.

controller

The component in a storage system that manages all storage functions. It is analogous to a computer and contains a processors, I/O devices, RAM, power supplies, cooling fans, and other sub-components as needed to support the operation of the storage system.

copy pair

A pair of volumes in which one volume contains original data and the other volume contains the copy of the original. Copy operations can be synchronous or asynchronous, and the volumes of the copy pair can be located in the same storage system (local copy) or in different storage systems (remote copy).

A copy pair can also be called a volume pair, or just pair. A pair created by Compatible FlashCopy® is called a relationship.

copy-on-write (COW)

Point-in-time snapshot copy of any data volume within a storage system. Copy-on-write snapshots only store changed data blocks, therefore the amount of storage capacity required for each copy is substantially smaller than the source volume.

COW

See *copy-on-write (COW)*.

COW Snapshot

Hitachi Copy-on-Write Snapshot

custom volume (CV)

A custom-size volume whose size is defined by the user using Virtual LVI/ Virtual LUN.

CV

See *custom volume*.

CVS

custom volume size

CXFS

clustered version of XFS file system

D

data drive

A physical data storage device that can be either a hard disk drive (HDD) or a flash drive (also called a solid-state device).

DBV

Hitachi Database Validator

DC

data center

delta resync

A disaster recovery solution in which TrueCopy and Universal Replicator systems are configured to provide a quick recovery using only differential data stored at an intermediate site.

device

A physical or logical unit with a specific function.

device emulation

Indicates the type of logical volume. Mainframe device emulation types provide logical volumes of fixed size, called logical volume images (LVIs), which contain EBCDIC data in CKD format. Typical mainframe device emulation types include 3390-9 and 3390-M. Open-systems device emulation types provide logical volumes of variable size, called logical units (LUs), that contain ASCII data in FBA format. The typical open-systems device emulation type is OPEN-V.

disaster recovery

A set of procedures to recover critical application data and processing after a disaster or other failure.

disk adapter (DKA)

The hardware component that controls the transfer of data between the drives and cache. A DKA feature consists of a pair of boards.

disk array

Disk array, or just array, is a complete storage system, including the control and logic devices, storage devices (HDD, SSD), connecting cables, and racks

disk controller (DKC)

The hardware component that manages front-end and back-end storage operations. The term DKC can refer to the entire storage system or to the controller components.

DKC

See *disk controller (DKC)*.

DKCMAIN

disk controller main. Refers to the microcode or software for the storage system.

DKU

disk unit. Refers to the cabinet (floor model) or rack-mounted hardware component that contains data drives and no controller components.

dump

A collection of data that is saved to a file when an error or crash occurs. The data is used by support personnel to determine the cause of the error or crash.

Dump tool

Downloads Device Manager - Storage Navigator configuration information onto recording media for backup and troubleshooting purposes.

Dynamic Provisioning (HDP)

An approach to managing storage. Instead of "reserving" a fixed amount of storage, it removes capacity from the available pool when data is actually written to disk.

E

EBED

See *encrypting back end director (EBED)*.

EBEM

See *encrypting back end module (EBEM)*.

emulation

The operation of a storage system to emulate the characteristics of a different storage system. For device emulation, the mainframe host recognizes the logical devices on the storage system as 3390-x devices. For controller emulation, the mainframe host recognizes the control units (CUs) on the storage system as 2105 or 2107 controllers.

The storage system operates the same as the storage system being emulated.

emulation group

A set of device emulation types that can be intermixed within a RAID group and treated as a group.

encrypting back end module (EBEM)

A special back end module (BEM) that provides data encryption.

encrypting back-end director (EBED)

A special back-end director (BED) that provides data encryption.

external application

A software module that is used by a storage system but runs on a separate platform.

external volume

A logical volume whose data resides on drives that are physically located outside the Hitachi storage system.

F

FC

Fibre Channel; FlashCopy

FC-AL

fibre-channel arbitrated loop

FCP

fibre-channel protocol

FCSP

fibre-channel security protocol

FED

See front-end director.

FICON

Fibre Connectivity

flash drive

A data drive that uses a solid-state memory device instead of a rotating hard disk.

flash module

A high speed data storage device that includes a custom flash controller and several flash memory sub-modules on a single PCB.

FMD

See flash module

front-end director (FED)

The hardware component that processes channel commands from hosts and manages host access to cache.

H

HBA

host bus adapter

HCS

Hitachi Command Suite - a set of software applications included in the system firmware. Via the GUI, they are used to configure, control, and monitor the storage system.

