Hitachi Virtual Storage Platform 5000 Series

Hitachi Virtual Storage Platform E Series

Hitachi Virtual Storage Platform G/F350, G/F370, G/F700, G/F900

SVOS RF 9.6

Encryption License Key User Guide

The Encryption License Key feature provides hardware-based Advanced Encryption Standard (AES) encryption, enabling you to implement and manage data-at-rest encryption for sensitive data on your storage system.

MK-98RD9017-08
February 2021

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 Vantara LLC at https://support.hitachivantara.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 Vantara LLC.

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; and
2. Verifying that your 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.

Contents

Preface

The Encryption License Key feature provides hardware-based Advanced Encryption Standard (AES) encryption, enabling you to implement and manage data-at-rest encryption for sensitive data on the storage system. This document describes and provides instructions for performing Encryption License Key operations on your storage system.

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

Intended audience

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

Readers of this document should be familiar with the following:

- Data processing and RAID storage systems and their basic functions.
- The *Hardware Guide* for your storage system model.
- The Hitachi Device Manager - Storage Navigator software.
- The concepts and functionality of data-at-rest encryption operations, including managing encryption keys on a key management server (KMS), if applicable.

Product version

This document revision applies to the following product versions:

- VSP 5000 series: 90-06-01 or later
- VSP E series: 93-04-01 or later
- VSP G/F350, G/F370, G/F700, G/F900: 88-07-01 or later
- SVOS RF 9.6 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 Vantara Support Connect: https://knowledge.hitachivantara.com/Documents.

Changes in this revision

- Updated the troubleshooting information for when the operations for encryption keys cannot be performed (Troubleshooting Encryption License Key operations (on page 71)).

Document conventions

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.

Convention	Description
	{ 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.
⚠	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, cache memory 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 the Hitachi Vantara Support Website: https://knowledge.hitachivantara.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

The Hitachi Vantara Support Website is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to the Hitachi Vantara Support Website for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

Hitachi Vantara Community is a global online community for Hitachi Vantara 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.hitachivantara.com, register, and complete your profile.

Comments

Please send us your comments on this document to doc.comments@hitachivantara.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 Vantara LLC.

Thank you!

Chapter 1: Overview of the encryption feature

The Encryption License Key feature provides hardware-based data-at-rest encryption for your sensitive data.

Encryption License Key benefits

The data-at-rest encryption feature, called Encryption License Key, protects your sensitive data against breaches associated with storage media (for example, loss or theft). Encryption License Key includes a controller-based encryption implementation as well as integrated key management functionality that can leverage third-party key management solutions via the OASIS Key Management Interoperability Protocol (KMIP).

The Encryption License Key feature provides the following benefits:

- Hardware-based Advanced Encryption Standard (AES) encryption, using 256-bit keys in the XTS mode of operation, is provided for open and mainframe systems.
- Encryption can be applied to some or all supported internal drives (HDD, SSD, FMD).
- Each encrypted internal drive is protected with a unique data encryption key.
- Encryption has negligible effects on I/O throughput and latency.
- Encryption requires little to no disruption of existing applications and infrastructure.
- Cryptographic erasure (media sanitization) of data is performed when an internal encrypted drive is removed from the storage system.

Encryption component description

Encryption License Key consists of three major components:

- Software license for Encryption License Key
- Encryption hardware
- Key management

Software license

The Encryption License Key software license must be installed on the storage system and valid (not expired). Note that an expired license can limit the operations that can be performed on an already configured storage system.

Encryption hardware

The data at-rest encryption (DARE) functionality is implemented using cryptographic chips included as part of the encryption hardware. The encryption hardware encrypt and decrypt data as it is being written to and read from the physical drives. These hardware components must be installed and configured before DARE can be used.

The encryption hardware depends on the storage system model:

- For VSP 5000 series, VSP E990, VSP G/F700, and VSP G/F900, encrypting back-end modules (EBEMs) perform the encryption.
- For VSP E590, VSP E790, VSP G/F350, and VSP G/F370, encrypting controllers (ECTLs) perform the encryption.

Enabling and disabling DARE is controlled at the parity group level (that is, all drives in a parity group are either encrypting or non-encrypting). While it is possible to have both encrypting and non-encrypting parity groups configured on an EBEM, it is recommended to encrypt all parity groups on an EBEM. It is also important to note that different spare drives are used for encrypting and non-encrypting parity groups.

Key management

Data security provided by encryption is only as good as the generation, protection, and management of the keys used in the encryption process. Further, encryption keys must be available when they are needed while being protected from possible compromise (for example, unauthorized access or destruction). To address these issues and meet a wide range of requirements associated with key management, the Encryption feature includes multiple options associated with key management.

It is important to understand the keys used by the storage system and the roles these keys play in the DARE solution. There is a hierarchy of keys that includes the following key types:

- Data encryption keys (DEKs): Each encrypted internal drive is protected with a unique DEK that is used with the AES-based encryption. AES-XTS uses a pair of keys, so each key used as a DEK is actually a pair of 256-bit keys.
- Certificate encryption keys (CEKs): Each encrypting back-end module or encrypting controller requires a key for the encryption of the certificate (registration of the EBEM/ECTL) and a key to encrypt the DEKs stored on the EBEM/ECTL.
- Key encryption keys (KEKs): A single key, the KEK, is used to encrypt the CEKs that are stored in the system.

Managing these keys in a secure manner is a critical aspect of the Encryption License Key feature. This key management functionality controls the full key life cycle, including the generation, distribution, storage, backup/recovery, rekeying, and destruction of keys. In addition, the design of this key management functionality includes protections against key corruption (for example, integrity checks on keys) as well as key backups (both primary and secondary).

After the key generation source (storage system or key management server) has been established in the initial encryption setup, the initial set of keys is generated. The number of generated keys depends on the storage system model and configuration. Any keys that are not assigned will be designated as free keys and will be available for use.

When encryption is enabled for a parity group, DEKs are automatically assigned to the drives in the parity group. Similarly, when encryption is disabled, DEKs are automatically replaced (old DEKs are destroyed, and keys from the free keys are assigned as new DEKs). You can combine this functionality with migrating data between parity groups to accomplish rekeying of the DEKs.

The key management can be configured in a stand-alone mode (integrated key management), or key management can be configured to use third-party key management (external key management). When external key management is leveraged, some or all the following functionality can be used:

- Initial and/or subsequent generation of keys used as CEKs and DEKs
- Generation and protection of KEKs
- Manual and automated backup of keys to a key management server (KMS)
- Restoration of keys from a key backup on a KMS

All communications with a KMS are performed using the OASIS Key Management Interoperability Protocol (KMIP) version 1.0 over a mutually authenticated Transport Layer Security (TLS) version 1.2 connection. The TLS authentication is performed using X.509 digital certificates for both the storage system and two cluster members of the KMS.

In addition to using the KMS for certain transactions (for example, generation of keys, key backups, and key recoveries), the storage systems can be configured to be dependent on the availability of the KMS. This dependency is achieved by protecting the KEK on the KMS, which means that the storage system must retrieve the KEK from the KMS as part of its boot-up sequence. If the KEK cannot be retrieved from the KMS, the storage system will not fully boot. This configuration is reversible (that is, you can change back to integrated key management) unless you configure the storage system in a special mode called KMIP-lock mode. When you configure the storage system in KMIP-lock mode, local key generation is prevented and the configuration cannot be changed back to allow local key generation.

Under a typical configuration, the storage systems store an encrypted copy of the CEKs and DEKs in shared memory. A primary backup (encrypted) of these keys is also made on the flash memory of the encryption hardware installed in the storage system. When the storage system boots, the keys in shared memory are used. If the keys in shared memory are missing or corrupted, one of the primary backups is used. This is the default behavior even when a KMS is used to protect the KEK.

It is also possible to generate secondary backups of the keys either to a key file or on a KMS. Generating secondary backups of the keys on a KMS is the only way to ensure that CEKs and DEKs are stored on a KMS. These secondary key backups can be used to recover keys when the keys are not available in the storage system (for example, when the storage system has been configured to purge all CEKs and DEKs at shutdown). If secondary key backups will be used, it is important that they contain the current CEKs and DEKS, and this is simplified with a KMS because secondary key backups are performed automatically after certain key operations (for example, generating keys) and by regular (automated) key backups. Note that automatic key backups have been optimized so they are performed only when the CEKs and DEKs have changed.

Support specifications for Encryption License Key

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 5000 series: Compliant to FIPS 140-2 Level 2 ▪ VSP E990: Compliant to FIPS 140-2 Level 2 ▪ VSP E590, VSP E790: Compliant to FIPS 140-2 Level 1 ▪ VSP G/F700, VSP G/F900: Compliant to FIPS 140-2 Level 2 ▪ VSP G/F350, VSP G/F370: Compliant to FIPS 140-2 Level 1
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	Requires data migration
Managing encryption keys	Creating and deleting encryption keys	You can use Device Manager - Storage Navigator (HDvM - SN) to create and delete encryption keys. If your storage system does not have an SVP, you can use the REST API (see Using the REST API to perform encryption operations (on page 17)). **Note:** Encryption keys that are allocated to implemented drives cannot be deleted. If you want to delete the encryption key allocated to an implemented drive and allocate a new encryption key, you must first disable encryption for the parity group to which the drive belongs.
	Unit of encryption/decryption	Encryption is applied to the parity group. Data encryption keys (DEKs) are used per drive.

Item		Specification
	Number of encryption keys	▪ VSP 5000 series: Up to 4,096 encryption keys can be created per storage system, including 2,304 DEKs, 48 certificate encryption keys (CEKs), and 1 key encryption key (KEK). ▪ VSP E990: Up to 4,096 encryption keys can be created per storage system, including 1,440 DEKs, 16 CEKs, and 1 KEK. ▪ VSP E590, VSP E790: Up to 4,096 encryption keys can be created per storage system, including 24 DEKs, 8 CEKs, and 1 KEK. ▪ VSP G/F900: Up to 4,096 encryption keys can be created per storage system, including 1,440 DEKs, 16 CEKs, and 1 KEK. ▪ VSP G/F700: Up to 4,096 encryption keys can be created per storage system, including 1,200 DEKs, 8 CEKs, and 1 KEK. ▪ VSP G/F350, VSP G/F370: Up to 1,024 encryption keys can be created per storage system, including 372 DEKs, 4 CEKs, and 1 KEK. The encryption keys are set in the following units: ▪ DEK: 1 key for each drive ▪ CEK: 2 keys for each EBEM, 2 keys for each ECTL (VSP G/F350, VSP G/F370), 4 keys for each ECTL (VSP E590, VSP E790) When the encryption environmental settings are initialized, the encryption keys are created. The number of encryption keys that are created depends on the hardware configuration. When the maximum number of EBEMs or ECTLs is installed, the following numbers of encryption keys are created: ▪ VSP 5000 series: 4,072 ▪ VSP E series: 4,088 ▪ VSP G/F900: 4,088 ▪ VSP G/F700: 4,092 ▪ VSP G/F350, VSP G/F370: 1,022

Item		Specification
	Attribute of encryption keys	Keys used for Encryption License Key are created with the Free attribute, and then another attribute is assigned according to the usage. The attributes for the encryption keys are: ▪ **Free:** Unused data encryption key that has not yet been allocated. ▪ **DEK:** Data encryption key. The key for the encryption of the stored data. ▪ **CEK:** Certificate encryption key. The key for the encryption of the certificate and the key for the encryption of DEK per drive to register DEK on EBEM or ECTL. ▪ **KEK:** Key encryption key. The key for encrypting a key in a storage system with an attribute other than KEK. All keys except the KEK are referred to as encryption keys. If you reconfigure the encryption environmental settings, encryption keys and CEKs are not updated, and unused keys are not created. The encryption keys created when the encryption environmental settings were configured for the first time are used.
	Backup/restore functionality	Redundant (primary and secondary) backup/ restore copies

Using the REST API to perform encryption operations

For the VSP E series and VSP G/F350, G/F370, G/F700, G/F900 storage systems, Encryption License Key operations can be performed by using Device Manager - Storage Navigator or the REST API.

If your storage system is configured with an SVP, you can use the Device Manager - Storage Navigator (HDvM - SN) software to perform Encryption License Key operations. If your storage system does not have an SVP, you can use the REST API and embedded Command Control Interface (CCI). You must have Security Administrator (View & Modify) access privileges to perform Encryption License Key operations.

The following table lists the Encryption License Key operations and indicates the user interface support for each operation. For details about using the REST API, see the *REST API Reference Guide*. For details about using CCI, see the *Command Control Interface Command Reference*.

Operations	HDvM - SN	REST API
Viewing and editing the encryption environmental settings	Supported	Supported*
Viewing and acquiring encryption keys	Supported	Supported
Viewing and acquiring the number of encryption keys	Supported	Supported
Editing the password policy	Supported	Not supported
Generating encryption keys	Supported	Supported*
Backing up encryption keys to a file on the Device Manager - Storage Navigator computer	Supported	Supported*
Backing up encryption keys to a key management server	Supported	Not supported
Restoring encryption keys from a file on the Device Manager - Storage Navigator computer	Supported	Supported*
Restoring encryption keys from the key management server	Supported	Not supported
Forcibly restoring encryption keys from a file on the Device Manager - Storage Navigator computer	Supported	Supported*
Forcibly restoring encryption keys from the key management server	Supported	Not supported
Backing up encryption keys regularly	Supported	Not supported
Deleting and generating unused encryption keys	Supported	Supported*
Listing data backed up in a key management server	Supported	Not supported
Deleting backed up data in the key management server	Supported	Not supported
Updating certificate encryption keys	Supported	Not supported
Updating key encryption keys	Supported	Not supported
Rekeying key encryption keys	Supported	Not supported
Enabling and disabling encryption on specific parity groups	Supported	Not supported
Enabling encryption when creating parity groups	Supported	Supported
* When the encryption environment for the storage system is configured to be linked with a key management server, these operations cannot be performed by using the REST API.		

When Free keys are used

After the encryption environment is set up, Free keys are used when the following operations are performed. If a problem occurs during one of these operations, additional Free keys might be required to recover from the problem.

- Maintenance operations for drives
- Maintenance operations for encrypting back-end modules (EBEMs)
- Maintenance operations for encrypting controllers (ECTLs)
- Updating certificate encryption keys (CEKs)

Free keys used for maintenance operations for drives

Adding drives: 1 for each drive being added

Replacing drives: 1 for each drive being replaced

Decrypting a parity group: 1 for each drive in the parity group being decrypted

Free keys used for maintenance operations for EBEMs

Adding SAS EBEMs: 3 for each SAS EBEM being added

Replacing SAS EBEMs: 3 for each SAS EBEM being added

Adding NVMe EBEMs: 2 for each NVMe EBEM being replaced

Replacing NVMe EBEMs: 2 for each NVMe EBEM being replaced

Free keys used for maintenance operations for ECTLs

Replacing ECTLs: 3 for each ECTL being replaced

Free keys used for updating CEKs

Updating CEKs for EBEMs: 2 for each EBEM being updated

Updating CEKs for ECTLs: 2 for each ECTL being updated

Primary and secondary backups of encryption keys

The storage system automatically creates and stores a primary backup of each encryption key. In addition, you can create secondary backups of the encryption keys. If a primary backup key is unavailable, the secondary backup is required to restore the key.

> **Important:** The creation and secure storage of backup keys must be included as part of your corporate security policy. It is strongly recommended that you back up each encryption key or group of keys immediately after you create them and that you schedule regular backups of all encryption keys to ensure data availability. You are responsible for storing the secondary backup keys securely.

> **Caution:** If a primary backup key becomes unavailable and no secondary backup key exists, the system cannot decrypt the encrypted data.

Automatic encryption key backup (key management server only)

When a key management server is used, encryption keys are automatically backed up after they are created. This operation is called an automatic backup.

When a key management server is not used, an automatic backup is not performed, and you must manually back up the encryption keys.

Regular encryption key backups

The Encryption License Key feature supports periodic encryption key backup operations to the key management server. These operations are called regular backup operations. To use this function, you must designate a specific user as the regular backup user and then enable the Encryption Key Regular Backup option on the Edit Encryption Environmental Settings window. Regular backup operations are performed automatically even when the designated regular backup user is not logged in.

Important: Performing regular backups is a supplemental function available only when the key management server is used and the Encryption Key Regular Backup option is enabled.

- If the key management server is used but you do not enable the regular backup option, the encryption keys are backed up automatically after they are created.
- If the key management server is not used, you must perform manual backups, especially immediately after you create encryption keys.

How regular backups are queued and performed

At the specified time for a regular backup, the regular backup operation is queued as a task. You can verify queued tasks in the **Tasks** window. If other tasks are already in the queue, the regular backup will not start until after the other tasks already in the queue are complete. Because of this, the time that the regular backup begins might be different from the time you specified. In addition, if the key management server has the latest backup, the regular backup task is skipped because it is not necessary to back up the same encryption keys again.

At the specified time for a regular backup, if the previous regular backup has not yet been performed because another queued task is still in progress, a second regular backup task is not added to the task queue, and only the first regular backup is performed. For example, if you specify 00:00 and 02:00 for regular backups, and a task started before 00:00 completes at 03:00, the 02:00 regular backup is not queued, and only the regular backup for 00:00 is performed at 03:00.

Note:

- When the SVP stops, regular backup operations are not performed. After the SVP is restarted, regular backups will resume queueing as a task.
- During a regular backup, your service representative cannot perform SVP operations or maintenance of the storage system. If a regular backup will occur during planned maintenance, you can revise the regular backup schedule or cancel the regular backup task temporarily.

Verifying regular backups

You should verify, on a regular basis, that regular backups are being performed successfully. You can verify the regular backup task results in the **Tasks** window. To view details about a regular backup task, you must have the System Administrator (System Resource Management) role, or you must be logged in as the designated regular backup user. You can also verify the regular backup task results in the audit log. The audit log records the regular backup user name for the regular backup tasks.

If a regular backup task is skipped (for example, because the key management server already has the latest backup), the skipped task is not output to the Tasks window or to the audit log. If a necessary regular backup task is not performed, the task is regarded as failed. You can check the details of the failed task in the audit log.

Discontinuing regular backups

If you want to discontinue regular backups, you can disable the Enable Encryption Key Regular Backup to Key Management Server option in the **Edit Encryption Environmental Settings** window.

Managing the number of backed up encryption keys

A regular backup deletes the old encryption key. Because of this, the number of encryption keys to be backed up regularly is always one. In the same way as manually backed up keys, the status of a regular backup encryption key can be viewed, and the key itself can be restored or deleted.

When you manually back up encryption keys, the old keys are not deleted. The number of keys that can be backed up on a key management server is limited. Make sure to delete unnecessary keys from the key management server whenever possible.

Audit logging of encryption events

The Audit Log feature provides logging of events that occur in the storage system, including events related to encryption and data encryption keys. When the KMIP key manager is configured, the interactions between the storage system and the KMIP key manager are also recorded in the audit log. You can use the audit log to check and troubleshoot key generation and backup.

If you enable and schedule regular encryption key backups, the regular backup tasks are recorded in the audit log with the regular backup user name, even if the regular backup user was not logged in when the backup was performed.

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

Workflow for implementing data encryption

Use the following workflow to implement data encryption on your storage system:

1. If you plan to use a key management server, configure the key management server first.

   For details, see Key management server connections (on page 23).

2. On the storage system, install the license key for the Encryption License Key software.

   For instructions, see Installing the license key for the Encryption License Key software (on page 33).

3. If you plan to enable regular backups on the key management server, designate the regular backup user.

   For instructions, see Designating the regular backup user (on page 35).

4. Configure the encryption environmental settings on the storage system.

   For instructions, see Performing the initial configuration of the encryption environmental settings (on page 36).

5. Create and back up the encryption keys.

   For details, see Creating and backing up encryption keys (on page 45).

6. Enable encryption on the desired parity groups.

   For instructions, see Enabling encryption (on page 51).

Chapter 2: Key management server connections

The Encryption License Key feature supports an optional connection to an external key management server. For the latest information about supported key management servers, see the Encryption Key Management Server Support Matrix on the interoperability site: https://support.hitachivantara.com/en_us/interoperability.html

Configuring the key management server

If you are planning to use a key management server, the following configuration tasks must be performed on the key management server before you perform the initial configuration of the encryption environmental settings:

- The key management server must be configured to allow the storage system's KMIP client to authenticate, store, fetch, and generate keys on the key management server.
- The storage system negotiates a secure TLS 1.2 channel to the key management server using the exchange of mutually authenticated certificates. The storage system requires that a certificate be generated for this purpose; a self-signed certificate cannot be used. The key management server KMIP TLS service must trust the certificate authority that signs the certificate generated for the storage system. A copy of the root certificate from the signing certificate authority is also required. For assistance in obtaining the unique certificates and proper connection parameters required for this operation, contact your Key Management Server administrator.

  If your key management server is Safenet KeySecure k460 or Enterprise Secure Key Manager, you can create or obtain the root certificate of the key management server on the key management server. For details, see the documentation for Safenet KeySecure k460 or Enterprise Secure Key Manager.
- If you want to connect to the key management server using the host name instead of the IP address, the IP address of the DNS server must be configured on the SVP of the storage system.
- If you plan to protect the key encryption key at the key management server, the key management server must be configured using two clustered servers, and you must enable the secondary key management server when you configure the encryption environmental settings.
- You must establish and verify the network connections from the storage system to each key management server.
- If you plan to enable regular encryption key backups on the key management server, you must designate a user for the regular backups (called the regular backup user) and assign the Security Administrator (View & Modify) role to this user.

Depending on the type of key management server (vendor, software version), you might need to perform additional configuration tasks. For further information about preparing the necessary services to accept connections from the storage system, refer to the documentation for your key management server.

Setting up the client certificate

Use the following procedure to prepare the client certificate. Encryption keys backed up on the key management server (KMS) are managed with the client certificate. The client certificate on the KMS must remain current and not expired. If the client certificate expires or is not current, the storage system will not be able to access the KMS.

⚠ **Caution:**

- If the client certificate is lost and the SVP is replaced due to a failure, the encryption keys that were backed up before the SVP replacement cannot be restored.
- When the connection settings are backed up to the KMS, the storage system does not back up the client certificate. Make sure that you back up a copy of the connection settings to the KMS and save a copy of the client certificate separately. Refer to your corporate security policy for procedures related to backups.
- The encryption keys backed up on the KMS are managed with the client certificate. If the client certificate is changed, the encryption keys that were backed up before the change cannot be restored. Make sure to back up the encryption keys immediately after changing the client certificate.

Procedure

1. VSP 5000 series: Download and install `openssl.exe` from http://www.openssl.org/ to the `C:\openssl` folder.

   For VSP E990, VSP G/F350, G/F370, G/F700, G/F900, perform either of the following:

   - Download and install `openssl.exe` from http://www.openssl.org/ to the `C:\openssl` folder.
   - Use OpenSSL on the SVP stored in `C:\Mapp\OSS\apache\bin\openssl`.

2. Create the key file. You can create the following types of key files:

   - Private key (.key) file
   - Public key (.csr) file

   For details about creating a Private or Public key, see the *System Administrator Guide*.

3. If you created a Public key (.csr) file, submit the Public key file to an appropriate trusted internal or third party Certificate Authority for signing. For details, see the documentation for Safenet KeySecure k460 or Enterprise Secure Key Manager.
4. Convert the client certificate to PKCS#12 format.

   a. 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.

b. Move the private SSL key file (.key) and the client certificate to the folder in the current directory, and run the command.

   Example of an output folder of `c:\key`, private key file (`client.key`), and a client certificate file (`client.crt:`):

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

   (VSP E990, VSP G/F350, G/F370, G/F700, G/F900) When using OpenSSL on the SVP: `C:\key>c:\Mapp\OSS\apache\bin\openssl pkcs12 -export -in client.crt -inkey client.key -out client.p12`

   > **Tip:** C:\Mapp indicates the installation directory for the storage management software and SVP software. If another directory is specified for the installation directory, change the installation directory.

c. Type the 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: ! # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

5. Upload the root and client certificates to the SVP.

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

b. In the **Encryption Keys** window, click **Edit Encryption Environmental Settings**.

c. Upload the certificates.

