HITACHI
Inspire the Next

Hitachi Unified Storage VM Block Module
Hitachi Storage Navigator User Guide

Hitachi Data Systems

Contents

3 Getting started using Storage Navigator... 3-1

4 Setting up and managing user accounts... 4-1

8 Troubleshooting

A Storage configuration reports

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Preface

This document provides information to help you set up Hitachi Storage Navigator for the Hitachi Unified Storage VM (HUS VM), set up end-user computers and web browsers, and establish user accounts and permissions. It explains the GUI features and provides basic navigation information.

Complete information for performing specific tasks in Storage Navigator is contained in the HUS VM software user guides.

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

☐ Intended audience

☐ Release notes

☐ Product version

☐ Document revision level

☐ Changes in this revision

☐ Referenced documents

☐ Document conventions

☐ Convention for storage capacity values

☐ Accessing product documentation

☐ Getting help

☐ Comments

Intended audience

This document is intended for system administrators, Hitachi Data Systems representatives, and authorized service providers who are involved in installing, configuring, and operating the Hitachi Unified Storage VM storage system.

Readers of this document should be familiar with the following:

- Data processing and RAID storage systems and their basic functions.
- The Hitachi Unified Storage VM storage system and the Storage Navigator software that runs on it.
- The operating system and web browser software on the system hosting the Storage Navigator software.
- The Unified Storage VM storage system and the *Hitachi Unified Storage VM Block Module Hardware User Guide*.

Release notes

The Hitachi Unified Storage VM release notes provide information about the HUS VM microcode (DKCMAIN and SVP), including new features and functions and changes. The Release Notes are available on Hitachi Data Systems Support Connect: https://support.hds.com/en_us/documents.html.

Product version

This document revision applies to HUS VM microcode 73-03-5*x* or later.

Document revision level

Revision	Date	Description
MK-92HM7016-00	September 2012	Initial release.
MK-92HM7016-01	December 2012	Supersedes and replaces MK-92HM7016-00
MK-92HM7016-02	March 2013	Supersedes and replaces MK-92HM7016-01
MK-92HM7016-03	May 2013	Supersedes and replaces MK-92HM7016-02
MK-92HM7016-04	October 2013	Supersedes and replaces MK-92HM7016-03
MK-92HM7016-05	November 2013	Supersedes and replaces MK-92HM7016-04
MK-92HM7016-06	March 2014	Supersedes and replaces MK-92HM7016-05
MK-92HM7016-07	May 2014	Supersedes and replaces MK-92HM7016-06
MK-92HM7016-08	March 2015	Supersedes and replaces MK-92HM7016-07
MK-92HM7016-09	June 2015	Supersedes and replaces MK-92HM7016-08
MK-92HM7016-10	December 2016	Supersedes and replaces MK-92HM7016-09

Revision	Date	Description
MK-92HM7016-11	October 2017	Supersedes and replaces MK-92HM7016-10

Changes in this revision

Updated the following sections:

- Added support for VSP G1500, VSP F1500.

Referenced documents

Hitachi Unified Storage VM Block Module documents:

- *Hitachi Audit Log User Guide*, MK-92HM7009
- *Hitachi Thin Image User Guide*, MK-90RD7010
- *Hitachi Unified Storage VM Block Module Performance Guide*, MK-92HM7011
- *Hitachi Unified Storage VM Block Module Provisioning Guide*, MK-92HM7012
- *Hitachi ShadowImage® User Guide*, MK-92HM7013
- *Hitachi SNMP Agent User Guide, MK-92HM7014*
- *Hitachi System Operations Using Spreadsheets*, MK-92HM7015
- *Hitachi Storage Navigator Messages*, MK-92HM7017 (includes Storage Navigator error codes)
- *Hitachi TrueCopy® User Guide, MK-92HM7018*
- *Hitachi Universal Replicator User Guide*, MK-92HM7019
- *Hitachi Universal Volume Manager*, MK-92HM7020

Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	Indicates the following: - Text in a window or dialog box, such as menus, menu options, buttons, and labels. Example: In the **Add Pair** dialog box, click **OK**. - Text appearing on screen or entered by the user. Example: The **-split** option. - The name of a directory, folder, or file. Example: The **CacheInfo.csv** file.

Convention	Description
Italic	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: copy *source-file target-file* **Note:** Angled brackets (< >) are also used to indicate variables.
`screen/code`	Indicates text that is displayed on screen or entered by the user. Example: `# pairdisplay -g oradb`
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: `# pairdisplay -g <group>` **Note:** Italic font is also used to indicate variables.
[ ] square brackets	Indicates optional values. Example: [a	b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a	b } indicates that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a	b] indicates that you can choose a, b, or nothing. { a	b } indicates that you must choose either a or b.

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

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

Convention for storage capacity values

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

Physical capacity unit	Value
1 KB	1,000 bytes
1 MB	$1,000^2$ bytes

Physical capacity unit	Value
1 GB	$1,000^3$ bytes
1 TB	$1,000^4$ bytes
1 PB	$1,000^5$ bytes
1 EB	$1,000^6$ bytes

Logical storage capacity values (logical device capacity) are calculated based on the following values:

Logical capacity unit	Value
1 KB	1,024 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
1 block	512 bytes

Accessing product documentation

Product documentation is available on Hitachi Data Systems Support Connect: https://knowledge.hds.com/Documents. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

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

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

Comments

Please send us your comments on this document: doc.comments@hds.com.
Include the document title and number, including the revision level (for
example, -07), and refer to specific sections and paragraphs whenever
possible. All comments become the property of Hitachi Data Systems
Corporation.

Thank you!

1

Storage Navigator overview

Hitachi Storage Navigator provides a unified GUI for managing and optimizing the Hitachi Unified Storage VM storage system. You access the system in Storage Navigator from any computer with a web browser. Besides the GUI, Storage Navigator provides a CLI to allow scheduling of storage system events.

Storage Navigator can be set up in either Windows or UNIX environments.

This chapter provides an overview of Storage Navigator features and components.

☐ Manage the storage system

☐ GUI feature highlights

☐ Storage Navigator CLI

☐ Storage Navigator components

Manage the storage system

With Storage Navigator, you can perform the following tasks:

- Provision storage.
- Set up data replication for restoring lost data.
- View and manage the configuration of the storage system.
- Monitor and tune performance.
- Acquire logs for actions and commands performed on the storage system.

GUI feature highlights

Storage Navigator allows you to set up and manage more than one storage system with a use-case in mind. Whether creating LDEVs or pools, adding host groups or LUN paths, enabling performance monitoring, or creating pairs for replication—these and all storage system tasks are made simpler because the GUI seamlessly crosses the underlying HUS VM software functionality. The use of wizards for major use-case tasks makes it possible to complete the set of tasks in one procedural flow, with a minimum of steps and a minimum of clicks.

The following illustration shows an example of the GUI main window.

Figure 1-1 Storage Navigator GUI

Emphasis on performance

Operations you perform are executed in the background. This means you can start the next operation without waiting for the previous one to complete.

Wizards and task management

Wizards are provided for each main task. The wizard guides you through all the subtasks that you ordinarily perform one at a time. For example, the Create LDEVs wizard guides you through a series of screens in which you create the LDEVs and add LUN paths by selecting LDEVs, selecting host groups, and mapping LUNs.

Storage Navigator also provides a window checking on the tasks you have committed to the system. The Task window provides detailed information about each task and shows the priority and status of each task you are tracking.

Reporting

Storage Navigator provides views of various aspects of your storage system. In addition to these views, you can generate a report for specific areas of the system. Reports can be generated for a summary of the system data, ports, Channel Adapters, and disk adapters. A total of 20 configuration reports can be generated. Reports are formatted in either CSV or HTML. Use these reports to determine if the storage system configurations have changed properly.

The Report Configuration Tool allows you to create a configuration report by using a command prompt. You can automate the creation or deletion of configuration reports by writing `.bat` script files. Use the Windows Task Scheduler to execute the script files at regular intervals.

Help

Storage Navigator online help provides procedural information for setting up and managing the storage system. Links to the major storage system tasks, search functions, and glossary are included.

Storage Navigator CLI

The Storage Navigator CLI allows you to perform commands on the storage system using the command prompt. To use the CLI, you need to install certain files on the Storage Navigator computer.

The CLI can be used to perform only specific operations for specific software. For details on the Storage Navigator CLI, see the *System Operations Using Spreadsheets*.

Storage Navigator components

The following figure shows an example of the Storage Navigator computer and SVP configuration.
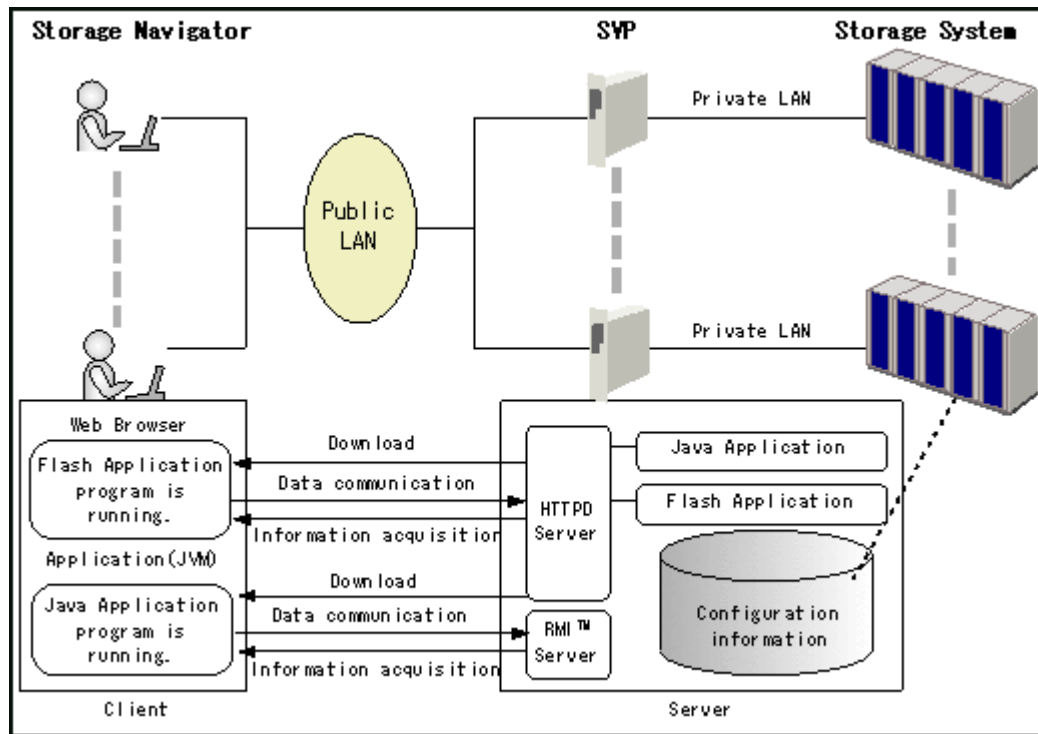
Figure 1-2 Storage Navigator and SVP configuration

2

Setting up Storage Navigator

This topic provides Storage Navigator requirements and set up procedures.

☐ Setup workflow

☐ Cable connection requirements

☐ Enabling IPv6 communication

☐ Configuring IPv6 communication in Windows 7

☐ Configuring IPv6 communication in Solaris 10

☐ Setting up SSL encryption

☐ Setting up the client computer

☐ Changing Java Security Settings

☐ Using the SMI-S function with a Storage Navigator user account

☐ Installing the report configuration tool

☐ Using the report configuration tool

☐ Enabling the compatibility view setting in Internet Explorer 11

Setup workflow

The following workflow describes the set up tasks for Storage Navigator:

- The HDS representative attaches the SVP in your storage system to the LAN. Storage Navigator is already set up on the SVP and is therefore ready for access by client computers.
- Ensure the correct LAN cabling and connections are in place. See Cable connection requirements on page 2-2.
- Set up network connections. See Enabling IPv6 communication on page 2-2, as needed. Also, you can set up additional communications security for remote operations with Secure Sockets Layer (SSL). See Setting up SSL encryption on page 2-3
- Set up the Storage Navigator computers. See Setting up the client computer on page 2-12.
- Set up user accounts. See Chapter 4, Setting up and managing user accounts on page 4-1.
- Configure Storage Navigator environment. See Chapter 5, Configuring the Storage Navigator environment on page 5-1.
- Install license keys for program products. See Chapter 6, License keys on page 6-1.

Requirements for the various elements are included in the following topics.

Cable connection requirements

The length of cables that can connect to the storage system is defined by the communication standard.

Enabling IPv6 communication

If Internet Protocol Version 6 (IPv6) addresses are used in the storage system LAN, you may need to enable IPv6 communication on the SVP. For Windows 7 and Solaris 10, you can enable IPv4 (standard) communication, IPv6 communication, or both. You determine which protocol to use based on the IP addresses that are used within the LAN. Use the same communication options for both the Storage Navigator computer and the SVP.

If you use IPv6 to display the Storage Navigator main window when both IPv4 and IPv6 are available, IPv6 addresses are displayed in the Storage Navigator secondary window but actually IPv4 communication is used.

For information on how to configure IP communication from an SVP, contact the Hitachi Data Systems customer support. The following topics give brief instructions on configuring IPv6 communication in Windows 7 and Solaris 10 environments.

Configuring IPv6 communication in Windows 7

To configure a Storage Navigator computer to use IPv6 for communication with an SVP:

1. Select **Control Panel** > **Network and Sharing Center** > **Manage network connections**.
2. Select and right-click the network where the SVP resides, and then click **Properties** in the pop-up menu.
   Click **Continue** if the User Account Control dialog box appears. Otherwise, the Networking dialog box appears.
3. Select the **Internet Protocol Version 6 (TCP/IPv6)** check box.
   Optionally, clear the **Internet Protocol Version 4 (TCP/IPv4)** check box.
4. Click **OK** to close the dialog box.

Configuring IPv6 communication in Solaris 10

To configure a Storage Navigator computer to use IPv6 for communication with an SVP:

1. Start the console.
2. Execute the following command:
   ```
   ipconfig network-interface-name inet down
   ```

Setting up SSL encryption

To improve security of remote operations from a Storage Navigator SVP to a storage system, you can set up Secure Sockets Layer (SSL) encrypted communication. By setting SSL encryption, the Storage Navigator User ID and Password are encrypted.

Note the following SSL terms:

- **Secure Sockets Layer**: SSL is a protocol first developed by Netscape to securely transmit data over the Internet. Two SSL-enabled peers use their private and public keys to establish a secure communication session, with each peer encrypting transmitted data with a randomly generated and agreed-upon symmetric key.
- **Keypair**: A keypair is two mathematically-related cryptographic keys consisting of a private key and its associated public key.
- **Server Certificate**: A Server Certificate (also called a Digital Certificate) forms an association between an identity (in this case the SVP server) and a specific keypair. A Server Certificate is used to identify the SVP server to a client so that the server and client can communicate using SSL. Server Certificates come in two basic types:
- **Self-signed**: You generate your owned self-signed certificate and the subject of the certificate is the same as the issuer of the certificate. If the

Storage Navigator computers and the SVP are on an internal LAN behind a firewall, you may find that this option provides sufficient security.

- **Signed and Trusted**: For a Signed and Trusted Server Certificate, a Certificate Signing Request (CSR) is sent to and certified by a trusted Certificate Authority (CA) such as VeriSign (http://www.verisign.com/)

If you enable SSL, you must make sure that the key pair and associated server certificate do not expire. If either the key pair or the server certificate expires, users will be unable to connect to the SVP. Server certificates require the use of a host name instead of an IP address.

Flow of SSL communication settings

The following shows a flow of required settings for SSL communication. that creation of private and public keys requires a dedicated program. Download one from the OpenSSL website (http://www.openssl.org/).
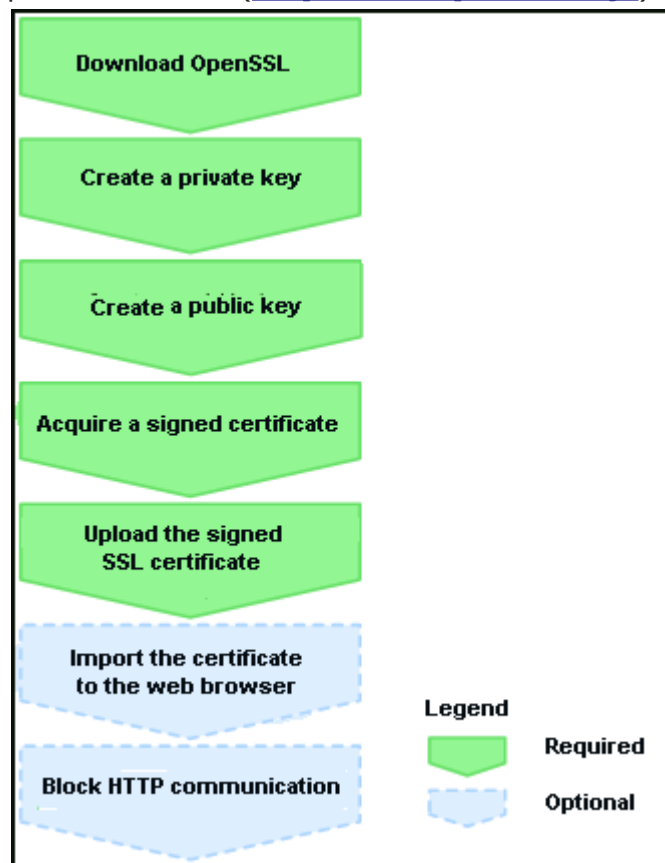
Notes on updating the signed certificate to the SVP

Read the following notes about uploading the signed certificate to the SVP:

- While the SVP certificate is being updated, tasks that are being executed or scheduled for execution on Storage Navigator are not executed.

- Certificates for RMI communication are updated asynchronously (within approximately two minutes).

- If an SVP certificate is updated during Command Suite setup operation, the Command Suite setup operation will result in an error.
- Update of the SSL certificate gives a great influence to the system and may lead to SVP failure. Therefore take sufficient care about the content of the certificate and private key to be set.
- Depending on the environment, the SVP web server restart may require 30 to 60 minutes after update of the certificate is completed. In that case, an internal server error occurs, and even after completion of the restart, the update completion dialog box for Update Certificate Files does not display, but the update of the certificate is complete.

Creating a private key (.key file)

To create a private key (.key file) in a Windows Vista environment:

1. Download OpenSSL from the OpenSSL website (http://www.openssl.org/) and install it.

   In this example, it is installed in the C:/ openssl folder.

2. See the properties of the openssl folder. If the read-only attribute is set, release it from the folder.

3. Open a command prompt.

4. Move the current directory to the folder to which the key file is output (such as c:\key), and execute the following command:

   ```
   c:\key > c:\openssl\bin\openssl genrsa -out server.key 1024
   ```

This procedure creates a file called server.key in the `c:\key` folder. This file becomes the private key.

Creating a public key (.csr file)

To create a public key (.csr file) in a Windows Vista environment:

1. Execute the following command in the command prompt.

   ```
   c:\key > c:\openssl req -sha256 -new -key server.key -config c:\openssl\bin\openssl.cfg -out server.csr
   ```

   This command uses SHA-256 as a hush algorithm. MD5 or SHA-1 is not recommended for a hush algorithm due to its low security level.

2. Enter the following information in the prompt:

   - Country Name (two-letter code)
   - State or Province Name
   - Locality Name
   - Organization Name
   - Organization Unit Name
   - Common Name
     To create a self-signed certificate, enter the IP address of the web server (SVP). To obtain a signed and trusted certificate, ensure that the server name is the same as the host name of the storage device.

- Email Address
- Challenge password (optional)
- Common name (optional)

An example of a command prompt when you create a public key is shown in the following figure.
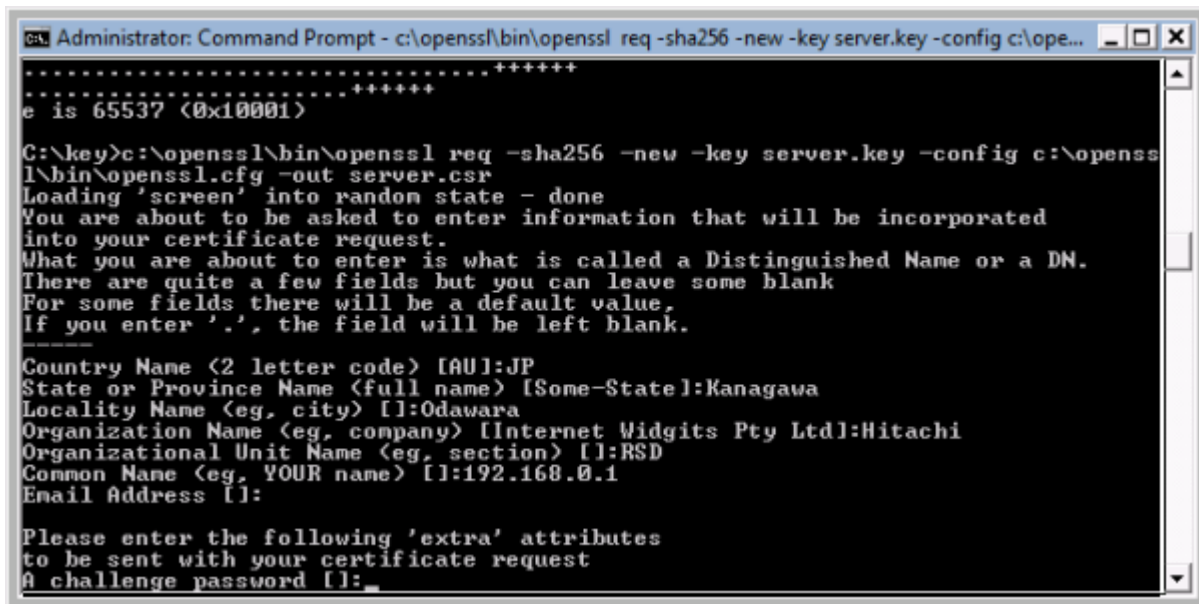
Figure 2-1 Creating a public key

Acquiring a signed certificate

Acquiring a self-signed certificate

To acquire a self-signed certificate, open the command prompt and execute the following command:

```
c:\key>c:\openssl\bin\openssl x509 -req -sha256 -days 10000 -in
server.csr -signkey server.key -out server.crt
```

This command uses SHA-256 as a hush algorithm. MD5 or SHA-1 is not recommended for a hush algorithm due to its low security level.

This creates a *server.crt* file in the *c:\key* folder, which is valid for 10,000 days. This is the signed private key, which is also referred to as a self-signed certificate.

Creating a signed and trusted certificate

If you want to create a signed and trusted certificate, you must create a certificate signing request (CSR), send that file to a Certificate Authority (CA), and request that the CA issue a signed and trusted certificate. Each certificate authority has its own procedures and requirements, and there is generally a cost for doing so. The signed and trusted certificate is the signed Public Key.

Verifying and releasing an SSL certificate passphrase

An SSL certificate cannot be applied for the SVP if the passphrase is set. If the passphrase is set, release the passphrase for the SSL certificate before applying the SSL certificate to the SVP. The following procedure explains how to verify and release the passphrase settings.

Prerequisites

- A private key (.key file) has been created.
- OpenSSL must be installed. In this procedure, it is installed in the C:\openssl folder.

Procedure

1. Open the Windows command prompt.
2. Move the current directory to the folder (for example, C:\key) where the key file is stored and execute the following command:

   Caution: Executing this command will overwrite the current key file. To prevent loss of the key file, do either of the following:

   - Back up the key file first.
   - Use a different key file input destination and output destination.

   ```
   C:\key>C:\openssl\bin\openssl rsa –in <Key file input
   destination> -out <Key file output destination>
   ```

   If **Enter pass phrase for server.key:** is displayed, the passphrase is set. Enter the passphrase. The passphrase in the SSL private key will be released and the SSL certificate can be applied to the SVP.

Example (when passphrase is set)

```
C:\key>c:\openssl\bin\openssl rsa -in server.key –out server.key
Enter pass phrase for server.key: "Enter passphrase"
Writing RSA key
```

Example (when passphrase is not set)

```
C:\key>c:\openssl\bin\openssl rsa -in server.key –out server.key
Writing RSA key
```

Uploading a signed SSL certificate

To use SSL communication, you must update and upload the private key and the signed Server Certificate (Public Key) to the SVP.

Prerequisites

- A private key (.key file) has been created. Change the file name to server.key unless the file is already named that.
- A signed public key certificate (.crt file) has been acquired. Change the file name to server.crt unless the file is already named that.

- The private key (server.key file) and the signed public key certificate (server.crt file) are in Base 64 encoded X509 format.
- The passphrase for the private key (.key file) is released.
- You must have Storage Administrator (Initial Configuration) role to perform this task.

Related information

- [Notes on updating the signed certificate to the SVP on page 2-4](#)

To upload the signed SSL certificate:

1. Log off all Storage Navigator web client sessions on the SVP.
2. Start a web browser on the Storage Navigator computer.
3. Specify the following URL to open the Tool Panel dialog box.
   ```
   http://IP-address-or-host-name-of-SVP/cgi-bin/utility/
   toolpanel.cgi
   ```

   ## Tool Panel

   | Control Panel |
   | Download Dump Files |
   | Update Certificate Files |
   | Set Up HTTP Blocking |
   | Release HTTP Blocking |
   | Update Certificate Files for SMI-S |
   | Upload Configuration Files for SMI-S |
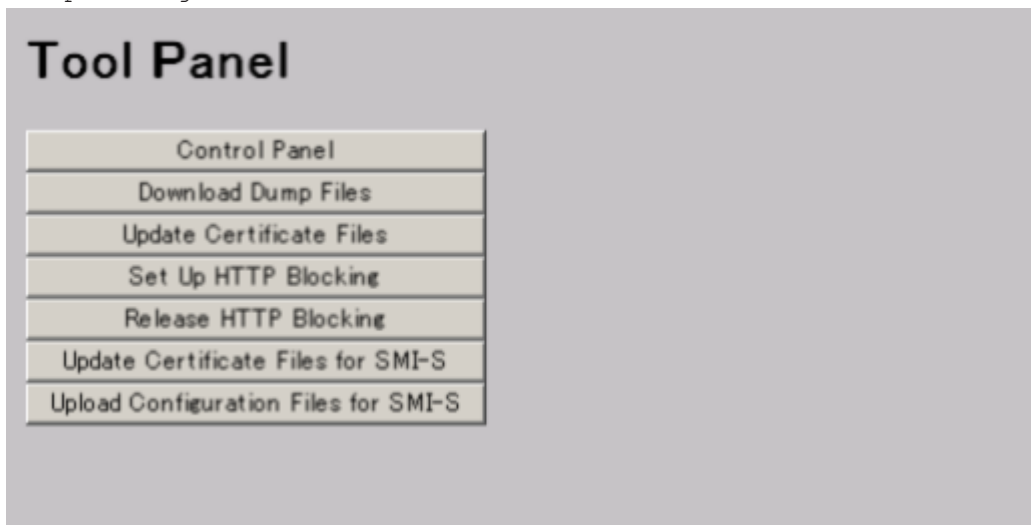
4. In the Tool Panel dialog box, click **Update Certificate Files**. If the SSL encrypted communications is set up and the Security Alert dialog box appears, click **OK**. The Security Alert dialog box for the certificate may also appear. In this case, click **View Certificate**, confirm the certificate is correct, and then click **Yes**.
5. Enter the User ID and Password for the administrator, then click **Login**. The upload dialog box for Update Certificate Files appears.
6. Enter both the public key certificate file name in the Certificate file (server.crt file) box and the private Key file (server.key file) box. You can enter the file names directly or by clicking **Browse**.
7. Click **Upload** on the upload dialog box of Update Certificate Files. The execution of Update Certificate Files confirmation dialog box appears.
8. Click **OK** to begin the certificate update. Once complete, the web server restarts and a dialog box appears.
9. Click **OK**. If the Security Alert dialog box for the certificate appears, click **View Certificate** to confirm that the certificate is correct, and click **Yes**.

If an error occurs during the certificate update, an error message will appear. Solve the problem, and restart from the logging in to **Update Certificate Files**.

Returning the Web server (SVP) certificate to default

You can return the certificate updated in <u>Uploading a signed SSL certificate on page 2-7</u> to default.

Prerequisites

- You must have Storage Administrator (Initial Configuration) role to perform this task.

Procedure

To return the certificate to default:

1. Log off all Storage Navigator web client sessions on the SVP.
2. Start a web browser on the Storage Navigator computer.
3. Specify the following URL to open the Tool Panel dialog box.
   ```
   https://SVP-IP-address-or-host-name/cgi-bin/utility/toolpanel.cgi
   ```
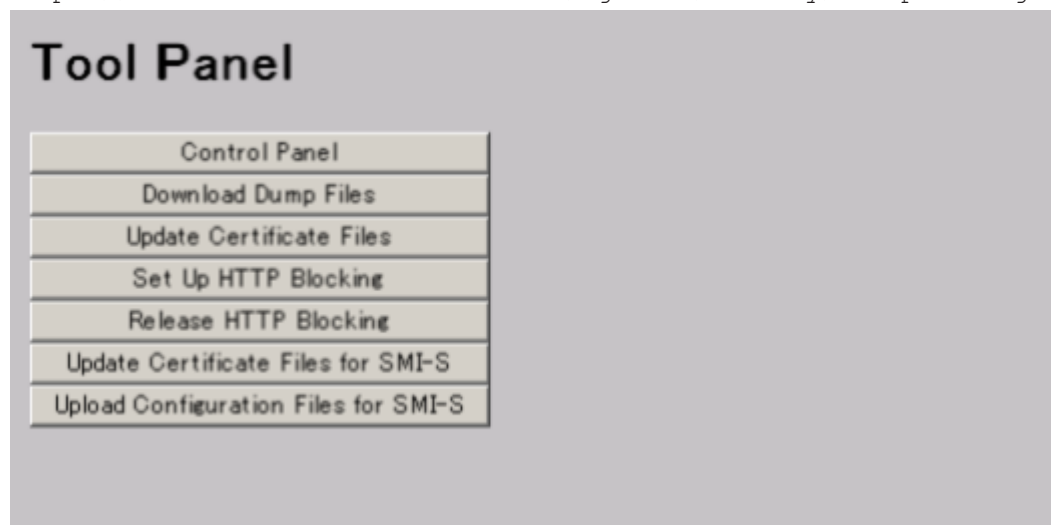

4. From the Tool Panel dialog box, click **Update Certificate Files**. A login dialog box for Update Certificate Files opens.

   If SSL communication has been established, the Security Alert dialog box displays before the login dialog box. In that case, click **OK**. If the Security Alert dialog box regarding the certificate displays at other times, ensure that the certificate is correct and then click **Yes**.

5. From the Update Certificate Files login dialog box, enter the administrator's user ID and password, and click **Login**. The upload dialog box for Update Certificate Files displays.

6. In the upload dialog box for Update Certificate Files, click **Return to Default**.

7. From the update completion dialog box for Update Certificate Files, click OK. The display returns to the login dialog box.

   Upon completion of the certificate update, the SVP web server restarts to reflect the update. When the restart of the SVP web server is complete, the update completion dialog box for Update Certificate Files displays.

8. Click **OK**. If the Security Alert dialog box for the certificate appears, click **View Certificate** to confirm that the certificate is correct, and click **Yes**.

If an error occurs during update of the certificate, an error message displays. If so, resolve the problem and then reexecute from login to Update Certificate Files.

Problems with a website security certificate

When "There is a problem with this website's security certificate." is displayed, click **Continue to this website (not recommended)**.

If the security certificate is not issued by a trusted certificate authority, the browser displays a warning message when it connects to an SSL-enabled Storage Navigator.
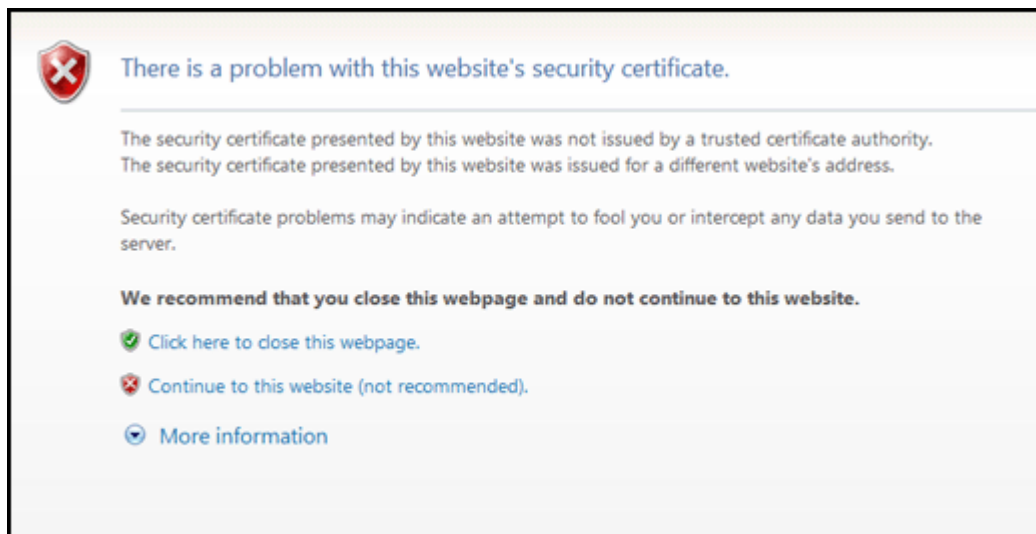
Figure 2-2 Security Alert dialog box

Blocking HTTP communication to the storage system

If the SVP supports SSL (HTTPS), the HTTP setting tool allows you to block access to port 80. When you block access to port 80, the connection used to import the certificate from the web browser to the SVP occurs on port 443 (HTTPS).

If you are using Command Suite to access Storage Navigator, blocking HTTP communication might interfere with that access. Make sure the Command Suite can use SSL communication to access Storage Navigator.

Prerequisites

- You must have Storage Administrator (Initial Configuration) role to perform this task.

Procedure

To block HTTP communication:

1. Log off all Storage Navigator web clients attached to the SVP.
2. Start both the Storage Navigator web client and web browser.
3. Specify the URL as follows:

   ```
   https://IP-address-or-host-name-of-SVP/cgi-bin/utility/
   toolpanel.cgi
   ```
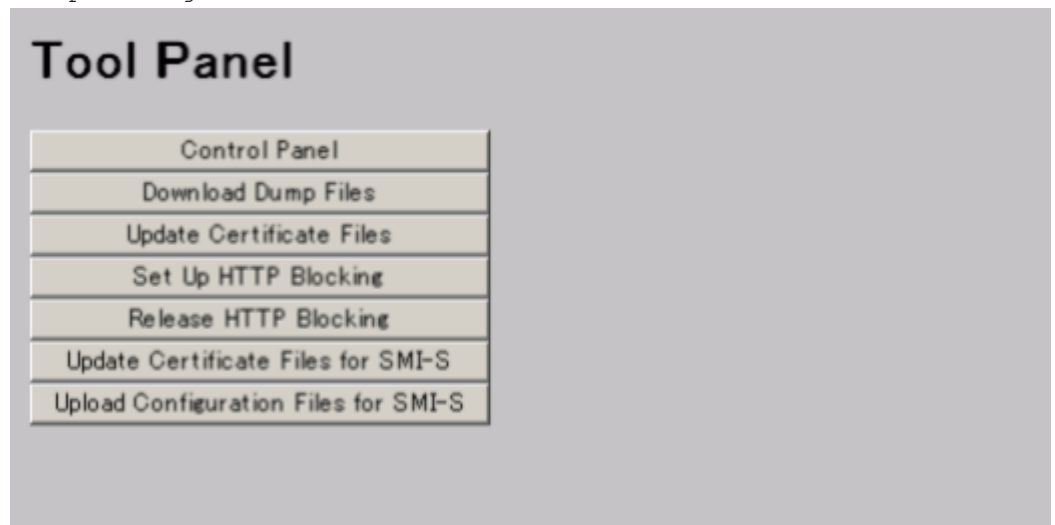

4. In the Tool Panel dialog box, click **Set up HTTP Blocking**.
5. Enter the User ID and Password for the storage administrator, then click **Logon**. The **Set up HTTP Blocking** dialog box appears.
6. Click **OK**. A confirmation dialog box appears.
7. Click **OK** to implement HTTP blocking. When the configuration change is complete, the web server on the SVP reboots. Once the reboot is complete, the HTTP Communications Blocked dialog box appears. If you want to cancel the operation and return to the logon dialog box, click **Cancel**.

   It may take 30 or 60 minutes for the web server to restart. In this case, the HTTP Communications Blocked dialog box does not appear and an internal server error occurs, but the setting is actually completed.
8. Click **OK**. You return to the logon dialog box.

Releasing HTTP communication blocking

Prerequisites

- You must have Storage Administrator (Initial Configuration) role to perform this task.

Procedure

To release the HTTP communication blocking:

1. Log off of all Storage Navigator web clients attached to the SVP.
2. Start both the Storage Navigator web client and web browser.
3. Specify the URL as follows:

   ```
   https://IP-address-or-host-name-of-SVP/cgi-bin/utility/
   toolpanel.cgi
   ```
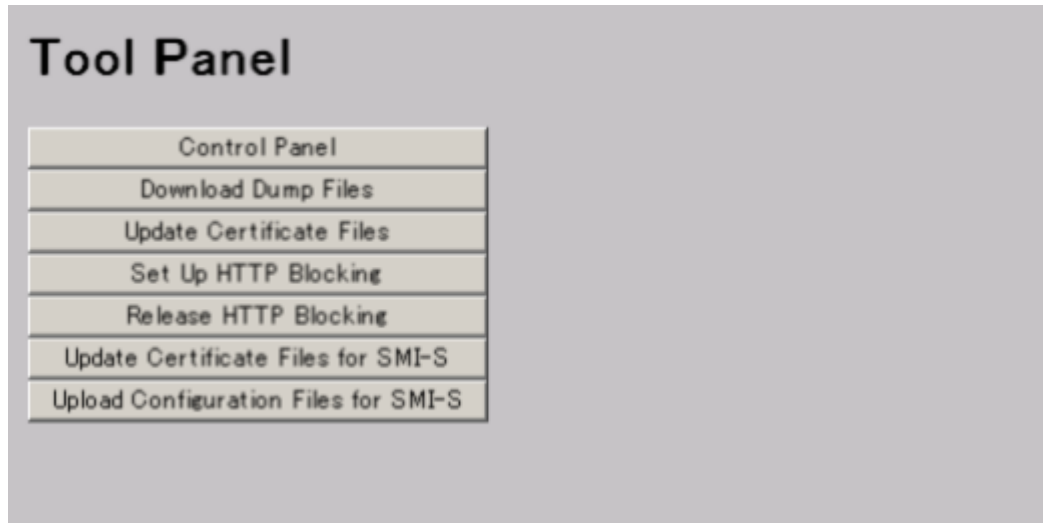

4. In the Tool Panel dialog box, click **Release HTTP Blocking**.
5. Enter the User ID and Password for the root storage administrator, then click **Logon**. The Release HTTP Blocking dialog box appears.
6. Click **OK**. A configuration dialog box appears.
7. Click **OK** to release HTTP blocking. When the configuration change is complete, the web server on the SVP reboots. Once the reboot is complete, the Release HTTP Blocking Complete dialog box appears. If you want to cancel the operation and return to the logon dialog box, click **Cancel**.

   It may take 30 or 60 minutes for the web server to restart. In this case, the Release HTTP Blocking Complete dialog box does not appear and an internal server error occurs, but the setting is actually completed.

8. Click **OK**.

Setting up the client computer

The Storage Navigator administrator is responsible for setting up the web client on Storage Navigator computers. This includes the following:

- Ensure that client computers can handle Storage Navigator. See Requirements for client computers on page 2-13.

- If you are using a Windows server as a Storage Navigator computer, make sure to follow the instructions in Configuring a Windows 2003/2008 Server on page 2-16 (if applicable).

Requirements for client computers

This topic explains the requirements for Storage Navigator computers on supported versions of the Windows and UNIX/Linux operating systems.

General requirement

A maximum of 32 Storage Navigator users can access the same storage system concurrently.

Requirements for Windows-based computers

Note: The Operating system/Browser/Java Runtime Environment/Flash player combinations and versions in this table are fixed requirements. Using other combinations or versions might produce unpredictable results such as the inability to operate GUI windows. Contact Hitachi Data Systems customer support to use other combinations or versions.

Table 2-1 Hardware requirements for Windows-based computers

Item	Requirement
Processor (CPU)	Pentium 4 640 3.2 GHz or better (Recommended: Core2Duo E6540 2.33GHz or better)
Memory (RAM)	2 GB or more Recommended: 3 GB
Available hard drive space	500 MB or more
Monitor	True Color 32-bit or better Resolution: 1280 x 1024 or better
Keyboard and mouse	You cannot use the mouse wheel feature.
Ethernet LAN card for TCP/IP network	100BASE-T 1000BASE-T

Table 2-2 Software requirements for Windows-based computers

Operating system [1]	32 bit / 64 bit	Browser [3, 4]	Java Runtime Environment[3, 5]	Flash Player
Windows XP (SP3)	32 bit	Internet Explorer 8.0	JRE 6.0 Update 20	10.1 10.2 10.3 11.1

Operating system [1]	32 bit / 64 bit	Browser [3, 4]	Java Runtime Environment[3, 5]	Flash Player
Windows Server ® 2003 (SP2)	32 bit	Internet Explorer 8.0	JRE 6.0 Update 20	10.1 10.2 10.3 11.1
Windows Server 2003 R2 (SP2)	32 bit	Internet Explorer 8.0	JRE 6.0 Update 20	10.1 10.2 10.3 11.1
Windows Server 2008 (SP2)[2]	32 bit	Internet Explorer 7.0	JRE 6.0 Update 15	10.1
			JRE 6.0 Update 20	10.1
	64 bit	Internet Explorer 7.0	JRE 6.0 Update 20	10.1
			JRE 6.0 Update 30	10.3
		Internet Explorer 8.0	JRE 6.0 Update 20	10.1 10.2 10.3 11.1
			JRE 7.0 Update 45	10.3
Windows Server 2008 R2 [2]	64 bit	Internet Explorer 8.0	JRE 6.0 Update 20	10.1 10.2 10.3 11.1
			JRE 6.0 Update 24	10.1 10.2 10.3 11.1 11.9
			JRE 7.0 Update 07	10.1
Windows Server 2008 R2 (SP1)[2]	64 bit	Internet Explorer 8.0	JRE 6.0 Update 20	10.3
			JRE 6.0 Update 37	11.5
			JRE 7.0 Update 43	10.3
			JRE 7.0 Update 45	10.3
		Internet Explorer 9.0	JRE 6.0 Update 27	10.3
Windows Server 2012	64 bit	Internet Explorer 10.0	JRE 7.0 Update 17	10.3
			JRE 7.0 Update 45	12.3
Windows Vista[2]	64 bit	Internet Explorer 7.0	JRE 6.0 Update 16	10.1 10.2 10.3

Setting up Storage Navigator

Operating system [1]	32 bit / 64 bit	Browser [3, 4]	Java Runtime Environment[3, 5]	Flash Player
				11.1
		Internet Explorer 8.0	JRE 6.0 Update 20	10.1
				10.2
				10.3
				11.1
Windows Vista (SP1)[2]	32 bit	Internet Explorer 7.0	JRE 6.0 Update 02	10.3
			JRE 6.0 Update 20	10.3
Windows Vista (SP2)[2]	32 bit	Internet Explorer 7.0	JRE 6.0 Update 16	10.3
			JRE 6.0 Update 20	10.3
	64 bit	Internet Explorer 8.0	JRE 6.0 Update 20	10.3
Windows 7[2]	32 bit	Internet Explorer 8.0	JRE 6.0 Update 20	10.1
	64 bit	Internet Explorer 8.0	JRE 6.0 Update 20	10.1
				10.2
				10.3
				11.1
Windows 7 (SP1) [2]	32 bit	Internet Explorer 8.0	JRE 6.0 Update 20	10.1
		Internet Explorer 9.0	JRE 6.0 Update 27	10.3
		Internet Explorer 10.0	JRE 6.0 Update 20	10.3
	64 bit	Internet Explorer 8.0	JRE 6.0 Update 20	10.3
			JRE 7.0 Update 45	
Windows 8.1[2]	64 bit	Internet Explorer 11.0	JRE 7.0 Update 67	18.0

Notes:

1. None of these operating systems is supported as a guest OS in a virtual server.

2. When the SVP supports Internet Protocol Version 6 (IPv6) , you can specify IPv6 addresses.

3. When a version is not specified, use 32-bit browser and 32-bit Java Runtime Environment.

4. You cannot use Internet Explorer 6.0 or earlier. When you use Internet Explorer 8.0 or later, turn off SmartScreen Filter.