HDD

hard disk drive

HDT

Hitachi Dynamic Tiering

HDU

hard disk unit

head LDEV

See *top LDEV*.

host group

A group of hosts of the same operating system platform.

host mode

Operational modes that provide enhanced compatibility with supported host platforms. Used with fibre-channel ports on RAID storage systems.

host mode option

Additional options for fibre-channel ports on RAID storage systems. Provide enhanced functionality for host software and middleware.

host port expansion chassis

A chassis that increases the number of front-end directors connected to the disk controller of a VSP G800 or VSP F800. This chassis is also referred to as a *channel board box (CHBB)*.

I

in-system replication

The original data volume and its copy are located in the same storage system. ShadowImage in-system replication provides duplication of logical volumes; Thin Image in-system replication provides "snapshots" of logical volumes that are stored and managed as virtual volumes (V-VOLs).

See also *remote replication*.

internal volume

A logical volume whose data resides on drives that are physically located within the storage system. See also *external volume*.

J

JNL

journal

journal volume

A volume that records and stores a log of all events that take place in another volume. In the event of a system crash, the journal volume logs are used to restore lost data and maintain data integrity.

In Universal Replicator, differential data is held in journal volumes on until it is copied to the S-VOL.

JRE

Java Runtime Environment

K

key management server

A server that manages encryption keys. Encryption keys can be backed up to, and restored from, a key management server that complies with the Key Management Interoperability Protocol (KMIP).

keypair

Two mathematically-related cryptographic keys: a private key and its associated public key.

L

LBA

logical block address

LCP

local control port; link control processor

LD

local directory; logical device

LDAP

lightweight directory access protocol

LDEV

logical device

LDKC

See *logical disk controller (LDKC)*.

LDM

Logical Disk Manager

license key

A specific set of characters that unlocks an application and allows it to be used.

local control port (LCP)

A serial-channel (ESCON) port configured to receive I/Os from a host or remote I/Os from a TrueCopy main control unit (MCU).

local copy

See *in-system replication*.

logical device (LDEV)

An individual logical data volume (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 logical disk controller (LDKC) number, control unit (CU) number, and LDEV number. The LDEV IDs within a storage system do not change.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 disk controller (LDKC)

A group of 255 control unit (CU) images in the RAID storage system that is controlled by a virtual (logical) storage system within the single physical storage system. For example, the Hitachi Universal Storage Platform V storage system supports two LDKCs, LDKC 00 and LDKC 01.

logical partition (LPAR)

A subset of a system's hardware resources that is virtualized as a separate system. For a storage system, logical partitioning can be applied to cache memory and/or storage capacity.

logical unit (LU)

A logical volume that is configured for use by open-systems hosts (for example, OPEN-V).

logical unit (LU) path

The path between an open-systems host and a logical unit.

logical volume (LV)

See *volume*.

logical volume image (LVI)

A logical volume that is configured for use by mainframe hosts (for example, 3390-9).

LU

See *logical unit (LU)*.

LUN

See logical unit number

LV

logical volume

LVI

See *logical volume image*.

M

MF, M/F

mainframe

modify mode

The mode of operation of Device Manager - Storage Navigator that allows changes to the storage system configuration. See also *view mode*.

O

OPEN-V

A logical unit (LU) of user-defined size that is formatted for use by open-systems hosts.

OPEN-x

A logical unit (LU) of fixed size (for example, OPEN-3 or OPEN-9) that is used primarily for sharing data between mainframe and open-systems hosts using Hitachi Cross-OS File Exchange.

P

P-VOL

This term is used only in the earlier version of the Device Manager - Storage Navigator GUI (still in use) for the primary volume. See *primary volume*.

pair

Two logical volumes in a replication relationship in which one volume contains original data to be copied and the other volume contains the copy of the original data. The copy operations can be synchronous or asynchronous, and the pair volumes can be located in the same storage system (in-system replication) or in different storage systems (remote replication).

parity group

See *RAID group*.

PAV

Hitachi Compatible PAV

PCB

printed circuit board

PCIe channel board

See *PCIe module*.

PCIe module

A module that connects a host port expansion chassis to the disk controller of a VSP G800 or VSP F800. This module is also referred to as a *PCIe channel board*.

PDEV

physical device

PG

parity group. See *RAID group*.

physical device

See *device*.

pool

A set of volumes that are reserved for storing pool volumes (pool-VOL), and used by Thin Image, Dynamic Provisioning, Dynamic Provisioning for Mainframe, Dynamic Tiering, Dynamic Tiering for Mainframe, active flash, or active flash for mainframe data.

A set of volumes that are reserved for storing pool volumes (pool-VOL), and used by Thin Image, Dynamic Provisioning, Dynamic Tiering, or active flash data.

pool volume (pool-VOL)

A logical volume that is reserved for storing snapshot data for Thin Image operations or write data for Dynamic Provisioning, Dynamic Provisioning for Mainframe, Dynamic Tiering, Dynamic Tiering for Mainframe, active flash, or active flash for mainframe.