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 Determining the encryption environmental settings for your system (on page 34), 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 Determining the encryption environmental settings for your system (on page 34) 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. In this case, the deletion of the key encryption key fails because the key encryption key cannot be deleted from the key management server before the update. However, the key encryption key update is complete.

Chapter 3: Installation of Encryption License Key

Installation of Encryption License Key includes installing the software license for Encryption License Key on the storage system and performing the initial configuration of the encryption environmental settings using Device Manager - Storage Navigator. If you plan to use a key management server, the key management server must be configured for operation with the storage system before you perform the initial configuration of the encryption environmental settings.

Storage system requirements

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

Item	Requirements
Encryption hardware	VSP 5000 series: Encrypting back-end modules (EBEMs) VSP E990: Encrypting back-end modules VSP E590, VSP E790: Encrypting controllers (ECTLs) VSP G/F700, VSP G/F900: Encrypting back-end modules VSP G/F350, VSP G/F370: Encrypting controllers
Firmware	VSP 5000 series: To encrypt data stored on NVMe drives, firmware 90-03-02 or later is required. VSP E590, VSP E790: Firmware 93-03-2*x* or later is required. VSP G/F350, G/F370, G/F700, G/F900: To encrypt data on a storage system without an SVP, firmware 88-03-2*x* or later is required.
Software license	Encryption License Key software license If the license for Encryption License Key is deleted or expires, encryption keys cannot be created.

Item	Requirements
Hitachi Device Manager - Storage Navigator (HDvM - SN)	The Security Administrator (View & Modify) role is required to perform encryption operations (for example, enabling and disabling encryption on parity groups, backing up and restoring keys). If you need to restore an encryption key that is not the latest key from a secondary backup copy, you must have the Security Administrator (View & Modify) and Support Personnel (View & Modify) roles. If you plan to enable regular encryption key backups on the key management server (KMS), you must designate a specific HDvM - SN user as the regular backup user. The regular backup user must have the Security Administrator (View & Modify) role. If you are not logged in as the designated regular backup user, the System Administrator (System Resource Management) role is required to view details about a regular backup task.
Data volumes	Emulation type: All volume emulation types (open-systems, mainframe, and multiplatform) are supported. Volume type: Internal. External volumes are not supported.
SVP (Web server)	If you want to protect the key encryption keys (KEKs) on the KMS, the SVP must always be up and running. If you want to connect to the KMS by specifying a host name instead of an IP address, you must set up a DNS server on the KMS, and the IP address of the DNS server must be configured on the SVP of the storage system. The SVP is required for VSP G/F350, G/F370, G/F700, G/F900 models with firmware 88-03-1*x* and earlier. For firmware 88-03-2*x* and later, the SVP is not required.

Key management server requirements

The following table lists the key management server (KMS) support specifications and requirements for the Encryption License Key feature.

Item	Requirements
Key Management Interoperability Protocol (KMIP)	VSP 5000 series: KMIP versions 1.0, 1.1, 1.2, 1.3, 1.4 VSP E990: KMIP version 1.0 VSP G/F350, G/F370, G/F700, G/F900: KMIP version 1.0

Item	Requirements
Software	Encryption License Key supports several key management servers (for example, SafeNet KeySecure, Enterprise Secure Key Manager). For the latest information about KMS software support, see the Encryption Key Management Server Support Matrix: https://support.hitachivantara.com/en_us/interoperability.html
TLS security settings	For VSP 5000 series, the TLS security settings for Device Manager - Storage Navigator (displayed and set on the **TLS Security Settings** window of the **Tool Panel**) must be enabled. For details, see the *System Administrator Guide*.
Certificates	**Caution about certificate expiration:** The certificates have expiration dates. If a certificate expires, you will not be able to connect to the KMS. Make sure to update the certificate before the expiration date. **(VSP 5000 series) Caution about revocation verification:** ▪ When performing revocation verification by using CRL, set the CRL repository URI for the cRLDistributionPoint (CRL distribution point) of the certificate. For VSP 5000 series, set the CRL repository URI for the CRL distribution point of the intermediate certificate and of the server certificate set on the connected server. The CRL repository must exist on a network that can be accessed from the SVP to communicate with the SVP. If the SVP and CRL repository cannot communicate, the communications with the KMS will fail. ▪ When performing revocation verification by using OCSP, set correctly the OCSP responder URI for the authorityInfoAccess (agency access information) of the certificate. For VSP 5000 series, set correctly the OCSP responder URI for the authorityInfoAccess (agency access information) of the intermediate certificate and of the server certificate set on the connected server. The OCSP responder must exist on a network that can be accessed from the SVP to communicate with the SVP. If the SVP and OCSP responder cannot communicate, the communications with the KMS will fail.

Item	Requirements
Certificate requirements for VSP 5000 series	**Requirements for the server certificate for the KMIP server:** ▪ If the public key of the server certificate is RSA, the key length must be 2,048 bits or more. ▪ If the public key of the certificate is ECDSA, the key length parameter must be one of the following: ECDSA_P256 (secp256r1), ECDSA_P384 (secp384r1), or ECDSA_P521 (secp521r1). ▪ The signature hash algorithm of the server certificate must be SHA-256, SHA-384, or SHA-512. ▪ When setting a host name to connect to the KMS, enter the host name of the server in `subjectAltName` or `CommonName` of the server certificate. ▪ When setting an IP address to connect to the KMS, enter the IP address of the server in `subjectAltName` or `CommonName` of the server certificate. **Requirements for the root certificate for the KMS:** ▪ Format: X.509 DER, or X.509 PEM ▪ The extended profile fields in the X.509 certificate must support the following items as specified in RFC5280: • subjectAltName • CRLDistributionPoint • AuthorityInfoAccess • BasicConstraints • KeyUsage • SubjectKeyIdentifier ▪ If the public key of the root certificate to be uploaded is RSA, the key length must not be less than the Minimum Key Length (Key Exchange) setting displayed on the **TLS Security Settings** window of the **Tool Panel**. ▪ If the public key of the certificate is ECDSA, the key length parameter must be one of the following: ECDSA_P256 (secp256r1), ECDSA_P384 (secp384r1), or ECDSA_P521 (secp521r1). ▪ The signature hash algorithm of the root certificate must be SHA-256, SHA-384, or SHA-512.

Item	Requirements
	Requirements for the client certificate: ▪ Format: PKCS#12 If you do not know the password of the client certificate in the PKCS#12 format, contact the KMS administrator. ▪ The client certificate must be signed by the CA (Certificate Authority) for the KMS. ▪ If the public key of the client certificate to be uploaded is RSA, the key length must not be less than the Minimum Key Length (Key Exchange) setting displayed on the **TLS Security Settings** window of the **Tool Panel**. ▪ If the public key of the certificate is ECDSA, the key length parameter must be one of the following: ECDSA_P256 (secp256r1), ECDSA_P384 (secp384r1), or ECDSA_P521 (secp521r1). ▪ The signature hash algorithm of the client certificate must be SHA-256, SHA-384, or SHA-512. ▪ If an intermediate certificate exists, you must prepare a signed public key certificate in a certificate chain that contains the intermediate certificate. ▪ The certificate chain for the certificate to be uploaded must have 20 tiers or fewer including the root CA certificate.
Certificate requirements for VSP E990 and VSP G/F350, G/F370, G/F700, G/F900	▪ The public key of the server certificate for the KMIP server must be RSA. ▪ The root certificate must be in X.509 DER or X.509 PEM format and must be placed on the KMS. For details, see the documentation for the server. ▪ The extended profile fields in the X.509 certificate must support the following items as specified in RFC5280: • BasicConstraints • KeyUsage • SubjectKeyIdentifier ▪ The client certificate must be current, not expired, and in PKCS#12 format. • If an intermediate certificate exists, you must prepare a signed public key certificate in a certificate chain that contains the intermediate certificate. • The certificate chain for the certificate to be uploaded must have 5 tiers or fewer including the root CA certificate. • The public key of the certificate to be uploaded must be RSA.

Item	Requirements
	▪ The client certificate must be converted to the PKCS#12 format. The client certificate that is not converted to the PKCS#12 format must be signed by the CA (Certificate Authority) for the KMS. ▪ If you do not know the password of the client certificate in the PKCS#12 format, contact the KMS administrator.

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	If the primary volume (P-VOL) of a pair (source volume for FlashCopy®) is encrypted, encrypt the secondary volume (S-VOL) (target volume for FlashCopy®) to ensure data security.
Thin Image	Match the encryption states of the P-VOL and pool-VOL. If the P-VOL is encrypted, encrypt all of the pool-VOLs. If the data pool contains an unencrypted pool-VOL, the differential data of the P-VOL is not encrypted. In this case, the security of the data in the S-VOL cannot be guaranteed.
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, active flash	When enabling encryption for data written to a data pool through a V-VOL, use a data pool that consists of encrypted pool volumes. However, if the data in virtual volumes being used is encrypted, you need to perform formatting for the virtual volumes.
Volume Migration	Encrypt the source LDEV and the target LDEV. The encryption states of the source and target LDEVs must match for the Encryption License Key feature to encrypt and guarantee the security of the data on the source and target LDEVs.

Functions	Interoperability requirements and considerations
Dedupe and compression	When disabling encryption on a parity group, you must disable the capacity saving settings on the virtual volumes associated with the parity group before you can disable encryption on the parity group.

Installing the license key for the Encryption License Key software

Use the following procedure to install the license key for the Encryption License Key software on the storage system.

Before you begin

- You must have the Storage Administrator (Initial Configuration) role to perform this task.
- Verify that your system meets the system requirements.

Procedure

1. In the **Explorer** pane, click **Administration**, and then click **License Keys**.
2. In the **License Keys** window, click **Install Licenses**.
3. In **License Key**, select **Key Code** or **File**, and then enter the license key code or specify the license key file for Encryption License Key.
4. Click **Add**.
5. In the **Selected License Keys** table, select the license key code that you added, and then click **Enable**.
6. Click **Finish**.
7. In the **Confirm** window, verify the settings, and enter a task name.

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

   If **Go to tasks window for status** is checked, the **Tasks** window opens.

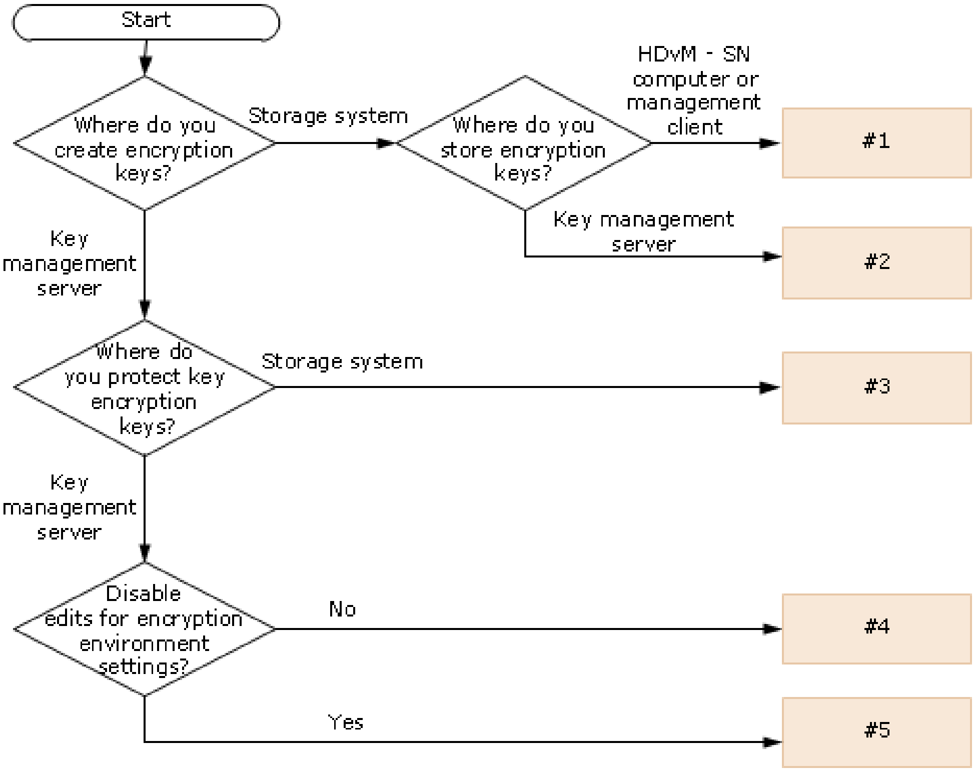
Next steps

- If you will use a key management server, configure the key management server. For instructions, see Configuring the key management server (on page 23).
- Assign the Security Administrator (View & Modify) role to the user who will initialize the encryption environmental settings.
- Initialize the encryption environmental settings on the storage system. After the encryption environmental settings have been initialized, you can enable encryption on the desired parity groups and back up the encryption keys.

Determining the encryption environmental settings for your system

To manage the encryption keys properly, you must select the appropriate encryption environmental settings in the Edit Encryption Environmental Settings window. After you perform the initial configuration of the encryption environmental settings, you will not be able to change certain settings.

Use the following flowchart and table to determine which encryption environmental settings are correct for your encryption environment.


Start
Where do you create encryption keys?
Storage system
Where do you store encryption keys?
HDvM - SN computer or management client
#1
Key management server
#2
Key management server
Where do you protect key encryption keys?
Storage system
#3
Key management server
Disable edits for encryption environment settings?
No
#4
Yes
#5

	Settings in the Edit Encryption Environmental Settings window						
		Server Settings					
	KMS	Primary Server	Secondary Server	Generate Encryption Keys on KMS	Protect the Key Encryption Key at the KMS	Delete Internal Encryption Keys at PS OFF	Disable local key generation
#1	Disable	--	--	--	--	--	--
#2	Enable	Specify settings	Enable and specify settings	--	--	--	--

	Settings in the Edit Encryption Environmental Settings window						
		Server Settings					
	KMS	**Primary Server**	**Secondary Server**	**Generate Encryption Keys on KMS**	**Protect the Key Encryption Key at the KMS**	**Delete Internal Encryption Keys at PS OFF**	**Disable local key generation**
#3	Enable	Specify settings	Enable and specify settings	Select	--	--	--
#4	Enable	Specify settings	Enable and specify settings	Select	Select	Select	--
#5	Enable	Specify settings	Enable and specify settings	Select	Select	Select	Select

Designating the regular backup user

The regular encryption key backup function is available only when the key management server is used. If you want to enable the regular backup function, you must first designate a specific user as the regular backup user and then enter the credentials (user name and password) for the regular backup user in the Edit Encryption Environmental Settings window when you enable regular backups.

Before you begin

- You must have the Security Administrator (View & Modify) role to perform this task.

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, expand **User Groups**, and then select the **Security Administrator (View & Modify)** user group.
2. On the **Users** tab, click **Create User**.
3. On the **Create User** window:
   a. In **User Name**, enter the desired user name (1-256 characters).

      You can use alphanumeric characters and the following symbols in the user name: # $ % & ' * + - . / = ? @ ^ _ ` { | } ~

   b. For **Account Status**, select **Enable**.

   c. For **Authentication**, select **Local**.

   d. In **Password**, enter the desired password (6-256 characters), and then enter the password again in **Re-enter Password**.

      You can use alphanumeric characters and all symbols in the password.

e. Click **Finish**.

4. On the confirmation window:

   a. In **Task Name**, enter the desired task name or accept the default task name.

   b. In **Selected User**, verify the information for the new user.

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

   d. Click **Apply**.

Performing the initial configuration of the encryption environmental settings

Before you can start enabling encryption on parity groups, you must perform the initial configuration of the encryption environmental settings using the **Edit Encryption Environmental Settings** window. The encryption environmental settings and options include the following:

- Enabling use of a key management server (KMS)
- Enabling use of a secondary KMS in addition to the primary KMS
- Enabling and scheduling regular backups of the encryption keys to the KMS
- Generating encryption keys on the KMS
- Protecting the key encryption key (KEK) on the KMS
- Deleting local/internal encryption keys when the storage system is powered off
- Disabling generation of encryption keys on the storage system

⚠ **Caution:** Make sure you select the correct encryption environmental settings for your operational environment. After you perform the initial configuration of the encryption environmental settings, you will not be able change certain settings. For details about determining the correct encryption environmental settings for your operational environment, see Determining the encryption environmental settings for your system (on page 34).

Before you begin

- You must have the Security Administrator (View & Modify) role.
- If you are enabling regular encryption key backups on a KMS, you must have the user name and password of the regular backup user.
- If you will use a KMS:
  - The KMS must already be configured. For instructions, see Configuring the key management server (on page 23).
  - You must have the network connection information (for example, IP address or host name, port number) for the KMS.
  - (VSP E990, VSP G/F350, G/F370, G/F700, G/F900) If you want to connect to the KMS using the host name instead of the IP address, the DNS server must be configured on the OS network settings of the SVP.
  - You must have the names and directory locations of the client and root certificates on the KMS.

Procedure

1. On the **Explorer** pane, select **Administration**, and then select **Encryption Keys**.
2. On the **Encryption Keys** pane, click **Edit Encryption Environmental Settings**.
3. Select the desired option for **Key Management Server**.
   - If you are using a KMS, select **Enable** for **Key Management Server**, and go to the next step.
   - If you are not using a KMS, select **Disable** for **Key Management Server**, click **Finish**, and go to the last step.
4. Expand **Server Settings**, and enter the network connection information for the primary KMS under **Primary Server**.
5. If you will use a secondary KMS, select **Enable** for **Secondary Server**, and enter the network connection information for the secondary KMS under **Secondary Server**.

   If you want to protect the key encryption key (KEK) at the KMS, you must enable the secondary server. If you want to disable encryption key generation on the storage system, you must enable the secondary server.
6. Test the connections to the primary and secondary KMSs by clicking **Check** next to **Server Configuration Test**.

   If the server configuration test fails, error messages are displayed. Resolve the errors before continuing.
7. If you want regular encryption key backups to be performed automatically:

   a. Select **Enable Encryption Key Regular Backup to Key Management Server**.

   b. Under **Regular Backup Time**, select the desired daily backup times.

   c. Under **Regular Backup User**, enter the user name and password of the designated regular backup user.

> **Caution:** If you enable regular encryption key backups, observe the following requirements and restrictions:
>
> - The Encryption License Key software license must be valid and enabled. If the Encryption License Key software license expires or is disabled or removed, regular backups are not performed.
> - The user account for the regular backup user must not be deleted or edited. If the user account of the regular backup user is deleted or edited, including changing the password or roles, a regular encryption key backup might fail. For this reason, every time the user account of the regular backup user is edited, make sure to respecify the user name and password of the regular backup user in the **Edit Encryption Environmental Settings** window.
> - If you change the time zone settings from a maintenance PC or on the SVP, you must restart the services of all storage systems in the **Storage Device List** window. If you do not restart the services, regular backups will not performed as scheduled.

8. If you want to generate the encryption keys on the KMS, select **Generate Encryption Keys on Key Management Server**.

   > **Note:** If you select **Generate Encryption Keys on Key Management Server**, this task will take a while to complete. Do not cancel this task while the settings are being configured.

9. If you want to store the KEK on the KMS, select **Protect the Key Encryption Key on the Key Management Server**, read the warning, and then select **I Agree**.

   > **Caution:** If you enable this option, the storage system will get the encryption keys backed up on the KMS when the storage system is powered on. Therefore, you must confirm that the SVP is properly connected to the KMS before powering on the storage system.

10. If you store the encryption keys in the KMS, and you want the encryption keys in the storage system to be deleted when the storage system is powered off, select **Delete Internal Encryption Keys at PS OFF**, read the warning, and then click **I Agree**.

    > **Caution:** If you enable this option, the storage system will get the encryption keys backed up on the KMS when it is powered on. Therefore, you must confirm that the SVP is properly connected to the KMS before powering on the storage system.

11. If you want to generate encryption keys on the KMS without creating encryption keys in the storage system, select **Disable Local Key Generation**, read the warning, and select **I Agree**.

    > **Caution:** If you enable this option, you will not be able to change this setting later.

12. When you are finished configuring the encryption environmental settings, click **Finish**.
13. In the confirmation window:

    a. Verify the selected settings.

b. In **Task Name**, enter the desired task name or accept the default task name.

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

d. Click **Apply**.

Result

Important: If the KMS is unavailable after you complete this task, the network connection settings might be incorrect. Contact the server administrator or the network administrator.

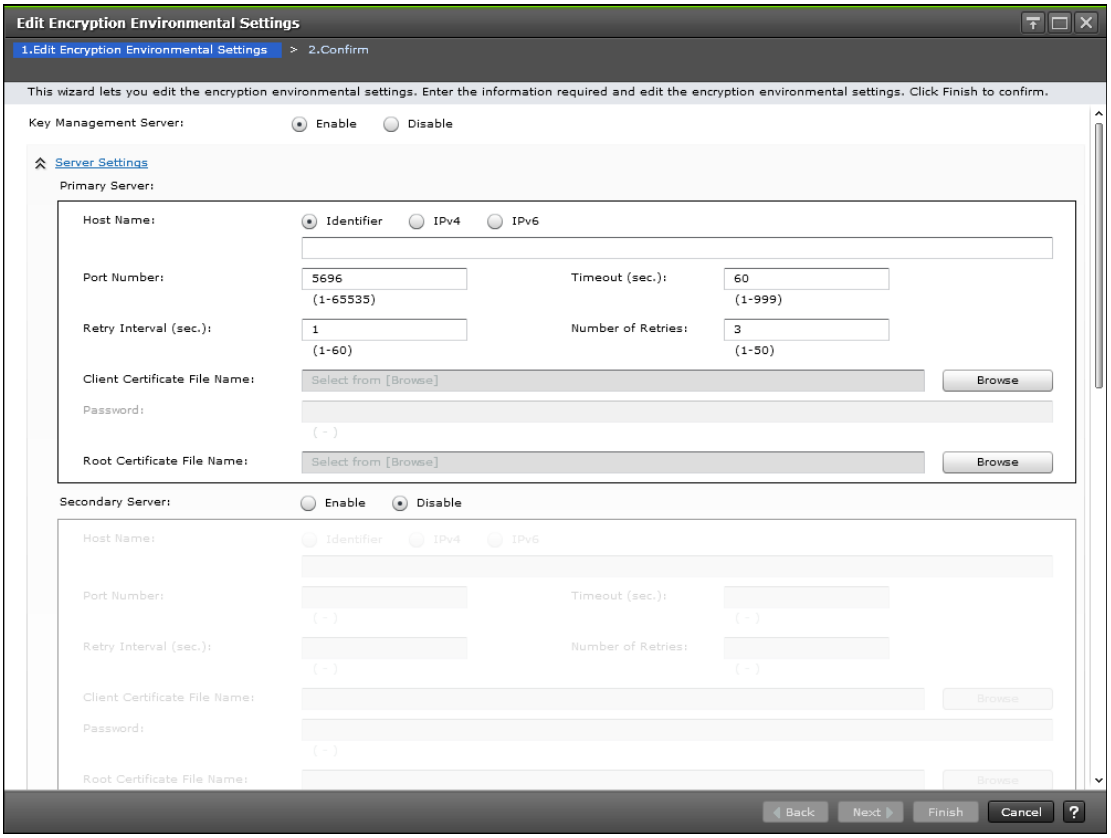
Next steps

- Save a backup copy of the client certificate.
- Back up the connection settings to the KMS by downloading the Key Management Server configuration file. For instructions, see the *System Administrator Guide*. The backup copy can be used to restore the Key Management Server configuration file if necessary.

Edit Encryption Environmental Settings window

After the encryption environmental settings have been initialized during installation, the settings in the **Edit Encryption Environmental Settings** window can be changed only 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.
- When you need to change the regular backup schedule or the regular backup user.



Edit Encryption Environmental Settings

1.Edit Encryption Environmental Settings > 2.Confirm

This wizard lets you edit the encryption environmental settings. Enter the information required and edit the encryption environmental settings. Click Finish to confirm.