5. Use the JRE that is provided by Oracle® Corporation.

Requirements for UNIX/Linux-based computers

Note: The Operating system/Browser/Java Runtime Environment/Flash player combinations and versions in this table are fixed requirements. Using other combinations or versions might produce unpredictable results such as the inability to operate GUI windows. Contact Hitachi Data Systems customer support to use other combinations or versions.

Table 2-3 Hardware requirements for UNIX/Linux-based computers

Item	Requirement
Processor (CPU)	Pentium 4 640 3.2 GHz or better (Recommended: Core2Duo E6540 2.33GHz or better)
Memory (RAM)	2 GB or more Recommended: 3 GB
Available hard drive space	500 MB or more
Monitor	Resolution: 1280 x 1024 or better
Keyboard and mouse	You cannot use the mouse wheel feature.
Ethernet LAN card for TCP/IP network	100BASE-T 1000BASE-T

Table 2-4 Software requirements for UNIX/Linux-based computers

Operating System[1]	32 bit / 64 bit	Browser [2, 4]	Java Runtime Environment [2, 3]	Flash Player
Solaris 10 (10/09) [2]	32 bit	Firefox 3.6.8	JRE 6.0 Update 20	10.1 10.2 10.3
Red Hat Enterprise Linux AS Ver 5.5	64 bit	Firefox 3.6.8	JRE 6.0 Update 20	10.1 10.2 10.3
			JRE 7.0 Update 45	10.3

Notes:
1. None of these operating systems is supported as a guest OS in a virtual server.
2. When a version is not specified, use 32-bit browser and 32-bit Java Runtime Environment.
3. Use the JRE that is provided by Oracle Corporation.
4. IPv6 HTTPS connections from Firefox are not supported.

Configuring a Windows 2003/2008 Server

If you are using a Windows Server 2003/2008 and Internet Explorer, set the following options before logging in to an SVP:

- Navigate to **Tools** > **Internet Options**, click **Advanced**, and click the **Use TLS 1.0** check box under **Security** to enable it.

- Navigate to **Tools** > **Internet Options**, click **Advanced**, and click the **Do not save encrypted pages to disk** check box to enable it.

- Navigate to **Tools** > **Internet Options**, click **Security** and register the URL of the SVP.

For more information on configuring these settings, see the Internet Explorer help documentation.

Setting up TCP/IP for a firewall

To connect the Storage Navigator computer and the SVP through a firewall, configure the firewall so that the TCP/IP port for the protocol you use becomes available.

When attaching Storage Navigator to multiple storage systems, the installer must log in to the SVP of each storage system using separate Storage Navigator sessions and separate web browser instances.

Table 2-5 Firewall configuration

Protocol	Port number	Direction of communication
HTTP	80	From the Storage Navigator web client to the SVP
HTTPS	443	
RMI	1099	
RMI	51099	
RMI	51100	
SMI-S	427	
SMI-S	5989	
SNMP*	161	
SNMP Trap*	162	From the SVP to the Storage Navigator web client
Command Control Interface	31001	From a host to the SVP
Command Control Interface	34001	From the SVP to a host
* Required if you use a Storage Navigator web client as an SNMP manager.		

Configuring the web browser

To configure the client web browser, note the following:

- The browser must allow first-party, third-party, and session cookies.
- Pop-up blocker and plug-ins must be disabled.
- There are two versions of Windows Flash Player: ActiveX for Internet Explorer and Plugin for other than Internet Explorer. Choose the Flash Player installer that is appropriate for your browser.
- Adobe Flash Player might be installed with Internet Explorer. In that case you can perform Windows Update to install the latest version.
- You can also download an earlier version from Microsoft Security Advisory (2755801).

Consult your browser's documentation for instructions.

⚠ **Caution:** Do not use a dial up modem to connect to the internet because connection speed is too slow.

Lowering the IE security level on Windows Server 2012 or later

One or more pages in Internet Explorer might not be displayed correctly due to the Internet Explorer security settings. The following procedure explains how to decrease the security level of the trusted Internet Explorer sites zone.

Prerequisites

You must add the URL of the SVP to the "trusted sites zone". See <u>Adding your SVP to the trusted sites zone—for Windows server on page 3-3</u>.

Procedure

1. From the Internet Explorer menu bar, click **Tools > Internet Options > Security.** The **Internet Options** window opens
2. Click the **Security** tab. The **Security** window opens.
3. In the **Security** window, select **Trusted sites**.
4. Set the **Security level for this zone** to **Medium-high.**
5. Click **OK** and close the IE window.

Enabling Flash Player

Flash Player is a standard feature of Internet Explorer in Windows 8 and Windows Server 2012 or later, but it is disabled by default. To enable Flash Player and make it available for Storage Navigator, use the following procedures.

- <u>Enabling Flash Player in Windows Server 2012 or later on page 2-18</u>
- <u>Enabling Flash Player in Windows 8 or later on page 2-21</u>

Enabling Flash Player in Windows Server 2012 or later

To enable Flash Player, run Internet Explorer in Desktop mode. Install **Desktop Experience** under **User Interfaces and Infrastructure.**

Procedure

1. In the **QUICK START** menu, click **Server Manager - Dashboard > WELCOME TO SERVER MANAGER > Add roles and features**.
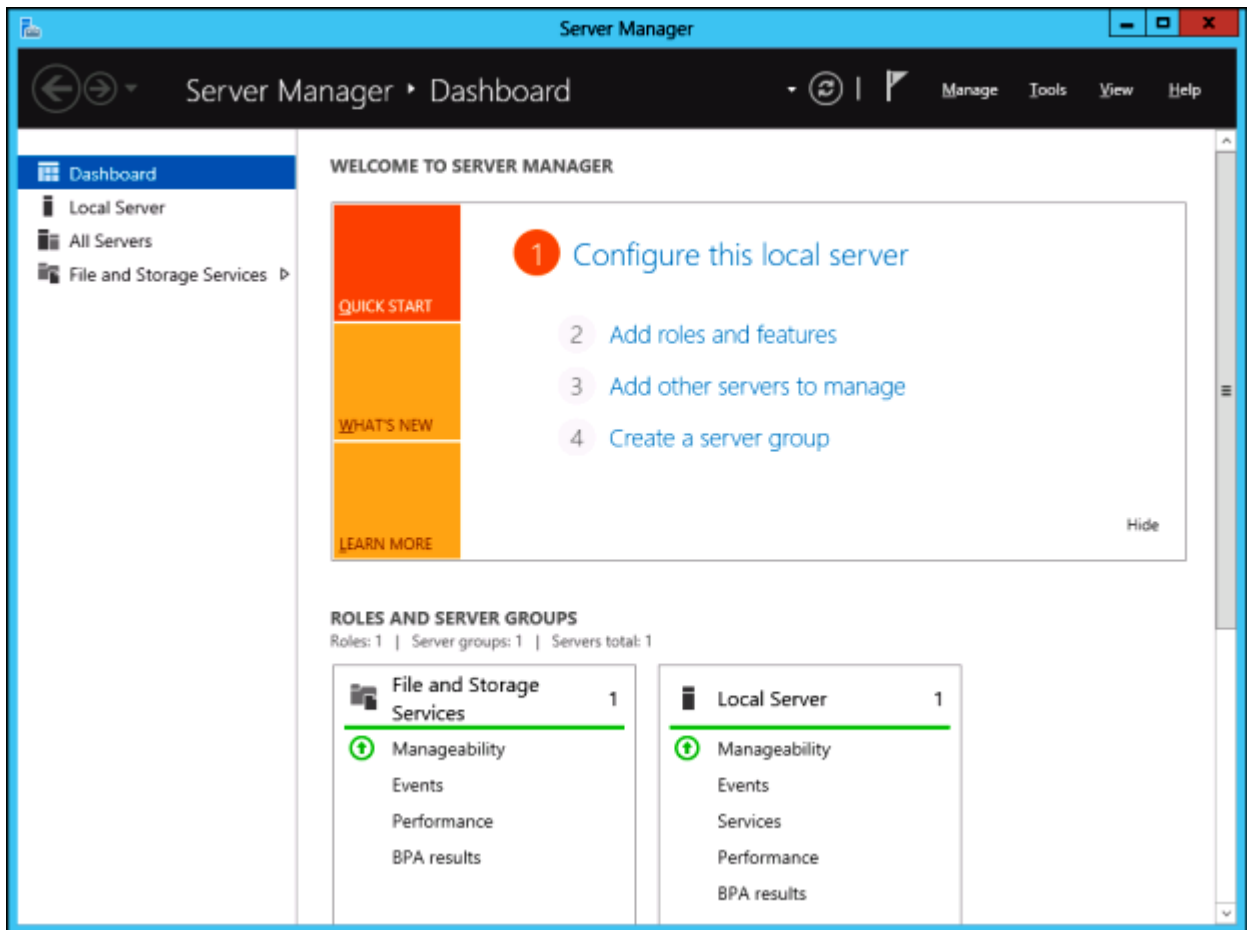
2. In the following windows and dialog boxes, click **Next**: **Before You Begin, Installation Type, Server Selection**, and **Server Roles.** In the **Features** window, select **User Interfaces and Infrastructure** > **Desktop Experience**. Then click **Next**.
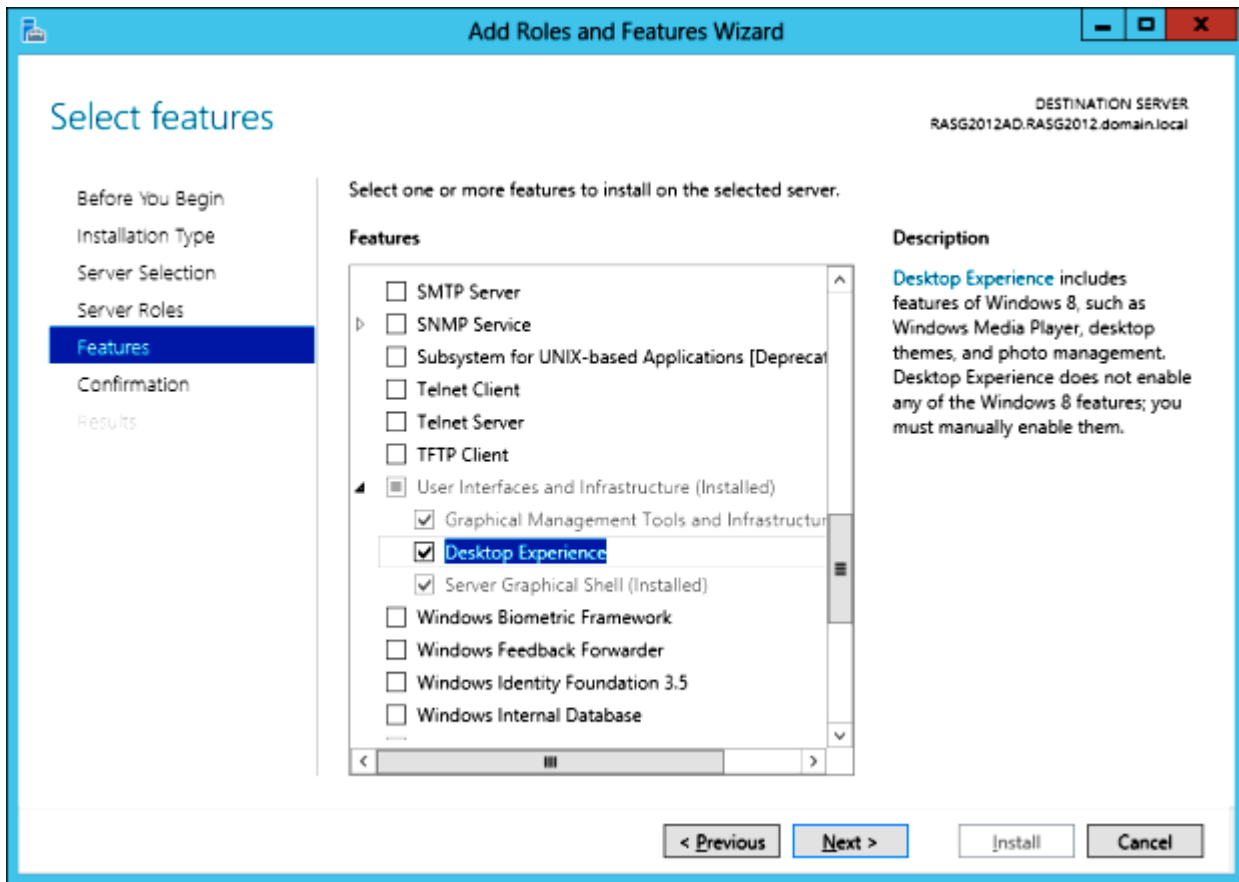
3. Click **Install**.
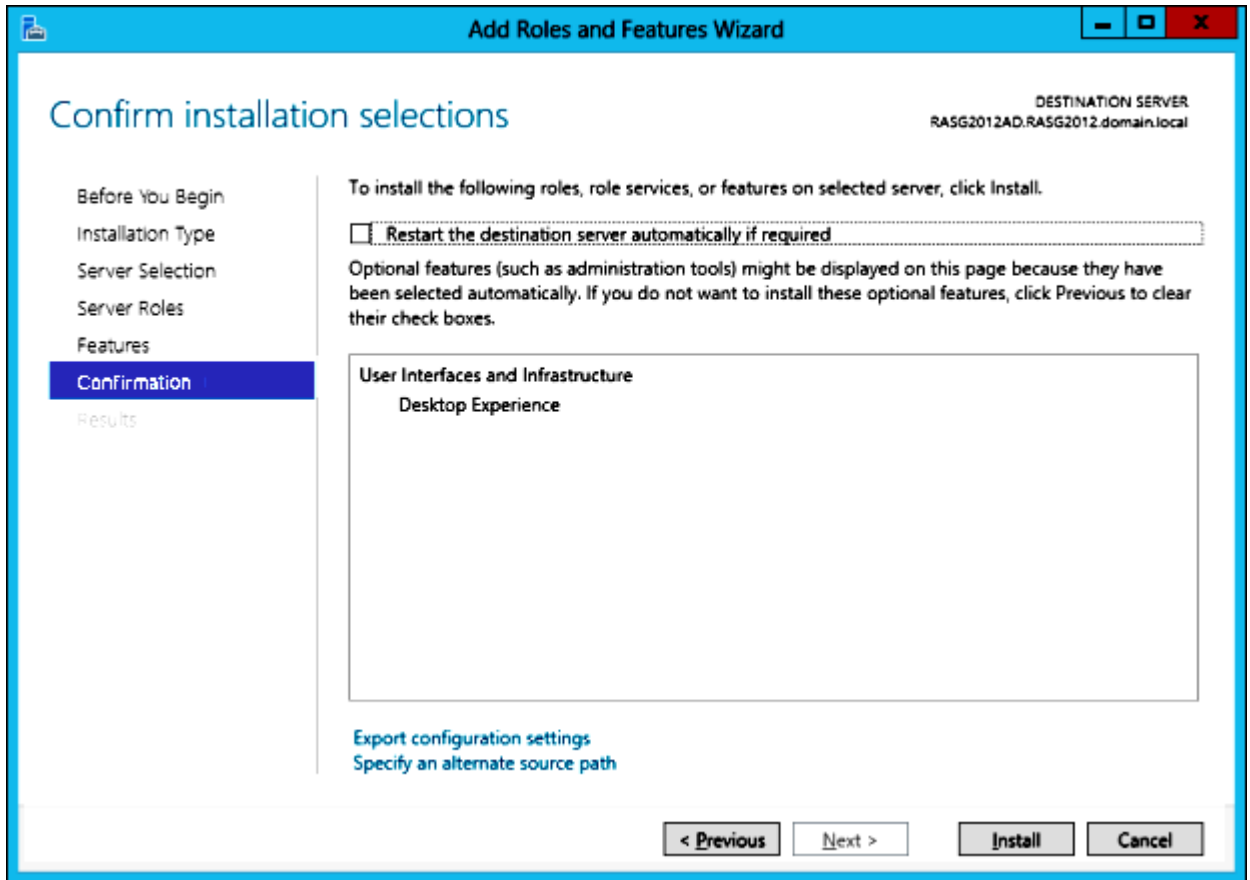
4. Reboot the computer.

Enabling Flash Player in Windows 8 or later

Internet Explorer 10 with Flash Player can be used in both Metro Mode and in Desktop Mode.

Metro Mode

Prerequisites

To use Adobe Flash Player in Metro mode, the Windows security update KB2809289 released on March 13, 2013, or security update for Internet Explorer 10 released after March 13, 2013 must be installed.

Procedure

1. To verify that the update is installed, open a command window, and enter systeminfo. Ensure that the update program (KB2809289) is in the displayed list.

2. If the update program (KB2809289) is not installed, run **Windows Update** and install the latest security update.

Desktop Mode

To use Adobe Flash Player in Desktop mode, switch from Metro Mode to Desktop Mode.

Procedure

1. Right-click anywhere in the Internet Explorer window.
2. When the application bar displays at the lower part of the screen, click the wrench icon, then click **View on the desktop**. Explorer will be switched to the desktop mode.
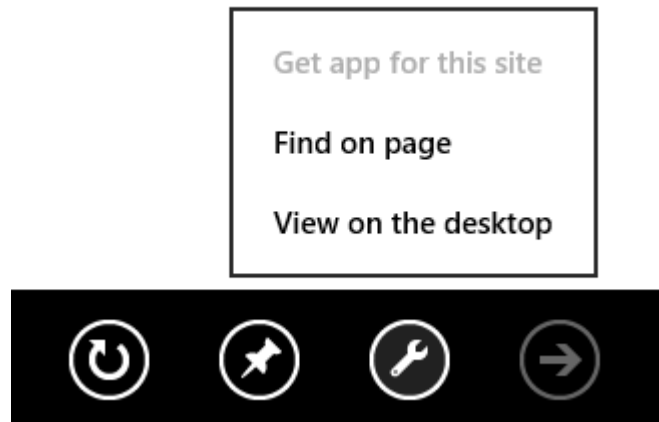
Enabling Javascript

Use the following procedure to enable Javascript in Windows 8, Windows 8.1, Windows Server 2012 or Windows Server 2012 R2.

Procedure

1. In the web browser menu, click **Tools** and select **Internet Options.**
2. In the **Internet Options** window select the **Security** tab.
3. In the **Security** tab, click **Custom level...** .
4. When the **Security Settings - Internet Zone** dialog box opens, look for the **Scripting** section.
5. In the **Active Scripting** item, select **Enable**.
6. When the **Warning** window opens, select **Yes**.
7. In the **Internet Option**s window, click **OK** to save changes and close the window.
8. Restart Internet Explorer.

Installing Adobe Flash Player

To install the latest Adobe® Flash® Player, go to http://get.adobe.com/flashplayer/ download the installer to your system, and run the installer.

To install a previous version of Adobe Flash Player:

1. Launch the web browser that you normally use and go to the Adobe website http://www.adobe.com.

2. Scroll upward as needed to display the top of the Adobe web page.

3. In the Adobe search box in the upper right corner of the web page (not the browser search box) enter **archived flash player** and click **Search**.

4. In the search results, select **Archived Flash Player versions**. The Archived Flash Player version web page on the Adobe website opens.

5. Scroll down to the list of archived Flash player versions, select the archived version you want, download the installer, and then install it.

Installing and configuring JRE

You can download and install the Java Runtime Environment from the Java website at http://www.oracle.com/technetwork/java/archive-139210.html

In a Windows environment, you can verify that JRE was successfully installed if you are able to view the Java icon in the Control Panel. You should be able to launch the Java Control Panel by double-clicking the Java icon.

In a UNIX or Linux environment, you can verify that JRE was successfully installed if you are able to open the ControlPanel.html file, which is located in the JRE root directory.

On the JRE of each Storage Navigator computer, Java log file trace and logging must be enabled and caching must be disabled. The Java log file can help you troubleshoot a problem when an application error occurs in the Storage Navigator web client. Disabling the caching feature can help prevent complications when the microcode is updated. See the http://java.sun.com website for more information on configuring JRE through the Java Control Panel.

Configuring JRE

After installing the JRE file on UNIX workstations, you must set the file path for the installation directory.

In a B Shell, issue the following command:
```
PATH=$PATH:[JRE installation directory path]/jre/bin
export PATH
```

In a C Shell, issue the following command:
```
setenv PATH ${PATH}:[JRE installation directory path]/jre/bin
```

Changing Java Security Settings

If you use a Storage Navigator computer in which Java 7 Update 55 or later is installed, or the one in which Java 8 Update 5 or later is installed, the execution of an application might be blocked when you try to open the

Storage Navigator secondary window. In this case, you need to change Java security settings according to the procedure below.

1. Check the version and update information of Java installed in your Storage Navigator computer. Click **Start** > **Control Panel** > **Java**.

2. On the **General** tab, click **About**.

3. Check the version and update information of Java, and then close the **About Java** dialog box. If your PC uses either Java 7 update 55 or later, or Java 8 Update 5 or later, you need to change Java security settings referring to Step 4 and after.

4. Select the **Security** tab.

5. Click **Edit Site List**.

6. In the **Exception Site List** dialog box, specify either of the following URLs, and then click **Add**.

    http://IP-address-of-SVP

    https://IP-address-of-SVP

7. Click **OK**.

8. Select the **Advanced** tab.

9. Select **Do not check (not recommended)** of **Perform signed code certificate revocation checks on**, and then click **OK**.

10. Close the **Control Panel** dialog box.

Using the SMI-S function with a Storage Navigator user account

HUS VM storage systems support the SMI-S function developed by SNIA. Storage administrators can use the SMI-S function by using SMI-S compliant management software.

Information and details about SMI-S are located at http://www.snia.org.

Using the SMI-S function

To use the SMI-S function, create a Storage Navigator user account and specify a storage system as the access destination from the management software.

Prerequisites

- SMI-S Provider software application must be installed.

Procedure

1. Create a Storage Navigator user account in the management software. The user account must belong to one of the following built-in user groups:

- **Storage Administrator (View & Modify) User Group.** Users have full permissions to access the SMI-S function from the management software.
- **Storage Administrator (View Only) User Group.** Users have read-only permissions to access the SMI-S function from the management software.

2. In the management software program, enter the following storage system information:

- **IP Address** of the storage system
- **Protocol**: specify **HTTPS**
- **Port**: **5989**
- **Namespace**:**root/hitachi/smis** or **interop**

Troubleshooting

If you cannot access the SMI-S function, check the network environment and access destination. If access cannot be made even though there is no problem with the network environment and access destination, contact Hitachi Data Systems Support Center.

The SMI-S certificate might have expired when you receive a storage system. In this case, you cannot use the SMI-S function. Therefore, perform the procedure in to update the certificate.

Uploading a signed certificate to the SMI-S provider

To use certificates in SSL communication with the SMI-S provider, you must update and upload the private key and the signed server certificate (public key) to the SMI-S provider to update the certificate. Use the following procedure to upload and update certificates using a certificate update tool.

Prerequisites

Ensure that the following items have been completed:

- A private key (.key file) has been created. Change the file name to server.key unless the file is already named that.
- A signed public key certificate (.crt file) has been acquired. Change the file name to server.crt unless the file is already named that.
- The private key (server.key file) and the signed public key certificate (server.crt file) are in Base 64 encoded X509 format.
- The passphrase for the private key (.key file) is released.
- Use an account which belongs to Storage Administrator (View & Modify) User Group.

Procedure

1. Terminate all Storage Navigators connected to the SMI-S provider.

2. From a PC on which Storage Navigator operates, start the Web browser.

3. Specify the following URL to open the Tool Panel dialog box.

    https://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi

Tool Panel

Control Panel
Download Dump Files
Update Certificate Files
Set Up HTTP Blocking
Release HTTP Blocking
Update Certificate Files for SMI-S
Upload Configuration Files for SMI-S
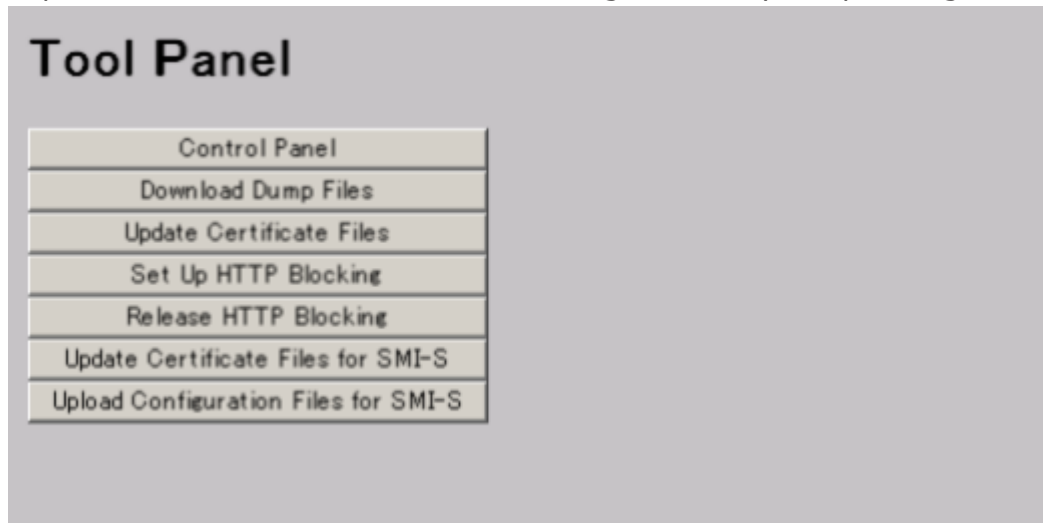
4. In the Tool Panel dialog box, click **Upload Configuration Files for SMI-S.** The login dialog box for Upload Configuration Files for SMI-S opens.

    If SSL communication has been established, the **Security Alert** dialog box opens before the login dialog box. Click **OK**. If the Security Alert dialog box regarding the certificate opens at other times, ensure that the certificate is correct and then click **Yes**.

5. In the login dialog box for Update Certificate Files for SMI-S, enter the administrator's user ID and password, and click **Login**. The upload dialog box for Update Certificate Files for SMI-S opens.

6. In the upload dialog box for Update Certificate Files for SMI-S, enter both the public key certificate file name in the Certificate file (server.crt file) box and the Private Key file (server.key file) box. You can enter the file names directly or by clicking **Browse**.

7. Click **Upload**. The execution confirmation dialog box for Update Certificate Files for SMI-S opens.

8. Click **OK** to update the certificate. Update of the certificate starts.

    Upon completion of the certificate update, the SMI-S provider restarts to reflect the update.

    Upon completion of the restart of the SMI-S provider, the update completion dialog box for Update Certificate Files for SMI-S opens

9. In the update completion dialog box for Update Certificate Files for SMI-S, click **OK**. The display returns to the login dialog box.

    In some cases, the Security Alert dialog box regarding the certificate may display before the login dialog box. If so, click View Certificate to confirm that the certificate is correct and then click **Yes**.

Note: If an error occurs during update of the certificate, an error message displays. Resolve the problem and then run the procedure again, starting with logging in, to upload configuration files for SMI-S.

Returning an SMI-S provider certificate to default

You can return a certificate updated in to default.

Prerequisites

Ensure that the following items have been completed:

- Use an account which belongs to Storage Administrator (View & Modify) User Group.

Procedure

To return a certificate to default:

1. Terminate all instances of Storage Navigator that are connected to the SMI-S provider.
2. From a PC on which Storage Navigator operates, start a Web browser.
3. Specify the following URL to open the Tool Panel dialog box.

   https://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi

   Tool Panel

   > Control Panel
   > Download Dump Files
   > Update Certificate Files
   > Set Up HTTP Blocking
   > Release HTTP Blocking
   > Update Certificate Files for SMI-S
   > Upload Configuration Files for SMI-S

4. In the Tool Panel dialog box, click **Update Configuration Files for SMI-S**. The login dialog box for upload configuration files for SMI-S opens.

   If SSL communication has been established, the Security Alert dialog box opens before the login dialog box. If so, click **OK**. If the Security Alert dialog box regarding the certificate opens at other times, click **View Certificate** to confirm that the certificate is correct and then click **Yes**.

5. In the login dialog box for Update Certificate Files for SMI-S, enter the administrator's user ID and password, and click **Login**. The upload dialog box for Update Certificate Files for SMI-S opens.

6. In the upload dialog box for Update Certificate Files for SMI-S, click **Return to the default configuration.** The execution confirmation dialog box for Update Certificate Files for SMI-S opens.

7. Click **OK** to update the certificate. Update of the certificate starts.

Upon completion of the certificate update, the SMI-S provider restarts to reflect the update. Upon completion of the restart of the SMI-S provider, the update completion dialog box for Update Certificate Files for SMI-S opens.

8. In the update completion dialog box for Update Certificate Files for SMI-S, click **OK**. The display returns to the login dialog box.

In some cases, the Security Alert dialog box regarding the certificate may display before the login dialog box. If so, click **View Certificate** to confirm that the certificate is correct and then click **Yes**.

> **Note:** If an error occurs during update of the certificate, an error message displays. Resolve the problem and then run the procedure again, starting with logging in, to upload configuration files for SMI-S.

Uploading an SMI-S provider configuration file

You can control the SMI-S function using the SMI-S provider configuration file that you create.

Prerequisites

- Ensure that the SMI-S provider configuration file (user-defined.properties) has already been created. Change the file name to user-defined.properties unless the file is already named that.
- Use an account which belongs to Storage Administrator (View & Modify) User Group.

Procedure

To upload the SMI-S provider configuration file:

1. Terminate all Storage Navigators connected to the SMI-S provider.
2. From a PC on which Storage Navigator operates, start the Web browser.
3. Specify the following URL to open the Tool Panel dialog box.
   http://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi

Tool Panel

Control Panel
Download Dump Files
Update Certificate Files
Set Up HTTP Blocking
Release HTTP Blocking
Update Certificate Files for SMI-S
Upload Configuration Files for SMI-S
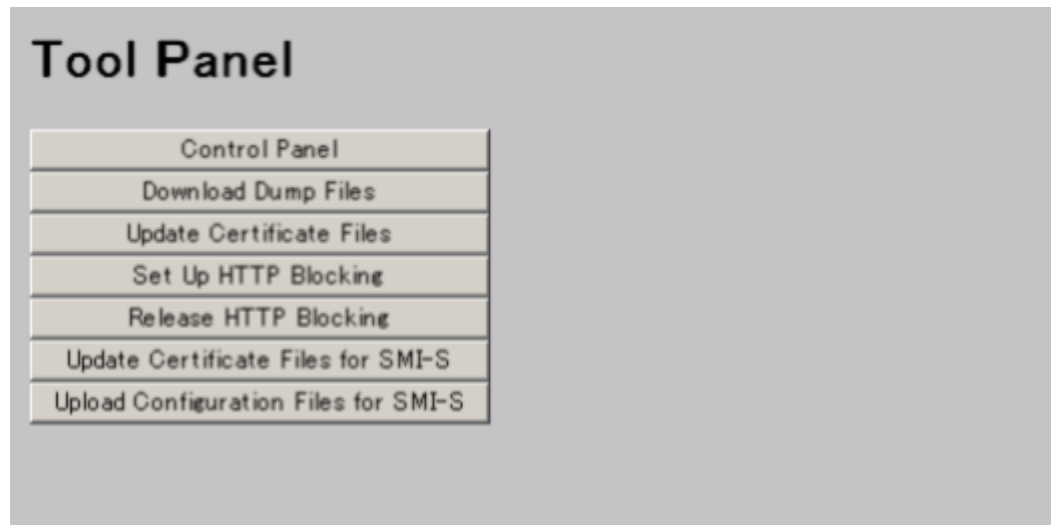
4. In the Tool Panel dialog box, click **Update Certificate Files for SMI-S.**
   The login dialog box for Update Certificate Files for SMI-S opens.

   If SSL communication has been established, the Security Alert dialog box
   opens before the login dialog box. Click **OK**. If the Security Alert dialog
   box regarding the certificate opens at other times, ensure that the
   certificate is correct and then click **Yes**.

5. In the login dialog box for Upload Configuration Files for SMI-S, enter the
   administrator's user ID and password, and click **Login**. The Upload
   Configuration Files for SMI-S opens.

6. In the upload dialog box for Upload Configuration Files for SMI-S, specify
   the SMI-S provider configuration file (user-defined.properties).

   Enter a file name in Configuration file. Alternatively click **Browse** and
   then select a file on the displayed dialog box.

7. Click **Upload**. The execution confirmation dialog box for Upload
   Configuration Files for SMI-S opens.

8. Click **OK** to update the configuration file. Update of the configuration file
   starts.

   Upon completion of the configuration file update, the SMI-S provider
   restarts to reflect the update.

   Upon completion of the restart of the SMI-S provider, the update
   completion dialog box for Upload Configuration Files for SMI-S opens.

9. In the **Upload Configuration Files for SMI-S** dialog box, click **OK**. The
   display returns to the login dialog box.

   In some cases, the Security Alert dialog box regarding the certificate may
   display before the login dialog box Click **View Certificate** to confirm that
   the certificate is correct and then click **Yes**.

Note: If an error occurs during update of the certificate, an error message
displays. Resolve the problem and then run the procedure again, starting with
logging in, to update certificate files for SMI-S.

Returning an SMI-S provider configuration file to default

You can return the configuration file updated in <u>Uploading an SMI-S provider configuration file on page 2-28</u> to default.

Prerequisites

Ensure that the following items have been completed:

- Use an account which belongs to Storage Administrator (View & Modify) User Group.

Procedure

To return the configuration file to default:

1. Terminate all instances of Storage Navigator that are connected to the SMI-S provider.
2. From a PC on which Storage Navigator operates, start a Web browser.
3. Specify the following URL to open the Tool Panel dialog box.

   https://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi

   ## Tool Panel

Control Panel
Download Dump Files
Update Certificate Files
Set Up HTTP Blocking
Release HTTP Blocking
Update Certificate Files for SMI-S
Upload Configuration Files for SMI-S

4. In the Tool Panel dialog box, click **Update Configuration Files for SMI-S**. The login dialog box for Upload Configuration Files for SMI-S opens

   If SSL communication has been established, the Security Alert dialog box opens before the login dialog box. If so, click **OK**. If the Security Alert dialog box regarding the certificate opens at other times, click **View Certificate** to confirm that the certificate is correct and then click **Yes**.

5. In the login dialog box for Upload Configuration Files for SMI-S, enter the administrator's user ID and password, and click Login. The upload dialog box for Upload Configuration Files for SMI-S opens.

6. In the upload dialog box for Upload Configuration Files for SMI-S, click **Return to the default configuration.** The execution confirmation dialog box for Upload Configuration Files for SMI-S opens.

7. Click **OK** to update the configuration file. Update of the configuration file starts.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Upon completion of the configuration file update, the SMI-S provider restarts to reflect the update. Upon completion of the restart of the SMI-S provider, the update completion dialog box for Upload Configuration Files for SMI-S opens.

8. In the update completion dialog box for Upload Configuration Files for SMI-S, click **OK**. The display returns to the login dialog box.

   In some cases, the Security Alert dialog box regarding the certificate may open before the login dialog box. If so, click **View Certificate** to confirm that the certificate is correct and then click **Yes**.

> **Note:** If an error occurs during update of the SMI-S provider configuration file, an error message displays. Resolve the problem and then run the procedure again, starting with logging in, to update certificate files for SMI-S.

Installing the report configuration tool

Complete the following instructions to install the report configuration tool.

Prerequisites

You need the following items to install the report configuration tool:

- **A computer** running Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Red Hat Enterprise Linux AS 5.0, Red Hat Enterprise Linux AS 4.0 on EM64T, Red Hat Enterprise Linux AS 5.0 on EM64T, Red Hat Enterprise Linux 6, or Red Hat Enterprise Linux 7.

  You can use either an IPv4 address or an IPv6 address to connect the SVP to the windows computer. You can also connect the computer to the SVP over an IPv4 proxy server. When you use the proxy server, specify a name and a port number of the proxy server as the `HTTP_PROXY` environment variable on the Windows computer. For example:

  `SET HTTP_PROXY=http://proxy.xx.co.jp:8080`

- **A user account** for exclusive use of the report configuration tool.

  To use the report configuration tool, you must create a user account that is used exclusively for the report configuration tool. Assign the Storage Administrator (Initial Configuration) role to this user account.

  For information on user accounts, see Creating user accounts on page 4-13.

- **The report configuration tool** installation software

  The Report Configuration Tool is located on the CD-ROM Disc 2, which is named *Host PP*.

Installation procedure

To install the report configuration tool:

1. Insert the Report Configuration Tool installation CD into the CD-ROM drive.

2. From the media, start the installer.

   ○ For Windows: Navigate to the **\program\Config_Report_CLI \Win32** folder, and double-click `setup.EXE`.

   ○ For Linux (32 bit): Move to the **/program/Config_Report_CLI/** directory, and type `./RIinstsh`.

   ○ For Linux (64 bit): Move to the **/program/Config_Report_CLI/ LINUX/X64/** directory, and type `../../RIinstsh`.

3. When prompted, enter the name of the directory in which to install the report configuration tool. The installer continues until the tool is installed.

Note: The directory where the report configuration tool is installed is not specified as an application path. When necessary, specify the directory as the application path

Using the report configuration tool

You can use the report configuration tool to create up to 20 configuration reports and then view or download them.

Creating a configuration report on page 7-8 describes how to create a configuration report. The list of commands for creating reports is located in Appendix B, Report Configuration Tool command reference (raidinf commands) on page B-1.

Enabling the compatibility view setting in Internet Explorer 11

To use Internet Explorer 11 for Adobe Flash Player versions earlier than 11.0, enable the compatibility view setting.

Procedure

1. From Internet Explorer's menu bar, click **Tools > Compatibility View Settings**. The **Compatibility View Settings** dialog box opens.

2. In **Add this website**, enter the IP address of the SVP.

3. Click **Add**.

4. In **Websites you've added to Compatibility View**, make sure that the IP address of the SVP is displayed.

5. Click **Close**.

Getting started using Storage Navigator

This chapter describes login and restrictions when using Storage Navigator.

For instructions on navigating to storage system information, see Chapter 7, Viewing and managing the storage system on page 7-1.

☐ Logging in to Storage Navigator

☐ Storage Navigator restrictions

☐ Refreshing your user view

☐ Setting your view back to default

☐ For more information about Storage Navigator

Logging in to Storage Navigator

There are two kinds of login for Storage Navigator:

- One-time only initial login by the administrator or super-user who logs in first to create other user accounts
- Normal login for all other Storage Navigator and storage system administrators

Initial super-user login

This topic describes the login procedure for the super-user who sets up Storage Navigator and logs in to it for the first time. This super-user has a built-in ID and password, which is set up with all permissions.

Once logged in, the super-user must change the super-user password to prevent unwarranted login.

To log in using the super-user ID and password:

1. In your web browser, specify the URL for your SVP:

   `https://IP-address-or-host-name-of-SVP/`.

2. Log in with the super-user ID maintenance and password raid-mainte.

3. Change the password for this account by clicking **Settings** > **User Management** > **Change Password**.

Normal login

This login procedure is for all users other than the super-user.

> **Note:** When connecting to a second storage system, you must start a new web browser instance and log in to the system's URL.

To log in to a storage system with Storage Navigator:

1. In your web browser, specify the following URL:

   `https://IP-address-or-host-name-of-SVP/`

2. The following actions might be required to open the login dialog box, depending on your environment:

   - If a message indicates that the enhanced security configuration is enabled on the computer, select **In the future, do not show this message** and click **OK**.

   - If the SVP is set to support SSL-encrypted communication and security messages appear, make sure the certificate is correct and follow the instructions on the dialog box.

   - If a message indicates that certain web sites are blocked, follow instructions in Adding your SVP to the trusted sites zone—for Windows server on page 3-3.

3. Type the user ID and password.

4. Click **Login**.

5. If the Security Information dialog box appears, click **Yes**.

6. If a local storage area pop-up dialog box of Adobe Flash Player Setting appears, click **Allow** to open the Storage Navigator main window. The cache function of Flash Player optimizes the process of Storage Navigator. Denial of the request might delay the processing speed of Storage Navigator.

Figure 3-1 Flash Player local storage area dialog box

Note: The roles and resource groups for each user are set up ahead of time and will be available to you when you log in to Storage Navigator. If the roles or resource group assigned to another user are changed after you log in, the changes will not be effective until you log out and log back in again.

Note: If login fails three times with the same user ID, Storage Navigator stops responding for one minute. This is for security purposes and is not a system failure. Wait, then try again.

Changing your password

After the administrator gives you a user ID and password, you should change the password.

To change your user account password:

1. Log in to Storage Navigator with the user ID and password given to you by the administrator.

2. Click **Settings** > **User Management** > **Change Password** to change your password.

Adding your SVP to the trusted sites zone—for Windows server

If you are using Storage Navigator on a Windows Server 2003/2008 computer, the following message may appear during login. If it does, you must add the SVP to the trusted sites zone.
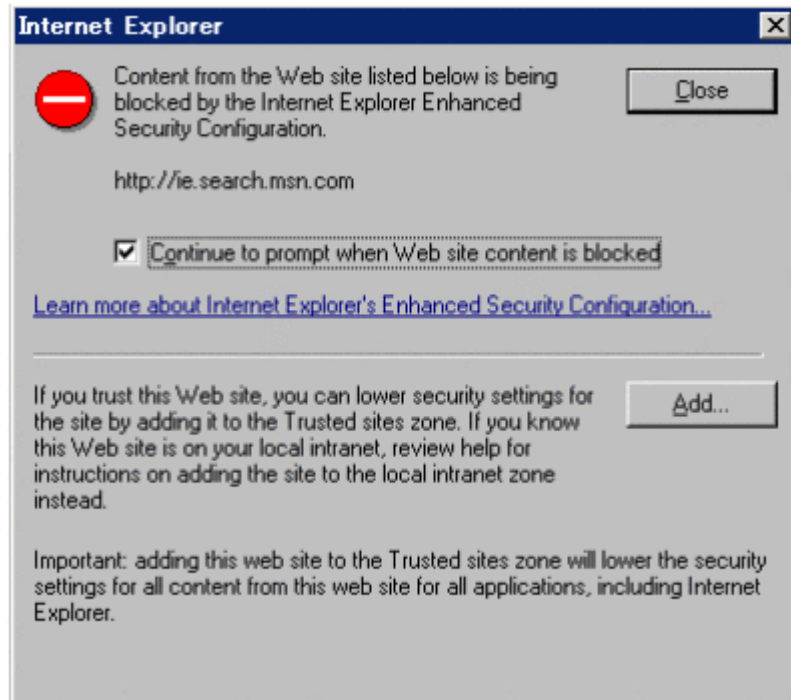
Figure 3-2 Trusted sites message

To add the SVP to the trusted sites zone:

1. Click **Add** in the message dialog box. The Trusted Sites dialog box opens.
2. In **Add this web site to the zone**, enter the URL of the SVP that you want to log in to. For example, if the host name is `host01`, the URL is `http://host01`. If the IP address is `127.0.0.1`, the URL is `http://127.0.0.1`.
3. Click **Add** to add the URL of the SVP to the **web sites** list.
4. Click **Close** to close the dialog box.

