HITACHI
Inspire the Next

Hitachi Universal Storage Platform V
Hitachi Universal Storage Platform VM
Hitachi Data-at-Rest Encryption Implementation User's Guide

FastFind Links

Hitachi Data Systems

MK-98RD6723-02

Copyright © 2009 Hitachi, Ltd., Hitachi Data Systems Corporation, ALL RIGHTS RESERVED

Notice: No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written permission of Hitachi, Ltd. and Hitachi Data Systems Corporation (hereinafter referred to as “Hitachi Data Systems”).

Hitachi, Ltd. and Hitachi Data Systems reserve the right to make changes to this document at any time without notice and assume no responsibility for its use. Hitachi, Ltd. and Hitachi Data Systems products and services can only be ordered under the terms and conditions of Hitachi Data Systems’ applicable agreements. All of the features described in this document may not be currently available. Refer to the most recent product announcement or contact your local Hitachi Data Systems sales office for information on feature and product availability.

This document contains the most current information available at the time of publication. When new and/or revised information becomes available, this entire document will be updated and distributed to all registered users.

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

ShadowImage and TrueCopy are registered trademarks or trademarks of Hitachi Data Systems.

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

Contents

Preface

This document describes and provides instructions for using the Hitachi Data-at-Rest Encryption feature to configure and perform encryption operations on Hitachi Universal Storage Platform V (USP V) and Hitachi Universal Storage Platform VM (USP VM) storage systems.

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

This preface includes the following information:

Notice: The use of the Hitachi Data-At-Rest Encryption feature and all other Hitachi Data Systems products is governed by the terms of your agreement(s) with Hitachi Data Systems.

Intended Audience

This document is intended for system administrators, Hitachi Data Systems representatives, and Authorized Service Providers who are involved in installing, configuring, and operating the Hitachi Universal Storage Platform V and VM storage systems.

This document assumes the following:

- The user has a background in data processing and understands RAID storage systems and their basic functions.
- The user is familiar with the Universal Storage Platform V/VM storage system and has read the *Universal Storage Platform V/VM User and Reference Guide*.
- The user is familiar with the Storage Navigator software for the Universal Storage Platform V/VM and has read the *Storage Navigator User's Guide*.
- The user is familiar with data encryption and its application within the storage ecosystem.

Product Version

This document revision applies to Universal Storage Platform V/VM microcode 60-05-0*x* and higher.

Document Revision Level

Revision	Date	Description
MK-98RD6723-P	November 2008	Preliminary Release
MK-98RD6723-00	December 2008	Initial Release
MK-98RD6723-01	March 2009	Revision 1, supersedes and replaces MK-98RD6723-00
MK-98RD6723-02	November 2009	Revision 2, supersedes and replaces MK-98RD6723-01

Source Documents for this Revision

- Not applicable.

Changes in this Revision

This revision includes editorial changes that enhance readability and usability. In addition, the following information has been added:

- Interoperability (see Interoperability Considerations).
- Troubleshooting (see Table 5-1).

Document Organization

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

Chapter	Description
About Hitachi Data-at-Rest Encryption	Provides an overview of Data-at-Rest Encryption and describes the encryption specifications and operations.
Preparing for Data-at-Rest Encryption Operations	Specifies the system requirements and provides instructions for preparing for Data-at-Rest Encryption operations.
Using the Encryption GUI	Describes the Storage Navigator windows and dialog boxes for Data-at-Rest Encryption operations.
Performing Data-at-Rest Encryption Operations	Provides instructions for performing Data-at-Rest Encryption operations.
Troubleshooting	Provides troubleshooting information for Data-at-Rest Encryption operations.
Acronyms and Abbreviations	Defines the acronyms and abbreviations used in this document.
Index	Lists the topics in this document in alphabetical order.

Document Conventions

The terms “Universal Storage Platform V” and “Universal Storage Platform VM” refer to all models of the Hitachi Universal Storage Platform V and VM storage systems, unless otherwise noted.

This document uses the following typographic conventions:

Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels. Example: Click **OK**.
Italic	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: copy *source-file target-file* ***Note:*** Angled brackets (< >) are also used to indicate variables.
screen/code	Indicates text that is displayed on screen or entered by the user. Example: `# pairdisplay -g oradb`
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: `# pairdisplay -g <group>` ***Note:*** Italic font is also used to indicate variables.
[ ] 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.
underline	Indicates the default value. Example: [a | b]

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

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

Convention for Storage Capacity Values

Physical storage capacity values (e.g., disk drive capacity) are calculated based on the following values:

1 KB = 1,000 bytes
1 MB = $1,000^2$ bytes
1 GB = $1,000^3$ bytes
1 TB = $1,000^4$ bytes
1 PB = $1,000^5$ bytes

Logical storage capacity values (e.g., logical device capacity) are calculated based on the following values:

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 block = 512 bytes

Getting Help

If you need to call the Hitachi Data Systems Support Center, make sure to provide as much information about the problem as possible, including:

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

The Hitachi Data Systems customer support staff is available 24 hours a day, seven days a week. If you need technical support, please call:

- United States: (800) 446-0744
- Outside the United States: (858) 547-4526

Comments

Please send us your comments on this document: doc.comments@hds.com. Include the document title, number, and revision, and refer to specific section(s) and paragraph(s) whenever possible.

Thank you! (All comments become the property of Hitachi Data Systems.)