Key Management Server: ● Enable ○ Disable

Server Settings

Primary Server:

Host Name: ● Identifier ○ IPv4 ○ IPv6

Port Number: 5696 (1-65535) Timeout (sec.): 60 (1-999)

Retry Interval (sec.): 1 (1-60) Number of Retries: 3 (1-50)

Client Certificate File Name: Select from [Browse] Browse

Password: (-)

Root Certificate File Name: Select from [Browse] Browse

Secondary Server: ○ Enable ● Disable

Host Name: ○ Identifier ○ IPv4 ○ IPv6

Port Number: (-) Timeout (sec.): (-)

Retry Interval (sec.): (-) Number of Retries: (-)

Client Certificate File Name: Browse

Password: (-)

Root Certificate File Name: Browse

Item	Description
Key Management Server	Select whether to use a key management server. By default, no option is selected. ▪ Enable: Key management server is used. ▪ Disable: Key management server is not used.
Server Settings	When Enable is selected for Key Management Server, the following items are displayed: ▪ Primary server ▪ Secondary server ▪ Server Configuration Test

Item	Description
Primary Server	Specify the network connection information for the primary key management server. ▪ Host Name: Select the method used to identify the host, Identifier, IPv4, or IPv6, and then enter the information: • If you selected Identifier, enter the identifier for the host. • If you selected IPv4, enter the IPv4 address of the host. • If you selected IPv6, enter the IPv6 address of the host. ▪ Port Number: Enter the port number of the key management server (range = 1 to 65535, default = 5696). ▪ Timeout (sec.): Enter the time (in seconds) until the connection attempt to the key management server times out (range = 1 to 999, default = 60). ▪ Retry Interval (sec.): Enter the interval to retry the connection to the key management server (range = 1 to 60, default = 1). ▪ Number of Retries: Enter the number of times to retry the connection to the key management server (range = 1 to 50, default = 3). ▪ Client Certificate File Name: Enter the client certificate file for connecting to the key management server by clicking Browse and selecting the file. The form of the client certificate is PKCS#12. For details about the client certificate file, contact the server administrator or the network administrator. • Password: Enter the password for the client certificate. Number of characters: 0 to 128 Valid characters: numbers (0 to 9), upper case letters (A-Z), lower case letters (a-z), symbols: ! # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ ▪ Root Certificate File Name: Enter the root certificate file for connecting to the key management server by clicking Browse and selecting the file. The form of the root certificate is X.509. For details about the root certificate file, contact the server administrator or the network administrator.

Item	Description
Secondary Server	If you are using a secondary key management server, select Enable and then specify the network connection information for the secondary server: Host Name, Port Number, Timeout (sec.), Retry Interval (sec.), Number of Retries, Client Certificate File Name, Root Certificate File Name. **Note:** You must enable the Secondary Server if you want to select any of these settings: Protect the Key Encryption Key at the Key Management Server, Delete Internal Encryption Keys at PS OFF, or Disable local key generation.
Server Configuration Test	Select Check to start a network connection test for the key management server based on the specified settings. Result: Displays the result of the network connection test for the key management server.
Enable Encryption Key Regular Backup to Key Management Server	Select this option to enable regular encryption key backup operations on the key management server. This item cannot be selected if Disable is selected for Key Management Server. ▪ Regular Backup Time: Select the time, or times, for the regular backup operations. Check Select All to schedule hourly backups. ▪ Regular Backup User Name: Enter the user name of the regular backup user. ▪ Password: Enter the password of the regular backup user. **Caution:** If the user account of the regular backup user is deleted, you must enter a new regular backup user on this window. If not, regular backups will not be performed. If the user account of the regular backup user is edited (for example, changing the password or roles), you must re-enter the user name and password of the regular backup user on this window. If not, regular backups will not be performed.
Generate Encryption Keys on Key Management Server	Select this option if you want to create encryption keys on the key management server. **Note:** If you want to select Protect the Key Encryption Key at the Key Management Server, Delete Internal Encryption Keys at PS OFF, or Disable local key generation, you must select Generate Encryption Keys on Key Management Server.

Item	Description
Protect the Key Encryption Key at the Key Management Server	Select this option if you want to save the key encryption keys on the key management servers. **Note:** To enable this option, you must read the Warning and confirm the content of the warning by selecting **I agree**.
Delete Internal Encryption Keys at PS OFF	Select this option if you want to save the encryption keys in the key management server and delete the encryption keys in the storage system when the storage system is powered off. This option can be selected only when Enable is selected for Secondary Server and when the Protect the Key Encryption Key at the Key Management Server option is enabled. **Note:** To enable this option, you must read the Warning and confirm the content of the warning by selecting **I agree**.
Disable local key generation	Select this option if you want to create encryption keys only on the key management server and not on the storage system. This option can be selected only when Enable is selected for Secondary Server and when the Protect the Key Encryption Key at the Key Management Server option is enabled. **Note:** To enable this option, you must read the Warning and confirm the content of the warning by selecting **I agree**. **Caution:** If you enable this option and apply the setting to the storage system, you will not be able to undo this action or restore the settings.
Initialize Encryption Environmental Settings	Initializes the encryption environmental settings on the storage system.

Disabling or removing the encryption software

Use this workflow to disable or remove the Encryption License Key software.

Note: When you disable a software license, you can re-enable the license. When you remove a software license, you must contact customer support if you want to reinstall the license. For additional information about disabling and removing software licenses, see the *System Administrator Guide*.

Before you begin

- Verify that encryption is disabled on all encrypted parity groups.

  If encryption is enabled on any parity groups, the software license cannot be disabled or removed. For instructions on disabling encryption, see Disabling data encryption on a parity group that does not contain pool volumes (on page 67).
- Verify that the encryption environmental settings have been initialized.

  If the encryption environmental settings have not been initialized, the software license cannot be disabled or removed. For instructions on initializing the encryption environmental settings, see Initializing the encryption environmental settings (on page 65).
- You must have the Storage Administrator (Initial Configuration) role to perform this task.

Procedure

1. In the **Explorer** pane, click **Administration**, and then click **License Keys**.
2. In the **License Keys** window, select **Encryption License Key**, and then click **Disable Licenses** or **Remove**.
3. Check the settings in the confirmation window, and then click **Apply**.

Chapter 4: Creating and backing up encryption keys

Encryption keys are commonly created in the storage system. However, when you use a key management server and enable the Generate Encryption Keys on Key Management Server option (**Edit Encryption Environmental Settings** window), encryption keys are created on a key management server and used in the storage system.

When encryption keys are created in the storage system, you must manually back up the encryption keys to a file or to a key management server. When you back up encryption keys manually to a file, you must specify the key restoration password. In configurations with an SVP, you can specify additional requirements for the key restoration password (for example, increasing the minimum number of characters, specifying the minimum number of uppercase letters, and so on).

When encryption keys are created on a key management server, the keys are automatically backed up when they are created. In addition, you can optionally schedule regular backups to the key management server, and you can change the regular backup schedule as needed.

Creating encryption keys

You can use Device Manager - Storage Navigator to create new encryption keys. Encryption keys are created automatically when you perform the initial configuration of the encryption environmental settings in the **Edit Encryption Environmental Settings** window. The number of keys created automatically depends on the number of installed encrypting back-end modules (EBEMs) or encrypting controllers (ECTLs).

- VSP 5000 series: The maximum number of encryption keys per storage system is 4,096. If the maximum number of EBEMs is installed, 4,072 keys are created automatically, so in this case you can create 24 more encryption keys.
- VSP E990: The maximum number of encryption keys per storage system is 4,096. If the maximum number of EBEMs are installed, 4,088 keys are created automatically, so in this case you can create 8 more encryption keys.
- VSP G/F900: The maximum number of encryption keys per storage system is 4,096. If the maximum number of EBEMs are installed, 4,088 keys are created automatically, so in this case you can create 8 more encryption keys.
- VSP G/F700: The maximum number of encryption keys per storage system is 4,096. If the maximum number of EBEMs is installed, 4,092 keys are created automatically, so in this case you can create 4 more encryption keys.
- VSP G/F350, VSP G/F370: The maximum number of encryption keys per storage system is 1,024. If the maximum number of ECTLs is installed, 1,022 keys are created automatically, so in this case you can create 2 more encryption keys.

Before you begin

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

Procedure

1. In the **Explorer** pane, select **Administration**, and then select **Encryption Keys**.
2. On the **Encryption Keys** tab, click **Create Keys**.
3. In the **Create Keys** window, specify the number of encryption keys you want to create. The new encryption keys will have with the **Free** attribute, and the key IDs will be assigned automatically.
4. Click **Finish**.
5. In the confirmation window:
   a. Verify the selected settings.
   b. In **Task Name**, enter the desired task name or accept the default task name.
   c. If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.
   d. Click **Apply**.

Next steps

If you are not using a key management server, create secondary backups of the new encryption keys. For instructions, see Backing up the encryption keys to a file (on page 46).

If you are using a key management server, the encryption keys are automatically backed up immediately after they are created. In addition, if you enabled the regular encryption key backup option, regular backups of the encryption keys will be performed daily according to the specified schedule.

Backing up encryption keys

Immediately after creating encryption keys, it is strongly recommended that you back up all keys (secondary backup). You can back up encryption keys to a file or to a key management server. If you do not use a key management server, you can back up encryption keys to a file using the **Backup Keys to File** window. If you use a key management server, the keys are automatically backed up. When you configure the key management server in the **Edit Encryption Environmental Settings** window, you can also schedule regular backups.

> ⚠ **Caution:** You are responsible for storing the secondary backup keys securely. Include this process in your corporate security policy. If the primary data encryption key becomes unavailable and the secondary backup data encryption key does not exist, the system cannot decrypt the encrypted data.

Encryption keys that you create are backed up in batch.

Backing up the encryption keys to a file

You can create secondary backups of the data encryption keys as a file on the Device Manager - Storage Navigator computer.

Before you begin

- Confirm that the storage system is not processing any other tasks (click Tasks in the Explorer pane). You cannot back up the encryption keys while a task is in process on the storage system.
- You must have the Security Administrator (View & Modify) role.

Procedure

1. On the **Explorer** pane, expand **Administration**, and then click **Encryption Keys**.
2. On the **Encryption Keys** tab, select the data encryption keys you want to back up, and then click **Backup Keys** > **To File**.
3. In the **Backup Keys to File** window, enter and re-enter the key restoration password (case sensitive), and then click **Finish**.

   Note: The character requirements for the key restoration password are displayed on the window. You can change these requirements using the **Edit Password Policy (Backup Encryption Keys)** window.

4. In the **Confirm** window, confirm the settings, and enter a task name in **Task Name**.

   If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.
5. 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**.

Next steps

The files and passwords are not automatically backed up. You are responsible for backing up the files as needed and maintaining the key restoration passwords.

Changing the password requirements for the backup encryption keys

When you back up the encryption keys to a file on the Device Manager - Storage Navigator computer, you must enter a key restoration password. If desired, you can specify the following additional character requirements for the password:

- Minimum number of numeric characters (0-9)
- Minimum number of uppercase letters (A-Z)
- Minimum number of lowercase letters (a-z)
- Minimum number of symbols (! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~)
- Minimum total number of characters

Before you begin

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

Procedure

1. In the **Settings** menu, select **Security** > **Encryption Keys** > **Edit Password Policy (Backup Encryption Keys)**.
2. In the **Edit Password Policy (Backup Encryption Keys)** window, enter the desired password requirements.
3. Click **Finish**.
4. In the **Confirm** window, confirm the settings, and enter a task name in **Task Name**.

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

Backing up the encryption keys manually to a key management server

You can create secondary backups of the data encryption keys on the key management server (KMS). The data encryption keys that you back up to the KMS are managed with the client certificate. When you manually back up to the KMS, the server uses another data encryption key to encrypt the original keys. Both keys reside on the server.

> **Note:** The number of keys that can be backed up on a KMS is limited. Delete unnecessary keys whenever possible.

Before you begin

- Confirm that the storage system is not processing any other tasks (click Tasks in the Explorer pane). You cannot back up the encryption keys while a task is in process on the storage system.
- You must have the Security Administrator (View & Modify) role

Procedure

1. On the **Explorer** pane, expand **Administration**, and then click **Encryption Keys**.
2. On the **Encryption Keys** tab, select the data encryption keys you want to back up, and then click **Backup Keys** > **To Server**.
3. In the **Backup Keys to Server** window, enter a description for the selected data encryption keys (or confirm the default description), and then click **Finish**.
4. In the **Confirm** window, confirm the settings, and enter a task name in **Task Name**.

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

Viewing encryption keys backed up on the key management server

You can view a list of the encryption keys that are backed up on the key management server. The following information is displayed for each key:

- **UUID:** UUID of the backup encryption key on the key management server
- **Backup date:** Date (YYYY/MM/DD) and time (HH:MM:SS) the encryption key was backed up on the server
- **Description:** Description entered on the **Backup Keys to Server** window when the key was backed up. If the encryption key was backed up by a regular backup operation, the description has the following format:

```
AutoBackup_[backup-year-month-date_backup-time]
```

Before you begin

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

Procedure

1. On the **Explorer** pane, select **Administration**, and then select **Encryption Keys**.
2. On the **Encryption Keys** tab, click **View Backup Keys on Server**.
   The **View Backup Keys on Server** window displays the encryption keys that are backed up on the key management server.

Changing the schedule for regular encryption key backups

Use this procedure to change the schedule for regular encryption key backups on the key management server.

> **Note:** During a regular backup, your service representative cannot perform SVP operations or maintenance of the storage system. If a regular backup will occur during planned maintenance, please revise the regular backup schedule as described below, or cancel the regular backup task temporarily.

Before you begin

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

Procedure

1. In the **Explorer** pane, select **Administration**, and then select **Encryption Keys**.
2. In the **Encryption Keys** pane, click **Edit Encryption Environmental Settings**.
3. Select the new daily backup times from **Regular Backup Time**, 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**.
5. Click **Apply**.

Changing the data encryption key for encrypted data

If you want to encrypt encrypted data with another encryption key, the data must be moved. You must create a new encrypted parity group and then move the data to that parity group using ShadowImage, TrueCopy, or Volume Migration. You can move data for each LDEV.

Note: After migrating data, if you disable encryption on the source parity group, the encryption keys assigned to the drives in the parity group are deleted, and new encryption keys are assigned. In addition, if a drive is replaced, the data encryption keys allocated to that drive are deleted, and new data encryption keys are allocated when the new drive is added.

Procedure

1. Create a new parity group.
2. Enable encryption with a new data encryption key. See Enabling encryption (on page 51).
3. Format the LDEVs in the encrypted parity group. For instructions, see the *Provisioning Guide*.
4. Migrate the source data to the new target LDEVs in the encrypted parity group.

Chapter 5: Enabling encryption

The Encryption License Key feature provides data-at-rest encryption. Encryption is enabled at the parity-group level to protect the data stored on the drives in the parity group.

Caution: Data encryption is not ensured in a pool with mixed encryption (that is, the pool contains both encrypted and nonencrypted pool-VOLs). To manage data encryption securely, make sure that all pool-VOLs in a pool are encrypted.

Enabling encryption on a parity group that does not contain pool volumes

Use this procedure to enable encryption on a parity group that does not contain any pool volumes.

You can enable encryption on a parity group only under the following conditions:

- The parity group must not contain any volumes, or all volumes in the parity group must be blocked. If the parity group contains any unblocked volumes, you must block the volumes before encryption can be enabled.
- Accelerated compression must not be enabled on the parity group. If accelerated compression is enabled on the parity group, you must disable accelerated compression before encryption can be enabled. For details about disabling accelerated compression, see the *Provisioning Guide*.

Before you begin

- You must have the Security Administrator (View & Modify) role to enable encryption.
- The encryption environmental settings must already be configured.
- If the target parity group contains volumes, you must have the Storage Administrator (Provisioning) role to format the volumes.

Caution: Enabling encryption on a parity group is a destructive operation. Verify the correct parity group ID before performing this operation. You are responsible for backing up the data in the target parity group, if necessary, before performing this operation.

Procedure

1. In the **Explorer** pane, expand the **Storage Systems** tree, and then select **Parity Groups**.

2. On the **Parity Groups** tab, select the target parity group, and then click **Edit Encryption**.

   > ⚠ **Caution:** If you do not select one or more specific parity groups, all parity groups are selected.

3. In the **Edit Encryption** window, select the desired settings for each parity group:
   a. In the **Available Parity Groups** table, select the parity group.
   b. For **Encryption**, select **Enable**.

      If the parity group contains unblocked volumes, or if accelerated compression is enabled for the parity group, an error will occur when you perform this task.
   c. For **Format Type**, select the desired format type.

      If the parity group does not contain pool volumes, you can select **Normal Format** or **Quick Format**. If you select **No Format**, the LDEVs in the encrypted parity group will be blocked.

      If the parity group contains pool volumes, select **Normal Format**. If you select **Quick Format**, an error will occur when you perform this task.
   d. Click **Add**.
      The parity group is added to the **Selected Parity Groups** list.

      If there are no volumes in the parity group, the format type in the **Selected Parity Groups** list is displayed as a hyphen (-).
   e. If you want to change the format type of a parity group in the **Selected Parity Groups** list, select the parity group, click **Remove**, and then add the parity group to the **Selected Parity Groups** list again with the desired format type.
4. When you are finished adding parity groups to the **Selected Parity Groups** list, 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**.
6. Click **Apply**, and then click **OK** in the message that appears.

Enabling encryption on a parity group that contains pool volumes

Use this procedure to enable encryption on a parity group that contains one or more pool volumes.

You can enable encryption on a parity group that contains pool volumes only under the following conditions:

- The parity group must not contain any volumes, or all volumes in the parity group must be blocked. If the parity group contains any unblocked volumes, you must block the volumes before encryption can be enabled.
- Accelerated compression must not be enabled on the parity group. If accelerated compression is enabled on the parity group, you must disable accelerated compression before encryption can be enabled. For details about disabling accelerated compression, see the *Provisioning Guide*.

Before you begin

- You must have the Security Administrator (View & Modify) role to enable encryption.
- The encryption environmental settings must already be configured.
- If the target parity group contains volumes, you must have the Storage Administrator (Provisioning) role to format the volumes.
- You must have the Storage Administrator (Provisioning) role to format virtual volumes and disable capacity saving.

> ⚠ **Caution:** Enabling encryption on a parity group is a destructive operation. Verify the correct parity group ID before performing this operation. You are responsible for backing up the data in the target parity group, if necessary, before performing this operation.

Procedure

1. On the **Explorer** pane, click **Storage Systems**, expand **Pools**, and click the pool to which the target parity group belongs.
2. Select the **Virtual Volumes** tab, and check the settings in the **Capacity Saving Status** column:
   - If the **Capacity Saving Status** of all virtual volumes is **Disabled**, go to the next step.
   - If the **Capacity Saving Status** of virtual volumes is not **Disabled**, perform the following actions for each virtual volume whose capacity saving status is not disabled:
     a. Block the virtual volume.
     b. Format the virtual volume.
     c. Disable the capacity saving setting on the virtual volume.
     d. Verify that **Capacity Saving Status** of the virtual volume shows **Disabled**.
3. On the **Virtual Volumes** tab, check the LDEV status in the **Status** column of the table:
   - If the status of all LDEVs is **Blocked**, or if there are no LDEVs, go to the next step.
   - If the status of all LDEVs is not **Blocked**, block the LDEVs.
4. Enable data encryption for the parity group as follows:
   a. On the **Explorer** pane, click **Parity Groups**.
   b. On the **Parity Groups** tab, select the target parity group, and then click **Edit Encryption**.

c. In the **Edit Encryption** window, select the parity group, and then select **Enable** for **Encryption**.

   If the parity group contains unblocked volumes, or if accelerated compression is enabled for the parity group, an error will occur when you perform this task.

d. For **Format Type**, select **Normal Format**.

e. Click **Add**.
   The parity group is added to the **Selected Parity Groups** list.

   If there are no volumes in the parity group, the format type in the **Selected Parity Groups** list is displayed as a hyphen (-).

f. If you want to change the format type of a parity group in the **Selected Parity Groups** list, select the parity group, click **Remove**, and then add the parity group to the **Selected Parity Groups** list again with the desired format type.

g. When you are finished adding parity groups to the **Selected Parity Groups** list, click **Finish**.

h. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.

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

i. Click **Apply**, and then click **OK** in the message that appears.

5. Format the virtual volumes belonging to the pool you selected in step 1.

> ⚠ **Caution:** Make sure to format the volumes in this step. Do not restore the volumes. Restoring the volumes might cause problems.

Next steps

If desired, you can now re-enable the capacity saving settings on the pool and virtual volumes.

- To re-enable the capacity saving function of the volumes, set Capacity Saving to Compression or Deduplication and Compression in the **Edit LDEVs** window.

Encrypting existing data

If you want to encrypt existing data on your storage system, you must migrate the data to an encrypted parity group. Use the following procedure to encrypt existing data.

Procedure

1. Create a new parity group.

2. Enable encryption on the new parity group as follows:

a. On the **Parity Groups** tab, select the target parity group, and then click **Edit Encryption**.

b. In the **Edit Encryption** window, select the parity group in the **Available Parity Groups** table, select **Enable** for **Encryption**, and then click **Add**.
   The parity group is added to the **Selected Parity Groups** list.

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

      If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.
   e. Click **Apply**, and then click **OK** in the message that appears.

3. Format the LDEVs in the encrypted parity group. For instructions, see the *Provisioning Guide*.
4. Migrate the existing data to the LDEVs in the encrypted parity group using ShadowImage or Volume Migration. For details about Volume Migration, contact your account team.
5. After the existing data has been migrated to the encrypted parity group, shred the (unencrypted) migration source volumes to prevent the data from being leaked. For instructions, see the *Hitachi Volume Shredder User Guide*.

Chapter 6: Restoring encryption keys

When all of the LDEVs in 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), the encryption keys can be restored from the primary or secondary backup copy.

When key information is lost or deleted, restoration is performed in a batch for the backed-up encryption keys. The maximum number of backed up encryption keys are as follows:

- VSP 5000 series: 4,128 keys
- VSP E990: 4,112 keys
- VSP G/F900: 4,112 keys
- VSP G/F700: 4,104 keys
- VSP G/F350, G/F370: 1,028 keys

The storage system automatically restores encryption keys from the primary backup. Users restore encryption keys from the secondary backup using Device Manager - Storage Navigator. If you need to restore an encryption key that is not the latest key from a secondary backup copy, you must have the Security Administrator (View & Modify) and Support Personnel (View & Modify) roles.

⚠ **Caution:** When you restore the encryption key, always restore the latest key. If the backed up encryption key (secondary backup) is not the latest key, it cannot be restored.

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

Restoring keys from a file

You can restore the data encryption keys from a file backed up on the computer.

Before you begin

- Block the LDEVs associated to the encrypted parity group. For details, see the *Provisioning Guide*.
- You must have the Security Administrator (View & Modify) role.

Procedure

1. On the **Explorer** pane, select **Administration**, and then 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 then click **Open**.
5. In the **Restore Keys from File** window, complete the following item and then click **Finish**:
   - **File Name** displays the name of the selected file.

     View-only: Yes
   - In **Password**, type the password for the data encryption key that you entered when you backed up the selected encryption key file.
6. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.

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

   Click **Apply**.

   The backup data encryption key is restored.

Restoring keys from a key management server

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

> **Caution:** If you do not have the client certificate and the SVP is replaced due to a failure, you cannot restore the backed up data encryption keys.

Before you begin

- Block the LDEVs associated to the encrypted parity group.
- You must have the Security Administrator (View & Modify) role.

Procedure

1. On the **Explorer** pane, select **Administration**, and then 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 **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.
6. Click **Apply**.

   The backup data encryption key is restored.

Forcibly restoring encryption keys

If encryption keys cannot be used, including the keys backed up as the primary backup in the storage system, restore the encryption keys backed up as the secondary backup. Backed-up encryption keys for which key information is lost or deleted are restored in a batch. The following table lists the maximum number of backed up encryption keys.

Storage system model	Maximum number of backed-up encryption keys
VSP 5000 series	4,128
VSP E990	4,112
VSP G/F900	4,112
VSP G/F700	4,104
VSP G/F350, VSP G/F370	1,028

Note: To restore an encryption key, all volumes in the encrypted parity group must be blocked. In addition, after the key is restored, the blocked volumes in the encrypted parity group must be restored.

