

Hitachi Virtual Storage Platform F series, G series, and N series

SVOS 7.4.1

Encryption License Key User Guide

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

© 2014, 2019 Hitachi, Ltd. All rights reserved.

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

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

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara Corporation 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 Corporation.

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

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; 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.

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

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

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

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

Contents

| | |
|---------------------------------------------------------------------------|---------------|
| Preface..... | 7 |
| Intended audience..... | 7 |
| Product version..... | 7 |
| Release notes..... | 7 |
| Changes made in this revision..... | 8 |
| Referenced documents..... | 8 |
| Document conventions..... | 8 |
| Conventions for storage capacity values..... | 10 |
| Accessing product documentation..... | 11 |
| Getting help..... | 11 |
| Comments..... | 12 |
| Chapter 1: Overview of Encryption License Key..... | 13 |
| Encryption License Key benefits..... | 13 |
| Encryption License Key component description..... | 13 |
| Encryption License Key support specifications..... | 15 |
| When encryption keys are used..... | 18 |
| Audit logging of encryption events..... | 19 |
| Primary and secondary backups of encryption keys..... | 19 |
| Automatic encryption key backup (key management server only)..... | 19 |
| Regular encryption key backups..... | 19 |
| Workflow for implementing data encryption..... | 21 |
| Chapter 2: Key management server connections..... | 22 |
| Setting up the client certificate..... | 22 |
| Configuring the key management server..... | 23 |
| Settings in the Edit Encryption Environmental Settings window..... | 26 |
| Restoring the key management server connection after SVP replacement..... | 27 |

| | |
|----------------------------------------------------------------------------------------|-----------|
| Chapter 3: Encryption License Key installation..... | 29 |
| System requirements..... | 29 |
| Interoperability requirements and considerations..... | 30 |
| Installing the Encryption License Key software..... | 31 |
| Configuring the encryption environmental settings..... | 32 |
| Disabling or removing the Encryption License Key software..... | 35 |
| Chapter 4: Creating and backing up encryption keys..... | 36 |
| Creating encryption keys..... | 36 |
| Backing up encryption keys..... | 37 |
| Backing up the encryption keys to a file..... | 38 |
| Changing the password requirements for the backup encryption keys | 38 |
| Backing up the encryption keys manually to a key management server..... | 39 |
| Viewing encryption keys backed up on the key management server..... | 40 |
| Changing the schedule for regular encryption key backups..... | 40 |
| Changing the encryption key for encrypted data..... | 41 |
| Chapter 5: Enabling encryption..... | 42 |
| Enabling encryption on a parity group that does not contain pool volumes..... | 42 |
| Enabling encryption on a parity group that contains pool volumes..... | 43 |
| Encrypting existing data..... | 45 |
| Chapter 6: Disabling encryption..... | 47 |
| Disabling data encryption on a parity group that does not contain pool volumes..... | 47 |
| Disabling data encryption on a parity group that contains pool volumes..... | 48 |
| Formatting LDEVs at the parity-group level..... | 50 |
| Chapter 7: Restoring encryption keys..... | 51 |
| Restoring keys from a file..... | 51 |
| Restoring keys from a key management server..... | 52 |
| Forcibly restoring encryption keys..... | 53 |
| Forcibly restoring keys from a file..... | 53 |
| Forcibly restoring keys from a key management server..... | 54 |

| | |
|------------------------------------------------------------------------|-----------|
| Chapter 8: Deleting encryption keys | 55 |
| Deleting encryption keys from a file..... | 55 |
| Deleting (Free) encryption keys in a storage system..... | 56 |
| Deleting backup encryption keys from the server..... | 56 |
| Exporting a list of encryption keys..... | 57 |
| Rekeying key encryption keys..... | 57 |
| Rekeying certificate encryption keys..... | 58 |
| Retrying Key Encryption Key Acquisition..... | 58 |
| Initializing the encryption environment settings..... | 59 |
| Chapter 9: Troubleshooting..... | 60 |
| Encryption events in the audit log..... | 60 |
| Troubleshooting Encryption License Key..... | 60 |
| Contacting customer support..... | 63 |
| Appendix A: Encryption License Key GUI reference..... | 64 |
| Encryption Keys window..... | 64 |
| Edit Encryption Environmental Settings wizard..... | 67 |
| Edit Encryption Environmental Settings window..... | 67 |
| Edit Encryption Environmental Settings confirmation window..... | 72 |
| Create Keys wizard..... | 74 |
| Create Keys window..... | 74 |
| Create Keys confirmation window..... | 76 |
| Edit Password Policy (Backup Encryption Keys) wizard..... | 76 |
| Edit Password Policy (Backup Encryption Keys) window..... | 77 |
| Edit Password Policy (Backup Encryption Keys) confirmation window..... | 78 |
| Backup Keys to File wizard..... | 79 |
| Backup Keys to File window..... | 80 |
| Backup Keys to File confirmation window..... | 81 |
| Backup Keys to Server wizard..... | 81 |
| Backup Keys to Server window..... | 82 |
| Backup Keys to Server confirmation window..... | 83 |
| Restore Keys from File wizard..... | 83 |
| Restore Keys from File window..... | 84 |

| | |
|---------------------------------------------------------|-----|
| Restore Keys from File confirmation window..... | 84 |
| Force Restore Keys from File wizard..... | 85 |
| Force Restore Keys from File window..... | 85 |
| Force Restore Keys from File confirmation window..... | 86 |
| Restore Keys from Server wizard..... | 86 |
| Restore Keys from Server window..... | 87 |
| Restore Keys from Server confirmation window..... | 88 |
| Force Restore Keys from Server wizard..... | 88 |
| Force Restore Keys from Server window..... | 89 |
| Force Restore Keys from Server confirmation window..... | 90 |
| Delete Keys wizard..... | 90 |
| Delete Keys window..... | 91 |
| Delete Keys confirmation window..... | 91 |
| Delete Backup Keys on Server window..... | 92 |
| View Backup Keys on Server window..... | 93 |
| Edit Encryption wizard..... | 94 |
| Edit Encryption window..... | 95 |
| Edit Encryption confirmation window..... | 98 |
| Rekey Certificate Encryption Keys window..... | 99 |
| Rekey Key Encryption Key window..... | 100 |
| Retry Key Encryption Key Acquisition window..... | 100 |

| | |
|----------------------|------------|
| Glossary..... | 102 |
|----------------------|------------|

Preface

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

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 Hitachi Vantara storage systems.

Readers of this document should be familiar with the following:

- Data processing and RAID storage systems and their basic functions.
- The storage systems and 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.

Product version

This document revision applies to the following product versions:

- VSP G1x00, VSP F1500: microcode 80-06-2x or later
- VSP G200, G400, G600, G800; VSP F400, F600, F800: firmware 83-05-2x or later
- VSP N400, N600, N800: firmware 83-06-0x or later
- SVOS: 7.4.1 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 made in this revision

- Added support for VSP N series storage systems.

Referenced documents

Hitachi Virtual Storage Platform G1000, G1500, and F1500 documents:

- *Hitachi Audit Log User Guide*, MK-94RD8008
- *Provisioning Guide for Mainframe Systems*, MK-92RD8013
- *Provisioning Guide for Open Systems*, MK-92RD8014
- *System Administrator Guide*, MK-92RD8016

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

- *Provisioning Guide*, MK-94HM8014
- *System Administrator Guide*, MK-94HM8016
- *Hitachi Audit Log User Guide*, MK-94HM8028

Document conventions

This document uses the following storage system terminology conventions:

| Convention | Description |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VSP G series | Refers to the following storage systems: <ul style="list-style-type: none"> ▪ Hitachi Virtual Storage Platform G1x00 ▪ Hitachi Virtual Storage Platform G200 ▪ Hitachi Virtual Storage Platform G400 ▪ Hitachi Virtual Storage Platform G600 ▪ Hitachi Virtual Storage Platform G800 |
| VSP F series | Refers to the following storage systems: <ul style="list-style-type: none"> ▪ Hitachi Virtual Storage Platform F1500 ▪ Hitachi Virtual Storage Platform F400 ▪ Hitachi Virtual Storage Platform F600 ▪ Hitachi Virtual Storage Platform F800 |





| Convention | Description |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VSP Gx00 models | Refers to all of the following models, unless otherwise noted. <ul style="list-style-type: none"> ▪ Hitachi Virtual Storage Platform G200 ▪ Hitachi Virtual Storage Platform G400 ▪ Hitachi Virtual Storage Platform G600 ▪ Hitachi Virtual Storage Platform G800 |
| VSP Fx00 models | Refers to all of the following models, unless otherwise noted. <ul style="list-style-type: none"> ▪ Hitachi Virtual Storage Platform F400 ▪ Hitachi Virtual Storage Platform F600 ▪ Hitachi Virtual Storage Platform F800 |

This document uses the following typographic conventions:

| Convention | Description |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bold | <ul style="list-style-type: none"> ▪ Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click OK. ▪ Indicates emphasized words in list items. |
| <i>Italic</i> | <ul style="list-style-type: none"> ▪ 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: <code>pairedisplay -g group</code> <p>(For exceptions to this convention for variables, see the entry for angle brackets.)</p> |
| Monospace | Indicates text that is displayed on screen or entered by the user. Example: <code>pairedisplay -g oradb</code> |
| < > angle brackets | <p>Indicates variables in the following scenarios:</p> <ul style="list-style-type: none"> ▪ Variables are not clearly separated from the surrounding text or from other variables. Example: <code>Status-<report-name><file-version>.csv</code> ▪ Variables in headings. |

| Convention | Description |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [] square brackets | Indicates optional values. Example: [a b] indicates that you can choose a, b, or nothing. |
| { } braces | Indicates required or expected values. Example: { a b } indicates that you must choose either a or b. |
| vertical bar | Indicates that you have a choice between two or more options or arguments. Examples: [a b] indicates that you can choose a, b, or nothing. { a b } indicates that you must choose either a or b. |

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

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

| Physical capacity unit | Value |
|------------------------|--------------------------------------|
| 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: <ul style="list-style-type: none"> ▪ OPEN-V: 960 KB ▪ Others: 720 KB |
| 1 KB | 1,024 (2 ¹⁰) bytes |
| 1 MB | 1,024 KB or 1,024 ² bytes |
| 1 GB | 1,024 MB or 1,024 ³ bytes |
| 1 TB | 1,024 GB or 1,024 ⁴ bytes |
| 1 PB | 1,024 TB or 1,024 ⁵ bytes |
| 1 EB | 1,024 PB or 1,024 ⁶ bytes |

Accessing product documentation

Product user documentation is available on Hitachi Vantara Support Connect: <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

[Hitachi Vantara Support Connect](https://support.hitachivantara.com/en_us/contact-us.html) is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect 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 Corporation.

Thank you!

Chapter 1: Overview of Encryption License Key

This chapter describes the Encryption License Key feature and specifications.

Encryption License Key benefits

The VSP G series, VSP N series, and VSP F series storage systems include a data at-rest encryption feature that can be used to provide protections against data breaches associated with storage media (for example, loss or theft). This feature, known as the Encryption License Key feature, includes a controller-based encryption implementation as well as integrated key management functionality that can also 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 or 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 License Key component description

The Encryption License Key feature consists of three major components:

- Encryption License Key software license
- Data at-rest encryption
- Key management

Encryption License Key software license

A valid (not expired) Encryption License Key software license must be installed before the Encryption License Key feature can be used. Note that an expired license can limit the operations that can be performed on an already configured storage system. The Encryption License Key software license is provided by Hitachi.

Data at-rest encryption (DARE)

The data at-rest encryption (DARE) functionality is implemented using cryptographic hardware (chips), included as part of the encrypting back-end directors (EBEDs), which must be installed and configured before DARE can be used. These EBEDs perform the I/O to the drives as well as encrypting and decrypting data as it is being written to or read from a physical drive.

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 EBED, it is recommended to encrypt all parity groups on an EBED. 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 License Key feature includes multiple options associated with key management.

It is important to understand what keys the storage systems use and the roles these keys play in the DARE solution. There is a hierarchy of keys that include:

- 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 EBED requires a key for the encryption of the certificate (registration of the EBED) and a key to encrypt the DEKs stored on the EBED.
- 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 lifecycle, 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. 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 every EBED installed in the storage system. When the storage system boots, the keys in shared memory are used unless they are missing or corrupted, at which point 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 automatically performed after certain key operations (for example, generating keys) and/or by leveraging regular (automated) key backups. Note that automatic key backups have been optimized such that they are only performed when the CEKs and DEKs have changed.