1

About Hitachi Data-at-Rest Encryption

This chapter describes the Hitachi Data-at-Rest Encryption feature:

- ☐ Hitachi Data-at-Rest Encryption
- ☐ Encryption Specifications
- ☐ Encryption Key Operations
- ☐ Data Encryption Operations
- ☐ Audit Logging of Encryption Events

Hitachi Data-at-Rest Encryption

The Hitachi Data-at-Rest Encryption feature of the Hitachi Universal Storage Platform V (USP V) and Universal Storage Platform VM (USP VM) enables users to implement and manage data encryption on the storage system. Data encryption prevents “leakage” of information from the storage system, for example, during disk drive replacement or in the case of theft.

The Data-at-Rest Encryption feature has two components: the encrypting back-end director (EBED) hardware component and the Encryption License Key software license. Data-at-Rest Encryption provides hardware-based strong encryption (AES-256) that is compatible with both open and mainframe systems. Encryption can be applied to some or all of the internal drives with no throughput or latency impacts for data I/O and little or no disruption to existing applications and infrastructure. Data-at-Rest Encryption includes integrated key management functionality that is both simple and safe to use.

Hitachi Data-at-Rest Encryption has the added benefit of being data-center friendly: it uses very little additional power (equivalent of a 25-watt light bulb), produces only negligible amounts of additional heat, and requires no additional floor or rack space.

Hitachi Data-at-Rest Encryption operations are performed using the Hitachi Storage Navigator software for the Universal Storage Platform V/VM storage system. Storage Administrator and Encryption Administrator access to Storage Navigator are required for data encryption operations. For information about Storage Navigator and the Storage Administrator and Encryption Administrator roles, see the *Storage Navigator User’s Guide*.

Encryption Specifications

Item		Specification
Hardware specifications	Encryption algorithm	Advanced Encryption Standard (AES) 256-bit.
	Encryption mode	ECB mode.
Encryptable volume	Volume type	All volume types: open, mainframe, multiplatform.
	Emulation type	All emulation types: OPEN-V, 3390-9, etc.
	Internal/external volumes	Internal volumes only.
	Volume with existing data	Supported. Requires data migration.
Encryption key management	Creation of encryption key	Performed automatically by the storage system.
	Scope of encryption key	Single key per storage system.
	Unit of encryption/decryption	Parity group.
	Backup functionality	Redundant (primary and secondary) backup copies.

Encryption Key Operations

The encryption key on the Universal Storage Platform V/VM storage system is used to encrypt and decrypt data. The key is created automatically when a parity group configured for encryption is formatted. There is one data encryption key per storage system (stored in shared memory), so once the key has been created, that key is used for all encryption operations.

Data-at-Rest Encryption provides redundant backup and restore operations for the encryption key to ensure data availability.

Encryption Key Backup

Data-at-Rest Encryption provides primary and secondary backup of the encryption key:

- Primary backup of the encryption key is executed automatically by the storage system. The primary backup is stored on each EBED in the USP V/VM storage system.
- Secondary backup of the encryption key is performed by the user via Storage Navigator. The secondary backup is required to restore the encryption key if the primary backup is unavailable. Encryption Administrator access to Storage Navigator is required to back up the key.

The encryption key should be backed up immediately after it is created, and regular backups (e.g., once a week) should be scheduled to ensure data availability. For instructions on backing up the key, see Backing Up the Encryption Key.

WARNING:

- If the primary backup becomes unavailable and there is no secondary backup, encrypted data cannot be decrypted.
- The user is responsible for storing the secondary backup securely.

Encryption Key Restore

If the existing encryption key becomes unavailable or can no longer be used (e.g., due to a failure), the key is restored from the primary or secondary backup copy:

- Restoring the encryption key from the primary backup is performed automatically by the storage system.
- Restoring the encryption key from the secondary backup is performed by the user via Storage Navigator. Encryption Administrator access to Storage Navigator is required to restore the key.

For instructions on restoring the key, see Restoring the Encryption Key.

Data Encryption Operations

Data encryption operations include:

- ☐ Data Encryption
- ☐ Data Decryption

Data Encryption

Hitachi Data-at-Rest Encryption provides data encryption at the parity-group level. First, encryption is enabled on a parity group, and then the logical devices (LDEVs) in the parity group are formatted. This encryption formatting operation writes encrypted zero data to the entire area of all drives in the parity group.

Enabling encryption is a **destructive** process. The user is responsible for backing up all data in the parity group before enabling encryption. Encryption must be enabled before (encryption) formatting operations can be performed.

Storage Administrator access to Storage Navigator is required to enable encryption. For instructions on enabling encryption, see Enabling Data Encryption.

Encrypting existing data

Data migration is required to encrypt existing data on the USP V/VM storage system. First, a new parity group is established and encryption is enabled, the encrypted parity group is formatted, and then the existing data is migrated to the new LDEVs in the encrypted parity group. This data migration is performed on a per-LDEV basis.

For information about data migration services, please contact your Hitachi Data Systems account team.

Data Decryption

Data decryption is also performed at the parity-group level. First, encryption is disabled for a parity group, and then the LDEVs in the parity group are formatted. This normal formatting operation writes (unencrypted) zero data to the entire area of all drives in the parity group.

Disabling data encryption is a **destructive** process. The user is responsible for backing up all data in the parity group before disabling encryption. Encryption must be disabled before (normal) formatting operations can be performed.

Storage Administrator access to Storage Navigator is required to disable encryption. For instructions on disabling encryption, see Disabling Data Encryption.