Java updates

Some Storage Navigator operations use Java. When navigating to an operation that uses a Storage Navigator secondary window, you may be prompted to update the Java application, as shown in the following figure.

Note: The following Java versions do not allow the Storage Navigator secondary window to display.

- Java 7 Update 55 or later
- Java 8 Update 5 or later

To start up the window, you need to change Java security settings.

Note: The Java Update Needed dialog box does not display unless a newer version of Java is available. The dialog box may differ in appearance, from the example shown below, according to your environment.
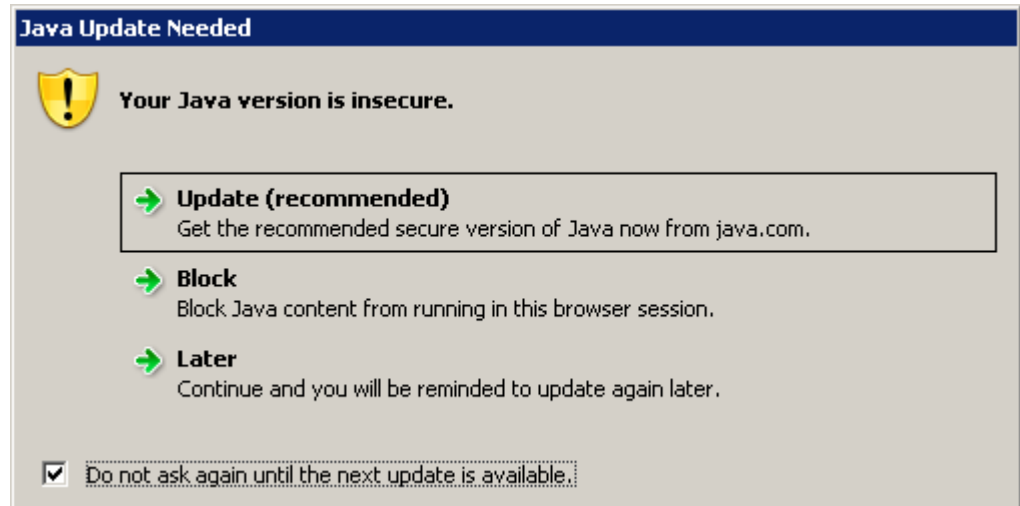
Figure 3-3 Java Update Needed dialog box

Setting the Java version

- Click **Update (recommended)** to download and install the recommended Java version. If the secondary window does not display after the update is complete, use the procedure Enabling secondary windows on page 3-5.
- Click **Block** to prevent Java content from displaying in the current browser session. If the secondary window does not display after you click Block, use the procedure Enabling secondary windows on page 3-5.
- Click **Later** to use the currently installed Java version. The Storage Navigator secondary window for the application you are using opens.

Note: If error 20020-108000 is displayed after you click Later, open the Storage Navigator main window and then open the secondary window again.

- Click the checkbox **Do not ask again until the next update is available** to prevent the Java Updated Needed dialog box from displaying until a new version of Java is available.

Enabling secondary windows

1. Open the **Java Control Panel**, and then click the **Security** tab.
2. If Enable Java content in the browser is selected, clear the check box, and then click **Apply**.
3. Select the check box again, and then click **Apply**.
4. Click **OK**, and close the window.
5. Restart Storage Navigator.

Storage Navigator restrictions

This topic lists actions that are restricted within Storage Navigator, and within the browser when using Storage Navigator:

General restrictions

To avoid an error, do not perform any of the following actions while using Storage Navigator:

- Do not change the local storage area value in Adobe Flash Player.
- Do not change the clock time of the Storage Navigator computer while you are logged in to the SVP.
- Do not adjust your computer display while using Storage Navigator. For example, do not change the screen resolution or use the Remote Desktop feature of Microsoft.
- Do not use screen savers that change the screen resolution automatically.
- Do not allow the computer to enter standby or hibernate mode when using Storage Navigator. If you do so, you must restart Storage Navigator.
- If applicable, disable the auto-login function of any web-based software or web site.
- You cannot use the **Home, End**, or **Delete** key for Storage Navigator operations.
- You cannot use function keys.

Web browser restrictions while using Storage Navigator

Do not use the web browser menus, shortcuts, or other browser options when logged in to Storage Navigator:

- If you use **Back**, **Next**, or web browser shortcut keys such as **F5** and **Esc**, you will be logged out of Storage Navigator and any settings will be canceled.
- Do not close the web browser window using the ☒ button, the **Close** option in the **File** menu, or the **Alt** + **F4** shortcut. To close Storage Navigator, click **Logout** or **File** > **Close** in the Storage Navigator menu.

- Do not change the web browser settings such as **Tools** > **Folder options** of Internet Explorer. If you do so and see unexpected results, close the web browser and log in to Storage Navigator again.
- Do not disable Flash Player because Flash Player is necessary for Storage Navigator and works as an add-on to a web browser. If you use Internet Explorer, do not change the settings in **Tools** > **Manage Add-ons**.
- Do not use the following web browser functions: character encoding, text size, the zoom function, the **Ctrl** + **F** (search), **Ctrl** + **A** (select all).
- Use the **Tab** shortcut only to move the focus to Flash Player; do not use the **Shift + Tab**.
- If you use **Shift** + **Tab** shortcut to move the focus in reverse, the focus may not move from web browser to the Flash Player. Use only **Tab** to move the focus to the Flash Player.
- In Internet Explorer, the window closes automatically when you click **Logout** at the upper right corner of the Storage Navigator main window.

   When you display an HTML format report saved in your local file system in a Web browser to which Adobe Flash Player version 23 or later is applied, add the folder containing the HTML format report to **Trusted Location Settings**. If a path to the folder where the report is stored is a Windows UNC path, perform either of the following beforehand:

   - Copy the report to a folder in the local drive.
   - Register the folder containing the report to a network drive.

Perform the following procedure to add the folder containing the HTML format report to Trusted Location Settings.

Procedure

In Internet Explorer and Firefox:

1. Open Adobe Flash Player Settings Manager.
2. On the **Advanced** tab, click **Trusted Location Settings** under **Developer Tools**. The **Trusted Location Settings** dialog box opens.
3. Click **Add**. The **Add Site** dialog box opens.
4. Click **Add Folder**. Select the folder that contains the HTML format report, and then click **OK**.
5. In the **Add Site** dialog box, click **Confirm**.
6. In the **Trusted Location Settings** dialog box, click **Close**.
7. Close Adobe Flash Player Settings Manager.

Unsupported actions in Windows version of Storage Navigator

The following actions are not supported in any version of Storage Navigator.

- You cannot use the right-click action in the Storage Navigator main window to open a pop-up menu. If you right-click, the Flash Player pop-up menu opens instead.

- You cannot use the copy (**Ctrl**+**C**) and paste (**Ctrl**+**V**) shortcuts to copy and paste text to a text box in Storage Navigator.
- No drag-and-drop operation is available in Storage Navigator.
- The mouse wheel may not function in the Storage Navigator secondary window.
- The zoom in and zoom out function of the web browser cannot be used in the Storage Navigator window. When you hold down on the **Ctrl** key and use the mouse wheel, a part of the Storage Navigator window may not be displayed because of the zoom in and zoom out function of the web browser.

Unsupported actions in UNIX version of Storage Navigator

The following actions are not supported in the UNIX version of Storage Navigator:

- You cannot change the Storage Navigator window size.
- You cannot drag-and-drop objects in the Volume Migration or LUN Manager windows.
- If you click the Storage Navigator secondary window when you are using Volume Migration, the Volume Migration window may be fully or partially hidden behind the Storage Navigator window. However you cannot use the front Storage Navigator window.

  Before you use the Storage Navigator secondary window, close the Volume Migration window. If the Volume Migration window is hidden behind the Storage Navigator window, click the Volume Migration window to bring it to the foreground.
- The **Close** ✕ button on the Volume Migration window remains active even if you click **Apply** while the Volume Migration process is running. If you click **Close** ✕ *after* clicking **Apply**, the Volume Migration window closes but the Volume Migration process continues.
- The word "`Loading...`" only appears in the Volume Migration window message dialog box for the first operation. This message does not re-appear after the first operation.

Applying changes made in Storage Navigator

When applying changes in Storage Navigator, be aware of the following behavior:

- When an internal process is running on the SVP (for example, a configuration change, option check, or an operational information acquisition), Storage Navigator processing might be temporarily delayed.
- If you request a change to the storage system configuration in the secondary window while another change is being made, an error message appears.

  If the error occurs while you are logging in or clicking **Apply** to implement changes, wait a few minutes, then retry the operation.

If the error occurs while you are either switching between Modify and View mode, or switching tabs, wait a few minutes, click **Refresh** on the **File** menu, and then retry the operation.

- When the microcode is being updated on the SVP, you must exit and restart all web client sessions on the Storage Navigator computer.
- When you use Storage Navigator on Windows, the **Add or Remove Programs** window in the Windows' **Control Panel** might or might not display Storage Navigator. Storage Navigator works in both cases.

Refreshing data after a Volume Migration or Quick Restore operation

During a Volume Migration operation or ShadowImage Quick Restore operation, a Storage Navigator window may display old information (data from before the operation) on logical volume (LDEV) configurations. Wait until the operation completes, and then click **File > Refresh >** or **File > Refresh All** to update the Storage Navigator window.

LUN ID displayed in Storage Navigator

The default LUN ID format used in the Storage Navigator main window in HUS VM and VSP G1000, G1500, and VSP F1500 is decimal. You can change this format to hexadecimal when needed. The format of LUN IDs in the Storage Navigator secondary window is always decimal. You cannot change this format.

In comparison, the LUN ID format used in Storage Navigator in both USP V/VM and Virtual Storage Platform is hexadecimal.

If the hexadecimal format is selected in HUS VM or VSP G1000, G1500, and VSP F1500, you can enter the USP V/VM or VSP LUN IDs as is. However, if the decimal format for LUN IDs is set in HUS VM or VSP G1000, G1500, and VSP F1500, convert the LUN IDs to decimal format before entering them in Storage Navigator.

To switch the LUN ID notation of the Storage Navigator main window between decimal and hexadecimal, use the Edit Information Display Settings window. See Edit Information Display Settings window on page D-18.

Refreshing data after operations performed with another application

Be aware that it may take time to refresh the information in Storage Navigator after you have performed an operation on the storage system using another application, such as Command Control Interface.

Refreshing your user view

When you remain in the same Storage Navigator view while other users change the configuration of the system, the changes that others make do not appear in your view. You can tell how long it has been since your screen was refreshed by checking the clock on the title bar to the left of the **Refresh**

View button. The clock displays server time, not the time on your local workstation. When you rest your mouse cursor over the clock, the system displays the number of minutes that have passed since the screen was refreshed.

To see changes that others might have made, click **Refresh View** on the far right title bar in the top right corner of the screen.

Setting your view back to default

You can adjust Storage Navigator settings for column width and order, table options, filter conditions, and similar parameters. Storage Navigator saves these settings after you logout. When you login again, your settings appear as you left them in your last session.

You can also return your settings to default.

To return your settings to default, select **Settings > Environmental Settings > Reset User's View Settings**.

The parts and items that are recorded as user settings are shown in Reset View Settings on page D-10.

For more information about Storage Navigator

After you log in, the Storage Navigator main window opens. You can navigate using the menu, tree, or General Tasks. Precise instructions for performing an operation can be found in the software user guides. Also, see Appendix D, Storage Navigator GUI reference (main windows) on page D-1 and Appendix E, Storage Navigator GUI reference (secondary windows) on page E-1.

4

Setting up and managing user accounts

When Storage Navigator has been set up on the SVP, and the client computers are set up, you create user accounts for Storage Navigator users and define their roles. This chapter provides information for setting up and managing user accounts.

Workflow for creating and managing user accounts

Administrators use Storage Navigator to create accounts for all users. The following steps show a basic workflow:

- If an authentication server is used, connect the client computers to it. An authentication server allows users to log in to Storage Navigator with the same password as the one used for other applications in a system.

- If an authentication server is not used, use a password dedicated to Device Manager - Storage Navigator to log in. Whether to use the authentication server can be specified for each user.

- Review Using an authentication server and authorization server on page 4-3 for information and instructions.

- Review User Groups on page 4-7 to understand the user groups and roles you can assign new or existing users.

- Create user accounts and assign roles. See Creating user accounts on page 4-13.

- Change, disable, or delete user passwords and permissions. See Changing user passwords on page 4-15.

Administrator tasks

To authenticate a user using an authentication server, specify settings for connecting to the server, as follows.

1. Log in to Device Manager - Storage Navigator as a built-in user. Use `maintenance` as the user name, and `raid-maintenance` as the password. The built-in user has all permissions.

2. Click **Settings** > **User Management** > **Change Password** to change the password of the built-in user account.

3. Create a user group. Some user groups, such as built-in groups, are available by default.

4. Create a user.

5. If necessary, change the environment parameter.

6. Save the user account information and environment parameter file.

7. Notify the user of the new user name and the password.

Note: When an administrator changes a support person's user account, he or she must notify the user. Otherwise, the user will not be able to log in.

User tasks

1. Use the user name and password provided by the administrator to log in to Device Manager - Storage Navigator.

2. Click **Settings** > **User Management** > **Change Password** to change the password to your own password.

Using an authentication server and authorization server

An authentication server enables users to log in to Storage Navigator with the same password as the password that they use for other applications. The authentication server must be configured for each user.

The following figure shows login workflow without an authentication server:
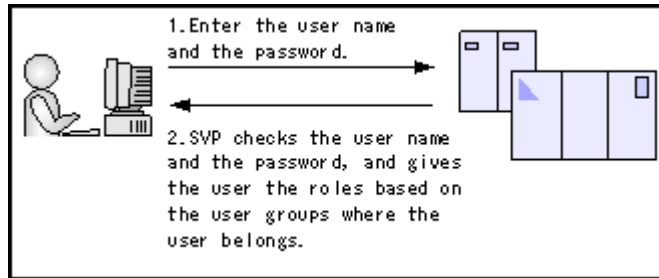
Figure 4-1 Logging in when an authentication server is not used

The following figure shows login workflow with an authentication server:
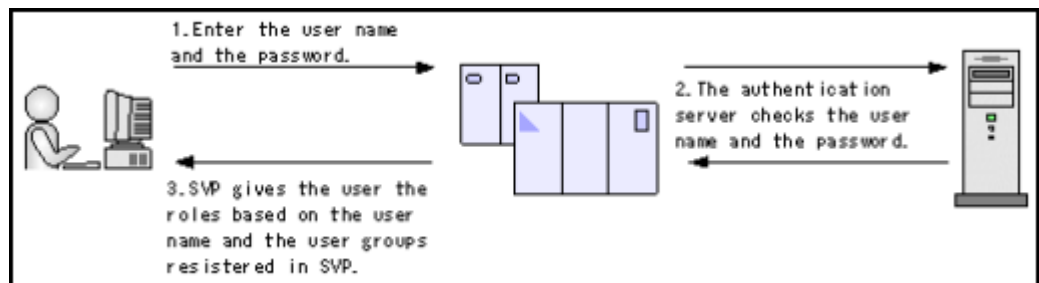
Figure 4-2 Logging in when an authentication server is used

If an authorization server works together with an authentication server, the user groups that are registered in the authorization server can be assigned to a user for Storage Navigator.

The following figure shows login workflow when an authentication server and an authorization server are used in combination:
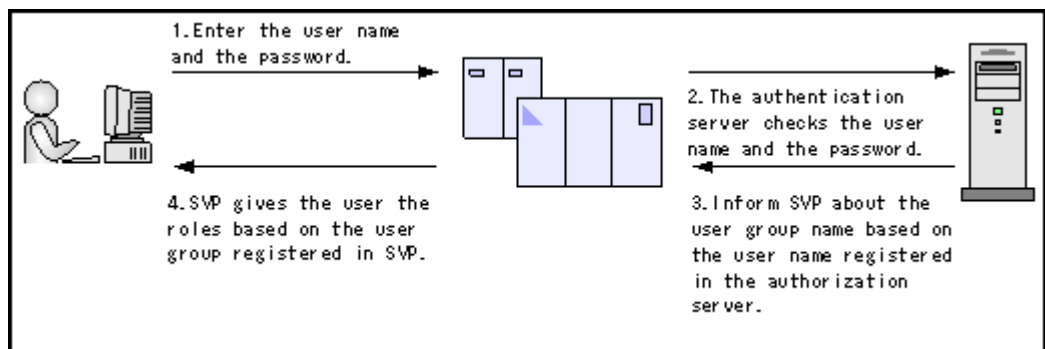
Figure 4-3 Logging in when an authentication server and an authorization server are used in combination

You can use the authentication server without knowing the host names and port numbers, if you register the information of the authentication server as

an SRV record in the DNS server. If you register multiple authentication servers to the SRV record, you can determine the authentication server to be used, based on the priority that has been set in advance.

Authentication server protocols

Authentication servers support the following protocols:

- LDAPv3 Simple bind authentication
- RFC2865 compliant RADIUS with PAP and CHAP authentication
- Kerberos v5

One of following encryption types must be used for the *Kerberos* server:

Windows

- AES128-CTS-HMAC-SHA1-96
- RC4-HMAC
- DES3-CBC-SHA1
- DES-CBC-CRC
- DES-CBC-MD5

Solaris or Linux

- DES-CBC-MD5

Authorization server requirements

The authorization server must satisfy the following requirements if it works together with the authentication server:

Prerequisite OS

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Prerequisite software

- Active Directory

Authentication protocol for user for searching

- LDAP v3 Simple bind

Connecting two authentication servers

Two authentication servers can be connected. When the servers are connected, the server configurations must be the same, except for the IP address and the port.

If you search for a server using information registered in the SRV records in the DNS server, confirm that the following conditions are satisfied:

LDAP server conditions:

- The environmental setting for the DNS server is completed at the LDAP server.
- The host name, the port number, and the domain name of the LDAP server are registered in the DNS server.

Kerberos server conditions:

- The host name, the port number, and the domain name of the Kerberos server are registered in the DNS server.
- You cannot use the SRV records on a RADIUS server.

Because UDP/IP is used to access the RADIUS server, no encrypted communications are available, such as negotiations between processes. To access the RADIUS server in a secure environment, encryption in the packet level is required, such as IPsec.

If an LDAP server or Kerberos server is used as an authentication server and works with an authorization server, the authentication server and the authorization server must use the same host.

If you use RADIUS servers as authentication servers, you can connect two authentication servers (primary server and secondary server) and one authorization server.

Connecting authentication and authorization servers

Before you can connect an authentication server and an authorization server, you must configure your network.

Prerequisites

- If you have not already done so, obtain a Security Administrator (View & Modify).
- Contact your server administrator for information about the values to be written in the LDAP, RADIUS, or Kerberos configuration file. If you use LDAP servers, the files of the LDAP servers must be certified; obtain certification.
- Contact your network administrator for information about the network settings.
- Give your service representative the IP address of the DNS server and ask that representative to configure the SVP.

To connect authentication and authorization servers:

1. Click **Settings** > **Environmental Setting** > **View External Authentication Server Properties**.

2. Click **Setup Server** to open the Setup Server window

3. Select the type of the authentication server.

4. Specify options to connect to the authentication server. If you use more than one authentication server or an authorization server, specify an option for each server.

5. To test the connection, in the Server Configuration Test field, click **Check**.

6. Click **Finish**.

7. Enter a task name and then click **Apply**.

When the authentication server and the authorization server cannot be used even if you execute the settings, a problem might exist in the server connections or the network. Contact the server administrator or the network administrator.

After you finish setting up the authentication and authorization servers and confirm that you can use the servers, save a copy of the configuration files for connecting the authentication server. For details on saving a copy, see Backing up and restoring Storage Navigator configuration files on page 5-7.

Enabling the cooperation with the authorization server

Using a user group of authorization server in Storage Navigator

Create a user group of the same name as the user group set in the value of the memberOf attribute value for each user in Active Directory. After entering the user group name, click **Check** and verify that the user group name that you entered is registered in the authorization server.

For details on how to create a user group, see Creating a new user group on page 4-12.

Register the Storage Navigator user group to the authorization server

To register the user group created using Storage Navigator to the authorization server, set the DN of the user group of the same name as the user group of Storage Navigator to the value of memberOf attribute value for each user.

Note: The domain name (DN) of the user group to be set to Active Directory must be between 1 and 250 characters. The number of user groups that can be registered at one time is 20 at maximum.

Caution: If a user needs to use different user groups for different purposes, create local user accounts on Storage Navigator. Do not use the authorization server.

User Groups

The administrator creates Storage Navigator user accounts and adds each user to a built-in group. Registered user are able to use Storage Navigator privileges allowed to them as determined by the user groups to which each user belongs. A user can belong to one or more groups.

Roles and user groups

The operations allowed to users depends on the roles of users. The roles are not set in each user but in each user group. There are two ways to change the operations that are allowed to users.

- Moving the users to another user group.
  See Changing user permissions on page 4-16 for more information.
- Changing the roles assigned to the user group where the user belongs.
  See Changing user group permissions on page 4-18 for more information.

Resource group and user groups

The resources that users can manipulate depend on the resource groups. The resource groups are not assigned to users but to user groups. There are two ways to change the resources that are allowed to users.

- Moving users to another user group.
  See Changing user permissions on page 4-16 for more information.
- Changing the resource groups assigned to the user group where the user belongs.
  See Changing resource groups assigned to a user group on page 4-19 for more information.

For details about resource groups, see the *Hitachi Unified Storage VM Block Module Provisioning Guide*.

User registering example

- The setting operations that affect the security of the whole system must be done by the administrator.
- The setting operations on the resource group 10 must be done by user A.
- The setting operations on the resource group 20 must be done by user B.

To implement the above configuration, assign the users to the user groups as shown below.

Table 4-1 User registration example

User	User group to be registered	Roles to be assigned to the user group	Resource group to be assigned to user group
Administrator	user group 1	Security Administrator (View & Modify)	All Resource Groups Assigned[1]
User A	user group 10	Storage Administrator[2]	Resource group 10
User B	user group 20	Storage Administrator[2]	Resource group 20

Notes:

1. For the user group that is assigned the Security Administrator role, All Resource Groups Assigned is automatically set to Yes.

2. There are a few types of storage administrators. See Table 4-2 Roles, Permissions, and Capabilities on page 4-8 for more information.

Caution: When multiple user groups are assigned to a user, the user has the permissions of all the roles in each user group that are enabled on the resource groups assigned to each user group.

Roles

The following table shows all the roles that are available for use and the permissions that each role provides to the users. You cannot create a custom role.

Table 4-2 Roles, Permissions, and Capabilities

Role	Permissions	Capabilities
Security Administrator	View Only	• Viewing information about user accounts and encryption settings • Viewing information about encryption key in the key management server
Security Administrator	View & Modify	• Configuring user accounts • Creating encryption keys and configuring encryption settings • Viewing and switching where encryption keys are generated • Backing up and restoring encryption keys • Deleting encryption keys backed up in the key management server • Viewing and changing the password policy for backing up encryption keys on the Storage Navigator computer • Connection to the external server • Backing up and restoring connection configuration to the external server • Configuring the certificate used for the SSL communication

Role	Permissions	Capabilities
		• Configuring the fibre channel authentication (FC-SP) • Configuring resource groups
Audit log Administrator	View Only	• Viewing audit log information and downloading audit logs
Audit log Administrator	View & Modify	• Configuring audit log settings and downloading audit logs
Storage Administrator	View Only	• Viewing storage system information
Storage Administrator	all permissions - initial configuration	• Configuring settings for storage systems • Configuring settings for SNMP • Configuring settings for e-mail notification • Configuring settings for license keys • Viewing, deleting, and downloading storage configuration reports • Acquiring all the information about the storage system and refreshing Storage Navigator window by clicking [Refresh All]
Storage Administrator	system resource management	• Configuring settings for CLPR • Configuring settings for MP Blade • Deleting tasks and releasing exclusive locks of resources • Completing SIMs • Configuring attributes for ports • Configuring LUN security • Configuring Server Priority Manager • Configuring tiering policies • Remote copy operations in general*
Storage Administrator	provisioning	• Configuring caches • Configuring LDEVs, pools, and virtual volumes • Formatting and shredding LDEVs • Configuring external volumes • Configuring Dynamic Provisioning • Configuring LUSE • Configuring host groups, paths, and WWN • Configuring Volume Migration except splitting Volume Migration pairs when using Command Control Interface • Configuring access attributes for LDEVs • Configuring LUN security • TrueCopy and High Availability Manager operations in general*
Storage Administrator	performance management	• Configuring monitoring • Starting and stopping monitoring
Storage Administrator	local copy	• Performing pair operations for local copy • Configuring environmental settings for local copy • Splitting Volume Migration pairs when using Command Control Interface

Role	Permissions	Capabilities
Storage Administrator	remote copy	• Remote copy operations in general*
Support Personnel	View & Modify	Configuring SVP • Normally, this role is for Hitachi Data Systems service representative. • Downloading dump files using the FD Dump tool.

Notes:

* Remote copy operations from Storage Navigator require all of the following roles:

For TrueCopy or High Availability Manager:

• Storage Administrator (System Resource Management) role

• Storage Administrator (Provisioning) role

• Storage Administrator (Remote Copy) role

For Universal Replicator

• Storage Administrator (System Resource Management) role

• Storage Administrator (Remote Copy) role

Note: Normally, the Support Personnel role is assigned to a HDS service representative, but if the role is assigned to a user account, dump files can be downloaded using the FD Dump tool.

Caution: If a user has All Resource Groups Assigned set to Yes, the user can access all the resources in the storage system. For example, if a user is a security administrator and a storage administrator taking care of some resources, have all resource groups assigned, and has roles of Security Administrator (View & Modify) and Storage Administrator (View & Modify), the user can edit the storage for all the resources. If this is a problem, the recommended solution is to register the following two user accounts in Storage Navigator and use these different accounts for different purposes

- A security administrator user account that has All Resource Groups Assigned set to Yes.

- A storage administrator user account that does not have all resource groups assigned and has only some of the resource groups assigned.

Caution: For the user groups whose roles are other than the Storage Administrator, All Resource Groups Assigned is automatically set to Yes. If you delete all the roles except the Storage Administrator, reassign resource groups to the user group because All Resource Groups Assigned is automatically set to No. To assign resource groups to the user group, see Changing resource groups assigned to a user group on page 4-19.

Built-in groups, roles, and resource groups

More than one built-in group is available to each user. You cannot change roles or resource groups set to the built-in groups. The following table shows the built-in groups, and their built-in roles and resource groups.

For more information about resource groups, see the *Hitachi Unified Storage VM Block Module Provisioning Guide*.

Table 4-3 Roles and resource groups configured in built-in groups

Built-in Group	Role	Resource group
Administrator	• Security Administrator (View & Modify) • Audit log Administrator (View & Modify) • Storage administrator (Initial Configuration) • Storage Administrator (System Resource Management) • Storage Administrator (Provisioning) • Storage Administrator (Performance Management) • Storage Administrator (Local Copy) • Storage Administrator (Remote Copy)	All Resource Groups Assigned
System	• Security Administrator (View & Modify) • Audit log Administrator (View & Modify) • Storage Administrator (Initial Configuration) • Storage Administrator (System Resource Management) • Storage Administrator (Provisioning) • Storage Administrator (Performance Management) • Storage Administrator (Local Copy) • Storage Administrator (Remote Copy)	All Resource Groups Assigned
Security Administrator (View Only)	• Security Administrator (View Only) • Audit log Administrator (View Only) • Storage Administrator (View Only)	All Resource Groups Assigned
Security Administrator (View & Modify)	• Security Administrator (View & Modify) • Audit log Administrator (View & Modify) • Storage Administrator (View Only)	All Resource Groups Assigned
Audit Log Administrator (View Only)	• Audit log Administrator (View Only) • Storage Administrator (View Only)	All Resource Groups Assigned

Built-in Group	Role	Resource group
Audit Log Administrator (View & Modify)	• Audit log Administrator (View & Modify) • Storage Administrator (View Only)	All Resource Groups Assigned
Storage Administrator (View Only)	• Storage Administrator (View Only)	meta_resource
Storage Administrator (View & Modify)	• Storage Administrator (Initial Configuration) • Storage Administrator (System Resource Management) • Storage Administrator (Provisioning) • Storage Administrator (Performance Management) • Storage Administrator (Local Copy) • Storage Administrator (Remote Copy)	meta_resource
Support Personnel	• Storage Administrator (Initial Configuration) • Storage Administrator (System Resource Management) • Storage Administrator (Provisioning) • Storage Administrator (Performance Management) • Storage Administrator (Local Copy) • Storage Administrator (Remote Copy) • Support Personnel • User Maintenance	All Resource Groups Assigned
Maintenance User	• Storage Administrator (View Only) • User Maintenance	All Resource Groups Assigned

Creating a new user group

This topic explains how administrators can create a user group.

Prerequisites

- You must have Security Administrator (View & Modify) role to perform this task.
- A user group name consists of 1 to 64 characters including alphanumeric characters (ASCII), spaces and the following symbols: ! # $ % & ' ( ) + - . = @ [ ] ^ _ ` { } ~
- You can create up to 256 user groups including the built-in groups.

To create a new user group

1. In the tree, click **Administration** > **User Groups**.

2. In the **User Groups** tab, click **Create User Group** to open the **Create User Group** window.

3. Enter a user group name.

4. If you use an authorization server, click **Check** and verify that the entered user group name is registered in the authorization server.

5. Click **Next** to open the **Assign Roles** window.

6. Select the roles to assign to the user group, and click **Add**.

7. Click **Next** to open the **Assign Resource Groups** window.

8. Select the resource groups to assign to the user group, and click **Add**.

> **Note:** If you select a role other than the storage administrator in the **Assign Roles** window, you do not need to select resource groups because all the resource groups are assigned automatically.

9. Click **Finish**.
   Clicking **Next** allows you to add a user.

10. Specify a task name and click **Apply.**

Managing user accounts

This topic provides instructions for the following tasks:

- Creating user accounts on page 4-13
- Changing user passwords on page 4-15
- Changing user permissions on page 4-16
- Disabling user accounts on page 4-16
- Deleting user accounts on page 4-17

Creating user accounts

This topic explains how to create a user account and register the account to a user group with appropriate roles.

Prerequisites

- You must have Security Administrator (View & Modify) role to perform this task.
- You can create up to 512 users including the built-in user.
- You can log in to SVP and CCI with user accounts that are created by Storage Navigator. You must have Support Personnel role to log in to the SVP.
- The allowable characters and length of user names and passwords depend on the applications (Storage Navigator, SVP, and/or Command Control Interface) that the user uses. The user names and the passwords must

satisfy the requirements of all the applications when the user uses multiple applications.

Table 4-4 User name and password for Storage Navigator

Item	Length in characters	Characters that can be specified
User name	1-256	• Alphanumeric (ASCII code) characters • The following symbols: # $ % & ' * + - . / = ? @ ^ _ ` {	} ~ You cannot use the # symbol when you enter a user name in a screen from the Tool Panel dialog box.
Password	6-256	• Alphanumeric (ASCII code) characters • All symbols You cannot use the quotation mark (") or backslash (\) symbols when you enter a password in a screen from the Tool Panel dialog box.

Note: If you cannot log in on a Tool Panel dialog box screen, check to see if you have used a number sign (#) in the user name, or used a quotation mark (") or a backslash (\) in the password.

Table 4-5 User name and password for logging in to SVP

Item	Length in characters	Characters that can be specified
User name	1-128	• Alphanumeric (ASCII code) characters • Following symbols: ! # $ % & ' - . @ ^ _ ` { } ~
Password	6- 127	• Alphanumeric (ASCII code) characters • All symbols

Table 4-6 User name and password for logging in to CCI

Item	Length in characters	Characters that can be specified
User name	1-63	• Alphanumeric (ASCII code) characters • Following symbols (see Note below): - . @ _
Password	6- 63	• Alphanumeric (ASCII code) characters • Following symbols (see Note below): - . @ _

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Note: When you use a Windows computer for CCI, you can also specify a backslash (\). When you use a UNIX computer for CCI, you can also specify a slash (/).

To create a user account:

1. In the tree, click **Administration** > **User Groups**.
2. In the **User Groups** tab, select a user group to which to add a user. This is dependent on which roles you want to give to the user.
3. In the **Roles** tab, confirm that the displayed roles are appropriate for the user.
4. Click the **Users** tab and then **Create User** to open the Create User window.
5. Enter a name.
6. Select **Enable** or **Disable** for the account. If you select **Disable**, the user of this account is disabled and cannot log in to Storage Navigator.
7. To use an authentication server, select **External**. To authenticate users with only Storage Navigator, select **Local**.
8. If you select **Local**, enter the password of this user account in two places.
9. Click **Finish**.
10. Specify a task name and click **Apply**.

Changing user passwords

This topic explains how to change or re-issue passwords for other users on Storage Navigator.

Prerequisites

- Security Administrator (View & Modify) role can change user passwords on Storage Navigator.
- If the target user has a local user account for Storage Navigator, the security administrator can use Storage Navigator to change the target user's password.
- If the target user has a local user account for the authentication server, the security administrator can use the authentication server to change the target user's password. After the password is changed, the target user can use the new password on both the authentication server and Storage Navigator.

To change the password of a user on Storage Navigator:

1. In the resource tree, click **Administration** > **User Groups**.
2. On the **User Groups** tab, select the user group to which the user belongs.
3. Click the **Users** tab, select the user, and then click **Change Password**. The Change Password dialog box opens.
4. Specify a new password for the user in the two password fields.

5. Click **Finish**.
6. Specify a task name and click **Apply**.

Changing user permissions

User permissions are determined by the groups to which the user belongs. You change these permissions by changing membership in the user group. A user can belong to multiple user groups.

For example, if you want to change the role of the user who manages security to the performance management role, add this user to the Storage Administrator (Performance Management) role group and then remove the user from the Security Administrator (View & Modify) role group. The change takes effect the next time the user logs in.

Prerequisites

- You must have Security Administrator (View & Modify) role to perform this task.
- The user whose permissions you want to change must belong to at least one user group.
- A user can belong to up to 8 user groups.
- 512 users can belong to a user group including the built-in user.

To change the permission of a user:

1. In the resource tree, click **Administration** > **User Groups**.
2. In the **User Groups** tab, select a user group to add the user to and then click **Add Users**.
3. In the Add User dialog box, select the user and click **Add**.
4. Click **Finish**.
5. Specify a task name and click **Apply**.
6. In the resource tree, click **Administration** > **User Groups**.
7. In the **User Groups** tab, click the user group to remove the user from.
8. Click the **Users** tab, select the user to remove from this user group, and then click **More Actions** > **Remove Users**.
9. Click **Finish**.
10. Specify a task name and click **Apply**.

Disabling user accounts

Security Administrators can disable a user account to temporarily prevent the user from logging in to Storage Navigator.

Prerequisites

- Log into an account that is different from the user whose account that you want to disable.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

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

To disable a user account:

1. In the resource tree, click **Administration** > **User Groups**.
2. In the **User Groups** tab, click a user group which the user belongs to.
3. Click the **Users** tab, select the user and then click **Edit User**.
4. Click the **Account Status** check box and click **Disable**.
5. Click **Finish**.
6. Specify a task name and click **Apply**.

To allow the user to log in to Storage Navigator, perform the operation above and click **Enable** instead of **Disable** in the Edit User window.

Deleting user accounts

Security Administrators can delete a user account when the account is no longer in use. Built-in user accounts cannot be deleted.

Prerequisites

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

To delete a user account:

1. In the resource tree, click **Administration** > **User Groups**.
2. In the **User Groups** tab, click the user group.
3. Click the **Users** tab, select the users and then click **More Actions** > **Delete Users** to open the Delete User dialog box.
4. Specify a task name and click **Apply**.

Releasing a user lockout

When a user who is attempting to log in to Storage Navigator or the Command Control Interface has entered an incorrect username / password combination three times, the system sets the login status to locked, preventing further attempts to log in. The account is locked for 60 seconds. To release the locked status before the lock has timed out, complete the following steps.

Prerequisites

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

Procedure

1. In the **Administration** tree, click **User Groups**.

2. In the **User Groups** tab, select the user group to which the user belongs.

3. In the **User** tab, select the user you want to unlock.

4. In the **User** tab, click **More Actions** > **Release Lockout**. The **Release Lockout** window opens.

5. Specify a task name and click **Apply**.

Related Topics

- Release Lockout window on page D-55
- Account lock policy on page 4-20

Changing the user group configuration

Changing a user group name

This topic explains how to change the name of a user group.

Prerequisites

- You must have Security Administrator (View & Modify) role to perform this task.
- The names of built-in groups cannot be changed.
- A user group name consists of 1 to 64 characters including alphanumeric characters (ASCII), spaces and the following symbols: ! # $ % & ' ( ) + - . = @ [ ] ^ _ ` { } ~

Procedure

1. In the tree, click **Administration** > **User Groups**.

2. In the **User Groups** tab, select the user group and then click **More Actions** > **Edit User Group** to open the **Edit User Group** window.

3. In the **Edit User Group** window, enter a new user group name.

4. If you use an authorization server, click **Check** and verify that the entered user group name is registered in the authorization server.

5. Click **Finish**.

6. Specify a task name and click **Apply**.

Changing user group permissions

This topic explains how to change the permissions that are assigned to user groups.

Prerequisites

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

- The permissions of a built-in group cannot be changed.

To change the permissions of a user group:

1. In the tree, click **Administration** > **User Groups**.
2. In the **User Groups** tab, select the user group and then click **More Actions** > **Edit Role Assignment**.
3. In the **Edit Role Assignment** window, change roles to be assigned to the user group.

   o Select roles to add, and then click **Add**.
   o Select a role to remove, and then click **Remove**.

4. Click **Finish**.
5. Specify a task name and click **Apply.**

⚠ **Caution:** For the user groups whose roles are other than the Storage Administrator, All Resource Groups Assigned is automatically set to Yes. If you delete all the roles except the Storage Administrator, reassign resource groups to the user group because All Resource Groups Assigned is automatically set to No. To assign resource groups to the user group, see Changing resource groups assigned to a user group on page 4-19.

Changing resource groups assigned to a user group

This topic explains how to change the resource groups that are assigned to the user group.

Prerequisites

- You must have Security Administrator (View & Modify) role to perform this task.
- Create a resource group to be assigned to the user group in advance.
- You cannot change the resource groups of the user group that has All Resource Groups Assigned set to Yes.
- You cannot change resource groups of the built-in group.

To change a resource group that is assigned to a user group:

1. In the tree, click **Administration** > **User Groups**.
2. In the **User Groups** tab, select a user group to change the resource group, and click **Edit Resource Group Assignment**.
3. In the **Edit Resource Group Assignment** window, change resource groups to be assigned to the user group.

   o Select the resource group to add, and click **Add**.
   o Select the resource group to remove, and click **Remove**.

4. Click **Finish**.
5. Specify a task name and click **Apply.**

Deleting a user group

Delete a user group when the user group is no longer needed.

Prerequisites

- You must have Security Administrator (View & Modify) role to perform this task.
- You cannot delete built-in groups.
- A user group cannot be deleted if there are users that belong to only the user group to delete.

To delete a user group:

1. In the tree, click **Administration** > **User Groups**.
2. In the **User Groups** tab, select user groups that you want to delete, and click **More Actions** > **Delete User Groups**.
3. Specify a task name in the **Delete User Groups** window, and click **Apply**.

Account lock policy

A user account is automatically locked after three unsuccessful logins to Storage Navigator or the Command Control Interface. The account is locked for 60 seconds. To release the lock before the lock has timed out, see Releasing a user lockout on page 4-17.

Session timeout

A session timeout occurs if the system receives no user operation for one minute due to a network error.

5

Configuring the Storage Navigator environment

This chapter provides instructions for setting customized behaviors on Storage Navigator, including timeout and polling periods, email notifications, and so on. Also, instructions are included for saving your Storage Navigator configuration settings and restoring them as needed.

☐ Configuration overview

☐ Creating a login message

☐ Setting email notification for SIMs or SNMP traps

☐ Setting time periods

☐ Backing up and restoring Storage Navigator configuration files

☐ Setting syslog notification for SIMs

Configuration overview

You can set up the following Storage Navigator behaviors:

- Create a message to display on the Storage Navigator login screen. See Creating a login message on page 5-2.
- Configure email notification when certain system failures occur. See Configuring email notification on page 5-3.
- Establish times for timeouts and polling limits. You can also hide the Alerts tab. See Setting time periods on page 5-5.
- Save Storage Navigator configuration settings, which are used if it becomes necessary to restore the settings. See Backing up and restoring Storage Navigator configuration files on page 5-7.
- Restore configuration settings. See Backing up and restoring Storage Navigator configuration files on page 5-7.
- Configure syslog notifications for system failures See Setting and configuring syslog notification for SIMs on page 5-9

Creating a login message

A login message is displayed in the Storage Navigator login window. You can use a login message to broadcast system messages and warnings. The following figure shows an example of a warning message in the login window.
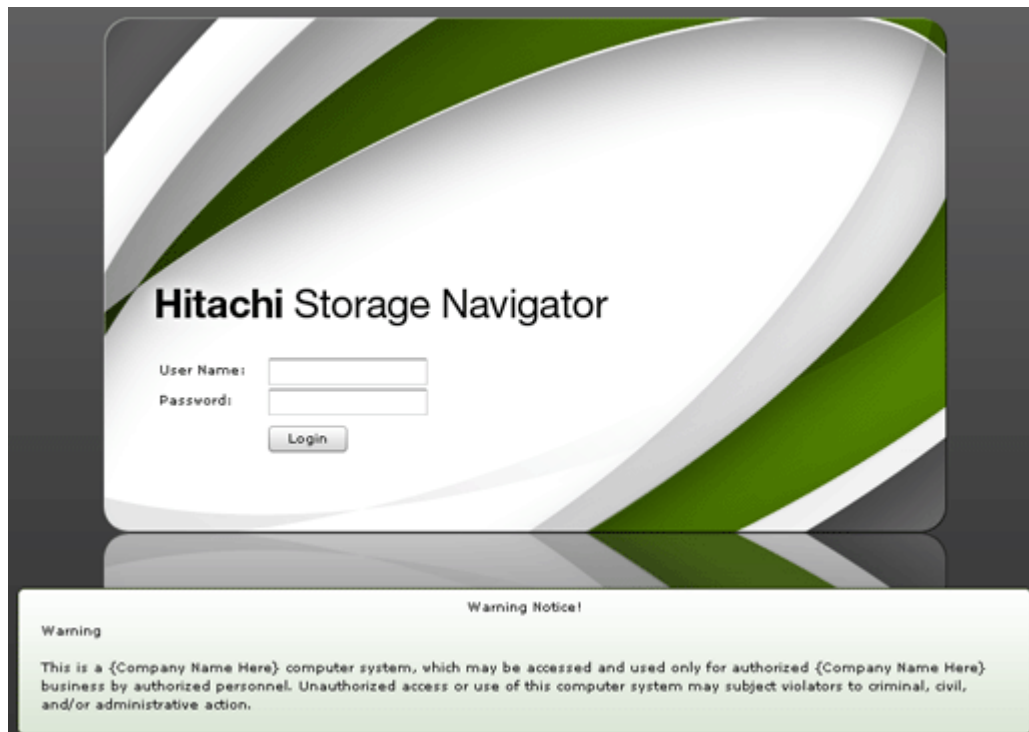
Figure 5-1 Warning banner on the login window

Prerequisites

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

To create a login message:

1. Click **Settings** > **Security** > **Login Message**. The Storage Navigator secondary window opens.

2. Click to change to Modify mode.

3. Enter the message in the window.

   Alphanumeric characters and symbols can be used in the message. The maximum length of the message is 2,048 characters.