Encryption License Key support specifications

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

| Item | | Specification |
|----------------------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hardware specifications | Encryption algorithm | Advanced Encryption Standard (AES) 256 bit |
| | Encryption mode | XTS mode |
| | Encryption module standard | <ul style="list-style-type: none"> VSP G200: Compliant to FIPS 140-2 Level 1 VSP G/N400, G/N600, G/N800, VSP F400, F600, F800: Compliant to FIPS 140-2 Level 2* VSP G1000, VSP G1500, and VSP F1500: Compliant to FIPS 140-2 Level 1 and Level 2* <p>*To use encryption modules compliant to FIPS 140-2 Level 2, contact customer support.</p> |
| 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 encryption keys | Use Device Manager - Storage Navigator (HDvM - SN) to create encryption keys. |
| | Deleting encryption keys | <p>Use Device Manager - Storage Navigator to delete encryption keys.</p> <p>Note: You cannot delete encryption keys that are allocated to implemented drives. You can delete the encryption key allocated to a drive and allocate a new encryption key only when encryption is disabled for the parity group.</p> |
| | Unit of encryption/decryption | <p>Encryption is applied to the parity group.</p> <p>Data encryption keys (DEKs) are used per drive.</p> |

| Item | | Specification |
|------|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | Number of encryption keys | <ul style="list-style-type: none"> ▪ VSP G200: Up to 512 Free keys or DEKs can be created per storage system. In addition, you can create 4 certificate encryption keys (CEKs) and one key encryption key (KEK), so the total maximum number of encryption keys, including DEKs, CEKs, and KEKs, is 517. ▪ VSP G/N400, G/N600, VSP F400, F600: Up to 1,024 Free keys or DEKs can be created per storage system. In addition, you can create 4 CEKs and one KEK, so the total maximum number of encryption keys, including DEKs, CEKs, and KEKs, is 1,029. ▪ VSP G/N800, VSP F800: Up to 2,048 Free keys or DEKs can be created per storage system. In addition, you can create 16 CEKs and one KEK, so the total maximum number of encryption keys, including DEKs, CEKs, and KEKs, is 2,065. ▪ VSP G1x00, VSP F1500: Up to 4,096 Free keys or DEKs can be created per storage system. In addition, you can create 32 CEKs and one KEK, so the total maximum number of encryption keys, including DEKs, CEKs, and KEKs, is 4,129. |
| | Attribute of encryption keys | <p>The attributes for the encryption keys are:</p> <ul style="list-style-type: none"> ▪ 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. ▪ KEK: Key encryption key. The key for the encryption of the CEK. |

| Item | | Specification |
|------|------------------------------|---------------------------------------------------------|
| | Backup/restore functionality | Redundant (primary and secondary) backup/restore copies |

When encryption keys are used

After the encryption environment is set up, encryption keys are used to perform the following operations. In addition, if a problem occurs during an operation, extra keys might be needed to recover from the problem.

Adding drives

A Free key is needed for each drive to allocate a DEK.

Replacing drives

A Free key is needed for each drive to change an encryption key.

Decrypting parity groups

A Free key is needed for each drive in a parity group to change an encryption key.

Adding or replacing encrypting back-end directors (EBEDs)

VSP G1x00, VSP F1500: To replace an EBED, 4 Free keys are used as CEKs, and 2 Free keys are used to register them.

VSP Gx00, VSP Nx00, VSP Fx00 models: To replace an EBED, 2 Free keys are used as CEKs, and 1 Free key is used to register them.

Replacing controllers

VSP G200: 2 Free keys are used as CEKs, and 1 Free key is used to register them.

VSP G/N400, G/N600, G/N800; VSP F400, F600, F800: Free keys are not used.

Updating CEKs

VSP G1x00, VSP F1500: 4 Free keys for each EBED (32 Free keys per storage system) are needed to change CEKs.

VSP G200: 2 Free keys for each controller and 4 Free keys per storage system are needed to change CEKs.

VSP G/N400, G/N600; VSP F400, F600: 2 Free keys for each EBED (4 Free keys per storage system) are needed to change CEKs.

VSP G/N800, VSP F800: 2 Free keys for each EBED (up to 16 Free keys per storage system, regardless of the number of EBEDs) are needed to change CEKs.

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.

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

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

If desired, you can configure regularly scheduled encryption key backups to the key management server. These operations are called regular backup operations. You can enable the Encryption Key Regular Backup option and specify the time(s) for the regular backup operations 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.



Note:

- 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.



Note: 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.

Workflow for implementing data encryption

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

1. If you will use a key management server, configure the key management server first. Several configuration tasks must be performed on the key management server before you can perform the initial configuration of the Encryption License Key feature.

For details, see [Key management server connections \(on page 22\)](#).

2. Install the Encryption License Key software.

For instructions, see [Installing the Encryption License Key software \(on page 31\)](#).

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

For instructions, see [Configuring the encryption environmental settings \(on page 32\)](#).

4. Create and back up the encryption keys.

For details, see [Creating and backing up encryption keys \(on page 36\)](#).

5. Enable encryption on the desired parity groups.

For instructions, see [Enabling encryption on a parity group that does not contain pool volumes \(on page 42\)](#).

Chapter 2: Key management server connections

The VSP F series, VSP G series, and VSP N series storage systems support an optional connection to an external key management server. For details about supported key management servers, see the Encryption Key Management Server Support Matrix on the Hitachi interoperability site: https://support.hitachivantara.com/en_us/interoperability.html.

When a key management server is used, several configuration tasks must be performed on the key management server before you can perform the initial configuration of the Encryption License Key feature. 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 server. The required configuration tasks for the key management server vary depending on the type of server (vendor, software version). For information about preparing the necessary services to accept connections from the storage system, refer to the documentation for your 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 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 Server administrator.

Setting up the client certificate

Use the following process to prepare the client certificate.



Note: The client certificate on the key management server 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 key management server.

Procedure

1. Download and install `openssl.exe` from <http://www.openssl.org/> to the C:\openssl folder.
2. Create the key file. You can create the following types of key files:
 - Private key (.key) file. For the creation of Private key, see the *System Administrator Guide*.
 - Public key (.csr) file. For the creation of Public key, see the *System Administrator Guide*.

3. If you created a Public key (.csr) file, submit the Public key (.csr) to an appropriate trusted internal or third party Certificate Authority for signing.
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.
The following is an example for an output folder of `c:\key`, private key file (`client.key`), and a client certificate file (`client.crt`):

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

Configuring the key management server

If you plan to use a key management server, you must establish and verify the network connection to the key management server. In addition, you can also configure the following important options for your encryption environment:

- Using a secondary key management server in addition to the primary key management server
- Generating encryption keys on the key management server
- Protecting the key encryption key (KEK) on the key management server
- Enabling regular backups of the data encryption keys on the key management server
- Disabling generation of encryption keys on the storage system



Note: If you plan 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.



Caution: Encryption keys backed up on the key management server are managed with the client certificate. If the client certificate is lost and the SVP is replaced due to a failure, the encryption keys that were backed up before the SVP replacement cannot be restored.

In addition, when the connection settings are backed up to the key management server, the storage system does not back up the client certificate. Make sure that you back up a copy of the connection settings to the key management server and save a copy of the client certificate separately. Refer to your corporate security policy for procedures related to backups.

To protect the key encryption key at the key management server, the key management server must be configured using two clustered servers. For this reason, you must enable the secondary server.

Before you begin

- You must have the Security Administrator (View & Modify) role.
- You must have the names and directory locations of the client and root certificates on the key management servers.
- If you are enabling regular encryption key backups, you must have the user name and password of the regular backup user. The regular backup user 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** pane, click **Edit Encryption Environmental Settings**.
3. For **Key Management Server**, select **Enable**.
4. In **Primary Server**, enter the network connection information for the key management server, and then click **Browse** to select the client and root certificates on the server.
5. If you will use a secondary key management server, select **Enable** for **Secondary Server**, and enter the network connection information and select the client and root certificates for the secondary server.



Note: If you want to disable key generation on the storage system, you must enable the secondary server.

6. For **Server Configuration Test**, click **Check** to test the network connection. If the server configuration test fails, error messages appear. 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.

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

To store the key encryption key on the key management server, select **Protect the Key Encryption Key on the Key Management Server**, read the warning, and then click **I Agree**.



Caution: If you apply the **Protect the Key Encryption Key on the Key Management Server** setting to the storage system, the storage system will get the encryption keys backed up on the key management server when the storage system is powered on. Therefore, you must confirm that the SVP is properly connected to the key management server before powering on the storage system.

9. If you store the encryption keys in the key management server, and you want to delete the encryption keys in the storage system when the storage system is turned off, select **Delete Internal Encryption Keys at PS OFF**, read the warning, and then click **I Agree**.



Caution: If you select **Delete Internal Encryption Keys at PS OFF**, the storage system will try to get the encryption keys backed up on the key management server when the storage system is turned on. Therefore, you must confirm that the SVP is properly connected to the key management server before turning the storage system on.

10. To generate encryption keys on the key management server without creating encryption keys in the storage system, select **Disable Local Key Generation**, read the warning, and click **I Agree**.



Caution: If you select **Disable Local Key Generation** and apply the setting to the storage system, you cannot undo this action.

11. When you are finished configuring the encryption environmental settings, click **Finish**.
12. 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**.
13. Click **Apply**.

Result



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

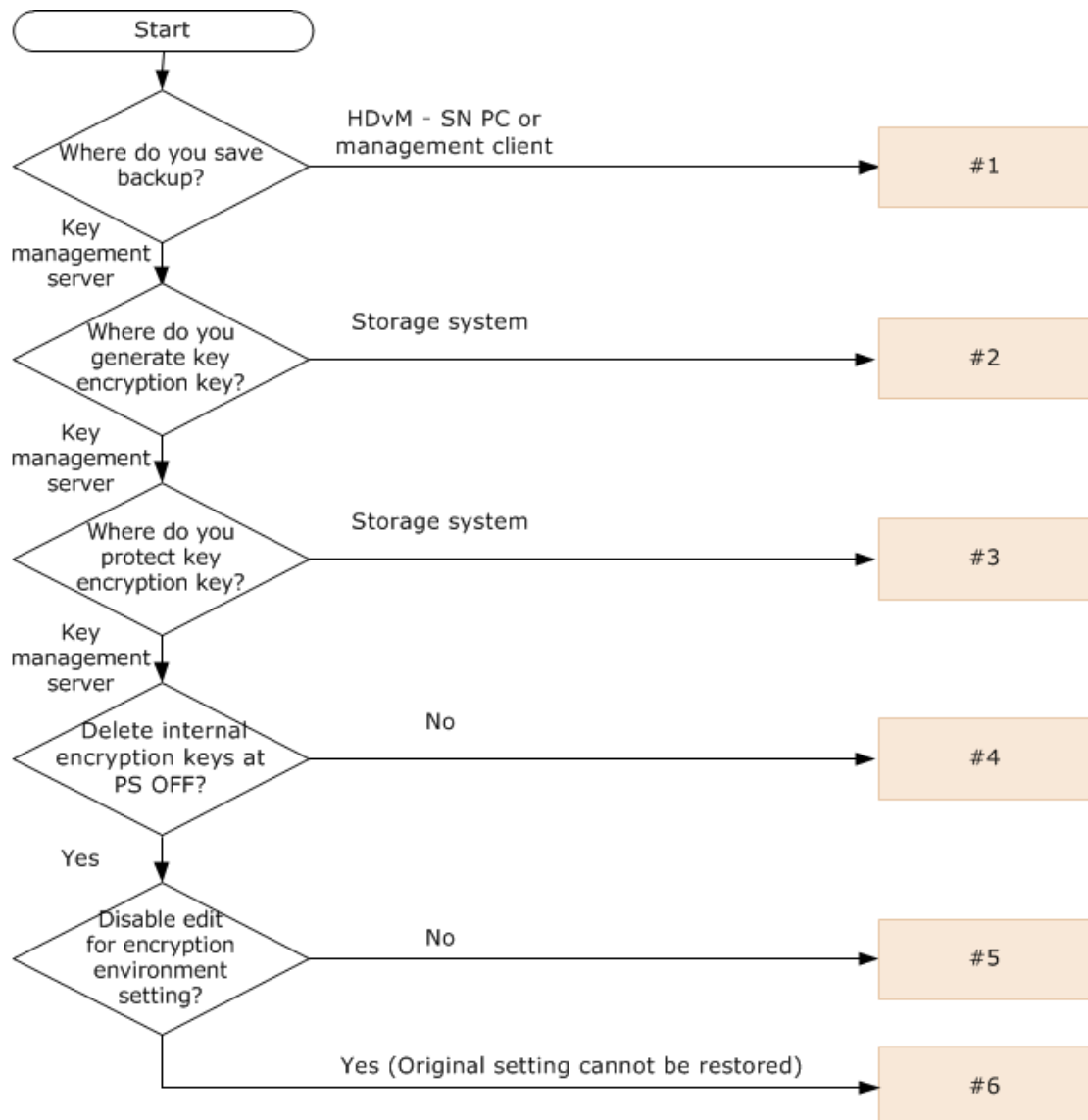
Next steps

1. Save a backup copy of the client certificate.

2. Back up the connection settings to the key management server 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.

Settings in the Edit Encryption Environmental Settings window

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



| | Settings in the Edit Encryption Environmental Settings window | | | | | | |
|----|---------------------------------------------------------------|------------------|-----------------------------|---------------------------------------------------|-------------------------------------------------------------|-------------------------------------------|------------------------------|
| | Key Management Server | Server Settings | | Generate Encryption Keys on Key Management Server | Protect the Key Encryption Key at the Key Management Server | Delete Internal Encryption Keys at PS OFF | Disable local key generation |
| | | Primary Server | Secondary Server | | | | |
| #1 | Disable | Do not specify | Do not specify | Clear | Clear | Clear | Clear |
| #2 | Enable | Specify settings | Enable and specify settings | Clear | Clear | Clear | Clear |
| #3 | Enable | Specify settings | Enable and specify settings | Select | Clear | Clear | Clear |
| #4 | Enable | Specify settings | Enable and specify settings | Select | Select | Clear | Clear |
| #5 | Enable | Specify settings | Enable and specify settings | Select | Select | Select | Clear |
| #6 | Enable | Specify settings | Enable and specify settings | Select | Select | Select | Select |

Restoring the key management server connection after SVP replacement

If you are restoring the key management server connection after the SVP replacement, restore the connection setting of the key management server which is already backed up. After doing so, if the setting in the **Edit Encryption Environmental Settings** window before the SVP replacement is a value other than #1 in the table in [Settings in the Edit Encryption Environmental Settings window \(on page 26\)](#), set the client certificate and root certificate of the key management server again.