Audit Logging of Encryption Events

The Audit Log feature of the Universal Storage Platform V/VM storage system provides audit logging of key events that take place on the array. Events related to Data-at-Rest Encryption, including data encryption operations and encryption key operations, are recorded in the audit log.

For information about audit logging and audit log events, see the *Storage Navigator User's Guide* and the *Audit Log User and Reference Guide*.

2

Preparing for Data-at-Rest Encryption Operations

This chapter provides information and instructions to prepare for Data-at-Rest Encryption operations:

- ☐ System Requirements
- ☐ Interoperability
- ☐ Configuring Storage Navigator

System Requirements

Item	Requirements
Hitachi Universal Storage Platform V/VM	Microcode 60-04-0*x* and later. Encrypting back-end director(s). Spare data drives behind each encrypting back-end director. ▪ Spare drives for encrypting back-end directors cannot be used as spare drives for standard back-end directors. ▪ Spare drives for normal back-end directors cannot be used as spare drives for encrypting back-end directors.
Hitachi Storage Navigator	Encryption License Key software license. Hitachi Virtual LVI/LUN software. Storage Administrator access to Storage Navigator is required to enable and disable data encryption. Encryption Administrator access to Storage Navigator is required to back up and restore the encryption key.
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. Volumes must be internal. External volumes are not supported.

Interoperability Considerations

Table 2-1 provides interoperability considerations for Data-at-Rest Encryption.

Table 2-1 Interoperability Considerations for Data-at-Rest Encryption

Function	Interoperability Considerations
Copy functions (ShadowImage, TrueCopy, FlashCopy, Compatible XRC, etc.)	When a P-VOL of a copy function is encrypted, the S-VOL should also be encrypted. If not, the copied data on the S-VOL is non-encrypted data. In that case, the security of the data on the S-VOL cannot be guaranteed.
Copy-on-Write Snapshot	When a P-VOL is encrypted, the pool should consist of only encrypted volumes. If the pool contains non-encrypted volumes, the differential data of the P-VOL is stored as non-encrypted data. In that case, the security of the data on the S-VOL cannot be guaranteed. When the encryption status of a P-VOL and the pool are not consistent (e.g., P-VOL is not encrypted and the pool consists of only encrypted volumes), the S-VOL can consist of both encrypted and non-encrypted data. To ensure data security, the P-VOLs and the pool must have the same encryption status.
Universal Replicator	When a P-VOL is encrypted, the S-VOL should also be encrypted. If not, the copied data on the S-VOL is non-encrypted data. In that case, the security of the data on the S-VOL cannot be guaranteed. When a P-VOL is encrypted, use a journal group to which only encrypted volumes are registered as journal volumes. If not, the journal in P-VOL would be stored as non-encrypted data, and so the security of the data cannot be guaranteed. This also applies to S-VOLs.
Migration functions	When a source volume of data migration is encrypted, the target volume should also be encrypted. If not, the migrated data on the target volume is non-encrypted data. In that case, the security of the data on the target volume cannot be guaranteed. When performing encryption data migration for a LUSE volume, migrate all LDEVs that constitute the LUSE volume. If you perform encryption migration for only some LDEVs, the LUSE volume would have both encrypted area and non-encrypted area. In this case, the security of the data cannot be guaranteed.
LUN Expansion (LUSE)	When storing encrypted data in a LUSE volume, use only encrypted LDEVs. If you build a LUSE volume that consists of encrypted LDEVs and non-encrypted LDEVs, the LUSE volume would have both encrypted area and non-encrypted area. In this case, the security of the data cannot be guaranteed.
Dynamic Provisioning	When encrypting data written to the pool via a virtual volume, use a pool that consists of encrypted volumes.
Cross-OS File Exchange	When a source volume of Cross-OS File Exchange is encrypted, the target volume should also be encrypted. If not, the data on the target volume is non-encrypted data. In that case, the security of the data on the target volume cannot be guaranteed.

Configuring Storage Navigator

Once you have verified that the requirements have been met, you are ready to configure Storage Navigator for Data-at-Rest Encryption operations.

To configure Storage Navigator for Data-at-Rest Encryption operations

1. Log on to Storage Navigator with Storage Administrator access, and change to **Modify** mode. For instructions, see the *Storage Navigator User's Guide*.
2. Open the **License Key** window, and enable the Encryption license key. For instructions, see the *Storage Navigator User's Guide*.

   Note: If the Encryption software license expires or is deleted, the encryption key will not be deleted.
3. Open the **Account** window, and assign the **Encryption Administrator Role** to the user who will be responsible for backing up and restoring the encryption key. This role can only be assigned to a user with Storage Administrator access.

Once the Encryption license key has been enabled and the Encryption Administrator role has been assigned, you are ready to start Data-at-Rest Encryption operations.