4. Click **Apply**.

Setting email notification for SIMs or SNMP traps

You can specify notification by email to key users when system failures occur. Failures reported in the email are the same as the SIMs displayed in the Alerts window or reported by SNMP traps.

- You can configure emails for any SIMs caused by software licensing events or Dynamic Provisioning threshold events.
- With SNMP traps, email notification eliminates the need for checking for failures in SNMP manager.

You can also send a test email.

SIMs failures reported by email typically require user action. These SIMs are caused either by reaching the threshold levels configured by the user, or by a software license needing user attention.

Configuring email notification

Prerequisites

- You must have the Storage Administrator (Initial Configuration) role to perform this task.
- You must have a mail server that supports the Simple Mail Transfer Protocol (SMTP).
- If a firewall is used, port 25 must be used.

To configure settings for email notice:

1. Click **Settings** > **Environmental Setting** > **E-mail Information**. The E-mail Information window opens.

2. Click to change to Modify mode.

3. Select **Enable** in **Mail Notice**.

4. Select **IPv4**, **IPv6**, or **Host Name**, and enter the IP address or host name of the mail server.

5. In **SMTP-AUTH**, select **Enable** to use SMTP authentication. Enter the account and password for SMTP authentication

   Select **Disable** not to use SMTP authentication.

6. Enter addresses in the **From Address** (required) and **Return Address** (optional).

7. In **To Address**, add an email address:

   a. Select a blank row in the list.

   b. Enter an email address in the text box.

   c. Select To, Cc, or Bcc for the attribute.

   d. Click **Update**.

8. Repeat the previous step for all email addresses.

   To delete an email address, select the target address in the list and click **Delete**. You can select multiple addresses and delete all of them at once.

   To change an email address, select the target address in the list and perform the same operation for adding an address.

9. Click **Apply** to apply the settings to the storage system.

Sending a test email

After configuring email notification, you can send a test email to confirm your settings.

Prerequisites

- You must have the Storage Administrator (Initial Configuration) role to perform this task.

- The mail server must be completely configured before you begin.

To send a test email:

1. Click **Settings** > **Environmental Setting** > **E-mail Information**. The E-mail Information window opens.

2. Click to change to Modify mode.

3. Make sure that **Mail Notice** is set to **Enable** and that the settings in the window are correct.

4. Click **Test Send**. A confirmation message appears.

5. Click **OK**.

6. Confirm that mail clients received the email with the reference code 7FFFFF.

An example of a test email follows:

```
Date: FRI 03 AUG 2012 10:10:10 +9000 (JST)
To: husvm_alarm@xxx.com
From: xxxx@itg.hitachi.com
Reply-To: xxxx@itg.hitachi.com
Subject: HUS VM Report
```

```
Date : 03/10/2009
Time : 10:09:30
Machine : HUS VM (Serial# 265307)
RefCode : 7FFFFF
Detail: This is Test Report.
```

The field definitions in the test email are listed in the following table:

Table 5-1 Email details for system failures notice

#	Item	Description
1	Date	Date and time when the email was sent. This time stamp is set by the mail server.
2	To	Email address of the receiver.
3	From	Email address of the sender.
4	Reply-To	Email address to which replies from the receivers will be sent. Optional.
5	Subject	email title. (Name of the storage system) + (Report)
6	Date	Date when a system failure occurred.
7	Time	Time when a system failure occurred.
8	Machine	Name and serial number of the storage system.
9	RefCode	Reference code. The same code as the one reported by SNMP traps.
10	Detail	Failure details. The same information as the one reported by SNMP traps.

See the *Hitachi SNMP Agent User Guide* for reference codes and failure details.

Setting time periods

You can set the following Storage Navigator time periods:

- Polling period for monitoring who is changing information while others are viewing
- Time interval for monitoring disk controller and drive box status
- Time period that a user is logged out of the SVP because of a network error
- Time period when no changes are made that access the RMI server and the user is released from Modify mode as a result

You can also specify whether to show or hide the **Alerts** tab.

Prerequisite

You must have the Storage Administrator (Initial Configuration) role to perform this task. See .

To set time periods:

1. Start a web browser and enter the following URL to open the tool panel.

   `http://`*IP-address-or-host-name-of-SVP*`/cgi-bin/utility/`
   `toolpanel.cgi`
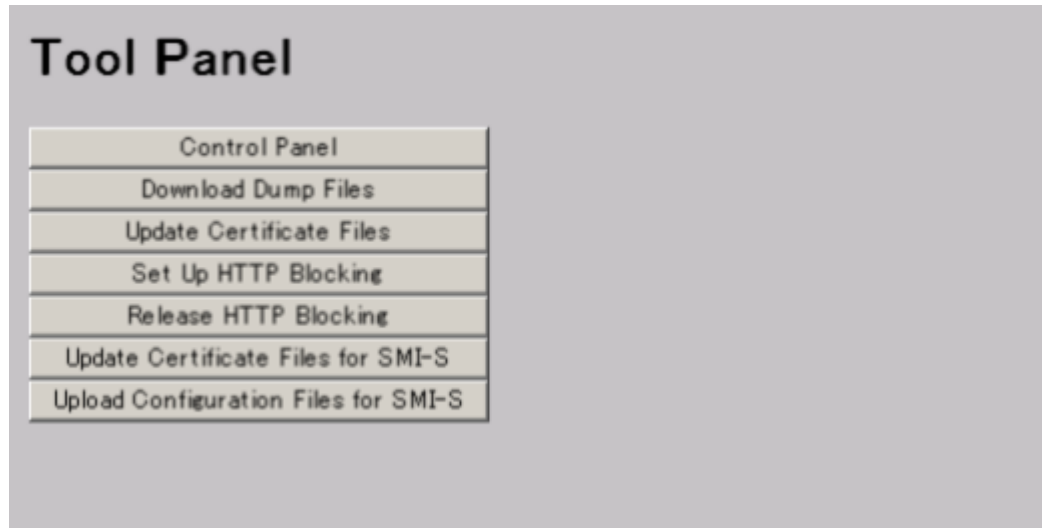
2. Click **Control Panel** to open the Control Panel.
3. Enter the user ID and password and click **Login**.
4. Click the **Set Env.** tab to open the Set Env. dialog box.
5. Specify the Storage Navigator parameters as required.
6. Click **Submit**.
7. Click **Exit** ( ) to close the Control Panel.
8. Log out of the Storage Navigator SVP and then log in again to make the new parameters take effect.
9. Back up the Storage Navigator configuration file by downloading the file from the SVP.

Storage Navigator environment parameters are described in the following table:

Table 5-2 Environment parameters

Item	Description
RMI time-out period	If the user cannot access the SVP for a certain period of time because of a network error, the RMI time-out logs the user out of the SVP.
	• The value of the RMI time-out period must be greater than the value set for the smallest polling period, either for checking exclusive lock or for checking obstacles (see below for those parameters). For example, specify a value of the RMI time-out period to satisfy the following condition:
	RMI time-out period > min [A, B]
	where
	A = Polling period for checking exclusive lock

Item	Description
	B = Polling period for checking obstacles, and min [A, B] indicates the minimum value selected from A and B. • The default is 1 minute. You can specify 1 minute, 5 – 60 minutes in 5-minute increments, 70 to 120 minutes in 10-minute increments, or one day (24 hours). • This parameter cannot be disabled.
RMI time-out period for Modify	If a user is in Modify mode but does not make any changes that access the RMI server for a specified period of time, Modify mode is released, and the View mode appears. • The default time period is 30 minutes. You can specify between 10 and 60 minutes in 10-minute increments, or between 120 and 360 minutes in 60-minute increments. • Specify **NO** to disable this parameter.
Polling period for checking exclusive lock	Specify the polling period for monitoring who is changing information while in Modify mode when other users are viewing the storage system information in View mode. The **Locked** and **Unlocked** icons are automatically updated either when a user who is in Modify mode either logs out from Storage Navigator or changes to View mode. • The shorter the time period you specify, the more frequently the Lock/Unlock status is updated, but this does increase network traffic. • The default time period is 35 seconds. You can specify 5 to 60 seconds in 5-second increments, or 70 to 120 in 10-second increments. • Specify **NO** to disable this parameter.
Polling period for checking obstacles	Specify a time interval to monitor the Disk Controller and Drive Box status, which is indicated by the **Alerts** window or the Storage Navigator secondary window. • The default time period is 110 seconds. You can specify 5 to 60 seconds in 5-second increments, and 70 to 120 seconds in 10-second increments for the parameter. • Specify **NO** to disable this parameter. • We recommend that you select **NO** when **Option to hide Alerts window** check box is selected.
Option to hide Alerts Window	Specify whether to display the **Alerts** window. If the **Hide Alerts Window** check box is selected, the **Alerts** tab does not appear. • By default, the check box is cleared. • We recommend that you select **NO** for **Polling period for checking obstacles** when the **Option to hide Alerts Window** check box is selected.

Backing up and restoring Storage Navigator configuration files

You can make backup copies of the various Storage Navigator configuration files by downloading them to a folder that you specify. You can then use the

backup copies to restore one or more configuration files if it becomes necessary.

Prerequisites

You must have one of the following roles, depending on the configuration you are backing up or restoring.

Table 5-3 Roles required to back up and restore configuration files

Configuration file	Description	Required role to back up a file	Required role to restore a file
User Account Information	User account information registered to the Storage Navigator.	Security Administrator (View Only)	Security Administrator (View & Modify)
Environment Parameter List	The parameters settings in the Set Env. window.	Storage Administrator (Initial Configuration)	Storage Administrator (Initial Configuration)
Log Transfer Information	Settings made in the Syslog, Audit Log Transfer windows, and the Edit SIM Syslog Server Settings window.	Audit log Administrator (View Only)	Audit log Administrator (View & Modify)
External Authentication	Connection to the authentication server.	Security Administrator (View & Modify)	Security Administrator (View & Modify)
Key Management Server	Connection to the key management server*	Security Administrator (View & Modify)	Security Administrator (View & Modify)
Password Policy	Password policy for backing up encryption keys on the Storage Navigator computer	Security Administrator (View & Modify)	Security Administrator (View & Modify)
* The client certificate in use when the key management (KMIP) server is connected cannot be backed up or restored by Storage Navigator. Consult the administrator of the key management server to determine the best way to use the server to manage and back up the certificate.			

To back up configuration files:

1. Start a web browser and enter the following URL to open the tool panel:

```
https://IP-address-or-host-name-of-SVP/cgi-bin/utility/
toolpanel.cgi
```


Tool Panel

- Control Panel
- Download Dump Files
- Update Certificate Files
- Set Up HTTP Blocking
- Release HTTP Blocking
- Update Certificate Files for SMI-S
- Upload Configuration Files for SMI-S
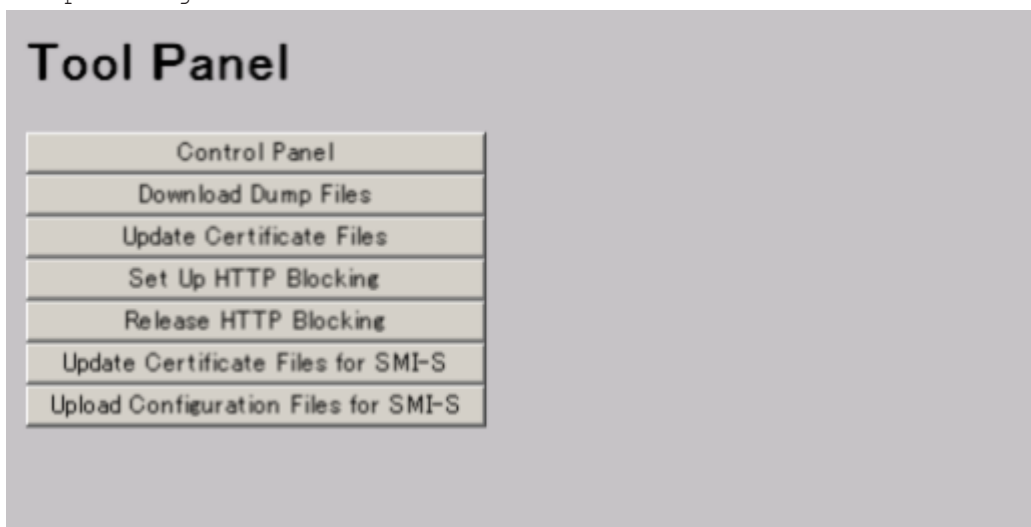
2. Click **Control Panel** to open the Control Panel.

3. Enter the user ID and password and click **Login**.

4. Click the **Download** tab to open the Download File Window.

5. Click the files to be downloaded. You can download only the files for which you have permission.

6. Click **Submit**. The Download File dialog box shows the list of the files to be downloaded.

7. Click **Download**. The File Download dialog box opens.

8. Click **Save**. The Save As dialog box opens.

9. Specify the name of a folder to save the compressed file, and then click **Save** to start downloading.

10. Decompress the downloaded `*.tgz` file as required. To decompress the `*.tgz` file, use the tool supporting tar and gzip.

To restore the configuration files:

1. Start a web browser and enter the following URL to open the tool panel:
   `http://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi`

2. Click **Control Panel** to open the Control Panel.

3. Enter the user ID and password and click **Login**.

4. Click the **Restore** tab to open the Restore File window.

5. Click the files and click **Browse** to specify the directory of the file. You can restore only the files for which you have permission.

6. Click **Next**.

7. Click the configuration files to restore.

8. Click **Submit**.

9. If the **Password check** dialog box opens, enter **User ID**, **Password**, and **Re-enter Password** of the storage administrator on the backup user list, and click **Submit** on the **Password check** dialog box.
   The Restore File dialog box opens.

10. Confirm the restoring process has been completed successfully.

11. Click **Close** to close the dialog box.

Setting syslog notification for SIMs

Setting and configuring syslog notification for SIMs

You can be notified in `syslog` format when storage system failures occur. Failures notified in `syslog` format are the same as failures reported by SIMs displayed in the Alerts window or failures reported by SNMP traps.

Prerequisites

- You must have the Storage Administrator (Initial Configuration) role to perform this task. See Table 4-2 Roles, Permissions, and Capabilities on page 4-8.
- You must have a server that supports `syslogs`.
- If a firewall is used, a port must be opened to transfer `syslogs`.

To configure settings for syslog notification:

1. Click **Settings** >**Environmental Setting**> **Edit SIM Syslog Server Settings**.
2. Select **Enable**, and enter the *IP Address* and *Port Number* to transfer syslogs to a primary server.
3. Select **Enable**, and enter the *IP Address* and *Port Number* to transfer syslogs to a secondary server.
4. Specify any name in the **Location Identification Name** field to identify the storage system.
5. Click **Finish**
6. Specify a *task name* and click **Apply**

Sending a test syslog

After configuring the syslog notification, send a test syslog to verify your settings.

Prerequisites

- You must have the Storage Administrator (Initial Configuration) role to perform this task. See Table 4-2 Roles, Permissions, and Capabilities on page 4-8.
- Complete the configuration of the syslog server.

To send a test syslog:

1. Click **Settings** > **Environmental Setting** > **Edit SIM Syslog Server Settings**.
2. Make sure that the servers are set to **Enable** and that the settings in the window are correct.
3. Check **Send a test message**.
4. Enter a name in the **Location Identification Name** field to identify the storage system.
5. Click **Finish**
6. Specify a *task name* and click **Apply**.
7. Confirm that the syslog servers received the following log: `RefCode: 7FFFFF, This is Test Report`.

_6_

License keys

Accessing software functionality requires a license key. This chapter provides information on license keys and instructions for installing, disabling, enabling, and uninstalling license keys.

☐ License keys overview

☐ License key types

☐ Using the permanent key

☐ Using the term key

☐ Using the temporary key

☐ Using the emergency key

☐ Estimating licensed capacity

☐ Installing and removing software

☐ Insufficient license capacity

☐ License key expiration

License keys overview

License keys are enabled automatically when you install them. At the same time, the functionality for the software that you installed is available in Storage Navigator.

License keys can be disabled when they are not needed. This allows you to conserve time on license that is good for only a specified time. For example, if you have a 365-day term key for a software product, the license server starts the count the day you install the key. However, if you don't need the license when you install it, you can disable the key and stop the counter from running. When you need the license, simply re-enable it.

This topic provides information in the order it is required:

- License key types on page 6-2. Lists the key types; explains whether keys are permanent or temporary; shows the term limit, if any; and provides the estimated license capacity, if required.
- Using the term key on page 6-3. Explains that you can conserve the term key when you are not using it.
- Using the temporary key on page 6-4. Explains that you can conserve the temporary key when you are not using it.
- Estimating licensed capacity on page 6-5. Provides information and instructions for calculating license capacity according to your system and organization requirements.
- Installing and removing software on page 6-7. Provides instructions for installing, disabling, enabling, and removing keys.
- Insufficient license capacity on page 6-10 and License key expiration on page 6-11 provide information for dealing with these situations.

License key types

To use a particular program product, you must enter a unique license key for the program product in Storage Navigator. License keys are provided when you purchase HUS VM software. The license key types are described in the following table:

⚠ **Caution:** If you overwrite a permanent key with a term key, you can use the software up to the licensed capacity of the term key until it expires. When the term key expires, if the licensed capacity of the permanent key is insufficient, operations you can perform are restricted. In this case, a SIM (7ff7xx) which indicates that the term key has expired is displayed in the storage system Alert window.

Table 6-1 License key types

Type	Description	Effective term*	Estimating licensed capacity
Permanent	For purchase	No limit	Required
Term	For purchase	365 days	Required
Temporary	For trial use before purchase (Try & Buy)	120 days	Not required
Emergency	For emergency use	30 days	Not required
*When you log in to Storage Navigator, a warning message appears if 45 days or less remain before the expiration.			

Using the permanent key

You can purchase the permanent key to use a program product indefinitely. You must estimate a licensed capacity required for using the program product and purchase a license key for the amount of the required capacity.

- If the license capacity is not enough, **Not Enough License** displays in the status field of the License Key window, and the program product is not enabled.

- If the capacity of the usable volume exceeds the licensed capacity while the storage system is running, for example, an LDEV was additionally installed, **Grace Period** displays in the status field of the License Key window. You can continue to perform the same operations, but the deficient amount of license must be purchased within 30 days.

- If the deficient amount of license is not installed, **Not Enough License** displays, and the program product is disabled.

Using the term key

You can purchase the term key to use the program product for a specific number of days. You must estimate a licensed capacity required for using the program product and purchase a license key for the amount of the required capacity.

- **Not Enough License** or **Grace Period** displays in the status field of the License Key window if there is a deficiency of the license capacity.

- You can enable or disable the term key for each program product. Unlike the temporary key and the emergency key, the number of days the term key is enabled is counted as the number of effective days of the term key rather than the number of elapsed days from the date of installation.

- The number of effective days is decremented by one day when the date changes to the next day.

For example, if the term key is set to be enabled for 150 days at the time of installation and the term key is disabled for 100 days and a total of 250 days have elapsed since the installation, the number of remaining effective days of the term key is 215 days. This is determined by subtracting 150 days from 365 days. By disabling the term key on the days when the program product is not used, you can prevent the unnecessary decrease of the period in which the term key can be used.

- If the term key is expired, **Not Installed** displays in the status field of the License key window, and the program product is disabled.

Using the temporary key

You can use the temporary key for trial purposes. The effective term is 120 days from the installation of the temporary key. The remaining days of the effective term are not increased even if the temporary key is reinstalled during the effective term. If you uninstall the temporary key though the effective term remains, **Not Installed** is displayed in the status field, **Temporary** is displayed in the Key Type field, and remaining days of the effective term are displayed in the Term (days) field of the License key window.

If the temporary key expires, you cannot reinstall the temporary key for 180 days. **Expired** displays in the status field of the License Key window, and the program product is disabled.

Using the emergency key

You can use the emergency key if the license key cannot be purchased if an emergency occurs, such as a system failure or a communication error.

You can also use the emergency key if the configuration of the program product that is installed by the temporary key remains in the changed status and cannot be restored to the original status. For example, if you do not plan to purchase the program product after using the temporary key for trial purposes, you can restore the changed configuration to the original status by temporarily enabling the program product with the emergency key.

Caution:

- If the emergency key is installed in the program product in which the permanent key, or the term key, is installed, the days of the effective term of the license key is 30 days. However, because the emergency key can be reinstalled during the effective term are, the days of the effective term can be restored to 30 days.
- In other scenarios, the emergency key can be installed only once.

Estimating licensed capacity

The licensed capacity is volume capacity that you are licensed to use with the program product. You need to estimate the amount of capacity which you want to use with the program product before you purchase the permanent key or the term key.

Software and licensed capacity

Two licensed capacity types are available. The one you choose depends on the software. The following table shows the licensed capacity types:

Table 6-2 Licensed capacity types

Type	Description
Mounted capacity/ Usable capacity	The licensed capacity is estimated using the capacity of all the LDEVs in the storage system.
Unlimited capacity	You can use the software regardless of the volume capacity.

Note: Licensed capacity starts at a minimum of 20TB and can be increased in 5TB increments up to a maximum of 80TB, at which time it is automatically upgraded to unlimited.

The following table lists the software and the licensed capacity.

Table 6-3 Software and licensed capacity

Option name	Licensed capacity	Notes
Basic Operating System Bundle		
Device Manager	Usable Capacity	
Storage Navigator	Usable Capacity	
Dynamic Provisioning	Usable Capacity	
Universal Volume Manager	Usable Capacity	For external capacity
SNMP Agent	Usable Capacity	
JAVA API	Usable Capacity	
SMI-S Provider	Unlimited	
Server Priority Manager	Usable Capacity	To use Server Priority Manager, first install Performance Monitor.
Encryption License Key	Unlimited	
LUN Manager	Usable Capacity	
Open Volume Management	Usable Capacity	
Volume Shredder	Usable Capacity	
Cache Residency Manager	Usable Capacity	

Option name	Licensed capacity	Notes
Performance Monitor	Usable Capacity	
Data Retention Utility	Usable Capacity	
Virtual Partition Manager	Unlimited	You may use up to four CLPRs without the Virtual Partition Manager license key. With a license key, you can define up to 32 CLPRs.
Resource Partition Manager	Unlimited	
Mobility Bundle		
Tiered Storage Manager	Usable Capacity	
Dynamic Tiering	Usable Capacity	To use Dynamic Tiering, first install Dynamic Provisioning.
Volume Migration V2	Usable Capacity	For information on Volume Migration V2, contact the Hitachi Data Systems customer support.
Replication Bundle		
Replication Manager	Usable Capacity	
TrueCopy	Usable Capacity	
Thin Image	Usable Capacity	To use Thin Image, first install Dynamic Provisioning.
Universal Replicator	Usable Capacity	To use Universal Replicator, first install TrueCopy.
High Availability Manager	Unlimited	To use High Availability Manager, first install TrueCopy.
ShadowImage	Usable Capacity	
Remote Replication Extended	Usable Capacity	To use Remote Replication Extended, first install Universal Replicator or TrueCopy.
Flash Acceleration	Unlimited	I/O performance is enhanced in I/O patterns with access to drives in a system containing SAS, SSD, or FMD drives.
Flash optimization	Unlimited	I/O performance is enhanced in I/O patterns with access to drives in a system containing SAS, SSD, or FMD drives.

Calculating licensed capacity for a normal volume

The normal volume capacity is the same as the capacity specified when creating the volume.

An example is shown in the following table:

Table 6-4 Example of estimating capacity for purchase

Item	Value
Volume emulation type	OPEN-V
Capacity of a volume	60 GB
Number of volumes	512
Total capacity of all the volumes	60 GB X 512 = 30,720 GB 30,720 GB / 1,024 = 30 TB
Estimated capacity for purchase	At least 30 TB

Calculating licensed capacity for an external volume

Use the following equation to calculate the licensed capacity for an external volume:

```
External Volume Capacity (KB) = Volume Capacity (number of
blocks) X 512 (bytes) / 1,024
```

Calculating pool capacity

The license capacity of Dynamic Provisioning is calculated using the total capacity of the Dynamic Provisioning pool. If you use Dynamic Provisioning V-VOLs as P-VOLs or S-VOLs of ShadowImage/TrueCopy/Universal Replicator, the license capacity of ShadowImage/TrueCopy/Universal Replicator is calculated using the page capacity allocated to the Dynamic Provisioning V-VOLs (that is, used pool capacity).

For more information on calculating pool capacity, see the *Hitachi Unified Storage VM Block Module Provisioning Guide*.

Installing and removing software

You must set up the shared memory before installing the following software:

- Volume Migration
- TrueCopy
- Universal Replicator
- ShadowImage
- Dynamic Provisioning
- Dynamic Tiering
- Thin Image

Contact technical support to find out whether the software listed above can be installed in the current configuration.

Installing software using a license key code

A Storage Administrator with modify permission can install license keys.

To install software by using the license key code:

1. Click **Settings** > **Environmental Setting** > **License Key**. The License Key window opens.

2. Click to change to Modify mode.

3. Select **Key Code** in Mode.

4. In **Key Code**, enter the license key code.

5. Click **Install**. The **Status** column changes to **Install**.

6. Click **Apply**. The status changes to **Installed**.

If installation fails, an error message window appears. Display error details by selecting the failed option and clicking **Detail**.

Installing software using a license key file

You can install multiple software in a single procedure using a license key file. The license key files are provided by HDS.

The required time for installing a license key file depends on the number of license keys included in the file. A file with 30 license keys can take about 3 minutes to install. A file with 1,000 license keys can take about 60 minutes to install.

Prerequisite

The license key file name can be up to 200 alphanumeric characters but cannot include the following symbols: " \ ; : , * ? < > | / .

To install software using the license key file:

1. Click **Settings** > **Environmental Setting** > **License Key**. The License Key window opens.

2. Click to change to Modify mode.

3. From **Mode**, click **File**. The **Browse** button becomes available.

4. Click **Browse** to display the dialog box, and select the license key file (the file extension is `plk`) to be used for installing options on the displayed window. The selected file name appears in the **File Name** text box.

5. Click **Install**.

6. Click **Apply**. The status changes to **Installed**.

7. If installation fails or an error occurs during the installation, a message appears listing the failed options. To display the error details in the dialog box, select the failed option and then click **Detail**.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

When the status is Installed (Disabled)

If you do not install the prerequisite software or set up shared memory before you install the license key software, the software will install correctly but will be disabled after you install it. To enable the license key, install the prerequisite software and/or set up the shared memory. then enable the license key. See the following table for details.

Causes	Recommended Actions
The prerequisite software was not installed before the license key software was installed.	Install the required prerequisite software. See Software and licensed capacity on page 6-5.
The shared memory was not set up before the following license key software was installed. • Volume Migration • TrueCopy • Universal Replicator • ShadowImage • Dynamic Tiering	Set up the shared memory, and then enable the license. See Enabling or disabling a license on page 6-9.

Enabling or disabling a license

The term key can be enabled or disabled. You can also enable a license when you install more than one software product. However, some software may not be available because the requirements for these products are not satisfied. When this is the case, satisfy the requirements first, then enable the license.

To enable or disable the license:

1. Click **Settings** > **Environmental Setting** > **License Key**. The License Key window opens.
2. Click ![icon] to change to Modify mode.
3. Select the software from the list.
4. In **License Status**, select **Enable** or **Disable**.
5. Click **Set**. The **Status** column changes to **Install** or **Install (Disabled)**.
6. Click **Apply**. The status changes.

Removing software

To remove software:

1. Click **Settings** > **Environmental Setting** > **License Key**. The License Key window opens.
2. Click ![icon] to change to Modify mode.
3. Select the desired option that you want to remove from the list.

4. From Mode, click **Key Code**.

5. Click **Uninstall**. The status changes to **Remove**.

6. Click **Apply**. The status changes from **Installed** to **Not Installed**.

7. On rare occasions, a software option that is listed as **Not Installed** but still has available licensed capacity (shown as *XX* TB) might remain in the list. In this case, select that option and select **Uninstall** to reset the information.

Removing Data Retention Utility

When you remove Data Retention Utility, an error might occur even if the **Permitted Volumes** column of the License Key window indicates that the licensed capacity is *0TB*.

To resolve the error and continue removal:

1. Click **Actions** > **Other Function** > **Data Retention** to open the Data Retention window.

2. In the Data Retention window, find logical volumes that are unusable as S-VOLs (secondary volumes).

3. Change the settings so that the logical volumes are usable as S-VOLs.

4. Click **Settings** > **Environmental Setting** > **License Key** to open the License Key window, and then remove Data Retention Utility.

Insufficient license capacity

Using Dynamic Provisioning

If license capacity becomes insufficient, a message appears when you log in to Storage Navigator.

If you use Dynamic Provisioning, the licensed capacity might become insufficient because the used capacity of Dynamic Provisioning pools could increase even if you do not add any volumes. If this occurs, you must purchase an additional license within 30 days to cover the capacity shortage. For details on how to calculate pool capacity, see the *Hitachi Unified Storage VM Block Module Provisioning Guide*.

Deleting LDEVs, pairs, or pool volumes

When the licensed capacity exceeds the mounted capacity after you reduce the number of LDEVs, pairs or pool volumes, **a Grace Period** or **Not Enough License** message might appear in the **Status** column in the License Key window. If this occurs, use the **Available** button to refresh the status.

To refresh the license status:

1. Click **Settings** > **Environmental Setting** > **License Key**. The License Key window opens.

2. Click ![icon] to change to Modify mode.

3. In Mode, click **Available**.

4. Click **Install**. The **Status** column changes to **Install**.

5. Click **Apply**. The status changes to **Installed**.

License key expiration

If the license key for software-A expires, the license key of software-B is also disabled if it requires an enabled software-A. In this scenario, **Installed (Disabled)** appears for software-B in the **Status** column of the **License Key** window. After that, when you re-enable software-A, software-B is also re-enabled. If the **Status** column for software-B continues to display **Installed (Disabled)**, go to the **License Key** window and manually change the status of software-B back to I**nstalled**.

After your license key expires, no new configuration settings can be made, and no monitoring functions can be used with Performance Monitor. Configuration settings made before the expiration of the license key remain in effect. You can cancel configuration changes for some software.

Configuration changes for Performance Monitor may be cancelled on the **Port Control** window from the SVP but not from the Storage Navigator computer.

Configuration changes for some other software products can be cancelled from SVP. These configuration changes cannot be cancelled from your Storage Navigator computer.

You can cancel configuration changes from SVP for the following software products:

- ShadowImage
- TrueCopy
- Universal Replicator
- High Availability Manager
- Remote Replication Extended
- LUN Manager
- Volume Migration
- Data Retention Utility

Configuration changes for the following software products cannot be deleted:

- Open Volume Management
- Cache Residency Manager

7

Viewing and managing the storage system

This chapter describes how to navigate to storage system information, create and download system configuration reports, and manage Storage Navigator tasks.

☐ Viewing and managing overview

☐ Viewing storage system information

☐ Managing tasks

☐ Using reports to verify system changes

Viewing and managing overview

This topic shows you how to do the following tasks in Storage Navigator:

- Perform basic navigation to storage system information. See Viewing storage system information on page 7-2.
- Create, download, and delete system configuration up to 20 reports. See Viewing a Storage Navigator report on page 7-8.
- Manage the queued operations you performed in Storage Navigator. This includes a discussion about tasks, and suspending, resuming and deleting tasks. Managing tasks on page 7-6.

Viewing storage system information

This topic describes high-level system information that is available in Storage Navigator. It also describes how to view this information in another application, how to create reports, and how to manage tasks.

The storage system information appears immediately when you start Storage Navigator.

Viewing basic information

The main window shows basic information about the storage system.

Viewing specific information

You can view more specific information when you make a selection in the resource tree in the left pane.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide
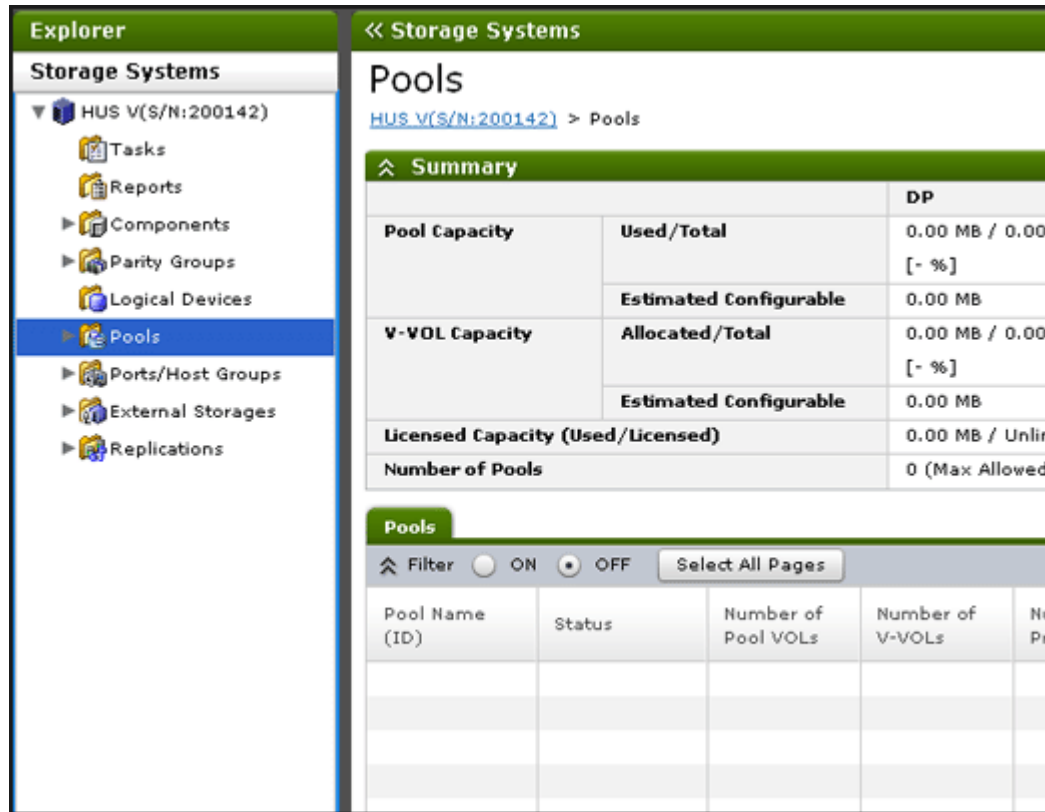
Viewing other system information

You can also find other system information such as a port status and data regarding used and unused resources. This information displays in a Storage Navigator secondary window.

To view other system information:

1. Click **Settings** > **Environmental Setting** > **License Key**. Java starts.
2. If a message appears and asks if you want to run the Java application, click **Run**. The Storage Navigator secondary window opens.
3. In the Storage Navigator secondary window, click **File** > **Basic Information**. The **Basic Information Display** dialog box opens.
4. Click the tab to display the **Basic Information Display** dialog box.
5. To save information in the dialog box, click **Export**. In the dialog box that opens, enter location and file name, then click **Save**.

Viewing port locations

You can view port locations by clicking **Actions** > **Component** > **View Port Location**.

Figure 7-1 Port Location window

Each cluster has up to 8 channel blades (CHBs) and the name of each CHB appears on the header of the port list. The icons show the port name, port LED status, and equipment information of port.

- 1A : This port is equipped and is currently in use. The cable is properly set. This port is available for the operation.

- 1A : This port is equipped and available for the operation.

- 1A : This port is not equipped or not available.

Status icons for certain resources

The status of certain resources is indicated by the following icons:

Status	Description
🟢	The resource can be used normally.
⚠	The resource has the following status: • The resource can be used, but has a limit on I/O performance and so on. • The status of the resource is changing. • The status of the resource is being confirmed.

Status	Description
	• The resource has subresources of different status. For example, parity groups are in this status if the statuses of logical volumes in the parity groups are not the same. In this case, the subresources might be blocked. Confirm the status of subresources.
	The resource has the following status: • The resource cannot be used because it is blocked due to a failure or maintenance operations. • The status of the resource is unknown. Restore the resource to the normal status.

Managing tasks

This topic describes tasks and the **Tasks** window, and provides instructions for managing tasks.

Because Storage Navigator operations are executed in the background, you start the next task immediately after performing the previous one. You keep track of your tasks' progress by entering a task name during each Storage Navigator procedure and then tracking its status and other information using the **Task** window.

- Each procedure you perform requires a task name. For example, when you provision or configure the system, create a pair, or any other procedure, you must assign a name for the task.
- Each task is queued and then processed by the storage system in the order of its arrival.

Only one task is executed at the same time, except for the following. In the case of the following operations, the next task may be executed before the current task completes or fails.

- Create LDEVs
- Format LDEVs
- Shred LDEVs
- Shrink Pool
- Editing encryption

Tasks window

The **Tasks** window can display 384 tasks, including up to 128 tasks with a status of In Progress, Waiting, and Suspended, and up to 256 tasks with a status of Completed and Failed. If the number exceeds these limits, the oldest completed tasks are automatically removed from the window.

Managing your tasks

Storage Navigator allows you to suspend, resume, cancel, and prevent tasks from being automatically deleted.

Prerequisites

- Users that execute the task or users with Storage Administrator (System Resource Management) role can view the details of tasks.
- Users with Storage Administrator (System Resource Management) can delete, suspend, resume tasks, and enable or disable auto-deletion of tasks.

To modify a task:

1. In the tree, click **Storage Systems > Tasks**. The list of tasks appears.
2. In the list, click the task or tasks that you want to modify.
3. In the bottom right corner of the window, click the corresponding button for the task you want to perform:

   - Click **Delete Tasks** to delete or cancel a task.
   - Click **Suspend Tasks** to suspend a queued task.
   - Click **Resume Tasks** to resume a suspended task.
   - Click **More Actions** > **Enable Auto Delete** to delete tasks from the Task list when they have completed and the task list is full. This allows you to check for completed tasks and to clear the list when the limit (384) is reached.
   - Click **More Actions** > **Disable Auto Delete** to keep tasks in the task list after the tasks are completed.

4. Verify the displayed settings and click **Apply**.

Stalled tasks

If a queued task is not performed over a reasonable period, check the following:

- Did the task fail? Click **failed** to view the reason. then delete the task, correct the problem, and try the task again.
- Are too many tasks in the task list because **Auto Delete** is disabled? Click **Enable Auto Delete** to remove tasks from the window.
- Is another program changing the storage system configuration? Check this by observing whether **Resource Lock** is displayed for too long a time. If so, verify that another program is running and then wait until its changes are completed.
- The percentage of progress of an ongoing task may not change if another operation is in progress.

Setting the status refresh interval of the Tasks window

The Tasks window automatically updates every 60 seconds by default. This interval can be changed using the following procedure.

To change the refresh interval:

1. Click **Settings > Environmental Setting > Edit Information Display Settings**.

2. Specify the interval for Task Screen Refresh Interval. If **No Update** is specified, the Tasks window will not be automatically updated. In this case, to refresh the window, you must use **Refresh View** or **Refresh Al**l.

3. Click **Apply**.

Using reports to verify system changes

This topic explains Storage Navigator reports and provides instructions for creating, viewing, and deleting them.

You can create reports of your storage system's physical configurations and logical settings. Doing this provides a copy of the settings when you intend to make changes. If you make a similar report after the changes, then you can compare the reports to verify that new settings were made as intended.

Storage Navigator reports can be saved in a CSV or HTML file. Tables in the HTML version of the configuration report are sortable.

Creating a configuration report

You can use the report configuration tool to create up to 20 configuration reports and then view or download them.

To create a configuration report:

1. From **General Tasks**, click **Create Configuration Report**.

2. Specify a task name and click **Apply**. This task name is used as the report name in the Reports window. This process takes approximately 10 minutes to complete.

3. Click **Refresh View** to update the Reports window. The created report appears in the list.

Viewing a Storage Navigator report

Adobe Flash Player is necessary to view reports. For details on Flash Player, see General restrictions on page 3-6 and Installing Adobe Flash Player on page 2-22.

Prerequisite

- Users that create the report or users with Storage Administrator (Initial Configuration) role can view the report.

To download and view a report:

1. In the Storage Navigator tree, click **Storage Systems** > **Reports**.
2. Specify the report to download.
3. Click **Download Reports**.
4. Specify a folder in which to save a `.tgz` file.
5. Extract the downloaded `.tgz` file.
6. Display the report in the following ways:
   For an HTML format report:
   Open html\index.html file in the extracted folder.
   For a CSV format report:
   Open a csv file in the csv folder in the extracted folder.

To display a report in the Reports window

You can view only HTML format reports in the **Reports** window. You can view CSV format reports in the previous procedure.

1. Click **Storage Systems > Reports**.
2. Click the report name to display in the **Reports** window.
   The report is displayed in the **Reports** window.
   In the **Reports** window, click the reports name in the list at the left, and you can view the report at the right.

For details about each report, see Appendix A, Storage configuration reports on page A-1.

Deleting a configuration report

You can delete a report when you no longer need it, or to make room in the **Reports** window when the report limit is about to be reached.

Prerequisite

Users that create the report or users with Storage Administrator (Initial Configuration) role can delete a configuration report.

To delete a report:

1. In the tree, click **Storage Systems** > **Reports**.
2. Specify the report to delete.
3. Click **Delete Reports**.
4. Click **Apply**.

Creating a configuration report using the Report Configuration Tool

You can create a configuration report by using a command prompt when you use the Report Configuration Tool. By preparing a script file that contains a series of commands and scheduling a task in Windows to execute the script

at regular intervals, you can automate the creation and the deletion of the configuration report.

Preparing a script file

Before creating the configuration report, you will need to write a series of commands in a script file. When you run the Report Configuration Tool, the commands in the script files execute sequentially and then create or delete a configuration report. See Appendix B, Report Configuration Tool command reference (raidinf commands) on page B-1 for a list of commands.

Two examples of scripts are shown next. You can refer to these examples and create a script file that suits your needs.

- Script example for creating a configuration report on page 7-10
- Script example for downloading a configuration report on page 7-11

Script example for creating a configuration report

This script logs the user in, deletes a configuration report, creates a configuration report, and logs the user out, using the Report Configuration Tool.

For each command, except the logout command, this example performs three retries at intervals of 2 minutes, assuming that communication errors and other errors can occur. In addition, the `delete report` command is executed with the `-fill` option before the `add report` command, so that the script does not terminate when 20 configuration reports accumulate in the SVP.

```
REM
REM Create Report Script(CreateReport.bat)
REM
SET USER=<Username for Storage Navigator>
SET PASS=<Password for Storage Navigator>
SET SERVER=<Hostname or IP address of SVP>
SET REPORT_NAME=DailyConfigurationReport
SET LOOP=2
REM LOOP:0-2 3Times
SET TIMEOUT=121
REM TIMEOUT 2[minutes]=120[s]
SET RAIDINF_PATH="C:\Program Files\raidinf"
SET /a CNT_LOGIN=0

:LOGIN_RETRY
REM ########################### LOGIN %CNT_LOGIN%
SET /a CNT_LOGIN=%CNT_LOGIN% + 1
%RAIDINF_PATH%\raidinf -login %USER% %PASS% -servername %SERVER%
if ERRORLEVEL 1 (
     if %CNT_LOGIN% GTR %LOOP% GOTO :ABEND
          CALL :SLEEP
          GOTO LOGIN_RETRY
)

SET /a CNT_DEL=0
:DEL_RETRY
REM ########################### DELETE %CNT_DEL%
SET /a CNT_DEL=%CNT_DEL% + 1
```

```
%RAIDINF_PATH%\raidinf delete report -servername %SERVER% ^
-report %REPORT_NAME% -fill
if ERRORLEVEL 1 (
          IF %CNT_DEL% GTR %LOOP% GOTO :ABEND
          CALL :SLEEP
          GOTO :DEL_RETRY
)

SET /a CNT_ADD=0
:ADD_RETRY
REM ########################### ADD %CNT_ADD%
SET /a CNT_ADD=%CNT_ADD% + 1
%RAIDINF_PATH%\raidinf add report -servername %SERVER% -report ^
%REPORT_NAME%
if ERRORLEVEL 1 (
          IF %CNT_ADD% GTR %LOOP% GOTO :ABEND
          CALL :SLEEP
          GOTO ADD_RETRY
)
GOTO :END
EXIT /B

:SLEEP
REM
REM ########################### SLEEP with %TIMEOUT% sec
REM
ping 127.0.0.1 -n %TIMEOUT% > NUL
EXIT /B

:ABEND
REM ########################### ABEND
ECHO "Create Report Script was ABEND"

:END
REM ########################### Logout
%RAIDINF_PATH%\raidinf -logout -servername %SERVER%
```

Script example for downloading a configuration report

This script logs the user in, downloads a configuration report, and logs the
user out, using the Report Configuration Tool.