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

If the setting in the **Edit Encryption Environmental Settings** window before the SVP replacement is #4 or #5 in the table in [Settings in the Edit Encryption Environmental Settings window \(on page 26\)](#) and you have already created a new client certificate after the SVP replacement, update the key encryption key after you set the connection for the key management server. When you do this, the key deletion key encryption fails because you cannot delete the key encryption key before the update; however, the key encryption key is already updated.

Chapter 3: Encryption License Key installation

This chapter describes the system requirements and provides instructions for installing the Encryption License Key software and configuring the environmental settings for encryption.

System requirements

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

| Item | Requirements |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Storage system | <ul style="list-style-type: none">▪ VSP G1000: Microcode 80-01-2x or later▪ VSP G1500, VSP F1500: Microcode 80-05-0x or later▪ VSP G200: Firmware 83-03-0x or later▪ VSP G/F400, G/F600, G/F800: Firmware 83-01-0x or later, VSP Nx00: Firmware 83-06-0x or later▪ Encryption License Key software license▪ Encrypting back-end directors (EBEDs) <p>For both EBEDs and standard BEDs, spare disks must be installed. The spare disk of an EBED cannot be used as a spare disk of a standard BED, and the spare disk of a standard BED cannot be used as a spare of an EBED.</p> |
| Hitachi Device Manager - Storage Navigator | <p>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).</p> <p>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.</p> |

| Item | Requirements |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | If you plan to enable regular encryption key backups on the key management server, you must designate a specific 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: All volume emulation types (open-systems, mainframe, and multiplatform) are supported. Type: Internal. External volumes are not supported. |
| SVP (Web server) | If you want to protect key encryption keys (KEKs) on the key management server, the SVP must always be up and running. If you want to connect to the key management server by specifying a host name instead of an IP address, you must set up a DNS server on the key management server, and the IP address of the DNS server must be configured on the SVP of the storage system. |
| Key management server (optional) | <ul style="list-style-type: none"> ▪ Protocol: Key Management Interoperability Protocol 1.0 (KMIP 1.0) ▪ Software: For the latest information about key management server support, see the Encryption Key Management Server Support Matrix on the Hitachi interoperability site: https://support.hitachivantara.com/en_us/interoperability.html ▪ Certificates: <ul style="list-style-type: none"> • The root certificate must be in X.509 format and must be placed on the key management server. For details, see the documentation for the server. • The client certificate must be current, not expired, and in PKCS#12 format. |

Interoperability requirements and considerations

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

| Functions | Interoperability requirements and considerations |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ShadowImage, TrueCopy, Compatible FlashCopy® V2, and Compatible XRC | Encrypt both the P-VOL and S-VOLs (S-VOL and T-VOLs for Compatible FlashCopy® V2) of pairs to ensure data security. |
| Thin Image | Match the encryption states of the P-VOL and pool-VOL. If the P-VOL is encrypted, encrypt all of the pool-VOLs. If the data pool contains an unencrypted pool-VOL, the differential data of the P-VOL is not encrypted. |
| Universal Replicator | Match the encryption states of a P-VOL and S-VOL. If you encrypt the P-VOL only, the data copied on the S-VOL is not encrypted and therefore not protected. When you encrypt a P-VOL or S-VOL, use a journal to which only encrypted LDEVs are registered as journal volumes. If the encryption states of the P-VOL, S-VOL, and journal volumes do not match, the journal data in the P-VOL is not encrypted, and the security of the data cannot be guaranteed. |
| Dynamic Provisioning, Dynamic Tiering, Dynamic Provisioning for Mainframe, Dynamic Tiering for Mainframe, active flash, and active flash for mainframe | 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. |
| dedupe and compression | When disabling encryption, you must disable the capacity saving function settings for the virtual volume. |

Installing the Encryption License Key software

Before you begin

- Verify that your system meets the system requirements.
- 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, 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 **Encryption License Key**, 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

- Assign the Security Administrator (View & Modify) role to the user who will configure the encryption environmental settings, enable and disable encryption on parity groups, and back up or restore encryption keys. For details and instructions, see the *System Administrator Guide*.
- If you will use a key management server, configure the key management server. For instructions, see [Configuring the key management server \(on page 23\)](#).
- Configure the encryption environmental settings on the storage system. For instructions, see [Configuring the encryption environmental settings \(on page 32\)](#).

Configuring the encryption environmental settings

Before you can enable encryption on parity groups, you must configure the settings and options for your encryption environment using the **Edit Encryption Environment Settings** window. The encryption environmental settings and options include the following:

- Enabling and disabling use of a key management server
- Enabling and disabling use of a secondary key management server
- Scheduling regular backups of encryption keys
- Generating encryption keys on the key management server
- Storing encryption keys on the key management server
- Deleting local encryption keys when the storage system is powered off
- Protecting the key encryption key on the key management server
- Disabling local generation of encryption keys on the storage system



Caution: If you plan to enable regular encryption key backups on a key management server, 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.
- 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. The user name and password of the regular backup user must be entered in the **Edit Encryption Environmental Settings** window. A regular backup might fail if you delete the regular backup user or edit the user account of the regular backup user, including if you change the password or roles of the regular backup user. For this reason, every time you edit the user account of the regular backup user, make sure to respecify the user name and password of the regular backup user in the **Edit Encryption Environmental Settings** window.
- (VSP Gx00, VSP Nx00, and VSP Fx00 models) 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.

Before you begin

- If you will use a key management server, configure the key management server. For instructions, see [Configuring the key management server \(on page 23\)](#).
- 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** pane, click **Edit Encryption Environmental Settings**.
3. In the **Edit Encryption Environmental Settings** window, select the desired option for **Key Management Server**.
 - If you will use a key management server, select **Enable** for **Key Management Server**, and go to the next step.
 - If you will not use a key management server, select **Disable** for **Key Management Server**, click **Finish**, and go to the last step.
4. Expand **Server Settings**, and enter the information for the primary key management server under **Primary Server**.
5. If you will use a secondary key management server, select **Enable** for **Secondary Server**, and enter the information for the secondary key management server under **Secondary Server**.
6. Test the connection to the primary and secondary key management servers by clicking **Check** next to **Server Configuration Test**. If the server configuration test fails, error messages are displayed.
7. If you want to schedule regular backups of the encryption keys, select **Enable Encryption Key Regular Backup to Key Management Server**, select the desired

daily backup times from **Regular Backup Time**, and then enter the user name and password of the regular backup user in **Regular Backup User**.

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.



Caution: If you enable this option, see the requirements and restrictions for regular backups listed above.

8. If you want to generate the encryption keys on the key management server, select **Generate Encryption Keys on Key Management Server**.
9. If you want to store the key encryption key on the key management server, select **Protect the Key Encryption Key on the Key Management Server**, read the warning, and then select **I Agree**.



Caution: If you select **Protect the Key Encryption Key on the Key Management Server** and apply this setting to the storage system, when the storage system is powered on it will get the encryption keys backed up on the key management server. You must confirm that the SVP is connected to the key management server properly before powering on the storage system.

10. If you want to store the encryption keys on the key management server and delete the encryption keys in the storage system when the storage system is powered off, select **Delete Internal Encryption Keys at PS OFF**, and then select **I Agree**.



Caution: If you apply the **Delete Internal Encryption Keys at PS OFF** setting to the storage system, the storage system will get the encryption keys backed up on the key management server when it is powered on. Therefore, you must confirm that the SVP is properly connected to the key management server before powering on the storage system.

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



Caution: If you select **Disable local key generation** and apply this setting to the storage system, you will not be able to change this setting later.

12. Click **Finish**.
13. 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**.

14. click **Apply**.



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

Next steps

1. Save a backup copy of the client certificate.
2. Back up the connection settings to the key management server 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.

Disabling or removing the Encryption License Key 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 re-enable 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 \(on page 47\)](#).
- 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 environment settings \(on page 59\)](#).
- You must have the Storage Administrator (Initial Configuration) role to disable or remove a software license key.

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. If desired, 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. Free keys or DEKs are created automatically when you configure the encryption environmental settings in the **Edit Encryption Environmental Settings** window for the first time. The number of keys created automatically depends on the number of installed EBEDs.

- VSP G1x00, VSP F1500: The maximum number of encryption keys per storage system is 4,096. If the maximum number of EBEDs are installed, 4,048 keys are created automatically, so in this case you can create 48 more encryption keys.
- VSP G200: The maximum number of encryption keys per storage system is 512. If the maximum number of EBEDs are installed, 506 keys are created automatically, so in this case you can create 6 more encryption keys.
- VSP G/N400, G/N600, VSP F400, F600: The maximum number of encryption keys per storage system is 1,024. If the maximum number of EBEDs are installed, 1,018 keys are created automatically, so in this case you can create 6 more encryption keys.
- VSP G/N800, VSP F800: The maximum number of encryption keys per storage system is 2,048. If the maximum number of EBEDs are installed, 2,024 keys are created automatically, so in this case you can create 24 more encryption keys.

Before you begin

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

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. In the **Explorer** pane, select **Administration**, and then select **Encryption Keys**.
3. On the **Encryption Keys** tab, click **Create Keys**.
4. In the **Create Keys** window, specify the number of encryption keys you want to create. The encryption keys with the attribute of **Free** will be set. The key IDs will be automatically assigned.
5. Click **Finish**.
6. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.
If you want the **Task** window to open after you click **Apply**, select **Go to tasks window for status**.
7. 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 \(on page 38\)](#).

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.

DEKs and CEKs 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. In the **Explorer** pane, expand **Administration**, and then click **Encryption Keys**.
2. On the **Encryption Keys** tab, select the key ID for the data encryption key 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 **Task** 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 a key management server. The data encryption keys that you back up to a key management server are managed with the client certificate. When you manually back up to a key management server, the server uses another data encryption key to encrypt the original keys. Both keys reside on the server.



Note: The number of keys that can be backed up on a key management server 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. In the **Explorer** pane, expand **Administration**, and then click **Encryption Keys**.
2. On the **Encryption Keys** tab, select the key ID for the data encryption key you want to back up, and then click **Backup Keys > To Server**.
3. (Optional) If desired, enter a description for the backup data encryption key.
4. Click **Finish**.
5. 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**.
6. Click **Apply**.

Viewing encryption keys backed up on the key management server

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

Before you begin

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

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. Select **Administration** in **Explorer**, and select **Encryption Keys**.
The **Encryption Keys** window is opened.
3. On the **Encryption Keys** tab, click **View Backup Keys on Server** to view the backup keys 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. In the **Edit Encryption Environmental Settings** window, select the new daily backup times from **Regular Backup Time**.
4. Click **Finish**.
5. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.
If you want the **Task** window to open after you click **Apply**, select **Go to tasks window for status**.
6. Click **Apply**.

Changing the 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 parity group with another encryption key and then move the data to that parity group using ShadowImage, TrueCopy, or Volume Migration. You can move data for each LDEV.