3

Using the Encryption GUI

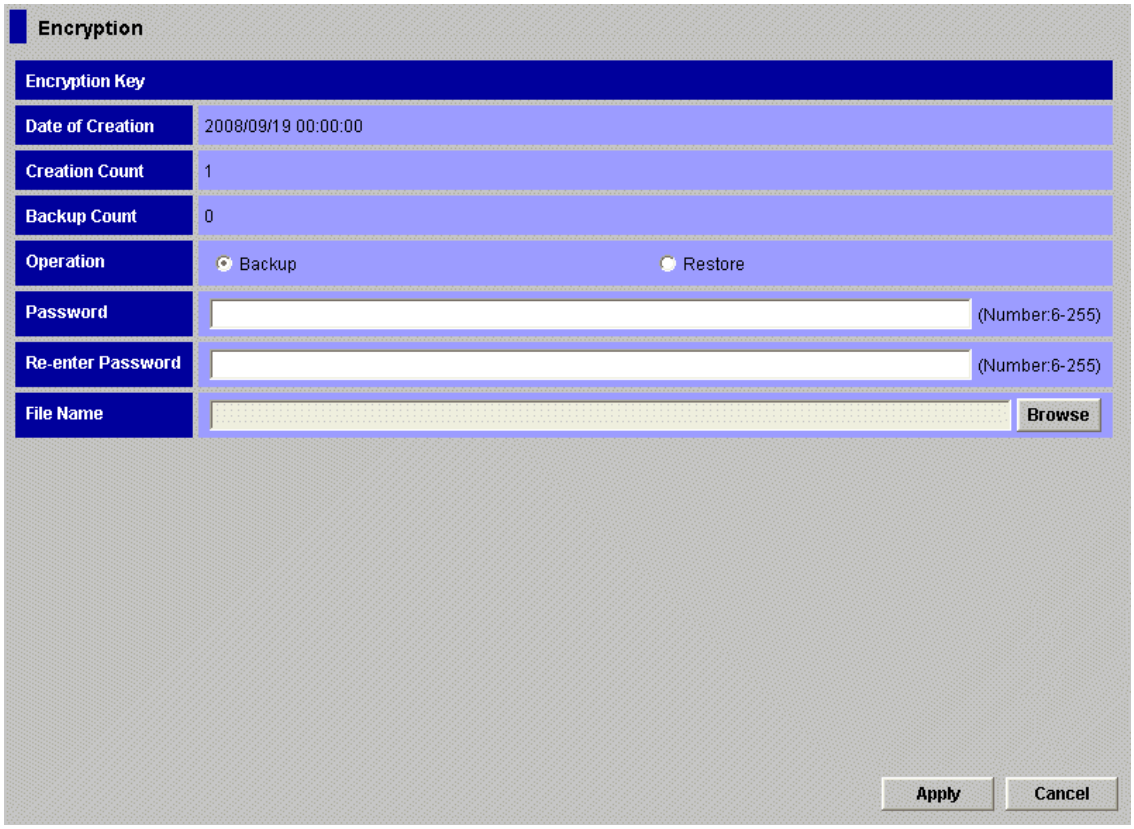
This chapter describes the Storage Navigator windows and dialog boxes for Data-at-Rest Encryption:

- Encryption Window
- Virtual LVI/LUN (VLL) Window
- Encryption Dialog Box

Encryption Window

Use this window to back up and restore the encryption key (see Backing Up the Encryption Key and Restoring the Encryption Key).

To open this window, click **Start** on the Storage Navigator main menu, click **Security**, and then click **Encryption**.