For each command except the logout command, this example performs 3
retries at intervals of 2 minutes, assuming that communication errors and
other errors can occur. The downloaded configuration report is accumulated
for 3 generations in the `C:\Reports` folder by names from
`Report_DailyConfigurationReport_1.tgz` to
`Report_DailyConfigurationReport_3.tgz`. In addition, if the script for
creating a configuration report fails, generation copy is terminated so that the
past configuration reports may not be overwritten.

```
REM
REM Download Report Script(DownloadReport.bat)
REM
SET USER=<Username for Storage Navigator>
SET PASS=<Password for Storage Navigator>
SET SERVER=<Hostname or IP Address of SVP>
SET REPORT_NAME=DailyConfigurationReport
SET LOOP=2
```

```
REM LOOP:0-2 3Times
SET TIMEOUT=121
REM TIMEOUT 2[minutes]=120[s]
SET TARGETFOLDER=C:\Reports\tmp
SET REPORTFOLDER=C:\Reports
SET RAIDINF_PATH="C:\Program Files\raidinf"
REM
REM Create Report Folder
REM
IF NOT EXIST %REPORTFOLDER% (
         MKDIR %REPORTFOLDER%
         IF NOT EXIST %TARGETFOLDER% (
                  MKDIR %TARGETFOLDER%
             )
)

SET /a CNT_LOGIN=0
:LOGIN_RETRY
REM ################################### Login %CNT_LOGIN%
SET /a CNT_LOGIN=%CNT_LOGIN% + 1
%RAIDINF_PATH%\raidinf -login %USER% %PASS% -servername %SERVER%
if ERRORLEVEL 1 (
         IF %CNT_LOGIN% GTR %LOOP% GOTO :ABEND
         CALL :SLEEP
         GOTO LOGIN_RETRY
)

SET /a CNT_DL=0
:DL_RETRY
REM ################################### Download %CNT_DL%
SET /a CNT_DL=%CNT_DL% + 1
%RAIDINF_PATH%\raidinf download report -servername %SERVER% ^
-report %REPORT_NAME% -targetfolder %TARGETFOLDER%
if ERRORLEVEL 1 (
         IF %CNT_DL% GTR %LOOP% GOTO :ABEND
         CALL :SLEEP
         GOTO :DL_RETRY
)

REM ################################### Create Error Check
IF EXIST %REPORTFOLDER%\Report_%REPORT_NAME%_1.tgz (
         IF EXIST %TARGETFOLDER%\Report_%REPORT_NAME%.tgz (
                  GOTO :FC_CHECK
         ) else (
                  GOTO :CHECK_END
         )
) else (
         GOTO :CHECK_END
)

:FC_CHECK
FC /B %REPORTFOLDER%\Report_%REPORT_NAME%_1.tgz ^
%TARGETFOLDER%\Report_%REPORT_NAME%.tgz > NUL
if ERRORLEVEL 1 (
         REM
) else (
          DEL %TARGETFOLDER%\Report_%REPORT_NAME%.tgz
          GOTO :END
)
```

```
:CHECK_END
REM ##################################### Migrate Reports
IF EXIST %TARGETFOLDER%\Report_%REPORT_NAME%.tgz (
        IF EXIST %REPORTFOLDER%\Report_%REPORT_NAME%_2.tgz (
                COPY %REPORTFOLDER%\Report_%REPORT_NAME%_2.tgz ^
%REPORTFOLDER%\Report_%REPORT_NAME%_3.tgz
        )
        IF EXIST %REPORTFOLDER%\Report_%REPORT_NAME%_1.tgz (
                COPY %REPORTFOLDER%\Report_%REPORT_NAME%_1.tgz ^
%REPORTFOLDER%\Report_%REPORT_NAME%_2.tgz
)
        IF EXIST %TARGETFOLDER%\Report_%REPORT_NAME%.tgz (
                COPY %TARGETFOLDER%\Report_%REPORT_NAME%.tgz ^
%REPORTFOLDER%\Report_%REPORT_NAME%_1.tgz
                DEL %TARGETFOLDER%\Report_%REPORT_NAME%.tgz
        )
)
GOTO :END
EXIT /B

:SLEEP
REM ##################################### SLEEP with %TIMEOUT%
ping 127.0.0.1 -n %TIMEOUT% > NUL
EXIT /B

:ABEND
REM ##################################### ABEND
ECHO "Download Report Script was ABEND"

:END
REM ##################################### Logout
%RAIDINF_PATH%\raidinf -logout -servername %SERVER%
```

Executing a regularly scheduled script file

To execute the created script file on a regular basis, register it as a scheduled task in Windows.

The following procedure uses the Windows `schtasks` command to register the script files created in the example shown in as tasks of Windows.

Registration example

- Create a configuration report at 21:00 every day (`CreateReport.bat`).
- Download a configuration report at 22:00 every day (`DownloadReport.bat`).

Procedure

1. Store the two script files in the C:\Reports folder.
   ```
   C:\Reports
      CreateReport.bat
      DownloadReport.bat
   ```
2. Run the Windows `schtasks` command to register the two script files as a task of Windows.

Make sure that the *<Username for Windows>* parameter of this command is a user who has write permissions to the following two folders.

- `C:\Reports` folder
- The log folder in the installation folder of the Report Configuration Tool.

```
schtasks /create /tn CreateReport /tr "C:\Reports
\CreateReport.bat" /sc DAILY /st. 21:00:00 /ru <Username
for Windows> /rp <Password for Windows> schtasks /
create /tn DownloadReport /tr "C:\Reports
\DownloadReport.bat" /sc DAILY /st 22:00:00 /ru <Username
for Windows> /rp <Password for Windows>
```

3. Run the `schtasks /Query` command to confirm that the Windows task is registered.

```
C:\>schtasks /Query

Task name         Time of next execution    Status
==============  ========================  ===============
CreateReport    21:00:00, 2011/05/17
DownloadReport 22:00:00, 2011/05/17
```

Example execution and explanation of script files

- The first time you execute the script files to create a configuration report and download a configuration file, the file Report_DailyConfigurationReport_1.tgz is created in the `C:\Reports` folder.

```
C:\Reports
   CreateReport.bat
   DownloadReport.bat
   Report_DailyConfigurationReport_1.tgz
```

- On the second day:

  `Report_DailyConfigurationReport_1.tgz` is renamed `Report_DailyConfigurationReport_2.tgz`, and `Report_DailyConfigurationReport_1.tgz` is newly created.

- From the third day on:

  `Report_DailyConfigurationReport_1.tgz` and `Report_DailyConfigurationReport_2.tgz` are renamed `Report_DailyConfigurationReport_2.tgz` and `Report_DailyConfigurationReport_3.tgz`, and `Report_DailyConfigurationReport_1.tgz` are newly created. Because `Report_DailyConfigurationReport_3.tgz` is overwritten, the reports for three days are always accumulated in the `C:\Reports` folder.

```
C:\Reports
  CreateReport.bat
  DownloadReport.bat
  Report_DailyConfigurationReport_1.tgz <-Generated today
  Report_DailyConfigurationReport_2.tgz <-Generated yesterday
  Report_DailyConfigurationReport_3.tgz <-Generated two days ago
```

Error in executing Report Configuration Tool

When using the Report Configuration Tool, you may see Storage Navigator error codes and other error codes that are unique to the Report Configuration Tool. For Storage Navigator error codes, see the manual *Hitachi Storage Navigator Messages*. The error codes unique to the Report Configuration Tool and the corresponding actions are as follows.

Error code	Error message	Cause of error and action	Return value
EW_COMERR	A certificate does not become effective. Please login again.	A certain period of time elapsed after a login. Log in again.	131
EW_COMERR	Login is necessary. Please login again.	A command was entered before logging in. Log in and then enter the command.	131
EW_ENFILE	No such folder. Please refer to the help.	The specified folder to download to is not found. See Appendix B, Report Configuration Tool command reference (raidinf commands) on page B-1 and specify the parameter again.	131
EW_ENOMEM	Memory allocate error. Please other program terminate.	Allocation of internal memory fails. Close unnecessary programs or reboot the server.	245
EW_INVOPA	Report name reserved. Please check input '-report' parameter.	You cannot use the report name specified by the -report option. Check the report name and specify a new one.	131
EW_INVOPT	Invalid option. Please refer to the help.	The hyphen (-) is not added to the option parameter. See Appendix B, Report Configuration Tool command reference (raidinf commands) on page B-1 and specify a new parameter.	131
EW_LNGARG	Argument too long. Please refer to the help.	Either of the following causes is possible. • The length of a parameter of the command exceeds 256 bytes. • The length of all the parameters of the command exceeds 1,021 bytes. See Appendix B, Report Configuration Tool command reference (raidinf commands) on page B-1 and specify a new parameter.	131
EW_MAXAPP	Maximum application start.	The maximum number of Savable that you can connect	131

Error code	Error message	Cause of error and action	Return value
	Please check starting application.	simultaneously is exceeded. Log out of unnecessary SVPs and reconnect.	
EW_MAXARG	Maximum argument. Please refer to the help.	The number of parameters of the command exceeds 10. See Appendix B, Report Configuration Tool command reference (raidinf commands) on page B-1 and specify a new parameter.	131
EW_REQOPT	Required option list. Please refer to the help.	The required option and parameters were not entered. See Appendix B, Report Configuration Tool command reference (raidinf commands) on page B-1 and specify a valid option and parameters.	131
EW_SYSERR	System error. Please call to service center.	An internal error occurred. Contact Hitachi Data Systems customer support.	131
EW_SYSERR	Install path is too long. Specify the install path with up to 240 bytes.	The installation path exceeds 240 bytes. Specify no more than 240 bytes.	131
EW_SYSERR	Certificate file invalid. Please call to service center.	Updating certificate file fails. Contact Hitachi Data Systems customer support.	131
EW_SYSERR	The file is illegal. Please move 'raidinfcer' file from the installation directory.	The installation directory includes a file that will overlap with another file to be created by the Report Configuration Tool and the Report Configuration Tool cannot start. Remove the overlapping file from the installation directory.	131
EW_SYSERR	Log file invalid. Please call to service center.	The log file cannot be accessed. Contact Hitachi Data Systems customer support.	131
EW_UNWCMD	Unknown command. Please refer to the help.	The syntax of the command is not valid. See Appendix B, Report Configuration Tool command reference (raidinf commands) on page B-1 and enter a valid parameter.	230
EW_UNWOPT	Unknown option. Please refer to the help.	The option and parameter are not valid. See Appendix B, Report Configuration Tool command reference (raidinf commands) on page B-1 and	252

Error code	Error message	Cause of error and action	Return value
		input a new option and parameter.	
EW_UNWOPT	Invalid environment value. Please confirm the setting of HTTP_PROXY.	Unable to connect to the proxy server specified by the environment variable. Check the proxy server name.	252
EW_WEBERR	Web access error. Please confirm the setting of server.	An internal error occurred while connecting to the server. Check the setting of the server.	131
EW_WEBERR	Server name can not be resolved. Please check the setting of server name.	The server specified by the –servername option does not exist. Check the server name and specify a new server.	131
EW_WEBERR	Server is no response. Input argument server is incorrect or server is not ready.	No response from the server specified by the–servername option. Make sure that: • The correct server name is specified. • The settings of the server are correct.	131
EW_WEBERR	Web access error. Please check your network equipment and cables.	An internal error occurred while connecting to the server. Check the network devices and cables.	131
EW_WEBERR	Web access error. Please confirm the setting of proxy server.	An internal error occurred while connecting to the proxy server. Check the settings of the proxy server.	131
EW_WEBERR	Proxy server name can not be resolved. Please check the setting of proxy server name.	Unable to connect to the proxy server specified by the environment variable. Check the proxy server name.	131
EX_CMDRJE	The control command rejected.	The execution of the entered command was rejected by the server. Check the error messages of Storage Navigator.	221

Viewing and managing the storage system

8

Troubleshooting

This chapter provides information for identifying and correcting problems with Storage Navigator.

☐ Getting help

☐ General troubleshooting

☐ Checking alerts

☐ Login errors

☐ Java application errors

☐ No-response errors

☐ Incorrect display errors

☐ UNIX operation errors

☐ Other errors

☐ Clearing Java and web browser caches

☐ Firefox web browser problems on UNIX

☐ Downloading dump files using the FD Dump tool

☐ Saving Java log and trace files

Getting help

If you have difficulty with any of the procedures included in this chapter, or if a procedure does not provide the answer or results you expect, contact Hitachi Data Systems support. See Getting help on page xvii in the preface of this manual.

General troubleshooting

A system administrator is responsible for the operation and normal maintenance of the Storage Navigator web client. The following are guidelines for troubleshooting the Storage Navigator web client:

- Check the cabling and the LAN. Verify that both the computer and LAN cabling are firmly attached, and that the LAN is operating properly.

- Reboot the computer. Close any programs that are not responding. If necessary, reboot the Storage Navigator computer and restart a Storage Navigator web client session.

- Check for any general error conditions. For a complete list of Storage Navigator error codes, see the *Hitachi Storage Navigator Messages* manual.

- Check the alert icon. Confirm the severity level of the storage system alert by clicking **Alert** on the Storage Navigator main window. If you cannot resolve an error condition, contact Hitachi Data Systems customer support.

The following figure shows the workflow for troubleshooting:
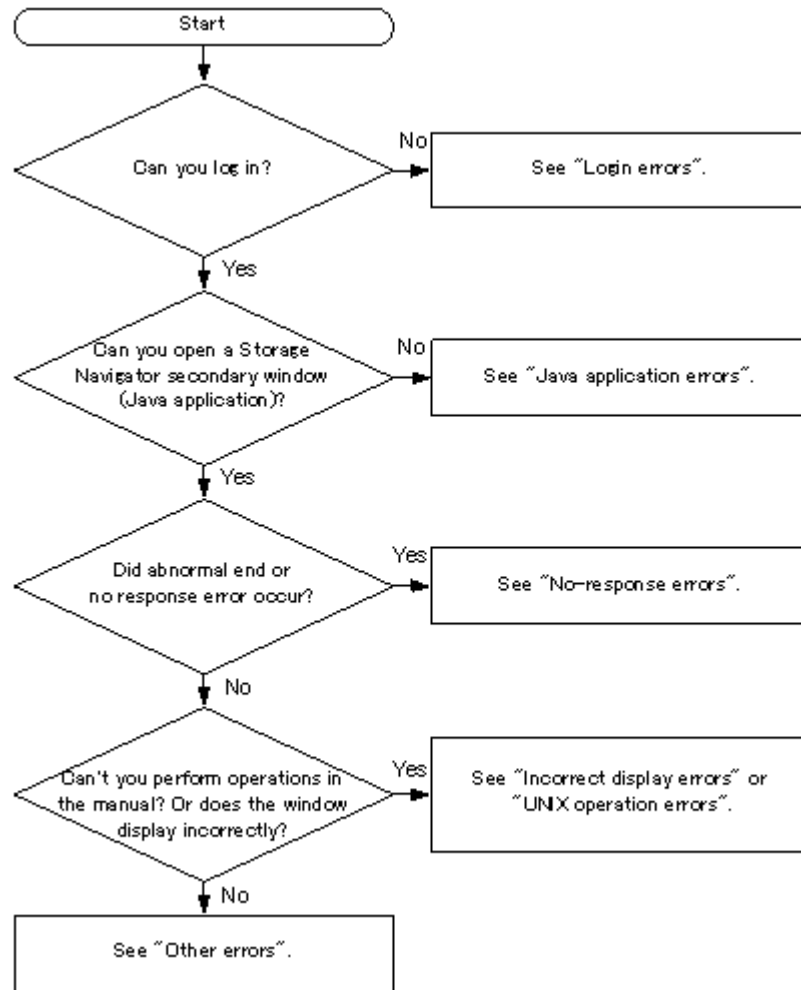
Figure 8-1 Troubleshooting workflow

Checking alerts

The Storage Navigator main window displays an icon indicating whether service information messages (SIMs) occurred in the storage system.

To check details of a SIM:

1. In the Storage Navigator main window, click **Alert**. The **Alerts** window opens.

Figure 8-2 Alert icon on Storage Navigator main window

2. To check the details of each alert, select one row, and then click **Detail**. The Alert Properties window opens.

3. If the following SIM reference codes appear, you must resolve the error (XXX indicates the pool ID):

   ○ 601XXX, 602XXX, 602FFE, 624000 (for Thin Image)

- 620XXX, 621XXX, 622XXX, 624000, 625000, and 626XXX (for Dynamic Provisioning)

For details on how to resolve the error, see the *Hitachi Unified Storage VM Block Module Provisioning Guide* or the *Hitachi Thin Image User Guide*.

Login errors

The following table lists login errors:

Table 8-1 Login errors

	Error condition	Probable cause / Recommended action
1	The page is not displayed because of an invalid syntax error.	Enter the URL of the desired SVP in the **Trusted sites** section of the Internet Options dialog box.
2	Storage Navigator does not start even with repeated attempts.	• Close all the web browser windows and then clear the Java and web browser cache. • Use the Task Manager to check for 'hung" or duplicate processes.
3	A network error occurred when you logged in to Storage Navigator.	Close all dialog boxes and log in to the Storage Navigator again. If the same error occurs, check the network environment.

Java application errors

The following table lists Java application errors:

Table 8-2 Java application errors

	Error condition	Probable cause / recommended action
1	When you click the Storage Navigator menu, the system does not respond. One minute later, application error (20020,108000) occurs.	The pop-up blocker function of your web browser might restrict Storage Navigator. If the problem still continues after you perform the operation multiple times, perform one or both of the following actions: • Disable the pop-up blocker function of your web browser. • Disable the pop-up blocker function of any browser plug-in/add-on. If neither of the above can be performed in Internet Explorer, you can open the window by clicking the Storage Navigator menu while holding down the **Ctrl** key. Another possible cause is that a Java application was not allowed to start. If a message appears and asks if you want to run an application, click **Run**. Java content might be disabled in the web browser in the JRE 7.0 Update 10 or later. To enable Java content in the web browser: 1. From Windows, open the **Java Control Panel**.

Error condition	Probable cause / recommended action
	2. In the **Java Control Panel**, click the **Security** tab.
	3. If **Enable Java content in the browser** is checked, uncheck and click **Apply**.
	4. The **User Account Control** dialog opens. Click **Yes**. The confirmation window opens. Click **OK**.
	5. Restart the browser.
	If none of the above actions solve the problem, reinstall the JRE.
2 When you click the Storage Navigator menu, a message appears asking you to download the file SJsvlSNStartServlet.do or SJsvlAppStartServlet.do. One minute later, the application error (20020,108000) occurs.	The possible causes are that the JRE is not installed in the Storage Navigator computer, the JRE installation failed, or the JRE add-on is disabled on the web browser. Cancel the message, and install the JRE. If the JRE is already installed, reinstall it.
3 • The application errors (20020, 108000 and 10,6027) occur when you click the Storage Navigator menu. • The application error (10,6027) occurs and Storage Navigator terminates when you click the Storage Navigator menu.	If the problem continues after you perform the operation multiple times, the probable causes are as follows: • Java on the Storage Navigator web client might have failed to start due to timeout. Close all other applications and perform the Storage Navigator operation again. • The version of Storage Navigator installed on the client computer might not match the SVP version. Close all the windows of your web browser and then clear the Java and web browser cache. • The Storage Navigator computer might have entered standby or hibernate mode. Restart Storage Navigator computer. • If a proxy server is used for network connections, the proxy cache may be storing the older version of the program. If the problem continues after you clear the Java and web browser caches, contact your network administrator. • The network connection between the SVP and the Storage Navigator computer might be blocked by a firewall or some kind of device. Check the firewall settings and contact your network administrator. If none of the above actions solve the problem, save the Storage Navigator dump file and the Java trace file and log file, and report to the Hitachi Data Systems customer support. Then restart the Storage Navigator.
4 When you click the Storage Navigator menu, the system does not respond.	If the problem continues after you perform the operation multiple times, close all the Storage Navigator windows and clear the Java and web browser caches.
5 The application error (1,7050) occurs when you click the Storage Navigator menu.	The version of Storage Navigator installed on the Storage Navigator computer might not match the

Error condition	Probable cause / recommended action
	SVP version. Close all the windows of your web browser and then clear the Java and web browser caches.
	In addition, if a proxy server is used for network connections, the proxy server cache may be storing the older version of the program. If the problem continues after you clear cache of both Java and web browser, contact your network administrator.

6 Java console is grayed out and does not start when you try to open the Storage Navigator secondary window (Java application).	Restart the Storage Navigator computer, or terminate the Storage Navigator process with the following method.
	• For Windows:
	    Exit all applications using Java, and then terminate the javaw.exe and javaws.exe applications through Task Manager.
	• For UNIX:
	    Exit all applications using Java, and then terminate javaw and javaws with the kill command.

7 A message box remains displayed when opening the Storage Navigator secondary window (Java application). The Storage Navigator secondary window does not appear for a long time.	Restart the Storage Navigator computer, or terminate the Storage Navigator process with the following method.
	• For Windows:
	    Exit all applications using Java, and then terminate the javaw.exe and javaws.exe applications through the Task Manager.
	• For UNIX:
	    Exit all applications using Java, and then terminate javaw and javaws with the kill command.

8 A message remains displayed when the Storage Navigator secondary window opens and the system does not respond.	The SVP may be set as an exception on the proxy setting of the web browser. Make the settings the same on the Network Configuration dialog box, which is located in the Java Control Panel's General dialog box.
9 If you open the Java console dialog box by selecting the Java icon on the system tray while opening the Storage Navigator secondary window (Java application), the browser and Java console may stop responding.	Do not open the Java console dialog box while opening the Storage Navigator secondary window. If the browser and Java console stop responding, restart the Storage Navigator computer.
10 When you click the Storage Navigator menu. The application error (20020, 108000) occurs.	If the problem continues after you repeat the operation several times, you might have cancelled the display of the secondary window. For example: • You might have clicked **Exit** on the **Security Warning** window. • You might have clicked **Cancel** on the **Warning – Security** window.

Error condition	Probable cause / recommended action
	Close all the Storage Navigator windows and clear the Java and web browser caches.
	If the problem continues after you clear both Java and web browser caches, save the Storage Navigator dump file and the Java trace file, and send them to Hitachi Data Systems customer support.
11 The following message displays in Storage Navigator. • Java has discovered application components that could indicate a security concern. • Block potentially unsafe components from being run? (recommended) • The application contains both signed and unsigned code. Contact the application vendor to ensure that it has not been tampered with.	Select **Yes** to continue using Storage Navigator. If the problem continues, the cause may be one of the following: • The version of Storage Navigator might not match the SVP version. Close all the windows of your web browser and then clear the cache of both Java and the web browser. • If a proxy server is used for network connections, the proxy server cache may be storing an older version of the program. Clear the cache of both Java and the web browser. If the problem remains, contact your network administrator.
12 In Internet Explorer, the following pop-up window appears when you open the Storage Navigator secondary window. "Internet Explorer has stopped working. A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available."	Third-party browser extensions of Internet Explorer might be enabled. Disable third-party browser extensions as follows: 1. In the Windows menu bar, click **Tools** > **Internet Options**, and then click the **Advanced** tab. 2. In the **Advanced** tab, clear the **Enable third-party browser extensions (requires restart)** check box. 3. Restart Internet Explorer.
13 In Internet Explorer, an application error (10,6027) occurs when you open the Storage Navigator secondary window.	The SmartScreen Filter function might be enabled when you use Internet Explorer 8.0 or later. Turn off SmartScreen Filter. 1. In the Windows menu bar, click **Safety** > **SmartScreen Filter** > **Turn Off SmartScreen Filter**. 2. Restart Internet Explorer.
14 In Internet Explorer, an application blocked by Java security or an application blocked by a security settings message appears when you open a Storage Navigator secondary window.	The certificate signed in the SVP program might be expired. To use the application, perform the following procedure and add the SVP URL to the exception site list: 1. Open the **Java Control Panel**. 2. On the **Security** tab, click **Edit Site List...**. The **Exception Site List** window opens. 3. Click **Add**. 4. Enter the URL beginning with http:// or https://. Example: http://<SVP IP address> https://<SVP IP address>

Error condition	Probable cause / recommended action

	5. Click **OK**.
	
	If a **Security Warning - HTTP Location** appears, click **Continue**.
	
	6. In the **Java Control Panel**, click **OK** to close the window.
	
	7. Restart Internet Explorer.
	
	Note: The following Java versions do not allow the Storage Navigator secondary window to display.
	
	   ○ Java 7 Update 55 or later
	
	   ○ Java 8 Update 5 or later
	
	To start up the window, you need to change Java security settings.

No-response errors

The following table lists no-response errors:

Table 8-3 No-response errors

	Error condition	Probable cause / Recommended action
1	The following errors occur when using Storage Navigator: • 20121,107024 • 20121,107024 and 10,6027	The web server on the SVP might have been restarted. Close Storage Navigator, wait 10 minutes, and then restart Storage Navigator.
2	Error (20121,107096) occurs repeatedly while you are using Storage Navigator.	A timeout error may have occurred on Flash Player. Close the Storage Navigator window by clicking ☒ on the web browser or pressing the **Alt** and **F4** key.
3	The following errors occur when using Storage Navigator: • 20121,107024 • 20121,107025 • 20121,107096 • 20121,107097	This error may occur if the load to the Storage Navigator computer is high, or if you start multiple Storage Navigators by using multiple tabs in a tab browser or multiple browsers. Close other applications which cause the high load, or make sure to start only one Storage Navigator.
4	The following errors occur when using Storage Navigator: • 20020,108000 and 10,6027 • 10,6027	• The version of Storage Navigator installed on the Storage Navigator computer might not match the SVP version. Close all the windows of your web browser and then clear the cache of both Java and web browser. • The Storage Navigator computer might have entered standby or hibernate mode. Restart the Storage Navigator computer. • If a proxy server is used for network connections, the proxy server cache may be

Error condition	Probable cause / Recommended action
	storing the older version of the program. If the problem continues after you clear cache of both Java and web browser, contact your network administrator.
	If none of the above actions solve the problem, save the Storage Navigator dump file and the Java trace file and log file, and send them to Hitachi Data Systems customer support. Then restart Storage Navigator.
5 Storage Navigator does not respond. Storage Navigator may hang in the following cases: • The Storage Navigator main window is grayed out and does not display the percentage of progress, and you cannot perform any operation for a long period of time. • When you move a window displayed in front of the Storage Navigator secondary window, the area behind the window remains gray and does not go back to normal for a long period of time. • The entire Storage Navigator window is gray and does not go back to normal for a long period of time. • You cannot perform any operation for a long period of time and the dialog box that says Loading... is not displayed. • The dialog box that says Loading... opens when the window switches. However, you cannot move the dialog box or perform any operation for a long period of time.	When using the Storage Navigator main window, close the web browser. When using the Storage Navigator secondary window, exit Storage Navigator by pressing the **Ctrl** + **Alt** + **Shift** + **D** key all at once. If you cannot exit Storage Navigator, reboot the Storage Navigator computer or restart Storage Navigator after finishing Storage Navigator forcibly by the following way. For the Storage Navigator main window: • For Windows: Exit all web browser, and then terminate the iexplorer.exe through the Task Manager. • For UNIX: Exit all web browser, and then terminate firefox-bin with the kill command. For the Storage Navigator secondary window: • For Windows: Exit all applications using Java, and then terminate the javaw.exe and javaws.exe through the Task Manager. • For UNIX: Exit all applications using Java, and then terminate javaw and javaws with the kill command.
6 A network error occurred. There is no response to any operation even after 30 minutes.	Restart the Storage Navigator computer. An operation may take over 30 minutes depending on the use condition. For example, when several Storage Navigator web clients are running, an operation may take a long time.
7 An internal error occurs, or a web browser ended abnormally.	Close all dialog boxes and log in to Storage Navigator again. If the same error occurs, restart the Storage Navigator computer.
8 During a Storage Navigator operation, the Internet Explorer web browser suddenly disappears.	Restart the Storage Navigator computer.
9 An error (1,4011) occurs while you are using Storage Navigator.	The clock time of the Storage Navigator computer may have been changed. Log in to Storage Navigator again.

Error condition	Probable cause / Recommended action
10	The Storage Navigator computer reboots on its own.	Restart the Storage Navigator computer.
11	A Storage Navigator window is forcibly closed during a time-consuming process, such as LDEV formatting.	Close all windows, wait until processing finishes, and then restart Storage Navigator.
12	A Storage Navigator window is incorrectly closed by when you do one of the following: • Click ☒ • Use commands such as **File** > **Close** on the web browser • Press the **Alt** and **F4** keys	Restart Storage Navigator. If you cannot log in, wait for one minute and try again.
13	During a Storage Navigator operation, an add-on (`Flash10e.ocx`) error occurs.	Restart the Storage Navigator computer. If this error occurs repeatedly, reinstall Adobe Flash Player on the Storage Navigator computer.
14	When you log out of Storage Navigator, an Internet Explorer error occurs.	The probable causes are as follows: • Internet Explorer has not been updated. Install the latest updates • Internet Explorer may be configured incorrectly. Re-install Internet Explorer.
15	• When you click **Refresh All** or **Refresh View** in the Storage Navigator main window, the percentage of progress remains 99%. • When you click **Refresh All** or **Refresh View** in the Storage Navigator secondary window, it displays the message "Loading" for a long time.	The probable causes are as follows: • Another application such as Command Control Interface may be changing configuration. The window will be refreshed shortly after the configuration change ends. • Volume Migration operations, Quick Restore operations, or Thin Image operations may be in progress. The window will be refreshed shortly after the operations end.
16	• Error 20123-108004 occurred during a Storage Navigator operation in the main window. • Error 110,67005 occurred during a Storage Navigator operation in the secondary window.	The probable causes are as follows: • Another application such as Command Control Interface may be changing configuration. • Volume Migration operations, Quick Restore operations, or Thin Image operations may be in progress. • The configuration information may not be matched if a communication error occurs between the storage system and SVP. Wait awhile and then click **File > Refresh All** to reread the configuration information, and then operate Storage Navigator again.
17	While you are using a Storage Navigator secondary Window, it closes unexpectedly and error 20020-108000 occurs.	Start the Storage Navigator secondary window from the Storage Navigator main window again. If this error occurs repeatedly, close all the Storage Navigator windows, and then clear the Java and web browser caches.

Error condition	Probable cause / Recommended action
18	The Storage Navigator window turns white and the icon shown below displays in the center of the web browser when you use Storage Navigator.	Restart the Storage Navigator computer.
19	Operations cannot be performed due to a problem on the Storage Navigator main window. For example, tables are not displayed correctly on the Storage Navigator main window, some buttons are not displayed, or another problem on the window. This error is not solved even after re-login.	An incorrect value of Storage Navigator window setting information might be saved. Clear the window setting information by clicking **Settings** > **Environmental Setting** > **Reset View Settings** on the Storage Navigator main window and then operate Storage Navigator again.

Incorrect display errors

The following table lists incorrect display errors:

Table 8-4 Incorrect display errors

Error condition	Probable cause / Recommended action
1	Only the **Exit** button and the **Refresh** and **Refresh All** commands are effective when accessing the SVP from Storage Navigator.	The SVP might not be ready to perform some write processes from the other system. Wait awhile and then click **File** > **Refresh**. If the SVP is not restored, click **Refresh All**.
2	Only the **Exit** button and the **Refresh All** command are effective when accessing the SVP from Storage Navigator.	An error may have occurred in the SVP. Click **File** > **Refresh All**. If the SVP is not restored, log in to Storage Navigator again.
3	You opened the Basic Information Display dialog box, and then you opened a dialog box for another software product before the display process (acquiring information for the Basic Information Display dialog box) is finished.	Close the other product's dialog box. After processing for the Basic Information Display dialog box completes, reopen the dialog box for the other software product.
4	The commands in the **Go** menu are unavailable.	The required software options might not be installed or an error might occur on the window that appears after you click the command. Make sure that all the required software options are installed. If they are installed, perform one of the following operations. • Click **File** > **Refresh**. • Click **File** > **Refresh All**. • Log in to Storage Navigator again.
5	When you switch windows from one window to the Storage Navigator window, the Storage Navigator window is not displayed.	• Close all windows, and then log in to Storage Navigator again. • In the **Java Control Panel**, click the **Temporary Internet Files** section. In the

Error condition	Probable cause / Recommended action
	Disk Space area, enter **1 MB**, and then click **Delete Files**. • In the **Java Control Panel**, click **Security**. Ensure that **Enable Java content in the browser** is checked. • Clear the browser cache. • Ensure that Java Plug-in is enabled. If none of the above actions solve the problem, the web browser might not recognize Plug-in correctly. Initialize and set the web browser settings again.
6	The items in a list are not synchronized with a scroll bar.	Click the scroll buttons (▲ or ▼) above and below the scroll bar.
7	The focus disappears from the edit box.	Close all dialog boxes, and then log in to Storage Navigator again.
8	The web browser does not display correctly, because some GUI items such as labels and icons cannot be loaded properly.	Log out of Storage Navigator, and then log in again. If this error occurs before you log in to the Storage Navigator, close all dialog boxes and then log in to Storage Navigator.
9	The characters are unreadable because they are overlapped or garbled.	Log out of Storage Navigator, and then log in again.
10	The characters are garbled in a window where a tree is displayed.	Click **File** > **Refresh**.
11	Even though you have clicked **Apply** to change storage system settings, the new settings are not displayed in Storage Navigator.	Click **File** > **Refresh**.
12	The dialog box that says **Loading…** stays open for a long period of time.	A Storage Navigator message dialog box other than the dialog box that says **Loading…** might be displayed behind this window. Press the **Alt** and **Tab** key to switch the dialog box. If the dialog box that says **Loading…** remains displayed for several hours after you apply the settings to the storage system, contact Hitachi Data Systems customer support.
13	A question mark (?) displays in a table or other area of the window.	• When the question mark appears in the **View Tier Properties** window, see the topic describing this window in the *Hitachi Unified Storage VM Block Module Provisioning Guide*. If the problem still persists, contact Hitachi Data Systems customer support. • When the question mark appears in the **Add External Volumes** window, see the topic describing this window in the *Hitachi Universal Volume Manager User Guide*. If the problem still persists, contact Hitachi Data Systems customer support. • If the question mark appears in another window, refresh the window. Contact Hitachi

Error condition	Probable cause / Recommended action
	Data Systems customer support if the question mark remains after you refresh the window.
14 The product name, vendor name, and function name displayed in Storage Navigator are incorrect.	Contact Hitachi Data Systems customer support.
15 A part of the Storage Navigator window is not displayed.	You may be using the zoom in and zoom out function of the web browser. Do not use this function of the web browser when using Storage Navigator.
16 The following information does not display on Storage Navigator windows: • Information on the storage system, such as ports or HDDs • Information configured with another Storage Navigator computer	Click **File** > **Refresh**. If the problem continues, close all Storage Navigator windows, and then clear the Java and Web browser caches.
17 The display on Storage Navigator's main window is not updated to the latest information. "Last Updated" on Storage Navigator's main window is not updated.	Volume Migration operations, Quick Restore operations, or Thin Image operations may be in progress. The window will be refreshed shortly after the operations end.
18 The following message is displayed when connected to Storage Navigator on Internet Explorer 9 or later. "Alternate HTML content should be placed here. This content requires the Adobe Flash Player. Get Flash."	This message displays when Flash Player is not installed. Do the following: • Install Flash Player • Disable ActiveX Filtering If you are using Internet Explorer 9 or later, click **Tools > Safety** and uncheck **ActiveX Filtering**.
19 When many items are set, some items might not be displayed even if you scroll through the table.	Depending on the size of a window, some items in a table might not be displayed. Do the following: 1. Increase the resolution so that more areas of the table can be shown. 2. Use the zoom in or zoom out function of your browser (scroll the mouse wheel while pressing the Ctrl key) to adjust the viewing area. **Note**: The text might become too small. If you still cannot solve the problem, contact customer support.

UNIX operation errors

The following table lists UNIX operation errors:

Table 8-5 UNIX operation errors

Error condition	Probable cause / Recommended action
1 If you click in a Storage Navigator secondary window while a dialog box is open, the dialog	Click on the dialog box once more.

Error condition	Probable cause / Recommended action
box disappears behind the Storage Navigator secondary window.	
2 If you click a Storage Navigator secondary window while the Volume Migration window is displayed, the window disappears behind the Storage Navigator secondary window.	Click on the Volume Migration window once more.
3 The ☒ button on the Volume Migration window remains active, even if you click **Apply** and the processing continues.	Click ☒ to close the window. Even if the window is closed, the processing will continue normally.

4 The web browser is incorrectly displayed because GUI items, such as labels and icons, cannot be loaded properly.
 	
Part of a button is outside the window.
	If you use Storage Navigator on the Japanese version of Firefox, log out of Storage Navigator, and then log in to Storage Navigator again. Enter the following commands using the X Server Emulator.
	
	• B Shell:
	
	`LANG=C`
	
	`export LANG`
	
	• C Shell:
	
	`setenv LANG C`

5 The web browser closes abnormally.	This problem can occur if a Java_vm or Mozilla process keeps running after Mozilla stops responding. Delete the "java_vm" and "mozilla" processes and continue with Storage Navigator operations.

Other errors

The following table lists other errors that might occur in Storage Navigator:

Table 8-6 Other errors

Error condition	Probable cause / Recommended action
1 • An error about insufficient capacity is displayed when a user attempts to create an LDEV with sufficient capacity. • An error about an LDEV operation that does not exist is displayed when a user attempts to create a pair for an existing LDEV.	The configuration information in Storage Navigator and the controller configuration information might not match. In the Storage Navigator main window, click **File > Refresh All** and reload the configuration information. Then run Storage Navigator again. If this does not solve the problem, contact Hitachi Data Systems customer support.
2 The microcode on the SVP is upgraded or downgraded.	Close all Storage Navigator windows, and then clear the Java and Web browser caches. Even when you are not sure that the microcode on the SVP is upgraded or downgraded, clear the Java and Web browser caches.

Error condition	Probable cause / Recommended action
3 Storage Navigator processing is temporarily delayed.	Internal processing (such as, configuration change, P.P. check, or operational information acquisition) might be running on the SVP.
4 Storage Navigator processing is delayed.	The local storage value for Adobe Flash Player might decrease. Follow these steps: 1. Right-click on the Storage Navigator main window and click **Settings** to open the Adobe Flash Player Settings window. 2. In the local storage settings, move the slider until **Unlimited** appears and then click **Close**. 3. Close Storage Navigator. 4. Restart Storage Navigator. 5. If the local storage confirmation dialog box appears, click **Allow**.
5 An error occurs because a digital signature or security certificate is expired.	You can continue using Storage Navigator even though the digital signature for the Storage Navigator Java application is expired.
6 You specify IPv6 communication addresses when you start Storage Navigator. However: • IPv4 communication is used. • IPv4 addresses are output to audit logs for operations on the Storage Navigator secondary window.	IPv4 has higher priority when both IPv4 communication and IPv6 communication can be used. As a result of this, IPv4 may be used when you specify IPv6 communication addresses. Also, IPv4 addresses may appear in audit logs. For details on configuring only IPv6 communication, see Enabling IPv6 communication on page 2-2.
7 Installing the signed SSL certificate fails when installing the SSL certificate.	Passphrase for the SSL certificate might be set. See Verifying and releasing an SSL certificate passphrase on page 2-7.
8 You cannot resolve an error condition.	Perform the following operations and then contact the Hitachi Data Systems customer support. • Copy the Storage Navigator detailed dump files onto floppy disks using the FD Dump Tool. • Obtain the Java log and trace files.

Clearing Java and web browser caches

When an error occurs on Storage Navigator, clear the Java and web browser caches to solve the problem.

Clearing Java cache

To clear the Java cache, click **Delete the temporary files** in the General dialog box of the Java Control Panel.

Clearing web browser cache

To clear the cache in Internet Explorer, click **Tools** > **Internet Options**, and then click the **General** tab. Click **Delete Files** in the General dialog box.

To clear the cache in Firefox, click **Edit** > **Preferences**. In the displayed dialog box, click **Advanced** > **Cache**, and then click **Clear Cache**.

Firefox web browser problems on UNIX

Note the following when using Firefox web browser on UNIX:

- If a `java_vm` process or a Firefox web browser process becomes unavailable, Storage Navigator performance is affected. Delete the abnormal process and continue with Storage Navigator operations.
- When using Storage Navigator on the Japanese version of the Firefox web browser, you must use the X Server Emulator to properly configure the browser, as follows:

  In a B Shell, enter the following command:

  ```
  LANG=C
  export LANG
  ```

  In a C Shell, enter the following command:

  ```
  setenv LANG C
  ```

When you use Storage Navigator with Firefox, movements of the focus may differ from movements of the focus in Internet Explorer. For example:

- When the Storage Navigator login window appears, the focus is not on the **User Name** box. Even is the **User Name** box is emphasized, you cannot enter any characters in it.
- When you move the focus by using the **Tab** key, the destination browser window does not become active.

When you click **Logout** at the upper right in the Storage Navigator main window on Firefox, the Storage Navigator login window appears after you logout. (With Internet Explorer, the window closes after the logout.

Downloading dump files using the FD Dump tool

Use the FD Dump tool to download dump files onto a hard disk drive. The downloaded dump files can be used for the following reasons:

- For troubleshooting purposes. Use the FD Dump tool to download dump files from SVP and give it to the HDS service personnel.
- For checking configuration. First click **Refresh All** command to refresh the configuration information, and then use the FD Dump tool to download dump files.

Prerequisites

- No other user (including SVP user) should be using the FD Dump tool.

- No maintenance operation is being performed.
- You must have Support Personnel role to log in.

To download dump files from the SVP:

1. Start a web browser and specify the following URL to open the Tool Panel:
   https://IP-address-or-host-name-of-SVP/cgi-bin/utility/
   toolpanel.cgi
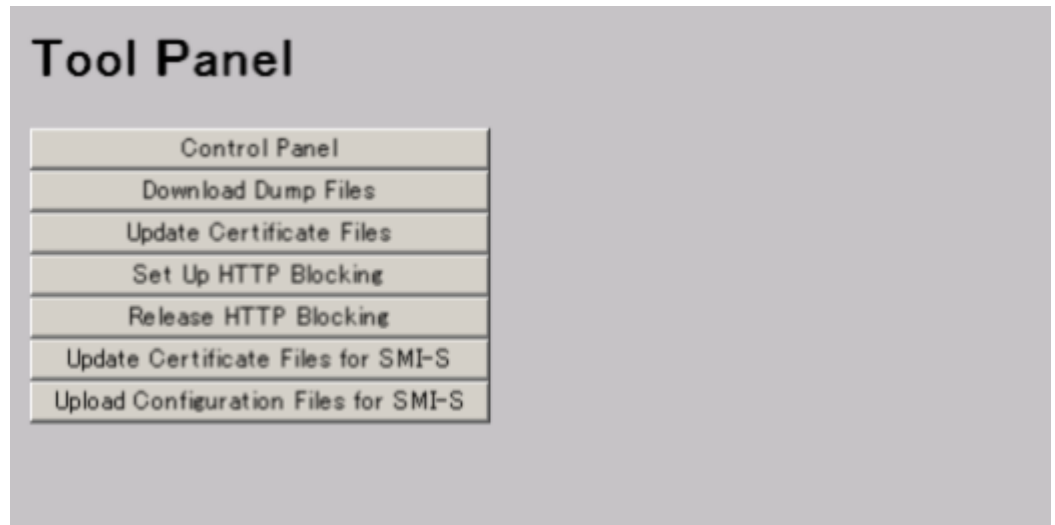
2. Click **Download Dump Files**. The Login dialog box opens.