Procedure

1. Create a new parity group.
2. Enable encryption with a new data encryption key. See [Enabling encryption \(on page 42\)](#).
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. After migrating data, if you disable encryption of the source parity group, the encryption key assigned to the drive in the parity group is deleted, and a new encryption key is assigned. In addition, if a drive is replaced, the data encryption keys that are allocated to that drive are deleted, and new data encryption keys are allocated when the new drive is added.

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.

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:

- When the parity group does not contain any volumes, or when all volumes in the parity group are blocked. If the parity group contains any unblocked volumes, you must block the volumes before encryption can be enabled. For instructions, see the *Provisioning Guide*.
- When accelerated compression is not enabled on the parity group. If accelerated compression is enabled, you must disable accelerated compression before encryption can be enabled. For instructions, 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 the task.
 - c. For **Format Type**, select the desired format type.
 - 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 only under the following conditions:

- When the parity group does not contain any volumes, or when all volumes in the parity group are blocked. If the parity group contains any unblocked volumes, you must block the volumes before encryption can be enabled. For instructions, see the *Provisioning Guide*.
- When accelerated compression is not enabled on the parity group. If accelerated compression is enabled, you must disable accelerated compression before encryption can be enabled. For instructions, 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. For details, see [Configuring the encryption environmental settings \(on page 32\)](#).

- 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. In the Explorer pane, expand the **Storage Systems** tree, 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:
 1. Block the virtual volume.
 2. Format the virtual volume.
 3. Disable the capacity saving setting on the virtual volume.
 4. Verify that **Capacity Saving Status** of the virtual volume shows **Disabled**.
3. When the **Capacity Saving Status** for all virtual volumes in the pool shows **Disabled**, check the deduplication setting for the pool (in the **Deduplication** row):
 - If **Not Available** or a hyphen is displayed, go to the next step.
 - If **Available** is displayed, open the **Edit Pools** window, and select **No** for **Assign Deduplication System Data Volume**.
4. 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.
5. Enable data encryption for the parity group as follows:
 - a. In the **Explorer** pane, select **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, select **Enable** for **Encryption**, and select **Normal Format** for **Format Type**.
 - 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.
- f. When you are finished adding parity groups to the **Selected Parity Groups** list, click **Finish**.
- g. 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**.
- h. Click **Apply**, and then click **OK** in the message that appears.

6. 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 deduplication function of the pool, select Yes for Assign Deduplication System Data Volume in the **Edit Pools** window.
- 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 **Task** 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: Disabling encryption

Encryption is disabled at the parity-group level. When you disable encryption for 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 when the parity group does not contain any volumes, or when all volumes in the parity group are blocked. If the parity group contains any unblocked volumes, you must block the volumes before encryption can be disabled.

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. In the **Explorer** pane, expand **Storage Systems**, and select **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**.



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

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 the 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 **Task** 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. If you want to disable encryption on a parity group that 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. In the Explorer pane, expand the **Storage Systems** tree, 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 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:
 1. Block the volume.
 2. Format the volume.
 3. Disable the capacity saving setting on the volume.
 4. Verify that **Capacity Saving Status** of the volume shows **Disabled**.

3. When the **Capacity Saving Status** for all volumes in the pool shows **Disabled**, check the deduplication setting for the pool (in the **Deduplication** row):
 - If **Not Available** or a hyphen is displayed, go to the next step.
 - If **Available** is displayed, open the **Edit Pools** window, and select **No** for **Assign Deduplication System Data Volume**.
4. 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.
5. Disable data encryption for the parity group as follows:
 - a. In 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.
 - 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 **Task** 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.
6. 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 deduplication function of the pool, select Yes for Assign Deduplication System Data Volume in the **Edit Pools** window.
- 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

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

Procedure

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

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

Click **Apply**.

Chapter 7: 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 (including Free keys, DEKs, and CEKs):

- VSP G200: 516 keys
- VSP G/N400, G/N600, VSP F400, F600: 1,028 keys
- VSP G/N800, VSP F800 models: 2,064 keys
- VSP G1x00, VSP F1500: 4,128 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 the key is set must be blocked. In addition, after the restoration of the key, the volumes belonging to the parity group for which encryption key is set must be restored.

Restoring keys from a file

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* for your storage system.
- You must have the Security Administrator (View & Modify) role.

Procedure

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

The **Encryption Keys** window is opened.

3. On the **Encryption Keys** tab, click **Restore Keys > From File**.
4. In the **Restore Keys from File** window, click **Browse** and then click **OK**.
5. In the **Open** dialog box, select the backup file and click **Open**.
6. In the **Restore Keys from File** window, complete the following item and then click **Finish**:
 - For **File Name**, shows the name of the selected file.
View-only: Yes
 - For **Password**, type the password for the data encryption key that you typed when you backed up the selected data encryption key.
7. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.

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

Click **Apply**.

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 system administrator replaces the SVP 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. Display the Device Manager - Storage Navigator main window.
2. Select **Administration** in **Explorer**, and select **Encryption Keys**.
The **Encryption Keys** window is opened.
3. On the **Encryption Keys** tab, click **Restore Keys > From Server**.
4. In the **Restore Keys from Server** window, select the data encryption key you want to restore.
5. Click **Finish**.
6. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.
If you want the **Task** window to open after you click **Apply**, select **Go to tasks window for status**.

Click **Apply**.

The backup data encryption key is restored.

Forcibly restoring encryption keys

If encryption keys cannot be used, including the keys backed up by the primary backup in the storage system, the encryption keys can be restored forcibly.



Note: To restore the encryption key, the volumes that belong to the parity group for which the key is set must be blocked. In addition, after the key is restored, the volumes that belong to the parity group for which the key is set must be restored.



Caution: If you restore an encryption key that is not the latest key, the drive, EBED, or controller 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. In the **Explorer** pane, expand **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 **Task** 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. In the **Explorer** pane, expand **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 **Task** window to open after you click **Apply**, select **Go to tasks window for status**.
6. Click **Apply**.

Chapter 8: Deleting encryption keys

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

Deleting encryption keys from a file

Delete encryption keys from a file on the HDvM - SN 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

- Create the secondary backup of the encryption key. See [Backing up encryption keys \(on page 37\)](#).
- Verify that the key is not allocated to the parity group.
- You must have the Security Administrator (View & Modify) role.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. Expand **Administration** in the **Explorer** pane, and select **Encryption Keys**.
3. 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**.
4. If you also want to back up other encryption keys to the key management server at this time, click **Next** (instead of Finish). For details about backing up keys to the key management server, see [Backing up the encryption keys manually to a key management server \(on page 39\)](#).
5. In the **Delete Keys** window, click **Finish**.
6. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**, and then click **Apply**.
If you want the **Task** window to open after you click **Apply**, select **Go to tasks window for status**.
7. In the message that appears asking whether to apply the setting to the storage system, click **OK**.

Result

The data encryption key is deleted.

Deleting (Free) encryption keys in a storage system

You can delete only Free keys (encryption key with the Free attribute). You cannot delete DEKs, CEKs, or KEKs.

Before you begin

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

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. Expand **Administration** in the **Explorer** pane, and select **Encryption Keys**.
3. 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**. If you want to create an encryption key, click **Next**.
4. Click **Finish**.
5. Check the settings, and then enter the task name in **Task Name**.
6. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**, and then click **Apply**. If you want the **Task** window to open after you click **Apply**, select **Go to tasks window for status**.
7. In the message that appears asking whether to apply the setting to the storage system, click **OK**.

Deleting backup encryption keys from the server

Use this procedure to delete a 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 another backed up encryption key.

Before you begin

- Create the secondary back up of the encryption key. See [Backing up encryption keys \(on page 37\)](#).
- Verify that the key is not allocated to the parity group.
- You must have the Security Administrator (View & Modify) role.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. Expand **Administration** in the **Explorer** pane, and select **Encryption Keys**.
3. On the **Encryption Keys** tab, click **View Backup Keys on Server**.
4. 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**.

5. In the **Delete Backup Keys on Server** window, confirm the settings, and enter your task name in **Task Name**, and then click **Apply**.
If you want the **Task** window to open after you click **Apply**, select **Go to tasks window for status**.
6. In the message that appears asking whether to apply the setting to the storage system, click **OK**.

Result

The data encryption key is deleted.

Exporting a list of encryption keys

You can output a list of encryption keys and their details that are shown in the Encryption Keys window. Output data includes key IDs, the dates and times the encryption keys were created on, the key attributes (CEK, DEK, KEK, or Free), the resources to which the encryption keys are assigned, the paths to which the keys were created, and the number of key backups.

Before you begin

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

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. Select **Administration** in **Explorer**, and select **Encryption Keys**.
The **Encryption Keys** window is opened.
3. On the **Encryption Keys** tab, select the key ID for the data encryption key information you want to output from the **Encryption Keys** table.
4. Click **More Actions** > **Export**.
5. When the **Ready to Download** message appears, click **OK**.

Rekeying key encryption keys

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

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

Before you begin

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

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. Select **Administration** in **Explorer**, and select **Encryption Keys**.
The **Encryption Keys** window is opened.

3. On the **Encryption Keys** tab, select the key ID for the data encryption key information you want to output from the **Encryption Keys** table.
4. Click **More Actions > Rekey Key Encryption Keys**.
5. In the **Rekey Key Encryption Key** window, confirm the settings, and enter your task name in **Task Name**.

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

Click **Apply**.

Rekeying certificate encryption keys

If you change certificate encryption keys, use the following procedure to rekey the keys. After rekeying certificate encryption keys, it is recommended that you back up each key.

Before you begin

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

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. Select **Administration** in **Explorer**, and select **Encryption Keys**. The **Encryption Keys** window is opened.
3. On the **Encryption Keys** tab, select **Rekey Certificate Encryption Keys**.
4. In the **Rekey Certificate Encryption Keys** window, confirm the settings, and enter your task name in **Task Name**.

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

Click **Apply**.

Retrying Key Encryption Key Acquisition

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

Before you begin

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

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. Select **Administration** in **Explorer**, and select **Encryption Keys**. The **Encryption Keys** window is opened.
3. On the **Encryption Keys** tab, select **More Actions > Retry Key Encryption Key Acquisition**.

4. In the **Retry Key Encryption Key Acquisition** window, confirm the settings, and enter your task name in **Task Name**.

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

Click **Apply**.

Result

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

Initializing the encryption environment settings

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

Before you begin

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

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. Select **Administration** in **Explorer**, and select **Encryption Keys**. The **Encryption Keys** window is opened.
3. On the **Encryption Keys** tab, select **Edit Encryption Environmental Settings**.
4. In the **Edit Encryption Environmental Settings** window, select **Initialize Encryption Environmental Settings**.
5. Select **Finish** to display the **Confirm** window.
6. In the **Confirm** window, confirm the settings, and enter your task name in **Task Name**.

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

Click **Apply**.

Chapter 9: Troubleshooting

This chapter provides troubleshooting information for Encryption License Key.

Encryption events in the audit log

The audit log records events related to Encryption License Key, including data encryption and Encryption License Key processes. You can export an audit log that contains encryption events in near real-time to an external syslog server.