Caution: If you restore an encryption key that is not the latest key, the drive, encrypting back-end module, or ECTL might be blocked, and the data might not be read.

Forcibly restoring keys from a file

Use this procedure to restore encryption keys forcibly from a file backed up on the Device Manager - Storage Navigator computer.

Before you begin

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

Procedure

1. Block the LDEVs associated with the target parity group.
2. On the **Explorer** pane, select **Administration**, and then select **Encryption Keys**.
3. On the **Encryption Keys** tab, click **Restore Keys** > **From File (Force)**.
4. In the **Force Restore Keys from File** window, click **Browse**, and then click **OK** .
5. In the **Open** dialog box, select the backup file, and then click **Open**.
   The name of the selected file is displayed in **File Name**.

   Note: Make sure **View-only: Yes** is displayed.

6. In the **Force Restore Keys from File** window, type the password that you entered when you backed up the selected encryption key, and then click **Finish**.

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

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

Forcibly restoring keys from a key management server

Use this procedure to restore encryption keys forcibly from a key management server.

Before you begin

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

Procedure

1. Block the LDEVs associated with the target parity group.
2. On the **Explorer** pane, select **Administration**, and then select **Encryption Keys**.
3. On the **Encryption Keys** tab, click **Restore Keys** > **From Server (Force)**.
4. In the **Force Restore Keys from Server** window, select the encryption key you want to restore forcibly, and then click **Finish**.
5. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.

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

Chapter 7: Deleting encryption keys

You can delete an encryption key from a file on the HDvM - SN computer or from a key management server.

Deleting (free) encryption keys from a file

You can delete free encryption keys from a file on the Device Manager - Storage Navigator computer.

You can only delete encryption keys with the Free attribute. Encryption keys with the other attributes (CEK, DEK, KEK) cannot be deleted.

Before you begin

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

Procedure

1. On the **Explorer** pane, select **Administration**, and then 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. In the **Delete Keys** window, click **Finish**.
4. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.

   If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.
5. Click **Apply**, and then click **OK**.
   The selected free encryption key is deleted.

Deleting (free) encryption keys from the storage system

You can delete free encryption keys from the storage system.

You can only delete encryption keys with the Free attribute. Encryption keys with the other attributes (CEK, DEK, KEK) cannot be deleted.

Before you begin

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

Procedure

1. On the **Explorer** pane, select **Administration**, and then 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. In the **Delete Keys** window, click **Finish**.
4. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.

   If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.
5. Click **Apply**, and then click **OK**.
   The selected free encryption key is deleted.

Deleting a secondary backup encryption key from the server

You can delete a secondary backup encryption key from the key management server.

⚠ **Caution:** Before deleting a secondary backup encryption key from the key management server, verify that you have the (primary) backup encryption key.

Before you begin

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

Procedure

1. On the **Explorer** pane, select **Administration**, and then 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 **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.
5. Click **Apply**, and then click **OK**.
   The backup data encryption key is deleted.

Chapter 8: Managing your encryption environment

After the encryption keys have been created, you can export the encryption key information. You can also rekey the key encryption key (KEK) and rekey the certificate encryption keys (CEKs). If your storage system is configured to acquire the KEK from the KMS when the storage system starts and the acquisition fails, you can retry the KEK acquisition. After you have disabled encryption on all parity groups, you can initialize the encryption environmental settings on your storage system.

Exporting the encryption key information

You can export the encryption key information displayed in the **Encryption Keys** window. The exported file includes the serial number of the storage system, the SVP firmware version, the date and time the file was exported, the filter conditions for the encryption key list, and the following information for each key:

- **Key ID:** ID of the encryption key
- **Created:** Date and time the encryption key was created
- **Attribute:** Attribute of the encryption key (CEK, DEK, KEK, or Free)
- **Assigned to:** Resource to which the encryption key is assigned
- **Generated on:** Location or path to which the key was generated
- **Number of backups:** Number of times the key was backed up

Before you begin

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

Procedure

1. On the **Explorer** pane, select **Administration**, and then select **Encryption Keys**.
2. On the **Encryption Keys** tab, select the key IDs for the encryption key information you want to export.

   If you do not select any key IDs, information for all keys will be exported.

   > **Tip:** If desired, filter the list of encryption keys, and then export the filtered key information.

3. Click **More Actions** > **Export**.
4. When the **Ready to Download** message appears, click **OK**.

Migrating the KMS to another server

If the key encryption key (KEK) was created on the key management server (KMS) and you want to migrate the KMS to another server, use the following procedure.

Caution: Do not power off the storage system during this procedure. If either (or both) of the following encryption environmental settings is enabled and the storage system is powered off during this procedure, the KEK and the encryption keys that were backed up to the KMS cannot be obtained when the storage system is powered back on, and therefore the encrypted data cannot be decrypted.

- Protect the key encryption key at the KMS
- Delete internal encryption keys at PS OFF

Before you begin

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

Procedure

1. Change the KMS connection settings in the **Edit Encryption Environmental Settings** window:

   a. On the Explorer pane, select **Administration**, and then select **Encryption Keys**.

   b. On the **Encryption Keys** pane, click **Edit Encryption Environmental Settings**.

   c. Expand **Server Settings**, and enter the network connection information for the new KMS.

   d. Test the connection to the new KMS by clicking **Check** next to **Server Configuration Test**.

      If the server configuration test fails, error messages are displayed. Resolve the errors before continuing.

   e. When you are finished updating the encryption environmental settings, click **Finish**.

   f. Verify the settings on the confirmation window, and then click **Apply**.

   For VSP G/F350, G/F370, G/F700, G/F900, proceed to steps 2 and 3.

   For VSP 5000 series, you do not need to perform step 2 or 3. The new KEK is automatically created on the new KMS, and the encryption keys are automatically backed up on the new KMS.

2. (VSP G/F350, G/F370, G/F700, G/F900) Create a new KEK on the new KMS:

   a. On the **Encryption Keys** tab, select the key ID of the KEK in the **Encryption Keys** table, and then click **More Actions** > **Rekey Key Encryption Key**.

   b. Select **Create a new key encryption key on the key management server**, and then click **Finish**.

   c. Verify the settings on the confirmation window, and then click **Apply**.

3. (VSP G/F350, G/F370, G/F700, G/F900) Back up the data encryption keys to the new KMS:

a. On the **Encryption Keys** tab, select the data encryption keys you want to back up, and then click **Backup Keys** > **To Server**.

b. Enter a description for the selected encryption keys (or confirm the default description), and then click **Finish**.

c. Verify the settings on the confirmation window, and then click **Apply**.

Rekeying the key encryption key

If you created the key encryption key (KEK) on the key management server, you can rekey the KEK.

(VSP E990, VSP G/F350, G/F370, G/F700, G/F900) After rekeying the KEK, back up the KEK.

Before you begin

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

Procedure

1. On the **Explorer** pane, select **Administration**, and then select **Encryption Keys**.
2. On the **Encryption Keys** tab, select the key ID of the KEK from the **Encryption Keys** table.
3. Click **More Actions** > **Rekey Key Encryption Key**.

   VSP G/F350, G/F370, G/F700, G/F900: Select **Create a new key encryption key on the key management server** on the **Rekey Key Encryption Key** window.

   VSP 5000 series: If you are migrating to a new KMS and the DKCMAIN firmware version is 90-03-0*x* or later, a new KEK is created automatically on the new KMS when you change the KMS connection settings in the **Edit Encryption Environmental Settings** window. Therefore, the **Rekey Key Encryption Key** window is not used to migrate the KMS to another server. However, if there was a problem connecting to the new KMS and you need to create the new KEK manually, select **Create a new key encryption key on the key management server**.
4. Click **Finish**.
5. Confirm the settings, and enter your task name in **Task Name**.

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

Rekeying the certificate encryption keys

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

After rekeying CEKs, back up each CEK immediately.

Before you begin

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

Procedure

1. On the **Explorer** pane, select **Administration**, and then select **Encryption Keys**.
2. On the **Encryption Keys** tab, select **More Actions** > **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 **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.
4. Click **Apply**.

Retrying acquisition of the key encryption key

If your storage system is configured to acquire the key encryption key (KEK) from the key management server when the storage system starts and the acquisition of the KEK fails, you can retry the acquisition of the KEK.

Before you begin

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

Procedure

1. On the **Explorer** pane, select **Administration**, and then 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 **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.
4. Click **Apply**.

Next steps

After retrying the acquisition of the KEK, you need to restore the encrypting back-end modules, encrypting controllers, and blocked drives or blocked volumes. For assistance, contact customer support.

Initializing the encryption environmental settings

Before you initialize the encryption environmental settings, data encryption must be disabled on all parity groups.

Before you begin

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

Procedure

1. Verify that encryption has been disabled on all parity groups:
   a. In the **Explorer** pane, expand the **Storage Systems** tree, and then select **Parity Groups**.
   b. On the **Parity Groups** tab, verify that **Disabled** is displayed in the **Encryption** column for all parity groups.
2. On the **Explorer** pane, select **Administration**, and then select **Encryption Keys**.
3. On the **Encryption Keys** tab, select **Edit Encryption Environmental Settings**.
4. In the **Edit Encryption Environmental Settings** window, and select **Initialize Encryption Environmental Settings** (in the lower left corner of the window).
5. Select **Finish**.
6. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.

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

Chapter 9: Disabling encryption

Encryption is disabled at the parity-group level. When you disable encryption on a parity group, the encryption key for the drives in the parity group is deleted, and then a new encryption key is assigned. After that, the volumes in the parity group are formatted by writing (nonencrypted) zero data to the entire disk area.

Disabling data encryption on a parity group that does not contain pool volumes

Use this procedure to disable encryption on a parity group that does not contain any pool volumes.

You can disable encryption on a parity group only under the following conditions:

- The parity group must not contain any volumes, or all volumes in the parity group must be blocked. If the parity group contains any unblocked volumes, you must block the volumes before encryption can be disabled.
- Accelerated compression must not be enabled on the parity group. If accelerated compression is enabled on the parity group, you must disable accelerated compression before encryption can be disabled. For details about disabling accelerated compression, see the *Provisioning Guide*.

Before you begin

- You must have the Security Administrator (View & Modify) role to disable encryption.
- If the target parity group contains volumes, you must have the Storage Administrator (Provisioning) role to format the volumes.

Procedure

1. On the **Explorer** pane, select **Storage Systems**, and then click **Parity Groups**.
2. On the **Parity Groups** tab, confirm that all volumes in the target parity group are blocked (**Blocked** is displayed in the **LDEV Status** column).

   If the LDEV status of the parity group is not **Blocked**, block the LDEVs. You will not be able to disable encryption if the parity group contains unblocked volumes.
3. On the **Parity Groups** tab, select the target parity group, and then click **Edit Encryption**.
4. In the **Edit Encryption** window, select the desired settings for each parity group:
   a. In the **Available Parity Groups** table, select the parity group.
   b. For **Encryption**, select **Disable**.

c. For **Format Type**, select the desired format type.

   If the parity group contains a pool volume, select **Normal Format**. If you select **Quick Format**, an error will occur when you perform this task.

   If the parity group consists of FMD drives, select **No Format**. If you select **Quick Format** or **Normal Format**, an error will occur when you perform this task.

d. Click **Add**.
   The parity group is added to the **Selected Parity Groups** list.

   If there are no volumes in the parity group, the format type in the **Selected Parity Groups** list is displayed as a hyphen (-).

e. If you want to change the format type of a parity group in the **Selected Parity Groups** list, select the parity group, click **Remove**, and then add the parity group to the **Selected Parity Groups** list again with the desired format type.

5. When you are finished adding parity groups to the **Selected Parity Groups** list, click **Finish**.
6. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.

   If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.
7. Click **Apply**, and then click **OK** in the message that appears.

Disabling data encryption on a parity group that contains pool volumes

Use this procedure to disable encryption on a parity group that contains pool volumes.

You can disable encryption on a parity group that contains pool volumes only under the following conditions:

- The parity group must not contain any volumes, or all volumes in the parity group must be blocked. If the parity group contains any unblocked volumes, you must block the volumes before encryption can be disabled.

- Accelerated compression must not be enabled on the parity group. If accelerated compression is enabled, you must disable accelerated compression before encryption can be disabled. For details about disabling accelerated compression, see the *Provisioning Guide*.

- If the parity group contains a pool volume associated with a pool for which capacity saving is enabled, you must disable the capacity saving setting on the pool before encryption can be disabled.

Before you begin

- You must have the Storage Administrator (Provisioning) role to disable capacity saving and format volumes.

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

Procedure

1. On the **Explorer** pane, select **Storage Systems**, expand **Pools**, and then click the pool to which the target parity group belongs.
2. Select the **Virtual Volumes** tab, and check the settings in the **Capacity Saving Status** column:
   - If the **Capacity Saving Status** of all volumes is **Disabled**, go to the next step.
   - If the **Capacity Saving Status** of all volumes is not **Disabled**, perform the following actions for each volume whose capacity saving status is not disabled:
     a. Block the volume.
     b. Format the volume.
     c. Disable the capacity saving setting on the volume.
     d. Verify that **Capacity Saving Status** of the volume shows **Disabled**.
3. On the **Virtual Volumes** tab, check the LDEV status in the **Status** column of the table:
   - If the status of all LDEVs is **Blocked**, or if there are no LDEVs, go to the next step.
   - If the status of all LDEVs is not **Blocked**, block the LDEVs, and then go to the next step.
4. Disable data encryption for the parity group as follows:
   a. On the **Explorer** pane, select **Parity Groups**.
   b. On the **Parity Groups** tab, confirm that all volumes in the target parity group are blocked (**Blocked** is displayed in the **LDEV Status** column).

   If the LDEV status of the parity group is not **Blocked**, block the volumes. You will not be able to disable encryption if the parity group contains unblocked volumes.

   c. On the **Parity Groups** tab, select the target parity group, and then click **Edit Encryption**.
   d. In the **Edit Encryption** window, select the parity group, select **Disable** for **Encryption**, and select the desired format type for **Format Type**.

   If the parity group contains a pool volume, select **Normal Format**. If you select **Quick Format**, an error will occur when you perform the task.

   If the parity group consists of FMD drives, select **No Format**. If you select **Quick Format** or **Normal Format**, an error will occur when you perform the task.

   e. Click **Add**.
   The parity group is added to the **Selected Parity Groups** list.

   If there are no volumes in the parity group, the format type in the **Selected Parity Groups** list is displayed as a hyphen (-).

   f. If you want to change the format type of a parity group in the **Selected Parity Groups** list, select the parity group, click **Remove**, and then add the parity group to the **Selected Parity Groups** list again with the desired format type.
   g. When you are finished adding parity groups to the **Selected Parity Groups** list, click **Finish**.

   h. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.

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

   i. Click **Apply**, and then click **OK** in the message that appears.

5. Format the virtual volumes belonging to the pool you selected in step 1.

Next steps

If desired, you can now re-enable the capacity saving settings on the pool and virtual volumes.

- To re-enable the capacity saving function of the volumes, set Capacity Saving to Compression or Deduplication and Compression in the **Edit LDEVs** window.

Formatting LDEVs at the parity-group level

When you enable or disable encryption on a parity group, all LDEVs in the parity group must be formatted after encryption is enabled or disabled.

The LDEV formatting operation writes zero data to the entire area of all drives in the parity group. This process is also referred to as encryption formatting. If you use a V-VOL, encryption/unencryption formatting for the V-VOL is required. For details about formatting volumes, see the *Provisioning Guide*.

Procedure

1. In the **Storage System** tree, select **Parity Groups**.
2. On the **Parity Groups** tab, select the parity group, and then click **Format LDEVs**.
3. In the **Format LDEVs** window, select the **Normal** format type (required for V-VOLs), and then click **Finish**.
4. In the confirmation window:
   a. Verify the selected settings.
   b. In **Task Name**, enter the desired task name or accept the default task name.
   c. If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.
   d. Click **Apply**.

Chapter 10: Troubleshooting

This chapter provides troubleshooting information for the Encryption License Key feature.

Encryption events in the audit log

The audit log on the storage system records events related to Encryption License Key, including data encryption and Encryption License Key processes. You can download the audit log files in near real-time to an external syslog server.

For instructions on downloading the audit log files, see the *Hitachi Audit Log User Guide*.

Troubleshooting Encryption License Key operations

For troubleshooting information for Device Manager - Storage Navigator, see the *System Administrator Guide*. 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 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 back up and restore data encryption keys with a key management server, the connection to the key management server is available. ▪ If you back up and restore data encryption keys with a key management server, the number of keys that you can back up on the key management server is not exceeded. ▪ If you back up 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). ▪ (VSP G/F350, G/F370, G/F700, G/F900) When RSA key exchange is disabled on the SVP, the SVP uses the following four cipher suites to communicate: • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 Check whether the KMS supports these cipher suites. If not, enable RSA key exchange on the SVP.

Problem	Action
Cannot create or delete data encryption keys.	Make sure that: ▪ The Encryption License Keysoftware license is valid and installed. ▪ You have the Security Administrator (View & Modify) role. ▪ 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. ▪ (VSP G/F350, G/F370, G/F700, G/F900) When RSA key exchange is disabled on the SVP, the SVP uses the following four cipher suites to communicate: • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 Check whether the KMS supports these cipher suites. If not, enable RSA key exchange on the SVP.
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. ▪ The accelerated compression feature is disabled on the parity group.
Cannot disable encryption for a parity group.	Make sure that all LDEVs in the parity group are in the blocked status.

Problem	Action
Server configuration test failed.	▪ Check the following key management server connection settings: • Host name • Port number • Client certificate file • Root certificate file ▪ If the communication failure is due to the length of time to connect to the server, try changing these settings: • Timeout • Retry interval • Number of retries ▪ (VSP G/F350, G/F370, G/F700, G/F900) When RSA key exchange is disabled on the SVP, the SVP uses the following four cipher suites to communicate: • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 Check whether the KMS supports these cipher suites. If not, enable RSA key exchange on the SVP.
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 operations for encryption keys could not be performed (03005 068905). An error has occurred on the storage system. The encryption keys might not have been obtained from the key management server.	If all volumes are blocked and SIM code 661000 or 661001 is returned, complete the following tasks: **1.** Restore the connection to the key management server. **2.** In the Edit Encryption Environmental Settings window, click **Check** for **Server Configuration Test**, and make sure that the connection test completes successfully. **3.** Contact customer support to restart the storage system. **4.** After the storage system is restarted, make sure that all blocked volumes are restored.

Problem	Action
	In other cases, perform the following tasks: **1.** Verify the system status, and then restore the blocked parts if blocked parts exist. If no blocked parts exist, retry the operation for the failed encryption key. **2.** After the blocked parts are restored, retry the operation for the failed encryption key.
Editing encryption environmental settings has failed with the error (00002-058578).	If you are performing the initial configuration of the encryption environmental settings and the operation fails, complete the following tasks: **1.** Wait a few minutes, and then click File > Refresh All to reread the configuration information. **2.** Initialize the encryption environmental settings: Open the **Edit Encryption Environmental Settings** window, and select Initialize Encryption Environmental Settings (in the lower left corner of the window). **3.** Perform the initial configuration of the encryption environmental settings again. If you are editing the encryption environmental settings (after initial configuration of the settings has been performed) and the operation fails, complete the following tasks: **1.** Wait a few minutes, and then click File > Refresh All to reread the configuration information. **2.** Edit 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 key management server is not supported by the connected key management server. Review the system requirements for Encryption License Key, and update the key management server software to the supported version.
The Edit Encryption operation failed even though a 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 operation executed prior to the Edit Encryption operation might have failed due to encryption hardware failure. Confirm in the **Tasks** window that the Edit Encryption Environmental Settings operation failed, remove the cause of error, initialize the encryption environmental settings, and then retry the Edit Encryption Environmental Settings operation and the Edit Encryption operation.
After a Free key (encryption key with the Free attribute) was deleted, SIM code 660100 or 660200 was returned.	The number of Free keys (encryption key with the Free attribute) might be smaller than the threshold for maintenance. Create the maximum number of Free keys.

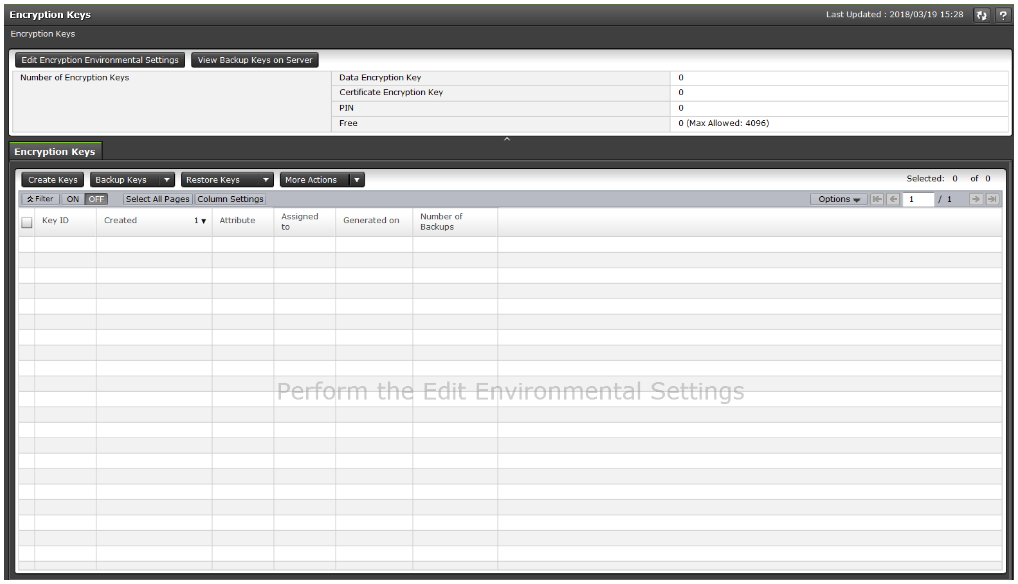
Problem	Action
Failed to initialize the encryption environmental settings.	When using Device Manager - Storage Navigator, complete the following tasks: **1.** Check if the encryption hardware is blocked. **2.** If it is blocked, open the **Encryption Keys** window, and check the attributes. **3.** If KEK, CEK, or KEK and CEK are listed under the Attribute column, create Free keys up to the maximum number for each attribute. **4.** Contact customer support to restore the blocked hardware. When using the REST API, complete the following tasks: **1.** Check if the encryption hardware is blocked. **2.** If it is blocked, obtain the number of encryption keys, and then check the attributes. **3.** When KEK, CEK, or KEK and CEK are listed under the Attribute column, the KART40325 error might appear. If the number of encryption keys are obtained and the required keys are created, do not take corrective action for the error. If another error occurs, take the corrective action specified in the error messages, and then create encryption keys. **4.** Contact customer support to restore the blocked hardware.
The encryption environmental settings for migrating the KMS to another server cannot be configured.	Complete the following tasks: **1.** Verify that the settings of the primary KMS and secondary KMS have been changed in the **Edit Encryption Environmental Settings** window. **2.** Create a new KEK on the new KMS manually: open the **Rekey Key Encryption Keys** window, select Create a new key encryption key on the key management server, and click Finish. **3.** Back up the KEK on the new KMS as specified in Backing up the encryption keys manually to a key management server (on page 48).

Appendix A: Encryption GUI reference

This chapter describes the Device Manager - Storage Navigator windows and dialog boxes for Encryption License Key.

Encryption Keys window

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



Number of Encryption Keys	Data Encryption Key	0
	Certificate Encryption Key	0
	PIN	0
	Free	0 (Max Allowed: 4096)

Selected: 0 of 0

1 / 1

□	Key ID	Created 1 ▾	Attribute	Assigned to	Generated on	Number of Backups

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

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

Encryption Keys tab

Use the Encryption Keys tab to view a list of the data encryption 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.

Item	Description
Restore Keys	Select From File to open the **Restore Keys from File** window. Select From Server to open the **Restore Keys from Server** window.
More Actions	Select Rekey Certificate Encryption Keys to display the **Rekey Certificate Encryption Keys** window. Select Rekey Key Encryption Keys to display the **Rekey Key Encryption Keys** window. Select Delete Keys from the list to delete a selected data encryption 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.