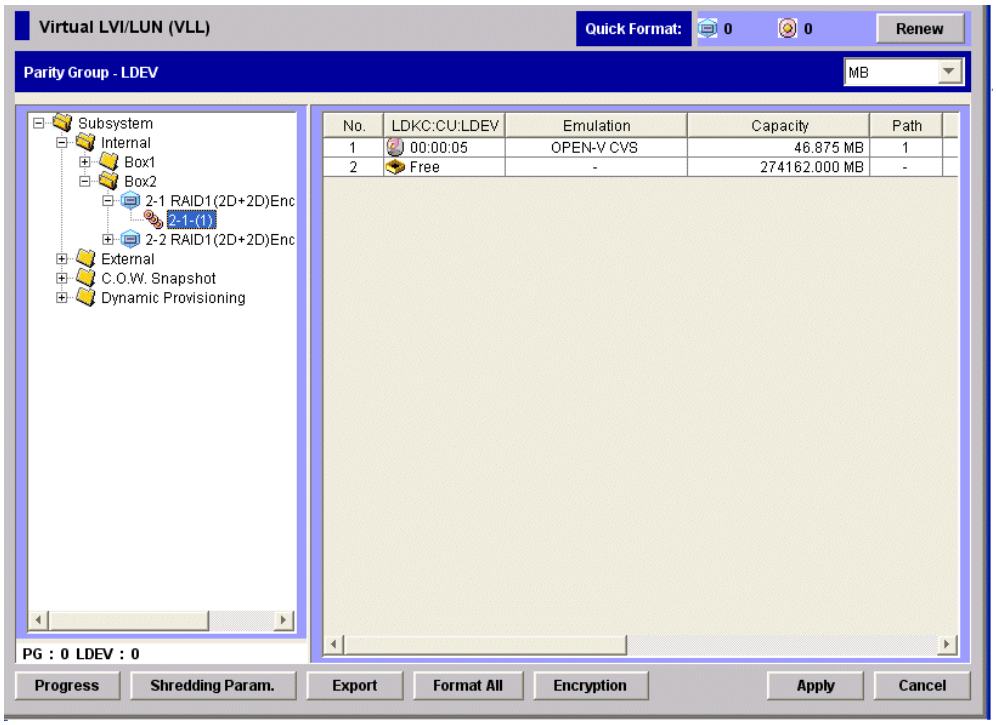


Item	Description
Date of Creation	Time when the encryption key was created. If encrypting back-end directors are not mounted, or if the encryption key has not yet been created, this column shows a hyphen (-).
Creation Count	Number of times that the encryption key has been created. If encrypting back-end directors are not mounted, this column shows a hyphen (-).
Backup Count	Number of times that a backup of the encryption key has been created. If encrypting back-end directors are not mounted, this column shows a hyphen (-).
Operation	Select the encryption key operation to perform: ▪ **Backup:** Selects the encryption key backup operation (default). ▪ **Restore:** Selects the encryption key restore operation. When **Restore** is selected, **Password**, **Re-enter Password**, and **File Name** are cleared.
Password	Type the password for the encryption key. The password must be at least 6 characters and up to 255 characters. The valid characters are: ▪ Numbers (0-9) ▪ Lowercase letters (a-z) ▪ Symbols: ! " # $ % & ' ( ) * + 、 . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
Re-enter Password	Type the password again for confirmation.
File Name	Type the encryption key file name including path (file extension *.ekf*). This field is cleared when **Restore** is selected.
Browse	Select the existing encryption key file (file extension *.ekf*). When an existing key is selected, the file name and path of the selected key appear in **File Name**.
Apply	Applies the settings to the storage system.
Cancel	Cancels the settings and closes the window.

Virtual LVI/LUN (VLL) Window

Use this window to access data encryption operations.

To open the **Virtual LVI/LUN** window, click **Go** on the Storage Navigator main menu, click **LUN Expansion/VLL**, and click **Virtual LVI/LUN (VLL)**.

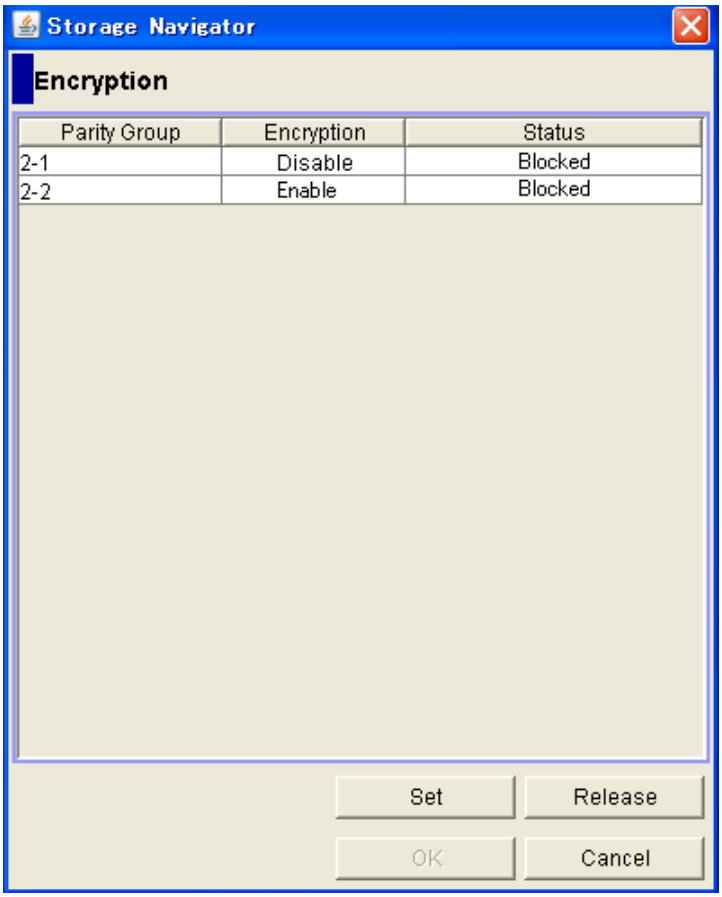


The **Encryption** button opens the Encryption Dialog Box. For more information about the Virtual LVI/LUN window, see the *Virtual LVI/LUN and Volume Shredder User's Guide*.

Encryption Dialog Box

Use this dialog box to perform data encryption operations (see Enabling Data Encryption and Disabling Data Encryption).

To open this dialog box, open the **Virtual LVI/LUN** window (see Virtual LVI/LUN (VLL) Window), and click **Encryption**.



Item	Description
Parity Group	Parity group ID (CU number - parity group number)
Encryption	Encryption setting for the parity group: ▪ **Enable:** encryption is enabled. ▪ **Disable:** encryption is disabled.

Item	Description
Status	Status of the volumes in the parity group: ▪ **Normal:** All volumes in the parity group have normal status. ▪ **Blocked:** One or more volumes in the parity group are blocked. Hosts cannot access blocked volumes. ▪ **Warning:** One or more volumes in the parity group are having a problem. ▪ **Format:** The format operation is in progress for one or more volumes in the parity group. ▪ **Preparing Quick Format:** One or more volumes in the parity group are being prepared for Quick Format. ▪ **Normal (Quick Format):** The Quick Format operation is in progress for one or more volumes in the parity group. ▪ **Correction Access:** The access attribute of one or more volumes is being changed. ▪ **Correction Access with Redundancy:** The access attribute of one or more volumes is being changed. ▪ **Copying:** A copy operation is in progress for one or more volumes in the parity group. ▪ **Read Only:** One or more volumes in the parity group have read-only access. Hosts cannot write data to read-only volumes. ▪ **Shredding:** The shredding operation is in progress for one or more volumes in the parity group. ▪ **Unknown:** The system does not recognize the status of one or more volumes. ▪ **- (hyphen):** There are no volumes in the parity group.
Set	Changes the encryption status of the selected parity group(s) from **Disable** to **Enable**. The change is not applied until you click **OK**.
Release	Changes the encryption status of the selected parity group(s) from **Enable** to **Disable**. The change is not applied until you click **OK**.
OK	Applies the encryption settings to the storage system.
Cancel	Cancels the encryption settings, and closes the dialog box.