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

Troubleshooting Encryption License Key

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

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

| Problem | Action |
|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cannot use the Encryption License Key feature to back up or restore a key. | <p>Verify the following:</p> <ul style="list-style-type: none"> ▪ The Encryption License Key software license is valid and installed. ▪ You have the Security Administrator (View & Modify) role. ▪ If you backup and restore data encryption keys with a key management server, the connection to the key management server is available. ▪ If you backup and restore data encryption keys with a key management server, the number of keys which you can back up on the key management server is not exceeded. ▪ If you backup and restore data encryption keys with a key management server, a time-out has not occurred due to the increase in the number of keys on the key management server. ▪ The latest key is restored (the key will not be updated after a secondary backup has been performed). |
| Cannot create or delete data encryption keys. | <p>Make sure that:</p> <ul style="list-style-type: none"> ▪ The Encryption License Key software license is valid and installed. ▪ You have the Security Administrator (View & Modify) role. ▪ If you have backed up and restored data encryption keys with a key management server, that the connection to the key management server is available. |
| Cannot enable encryption for a parity group. | <p>Make sure that:</p> <ul style="list-style-type: none"> ▪ 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. |
| Cannot disable encryption for a parity group. | <p>Make sure that all LDEVs in the parity group are in the blocked status.</p> |

| Problem | Action |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server configuration test failed. | <p>Check the following key management server connection settings:</p> <ul style="list-style-type: none"> ▪ Host name ▪ Port number ▪ Client certificate file ▪ Root certificate file <p>If the communication failure is due to the length of time to connect to the server, try changing these settings:</p> <ul style="list-style-type: none"> ▪ Timeout ▪ Retry interval ▪ Number of retries |
| The Edit Encryption wizard operation failed, but the status of encryption (enable or disable) has changed. | The change of the status succeeds, but the format of the volume fails. Confirm the message, remove the error, and format volumes again. |
| The storage system failed to get encryption keys backed up on the key management server and all volumes are blocked when the storage system is turned on. The SIM code 661000 or 661001 is returned. | <p>Complete the following tasks:</p> <ul style="list-style-type: none"> ▪ Restore the connection to the key management server. ▪ Retry key encryption key acquisition. ▪ Contact customer support to restore the EBEDs and blocked drives or blocked volumes. |
| Editing encryption environmental settings has failed with the error (00002-058578). | <p>If it is the first time you are configuring encryption environmental settings in the Edit Encryption Environmental Settings window and it fails (error message 00002-058578), complete the following tasks:</p> <ol style="list-style-type: none"> 1. Wait a few minutes, and then click File > Refresh All to reread the configuration information. 2. Initialize the encryption environmental settings. 3. Configure the encryption environmental settings again. <p>If it is not the first time you are configuring encryption environmental settings in the Edit Encryption Environmental Settings window and it fails (error message 00002-058578), complete the following tasks:</p> <ol style="list-style-type: none"> 1. Wait a few minutes, and then click File > Refresh All to reread the configuration information. 2. Configure the encryption environmental settings again. |

| Problem | Action |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server configuration test has succeeded, but the following error is displayed: 10126-105022 The connected key management server does not support the required functions. | A required function for the setting of the key management server is not supported with the connected key management server. See System requirements (on page 29) , and update the software of the key management server to the latest version. |
| The Edit Encryption Wizard operation failed though the Free key (Encryption key with the Free attribute) exists. The error below is displayed. 03005-108104 There are not enough Free keys. | The Edit Encryption Environmental Settings wizard executed prior to the Edit Encryption wizard might have failed because of disk board failure. Confirm in the Task window that the Edit Encryption Environmental Settings wizard failed and if so, move the cause of error. Then retry the Edit Encryption Environmental Settings wizard and the Edit Encryption wizard after initializing the Encryption Environmental Setting . |
| 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. |

Contacting customer support

When contacting customer support, provide as much information about the problem as possible, including:

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

The customer support center is available 24 hours a day, seven days a week. If you need technical support, log on to customer support for contact information: <https://support.hitachivantara.com/en-us/contact-us.html>

Appendix A: Encryption License Key GUI reference

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

Encryption Keys window

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

Encryption Keys Last Updated : 2014/02/03 13:39

Encryption Keys

[Edit Encryption Environmental Settings](#) [View Backup Keys on Server](#)

| | | |
|---------------------------|----------------------------|--------------------------|
| Number of Encryption Keys | Data Encryption Key | 17 |
| | Certificate Encryption Key | 8 |
| | Free | 4067 (Max Allowed: 4096) |

Encryption Keys

Create Keys Backup Keys Restore Keys More Actions

Selected: 0 of 4093

Filter ON OFF Select All Pages Column Settings Options 1 / 5

| Key ID | Created | Attribute | Assigned to | Generated on | Number of Backups |
|--------|---------------------|-----------|-------------|----------------|-------------------|
| - | 2014/01/16 04:12:04 | CEK | DKA-2P... | Disk Contro... | 0 |
| - | 2014/01/16 04:12:04 | CEK | DKA-2P... | Disk Contro... | 0 |
| - | 2014/01/16 04:12:04 | CEK | DKA-2P... | Disk Contro... | 0 |
| - | 2014/01/16 04:12:04 | CEK | DKA-2P... | Disk Contro... | 0 |
| - | 2014/01/16 04:12:01 | CEK | DKA-1P... | Disk Contro... | 0 |
| - | 2014/01/16 04:12:01 | CEK | DKA-1P... | Disk Contro... | 0 |
| - | 2014/01/16 04:11:59 | CEK | DKA-1P... | Disk Contro... | 0 |
| - | 2014/01/16 04:11:59 | CEK | DKA-1P... | Disk Contro... | 0 |
| 12 | 2014/01/16 04:10:57 | DEK | HDD000... | Disk Contro... | 0 |
| 13 | 2014/01/16 04:10:57 | DEK | HDD002... | Disk Contro... | 0 |
| 14 | 2014/01/16 04:10:57 | DEK | HDD004... | Disk Contro... | 0 |
| 15 | 2014/01/16 04:10:57 | DEK | HDD006... | Disk Contro... | 0 |
| 16 | 2014/01/16 04:10:57 | DEK | HDD001... | Disk Contro... | 0 |
| 17 | 2014/01/16 04:10:57 | DEK | HDD003... | Disk Contro... | 0 |
| 18 | 2014/01/16 04:10:57 | DEK | HDD005... | Disk Contro... | 0 |
| 19 | 2014/01/16 04:10:57 | DEK | HDD007... | Disk Contro... | 0 |
| 20 | 2014/01/16 04:10:57 | DEK | HDD010... | Disk Contro... | 0 |
| 21 | 2014/01/16 04:10:57 | DEK | HDD010... | Disk Contro... | 0 |
| 22 | 2014/01/16 04:10:57 | DEK | HDD010... | Disk Contro... | 0 |
| 23 | 2014/01/16 04:10:57 | DEK | HDD012... | Disk Contro... | 0 |
| 24 | 2014/01/16 04:10:57 | DEK | HDD012... | Disk Contro... | 0 |
| 25 | 2014/01/16 04:10:57 | DEK | HDD014... | Disk Contro... | 0 |
| 26 | 2014/01/16 04:10:57 | DEK | HDD014... | Disk Contro... | 0 |
| 27 | 2014/01/16 04:10:57 | DEK | HDD016... | Disk Contro... | 0 |
| 28 | 2014/01/16 04:10:57 | DEK | HDD016... | Disk Contro... | 0 |
| 29 | 2014/01/16 04:10:57 | Free | | Disk Contro... | 0 |
| 30 | 2014/01/16 04:10:57 | Free | | Disk Contro... | 0 |
| 31 | 2014/01/16 04:10:57 | Free | | Disk Contro... | 0 |
| 32 | 2014/01/16 04:10:57 | Free | | Disk Contro... | 0 |
| 33 | 2014/01/16 04:10:57 | Free | | Disk Contro... | 0 |
| 34 | 2014/01/16 04:10:57 | Free | | Disk Contro... | 0 |
| 35 | 2014/01/16 04:10:57 | Free | | Disk Contro... | 0 |
| 36 | 2014/01/16 04:10:57 | Free | | Disk Contro... | 0 |
| 37 | 2014/01/16 04:10:57 | Free | | Disk Contro... | 0 |
| 38 | 2014/01/16 04:10:57 | Free | | Disk Contro... | 0 |
| 39 | 2014/01/16 04:10:57 | Free | | Disk Contro... | 0 |

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 | <p>Shows the number of data encryption keys:</p> <ul style="list-style-type: none"> Data Encryption Key: Number of data encryption keys Certificate Encryption Key: Number of certificate encryption keys Free: Number of Free keys (Number of keys that can be created)The number of key encryption keys are not included. |

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

Encryption Keys tab

Use the Encryption Keys tab to view a list of the data encryption 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 | <p>Select From File to open the Restore Keys from File window.</p> <p>Select From Server to open the Restore Keys from Server window.</p> |
| More Actions | <p>Select Rekey Key Encryption Keys to display the Rekey Key Encryption Keys window.</p> <p>Select Delete Keys from the list to delete a selected data encryption key.</p> <p>Select Retry Key Encryption Key Acquisition to display the Retry Key Encryption Key Acquisition window.</p> <p>Select Export from the list to open the window for outputting table information.</p> |

Edit Encryption Environmental Settings wizard

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

Edit Encryption Environmental Settings window

After the encryption environmental settings are configured for the first time during installation, items in the **Edit Encryption Environmental Settings** window can be changed under the following conditions:

- When the key management server is not in use.
- When local key generation is disabled.
- When the key encryption key for the key management server is stored on the storage system.
- When the Enable Encryption Key Regular Backup to Key Management Server option is enabled and you need to change the regular backup schedule or 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: (1-65535)

Timeout (sec.): (1-999)

Retry Interval (sec.): (1-60)

Number of Retries: (1-50)

Client Certificate File Name:

Password:

Root Certificate File Name:

Secondary Server: ☐ Enable ☒ Disable

Host Name: ☐ Identifier ☐ IPv4 ☐ IPv6

Port Number: Timeout (sec.):

Retry Interval (sec.): Number of Retries:

Client Certificate File Name:

Password:

Root Certificate File Name:

| Item | Description |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Key Management Server | <p>Select whether to use the key management server:</p> <ul style="list-style-type: none"> Enable: (default) key management server is used Disable: key management server is not used |
| Server Setting | <p>When you use the key management server, the following items display:</p> <ul style="list-style-type: none"> Primary server Secondary server Server Configuration test |
| Primary Server | <p>Specify the primary server information.</p> <ul style="list-style-type: none"> Host Name: Enter the host name of the key management server. Identifier: Enter the host identifier. IPv4: Enter the host IPv4 address. IPv6: Enter the host IPv6 address. Port number: Enter the port number of the key management server. Values: 1 to 65535. Default: 5696. |

| Item | Description |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <ul style="list-style-type: none"> ▪ Timeout (sec.): Enter the time until the connection attempt to the key management server times out. Values: 1 to 999. Default: 60. ▪ Retry Interval (sec.): Enter the interval to retry the connection to the key management server. Values: 1 to 60. Default: 1. ▪ Number of Retries: Enter the number of times to retry the connection to the key management server. Values: 1 to 50. Default: 3. ▪ Client Certificate File Name: Select the client certificate file for connecting to the key management server. Click Browse and select the file. ▪ Browse: Select the client certificate file. The form of the client certificate is PKCS#12. For information about the client certificate file, contact the server or network administrator. The file name appears in the Client Certificate File Name field. ▪ Password: Enter the password for the client certificate. Character limits: 0 to 128. Valid characters: Numbers (0 to 9) Upper case: (A-Z) Lower case: (a-z) Symbols: ! # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~ ▪ Root Certificate File Name: Select the root certificate file for connecting to the key management server. Click Browse and select the file. ▪ Browse: Select the root certificate file. The form of the client certificate is X.509. If you do not know about the root certificate file, contact the server administrator or the network administrator. The name of the selected file appears in the Root Certificate File Name field. |
| Secondary Server | When the secondary server is set to Enable, the same settings can be specified as the primary server. |

| Item | Description |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | Note: You must select Enable for Secondary Server before you can select Protect the Key Encryption Key at the Key Management Server or Disable local key generation. |
| Server Configuration Test | Select Check to start a server connection test for the key management server based on the specified settings. |
| Check | Start a server connection test for the key management server based on the specified settings |
| Result | Shows the result of the server connection test for the key management server |
| 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, you want to back up encryption keys. Check Select All to schedule hourly backups. |
| Regular Backup User | <p>Defines the regular backup user.</p> <ul style="list-style-type: none"> ▪ User Name: Enter the user name of the regular backup user. ▪ Password Enter the password of the regular backup user. <p>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.</p> |
| Generate Encryption Keys on Key Management Server | Checks when encryption keys are created on a key management server |
| Protect the Key Encryption Key at the Key Management Server | <p>Specifies when key encryption keys are saved on key management servers. If Warning is displayed, confirm the content of the warning, and select I Agree.</p> <p>Note: This item cannot be selected if Disable is selected for Secondary Server.</p> |

| Item | Description |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Delete Internal Encryption Keys at PS OFF | <p>Select this option to save the encryption key in the key management server, and to delete the encryption key in the storage system when it is turned off. When you select this check box, Warning appears. Confirm the content of the warning, and select I Agree.</p> <p>Note: When Disable is selected for Secondary Server, you cannot select the check box.</p> |
| Disable local key generation | <p>Specifies when encryption keys are created on the key management server and that encryption keys cannot be created on the storage system. If Warning is displayed, confirm the content of the warning, and select I Agree.</p> <p>Caution: If you select this option and select I Agree when prompted, you will not be able to undo this action or restore the settings.</p> <p>Note: This item cannot be selected if Disable is selected for Secondary Server.</p> |
| Initialize Encryption Environmental Settings | Select to initialize the encryption environmental settings |

| Item | Description |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Primary Server | <p>Displays the primary server information.</p> <ul style="list-style-type: none"> ▪ Key Management Server: Shows whether the key management server is used <ul style="list-style-type: none"> 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 |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <ul style="list-style-type: none"> ▪ 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 | <ul style="list-style-type: none"> ▪ 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 | <p>Displays whether encryption keys are created on a key management server.</p> <ul style="list-style-type: none"> ▪ 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 | <p>Displays whether key encryption keys are saved on key management servers.</p> <ul style="list-style-type: none"> ▪ 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 |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>Yes: Saves the encryption key in the key management server, and deletes the encryption key in the storage system when it is turned off.</p> <p>No: The encryption key in the storage system is not deleted when it is turned off.</p> |
| Disable local key generation | <p>Displays whether encryption keys are created on key management servers and encryption keys cannot be created on the storage system</p> <ul style="list-style-type: none"> ▪ Yes: Encryption keys are created on key management servers and encryption keys cannot be created on the storage system. ▪ No: Encryption keys are not created on key management servers. Encryption keys are created on storage systems. |

Create Keys wizard

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

This wizard includes the following windows:

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

Create Keys window

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

Create Keys

1.Create Keys > 2.Confirm

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

Number of Encryption Keys: (1-4049)

Back Next Finish Cancel ?

| Item | Description |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Number of Encryption Keys | <p>Enter the number of encryption keys to be created. The number you enter must be within the specified range.</p> <p>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 DEK and Free keys from the maximum number of keys (for example, 4096 - 47 = 4049).</p> |

Create Keys confirmation window

[illegible]

| 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): | 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 |

| Item | Description |
|---------|----------------------------------------------------------------------------------------------------------------------|
| | Default: 0 |
| Symbols | <p>The minimum number of symbols that should be used for this password</p> <p>Values: 0 to 255</p> <p>Default: 0</p> |
| Total | <p>The minimum number of characters for this password</p> <p>Values: 6 to 255</p> <p>Default: 6</p> |

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.