Edit Encryption Environmental Settings wizard

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

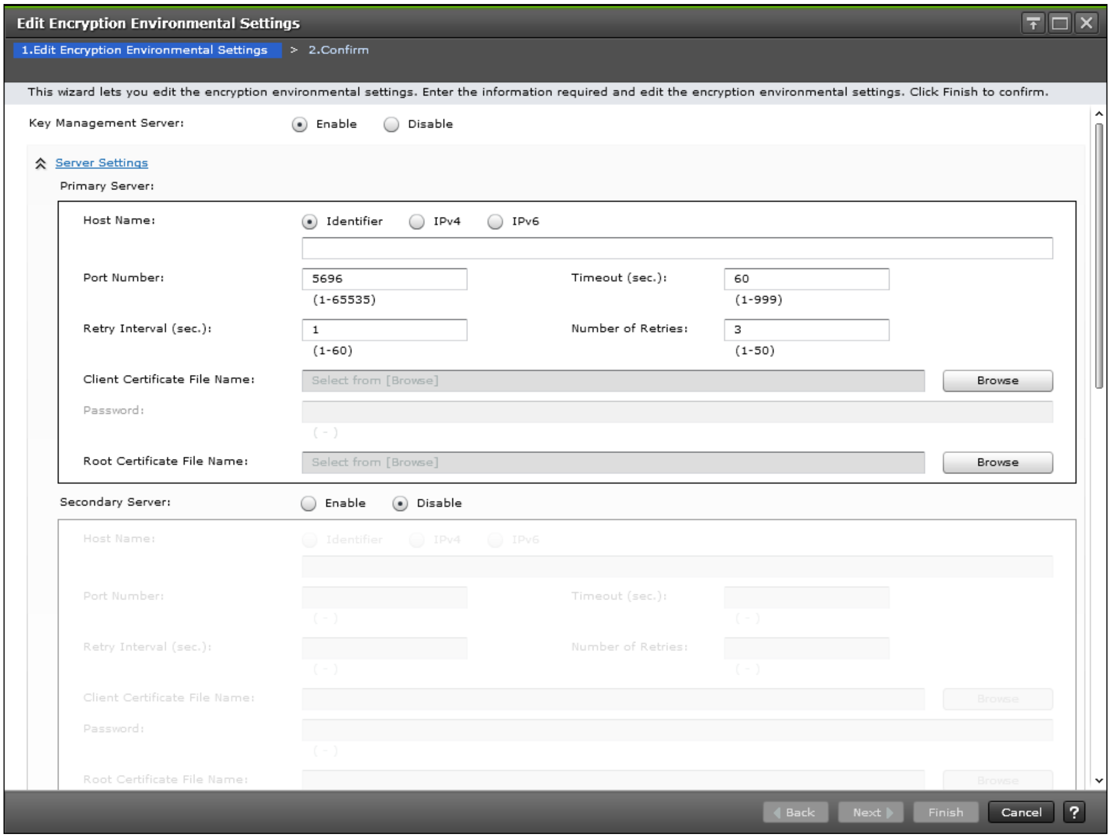
This wizard includes the following windows:

- **Edit Encryption Environmental Settings** window
- **Edit Encryption Environmental Settings** confirmation window

Edit Encryption Environmental Settings window

After the encryption environmental settings have been initialized during installation, the settings in the **Edit Encryption Environmental Settings** window can be changed only 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.
- When you need to change the regular backup schedule or the regular backup user.



Edit Encryption Environmental Settings

1.Edit Encryption Environmental Settings > 2.Confirm

This wizard lets you edit the encryption environmental settings. Enter the information required and edit the encryption environmental settings. Click Finish to confirm.

Key Management Server: ● Enable ○ Disable

Server Settings

Primary Server:

Host Name: ● Identifier ○ IPv4 ○ IPv6

Port Number: 5696 (1-65535) Timeout (sec.): 60 (1-999)

Retry Interval (sec.): 1 (1-60) Number of Retries: 3 (1-50)

Client Certificate File Name: Select from [Browse] Browse

Password: (-)

Root Certificate File Name: Select from [Browse] Browse

Secondary Server: ○ Enable ● Disable

Host Name: ○ Identifier ○ IPv4 ○ IPv6

Port Number: (-) Timeout (sec.): (-)

Retry Interval (sec.): (-) Number of Retries: (-)

Client Certificate File Name: Browse

Password: (-)

Root Certificate File Name: Browse

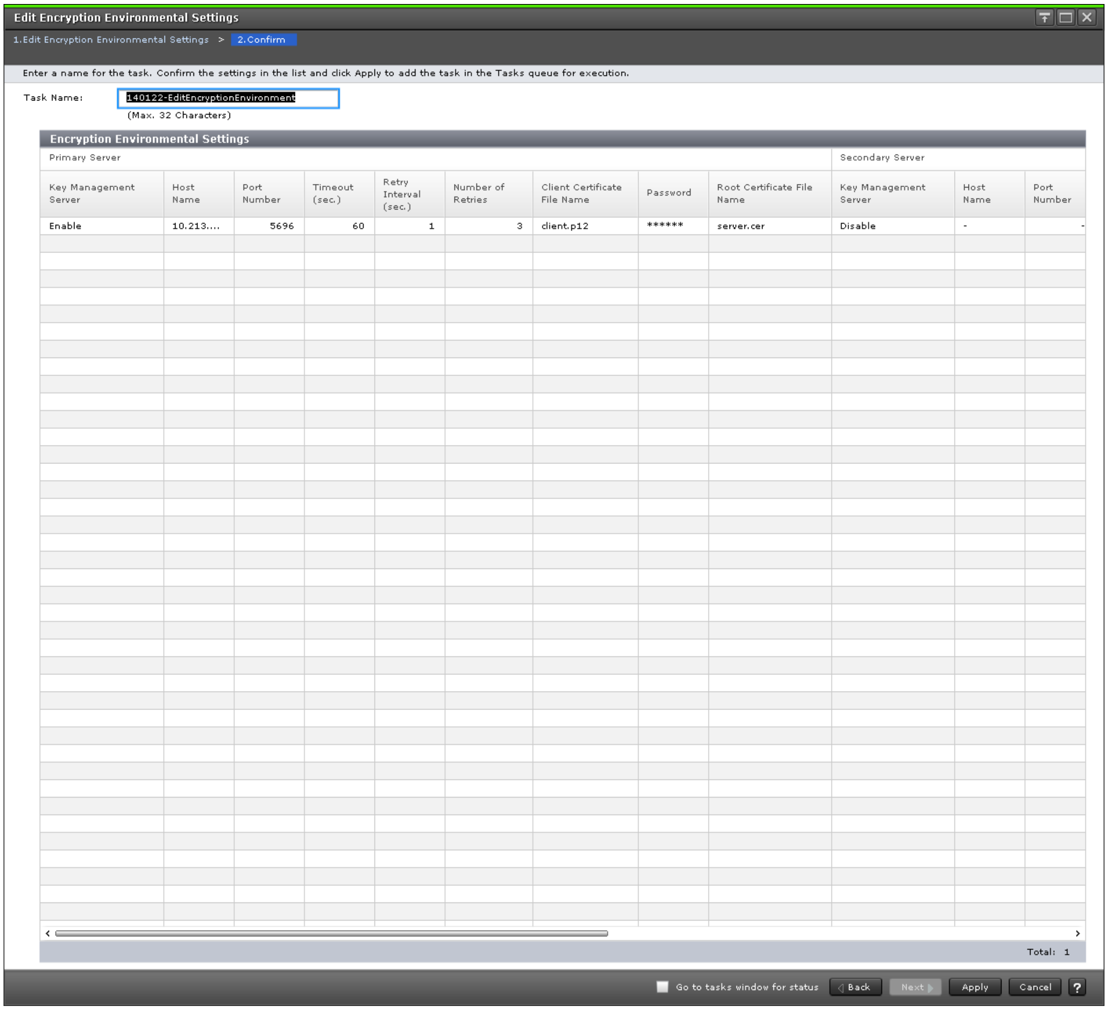
Item	Description
Key Management Server	Select whether to use a key management server. By default, no option is selected. ▪ Enable: Key management server is used. ▪ Disable: Key management server is not used.
Server Settings	When Enable is selected for Key Management Server, the following items are displayed: ▪ Primary server ▪ Secondary server ▪ Server Configuration Test

Item	Description
Primary Server	Specify the network connection information for the primary key management server. ▪ Host Name: Select the method used to identify the host, Identifier, IPv4, or IPv6, and then enter the information: • If you selected Identifier, enter the identifier for the host. • If you selected IPv4, enter the IPv4 address of the host. • If you selected IPv6, enter the IPv6 address of the host. ▪ Port Number: Enter the port number of the key management server (range = 1 to 65535, default = 5696). ▪ Timeout (sec.): Enter the time (in seconds) until the connection attempt to the key management server times out (range = 1 to 999, default = 60). ▪ Retry Interval (sec.): Enter the interval to retry the connection to the key management server (range = 1 to 60, default = 1). ▪ Number of Retries: Enter the number of times to retry the connection to the key management server (range = 1 to 50, default = 3). ▪ Client Certificate File Name: Enter the client certificate file for connecting to the key management server by clicking Browse and selecting the file. The form of the client certificate is PKCS#12. For details about the client certificate file, contact the server administrator or the network administrator. • Password: Enter the password for the client certificate. Number of characters: 0 to 128 Valid characters: numbers (0 to 9), upper case letters (A-Z), lower case letters (a-z), symbols: ! # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ ▪ Root Certificate File Name: Enter the root certificate file for connecting to the key management server by clicking Browse and selecting the file. The form of the root certificate is X.509. For details about the root certificate file, contact the server administrator or the network administrator.

Item	Description
Secondary Server	If you are using a secondary key management server, select Enable and then specify the network connection information for the secondary server: Host Name, Port Number, Timeout (sec.), Retry Interval (sec.), Number of Retries, Client Certificate File Name, Root Certificate File Name. **Note:** You must enable the Secondary Server if you want to select any of these settings: Protect the Key Encryption Key at the Key Management Server, Delete Internal Encryption Keys at PS OFF, or Disable local key generation.
Server Configuration Test	Select Check to start a network connection test for the key management server based on the specified settings. Result: Displays the result of the network connection test for the key management server.
Enable Encryption Key Regular Backup to Key Management Server	Select this option to enable regular encryption key backup operations on the key management server. This item cannot be selected if Disable is selected for Key Management Server. ▪ Regular Backup Time: Select the time, or times, for the regular backup operations. Check Select All to schedule hourly backups. ▪ Regular Backup User Name: Enter the user name of the regular backup user. ▪ Password: Enter the password of the regular backup user. **Caution:** If the user account of the regular backup user is deleted, you must enter a new regular backup user on this window. If not, regular backups will not be performed. If the user account of the regular backup user is edited (for example, changing the password or roles), you must re-enter the user name and password of the regular backup user on this window. If not, regular backups will not be performed.
Generate Encryption Keys on Key Management Server	Select this option if you want to create encryption keys on the key management server. **Note:** If you want to select Protect the Key Encryption Key at the Key Management Server, Delete Internal Encryption Keys at PS OFF, or Disable local key generation, you must select Generate Encryption Keys on Key Management Server.

Item	Description
Protect the Key Encryption Key at the Key Management Server	Select this option if you want to save the key encryption keys on the key management servers. **Note:** To enable this option, you must read the Warning and confirm the content of the warning by selecting **I agree**.
Delete Internal Encryption Keys at PS OFF	Select this option if you want to save the encryption keys in the key management server and delete the encryption keys in the storage system when the storage system is powered off. This option can be selected only when Enable is selected for Secondary Server and when the Protect the Key Encryption Key at the Key Management Server option is enabled. **Note:** To enable this option, you must read the Warning and confirm the content of the warning by selecting **I agree**.
Disable local key generation	Select this option if you want to create encryption keys only on the key management server and not on the storage system. This option can be selected only when Enable is selected for Secondary Server and when the Protect the Key Encryption Key at the Key Management Server option is enabled. **Note:** To enable this option, you must read the Warning and confirm the content of the warning by selecting **I agree**. **Caution:** If you enable this option and apply the setting to the storage system, you will not be able to undo this action or restore the settings.
Initialize Encryption Environmental Settings	Initializes the encryption environmental settings on the storage system.

Edit Encryption Environmental Settings confirmation window



Edit Encryption Environmental Settings
1.Edit Encryption Environmental Settings > 2.Confirm

Enter a name for the task. Confirm the settings in the list and click Apply to add the task in the Tasks queue for execution.

Task Name: 140122-EditEncryptionEnvironment
(Max. 32 Characters)

Encryption Environmental Settings

Primary Server									Secondary Server		
Key Management Server	Host Name	Port Number	Timeout (sec.)	Retry Interval (sec.)	Number of Retries	Client Certificate File Name	Password	Root Certificate File Name	Key Management Server	Host Name	Port Number
Enable	10.213....	5696	60	1	3	client.p12	******	server.cer	Disable	-	-

Total: 1

Item	Description
Primary Server	Displays the primary server information. ▪ Key Management Server: Shows whether the key management server is used Enable: The key management server is used Disable: The 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

Item	Description
	▪ 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, the same items display as for the primary server.
Enable Encryption Key Regular Backup to Key Management Server	▪ Yes: An encryption key is being regularly backed up. ▪ No: An encryption key is not being regularly backed up.
Regular Backup Time	Displays the times of day an encryption key is backed up.
Regular Backup User	Displays the name of the regular backup user.
Password	Displays six asterisks (******) for the password of the regular backup user.
Generate Encryption Keys on Key Management Server	Displays whether encryption keys are created on a key management server. ▪ 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. ▪ Yes: Encryption keys are created on a key management server. ▪ No: Encryption keys are not created on a key management server.
Delete Internal Encryption Keys at PS OFF	Indicates whether to save an encryption key to the key management server, and to delete the encryption key in the storage system when it is turned off:

Item	Description
	Yes: Saves the encryption key in the key management server, and deletes the encryption key in the storage system when it is turned off. No: The encryption key in the storage system is not deleted when it is turned off.
Disable local key generation	Displays whether encryption keys are created 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

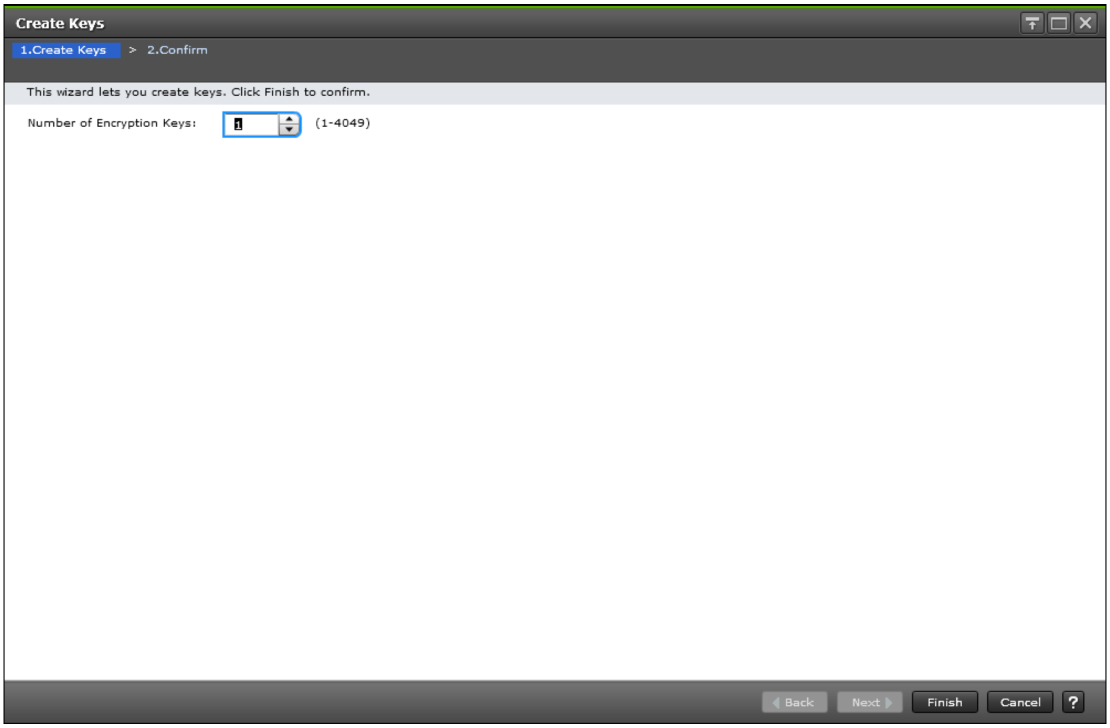
Use the Create Keys wizard to create keys and (optionally) back up the new keys to the key management server.

This wizard includes the following windows:

- **Create Keys** window
- **Create Keys** confirmation window

Create Keys window

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



Create Keys

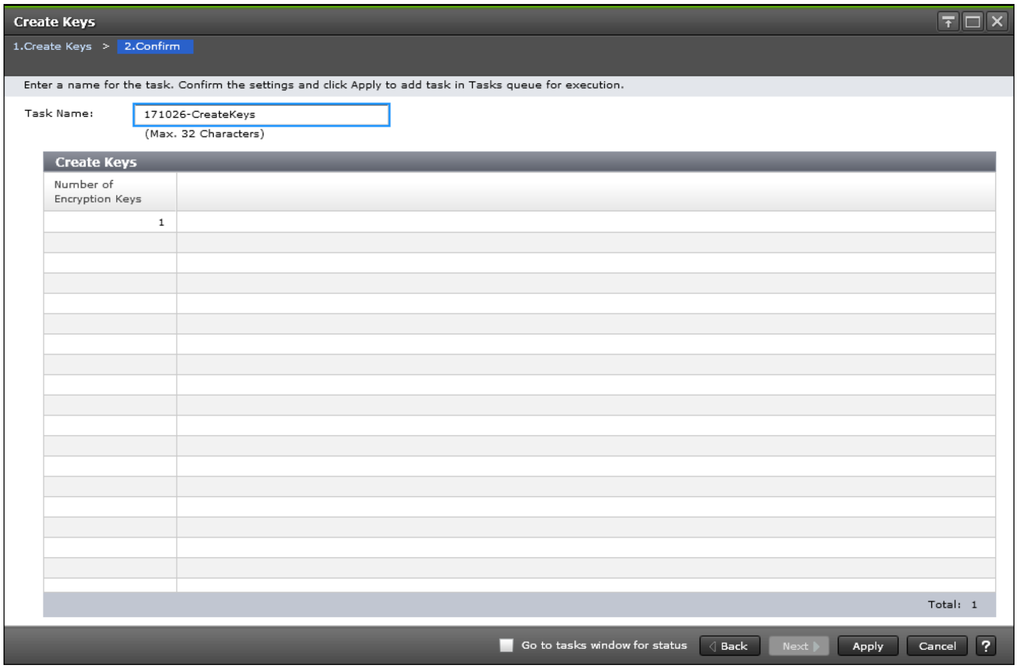
1.Create Keys > 2.Confirm

This wizard lets you create keys. Click Finish to confirm.

Number of Encryption Keys: 1 (1-4049)

Item	Description
Number of Encryption Keys	Enter the number of encryption keys to be created. The number you enter must be within the specified range. The range specified in parentheses (for example, 1-4049) indicates the number of keys that you can create. The maximum value in this range is obtained by subtracting the number of created encryption keys from the maximum number of keys (for example, 4096 - 47 = 4049).

Create Keys confirmation window



Enter a name for the task. Confirm the settings and click Apply to add task in Tasks queue for execution.

Task Name: 171026-CreateKeys
(Max. 32 Characters)

Create Keys

Number of Encryption Keys
1

Total: 1

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

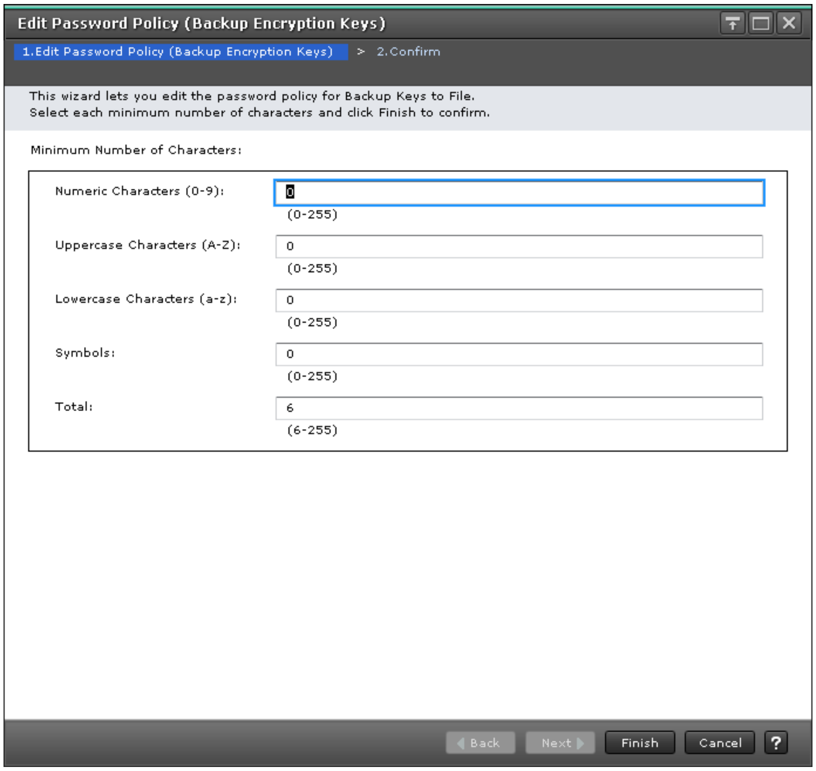
Edit Password Policy (Backup Encryption Keys) wizard

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



Edit Password Policy (Backup Encryption Keys)
1.Edit Password Policy (Backup Encryption Keys) > 2.Confirm

This wizard lets you edit the password policy for Backup Keys to File.
Select each minimum number of characters and click Finish to confirm.

Minimum Number of Characters:

Numeric Characters (0-9): 0 (0-255)

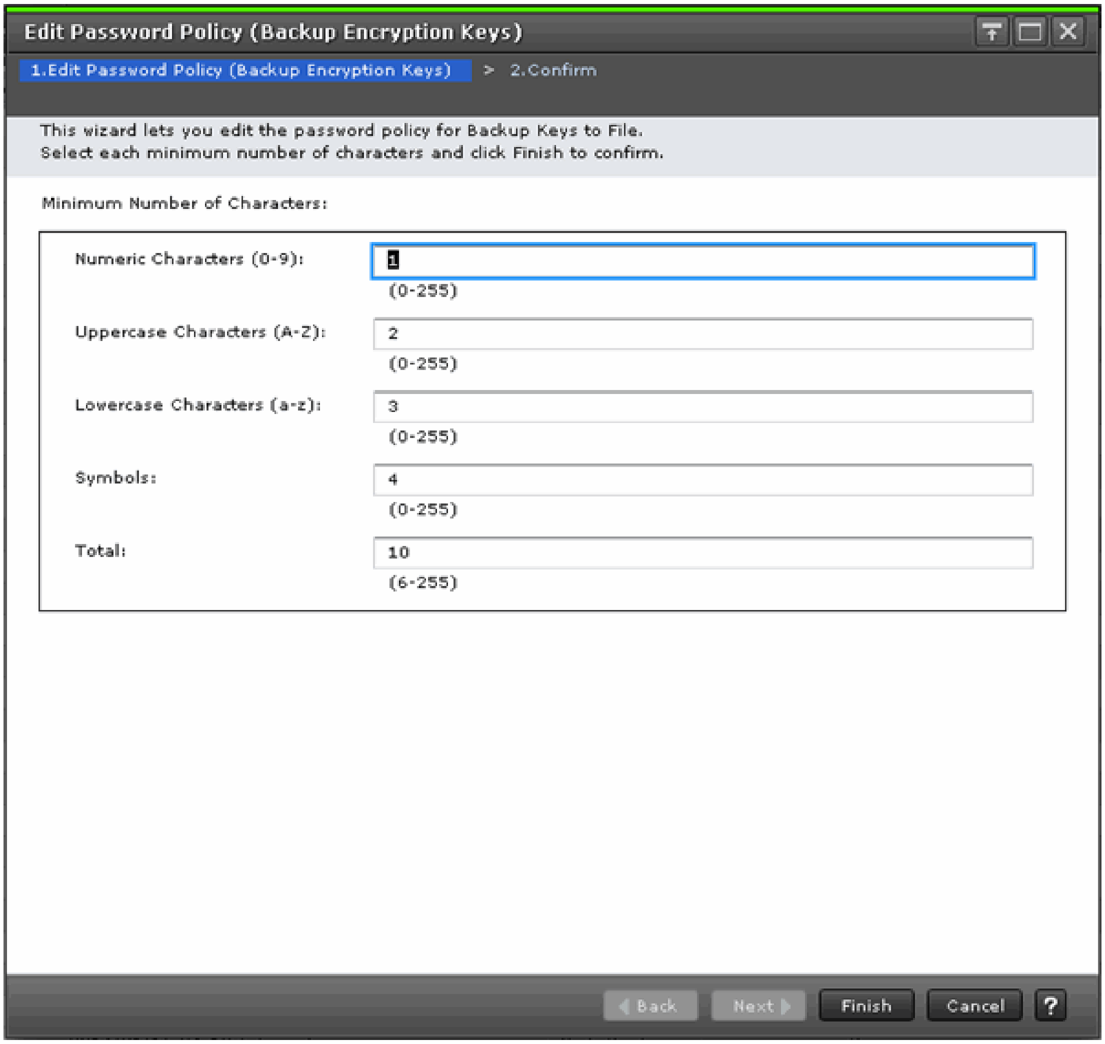
Uppercase Characters (A-Z): 0 (0-255)

Lowercase Characters (a-z): 0 (0-255)

Symbols: 0 (0-255)

Total: 6 (6-255)

◀ Back
Next ▶
Finish
Cancel
?