4

Performing Data-at-Rest Encryption Operations

This chapter provides instructions for performing Data-at-Rest Encryption operations:

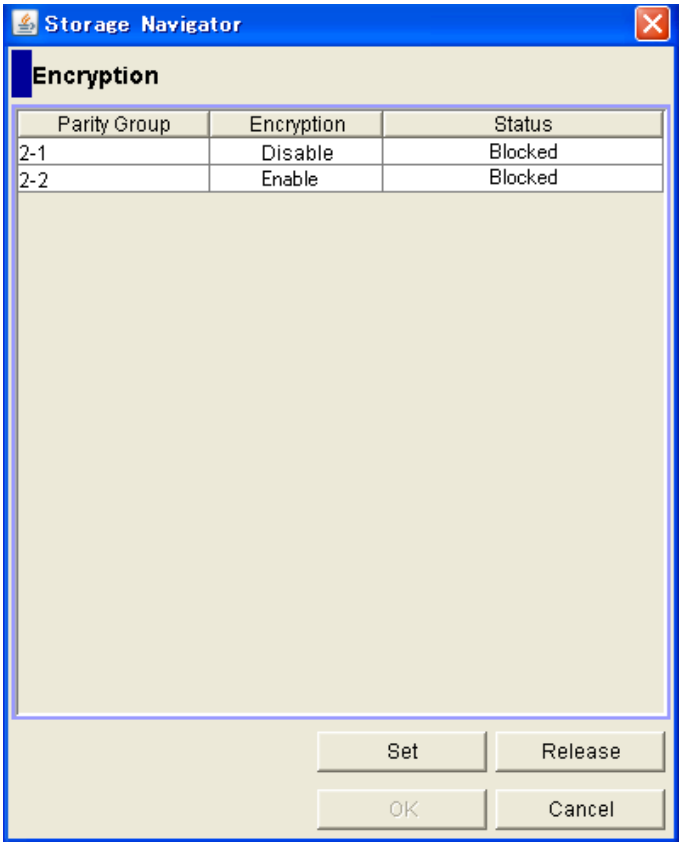
- ☐ Enabling Data Encryption
- ☐ Backing Up the Encryption Key
- ☐ Disabling Data Encryption
- ☐ Restoring the Encryption Key

Enabling Data Encryption

You can enable data encryption on a parity group only when all volumes in the parity group can be formatted (i.e., blocked status). If there are any volumes that cannot be formatted, encryption cannot be enabled.

To enable data encryption

1. Log on to Storage Navigator with Storage Administrator access, and change to **Modify** mode.
2. Open the **Virtual LVI/LUN** window, and click **Encryption** to open the **Encryption** dialog box. The **Encryption** column shows the current encryption status (**Enable** or **Disable**) of each parity group.



3. Select the parity group(s) to encrypt, and click **Set**. The **Encryption** column shows **Enable** next to each parity group to be encrypted.
4. Verify the **Enable**/**Disable** settings, and click **OK** to apply the settings to the storage system.
5. After encryption has been enabled, the next step is to format the LDEVs in the encrypted parity group(s). The encryption key is created when the first encrypted LDEVs are formatted.

   For instructions on formatting the LDEVs in a parity group, see the Virtual *LVI/LUN and Volume Shredder User's Guide*.

Backing Up the Encryption Key

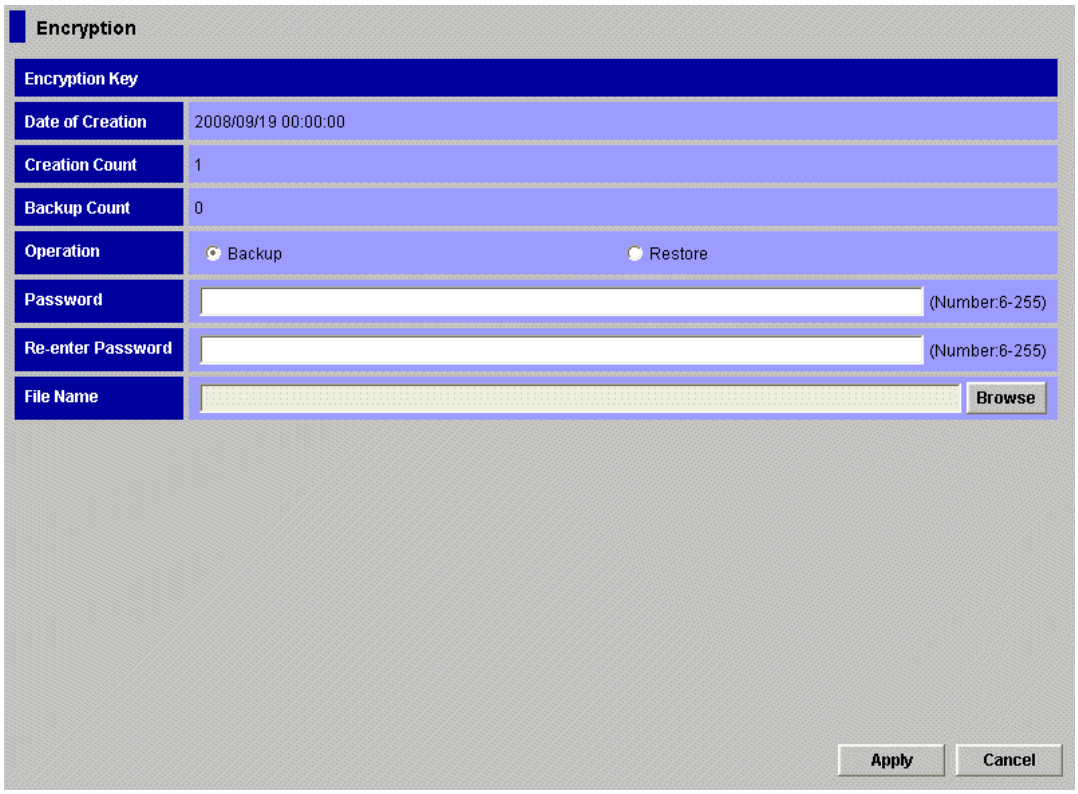
You should back up the encryption key immediately after the first encrypted LDEVs are formatted, and you should schedule regular backups (e.g., once a week) to ensure data availability.