[illegible]

| 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.

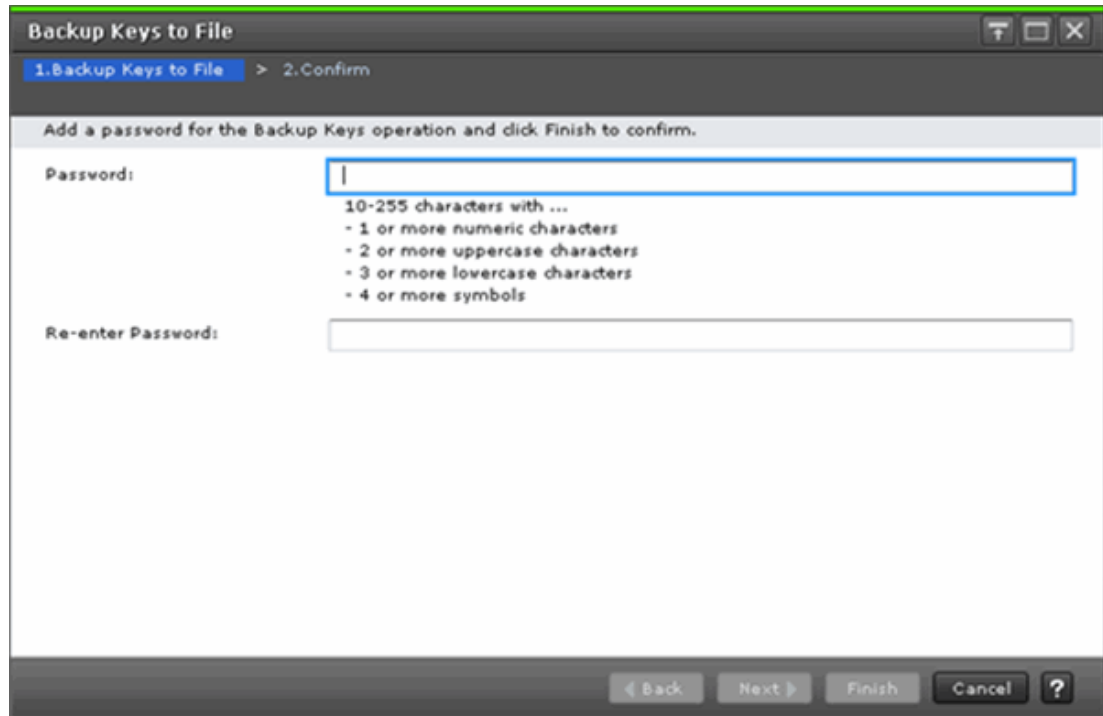
This wizard includes the following windows:

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

Backup Keys to File window

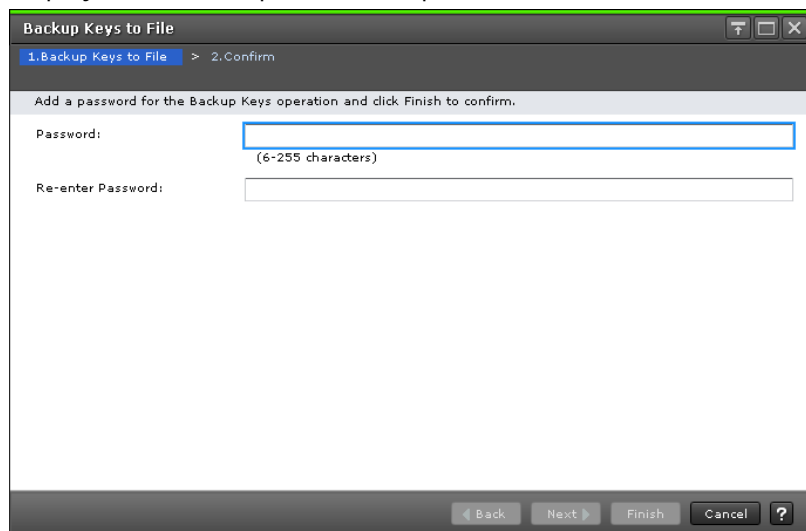
The appearance of this window depends on whether the password policy for backup encryption keys has been edited using the **Edit Password Policy (Backup Encryption Keys)** window.

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



The screenshot shows the 'Backup Keys to File' window with the '1.Backup Keys to File' step selected. The instruction reads: 'Add a password for the Backup Keys operation and click Finish to confirm.' There are two input fields: 'Password:' and 'Re-enter Password:'. The 'Password:' field is highlighted with a blue border. To its right, the following requirements are listed: '10-255 characters with ...', '- 1 or more numeric characters', '- 2 or more uppercase characters', '- 3 or more lowercase characters', and '- 4 or more symbols'. At the bottom, there are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and a help icon.

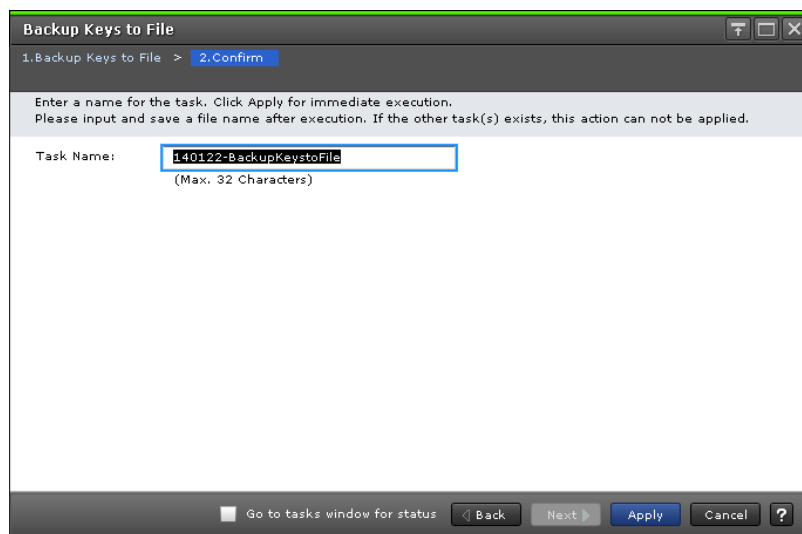
- When the backup encryption key password policy has not been edited, the window displays the default password requirements:



The screenshot shows the 'Backup Keys to File' window with the '1.Backup Keys to File' step selected. The instruction reads: 'Add a password for the Backup Keys operation and click Finish to confirm.' There are two input fields: 'Password:' and 'Re-enter Password:'. The 'Password:' field is highlighted with a blue border. Below it, the text '(6-255 characters)' is displayed. At the bottom, there are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and a help icon.

| Item | Description |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Password | <p>Password for the backup data encryption key.</p> <p>Character limits: 6 to 255</p> <p>Valid characters:</p> <ul style="list-style-type: none"> ▪ Numbers (0 to 9) ▪ Upper case (A-Z) ▪ Lower case (a-z) ▪ Symbols: ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~ <p>Note: When the backup encryption key password policy has been edited, the window displays the user-specified password requirements.</p> |
| Re-enter Password | Type the password again for confirmation. |

Backup Keys to File confirmation window



When you click Apply in the **Confirm** window, a confirmation message will appear. After you click OK, a window for saving the file for encryption keys will appear. Enter the backup file name with the extension of “.ekf” and save the file.

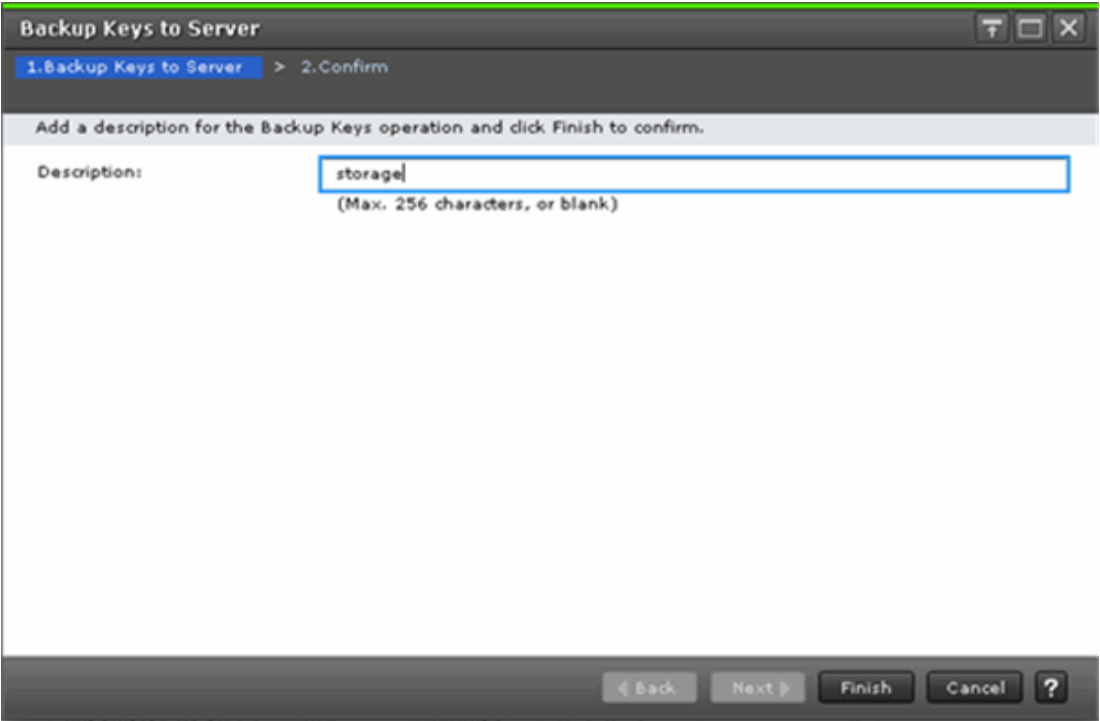
Backup Keys to Server wizard

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

This wizard includes the following windows:

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

Backup Keys to Server window



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

Backup Keys to Server confirmation window

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: (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

Restore Keys from File

1.Restore Keys from File

> 2.Confirm

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:

Browse

Password:

(6-255 Characters)

Back

Next

Finish

Cancel

?

| 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

Restore Keys from File

1.Restore Keys from File

> 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-RestoreKeysfromFile

(Max. 32 Characters)

Selected Backup Keys

| Item | Value |
|-----------|----------------|
| File Name | HMSN200163.ekf |

☐ Go to tasks window for status

Back

Next

Apply

Cancel

?

| 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

| 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**

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: (Max. 32 Characters)

| Selected Backup Keys | |
|----------------------|-----------------------|
| Item | Value |
| File Name | H876_changeSN2636.ekf |

☒ Go to tasks window for status < Back Next > Apply Cancel ?