A logical volume that is reserved for storing snapshot data for Thin Image operations or write data for Dynamic Provisioning, Dynamic Tiering, or active flash.

port attribute

Indicates the type of fibre-channel port: target, RCU target, or initiator.

primary volume (P-VOL)

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

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

See also *secondary volume*.

prio

priority mode. Used in Cache Residency Manager.

Q

quick format

The quick format feature in Virtual LVI/Virtual LUN in which the formatting of the internal volumes is done in the background. This allows system configuration (such as defining a path or creating a TrueCopy pair) before the formatting is completed. To execute quick formatting, the volumes must be in blocked status.

quick restore

A reverse resynchronization in which no data is actually copied: the primary and secondary volumes are swapped.

quorum disk

Used to determine the volume in the global-active device pair on which server I/O should continue when a failure occurs in a path or a storage system. Quorum disks reside in an external storage system.

R

RAID

redundant array of inexpensive disks

RAID group

A set of RAID disks that have the same capacity and are treated as one group for data storage and recovery. A RAID group contains both user data and parity information. This allows user data to be accessed in the event that one or more of the drives within the RAID group are not available. The RAID level of a RAID group determines the number of data drives and parity drives and how the data is "striped" across the drives. For RAID1, user data is duplicated within the RAID group, so there is no parity data for RAID1 RAID groups.

A RAID group can also be called an array group or a parity group.

RAID level

The type of RAID implementation. RAID levels include RAID0, RAID1, RAID2, RAID3, RAID4, RAID5 and RAID6.

RCU

See *remote control unit*.

RCU target port

A fibre-channel port that is configured to receive remote I/Os from an initiator port on another storage system.

remote control unit (RCU)

A storage system at a secondary or remote site that is configured to receive remote I/Os from one or more storage systems at the primary or main site.

remote copy

See *remote replication*.

resync

resynchronize.

RMI

Remote Method Invocation

S

S-VOL

See *secondary volume* or *source volume*. When used for "secondary volume", "S-VOL" is only seen in the earlier version of the Device Manager - Storage Navigator GUI (still in use).

SAS

serial-attached SCSI

secondary volume (S-VOL)

The volume in a copy pair that is the copy of the original data on the primary volume (P-VOL). The following Hitachi products use the term "secondary volume": Thin Image, Copy-on-Write Snapshot, ShadowImage, TrueCopy, Universal Replicator, Universal Replicator for Mainframe, and High Availability Manager.

See also *primary volume*.

service information message (SIM)

Messages generated by a RAID storage system when it detects an error or service requirement. SIMs are reported to hosts and displayed on Device Manager - Storage Navigator.

service processor

The computer in a storage system that hosts the Device Manager - Storage Navigator software and is used to configure and maintain the storage system.

severity level

Applies to service information messages (SIMs) and Device Manager - Storage Navigator error codes.

SFP

small form-factor pluggable

shared memory

Memory that exists logically in the cache. It stores common information about the storage system and the cache management information (directory). The storage system uses this information to control exclusions and differential table information. Shared memory is managed in two segments and is used when copy pairs are created.

In the event of a power failure, the shared memory is kept alive by the cache memory batteries while the data is copied to the cache flash memory (SSDs).

shredding

See *volume shredding*.

SI

Hitachi ShadowImage

SIM

See *service information message*.

SIz

ShadowImage for Mainframe

size

Generally refers to the storage capacity of a memory module or cache. Not usually used for storage of data on disk or flash drives.

SLU

See *subsidiary logical unit*.

SM

shared memory

SMTP

simple mail transfer protocol

SN

Device Manager - Storage Navigator

snapshot

A point-in-time virtual copy of a Hitachi Thin Image primary volume (P-VOL). The snapshot is maintained when the P-VOL is updated by storing pre-updated data (snapshot data) in a data pool.

SNMP

See *Simple Network Management Protocol*.

SOM

See *system option mode*.

source volume (S-VOL)

Used only in the earlier version of the Device Manager - Storage Navigator GUI (still in use). This is the volume in a mainframe copy pair containing the original data that is duplicated on the target volume (T-VOL). The following Hitachi products use the term source volume: ShadowImage for Mainframe, Dataset Replication, and Compatible FlashCopy®.

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

See also *source volume*.

space

Generally refers to the data storage capacity of a disk drive or flash drive.

SRM

Storage Replication Manager

SSD

solid-state drive. Also called flash drive.

SSID

See *storage subsystem identifier*.