Edit Password Policy (Backup Encryption Keys)
1.Edit Password Policy (Backup Encryption Keys)
> 2.Confirm

This wizard lets you edit the password policy for Backup Keys to File.
Select each minimum number of characters and click Finish to confirm.

Minimum Number of Characters:

Numeric Characters (0-9):	1	(0-255)
Uppercase Characters (A-Z):	2	(0-255)
Lowercase Characters (a-z):	3	(0-255)
Symbols:	4	(0-255)
Total:	10	(6-255)

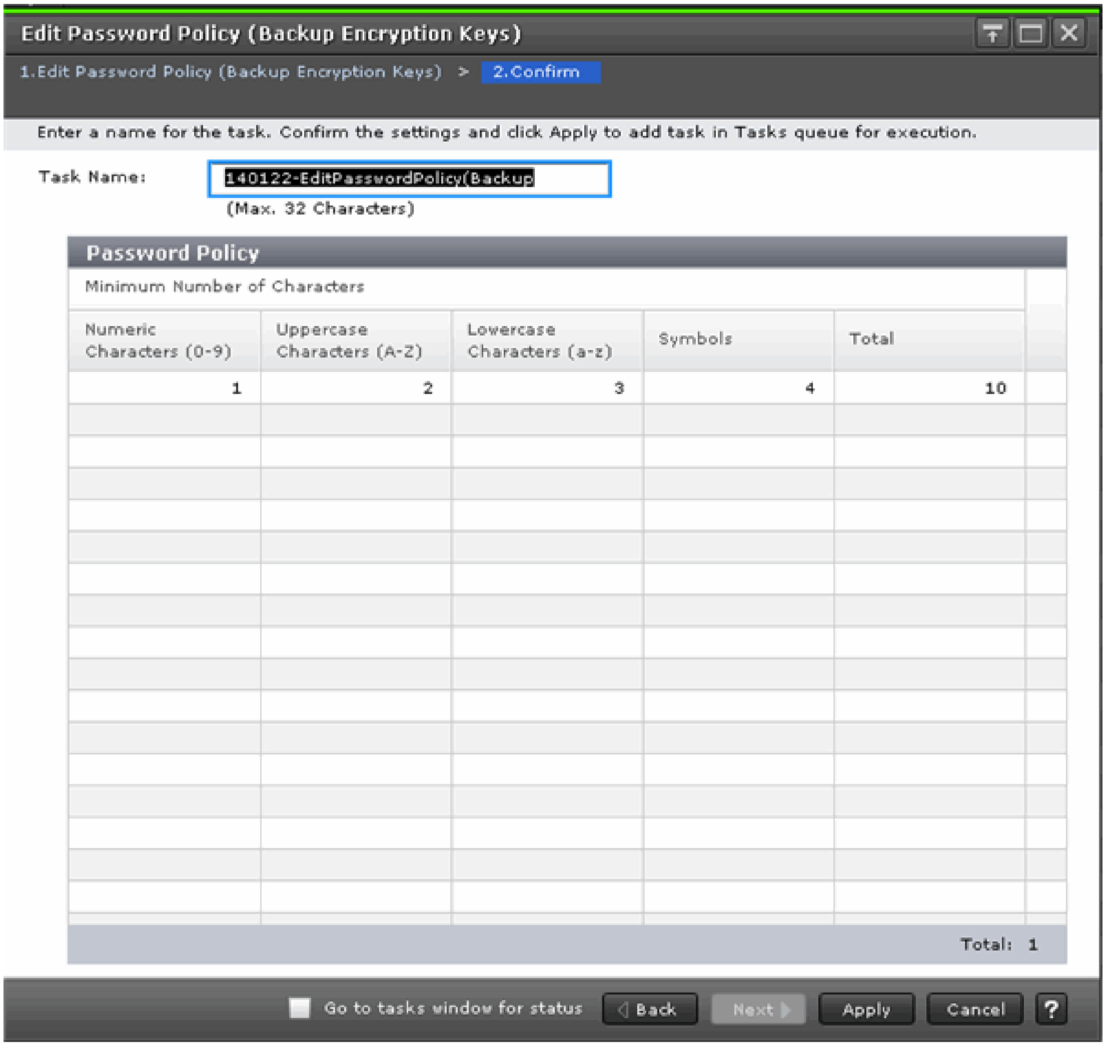
◀ Back
Next ▶
Finish
Cancel
?

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

Item	Description
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.



Edit Password Policy (Backup Encryption Keys)

1.Edit Password Policy (Backup Encryption Keys) > 2.Confirm

Enter a name for the task. Confirm the settings and click Apply to add task in Tasks queue for execution.

Task Name: 140122-EditPasswordPolicy(Backup

(Max. 32 Characters)

Password Policy

Minimum Number of Characters

Numeric Characters (0-9)	Uppercase Characters (A-Z)	Lowercase Characters (a-z)	Symbols	Total
1	2	3	4	10

Total: 1

□ Go to tasks window for status
Back
Next
Apply
Cancel
?

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 HDvM - SN computer.

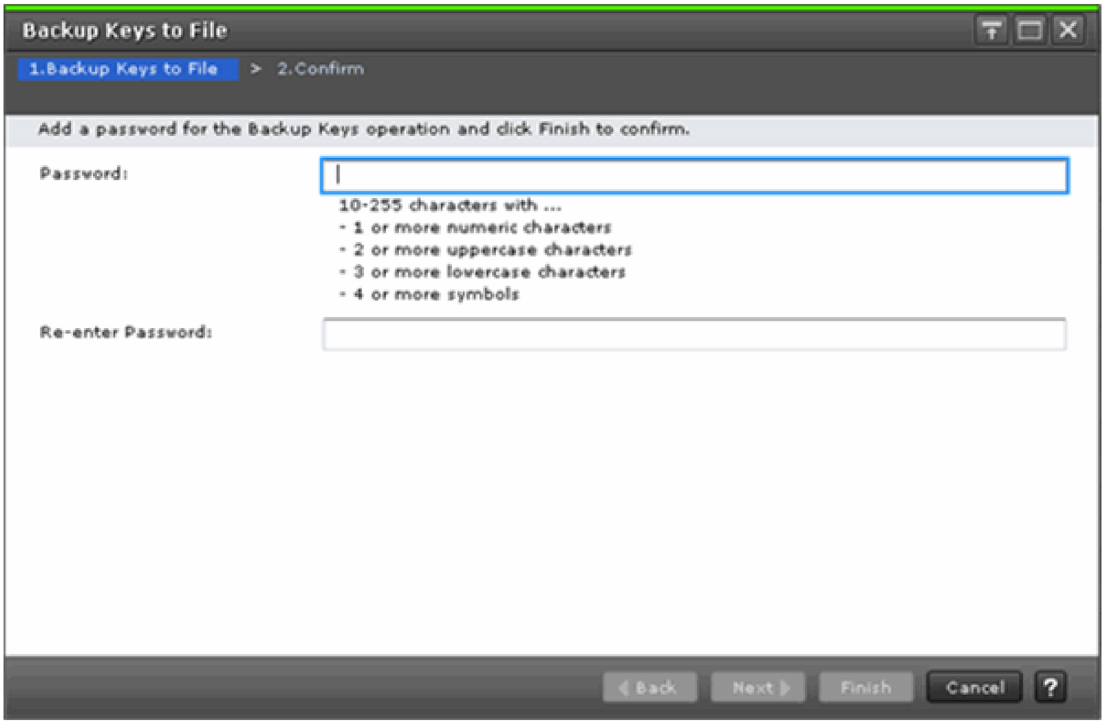
This wizard includes the following windows:

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

Backup Keys to File window

The appearance of this window depends on whether the password policy for backup encryption keys has been edited using the **Edit Password Policy (Backup Encryption Keys)** window.

When the backup encryption key password policy has been edited, the window displays the user-specified password requirements, for example:



Backup Keys to File

1.Backup Keys to File > 2.Confirm

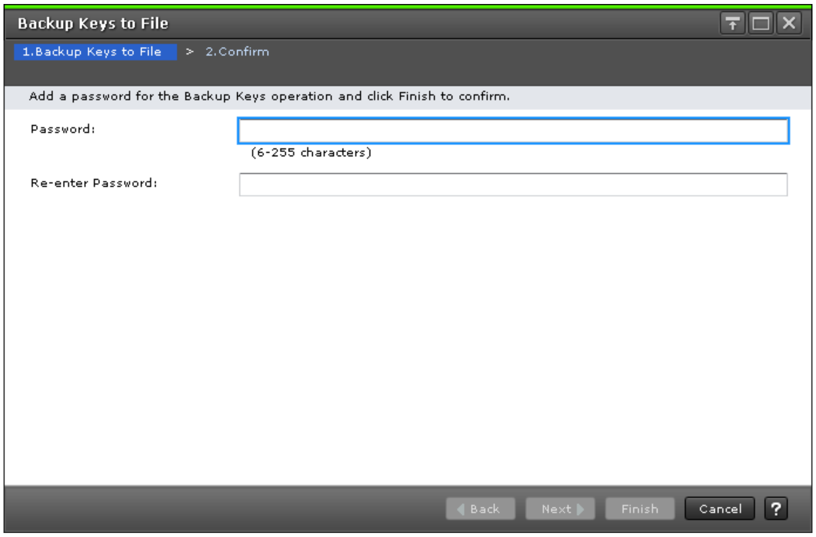
Add a password for the Backup Keys operation and click Finish to confirm.

Password:

10-255 characters with ...
- 1 or more numeric characters
- 2 or more uppercase characters
- 3 or more lowercase characters
- 4 or more symbols

Re-enter Password:

When the backup encryption key password policy has not been edited, the window displays the default password requirements:



Backup Keys to File

1.Backup Keys to File > 2.Confirm

Add a password for the Backup Keys operation and click Finish to confirm.

Password:

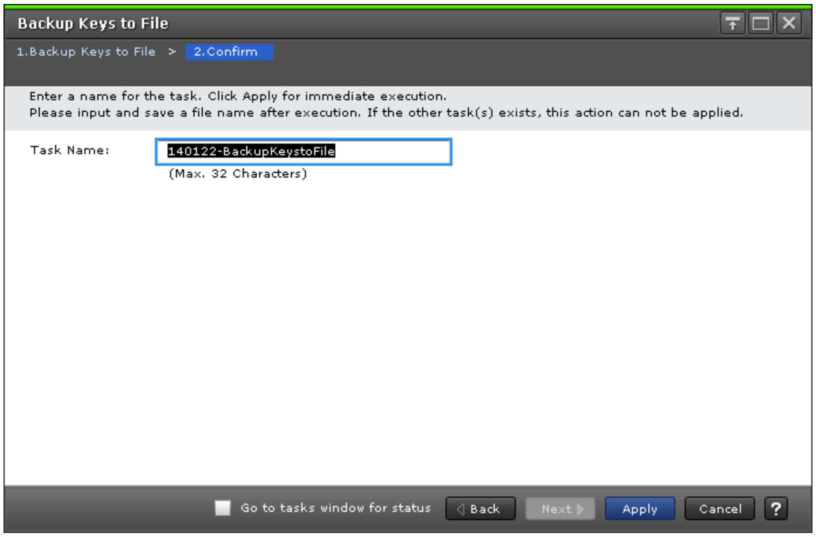
(6-255 characters)

Re-enter Password:

Item	Description
Password	Password for the backup data encryption key. Character limits: 6 to 255

Item	Description
	Valid characters: ▪ Numbers (0 to 9) ▪ Upper case (A-Z) ▪ Lower case (a-z) ▪ Symbols: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ **Note:** When the backup encryption key password policy has been edited, the window displays the user-specified password requirements.
Re-enter Password	Type the password again for confirmation.

Backup Keys to File confirmation window


Backup Keys to File
1.Backup Keys to File > 2.Confirm
Go to tasks window for status
Back
Next
Apply
Cancel
?

Enter a name for the task. Click Apply for immediate execution.
Please input and save a file name after execution. If the other task(s) exists, this action can not be applied.

Task Name: 140122-BackupKeystoFile
(Max. 32 Characters)

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.

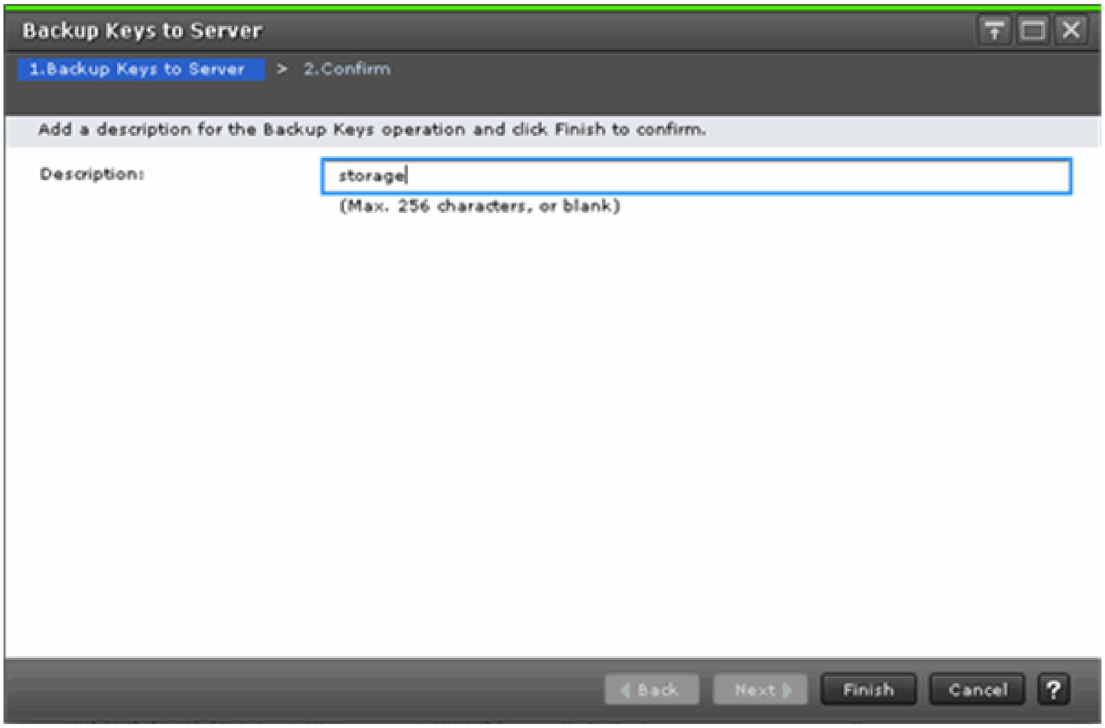
Backup Keys to Server wizard

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



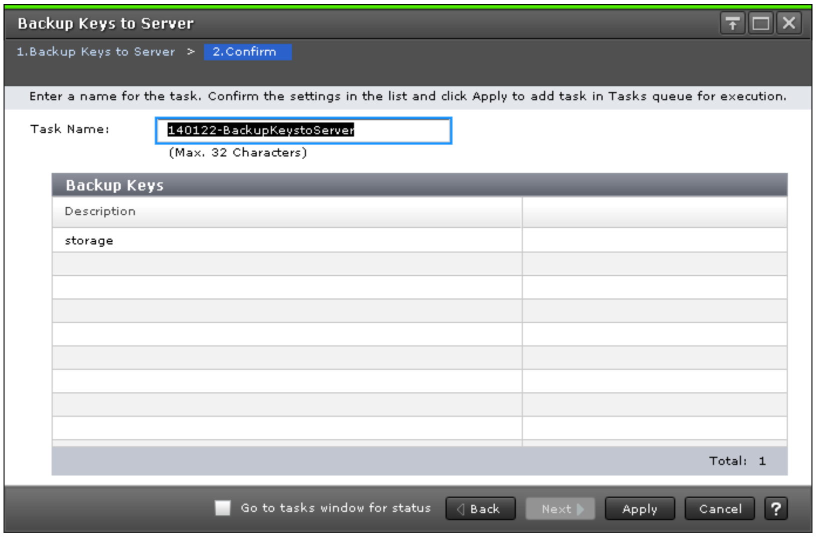
Add a description for the Backup Keys operation and click Finish to confirm.

Description: storage

(Max. 256 characters, or blank)

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

Backup Keys to Server confirmation window



Backup Keys to Server
1.Backup Keys to Server > 2.Confirm

Enter a name for the task. Confirm the settings in the list and click Apply to add task in Tasks queue for execution.

Task Name: 140122-BackupKeystoServer

(Max. 32 Characters)

Backup Keys

Description	
storage	

Total: 1

□ Go to tasks window for status
Back
Next
Apply
Cancel
?

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

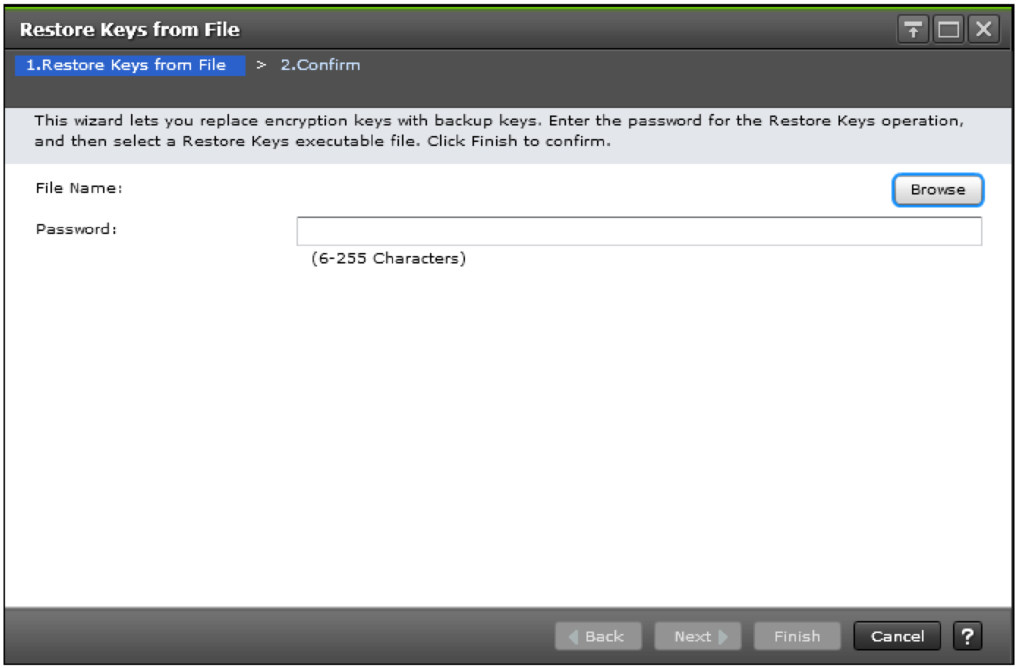
Restore Keys from File wizard

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

This wizard includes the following windows:

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

Restore Keys from File window



This wizard lets you replace encryption keys with backup keys. Enter the password for the Restore Keys operation, and then select a Restore Keys executable file. Click Finish to confirm.

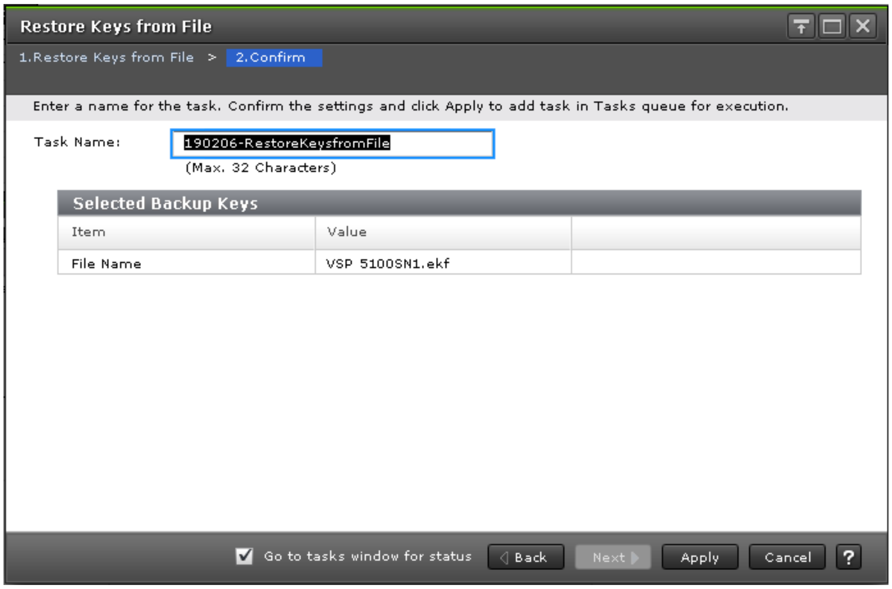
File Name:

Password:

(6-255 Characters)

Item	Description
File Name	File name of the selected backup file
Browse	Select the backup file (.ekf). The name of the selected file is displayed in File Name.
Password	Password that you typed when you backed up the encryption key

Restore Keys from File confirmation window



Enter a name for the task. Confirm the settings and click Apply to add task in Tasks queue for execution.