3. Enter the user ID and password and click **Login**. The Download Dump Files dialog box opens.

4. Select a file that you want to download.

   ○ **Existing Dump Files** indicates the dump file for the last time you downloaded. Select this when you want to re-download a previously downloaded dump file. If you have not downloaded any dump files from Tool Panel, this item does not display even if you have acquired a dump file via the SVP.

   ○ **Normal Dump** includes all information about SVP and the minimum information about the storage system. Select this when you have a less serious problem such as incorrect display.

   ○ **Detail Dump** includes all information about the SVP and the storage system. Select this when Storage Navigator has a serious problem (for example, Storage Navigator does not start) or when you need to determine if the storage system has a problem.

   ○ **Detail Dump (for DKC Performance)** contains the I/O-performance-related information. This includes performance monitor collection information, in addition to information applicable to Detail Dump. Choose Detail Dump (for DKC Performance) to check for I/O performance problems.

   Note that while processing takes place, DKC I/O performance may be affected. During processing, Storage Navigator apply operations and SVP maintenance operations are not allowed.

5. Click **Next >>**. A message appears confirming the execution of compression of the dump files.

6. Click **OK**. File compression processing starts. When the file is compressed, the Download Dump Files dialog box opens for the download.

7. Click **Download**. The File Download dialog box opens.

8. On the File Download dialog box, click **Save this file to disk**, and then click **OK**. The Save As dialog box opens.

9. Specify the download destination, and then click **Save**. When the file is downloaded successfully, the Download complete dialog box opens.

Saving Java log and trace files

Before you contact your service representative, save the Java log and trace file on your Storage Navigator computer, and then restart the web browser.

Examples of the Windows trace and log file locations are shown below:

- `C:\Users\logon user ID\AppData\LocalLow\Sun\Java\Deployment \log\*.trace`

- `C:\Users\logon user ID\AppData\LocalLow\Sun\Java\Deployment \log\*.log`

Examples of the UNIX trace and log file locations follow:

- *user home directory*`\.java\deployment\log\*.trace`

- *user home directory*`\.java\deployment\log\*.log`

A

Storage configuration reports

This appendix describes the configuration reports you can generate. They are shown here according to the way they display: in tables, graphs, or CSV files.

To create, download, and delete reports, see Viewing a Storage Navigator report on page 7-8.

☐ Reports in table view

☐ Reports in graphical view

☐ CSV files

Reports in table view

The reports described in this topic appear in table format, as seen in the following example. ⬛ icons are displayed before names in Report Types list. If icons do not display properly, refresh the window.

Figure A-1 Table report (example: Ports)

- Click each column header to sort tables in table reports.
- When the table is reading a large amount of data, the table columns cannot be manipulated, sorted, and resized. You can view already displayed items, select rows, and scroll. The remaining number of records is displayed under the list.

Disk Blades report

This report is about disk blades. A record is created for each disk blade.

Table A-1 Disk Blades report

Item	Description
DKB	Location of the disk blade "External" is displayed when the storage system has an external storage systems.
Number of PGs	The number of the parity groups that the disk blade controls

Item	Description
	If "DKB" is "External", this item indicates the number of parity groups mapped to external volumes.
Number of LDEVs (Total)	The number of the logical volumes belonging to the parity groups that the disk blade controls
Number of LDEVs (Unallocated)	The number of the logical volumes that are inaccessible from the host and belong to the parity groups controlled by the disk blade
Total LDEV Capacity (MB)	Total capacity of the logical volumes belonging to the parity groups that the disk blade controls
Unallocated LDEV Capacity (MB)	Total capacity of the logical volumes that are inaccessible from the host and belong to the parity groups controlled by the disk blade

Host Groups report

This report is about host groups. A record is created for each host group.

Table A-2 Host Groups report

Item	Description
Port Location	Name of the port
Host Group	Name of the host group
Resource Group Name	Resource Group Name where the host group belongs
Resource Group ID	Resource Group ID where the host group belongs
Number of LUNs	The number of LU paths defined to the host group
Number of LDEVs	The number of logical volumes that are accessible from the hosts in the host group
Number of PGs	The number of parity groups with logical volumes that are accessible from the hosts in the host group
Number of DKBs	The number of disk blades controlling the parity groups where the logical volumes that are accessible from the hosts in the host group belong
Total LDEV Capacity (MB)	Total capacity of the logical volumes accessible from the hosts in the host group This is the total capacity of LDEVs referred to in "Number of LDEVs".
Port Security	Security of the port
Host Mode	Host mode of the host group
Host Mode Option	Host mode option of the host group Host mode options are separated by semicolons (;) when more than one option is specified.
Number of Hosts	The number of the hosts in the host group

Hosts report

This report is about hosts. A record is created for each host. When a host is registered to more than one port, more than one record shows information about the same host.

Table A-3 Hosts report

Item	Description
Port Location	Name of the port
Port Internal WWN	WWN of the port
Port Security	Security of the port
Host Group	Name of the host group
Host Mode	Host mode of the host group
Host Mode Option	Host mode option of the host group Host mode options are separated by semicolons (;) when more than one option is specified.
Host Name	Name of the host that can access the LU path through the port
HBA WWN	WWN of the host

Logical Device Expansions report

This report is about LUN Expansion (LUSE). Information about one LUSE volume consists of contiguous records.

You can sort only Top LDEVs in this report.

Table A-4 Logical Device Expansions report

Item	Description
Top LDEV	Logical volume number of the first volume
Member LDEVs	Logical volume number of the logical volume of the LUSE
Emulation Type	Emulation type of the logical volume of the LUSE volume
Total LDEV Capacity (MB)	Capacity of the LUSE volume
Individual LDEV Capacity (MB)	Capacity of each logical volume of the LUSE volume
Number of Member LDEVs	The number of the logical volumes of the LUSE volume
PG	Parity group number of the parity group to which the logical volumes of the LUSE volume belong If the number starts with "E" (for example, E-1), the parity group contains external volumes.

Item	Description
RAID Level	RAID level of the parity group where the logical volumes comprising the LUSE volume belong
Drive Type-Code	Type code of the drive of the parity group where the logical volumes comprising the LUSE volume belong
Drive Capacity	Capacity of the drives of the parity group where the logical volumes comprising the LUSE volume belong
SSID	SSID of the logical volume of the LUSE volume
CMD Dev	Information about whether the LUSE volume is a command device

Logical Devices report

This report is about logical volumes. A record is created for each logical volume.

Table A-5 Logical Devices report

Item	Description
LDEV ID	The logical volume number
LDEV Name	The logical volume name
Capacity (MB)	Capacity of the logical volume
Emulation Type	Emulation type of the logical volume
Resource Group Name	Resource group name where LDEV belongs
Resource Group ID	Resource group ID where LDEV belongs
PG	The parity group number If the number starts with "E" (for example, E1-1), the parity group contains external volumes.
RAID Level	RAID level of the parity group where the logical volume belongs If the LDEV is an external volume, a hyphen (-) is displayed.
Drive Type/RPM	Drive type and round-per-minute (RPM) of the drive of the parity group where the logical volume belongs A hyphen (-) is displayed as RPM when the drive is SSD. If the LDEV is an external volume, a hyphen (-) is displayed.
Drive Type-Code	Type code of the drive of the parity group where the logical volume belongs If the LDEV is an external volume, a hyphen (-) is displayed.
Drive Capacity	Capacity of the drive of the parity group where the logical volume belongs

Item	Description
	If the LDEV is an external volume, a hyphen (-) is displayed.
PG Members	List of the drive locations of the parity group where the logical volume belongs
	If the LDEV is an external volume, a hyphen (-) is displayed.
Allocated	Information about whether the host can access the logical volume
	For logical volumes of a LUSE volume, "Y" is displayed if the LU path is defined to the LUSE volume.
SSID	SSID of the logical volume
CVS	Information about whether the logical volume is a customized volume
OCS	Oracle checksum
LUSE	Information about whether the logical volume is a part of a LUSE volume • "On" is displayed when the logical volume is the first volume of a LUSE volume. • "Off" is displayed when the logical volume is the second or later volume of a LUSE volume, or not a part of a LUSE volume.
Attribute	The attribute of the logical volume
Provisioning Type	Provisioning type of the logical volume
Pool Name	Pool name • If the provisioning type is Dynamic Provisioning, the name of the pool related to the logical volume is displayed. • If the logical volume attribute is Pool, the name of the pool where the logical volume belongs is displayed. • If neither of the above is applied, a hyphen (-) is displayed.
Pool ID	The ID of the pool The ID of the pool shown in "Pool LDEV)" is displayed.
Current MPU	The MP unit that currently controls the logical volume
Setting MPU	The MP unit that you specified to control the logical volume
Command Device : Security	Indicates whether Security is specified as the attribute for the command device. If the attribute of the logical volume is not CMDDEV, a hyphen (-) is displayed.
Command Device : User Authentication	Indicates whether User Authentication is specified as the attribute for the command device.

Storage configuration reports

Item	Description
	If the attribute of the logical volume is not CMDDEV, a hyphen (-) is displayed.
Command Device : Device Group Definition	Indicates whether Device Group Definition is specified as the attribute for the command device.
	If the attribute of the logical volume is not CMDDEV, a hyphen (-) is displayed.

LUNs report

This report is about LU path definitions. A record is created for each LU path.

Table A-6 LUNs report

Item	Description
Port Location	Name of the port
Port Internal WWN	WWN of the port
Port Security	Security of the port
Host Group	Name of the host group
Host Mode	Host mode of the host group
Host Mode Option	Host mode option of the host group
	Host mode options are separated by semicolons (;) when more than one option is specified.
LUN	Logical unit number
LDEV ID	Logical volume number
Emulation Type	Emulation type of the logical volume
Capacity (MB)	Capacity of the logical volume
	Capacity of the LUSE volume is displayed when the logical volume is the first volume of the LUSE volume.

MP Units report

This report shows MP units. A record is created for each MP unit.

Table A-7 MP Units report

Item	Description
MP Unit ID	MP unit ID
MP Blade ID	MP blade ID
Auto Assignment	Auto assignment attribute for the MP unit
Number of Resources (LDEV)	The number of logical volumes that the MP unit controls

Item	Description
Number of Resources (Journal)	The number of journals that the MP unit controls
Number of Resources (External Volume)	The number of external volumes that the MP unit controls
Number of Resources (Total)	The total number of resources that the MP unit controls
	The sum of "Number of Resources (LDEV)", "Number of Resources (Journal)", and "Number of Resources (External Volume)".

MP Unit Details report

This report shows MP unit details. A record is created for each resource controlled by an MP unit.

Table A-8 MP Unit Details report

Item	Description
MP Unit ID	MP unit ID
MP Blade ID	MP blade ID
Auto Assignment	Auto assignment attribute for the MP unit
Resource ID	ID of this resource that the MP unit controls
Resource Name	The name of the resource that the MP unit controls
	If "Type" is LDEV, the LDEV name that is set is displayed.
	If "Type" is not LDEV, a hyphen (-) is displayed.
Type	The type of the resource that the MP unit controls

Parity Groups report

This report is about parity groups. A record is created for each parity group.

Table A-9 Parity Groups report

Item	Description
PG	Parity group number
	If the number starts with "E" (for example, E1-1), the parity group contains external volumes (Universal Volume Manager).
DKB	Name of the disk adapter that controls the parity group[1]
RAID Level	RAID level of the parity group[1]

Storage configuration reports

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
Resource Group Name	Name of the resource group in which the parity group belongs
Resource Group ID	ID for the resource group in which the parity group belongs
Emulation Type	Emulation type of the parity group[1]
Number of LDEVs (Total)	The number of the logical volumes in the parity group
Number of LDEVs (Unallocated)	The number of the logical volumes in the parity group that the host cannot access
Total LDEV Capacity (MB)	Capacity of the logical volumes in the parity group
Unallocated LDEV Capacity (MB)	Capacity of the logical volumes in the parity group that the host cannot access
Drive Type-Code	Type code of the drive in the parity group If the parity group contains external volumes, this displays the vendor, the model, and the serial number of the storage system.
Drive Type/RPM	Drive type and round-per-minute (RPM) of the drive in the parity group[1] A hyphen (-) is displayed as RPM when the drive is SSD.
Drive Capacity	Capacity of the drive in the parity group[1]
RAID Concatenation #0	The number indicating a parity group #0 connected to this parity group[2]
RAID Concatenation #1	The number indicating a parity group #1 connected to this parity group[2]
RAID Concatenation #2	The number indicating a parity group #2 connected to this parity group[2]
Encryption	Whether the parity group is encrypted or not[1]

Notes:

1. If the parity group contains external volumes, a hyphen (-) is displayed.
2. If the parity group is not connected with another parity group or if the parity group contains external volumes, a hyphen (-) is displayed.

Ports report

This report is about ports. A record is created for each port.

Table A-10 Ports report

Item	Description
CHB	Name of the channel blade
Type	Package type of the channel blade

Item	Description
Port Location	Name of the port on the channel blade
Port Attribute	Port attribute
Port Internal WWN	WWN of the port
Fabric	One of the Fibre topology settings indicating the setting status of the Fabric switch
Connection Type	One of the Fibre topology settings • Point to Point • FC-AL
Address (Loop ID)	Fibre port address and Loop ID of the port
Port Security	Security of the port
Speed	Data transfer speed of the port
Resource Group Name	Name of the resource group in which the port belongs
Resource Group ID	ID for the resource group in which the port belongs
Number of Hosts	The number of the hosts registered to the port
Number of LUNs	The number of the LU paths defined to the port
Number of LDEVs	The number of the logical volumes that can be accessed through the port
Number of PGs	The number of the parity groups having the logical volumes that can be accessed through the port
Number of DKBs	The number of the disk blades controlling the parity group that contains the logical volumes that can be accessed through the port

Spare Drives report

This report is about spare drives. A record is created for each spare drive.

Table A-11 Spare Drives report

Item	Description
Drive Type-Code	Type code of the spare drive
Drive Capacity	Capacity of the spare drive
Location	Location of the spare drive

SSD Endurance report

This report is about SSD endurance. A record is created for each SSD. Only SSDs having endurance information are displayed.

Table A-12 SSD Endurance report

Item	Description
Drive Type-Code	Type code of the SSD
Drive Capacity	Capacity of the SSD
Location	Location of the SSD
Used Endurance Indicator (%)	Used endurance of the SSD

Storage System Summary report

This report shows a summary of the storage system.

Table A-13 Storage System Summary report

Item	Description
Storage System Type	Type of the storage system
Serial Number	Serial number of the storage system
IP Address	IP address of the SVP
Microcode Versions	Version of the following programs • Main • SVP • DKB • CUDG4 • RAM BOOT • ROM BOOT • CMBK • Config • HDD • HDD (SVP) • Expander • Expander (DBF) • Expander (DB6A) • CFM • Printout Tool
Number of CUs	The number of control units in the storage system
Shared Memory Size (GB)	Capacity of shared memory
Cache Size (GB)	Capacity of the cache on the storage system
Number of DKBs	The number of disk blades on the storage system
System Options	List of the system options specified for the storage system

Item	Description
Drive Capacity (TB)	Total capacity of drives in the storage system except for external volumes
Spare Drive Capacity (TB)	Total capacity of the spare drives in the storage system
Volume Capacity*	List of the capacity of the volumes
Number of LDEVs*	List of the numbers of the volumes in the following status • allocated • unallocated • reserved • free
*You cannot sort the list.	

Reports in graphical view

The reports described in this topic display as graphics. ▦ icons are displayed before names of reports in graphical view. If the icons or graphics do not display properly, refresh the window

Cache Memories report

This report shows cache memory data, including shared memory capacity and MAIN blades and DIMMs. Total capacity of the cache memory is also displayed.

Figure A-2 Cache Memories report

Channel Blades report

This report is about channel blades. It shows channel blades, ports, and a list of types of channel blades. On the bottom of the view, you can see the legend of ports (Installed or Not Installed).
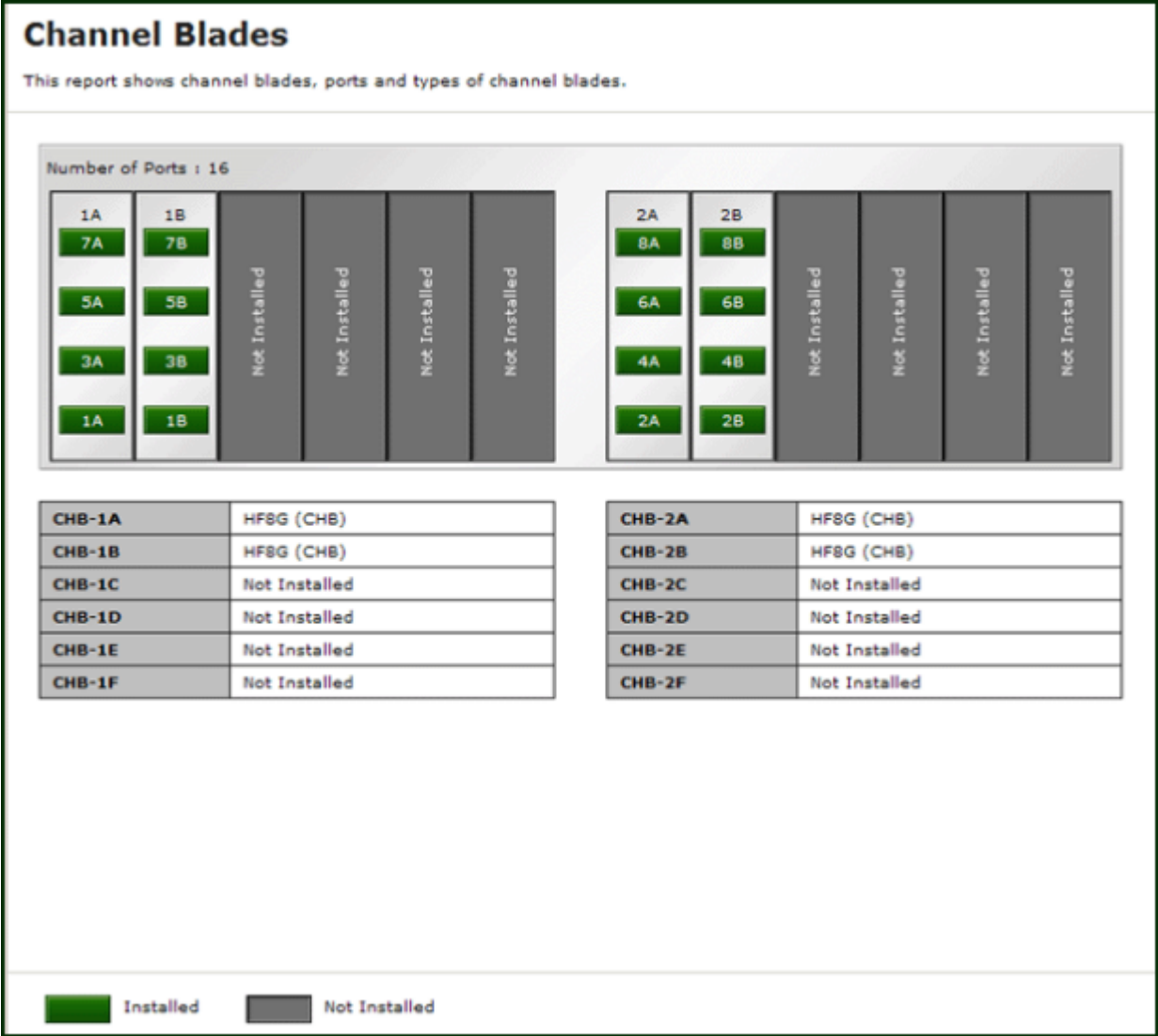
Figure A-3 Channel Blades report

Physical View report

This report shows disk controllers and disk units, and includes MAIN blades, MP blades, channel blades, disk blades, data drives, and spare drives.
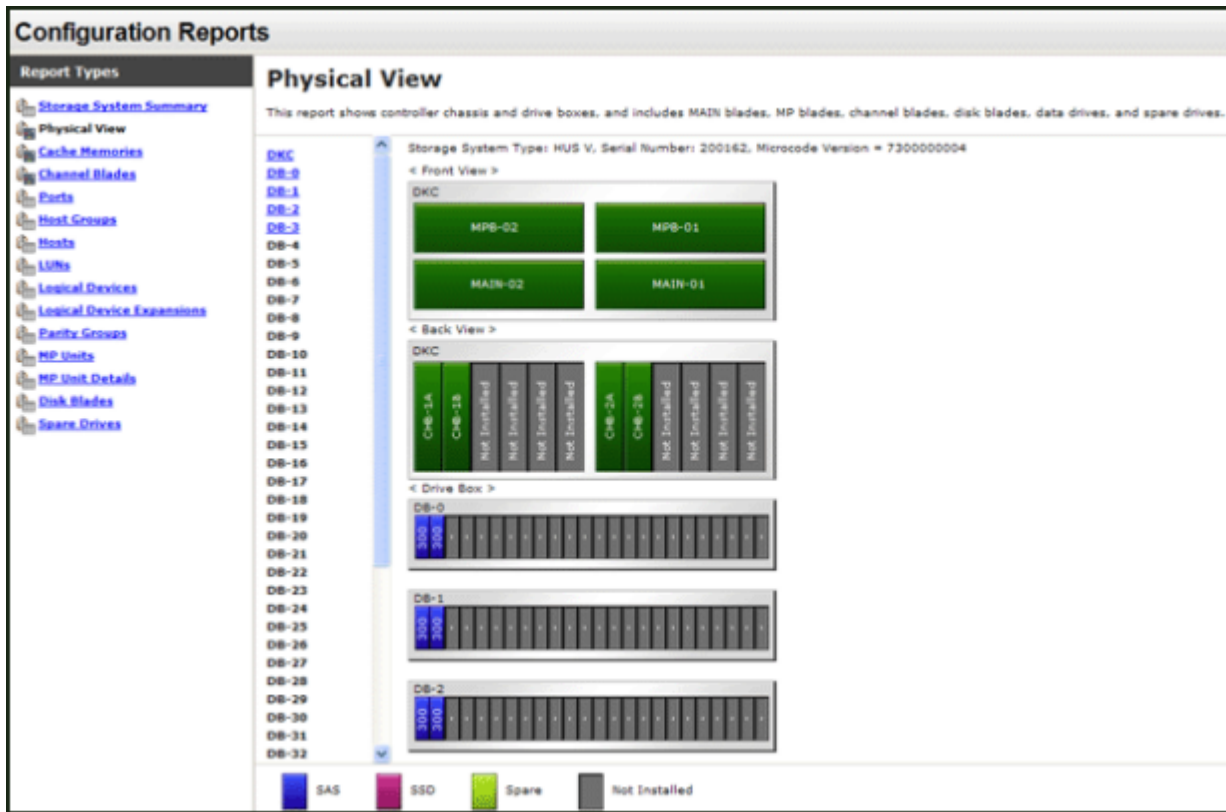
Figure A-4 Physical View report

This report consists of a link list and graphics, which show the front view and back view of DKC and a view of 48 drive boxes (DBs). The drive box number starts at DB-0 and ends at DB-47. On the top of the graphics area, you can check the storage system type, serial number and microcode version. On the bottom of the view, the legend of drive boxes (SAS, SSD, Spare, and Not Installed) is displayed.

The view of drive boxes differs depending on the types of drive boxes. Examples are shown below.

- A drive box for 2.5 inch drives

  2.5 inch drives can be installed in this drive box.

- A drive box for 3.5 inch drives

  3.5 inch drives can be installed in this drive box.
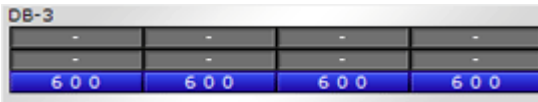
- A dense drive box

  3.5 inch drives can be installed densely in this drive box.

DB-0

(Front Side)
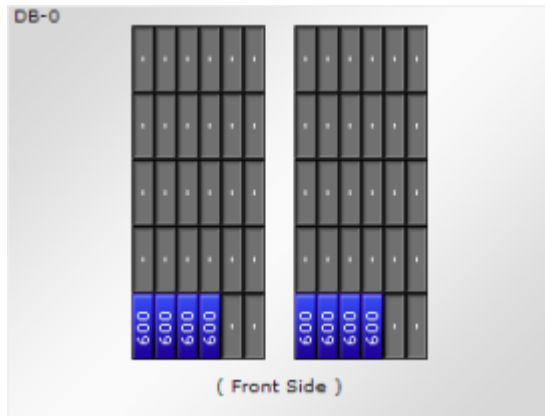
CSV files

The reports described in this topic are saved as CSV files.

AllConf.csv

This is the concatenated file of all the csv files.

CacheInfo.csv

This CSV file contains information about MAIN blades. A record is created for each MAIN blade.

Table A-14 CacheInfo.csv file (Title: <<Cache>>)

Item	Content
Label	MAIN blade label Example: • Cache Memory A Basic
CMG#0 Size(GB)	CMG size per MAIN blade (in GB)
CMG#1 Size(GB)	CMG size per MAIN blade (in GB)
Cache Size(GB)	Total cache capacity of MAIN blade (in GB)
SM Size(GB)	Shared memory capacity (in GB)
Cache Residency Size(MB)	Capacity allocated to the MAIN blade for Cache Residency Manager (in MB)

ChaStatus.csv

This CSV file contains information about the status of channel blades (CHBs). A record is created for each CHB.

Table A-15 ChaStatus.csv file (Title: <<CHB Status>>)

Item	Content
CHB Location	CHB name
PCB Status	Status of this CHB 1: Normal, 0: Abnormal
FCP#00, #01, …, #03	Status of ports on this CHB 1: Normal, 0: Abnormal, Blank: Not installed

DcrInfo.csv

This CSV file contains information about Cache Residency Manager. A record is created for each logical volume for which Cache Residency Manager is set.

For details of Cache Residency Manager, see the *Hitachi Unified Storage VM Block Module Performance Guide*.

Table A-16 DcrInfo.csv file (Title: <<DCR Information>>)

Item	Content
HDEV#	ID of the logical volume for which Cache Residency Manager is set
Type	Cache Residency Manager type • BIND • PRIO
From (LBA)	Start slot (LBA) for Cache Residency Manager
To (LBA)	End slot (LBA) for Cache Residency Manager
PreStaging Request	Information about whether data is the target of prestaging or not • On • Off

DeviceEquipInfo.csv

This CSV file contains information about equipment of devices such as DKC PS, DB PS, Battery, and SVP. A record is created for each device.

Table A-17 DeviceEquipInfo.csv file (Title: <<Device Equipment Information>>)

Item	Content
Device Location	Device location name Example: • For DKC PS: DKCPS1 • For DB PS: DBPS0-0

Item	Content
	• For Battery: MAIN1 BATT • For SVP: SVP
Equip Status	Equipment status of the device • Equipped • Not Equipped
Status	Status of the device • Normal • Abnormal • Blank (if Equip Status is Not Equipped)

DkaInfo.csv

This CSV file contains information about disk blades (DKBs). A record is created for each DKB.

Table A-18 DkaInfo.csv file (Title: <<DKB Information>>)

Item	Content
Basic/Option	DKB location • Basic • Option
DKB Location	DKB name
Package Type	DKB type Example: • BS6G (DKB)

DkaStatus.csv

This CSV file contains information about the status of disk blades (DKBs). A record is created for each DKB.

Table A-19 DkaStatus.csv file (Title: <<DKB Status>>)

Item	Content
DKB Location	DKB name
PCB Status	Status of this DKB 1: Normal, 0: Abnormal
BECON#00	Status of BECON on this DKB 1: Normal, 0: Abnormal, Blank: Not installed
BEPORT#0000, #0001	Status of BEPORT on this DKB 1: Normal, 0: Abnormal, Blank: Not installed

DkcInfo.csv

This CSV file contains information about DKC. A record is created for each storage system.

Table A-20 DkcInfo.csv file (Title: <<DKC Information>>)

Item	Content
Storage System Type	Storage system type Example: HUS VM
Serial Number#	Serial product number (200001 to 299999)
IP Address	IP address
Subnet Mask	Subnet mask
Number of CUs	Number of CUs
Number of DKBs	Number of DKBs
Configuration Type	Configuration type Example: PCM

ELunInfo.csv

This CSV file contains information about external volumes. Information about one external volume is output to multiple records according to the number of prioritized paths between the local and the external storage systems.

For details of external volumes, see *Hitachi Universal Volume Manager User Guide*.

Table A-21 ELunInfo.csv file (Title: <<External LUN Information>>)

Item	Content
VDEV#	Virtual device number to which the external volume is mapped
Characteristic1	Identification number of the external volume*
Characteristic2	Extended information for identifying the external volume*
Device	Product name reported to the host by the external volume*
Capacity(blocks)	Capacity of the external volume (in blocks)
Cache Mode	Indicates whether the write data from the host to the external storage system is reflected synchronously or asynchronously • Enable: Asynchronously • Disable: Synchronously
ECC Group	Number of parity group to which the external volume is mapped If the number starts with "E" (for example, E-1), the parity group contains external volumes.

Item	Content
Current MPU	Number of a current MP unit controlling the parity group to which the external volume is mapped
Setting MPU	Number of an MP unit configured to control the external volume indicated by the ECC Group
Vendor	Vendor name of the external storage system
Product Name	Product name of the external storage system
Serial Number#	Serial product number of the external storage system
Path Mode	Mode which indicates how the paths between local and external storage systems operate • Multi • Single • APLB
Port	Number of a local port from which the external path is connected to the external storage system
WWN	Port identifier number of the external storage system
LUN	LU number set for the external volume
Priority	Priority of the paths between the storage systems to be used for connection with the external volume "1" indicates the path of the highest priority.
Status	Status of the path between storage systems • Normal • Blocked
IO TOV	I/O timeout value for the external volume
QDepth	The number of Read/Write commands that can be issued to the external volume at a time
Resource Group ID (ECC Group)	Resource group ID for the parity group that is mapping external volumes
Resource Group Name (ECC Group)	Resource group name of the parity group that is mapping external volumes
Load Balance Mode	I/O load balance distribution logic specified for external volume • Normal Round-robin • Extended Round-robin • Disable A hyphen (-) displays when Single is specified in Path Mode.
* Note: If the character string contains a comma, the comma is converted to a tab.	

FcSpNameInfo.csv

This CSV file contains information about Fibre Channel Security Protocols (FCSPs). A record is created for each initiator (host).

For details of port setting, see the *Hitachi Unified Storage VM Block Module Provisioning Guide*.

Table A-22 FcSpNameInfo.csv file (Title: <<FC-SP Name Information>>)

Item	Content
Port	Port name
Host Group	Host group name
Target Username	WWN information about the storage system required for authentication (16-digit number in the hexadecimal format)*
Authentication of Group	Information about whether to perform authentication or not • Enable • Disable
Initiator Username	WWN information about the host required for authentication (16-digit number in the hexadecimal format)*
Protocol	Protocol used for authentication ("CHAP" or blank)
* Note: If the character string contains a comma, the comma is converted to a tab.	

FcSpPortInfo.csv

This CSV file contains information about ports related to Fibre Channel Security Protocols (FCSPs). A record is created for each port.

For details of port setting, see the *Hitachi Unified Storage VM Block Module Provisioning Guide*.

Table A-23 FcSpPortInfo.csv file (Title: <<FC-SP Port Information>>)

Item	Content
Port	Port name
Time out(Sec)	Time interval (in seconds) before retrying authentication in case of failure in authentication
Refusal Intvl.(Min)	Time interval (in minutes) before starting next authentication in case of failure in authentication for the number of times displayed by "Refusal Freq.(Counts)"
Refusal Freq.(Counts)	Number of times of authentication allowable for connection to a port
Switch Port Username	WWN information about the Fabric switch required for authentication (16-digit number in the hexadecimal format)*
Mode	Mode of authentication between ports and Fabric switches • bidirectional • unidirectional

Item	Content
Authentication of Fabric Switch	Information about whether to perform authentication of the Fabric switch identified by "Switch Port Username" • Enable • Disable
* Note: If the character string contains a comma, the comma is converted to a tab.	

HduInfo.csv

This CSV file contains information about drive boxes (DBs). A record is created for each DB.

Table A-24 HduInfo.csv file (Title: <<DB Information>>)

Item	Content
DB Location	DB location name Example: DB00
DB Status	Information about whether this DB is installed or not • Installed • Not installed
Slot Size	Slot size (inches) • 2.5 • 3.5 • Blank for DBF (FMD)
DB Type	DB Type When not using DB60 • DBS (2.5-inch HDD and SSD) • DBL (3.5-inch HDD and SSD) • DBX (3.5-inch HDD and SSD in dense drive box) • DBF for FMD When using DB60 • DBS (2.5-inch HDD and SSD) • DBL (3.5-inch HDD and SSD) • DB60 (3.5-inch HDD and SSD in dense drive box) • DBF for FMD

JnlInfo.csv

This CSV file contains information about journals. A record is created for each journal.

Table A-25 JnlInfo.cvs file (Title: <<JNL Information>>)

Item	Content
JNL#	Journal number
Current MPU	Number of MP unit currently controlling the journal
Setting MPU	Number of MP unit configured to control the journal

LdevCapaInfo.csv

This CSV file contains information about LDEV capacities. A record is created for each of three classifications shown in "Volume Kind".

Table A-26 LdevCapaInfo.csv file (Title: <<LDEV Capacity Information>>)

Item	Content
Volume Kind	The following three classifications are output. • Internal OPEN Volumes • External OPEN Volumes • Total OPEN Volumes
Allocated LDEV Capacity (GB)	Allocated LDEV capacity (in GB)
Unallocated LDEV Capacity (GB)	Unallocated LDEV capacity (in GB)
Reserved Capacity (GB)	Reserved LDEV capacity (in GB)
Total Volume Capacity (GB)	Total capacity (in GB) of "Allocated LDEV Capacity (GB)", "Unallocated LDEV Capacity (GB)" and "Reserved Capacity (GB)"
Free Space (GB)	Free Space (in GB)
Total Capacity (GB)	Total Capacity (in GB) The sum of "Total Volume Capacity (GB)" and "Free Space (GB)"

LdevCountInfo.csv

This CSV file contains information about the number of logical devices (LDEVs). A record is created for each of three classifications shown in "Volume Kind".

Table A-27 LdevCountInfo.csv file (Title: <<LDEV Count Information>>)

Item	Content
Volume Kind	The following three classifications are output • Internal Volumes • External Volumes

Item	Content
	• Total Volumes
Allocated OPEN LDEVs	The number of allocated volumes (LDEVs)
Unallocated OPEN LDEVs	The number of unallocated volumes (LDEVs)
Reserved OPEN LDEVs	The number of reserved volumes (LDEVs)
V-VOL	The number of virtual volumes Output only when "Volume Kind" is Total Volumes.
Total(All LDEVs)	Total number of LDEVs
ECC Groups	Total number of parity groups

LdevInfo.csv

This CSV file contains information about logical devices (LDEVs). A record is created for each LDEV.

For details of LDEVs, see the *Hitachi Unified Storage VM Block Module Provisioning Guide*.

Table A-28 Ldevinfo.csv file (Title: <<LDEV>>)

Item	Content
ECC Group	Number of parity group where the LDEV belongs • If the number starts with "E" (for example, E-1), the parity group contains external volumes (Universal Volume Manager). • If "LDEV Type" is Dynamic Provisioning or Snapshot, a hyphen (-) is output.
LDEV#	LDEV number
LDEV Name	LDEV name[1]
LDEV Emulation	LDEV emulation type
LDEV Type	LDEV type: • Basic • Dynamic Provisioning • External • Snapshot (Volume for Thin Image)
LDEV Attribute	LDEV Attribute: • CMDDEV (Command device) • CMDDEV* (Remote command device) • System Disk (System disk) • Journal (Journal volume) • Pool (Pool volume) • Quorum Disk (Quorum disk used in High Availability Manager) • Reserve (Reserved volume)

Item	Content
	• Nondisruptive Migration (Volume for nondisruptive migration) • Regular (Others)
Volume Size(Cyl)	LDEV capacity (in cylinders)
Volume Size(MB)	LDEV capacity (in MB)
Volume Size(Blocks)	LDEV capacity (in blocks)
CVS	Information about whether the LDEV is a custom-sized volume or not: • On: Custom-sized volume • Off: Others
LUSE	Information about whether this LDEV is the top volume of LUSE or not: • On • Off
Pool ID	Pool number This is blank except for the following cases: • If LDEV Type is Dynamic Provisioning • If LDEV Attribute is Pool
RAID Concatenation#0	Number of parity group to be concatenated to parity group (#0) identified by ECC Group[2]
RAID Concatenation#1	Number of parity group to be concatenated to parity group (#1) identified by ECC Group[2]
RAID Concatenation#2	Number of parity group to be concatenated to parity group (#2) identified by ECC Group[2]
ORACLE CHECK SUM	Information about whether this LDEV is Oracle check sum target or not • On • Off
Current MPU	Number of MP unit currently controlling the LDEV
Setting MPU	Number of MP unit configured to control LDEV
Allocated	Information about whether this LDEV is allocated to a host or not "Y" is output for volumes accessible to host.
Pool Name	The pool's name[1] The name of the pool shown in "Pool ID" is displayed.
CmdDevSecurity	Indicates whether Security is specified as the attribute for the command device.
CmdDevUserAuth	Indicates whether User Authentication is specified as the attribute for the command device.
CmdDevDevGrpDef	Indicates whether Device Group Definition is specified as the attribute for the command device.

Storage configuration reports

Item	Content
Resource Group ID (LDEV)	Resource group ID of LDEV
Resource Group Name (LDEV)	Resource group name of LDEV
Encryption	Specifies whether the parity group shown with "ECC Group" is encrypted or not. • Local storage volume: Enabled (encrypted) or Disabled • Other than the above: Blank
Notes: 1. If the character string contains a comma, the comma is converted to a tab. 2. Blank if the parity group is not concatenated to another parity group.	

LdevStatus.csv

This CSV file contains information about the status of logical devices (LDEVs). A record is created for each LDEV.

Table A-29 LdevStatus.csv file (Title: <<LDEV Status>>)

Item	Content
VDEV#	Virtual device number in which the LDEV is defined
VDEV Status	VDEV status of "VDEV#" 1: Normal, 0: Abnormal
HDEV#	LDEV number
HDEV Status	LDEV status 1: Normal, 0: Abnormal
LDEV Emulation	LDEV emulation type
ECC Group	Number of parity group where the LDEV belongs • If the number starts with "E" (for example, E-1), the parity group contains external volumes. • If the type of the LDEV is Dynamic Provisioning or Thin Image, a hyphen (-) is output. Refer to "LDEV Type" in "LdevInfo.csv" for information about the LDEV type.

LPartition.csv

This CSV file contains information about the cache logical partitioning function. A record is created for each cache partition for a managed resource.

For details of the cache logical partitioning function, see the *Hitachi Unified Storage VM Block Module Performance Guide*.

Table A-30 LPartition.csv file (Title: <<Logical Partitioning>>)

Item	Content
CLPR#	CLPR number
CLPR Name	CLPR name
Cache Size(MB)	Cache size allocated to this CLPR number (in MB)
Cache Residency Size(MB)	Cache Residency Manager cache size allocated to this CLPR number (in MB)
ECC Group	Number of parity group allocated to this CLPR number
LDEV#(V-VOL)	LDEV number allocated to this CLPR number The type of this LDEV is Dynamic Provisioning or Snapshot.

LunInfo.csv

This CSV file contains information about LU path definition. A record is created for each LU path definition.

For details of LU path definition, see the *Hitachi Unified Storage VM Block Module Provisioning Guide*.

Table A-31 LunInfo.csv file (Title: <<LUN Information>>)

Item	Content
Port	Port name
Host Group	Host group name
Host Mode	Host mode specified for this host group
Host Mode Option	Host mode option set for this host group If more than one option is specified, the options are separated with semicolons (;).
LUN#	LUN number for this LU path definition
LDEV#	LDEV number for this LU path definition
Number of LDEVs	Number of LDEVs defined for the LU path definition • If the LDEV identified by the LDEV# is the top LDEV of a LUSE volume, 2 to 36 is output. • If the LDEV is a non-LUSE volume, 1 is output.
Command Device	Information about whether the LDEV is a command device or not: • On: Command Device • On*: Remote Command Device • Off: others
Command Security	Information about whether the command device is secured: • On • Off

Item	Content
CVS	Information about whether the LDEV is a custom-sized volume or not: • On: Customized volume • Off: Others
CHB Location	Name of a channel blade (CHB) on which this port is installed
Package Type	Type of the CHB indicated by CHB location Example: HF8G (CHB)
Resource Group ID (Host Group)	Resource group ID of host group
Resource Group Name (Host Group)	Resource group name of host group

LunPortInfo.csv

This CSV file contains information about LU path definition. A record is created for each port.

For details of LU path definition, see *Hitachi Unified Storage VM Block Module Provisioning Guide*.

Table A-32 LunPortInfo.csv file (Title: <<LUN Port Information>>)

Item	Content
Port	Port name
Security Switch	The setting status of the security switch: • On • Off
Port Address	Port address (2-digit number in the hexadecimal format)
Loop ID	Port address (number in the decimal format)
Fabric	One of the Fibre topology settings indicating the setting status of the Fabric switch: • On • Off
Connection	One of the Fibre topology settings: • Point to Point • FC-AL
Channel Speed	Channel Speed of this port: • 2Gbps • 4Gbps • 8Gbps • Auto

Item	Content
WWN	WWN of this port

LuseInfo.csv

This CSV file contains information about a LUN Expansion (LUSE) volume or a single volume. A record is created for each LUSE volume or a single volume that is not extended.

For details about LUN Expansion, see the *Hitachi Unified Storage VM Block Module Provisioning Guide*.

Table A-33 LuseInfo.csv file (Title: <<LUSE Information>>)

Item	Content
LDKC:CU:LDEV	Top LDEV number of the LUSE volume If the volume is a non-LUSE volume, the LDEV number is displayed.
LDEV Emulation	Emulation type of LDEVs configuring the LUSE volume
Volume Size(MB)	The total capacity of this volume (in MB)
Number of LDEVs	Number of LDEVs configuring the LUSE volume (2 to 36) If the volume is a non-LUSE volume, 1 is indicated.
LDKC:CU:LDEV(0), (1), …, (35)	List of LUSE volume components The top LDEV is displayed by "LDKC:CU:LDEV", starting with LDEV as the head. If the volume is a non-LUSE volume, (1) to (35) are blank.

MicroVersion.csv

This CSV file contains information about microcode versions.