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

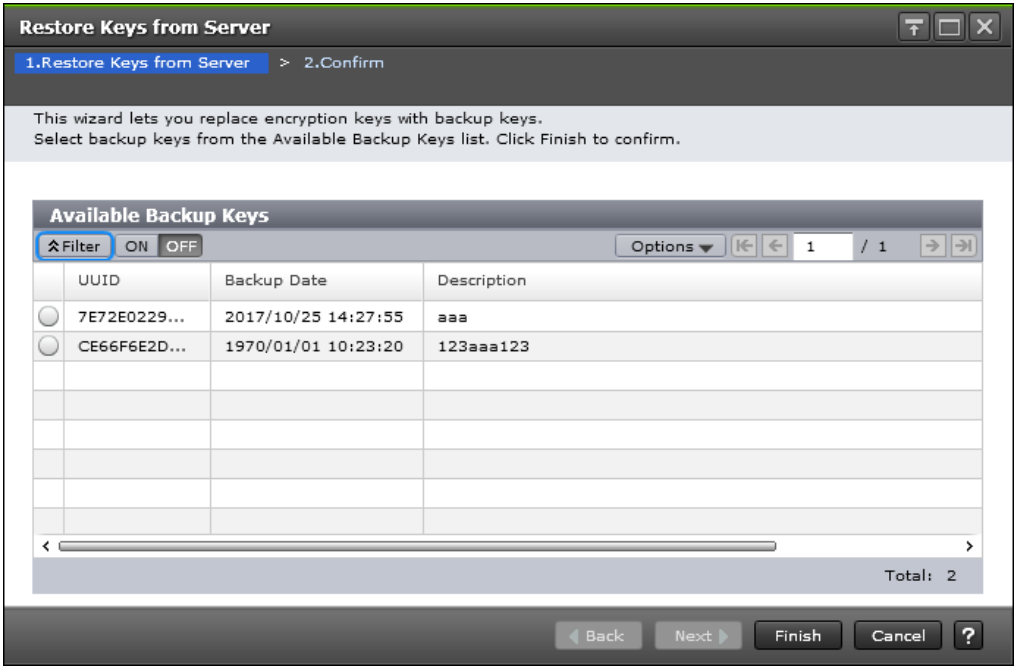
Restore Keys from Server wizard

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



| Item | Description |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UUID | Shows the UUID of the encryption key that you backed up on the key management server |
| Backup Date | Shows the time you backed up the encryption key on the key management server |
| Description | <div>Shows the description you defined when you backed up the encryption key on the key management server</div> <div>The encryption key for a regular backup is displayed in the following format:</div> <div>RegularBackup_<i>[backed-up-year-month-date_backed-up-time]</i></div> |

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: (Max. 32 Characters)

| Selected Backup Keys | | |
|----------------------|---------------------|-------------|
| UUID | Backup Date | Description |
| 4BE4E2C93... | 2014/01/21 15:06:10 | storage |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Total: 1

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

| Item | Description |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UUID | Shows the UUID of the encryption key you backed up on the key management server |
| Backup Date | Shows the time when you backed up the encryption key on the key management server |
| Description | <p>Shows the description you defined when you backed up the encryption key on the key management server</p> <p>The encryption key for a regular backup is displayed in the following format:</p> <pre>RegularBackup_[backup-year-month-date_backup-time]</pre> |

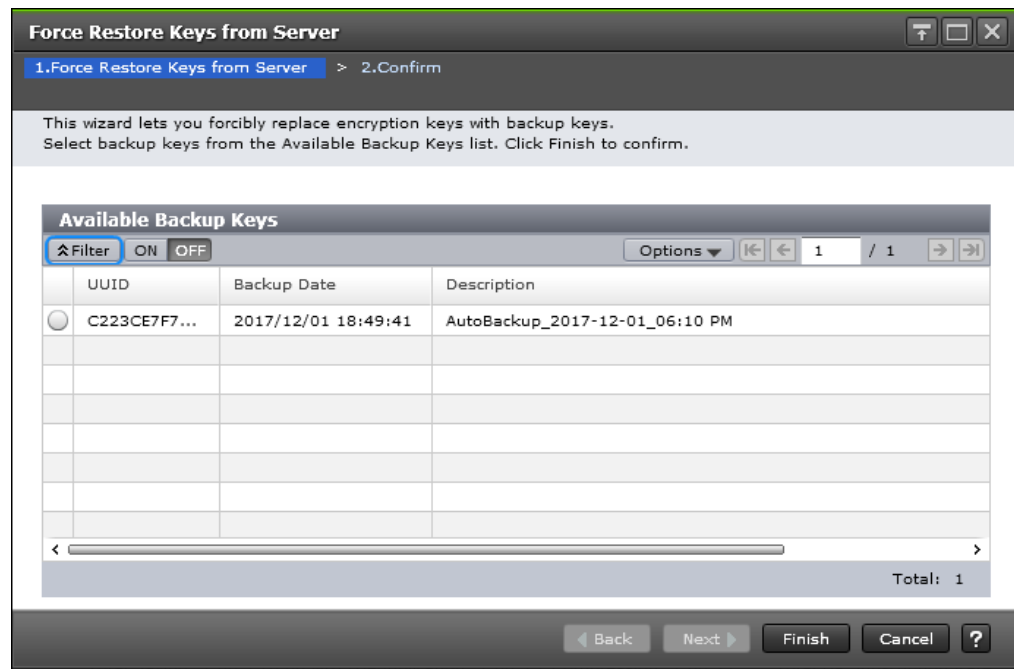
Force Restore Keys from Server wizard

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



| 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: RegularBackup_ <i>[backup-year-month-date_backup-time]</i> |

Force Restore Keys from Server confirmation window

Force Restore Keys from Server

1. Force Restore Keys from Server > 2. Confirm

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: (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 < Back Next > Apply Cancel ?

| 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: RegularBackup_ <i>[backup-year-month-date_backup-time]</i> |

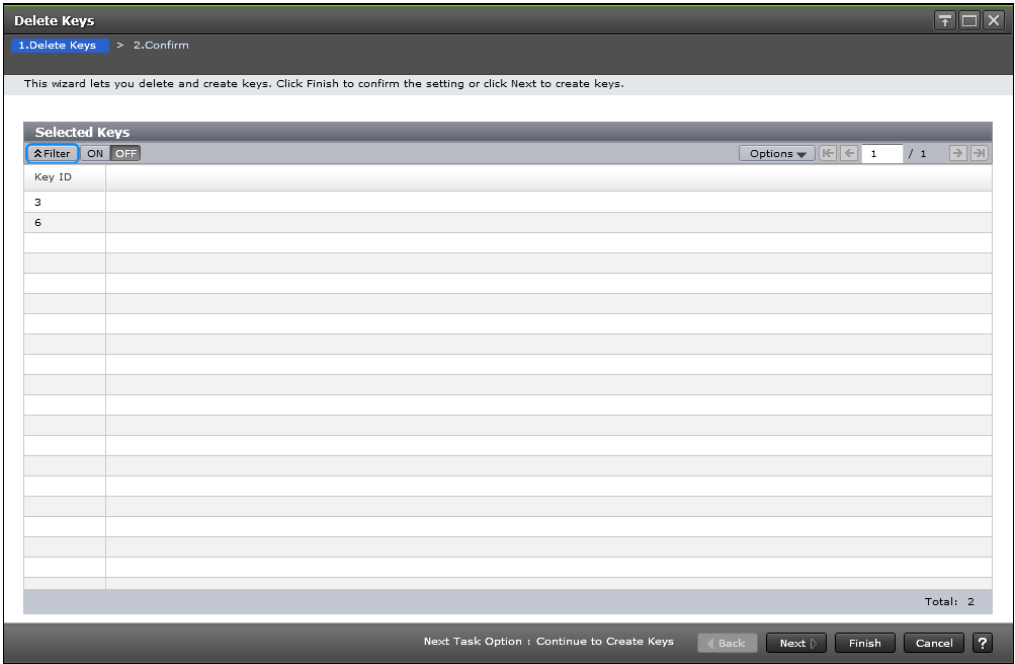
Delete Keys wizard

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

This wizard includes the following windows:

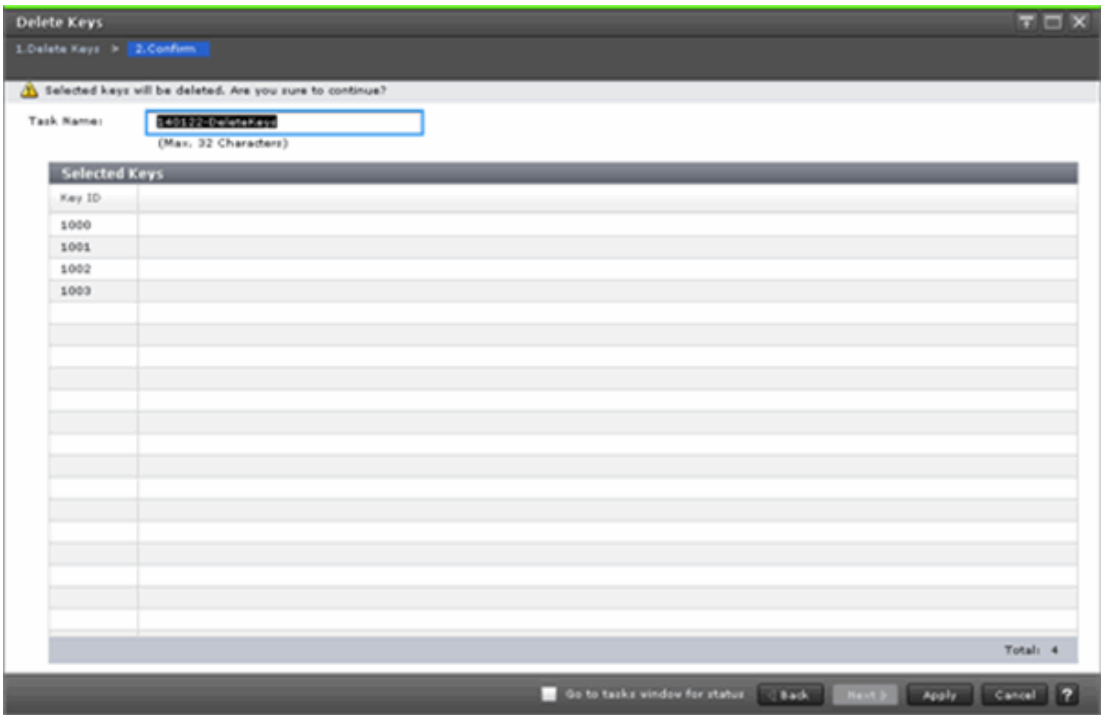
- **Delete Keys** window
- **Confirm** window

Delete Keys window



| Item | Description |
|--------|-----------------------------|
| Key ID | IDs of data encryption keys |

Delete Keys confirmation window



| Item | Description |
|--------|----------------------------------------------|
| Key ID | The identifiers for the data encryption keys |

Delete Backup Keys on Server window

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

Delete Backup Keys on Server

1. Confirm

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

Task Name: (Max. 32 Characters)

| Selected Backup Keys | | |
|----------------------|---------------------|-----------------|
| UUID | Backup Date | Description |
| 48E4E2C33... | 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

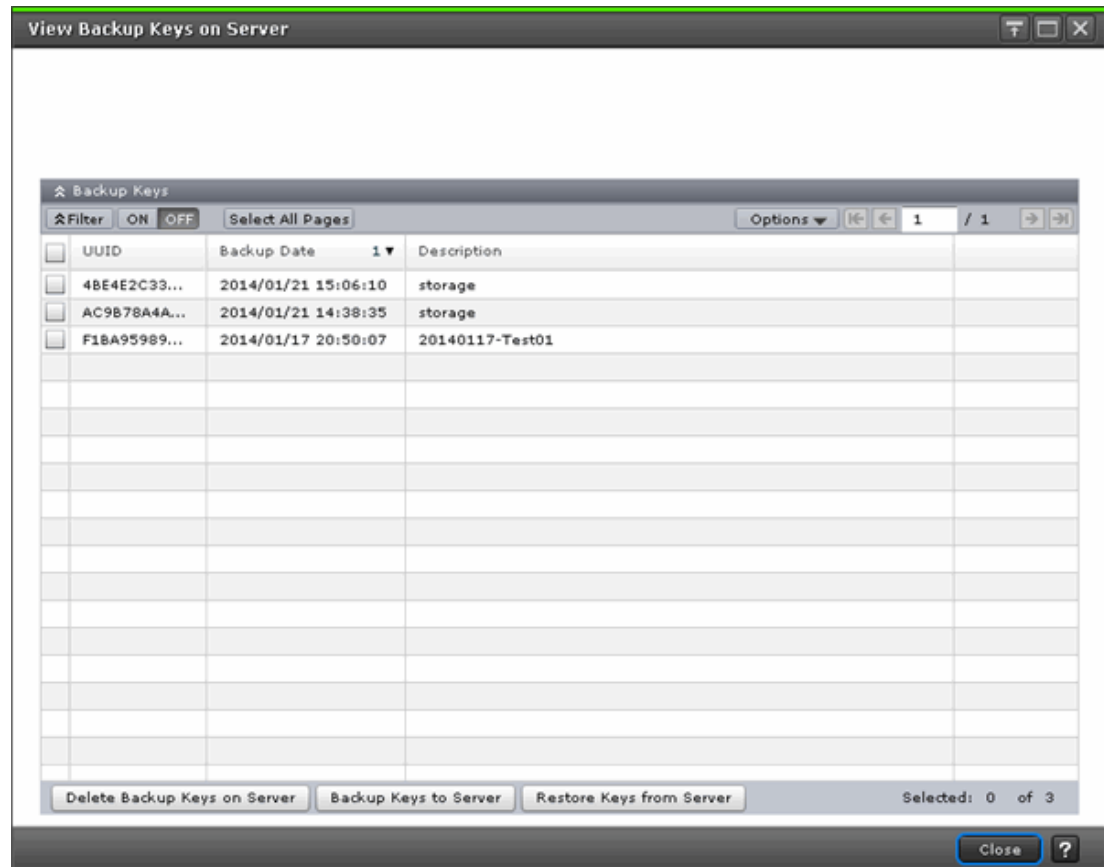
☐ Go to tasks window for status Back Next Apply Cancel ?

| Item | Description |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UUID | Shows the UUID of the encryption key you backed up on the key management server |
| Backup Date | Shows the time when you backed up the encryption key on the key management server |
| Description | Shows the description you defined when you backed up the encryption key on the key management server The encryption key for a regular backup is displayed in the following format: RegularBackup_ <i>[backup-year-month-date_backup-time]</i> |

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.