WARNING:

- If the primary backup becomes unavailable and there is no secondary backup, encrypted data cannot be decrypted.
- The user is responsible for storing the secondary backup securely.

To back up the encryption key

1. Log on to Storage Navigator with Encryption Administrator access, and change to **Modify** mode.
2. On the Storage Navigator main menu, click **Start**, click **Security**, and then click **Encryption** to open the **Encryption** window.



3. Select **Backup** in the **Operation** area.
4. Type the desired password in **Password**. This password will be required to restore the encryption key. The requirements for the password are:
   - Length: minimum 6 characters, maximum 255 characters
   - Valid characters: numbers (0-9), lowercase letters (a-z), symbols: ! " # $ % & ' ( ) * + 、 - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

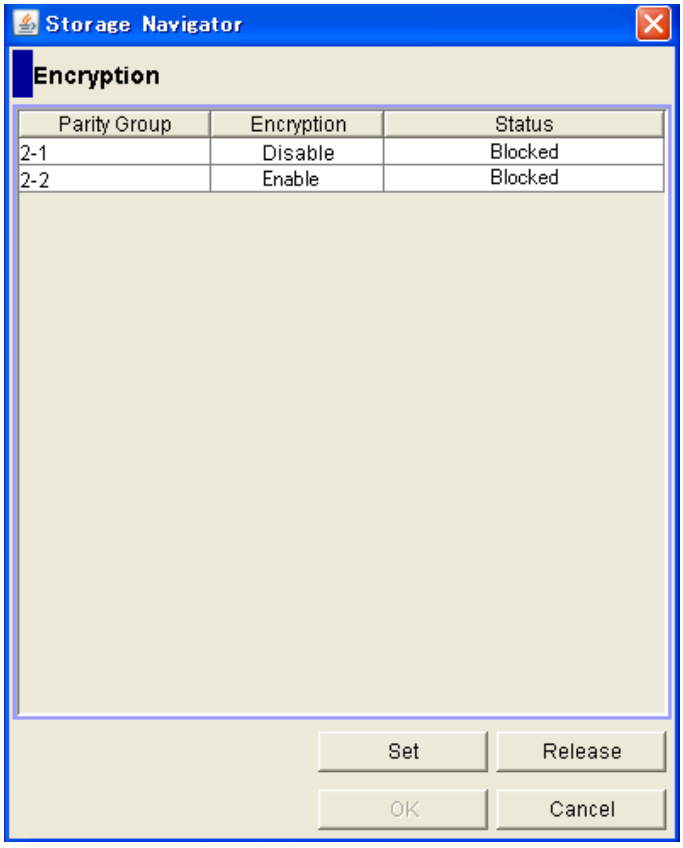
5. Type the password again in **Re-enter Password** for confirmation.
6. Type the desired name for the backup file in **File Name**, or click **Browse** to locate and select an existing backup file. The file name must include the full path, and the file extension must be **.ekf**.
7. Verify the settings on the **Encryption** window, and click **Apply** to apply the settings to the storage system.

Disabling Data Encryption

You can disable data encryption on a parity group only when all volumes in the parity group can be formatted (i.e., blocked status). If there are any volumes that cannot be formatted, encryption cannot be disabled.

To disable data encryption

1. Log on to Storage Navigator with Storage Administrator access, and change to **Modify** mode.
2. Open the **Virtual LVI/LUN** window, and click **Encryption** to open the **Encryption** dialog box. The **Encryption** column shows the current encryption status (**Enable** or **Disable**) of each parity group.



3. Select the parity group(s) to decrypt, and click **Release**. The **Encryption** column shows **Disable** next to each parity group to be decrypted.
4. Verify the **Enable**/**Disable** settings, and click **OK** to apply the settings to the storage system.
5. After encryption has been disabled, the next step is to format the LDEVs in the decrypted parity group(s).