Table A-34 MicroVersion.csv file (Title: <<Micro Version>>)

Item	Content
DKCMAIN	The version of the microcode for the RAID storage system
SVP	The version of the microcode installed on the service processor
CUDG4	CUDG4 version
ROM BOOT	ROM BOOT version
RAM BOOT	RAM BOOT version
CMBK	CMBK version
Config	Config version

Item	Content
HDD	HDD microcode version. HDD version in the format of "(HDD device type - code):(version)." If an HDD is not installed, only a colon (:) is displayed.
HDD(SVP)	HDD(SVP) version
Expander	Expander version
CFM	CFM version
DKB	FW version for SAS-CTL
Printout Tool	Printout tool version
Expander (DBF)	DBF Expander version
Expander (DB6A)	DB6A Expander version[1]
Note 1. This item appears only when using the DB60 dense drive box. All other items appear whether the DB60 dense drive box is used or not.	

MlcEnduranceInfo.csv

This CSV file contains information about endurance information of MLC. A record is created for each MLC endurance information.

If you change the SVP time 1 month or more, the history acquisition months will not be in order.

Table A-35 MlcEnduranceInfo.csv file (Title: <<MLC Endurance Information>>)

Item	Content
ECC Group	Number of parity group of which this MLC (including FMD) is a component
CR#	C# and R#, which identify the PDEV
Device Type-Code	Drive type code of this drive Output example: SLR5B-M200SS
Used Endurance Indicator (%)	Current SSD life [%]
History1 (date)	Date on which SSD life was acquired (1 month ago)
History1 (%)	SSD life [%] (1 month ago)
History2 (date)	Date on which SSD life was acquired (2 months ago)
History2 (%)	SSD life [%] (2 months ago)
History3 (%) ... History 119 (%)	SSD life [%] (3 months ago ...119 months ago)
History120 (date)	Date on which SSD life was acquired (120 months ago)
History120 (%)	SSD life [%] (120 months ago)

ModePerLpr.csv

This CSV file contains information about system option modes. A record is created for each system option mode.

Table A-36 ModePerLpr.csv file (Title: <<System Option Mode Per LPR>>)

Item	Content
System Option Mode#	System option mode #
LPR#0, LPR#1, …, LPR#31	System option mode for LPR#0 to LPR#31 • If the system option mode is on: On • If the system option mode is not on: Blank

MpPathStatus.csv

This CSV file contains information about the status of logical paths. A record is created for each MP unit or HMA.

Table A-37 MpPathStatus.csv file (Title: <<MP Path Status>>)

Item	Content
MPU#/HMA#	MP unit number or HMA number • For MP unit number MPU#00 to MPU#03 • For HMA number HMA#00 to HMA#01
CMG#00, …, CMG#03	Cache module group path status for MP unit number in the format of "CMG#*XX*" 1: Normal, 0: Abnormal *XX*: Cache module group number
MPU#00-00, …, MPU#00-03 MPU#01-00, …, MPU#01-03	MP unit path status for MP unit number in the format of "MPU#*XX-YY*" 1: Normal, 0: Abnormal *XX*: HMA number *YY*: MP unit number
CMG#00-00, …, CMG#00-03 CMG#01-00, …, CMG#01-03	Cache module group path status for HMA number in the format of "CMG#*XX-YY*" 1: Normal, 0: Abnormal *XX*: I path number *YY*: Cache module group number
MPU#00, …,MPU#03	MP unit number path status for HMA number in the format of "MPU#*XX*" 1: Normal, 0: Abnormal

Item	Content
	XX: MP unit number

MpPcbStatus.csv

This CSV file contains information about the status of MP units. A record is created for each MP unit.

Table A-38 MpPcbStatus.csv file (Title: <<MP Pcb Status>>)

Item	Content
MPU ID	MP unit ID

Auto Assignment	Information about whether this MP unit is set to be automatically assigned to each resource or not
	 • Enabled
	   Set to be automatically assigned.
	 • Disabled
	   Not set to be automatically assigned.

MP PCB Location	Name of MP blade where the MP unit is installed
MP PCB ID	ID of MP blade where the MP unit is installed
MPU Status	MP unit status 1: Normal, 0: Abnormal
MP#00, #01, #02, #03	MP status on this MP unit 1: Normal, 0: Abnormal

PcbRevInfo.csv

This CSV file contains information about revisions of packages such as channel blades (CHBs) and others. A record is created for each package.

Table A-39 PcbRevInfo.csv file (Title: <<PCB Revision Information>>)

Item	Content
Cluster#	Cluster number
Location	Package name Example: • For CHB: CHB-1A • For port: 1A
Name	Product name of the package or some other name
PK Revision	Revision of the package
Factory	Factory manufacturing the package
Number	Serial product number

Item	Content
MAC Address	MAC address of the product

PdevCapaInfo.csv

This CSV file contains information about physical device (PDEV) capacities. A record is created for each of three classifications shown in "PDEV Kind".

Table A-40 PdevCapaInfo.csv file (Title: <<PDEV Capacity Information>>)

Item	Content
PDEV Kind	The following three classifications are output: • OPEN System (TB) • Total Capacity (TB) • Number of PDEVs
SAS Drive	SAS drive capacity (in TB)
Spare Drive	Spare drive capacity (in TB)
SSD Drive	SSD capacity (in TB)

PdevInfo.csv

This CSV file contains information about physical devices (PDEVs). A record is created for each PDEV.

Table A-41 PdevInfo.csv file (Title: <<PDEV>>)

Item	Content
ECC Group	Number of parity group of which this PDEV is a component If it is a spare drive, Spare Drive is output.
Emulation Type	Emulation type for the parity group indicated by "ECC Group" Blank if the "ECC Group" is Spare Drive.
CR#	C# and R#, which identify the PDEV
PDEV Location	PDEV location name
Device Type	Drive type • SAS • SSD
RPM	Rotations per minute of this drive A hyphen (-) is displayed as RPM when the drive is SSD.
Device Type-Code	Device type code of this drive Output example: DKR5D-J900SS
Device Size	Drive size (inches)

Item	Content
	• 2.5 • 3.5
Device Capacity	Drive capacity in GB or TB
Drive Version	Drive firmware version
DKB1	Name of the DKB (1) controlling the PDEV
DKB2	Name of the DKB (2) controlling the PDEV
Serial Number#	Serial number of this drive
RAID Level	RAID level of the parity group indicated by "ECC Group" Blank if the "ECC Group" indicates Spare Drive.
RAID Concatenation #0	Number of parity group to be concatenated to parity group (#0) identified by "ECC Group" Blank if the parity group is not concatenated to another parity group or is Spare Drive.
RAID Concatenation #1	Number of parity group to be concatenated to parity group (#1) identified by "ECC Group" Blank if the parity group is not concatenated to another parity group or is Spare Drive.
RAID Concatenation #2	Number of parity group to be concatenated to parity group (#2) identified by "ECC Group" Blank if the parity group is not concatenated to another parity group or is Spare Drive.
Resource Group ID (ECC Group)	Resource group ID of parity group
Resource Group Name (ECC Group)	Resource group name of parity group
Encryption	Encryption status of the parity group to which the PDEV belongs. • Enabled: Encryption enabled • Disabled: Encryption disabled

PdevStatus.csv

This CSV file contains information about the status of physical devices (PDEVs). A record is created for each PDEV.

Table A-42 PdevStatus.csv file (Title: <<PDEV Status>>)

Item	Content
CR#	C# and R#, which identify the PDEV
Pdev Status	PDEV status 1: Normal, 0: Abnormal
Port0 Status	Status of Port 0 on this PDEV

Item	Content
	1: Normal, 0: Abnormal
Port1 Status	Status of Port 1 on this PDEV 1: Normal, 0: Abnormal
Pdev Location	Location name of this PDEV

PkInfo.csv

This CSV file contains information about channel blades (CHBs). A record is created for each CHB.

Table A-43 PkInfo.csv file (Title: <<PK>>)

Item	Content
Basic/Option	Package location: • Basic • Option1 to Option5
CHB Location	CHB name
Port#	Number of ports installed on the CHB
Port	Name of ports installed on the CHB
Package Type	CHB type Example: HF8G (CHB)
SFP Kind	SFP (Small Form factor Pluggable) Kind • Short Wave
SFP Status	SFP Status: • Normal • Failed • Not Fix
Port Type	Port Type Example: • Initiator • Target • External
Fabric	One of the Fibre topology settings indicating the setting status of the Fabric switch: • On • Off
Connection	One of the Fibre topology: • Point to Point • FC-AL
Port Address	Port address (2-digit number in the hexadecimal format)

Item	Content
Resource Group ID (Port)	Resource group ID of port
Resource Group Name (Port)	Resource group name of port

PpInfo.csv

This CSV file contains information about the software. A record is created for each software product.

For details about the license key, see .

Table A-44 PpInfo.csv file (Title: <<PP Information>>)

Item	Content
Program Product name	Software name
Install	Information about whether the installed license key is enabled or not • Enable: Installed and the software can be used. • Disable: Installed but the software cannot be used.
Key Type	Installed license key type • Permanent • Temporary • Emergency • Term If no license key is installed, "Not Installed" is output.
Permitted Volumes(TB)	Permitted volume capacity for this software (in TB) The used volume capacity is not output. If no upper limit value is set for the capacity, "Unlimited" is output.
Expiration Date	Expiration date of the software The format is mm/dd/yyyy (Month/Day/Year).
Status	License key status of the software • Installed • Not Enough • Capacity Insufficient • Time Out • Not Installed • Installed (Disable)

SMfundat.csv

This CSV file contains information about SM functions. A record is created for each of five classifications shown in "SM Install Function".

Table A-45 SMfundat.csv file (Title: <<SM Install function>>)

Item	Content
SM Install function	The following five classifications are output • Base (SI/VM/DP) • SI/VM/DP Extension1/TC/UR/TI • SI/VM/DP Extension2/TI Extension • TC/UR Extension • HDT
Availability	Information about whether the function of "SM Install function" is enabled or not • Enable • Disable

SsdDriveInfo.csv

This CSV file contains information about SSDs. A record is created for each SSD.

Table A-46 SsdDriveInfo.csv file (Title: <<SSD Drive Status>>)

Item	Content
ECC Group	Number of the parity group of which this SSD is a component.
CR#	C# and R#, that identify the PDEV
PDEV Location	Drive type code of this drive PDEV location name Output example: SLR5B-M200SS
Device Type-Code	Drive type code (for example, SLR5B-M200SS)
Device Capacity	Drive capacity in GB or TB
SSD Device Type	SSD drive type. • SLC • MLC • FMD
Used Endurance Indicator (%)	SSD life [%] Blank if SSD is SLC
Used Endurance Indicator Threshold (%)	SSD life threshold [%] Blank if SSD is SLC
Used Endurance Indicator Warning SIM (%)	Warning SIM threshold [%] Blank if SSD is SLC

Item	Content
FMD Battery Life Indicator Warning SIM (%)	Threshold of battery life warning SIM (in %) Blank if SSD is other than FMD.
FMD Battery Life Indicator (%)	Lapsed battery life (in %) Blank if SSD is other than FMD

SsidInfo.csv

This CSV file contains information about SSIDs. A record is created for each SSID.

Table A-47 SsidInfo.csv file (Title: <<Subsystem ID>>)

Item	Content
DEV# Start	Starting LDEV number of the subsystem ID
DEV# End	Last LDEV number of the subsystem ID
SSID	Subsystem ID

SysoptInfo.csv

This CSV file contains information about system options.

Table A-48 Sysoptinfo.csv file (Title: <<System Option Information>>)

Item	Content
Spare Disk Recover	Speed of copying data to the spare drive • Interleave mode • Full Speed mode
Dynamic Sparing	Information about whether to perform automatic copy to a spare drive if the occurrences of drive failures exceed the threshold. • On • Off
Correction Copy	Information about whether to perform correction copy to a spare drive if a drive is blocked • On • Off
Disk Copy pace	Speed of copying the spare drive in the Interleave mode • Faster • Medium • Slower
System Option On	System options that are set to ON
Link Failure Threshold	Threshold to notify the link failure

WwnInfo.csv

This CSV file contains information about hosts. A record is created for each host.

For details about the host setting, see the *Hitachi Unified Storage VM Block Module Provisioning Guide*.

Table A-49 WwnInfo.csv file (Title: <<World Wide Name Information>>)

Item	Content
Port	Port name
Host Group	Host group name
Host Mode	Host mode which is set for the host group
Host Mode Option	Host mode option which is set for the host group Multiple options are separated by semicolons (;).
WWN	World Wide Name of the host bus adapter registered to the host group
Nickname	Nickname of the host
Host Group#	Host group number (hexadecimal)

B

Report Configuration Tool command reference (raidinf commands)

This appendix describes the `raidinf` commands, symbols, and reports.

raidinf command list and command description

The following lists the `raidinf` commands and symbols.

Table B-1 raidinf command list

Command	Description
`raidinf add report`	Creates a report.
`raidinf delete report`	Deletes a report.
`raidinf download report`	Downloads a report.
`raidinf get reportinfo`	Displays a list of reports.

Table B-2 Conventions of the command format

Symbol	Description
< >	The item enclosed in this symbol is variable.
| Vertical bar	Symbol is placed between multiple items to indicate "or". For example: `-A | -B` Specifies -A or -B.

[ ]
Square brackets
	Theenclosed item can be omitted. If some items are delimited by the vertical bar, specify one or omit all items.
	For example:
	`[ -A ]`
	Specifies nothing or specifies -A.
	`[ -a | -b ]`
	Specifies nothing or specifies -a or -b.

{ }
Curly brackets
	The meaning differs depending on the enclosed item.
	• If items in curly brackets are delimited by vertical bars, one of the items must be specified.
	   For example:
	   `{ -A | -B |-C }`
	   Specifies -A, -B, or -C.
	• If curly brackets enclose items enclosed by square brackets, at least one of the items must be specified.
	   For example:
	   `{ [ -A ][ -B ][ -C ]}`
	   Specifies one or more items from -A, -B, or -C.

raidinf command syntax

The syntax of the `raidinf` commands and the basic format of the options and parameters are described next.

Syntax

```
raidinf [-h] <action> <object> –servername <hostname/ipaddress>
 [{-report <report_name> | -report_id <report_id>}] [-targetfolder
 <folder>] [-fill]

raidinf [-h] –login <user_name> <password> –servername <hostname/
ipaddress>

raidinf [-h] –logout –servername <hostname/ipaddress>
```

Options and parameters

Option	Description
`[-h]`	Displays help for raidinf.
<action>	Specifies command operation. You can specify the following commands. • `get`: Displays a list of reports. • `add`: Creates a report. • `delete`: Deletes a report. • `download`: Downloads a report.
<object>	Specifies an operation target object. You can specify the following objects. • `reportinfo` to display a list of reports. • `report` to create, delete, or download a report.
`–servername` *<hostname/ipaddress>*	Specifies the host name or the IP address of the SVP.
`[{-report` *<report_name>* `| -report_id` *<report_id>*`}]`	• `-report` specifies a report name within 32 characters. If you specify more than 32 characters, the 33rd and subsequent characters are ignored. • `-report_id` specifies a report ID displayed by the report list. Because a report ID is a unique ID to each of the reports, a specific report can be identified even if reports of the same name exist.
`[-targetfolder` *<folder>*`]`	Specifies a folder name to which a report is downloaded. The folder whose name you specify must already exist and you must have permissions to the folder.
`[-fill]`	Deletes a report only if the number of created reports is 20.
`–login` `[`*<user_name>* *<password>*`]`	Executes a user authentication for Storage Navigator. Specifies a user name and a password. The user is logged out automatically three minutes (180 seconds) after the last command is entered.
`–logout`	Logs out of Storage Navigator.

Examples

This example authenticates *user01* using the password *xxxxxx*.

```
# raidinf –login user01 xxxxxx –servername svp.xxx.co.jp
```

This example executes a logout.

```
# raidinf -logout -servername svp.xxx.co.jp
```

Displays help.

```
# raidinf -h
Model  : RAIDINF/WindowsNT
Ver&Rev: 01-00-03/00

Usage:  raidinf [options]
        raidinf <action> <object> [parameters]
Options:
  -h                                 Help/Usage
  -login <user_name> <password>      Specify LOGIN explicitly
  -logout                            Specify LOGOUT

<User authentification>
  <option>        <parameters>
  -login          <user_name> <password> -servername <hostname/
ipaddress>
  -logout         -servername <hostname/ipaddress>

<Report management>
 <action> <object>    <parameters>
  get     reportinfo -servername <hostname/ipaddress>
  add     report     -servername <hostname/ipaddress>
                     [-report <report_name>]
  download report    -servername <hostname/ipaddress> {-report
    <report_name> | -report_id <report_id>} -targetfolder <folder>
  delete  report     -servername <hostname/ipaddress> {-report
    <report_name> | -report_id <report_id>} [-fill]

Parameters:
  -servername   <hostname/ipaddress>  Specify the SVP hostname or
    IP address.
  -report        <report_name>        Specify the Report Name.
  -report_id    <report_id>           Specify the ReportID.
  -targetfolder <folder>              Specify the download folder.
  -fill                               Report is deleted only full
    of the server reports.
```

raidinf add report

The `raidinf add report` command creates a report.

If other users have created 20 reports, the logged in user cannot create a report and will receive an error.

Syntax

```
raidinf add report -servername <hostname/ipaddress> [-report
<report_name>]
```

Options and parameters

Option	Description
servername <*hostname/ipaddress*>	Specifies the host name or the IP address of the SVP.
[-report <*report_name*>]	Specifies a report name, up to 32 characters. If you specify more than 32 characters, the 33rd and subsequent characters are ignored. If the report name is omitted, the default report name YYMMDD-CreateConfigurationReport is specified. The hyphen (-) cannot be specified at the beginning of the report name.

Examples

This example creates a report with the default report name.

```
# raidinf add report -servername 10.213.74.121
ReportName UserName CreateTime
101009-CreateConfigurationReport user01    2010/10/09-12:43:10
```

This example specifies the report name 101009-CreateConfigurationReport and creates a report.

```
# raidinf add report -servername 10.213.74.121 -report
101009-
CreateConfigurationReport
ReportName                           UserName
CreateTime
101009-CreateConfigurationReport user01    2010/10/09-12:43:10
```

The respective items of the output example are explained next.

- ReportName
  The report name is displayed (up to 32 characters).
- UserName
  The user name is displayed (up to 16 characters). If the user name exceeds 16 characters, an ellipsis (...) is displayed.
- CreateTime
  The time of creating a report is displayed (up to 9 characters).

raidinf delete report

The raidinf delete report command deletes a report.

If multiple reports of the same name exist, the command deletes the oldest report. If the specified report does not exist, the command does not do anything and is normally terminated.

Reports created using Storage Navigator can also be deleted.

Syntax

```
raidinf delete report -servername <hostname/ipaddress>
 {-report<report_name> | -report_id
 <report_id>} [-fill]
```

Options and parameters

Option	Description
`servername` <*hostname/ipaddress*>	Specifies the host name or the IP address of the Web server (SVP).
{`-report` <*report_name*> | `-report_id` <*report_id*>}	Specifies either `-report` or `-report_id`. • `-report` specifies a report name (up to 32 characters). If you specify more than 32 characters, the 33rd and subsequent characters are ignored. • `-report_id` specifies a report ID displayed by the report list. Because a report ID is a unique ID to each of the reports, a specific report can be identified even if reports of the same name exist.
[`-fill`]	Deletes the report only if the total number of reports is 20. In there are less 20 reports, the specified report is not deleted even if it exists.

Examples

This example specifies the report name `101009-CreateConfigurationReport` and deletes the report.

```
# raidinf delete report -servername 10.213.74.121 -report 101009-
CreateConfigurationReport
```

`101009-CreateConfigurationReport` is deleted in the SVP.

raidinf download report

The `raidinf download report` command downloads a report.

Reports created by Storage Navigator can also be downloaded. The report in process of creation cannot be downloaded.

The name of the downloaded file is Report_*report name*.tgz. Note that the files are overwritten if reports of the same name has already existed.

Example: the name of the downloaded file when the report name is `110309-CreateConfigurationReport`

```
Report_110309-CreateConfigurationReport.tgz
```

Syntax

```
raidinf download report -servername <hostname/ipaddress>
 {-report <report_name> | -report_id <report_id>}
 -targetfolder <folder>
```

Options and parameters

Option	Description
`servername <`*hostname/ipaddress*`>`	Specifies the host name or the IP address of theSVP.

`{-report <`*report_name*`> | -report_id <`*report_id*`>}`	Specifies either `-report` or `-report_id`.
	
	• `-report`: specifies a report name within 32 characters. If you specify more than 32 characters, the 33rd and subsequent characters are ignored.
	
	   If a special name `LatestReport` is specified as a report name, the report created on the newest date is downloaded. To download a report named LatestReport, which has the same name as the special name, specify a report ID by -report_id option.
	
	   If multiple reports of the same name exist, the report of the newest date is the target of download.
	
	• `-report_id`: specifies a report ID displayed by the report list. As a report ID is a unique ID to each of the reports, a specific report can be identified even if reports of the same name exist.

`-targetfolder <`*folder*`>`	Specifies a folder name to which a report is downloaded. The folder whose name you specify must already exist and you have permissions to the folder.

Examples

Downloads the most recently created report.

```
# raidinf download report -servername 10.213.74.121
 -report LatestReport -targetfolder C:\tmp
```

`Report_101009-CreateConfigurationReport.tgz` is downloaded to `C:\tmp`.

This example specifies the report name `101009-CreateConfigurationReport` and downloads the report.

```
# raidinf download report -servername 10.213.74.121
 -report 101009-CreateConfigurationReport -targetfolder C:\tmp
```

`Report_101009-CreateConfigurationReport.tgz` is downloaded to `C:\tmp`.

raidinf get reportinfo

The `raidinf get reportinfo` command displays a list of reports.

Reports created using Storage Navigator are also displayed. A report currently being created cannot be downloaded

Syntax

```
raidinf get reportinfo –servername <hostname/ipaddress>
```

Options and parameters

Option	Description
servername <*hostname/ ipaddress*>	Specifies the host name or the IP address of the SVP.

Examples

Displays a list of reports.

```
# raidinf get reportinfo -servername 10.213.74.121
ReportName                          UserName    CreateTime     ReportID
101009-CreateConfigurationReport user01     2010/10/09-12:43:10 33S3
101008-CreateConfigurationReport user01     2010/10/08-11:22:31 33J3
101007-CreateConfigurationReport user01     2010/10/07-11:17:20 2344
101006-CreateConfigurationReport configuration...
2010/10/06-15:30:42 4n1j
```

The respective items of the output example are explained next.

- ReportName

  The report name is displayed (up to 32 characters).

- UserName

  The user name is displayed (up to 16 characters). If the user name exceeds 16 characters, an ellipsis (...) is displayed.

- CreateTime

  The time of creating a report is displayed (up to 9 characters).

- ReportID

  The report ID is displayed.

SMI-S provider configuration file

This appendix describes the SMI-S provider configuration files.

☐ [User-defined.properties file](#)

User-defined.properties file

This section describes the description format and organization format of SMI-S provider user configuration files and parameters to be defined. The user-defined.properties file is an SMI-S provider user configuration file.

File description format

The format of the user-defined.properties file includes the following items:

- File format: text
- Character code: ISO 8859-1
- Line-end symbol: \n, \r, or \r\n
- Comment: Line on which # or ! is the first non-space character

File organization format

The organization of the user-defined.properties file is shown here:

comment line

  parameter1= parameter1_setting_value

 parameter2= parameter2_setting_value

comment line

Parameters defined in user configuration files

Table C-1 Parameters defined in user configuration files

Parameter name	Description
CipherSuites	Specifies usable cipher suites. Optional item. If no value is specified, the default value applies. For parameter details, see CipherSuites parameter on page C-3.
VVolForSnapshot	Specifies virtual volumes that can be used by the SMI-S provider. Optional item. If no value is specified, the default value applies. If you specify this item, be sure to specify PoolIDForSnapshot as well. For detail parameter details, see VVolForSnapshot parameter on page C-3.
PoolIDForSnapshot	Specifies pools that can be used by the SMI-S provider. Optional item. If no value is specified, the default value applies. If you specify this item, be sure to specify VVolForSnapshot as well. For parameter details, see PoolIDForSnapshot parameter on page C-4.

Parameter name	Description
DefaultSnapshotFunction	Specifies which of Thin Image and Copy-on-Write Snapshot is enabled. Optional item. If no value is specified, the default value applies. For parameter details, see DefaultSnapshotFunction parameter on page C-5.

CipherSuites parameter

Use the CipherSuites parameter to specify usable cipher suites (encryption algorithms). All cipher suites that can be set are specified by default.

The CipherSuites parameter can use any of the following values:

- SSL_RSA_WITH_RC4_128_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA

Setting up the CipherSuites parameter

Connect cipher suites with a comma (,) as a delimiter.

Example

```
CipherSuites=SSL_RSA_WITH_RC4_128_SHA,TLS_DHE_RSA_WITH_AES_128_CB
C_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_S
HA, SSL_RSA_WITH_3DES_EDE_CBC_SHA
```

VVolForSnapshot parameter

Use the VVolForSnapshot parameter to specify virtual volumes that the SMI-S provider can use when you operate Thin Image or Copy-on-Write Snapshot from CreateElementReplica of HITACHI_ReplicationService.

All virtual volumes are specified by default.

Setting up the VVolForSnapshot parameter

Set up the parameter by using <RangeOfVVol> and <SingleVVol> with a comma (,) as a delimiter:

- <RangeOfVVol>: Specifies a range of virtual volumes
- <SingleVVol>: Specifies a single virtual volume

<RangeOfVVol> format

<S2HexLDKC>:<S2HexCU>:<S2HexLDEV>to<E2HexLDKC>:<E2HexCU>:<E2HexLDEV>

- <S2HexLDKC>: LDKC number (two-digit hexadecimal) of the first virtual volume in the specified range
- <S2HexCU>: CU number (two-digit hexadecimal) of the first virtual volume in the specified range
- <S2HexLDEV>: LDEV number (two-digit hexadecimal) of the first virtual volume in the specified range
- <E2HexLDKC>: LDKC number (two-digit hexadecimal) of the last virtual volume in the specified range
- <E2HexCU>: CU number (two-digit hexadecimal) of the last virtual volume in the specified range
- <E2HexLDEV>: LDEV number (two-digit hexadecimal) of the last virtual volume in the specified range

<SingleVVol> format

<2HexLDKC>:<2HexCU>:<2HexLDEV>

- <2HexLDKC>: LDKC number (two-digit hexadecimal) of the single virtual volume to be specified
- <2HexCU>: CU number (two-digit hexadecimal) of the single virtual volume to be specified
- <2HexLDEV>: LDEV number (two-digit hexadecimal) of the single virtual volume to be specified

Example

```
VVolForSnapshot=00:00:00to00:00:FF,00:02:00,00:04:00to00:04:FF
```

In this example, a virtual volume having one of the following LDEV IDs is used as the snapshot target:

- From 00:00:00 (LDKC=0,CU=0,LDEV=0) to 00:00:FF (LDKC=0,CU=0,LDEV=255)
- 00:02:00 (LDKC=0,CU=2,LDEV=0)
- From 00:04:00 (LDKC=0,CU=4,LDEV=0) to 00:04:FF (LDKC=0,CU=4,LDEV=255)

PoolIDForSnapshot parameter

Use the PoolIDForSnapshot parameter to specify pools that the SMI-S provider can use when you run Thin Image or Copy-on-Write Snapshot from CreateElementReplica of HITACHI_ReplicationService.

All pools are specified by default.

Setting up the PoolIDForSnapshot parameter

Set up the parameter by using <RangeOfPoolID> and <SinglePoolID> with a comma (,) as a delimiter:

- <RangeOfPoolID>: Specifies a range of pool IDs
- <SinglePoolID>: Specifies a single pool ID

<RangeOfPoolID> format

<Start PoolID>to<End PoolID>

- <Start PoolID>: ID of the first pool in the specified range
- <End PoolID>: ID of the last pool in the specified range

<SinglePoolID> format

<PoolID>

- <PoolID>: ID of the pool to be specified

Example

PoolIDForSnapshot=1to2,4,6to8

In this example, pools having one of the following pool IDs are used as snapshot pools:

- 1 to 2
- 4
- 6 to 8

DefaultSnapshotFunction parameter

Use the DefaultSnapshotFunction parameter to specify the replication function that will be enabled in CreateElementReplica in HITACHI_ReplicationService. Thin Image is specified by default.

Table C-2 Values for the DefaultSnapshotFunction parameter

Value	Description
TI	Enables Thin Image

Setting up the PoolIDForSnapshot parameter

Specify TI

Example

DefaultSnapshotFunction=TI

SMI-S provider configuration file

D

Storage Navigator GUI reference (main windows)

This appendix describes the Storage Navigator main window and wizards.

☐ Storage Navigator main window

☐ Column Settings window

☐ Storage Systems window

☐ Edit Storage System wizard

☐ Edit Information Display Settings window

☐ Resource Lock Properties window

☐ Tasks window

☐ Task Properties window

☐ Suspend Tasks window

☐ Resume Tasks window

☐ Delete Tasks window

☐ Disable Auto Delete window

☐ Enable Auto Delete window

☐ Reports window

- ☐ [Create Configuration Report window](#)

- ☐ [Delete Reports window](#)

- ☐ [User Groups window](#)

- ☐ [Window when User Group is selected](#)

- ☐ [Create User wizard](#)

- ☐ [Change Password wizard](#)

- ☐ [Edit User wizard](#)

- ☐ [Add Users wizard](#)

- ☐ [Remove Users window](#)

- ☐ [Delete Users window](#)

- ☐ [Create User Group wizard](#)

- ☐ [Edit User Group wizard](#)

- ☐ [Delete User Groups window](#)

- ☐ [Release Lockout window](#)

- ☐ [Edit Resource Group Assignment wizard](#)

- ☐ [Edit Role Assignment wizard](#)

- ☐ [Alerts window](#)

- ☐ [Alert Properties window](#)

- ☐ [LDAP Properties window](#)

- ☐ [RADIUS Properties](#)

- ☐ [Kerberos Properties](#)

- ☐ [Setup Server wizard](#)

☐ Setup Server for LDAP

☐ Setup Server for RADIUS

☐ Setup Server for Kerberos

☐ Edit SIM Syslog Server Settings wizard

Storage Navigator main window

Menu

Item	Description
←	Click to return to the previous window.
→	Click to advance to the next window.
File	• **Refresh All**: Acquires all the information about the storage system and updates both the SVP and Storage Navigator. You must have Storage Administrator (Initial Configuration) role to use this function. See Table 4-2 Roles, Permissions, and Capabilities on page 4-8. • **Logout:** Logs the current user out of Storage Navigator.
Actions	Provides actions to the storage system such as creating LDEVs or performing replication copy.
Reports	• **Task Management:** Manages the tasks that will be applied to the storage system. • **Configuration Report**: Creates and downloads the configuration report about the storage system.

Item	Description
	• **Performance Monitor:** Monitors performance of the storage system. • **Shredding Report**: Downloads the shredding report.
Settings	• **User Management:** Manages user accounts of Storage Navigator including changing password. • **Resource Management**: Manages resource groups. • **Security**: Performs audit log and security operations. • **Environmental Setting**: Configures license key, authentication servers, or refresh interval of the window. Resets view settings that can be customized, such as width or order of table column. See the table, Column Settings window on page D-11, for items that are reset using Reset View Settings.
View	Changes the font size in the window.
Alert	Indicates that an alert (SIM) has occurred in the storage system. When you click **Alert**, the details of the alert appear. Once an alert occurs, it exists until you complete all SIM on SVP. • 🟢: No alert has occurred. • ⓘ: Service level information appears. • ⚠: A warning level alert has occurred (Moderate). • ▼: An error level alert has occurred (Serious). • ▦: An acute level alert has occurred. • ❔: No information can be retrieved from the SVP.
Audit Log	Indicates how many of the audit log files are stored. When you click **Audit Log**, you can download the audit log files. • ⬛: Audit log file is under the threshold. • ⬛: Audit log file exceeds the threshold. • ⬛: Audit log file has exceeded the threshold. Some data has been overwritten. • ❔: No information can be retrieved from the SVP.
Resource Lock	Indicates that a user or program is applying a task to the storage system. • 🔓 Resource Unlocked: no one is applying a task to the storage system. • 🔒 Resource Locked: a user or program is applying a task to the storage system. • ❔: no information can be retrieved from SVP. When the value of Top Status Indicator Refresh Interval is large (the default value is 60 seconds), this may not display the same status as "**Status**" on the **Resource Lock Properties** window.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
Logged in as	The user name of the person who is logged in
Logout	Logs the current user out from Storage Navigator
Refresh View	Redisplays the displayed window
Help	Opens the help screen for the displayed window

Table
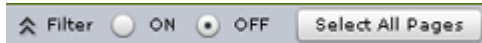
Item	Description
Filter	Open the filtering area.
ON OFF	When filter is ON, the items in the table are narrowed down according to the specified filtering conditions.
Select All Pages	Selects all pages when the table has multiple pages.

Item	Description
Options	Sets the table options. • Column Settings: Specifies whether you display or hide table columns. • Rows / Page: Specifies how many rows to display in one page. • Capacity Unit: Specifies the capacity unit of LDEVs (If you change the capacity unit from MB to GB, TB, or some other unit, the capacity is rounded down to two decimal places).
⏮	Displays the first page.
⏪	Displays the previous page.
1 / 2	Specifies the number of the page to display.
⏩	Displays the next page.
⏭	Displays the last page.

Using the main window and wizard

When you select an operation to perform, a wizard or secondary window appears.

3. Click to open a wizard.
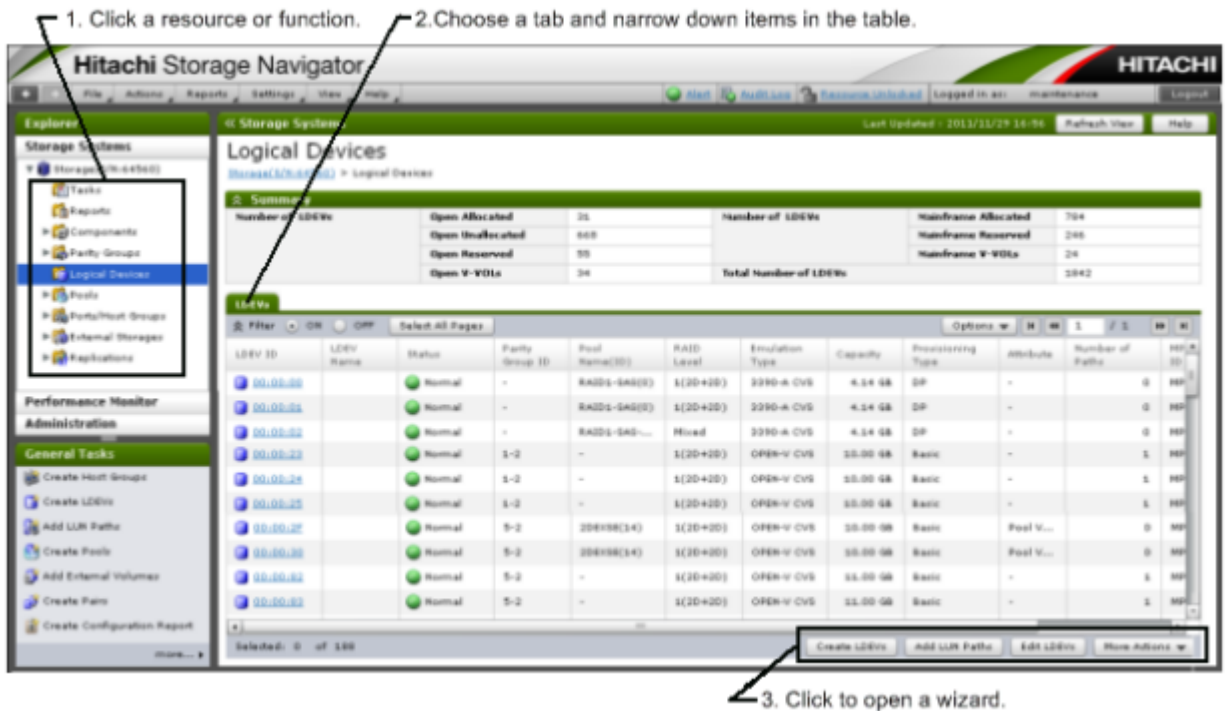
Figure D-1 Using Storage Navigator main window

To perform an operation using the main window and a wizard:

1. Click a function in the resource tree in the Explorer.

2. If necessary, choose a tab and use a filter to narrow down the items in the table.
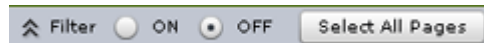
3. Select an item in the table and click a button to open a wizard.

4. Set options in the wizard and click **Finish** to confirm the setting.

5. Enter a task name and click **Apply** to apply the setting to the storage system. The setting is queued as a task and performed in order.

Tip: To open the task window after closing the wizard, select **Go to tasks window for status** and click **Apply** in the wizard.

Figure D-2 Using wizard buttons

6. Open the task window to verify the result of the operation. A task can be suspended or canceled if the processing of the task is not started.

Main window controls

Buttons

The following figure shows the Back and Next buttons that appear at upper left of the main window:
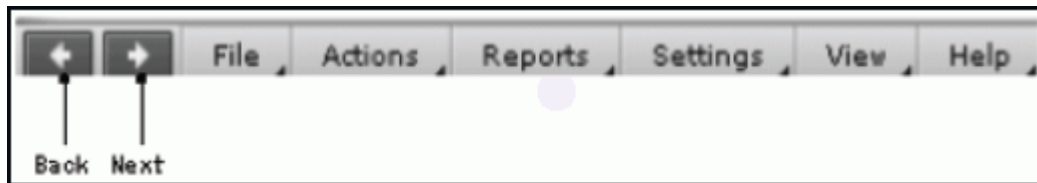
Figure D-3 Back and Next buttons in main window

The Back button displays the previous window; the Next button displays the next window. Storage Navigator tracks up to 10 operations and the windows that display depends the selection from the navigation tree.

The following figure shows the buttons that appear at upper right of the main window:
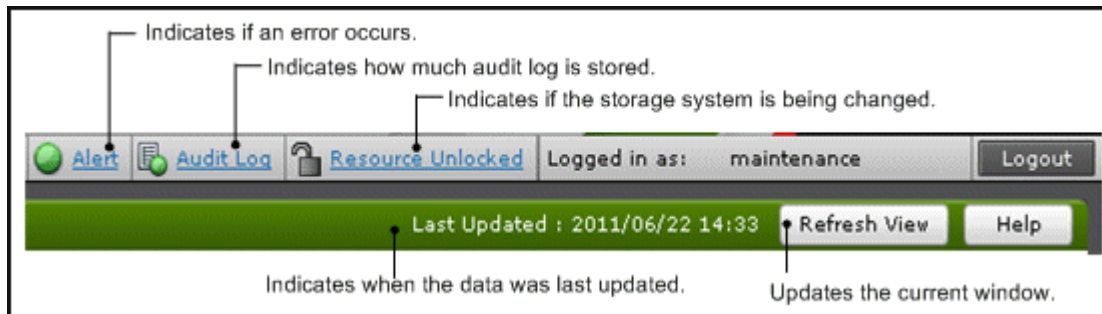
Figure D-4 Buttons at upper right of main window

Alert, **Audit Log**, and **Resource Lock** are updated every 60 seconds by default. To change the refresh interval, click **Settings** > **Environmental Settings** > **Edit Information Display Settings**, then change the value for **Top Status Indicator Refresh Interval**.

If you place the mouse cursor over "Last Updated", Storage Navigator displays a tooltip (a small "hover box") that shows how many minutes ago the last update was made. The update interval is 1 minute. If "----/--/-- --:--" is displayed, click **Refresh View** to show the minutes correctly.

Storage Navigator GUI reference (main windows)

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Table

The following figures shows the controls used to view and filter the results in a main window table:
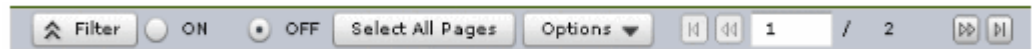
Figure D-5 Table options in main window

To scroll through pages of the table, use the left and right arrows or type a page number into the number field. To select all rows in the table, click **Select All Pages**. If filter is ON, the filtered rows are selected. To sort the table, click the header of the column that you want to use to sort.

Use the **Options** drop-down list to change the number of rows in a page or to change the capacity unit to display.

To save the displayed information to a TSV file, click **Export** under **More Actions**. This action is demonstrated in the following figure.
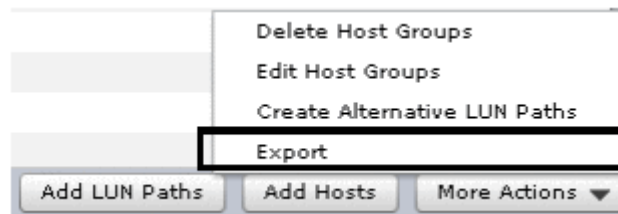
Figure D-6 Export button to save a TSV file

When you change the default file name, confirm that the file name contains the .tsv extension to save the file.

Filtering

To filter the table, select or input the desired filtering conditions and click **Apply**.

Note:

- Users can set up to 16 conditions.
- When the input condition is wrong, click **Apply** to clear the condition.
- Select the attribute whose date and time values must be entered, and then enter the values.
- The values of date and time are "YYYY/MM/DD" and "hh:mm:ss", respectively.
- After you enter the date in the first box, "00:00:00" is displayed in the second box as a default time value. Edit this value as needed and click Apply.
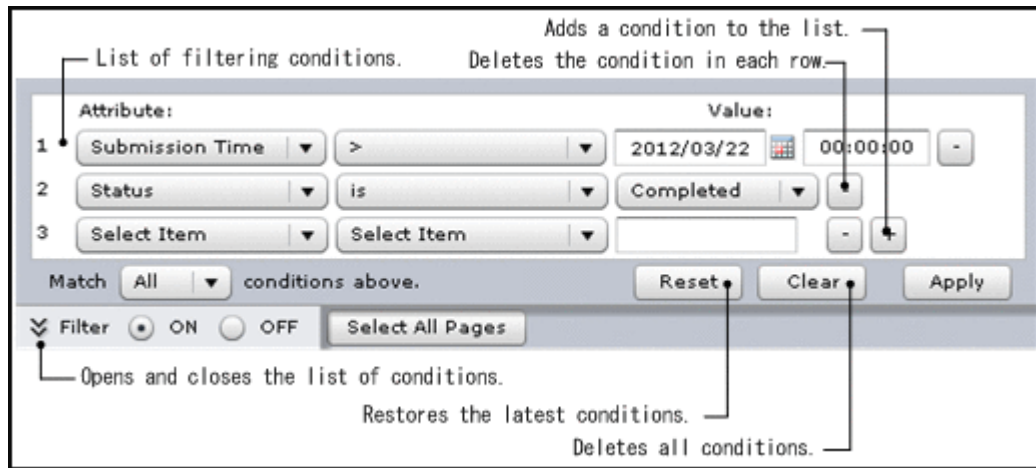
Figure D-7 Filtering in main window

Tooltip

When text is displayed in the main window, ellipses (...) may be displayed to show that the text is truncated. If you place the mouse cursor over an ellipsis (...), the full text is displayed in a tooltip (a small "hover box").
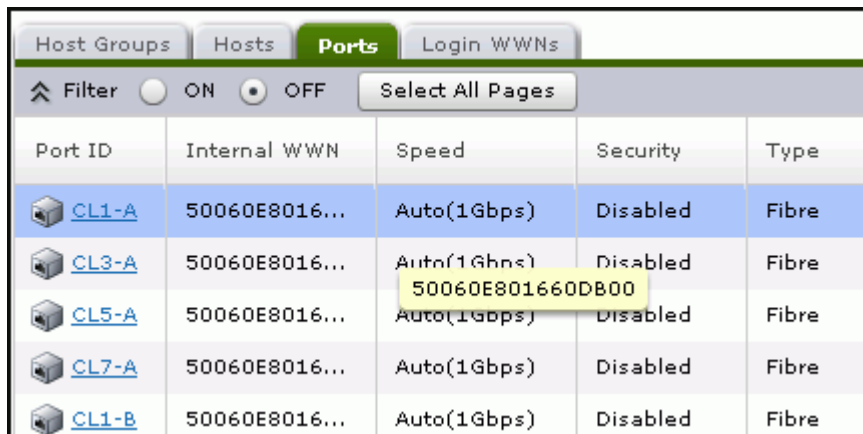
Figure D-8 Tooltip in main window

Reset View Settings

Window part		Item	State after reset
Magnification		-	Normal (100%)
Summary		Open/Closed	Open
Table	General	Selecting row	NA
		Page	First page
		Scroll position	Top left
	Column	Sort	NA

Storage Navigator GUI reference (main windows)

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Window part		Item	State after reset
		Width	Default state*
		Order	Default state*
	Option	Row/Page	1000
		Capacity unit	GB
		Setting column	Default state*
	Filter	ON/OFF	OFF
		Settings	NA
		Open/Closed	Closed
Wizard	Option part	Open/Closed	Default state*
LUN ID Notation		-	Decimal
*The default state varies from window to window.			