Task Name: 190206-RestoreKeysfromFile
(Max. 32 Characters)

Selected Backup Keys

Item	Value
File Name	VSP 5100SN1.ekf

☑ Go to tasks window for status

Item	Description
Item	File name
Value	File name of the encryption key to restore

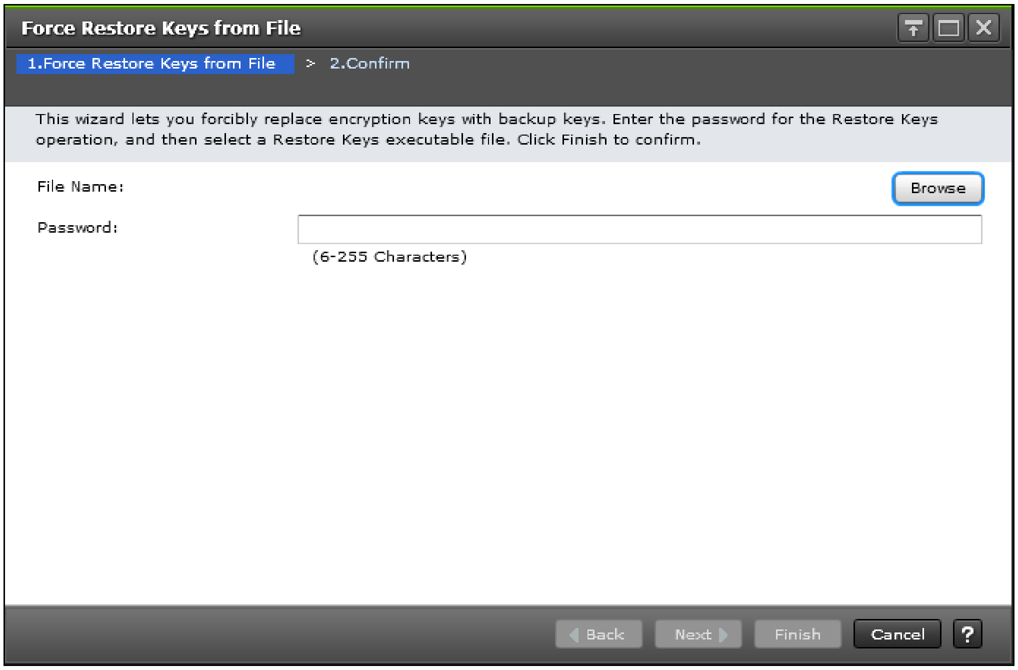
Force Restore Keys from File wizard

Use the **Force Restore Keys from File** wizard to forcibly restore encryption keys from a file you backed up on the Device Manager - Storage Navigator computer.

This wizard includes the following windows:

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

Force Restore Keys from File window

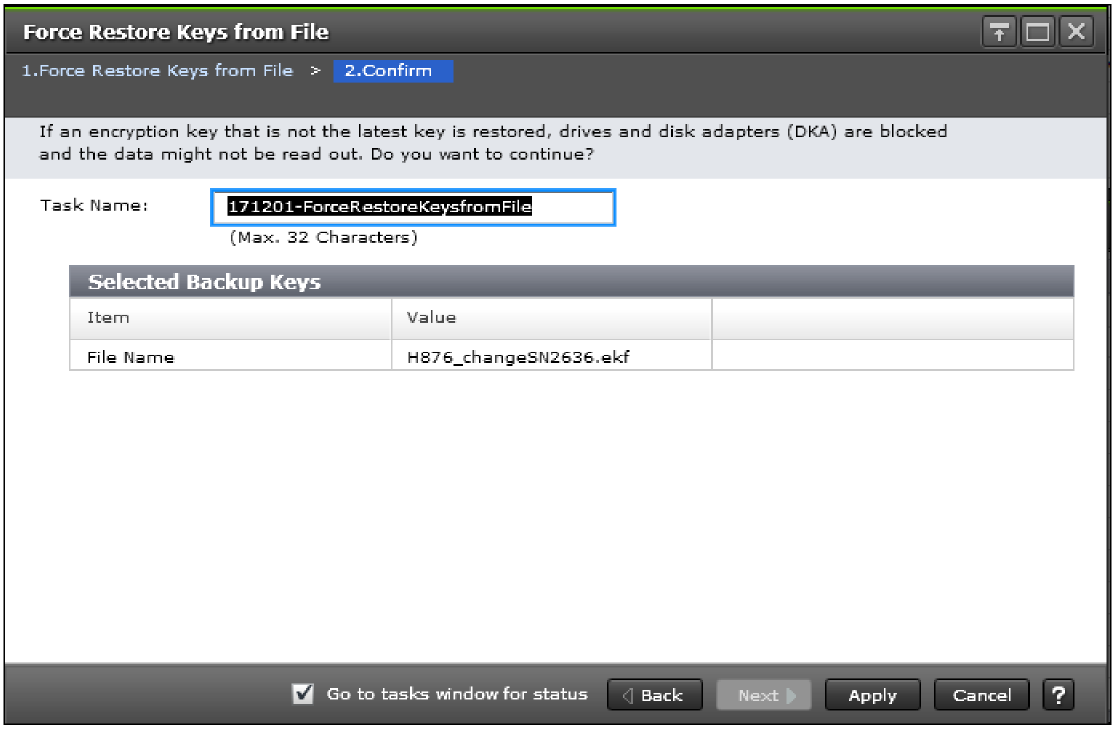


This wizard lets you forcibly replace encryption keys with backup keys. Enter the password for the Restore Keys operation, and then select a Restore Keys executable file. Click Finish to confirm.

(6-255 Characters)

Item	Description
File Name	File name of the selected backup file
Browse	Select the backup file (.ekf). The name of the selected file is displayed in File Name.
Password	Password that you typed when you backed up the encryption key

Force Restore Keys from File confirmation window


Force Restore Keys from File
1.Force Restore Keys from File > 2.Confirm
☑ Go to tasks window for status
Back
Next
Apply
Cancel
?

If an encryption key that is not the latest key is restored, drives and disk adapters (DKA) are blocked and the data might not be read out. Do you want to continue?

Task Name: 171201-ForceRestoreKeysfromFile

(Max. 32 Characters)

Selected Backup Keys

Item	Value	
File Name	H876_changeSN2636.ekf	

Item	Description
Item	File name
Value	File name of the encryption key to restore

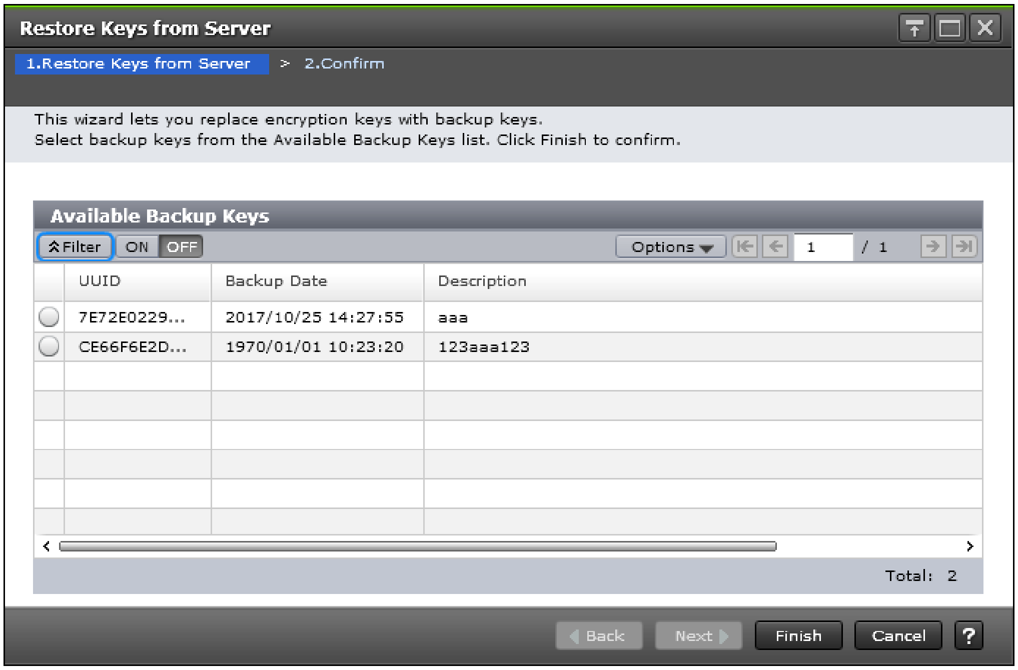
Restore Keys from Server wizard

Use the Restore Keys from Server wizard to restore 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



Restore Keys from Server

1.Restore Keys from Server > 2.Confirm

This wizard lets you replace encryption keys with backup keys.
Select backup keys from the Available Backup Keys list. Click Finish to confirm.

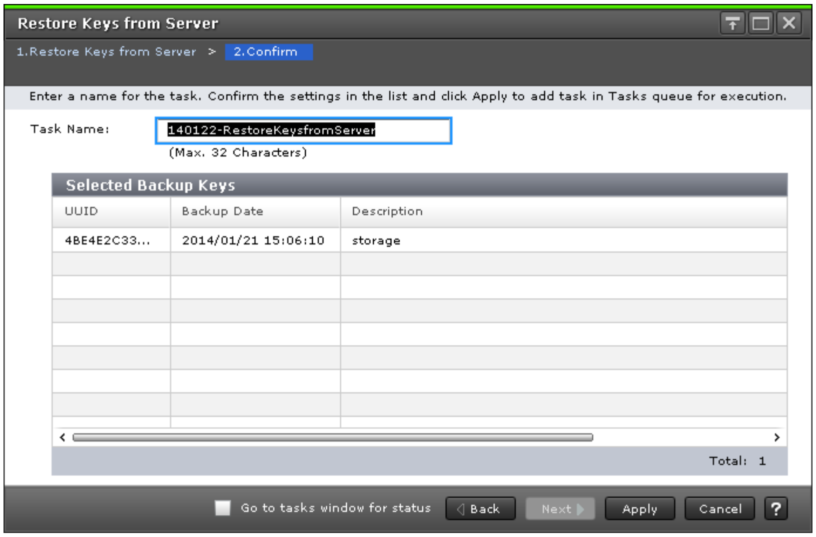
Available Backup Keys

	UUID	Backup Date	Description
○	7E72E0229...	2017/10/25 14:27:55	aaa
○	CE66F6E2D...	1970/01/01 10:23:20	123aaa123

Total: 2

Item	Description
UUID	Displays the UUID of the encryption key backed up on the key management server.
Backup Date	Displays the time the encryption key was backed up on the key management server.
Description	Displays the description defined when the encryption key was backed up on the key management server. The encryption key for a regular backup is displayed in the following format: `AutoBackup_[backed-up-year-month-date_backed-up-time]`

Restore Keys from Server confirmation window


Restore Keys from Server
1.Restore Keys from Server > 2.Confirm

Enter a name for the task. Confirm the settings in the list and click Apply to add task in Tasks queue for execution.

Task Name: 140122-RestoreKeysfromServer
(Max. 32 Characters)

Selected Backup Keys

UUID	Backup Date	Description
4BE4E2C33...	2014/01/21 15:06:10	storage

Total: 1

□ Go to tasks window for status
Back
Next
Apply
Cancel
?

Item	Description
UUID	Displays the UUID of the encryption key backed up on the key management server.
Backup Date	Displays the time when the encryption key was backed up on the key management server.
Description	Displays the description defined when the encryption key was backed up on the key management server. The encryption key for a regular backup is displayed in the following format: `AutoBackup_[backup-year-month-date_backup-time]`

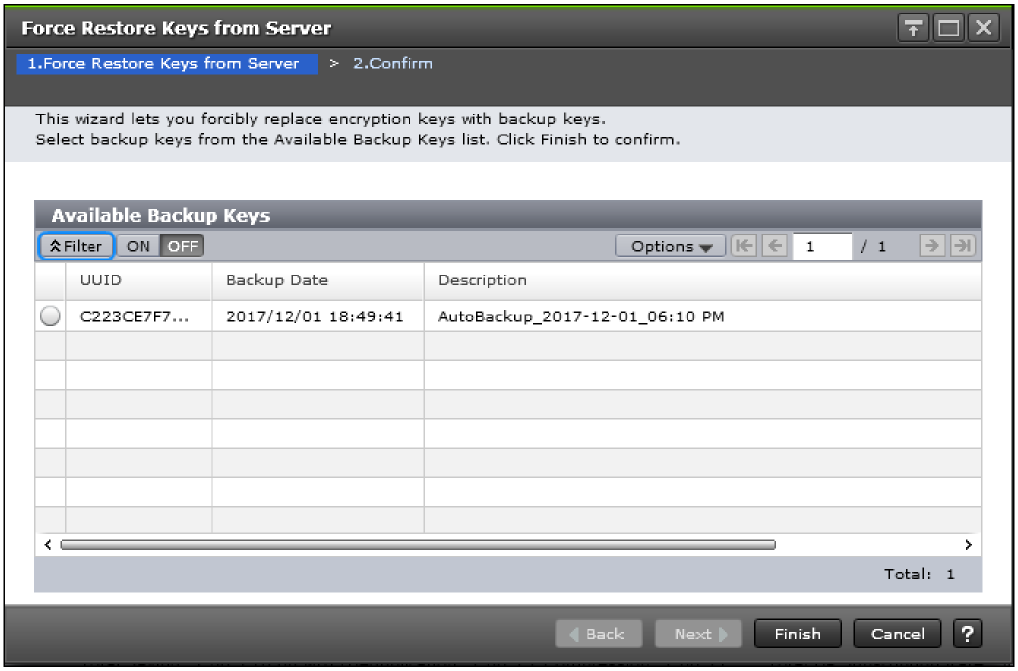
Force Restore Keys from Server wizard

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

This wizard includes the following windows:

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

Force Restore Keys from Server window



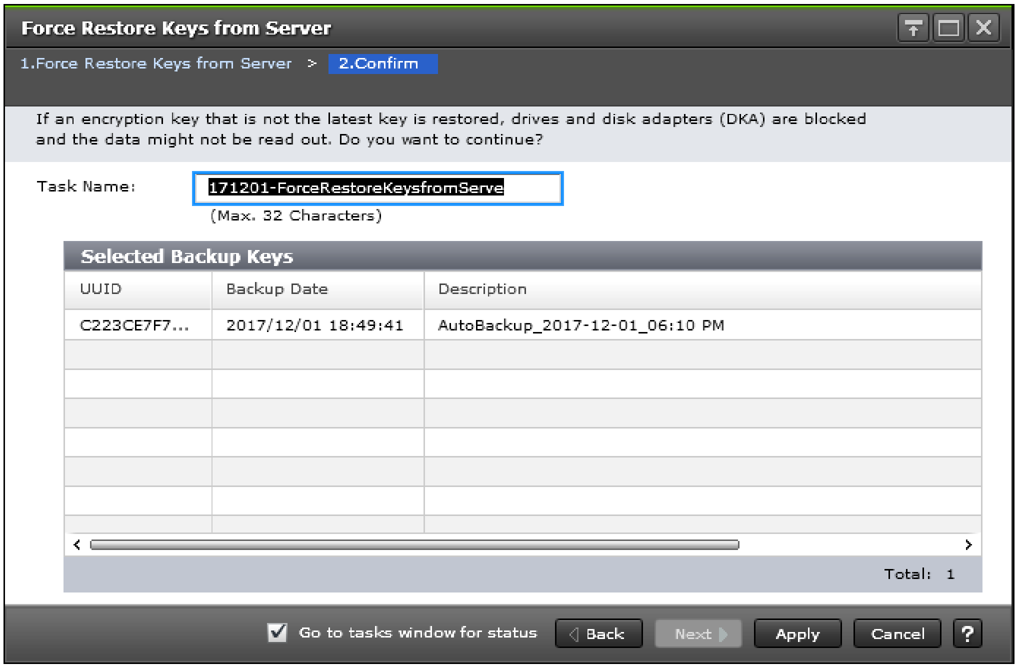
This wizard lets you forcibly replace encryption keys with backup keys.
Select backup keys from the Available Backup Keys list. Click Finish to confirm.

	UUID	Backup Date	Description
○	C223CE7F7...	2017/12/01 18:49:41	AutoBackup_2017-12-01_06:10 PM

Total: 1

Item	Description
UUID	UUID of the encryption key that is backed up on the key management server.
Backup Date	Date and time when the encryption key was backed up on the key management server.
Description	Description that was defined when the encryption key was backed up on the key management server. The encryption key for a regular backup is displayed in the following format: `AutoBackup_`*`[backup-year-month-date_backup-time]`*

Force Restore Keys from Server confirmation window


Force Restore Keys from Server
1.Force Restore Keys from Server > 2.Confirm
Back
Next
Apply
Cancel
?

If an encryption key that is not the latest key is restored, drives and disk adapters (DKA) are blocked and the data might not be read out. Do you want to continue?

Task Name: 171201-ForceRestoreKeysfromServe

(Max. 32 Characters)

Selected Backup Keys

UUID	Backup Date	Description
C223CE7F7...	2017/12/01 18:49:41	AutoBackup_2017-12-01_06:10 PM

Total: 1

☑ Go to tasks window for status

Item	Description
UUID	UUID of the encryption key that is backed up on the key management server
Backup Date	Date and time when the encryption key was backed up on the key management server
Description	Description that was defined when the encryption key was backed up on the key management server. The encryption key for a regular backup is displayed in the following format: `AutoBackup_[backup-year-month-date_backup-time]`

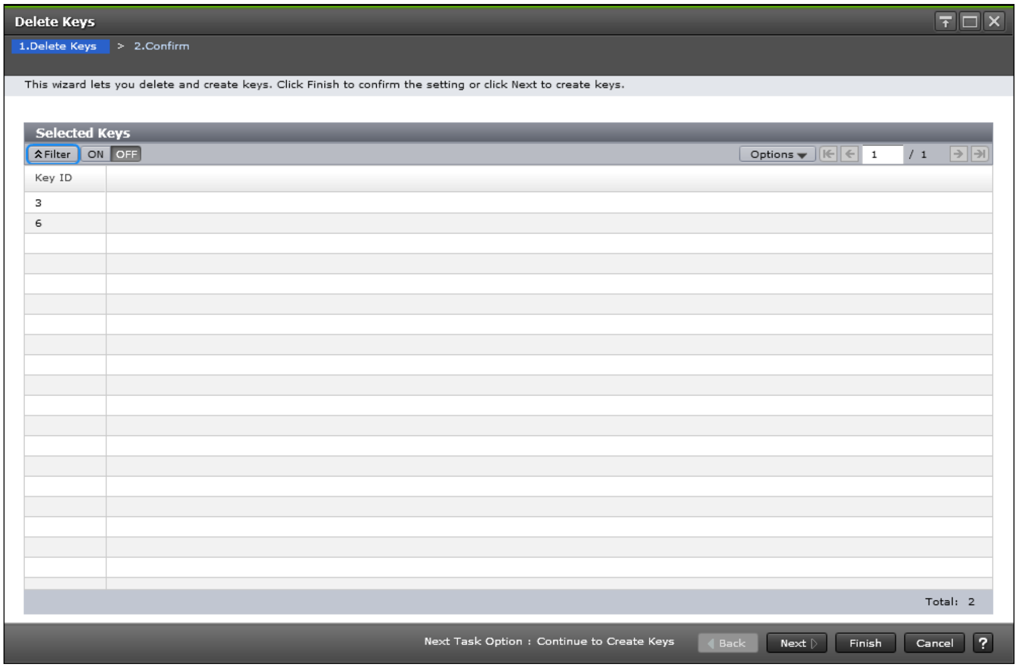
Delete Keys wizard

Use the Delete Keys wizard to delete encryption keys.

This wizard includes the following windows:

- **Delete Keys** window
- **Delete Keys** confirmation window

Delete Keys window



This wizard lets you delete and create keys. Click Finish to confirm the setting or click Next to create keys.

Selected Keys

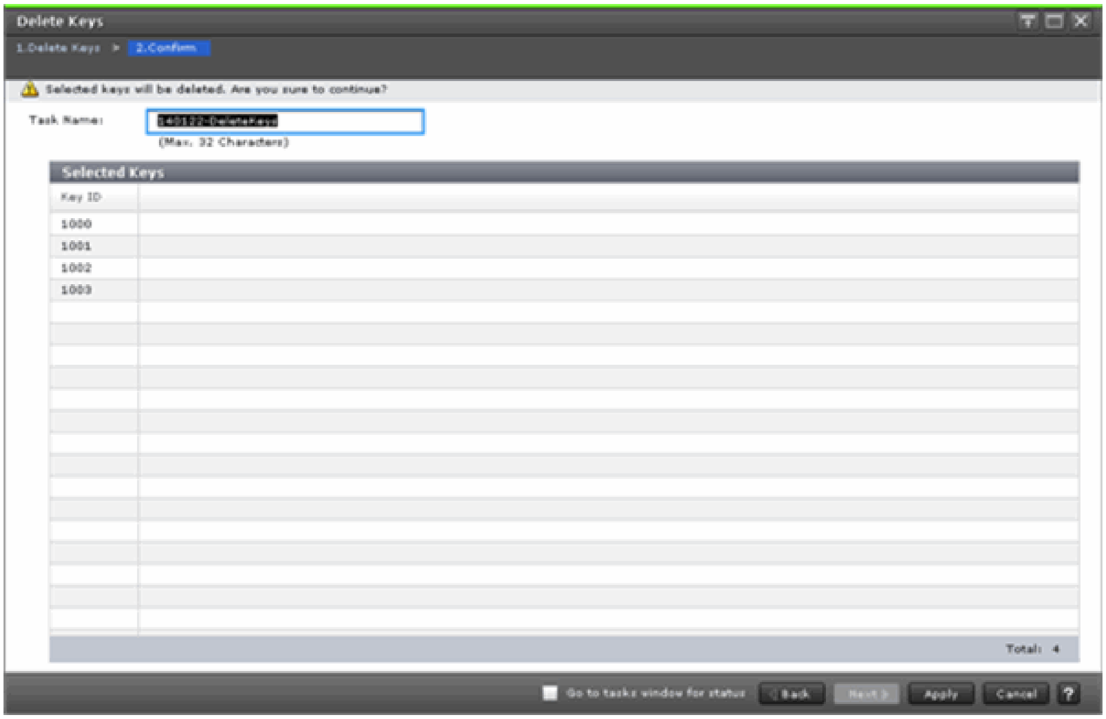
Key ID
3
6

Total: 2

Next Task Option : Continue to Create Keys

Item	Description
Key ID	IDs of data encryption keys

Delete Keys confirmation window



Selected keys will be deleted. Are you sure to continue?

Task Name: 140122-DeleteKeys
(Max. 32 Characters)

Selected Keys

Key ID
1000
1001
1002
1003

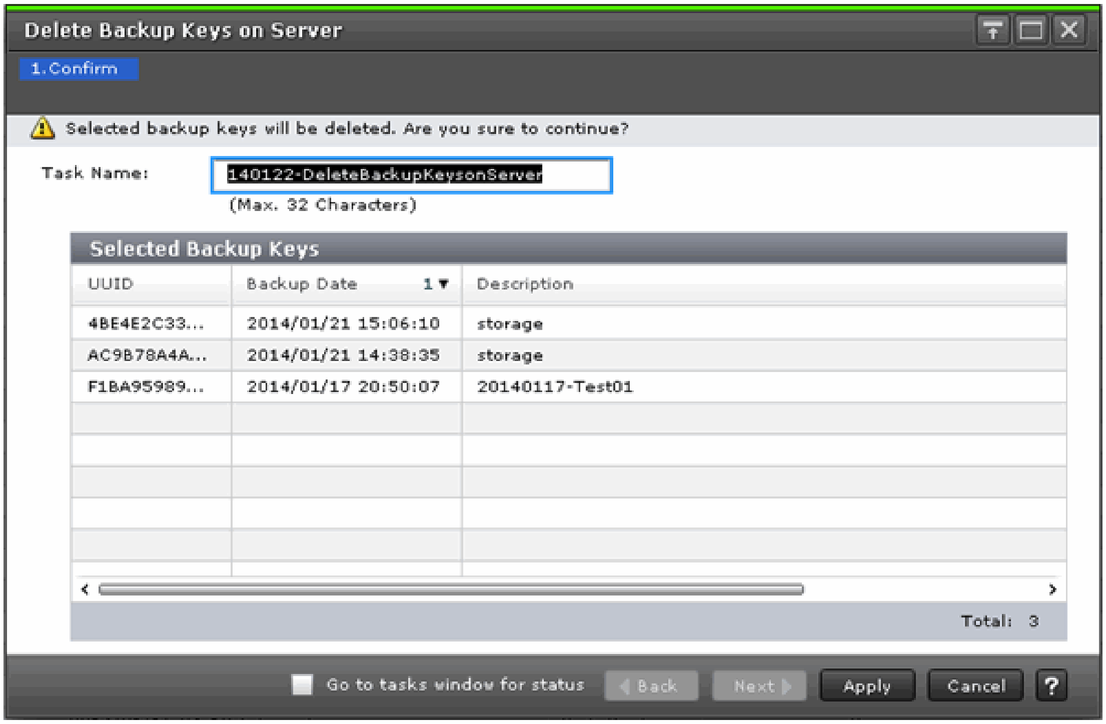
Total: 4

□ Go to tasks window for status

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 delete backup keys on the key management server.