This window includes the Backup Keys table.



Backup Keys table

The Backup Keys table is shown on the **View Backup Keys on Server** window. This table lists the backup encryption keys.

| Item | Description |
|-------------|-------------------------------------------------------------------------------------------------------|
| UUID | Shows the UUID of the backup encryption key on the key management server. |
| Backup Date | Shows the time you backed up the encryption key on the key management server. |
| Description | Shows the description you defined when you backed up the encryption key on the key management server. |

| Item | Description |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>The encryption key for a regular backup is displayed in the following format:</p> <p><code>RegularBackup_[backup-year-month-date_backup-time]</code></p> |
| Delete Backup Keys on Server button | Opens the Delete Backup Keys on Server window |
| Backup Keys to Server button | Open the Backup Keys to Server window |
| Restore Keys from Server button | Opens the Restore Keys from Server window |

Edit Encryption wizard

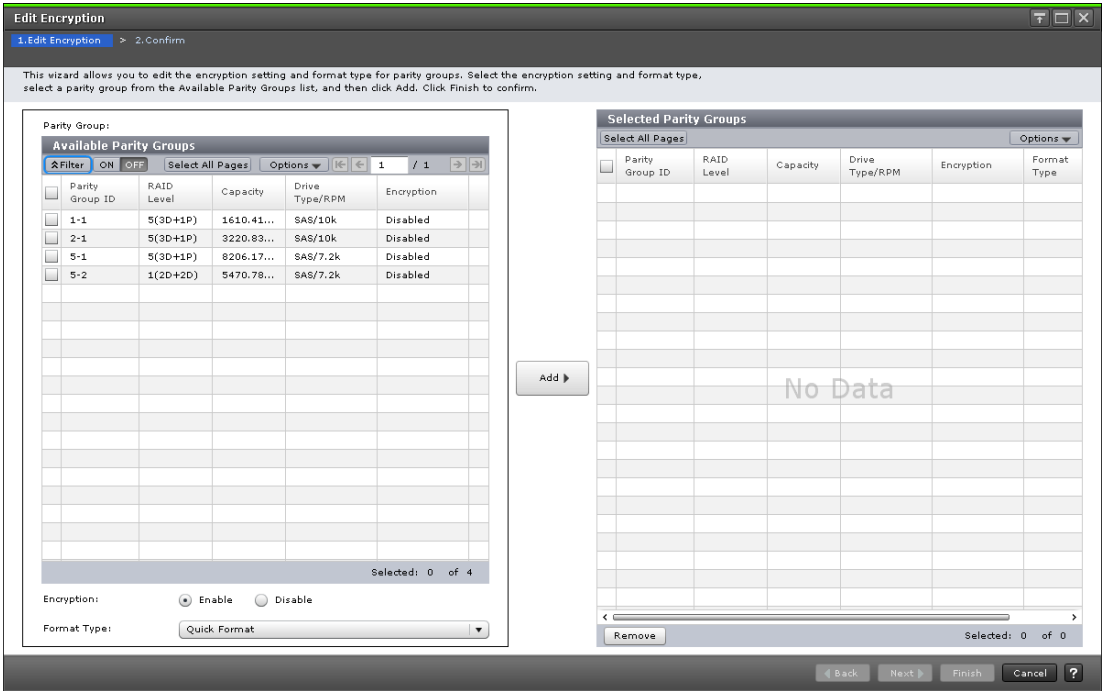
Use the Edit Encryption wizard to do the following:

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

This wizard includes the following windows:

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

Edit Encryption window



Available Parity Groups table

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

| | | | | | |
|-----------------------------------------------------------------------------------|------------|------------|------------------|------------|-------|
| Parity Groups: | | | | | |
| Available Parity Groups | | | | | |
| Filter | ON | OFF | Select All Pages | Options | 1 / 1 |
| Parity Group ID | RAID Level | Capacity | Drive Type/RPM | Encryption | |
| 1-1 | 5(3D+1P) | 1610.41... | SAS/10k | Disabled | |
| 2-1 | 5(3D+1P) | 3220.83... | SAS/10k | Disabled | |
| 5-1 | 5(3D+1P) | 8206.17... | SAS/7.2k | Disabled | |
| 5-2 | 1(2D+2D) | 5470.78... | SAS/7.2k | Disabled | |
| Selected: 0 of 4 | | | | | |
| Encryption: <input checked="" type="radio"/> Enable <input type="radio"/> Disable | | | | | |
| Format Type: Quick Format | | | | | |
| Add | | | | | |

| Item | Description |
|-----------------|------------------------------------------|
| Parity Group ID | Shows the parity group IDs |
| RAID Level | Shows the RAID level of the parity group |

| Item | Description |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | For an interleaved parity group, the interleaved number appears after the RAID level. Example: 1(2D+2D)*2 |
| Capacity | Shows the total capacity (unit) of the parity group |
| Drive Type/RPM | Shows the drive types and RPM (rotation per minute) of the LDEV in the parity group |
| Encryption | Shows the encryption setting for the parity group. <ul style="list-style-type: none"> ▪ Enabled: Encryption is enabled. ▪ Disabled: Encryption is disabled. <p>If accelerated compression of the parity group is enabled, do not select Enable for Encryption. If you select Enable for Encryption, an error occurs when performing the task.</p> |
| Format Type | Select the format types of the parity group. You do not need to format volumes when there are none in the selected parity group. Therefore, the format type in the Selected Parity Groups list becomes a hyphen (-) regardless of the status of the format type. |

Add

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

Selected Parity Groups table

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

[illegible]

| Item | Description |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parity Group ID | Shows parity group IDs |
| RAID Level | Shows the RAID level of the parity group For an interleaved parity group, the interleaved number appears after the RAID level. Example: 1(2D+2D)*2 |
| Capacity | Shows the total capacity (unit) of the parity group |
| Drive Type/RPM | Shows the drive types and RPM (rotation per minute) of the LDEV in the parity group |
| Encryption | Shows the encryption setting for the parity group: <ul style="list-style-type: none"> ▪ Enable: Encryption is enabled. ▪ Disable: Encryption is disabled |
| Format Type | Shows the format types of the parity group |

| Item | Description |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | You do not need to format volumes when there are none in the selected parity group. Therefore, the format type in the Selected Parity Groups list becomes a hyphen (-) regardless of the status of the format type. |
| Remove | Removes parity groups from the Selected Parity Groups table |

Edit Encryption confirmation window

Use the **Confirm** window to confirm the changes to the data encryption key and to view a list of the selected parity groups related to the data encryption key.

Selected Parity Groups table

Use the Selected Parity Groups table to view a list of the selected parity groups related to the data encryption key.

| Item | Description |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Parity Group ID | Shows parity group identifier |
| RAID Level | Shows the RAID level of the parity group For an interleaved parity group, the interleaved number appears after the RAID level. |

| Item | Description |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | Example: 1(2D+2D)*2 |
| Capacity | Shows the total capacity of the parity group |
| Drive Type/RPM | Shows the drive types and RPM (rotation per minute) of the LDEV in the parity group |
| Encryption | Encryption setting for the parity group: <ul style="list-style-type: none"> ▪ Enable - encryption enabled ▪ Disable - no encryption |
| Format Type | Shows the format types of the parity group You do not need to format volumes when there are no volumes in the selected parity group. Therefore, the format type in the Selected Parity Groups list becomes "-" (a hyphen) regardless of the status of Format Type. |

Rekey Certificate Encryption Keys window

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

Rekey Certificate Encryption Keys

1. Confirm

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

Task Name:

(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. |

Rekey Key Encryption Key window

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

Rekey Key Encryption Key

1. Confirm

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

Task Name:

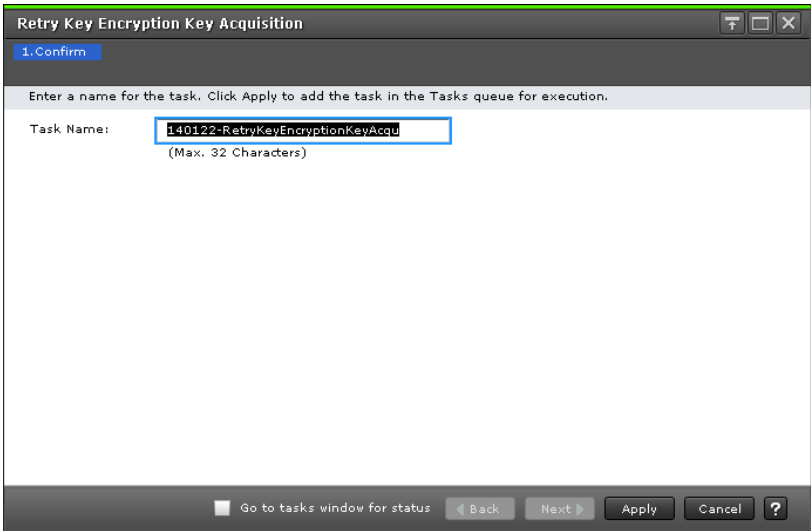
(Max. 32 Characters)

☐ 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. |

Retry Key Encryption Key Acquisition window

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



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

Glossary

audit log

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

back end module (EBEM)

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

back-end director (BED)

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

BED

See back-end director.

BEM

See *back end module (BEM)*.

disk array

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

disk controller (DKC)

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

DKA

disk adapter. Another name for a back-end director (BED).

EBED

See *encrypting back end director (EBED)*.

EBEM

See *encrypting back end module (EBEM)*.

encrypting back end module (EBEM)

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

encrypting back-end director (EBED)

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

flash module

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

FMD

See flash module

key management server

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

keypair

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

license key

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

logical device (LDEV)

An individual logical data volume (on multiple drives in a RAID configuration) in the storage system. An LDEV may or may not contain any data and may or may not be defined to any hosts. Each LDEV has a unique identifier or "address" within the storage system composed of the logical disk controller (LDKC) number, control unit (CU) number, and LDEV number. The LDEV IDs within a storage system do not change. An LDEV formatted for use by mainframe hosts is called a logical volume image (LVI). An LDEV formatted for use by open-system hosts is called a logical unit (LU).

parity group

See RAID group.

PG

parity group. See RAID group.

pool

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

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

pool volume (pool-VOL)

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

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

quick format

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

quick restore

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

service information message (SIM)

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

service processor

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

shared memory

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

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

shredding

See volume shredding.

SIM

See service information message.

SM

shared memory

SN

Device Manager - Storage Navigator

SOM

See system option mode.

SSD

solid-state drive. Also called flash drive.

SVP

See *service processor*.

syslog

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

system option mode (SOM)

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

V-VOL

virtual volume

virtual volume (V-VOL)

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

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

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

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

volume (VOL or vol)

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

volume shredding

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

Hitachi Vantara Corporation



Corporate Headquarters

2535 Augustine Drive

Santa Clara, CA 95050-2639 USA

www.HitachiVantara.com | community.HitachiVantara.com

Regional Contact Information

Americas: +1 866 374 5822 or info@hitachivantara.com

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

Asia Pacific: + 852 3189 7900 or info.marketing.apac@hitachivantara.com