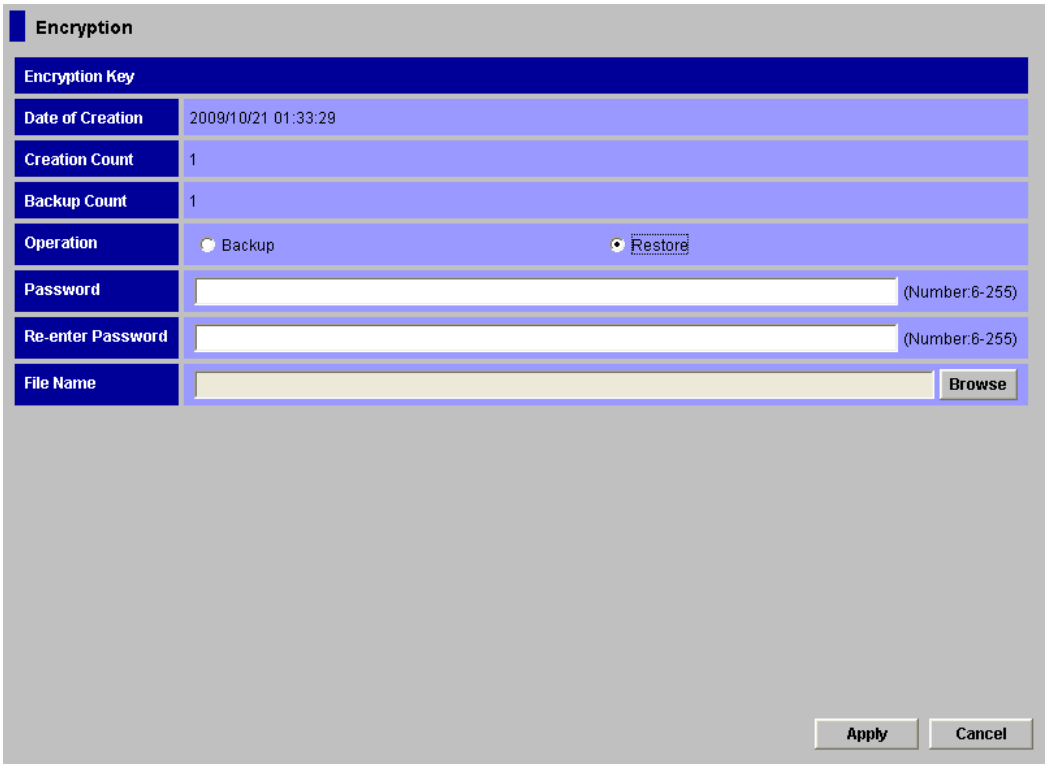
   For instructions on formatting the LDEVs in a parity group, see the Virtual *LVI/LUN and Volume Shredder User's Guide*.

Restoring the Encryption Key

If the encryption key and primary backup copy are not available or cannot be used (e.g., due to failure), encrypted user data becomes unreadable. In this case you must restore the encryption key from the secondary backup copy.

To restore the encryption key

1. Log on to Storage Navigator with Encryption Administrator access, and change to **Modify** mode.
2. On the Storage Navigator main menu, click **Start**, click **Security**, and then click **Encryption** to open the **Encryption** window.
3. Select **Restore** in the **Operation** area.



4. Type the password for the encryption key in **Password**. This is the password that was entered when the key was backed up.
5. Type the password again in **Re-enter Password** for confirmation.
6. Type the name of the existing backup file in **File Name**, or click **Browse** to locate and select the backup file. The file name must include the full path, and the file extension must be **.ekf**.
7. Verify the settings on the **Encryption** window, and click **Apply** to apply the settings to the storage system.

5

Troubleshooting

This chapter provides troubleshooting information for Data-at-Rest Encryption:

- Troubleshooting
- Calling the Hitachi Data Systems Support Center

Troubleshooting

For troubleshooting information about the Universal Storage Platform V/VM storage system, see the *Universal Storage Platform V/VM User and Reference Guide*.

For troubleshooting information about Storage Navigator, see the *Storage Navigator User's Guide* and *Storage Navigator Messages*.

The following table provides general troubleshooting information for Data-at-Rest Encryption operations. If you need technical assistance, see Calling the Hitachi Data Systems Support Center.

Table 5-1 General Troubleshooting

Problem	Recommended Action
Cannot access encryption key operations (backup/restore key).	Verify the following: ▪ The Encryption license key is enabled and not expired. ▪ You are logged in as Encryption Administrator.
Cannot access encryption operations (enable/disable encryption).	Verify the following: ▪ The Encryption license key is enabled and not expired. ▪ You are logged in as Storage Administrator.
Cannot enable encryption for a parity group.	Verify the following: ▪ The parity group is behind an encrypting back-end director. ▪ All volumes in the parity group are in the blocked status.
Cannot disable encryption for a parity group.	Verify that all volumes in the parity group are in the blocked status.
Cannot restore the encryption key.	Verify that the Encryption license key is enabled and not expired. If not, the encryption key cannot be restored.

Calling the Hitachi Data Systems Support Center

If you need to call the Hitachi Data Systems Support Center, please provide as much information about the problem as possible, including:

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

The Hitachi Data Systems customer support staff is available 24 hours/day, seven days a week. If you need technical support, please call:

- United States: (800) 446-0744
- Outside the United States: (858) 547-4526

Acronyms and Abbreviations

AES	Advanced Encryption Standard
EBED	encrypting back-end director
ECB	Electronic Code Book
GB	gigabyte (see Convention for Storage Capacity Values)
KB	kilobyte (see Convention for Storage Capacity Values)
LDEV	logical device
LUN	logical unit number
LUSE	LUN Expansion
LVI	logical volume image
MB	megabyte (see Convention for Storage Capacity Values)
PB	petabyte (see Convention for Storage Capacity Values)
P-VOL	primary volume (of a copy pair)
SIM	service information message
S-VOL	secondary volume (of a copy pair)
TB	terabyte (see Convention for Storage Capacity Values)
USP V/VM	Hitachi Universal Storage Platform V/VM
VLL	Virtual LVI/LUN
XRC	Extended Remote Copy

Index

Hitachi Data Systems

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

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

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

Hitachi Data Systems

MK-98RD6723-02