SSL

secure socket layer

storage cluster

See *cluster*.

storage tiers

See *tiered storage*.

subsidiary logical unit (SLU)

An LU used for the conglomerate LUN structure, a SCSI architecture model. An SLU is an LU that stores actual data. You can use a DP-VOL or snapshot data (or a V-VOL allocated to snapshot data) as an SLU. All host access to SLUs is through the administrative logical unit (ALU). An SLU is called a virtual volume (VVol) in vSphere. See *administrative logical unit*.

SVP

See *service processor*.

SVS

Storage Virtualization System

SW, sw

short wavelength, software

syslog

The file on the SVP that includes both syslog and audit log information, such as the date and time.

system disk

The volume from which an open-systems host boots.

system option mode (SOM)

Additional operational parameters for the RAID storage systems that enable the storage system to be tailored to unique customer operating requirements. SOMs are set on the service processor.

T

T-VOL

See *target volume*.

target port

A fibre-channel port that is configured to receive and process host I/Os.

target volume (T-VOL)

The volume in a mainframe copy pair that is the copy of the original data on the source volume (S-VOL). The term is used only in the earlier version of the Device Manager - Storage Navigator GUI (still in use), for the following Hitachi products: ShadowImage for Mainframe, Dataset Replication, and Compatible FlashCopy® V2.

See also *source volume*.

TC

Hitachi TrueCopy

TCz

Hitachi TrueCopy for mainframe

TI

See Thin Image.

tiered storage

A layered structure of performance levels, or tiers, that matches data access requirements with the appropriate performance tiers. The tiers are:

Tier 1: Static content. Tier 1 is fully supported computing expected to be production quality.

Tier 2: Application logic. Tier 2 platforms are not supported by the security officer and release engineering teams. Tier 2 systems are targeted for Tier 1 support, but are still under development.

Tier 3: Database. Tier 3 platforms are architectures for which hardware is not or will not be available or that are considered legacy systems unlikely to see broad future use.

Tier 4 systems are not supported.

total capacity

The aggregate amount of storage space in a data storage system.

TPF

Transaction Processing Facility

U

UR

Hitachi Universal Replicator

URz

Hitachi Universal Replicator software for Mainframe

V

V-VOL

virtual volume

VDEV

See *virtual device*.

view mode

The mode of operation of Device Manager - Storage Navigator that allows viewing only of the storage system configuration. The two Device Manager - Storage Navigator modes are view mode and modify mode.

virtual device (VDEV)

A group of logical devices (LDEVs) in a RAID group. A VDEV typically consists of some fixed volumes (FVs) and some free space. The number of fixed volumes is determined by the RAID level and device emulation type.

Virtual LVI/LUN

A custom-size volume whose size is defined by the user using Virtual LVI/LUN. Also called a custom volume (CV).

virtual volume (V-VOL)

A logical volume in a storage system. A V-VOL has no physical storage space.

Thin Image uses V-VOLs as secondary volumes of copy pairs.

In Dynamic Provisioning, Dynamic Provisioning for Mainframe, Dynamic Tiering, Dynamic Tiering for Mainframe, active flash, and active flash for mainframe, V-VOLs are called DP-VOLs.

In Dynamic Provisioning, Dynamic Tiering, and active flash, V-VOLs are called DP-VOLs.

VLUN

Hitachi Virtual LUN

VLVI

Hitachi Virtual LVI

VM

volume migration; volume manager

volume (VOL or vol)

A logical device (LDEV), or a set of concatenated LDEVs in the case of LUSE, that has been defined to one or more hosts as a single data storage unit. An open-systems volume is called a logical unit (LU), and a mainframe volume is called a logical volume image (LVI).

volume shredding

Deleting the user data on a volume by overwriting all data in the volume with dummy data.

W

WWN

worldwide name

X

XRC

IBM® Extended Remote Copy

Index

A

AES-256 14
audit log 54
audit logging 19

D

data encryption operations
  audit logging of 19
  disabling encryption 18, 42
  enabling encryption 17, 40, 44
  encrypting existing data 17, 18
  troubleshooting 54
decrypting data 42
disabling encryption 42

E

emulation types 14
enabling data encryption workflow 40
encryption key operations
  audit logging of 19
  backing up the key 16, 35
  restoring the key 44
  troubleshooting 54
encryption setting status 81, 86
external volumes 22

L

license key 23

P

primary backup key 16, 35

R

requirements 22
  Device Manager - Storage Navigator 22
  host platforms 22
  license key 22
  microcode 22
  password for encryption key 70
  volume types 22

T

technical support 56
troubleshooting 54

V

volume types 14

X

XTS mode 14

Hitachi Data Systems

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

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

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

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

Contact Us
www.hds.com/en-us/contact.html

Hitachi Data Systems

MK-92RD8009-10

October 2016