⚠ Selected backup keys will be deleted. Are you sure to continue?

Task Name: 140122-DeleteBackupKeysonServer

(Max. 32 Characters)

Selected Backup Keys

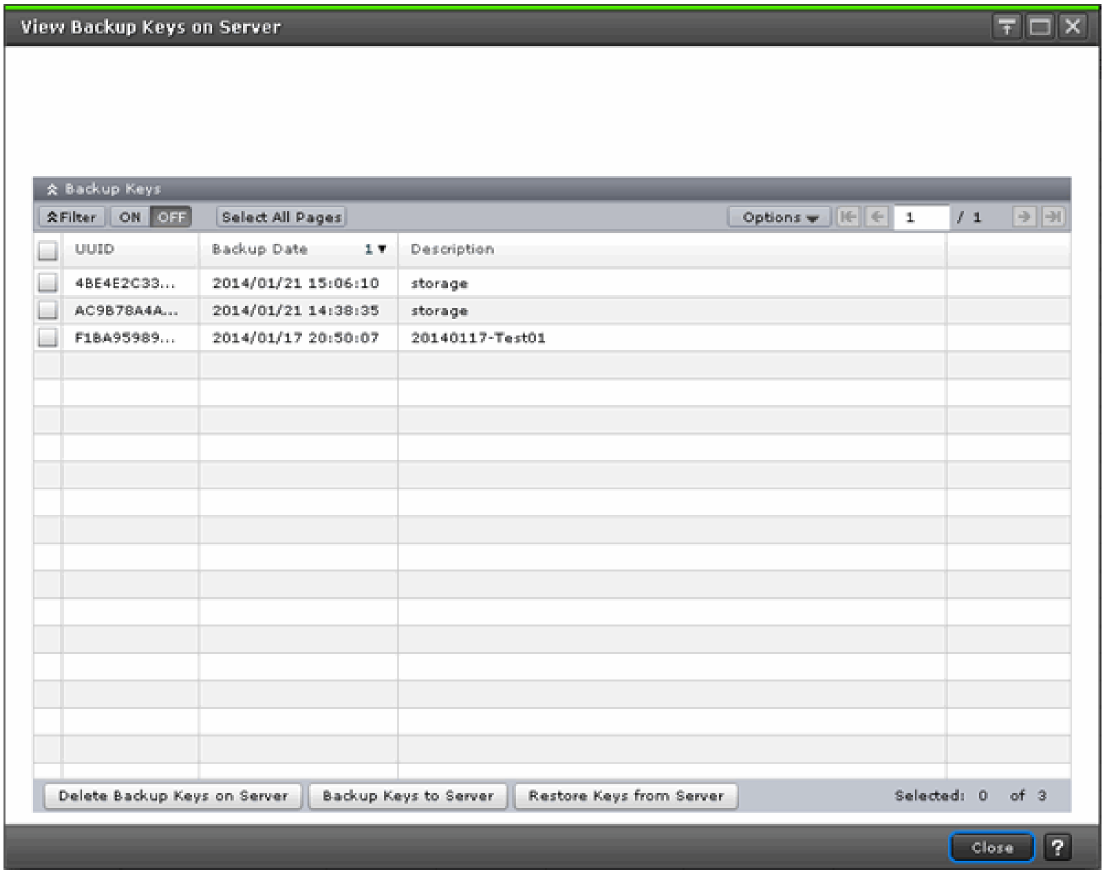
UUID	Backup Date 1▼	Description
4BE4E2C33...	2014/01/21 15:06:10	storage
AC9B78A4A...	2014/01/21 14:38:35	storage
F1BA95989...	2014/01/17 20:50:07	20140117-Test01

Total: 3

Item	Description
UUID	Displays the UUID of the encryption key backed up on the key management server
Backup Date	Displays the date and time when the encryption key was backed up on the key management server
Description	Displays the description entered when the encryption key was backed up on the key management server. The encryption key for a regular backup is displayed in the following format: `AutoBackup_`*`[backup-year-month-date_backup-time]`*

View Backup Keys on Server window

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



□	UUID	Backup Date 1▼	Description
□	4BE4E2C33...	2014/01/21 15:06:10	storage
□	AC9B78A4A...	2014/01/21 14:38:35	storage
□	F18A95989...	2014/01/17 20:50:07	20140117-Test01

Selected: 0 of 3

Backup Keys table

Item	Description
UUID	Displays the UUID of the backup encryption key on the key management server.
Backup Date	Displays the time the encryption key was backed up on the key management server.
Description	Displays the description defined when the encryption key was backed up on the key management server. The encryption key for a regular backup is displayed in the following format: `AutoBackup_[`*`backup-year-month-date_backup-time`*`]`

Item	Description
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

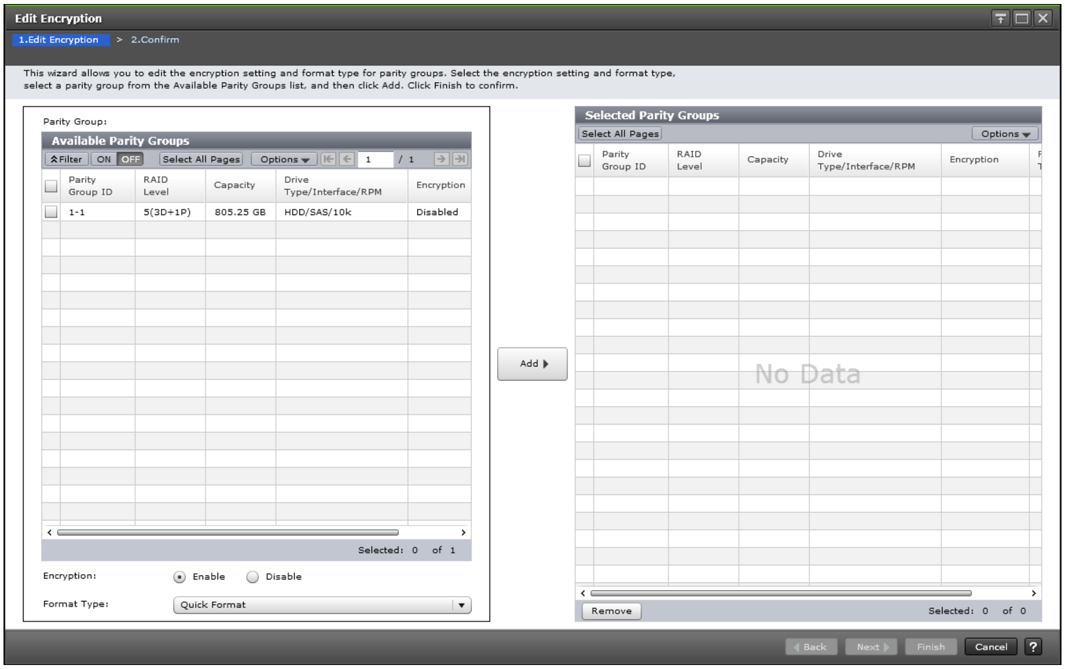
Use the Edit Encryption wizard to do the following:

- 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



Edit Encryption

1.Edit Encryption > 2.Confirm

This wizard allows you to edit the encryption setting and format type for parity groups. Select the encryption setting and format type, select a parity group from the Available Parity Groups list, and then click Add. Click Finish to confirm.

Parity Group:

Available Parity Groups

□	Parity Group ID	RAID Level	Capacity	Drive Type/Interface/RPM	Encryption
□	1-1	5(3D+1P)	805.25 GB	HDD/SAS/10k	Disabled

Selected: 0 of 1

Encryption: ● Enable ○ Disable

Format Type: Quick Format

Selected Parity Groups

□	Parity Group ID	RAID Level	Capacity	Drive Type/Interface/RPM	Encryption

No Data

Selected: 0 of 0

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	Displays the parity group ID.
RAID Level	Displays 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	Displays the total capacity (unit) of the parity group.
Drive Type/Interface/RPM	Displays the type of drives in the parity group: ▪ Drive type (for example, HDD, SSD, FMD) ▪ Interface (for example, SAS, NVMe) ▪ RPM (for example, 7.2k, 10k)
Encryption	Displays the encryption setting for the parity group: ▪ Enabled: Encryption is enabled. ▪ Disabled: Encryption is disabled. If accelerated compression is enabled on the parity group, do not select Enable for Encryption. If you do, an error will occur when you perform the task.
Format Type	Select the format type 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.

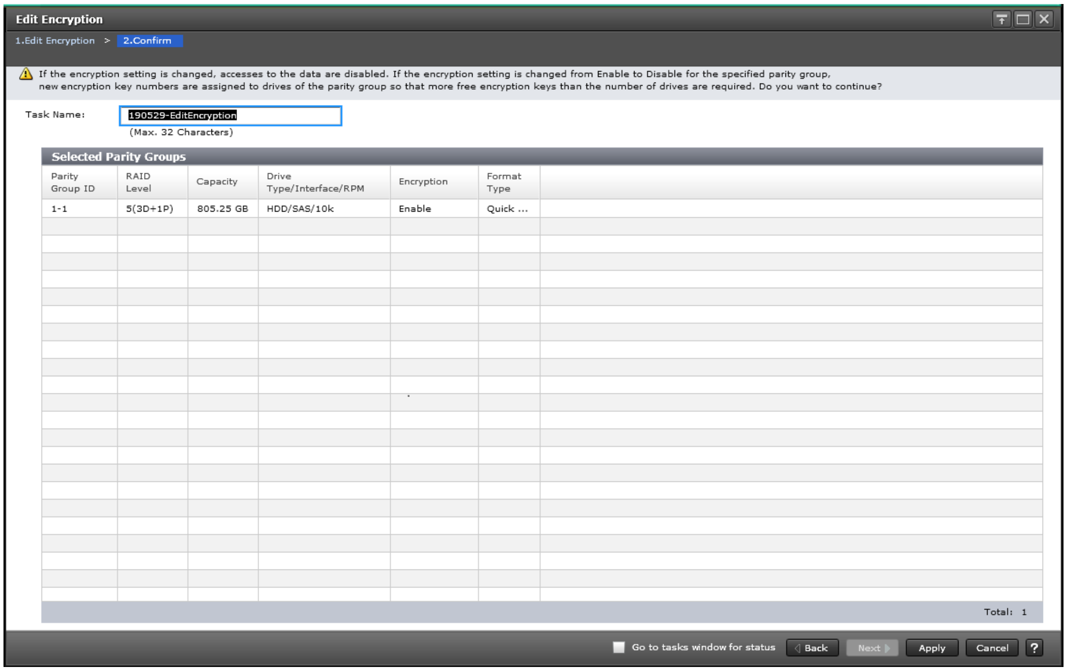
Selected Parity Groups table

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

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

Item	Description
Capacity	Displays the total capacity (unit) of the parity group.
Drive Type/Interface/RPM	Displays the type of drives in the parity group: ▪ Drive type (for example, HDD, SSD, FMD) ▪ Interface (for example, SAS, NVMe) ▪ RPM (for example, 7.2k, 10k)
Encryption	Displays the encryption setting for the parity group: ▪ Enable: Encryption is enabled. ▪ Disable: Encryption is disabled.
Format Type	Displays the selected format type of the parity group. You do not need to format volumes when there are none in the selected parity group. In this case, the format type in Selected Parity Groups becomes a hyphen (-) regardless of the status of the format type.
Remove	Removes the selected parity groups from the Selected Parity Groups table.

Edit Encryption confirmation window


Edit Encryption
1.Edit Encryption > 2.Confirm
Selected Parity Groups
□ Go to tasks window for status
Back
Next
Apply
Cancel
?

⚠ If the encryption setting is changed, accesses to the data are disabled. If the encryption setting is changed from Enable to Disable for the specified parity group, new encryption key numbers are assigned to drives of the parity group so that more free encryption keys than the number of drives are required. Do you want to continue?

Task Name: 190529-EditEncryption
(Max. 32 Characters)

Parity Group ID	RAID Level	Capacity	Drive Type/Interface/RPM	Encryption	Format Type
1-1	5(3D+1P)	805.25 GB	HDD/SAS/10k	Enable	Quick ...

Total: 1

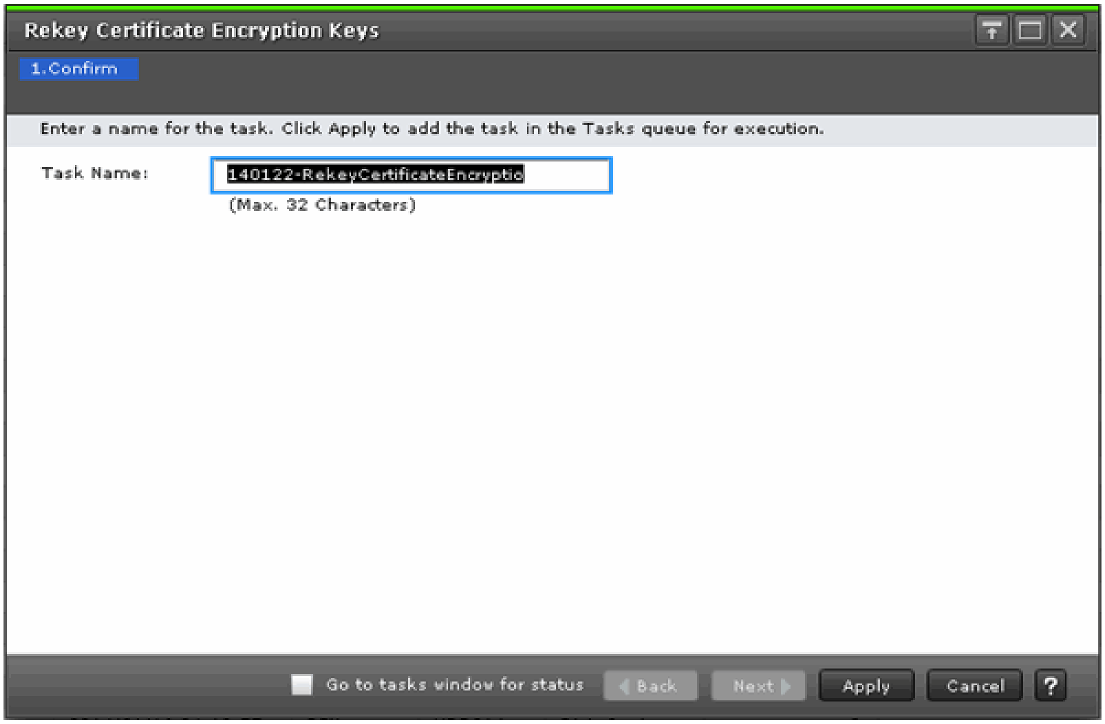
Selected Parity Groups table

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	Displays parity group identifier.
RAID Level	Displays 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	Displays the total capacity of the parity group.
Drive Type/Interface/RPM	Displays the type of drives in the parity group: ▪ Drive type (for example, HDD, SSD, FMD) ▪ (VSP 5000 series) Interface (for example, SAS, NVMe) ▪ RPM (for example, 7.2k, 10k)
Encryption	Displays the encryption setting for the parity group: ▪ Enable: Encryption is enabled. ▪ Disable: Encryption is disabled.
Format Type	Displays the format type 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.


Rekey Certificate Encryption Keys
1.Confirm
Go to tasks window for status
Back
Next
Apply
Cancel
?

Enter a name for the task. Click Apply to add the task in the Tasks queue for execution.

Task Name: 140122-RekeyCertificateEncryptio

(Max. 32 Characters)

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 wizard

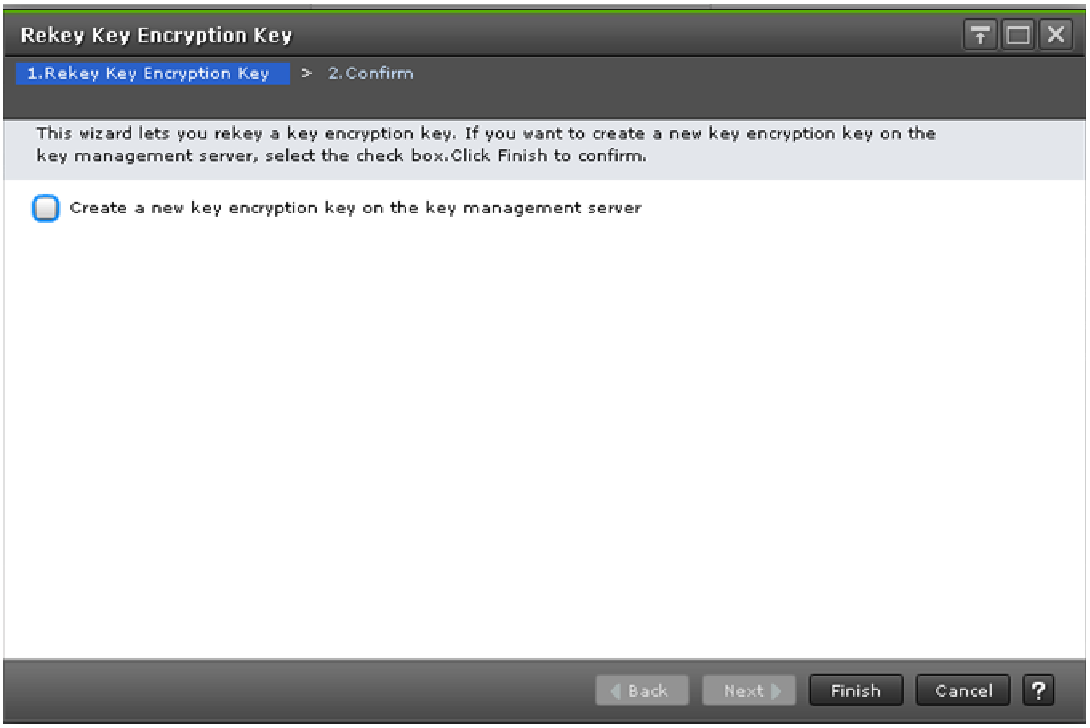
Use the Rekey Key Encryption Key wizard to rekey the key encryption key (KEK).

This wizard includes the following windows:

- **Rekey Key Encryption Key** window
- **Rekey Key Encryption Key** confirmation window

Rekey Key Encryption Key window

Use the **Rekey Key Encryption Keys** window to rekey the key encryption key (KEK) and to create a new KEK after migrating the KMS to another server.

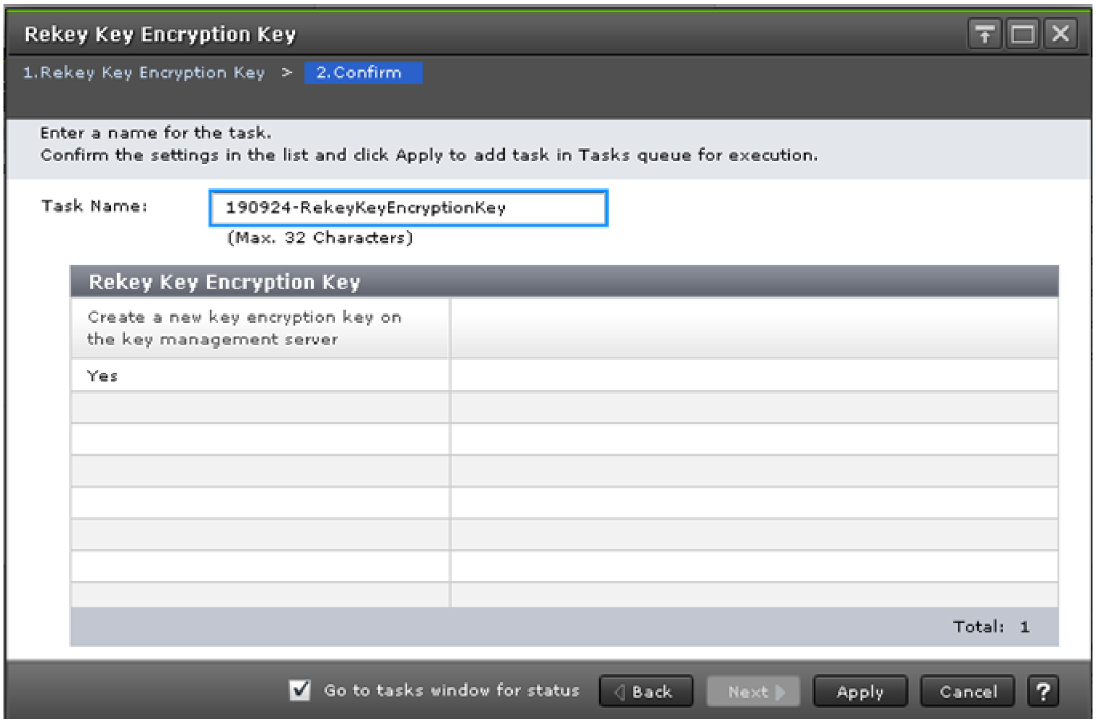


This wizard lets you rekey a key encryption key. If you want to create a new key encryption key on the key management server, select the check box.Click Finish to confirm.

□ Create a new key encryption key on the key management server

Item	Description
Create a new key encryption key on the key management server	Select this check box only when creating a new KEK. **Note about migrating the KMS:** If you are migrating to a new KMS, a new KEK is created automatically on the new KMS when you change the KMS connection settings in the **Edit Encryption Environmental Settings** window. Therefore, the **Rekey Key Encryption Key** window is not used to migrate the KMS to another server. However, if there was a problem connecting to the new KMS and you need to create the new KEK manually, select Create a new key encryption key on the key management server.

Rekey Key Encryption Key confirmation window


Rekey Key Encryption Key
1.Rekey Key Encryption Key > 2.Confirm
☑ Go to tasks window for status
Back
Next
Apply
Cancel
?

Enter a name for the task.
Confirm the settings in the list and click Apply to add task in Tasks queue for execution.

Task Name: 190924-RekeyKeyEncryptionKey
(Max. 32 Characters)

Rekey Key Encryption Key

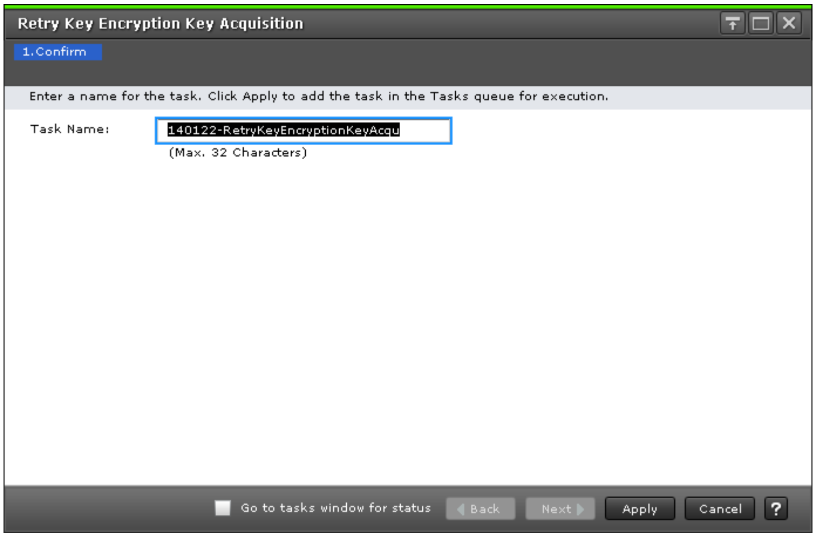
Create a new key encryption key on the key management server	
Yes	

Total: 1

Item	Description
Task Name	You can enter up to 32 ASCII characters (letters,numerals, and symbols) in Task Name. Task names are case-sensitive.
Create a new key encryption key on the key management server	Indicates whether Create a new key encryption key on the key management server was selected in the **Rekey Key Encryption Key** window.

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.


Retry Key Encryption Key Acquisition
1.Confirm

Enter a name for the task. Click Apply to add the task in the Tasks queue for execution.

Task Name: 140122-RetryKeyEncryptionKeyAcqu
(Max. 32 Characters)

□ Go to tasks window for status
Back
Next
Apply
Cancel
?

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

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
HitachiVantara.com | community.HitachiVantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
HitachiVantara.com/contact