Column Settings window

Setting fields

Item	Description
Restore Default Settings	Changes the selection of the displayed columns to the factory default settings.
Checkbox	Selects the columns to display. Click the checkbox next to the name of each column that you want to display. After making the selections, click OK. Only the columns whose checkboxes are selected are displayed. Columns whose checkboxes are not selected are not displayed. Note that you cannot select the checkboxes of the columns that must always be displayed because they are deactivated. When you deselect the checkbox of a column with sort/filter settings, the sort/filter settings are released.
Column Name	Displays the names of the columns in the table. If a column contains two rows, the name of the upper row is shown on the left of the vertical bar (|). The name of the lower row is shown on the right of the vertical bar.

Storage Systems window

- Hardware Summary on page D-13
- Allocation Summary on page D-13
- Physical Summary on page D-14

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Hardware Summary

Item	Description
Storage System Name	Device name of the storage system
Storage System Type	Model type of the storage system
Serial Number	Serial number of the storage system
IP Address	IP address of the SVP
Contact	Contact information such as personnel and telephone number where you can inquire about the storage system
Location	Location of the connected storage system
Microcode Version	**Main:** Version of the microcode installed in the connected storage system **SVP:** Version of the Storage Navigator installed in the SVP. **RMI Server**: Version of the RMI server installed in the SVP
Total Cache Size	This is the total size of the cache memory in the storage system.
Edit Storage System	This item allows editing of storage system name, contact, and location.

Allocation Summary

Item	Description
Internal / External	This item switches the displayed items. • **Total:** Displays information on both the internal volumes and the external volumes. • **Internal Only:** Displays information on only the internal volumes. • **External Only:** Displays information on only the external volumes.
Capacity Unit	This item switches the displayed units of the capacity. • **Appropriate:** Displays capacity in appropriate unit depending on the capacity of each item. • **TB/GB/MB:** Displays capacity in the specified unit.
Physical Summary	This item displays the capacity of physical logical devices and the number of devices. For details about this item, see the Physical Summary table.
Virtual Summary	This item displays the capacity of physical logical devices and the number of devices. For details on this item, see the Virtual Summary table.
Total DP Subscription Rate	This item displays the ratio of virtual logical device capacity to physical logical device capacity in the pool volume of Dynamic Provisioning.

Item	Description
Total Number of LDEVs	The number of LDEVs. The information displayed in this field depends on type of system. See the following table.

Physical Summary

#	Item	Description
1	Allocated	This item displays the capacity of the volumes and the number of logical devices that the host can recognize. The volumes include all LDEVs configuring LUSE volumes.
2	Reserved - Used DP Pool	When Total is selected in Internal / External, this item displays the total capacity of pages that are actually used in the Dynamic Provisioning pool volume and the number of logical devices. Thin Image pool volumes are not included in Dynamic Provisioning pool volumes.
		When an item other than Total is selected in Internal / External, this item displays the number of logical devices that are actually used in the Dynamic Provisioning pool volume. The capacity does not display in this item, but is included in Reserved - Other.
3	Reserved - Unused DP Pool	When Total is selected in Internal / External, this item displays the capacity that is subtracted Used DP Pool value from total capacity of pool volume of Dynamic Provisioning. Pool volume of Copy-on-Write Snapshot is not included in pool volume of Dynamic Provisioning. Control cylinder is not included in the capacity. The number of logical devices does not display.
		When an item other than Total is selected in Internal / External, neither the capacity or the number of logical devices displays in this item, but the capacity is included in Reserved - Other.
4	Reserved - Other	This item displays the total capacity and the number of logical devices of the following volumes: • Reserved volumes of Volume Migration • Journal volumes • System disk • Pool volumes of Thin Image • Quorum disk used in High Availability Manager The total capacity includes: • The pool-VOL capacity that is not used as pool capacity • The capacity of the system pool-VOL management area (approx. 4.1GB per pool) The reserved volumes of ShadowImage and Volume Migration that are defined paths are not included. When an item other than Total is selected in Internal / External, the capacities for Reserved - Used DP Pool and Reserved - Unused DP Pool are included in Reserved - Other.

#	Item	Description
5	Available Space - Unallocated	This item displays the volume capacity and the number of logical devices that are not defined paths. The Reserved - Used DP Pool, Reserved - Unused DP Pool, and Reserved - Other volumes are not included.
6	Available Space - Free Space	This item displays the free space where users can create volumes. The number of logical devices is not displayed.
7	Physical Total	This item displays the total capacity of physical logical devices and the number of logical devices.

Virtual Summary

#	Item	Description
1	DP Allocated[1]	When Total is selected in Internal / External, this item displays the virtual volume capacity of Dynamic Provisioning that is defined paths and the number of logical devices. Virtual volumes of Thin Image are not included.
2	DP Unallocated[1]	When Total is selected in Internal / External, this item displays the virtual volume capacity of Dynamic Provisioning that is not defined paths and the number of logical devices. Virtual volumes of Thin Image are not included.
3	Other[1]	When Total is selected in Internal / External, this item displays the virtual volumes except Dynamic Provisioning and the number of logical devices.
4	Virtual Total	This item displays the total capacity of virtual logical devices and the number of logical devices.
1. When an item other than Total is selected in Internal / External, the capacity and the number of logical devices are not displayed.		

Edit Storage System wizard

Edit Storage System window

This window lets you set storage system values. The configured values are required to use SNMP agents. Make sure to document the information, because the settings will be cleared when the SVP is replaced.

- Enter a device name using up to 180 alphanumeric characters (ASCII codes), except for some symbols, such as ", \, ;, :, ,, *, ?, <, >, |, /, ^, &, and %.

- You can also use a space, except for before and after the settings.

> ⚠ **Caution:** You can change more than one parameter, multiple times. But to do so, wait until the current task finishes.
> If you apply a setting (a new task) before the current task finishes, only the new task will be applied, so the result might be different from what you expected.

Setting fields

Item	Description
Storage System Name	Device name of the storage system.

Storage Navigator GUI reference (main windows)
Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
Contact	Contact information such as personnel and telephone number where you can inquire about the storage system.
Location	Location of the connected storage system.

Edit Storage System confirmation window

Edit Storage System table

Item	Description
Storage System Name	Device name of the storage system.
Contact	Contact information such as personnel and telephone number where you can inquire about the storage system.
Location	Location of the connected storage system.

Edit Information Display Settings window
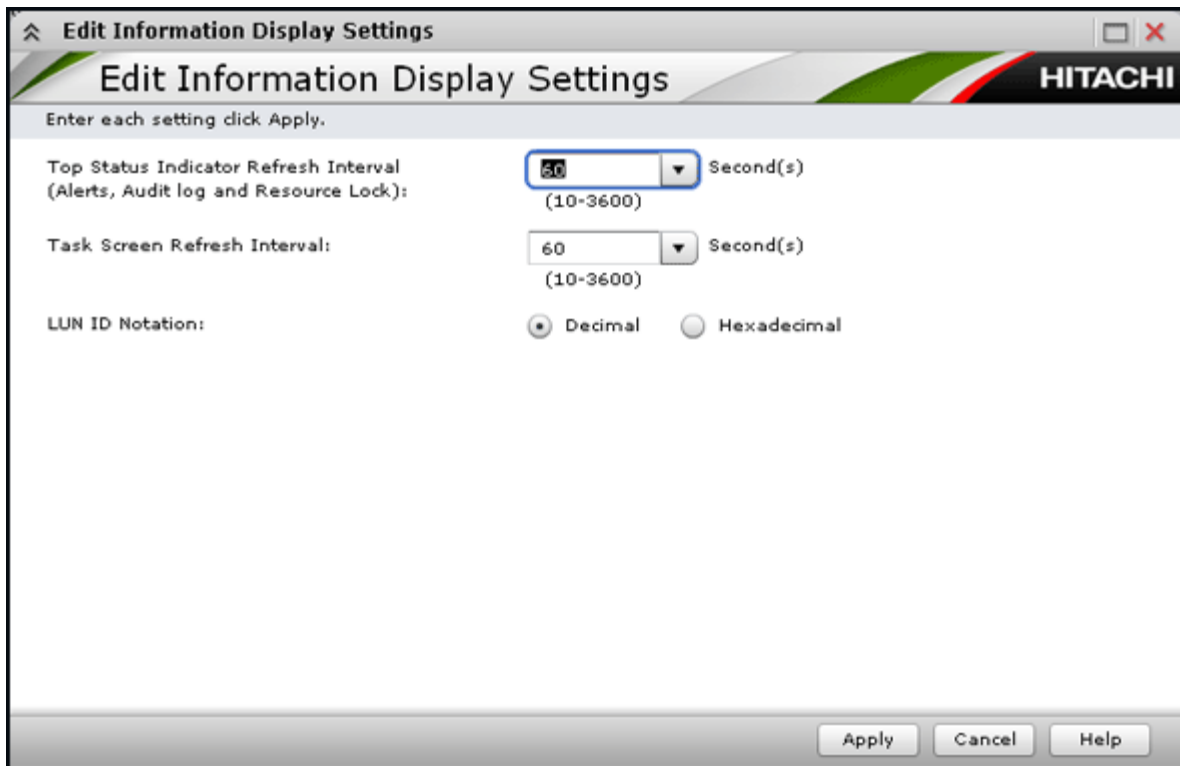
Use this wizard to change the displayed parameters.

Setting fields

Item	Description
Top Status Indicator Refresh Interval (Alerts, Audit log and Resource Lock)	Interval for the automatic updates of the icons on the upper-right corner of the Storage Navigator main window. You can specify 10–3600 seconds. The default value is 60 seconds.
Task Screen Refresh Interval	Interval for the automatic updates of the task window. You can specify 10–3600 seconds, or **No Update**. The default value is 60 seconds. **No Update** indicates the task window will be updated only when the user performs **Refresh View** or **Refresh All**.
LUN ID Notation	LUN ID notation. You can select decimal or hexadecimal format.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Resource Lock Properties window
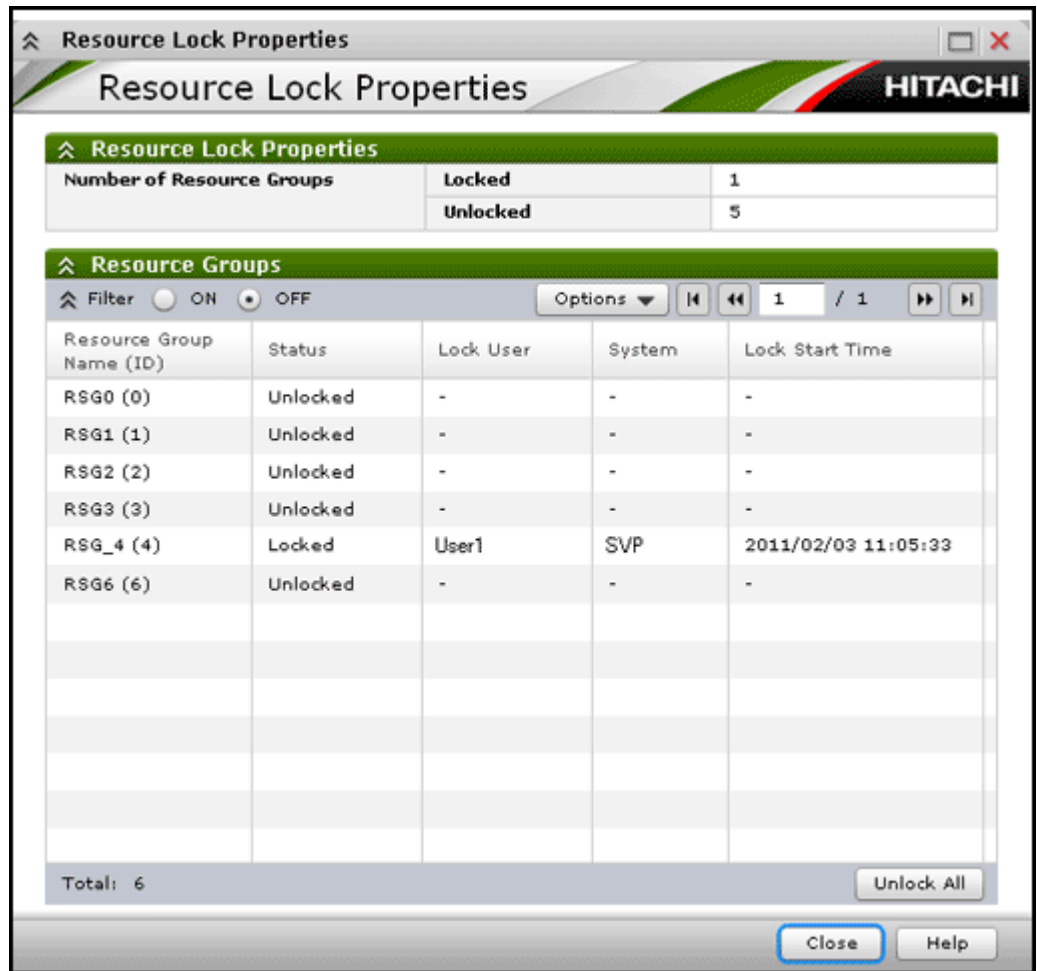
Displays information about the user who locks the storage system.

Resource Lock Properties table

Item	Description
Number of Resource Groups – Locked	Displays the number of locked resource groups.
Number of Resource Groups – Unlocked	Displays the number of unlocked resource groups.

Resource Groups table

Item	Description
Resource Group Name (ID)	Displays resource group name and resource group ID that user can operate.
Status	Displays lock status of resource groups. Locked: Locked user exists.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
	Unlocked: Locked user does not exist.
Lock User	Displays the user name who locks.
System	Displays the system that locked user is using.
Lock Start Time	Displays the time when the lock starts.
Unlock All	All locked resource groups are forcibly unlocked.

Tasks window

This window displays a list of tasks performed on the storage system. Up to 384 tasks can display, including 256 that are Completed and/or Failed. Up to 128 tasks whose statuses are In Progress, Waiting, and Suspended can also display.

Summary

Item	Description
Completed	Number of completed tasks.
In Progress	Number of tasks in progress.
Waiting	Number of tasks waiting.
Suspended	Number of suspended tasks.
Failed	Number of tasks in which an error occurred.

Tasks tab

Item	Description
Task Name	Task name specified by a user when the user performed the task. Click to view the detail of the task.
Status	Task status. Click to view more details about status or errors. • : Completed or Completed(Request): the task completed normally. • : In progress: the task is being processed by the system. • : Waiting: the task is not yet started. • : Suspended: the task has been suspended. • : Failed: the task ended abnormally.
Type	General name of the task.
User Name	User name who performed the task.
Submission Time	Date and time when the task was submitted.
Start Time	Date and time when the task was started. Blank indicates the task has not started yet.
End Time	Date and time when the task ended. Blank indicates the task has not ended yet.
Auto Delete	**Enabled**: A task is automatically deleted when the following two events occur: • The task is completed • The number of tasks in the Task list reaches the maximum number the window can display (384) **Disabled**: Tasks will remain displayed until users delete them. Tasks whose status is Failed are automatically Disabled by the system.
Suspend Tasks	Suspends the selected tasks. They will not be started even if the storage system is ready. Only waiting tasks can be suspended.
Resume Tasks	Resume the selected tasks. The status goes back to waiting.

Item	Description
Delete Tasks	Deletes the selected tasks from the window. • The waiting or suspended tasks will be cancelled. • The failed or aborted tasks can be deleted from the window. • Tasks in progress cannot be deleted.
Disable Auto Delete*	When disabled, the selected task remains in the task list after the task is completed.
Enable Auto Delete*	When enabled, the selected task is deleted from the Task list when the following two events occur: • The task is completed • The number of tasks in the Task list reaches the maximum number the window can display (384)
Export*	Displays the window for outputting table information.
*Appears when you click **More Actions**.	

Task Properties window

This window displays details about a task performed on the storage system.

Suspend Tasks window

Use this window to suspend waiting tasks.

Selected Tasks table

Item	Description
Task Name	Task name specified by a user when the user performed the task.
Status	Task status.
Type	General name of the task.
User Name	User name who performed the task.
Submission Time	Date and time when the task was submitted.

Storage Navigator GUI reference (main windows)

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Resume Tasks window
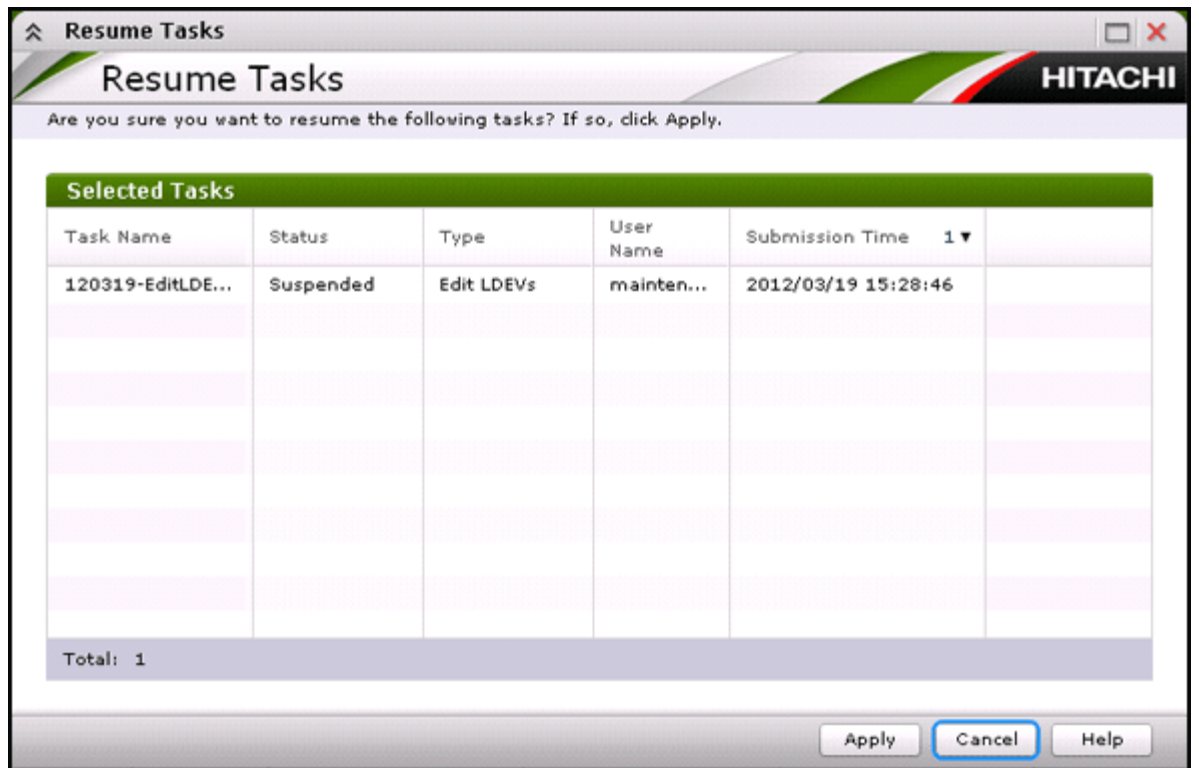
Use this window to resume suspended tasks.

Selected Tasks table

Item	Description
Task Name	Task name specified by a user when the user performed the task.
Status	Task status.
Type	General name of the task.
User Name	User name who performed the task.
Submission Time	Date and time when the task was submitted.

Delete Tasks window
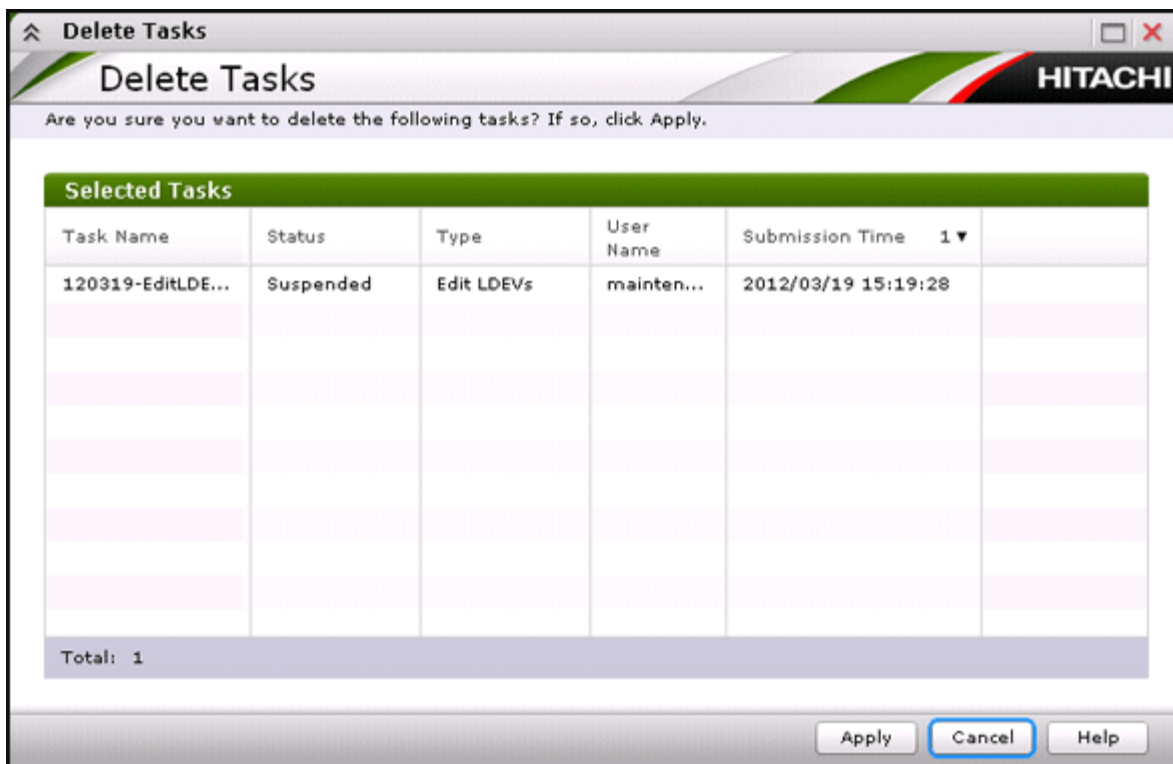
Use this window to delete tasks. If you delete a waiting task, the task will be cancelled.

Selected Tasks table

Item	Description
Task Name	Task name specified by a user when the user performed the task.
Status	Task status.
Type	General name of the task.
User Name	User name who performed the task.
Submission Time	Date and time when the task was submitted.

Storage Navigator GUI reference (main windows)

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Disable Auto Delete window
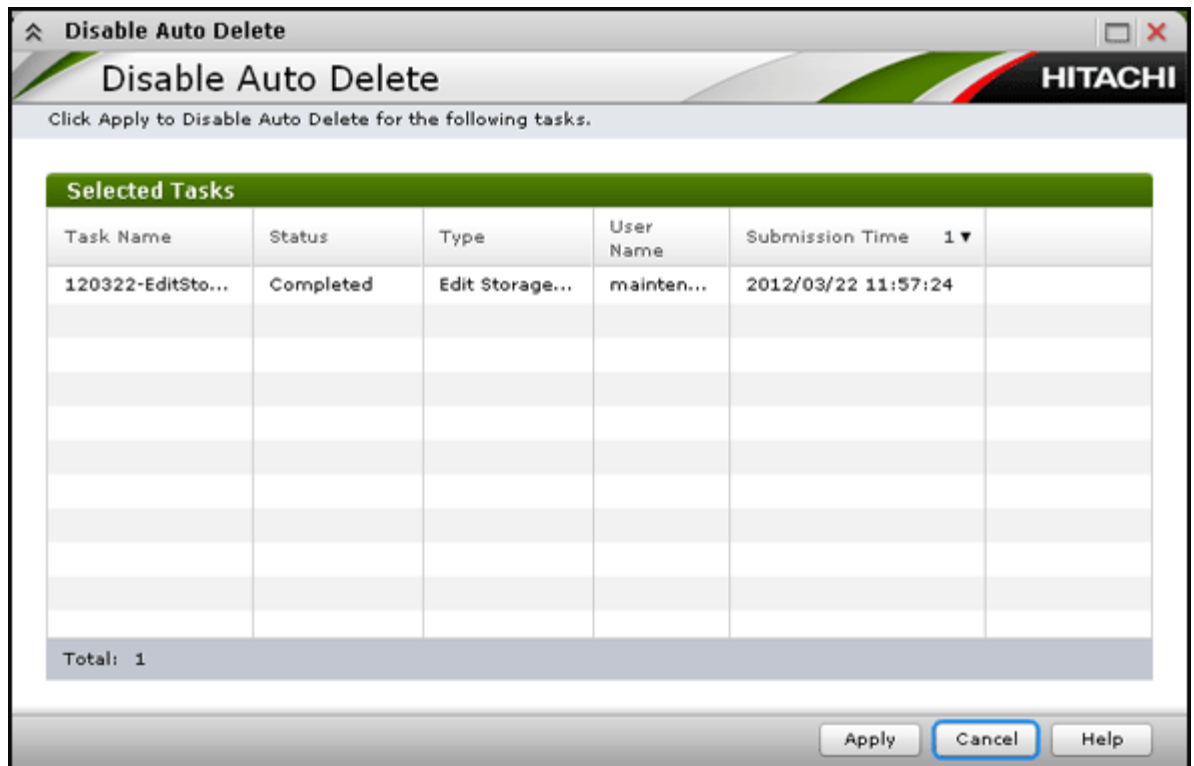
Use this window to prevent a task from being automatically deleted from the task window.

Selected Tasks table

Item	Description
Task Name	Task name specified by a user when the user performed the task.
Status	Task status.
Type	General name of the task.
User Name	User name who performed the task.
Submission Time	Date and time when the task was submitted.

Enable Auto Delete window
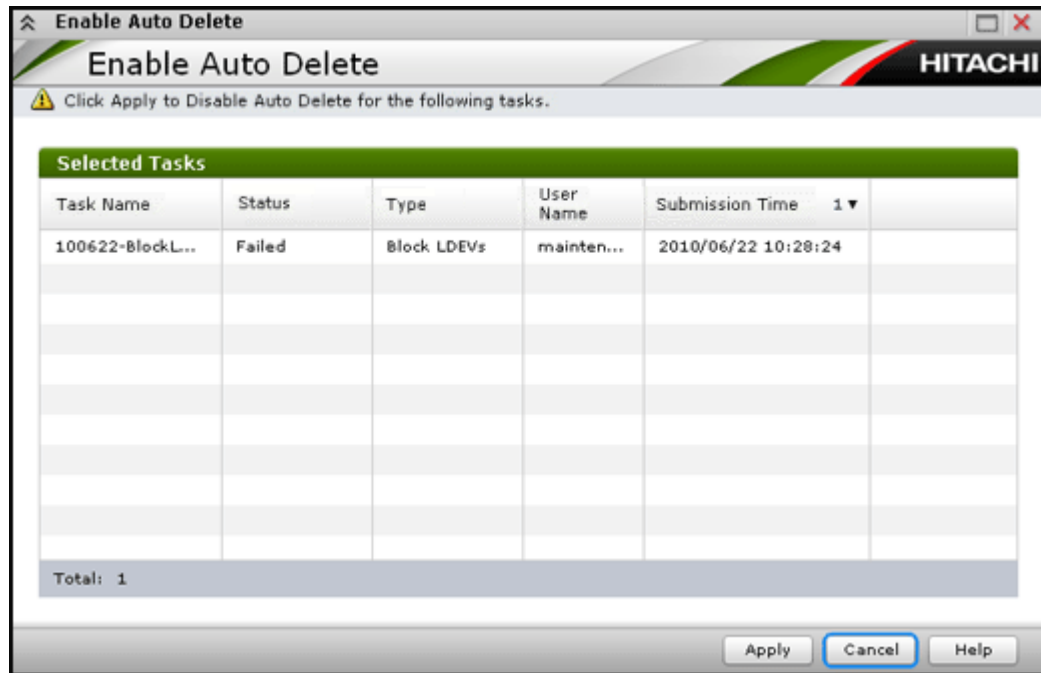
Use this window to automatically delete completed tasks from the task window when the number of displayed tasks reaches the maximum (384 tasks).

Selected Tasks table

Item	Description
Task Name	Task name specified by a user when the user performed the task.
Status	Task status.
Type	General name of the task.
User Name	User name who performed the task.
Submission Time	Date and time when the task was submitted.

Reports window
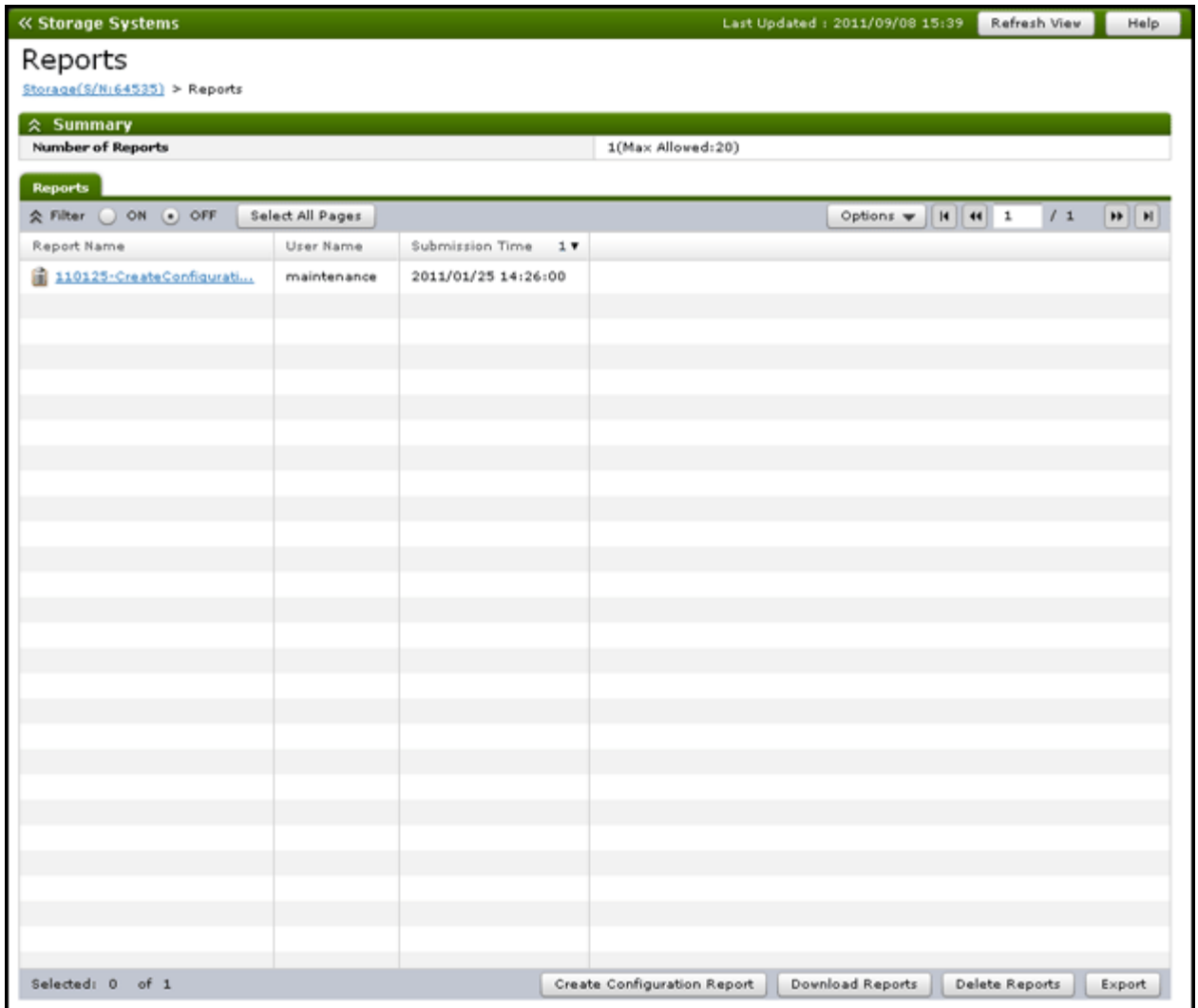
This window lists configuration reports about the storage system.

You can create up to 20 reports.

Summary

Item	Description
Number of Reports	Number of created reports.

Reports tab

Item	Description
Report Name	Task name specified when users created a report. Click to view the report in HTML format.
User Name	User name who created the report.

Item	Description
Submission Time	Date and time when the report was created.
Create Configuration Report	Creates a new report.
Download Reports	Downloads the created report in both HTML and CSV format.
Delete Reports	Deletes the selected report.
Export	Displays the window for outputting table information.

Create Configuration Report window
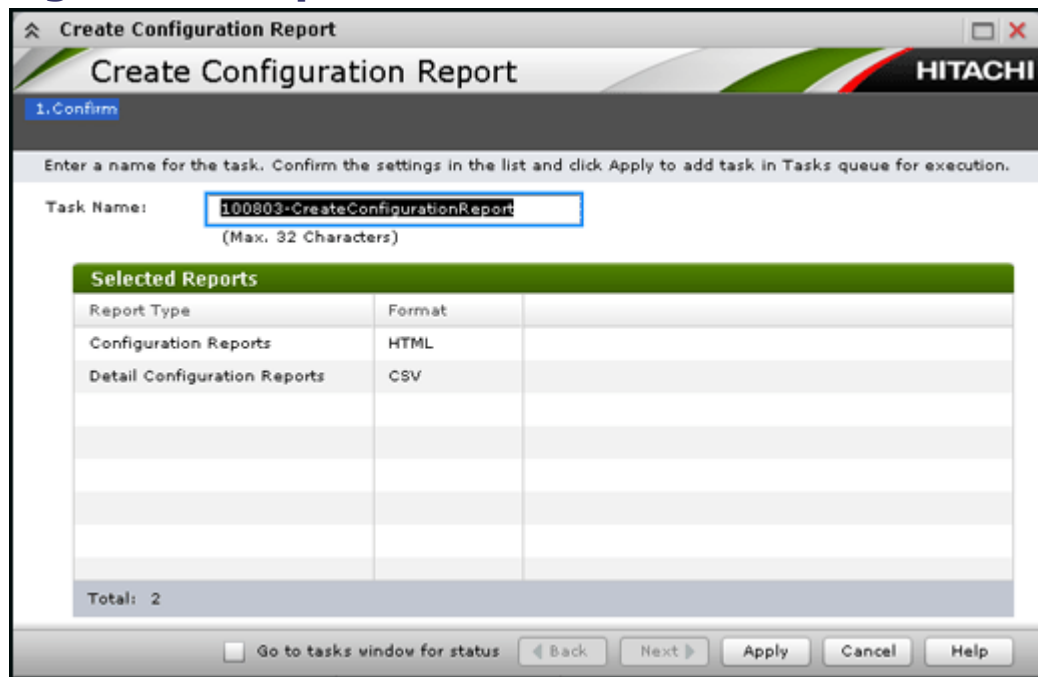
Use this window to create storage system configuration reports.

Selected Reports table

Item	Description
Report Type	Type of the report to be created.
Format	File format.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Delete Reports window
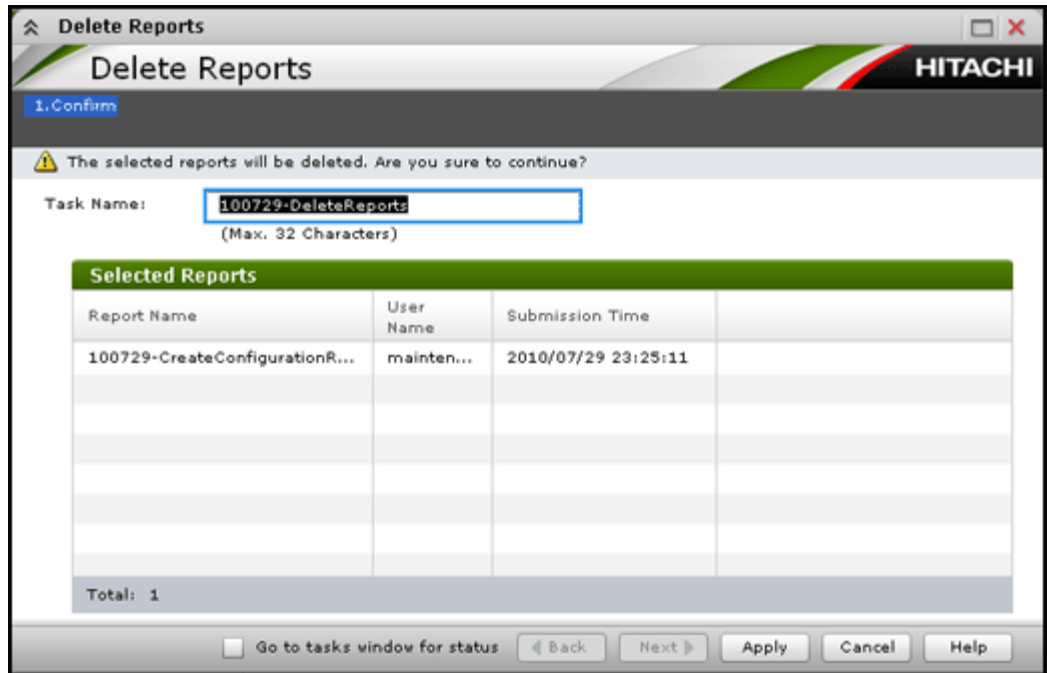
Use this window to delete configuration reports.

Selected Reports table

Item	Description
Report Name	Task name specified when users created a report.
User Name	User name who created the report.
Submission Time	Date and time when the report was created

User Groups window

This window lists all user groups created in Storage Navigator.

Summary

Item	Description
Number of User Groups	Number of user groups created in Storage Navigator.

User Groups tab

Item	Description
User Group Name	Displays user group name.
User Group Type	Displays the user group type. Built-in: Indicates a built-in user group. User-created: Indicates a user group that users created.
Number of Roles	Displays the number of the roles that are assigned to the user group.
Number of Resource Groups	Displays the number of the resource groups that are assigned to the user group.
Number of Users	Displays the number of users who belong to the user group.
All Resource Groups Assigned	Displays whether all the resource groups are assigned. Yes: All the resource groups are assigned to the user group. No: All the resource groups are not assigned to the user group.
Create User Group	Creates a new user group.
Add Users	Adds the created users to the selected user group.
Edit Resource Group Assignment	Assigns the created resource groups to the selected user groups.
Edit Role Assignment*	Assigns the created roles to the selected user groups.
Delete User Groups*	Deletes the selected user groups.
Edit User Group*	Edits the user group name.
Export*	Displays the window for outputting table information.
* Appears when you click **More Actions**.	

Window when User Group is selected

- [Summary on page D-35](#)
- [Users tab on page D-35](#)
- [Roles tab on page D-36](#)
- [Resource Groups tab on page D-37](#)

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Summary

Item	Description
Number of Roles	Displays the number of roles that are assigned to the selected user group.
Number of Resource Groups	Displays the number of resource groups that are assigned to the selected user group.
Number of Users	Displays the number of users who belong to the selected user group.
User Group Type	Displays the user group type. Built-in: Indicates a built-in user group. User-created: Indicates a user group that a user created.
All Resource Groups Assigned	Displays whether all the resource groups are assigned. Yes: All the resource groups are assigned to the user group. No: All the resource groups are not assigned to the user group.

Users tab

Lists all users who belong to the selected user group.

Item	Description
User Name	Name of user who belongs to the user group
Account Status	Displays the account status. Enabled: The user can use the account. Disabled: The user cannot use the account or log in to Storage Navigator or the Command Control Interface.
Lockout[1]	Displays the lockout status. • Yes: The user account is locked. The user cannot log in to Storage Navigator or the Command Control Interface. • No: The user account is not locked. The user can log in to Storage Navigatoror the Command Control Interface.
Authentication	Authentication method. The following methods are available: Local: Does not use authentication server. Uses a dedicated password for Storage Navigator. External: Uses the authentication server.
User Type	User type. The following types are available: Built-in or User-created
Number of User Groups	Displays the number of the user groups where the user belongs
Create User	Creates a new user account
Change Password	Changes your own password if you click this. Changes the password of other users if you select a user and then click this

Item	Description
Edit User	Changes the setting for authentication or for the account status. You can set the password of the selected user if you change Authentication from External to Local.
Add Users[2]	Adds the created users to the selected user group
Remove Users[2]	Removes the selected user from the user group. The user account itself will not be deleted.
Delete Users[2]	Deletes the selected users
Export[2]	Displays the window for outputting table information
Notes:	
1. This content is not displayed as default. To display this content, change the settings in the Column Settings window.	
2. Appears when you click More Actions	

Roles tab
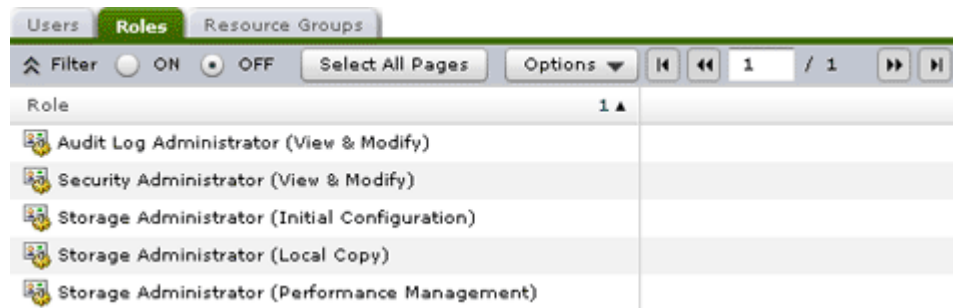
Roles displays the roles assigned to the user group, which determines the operations the user can perform.

Role	Permitted operations
Role	Displays the roles that are assigned to the user group.
Edit Role Assignment	Assigns the created roles to the selected user groups.
Export	Displays the window for outputting table information.

Resource Groups tab

Lists the resource groups that are assigned to the selected user group.

Item	Description
Resource Group Name (ID)	Displays the name and ID of the resource group assigned to the user group.
Number of User Groups	Displays the number of user groups that are assigned to the resource group.
Number of Parity Groups	Displays the number of the parity groups that are assigned to the resource group.
Number of LDEVs	Displays the number of the LDEVs that are assigned to the resource group.
Number of Ports	Displays the number of the ports that are assigned to the resource group.
Number of Host Groups	Displays the number of the host groups that are assigned to the resource group.
Edit Resource Group Assignment	Assigns the created resource groups to the user groups.
Export	Displays the window for outputting table information.

Create User wizard

Create User window

Use this window to create a new user account.

Setting fields

Item	Description
User Name	Enter the user name to be created. The allowable characters and length of user names depend on the application that the user uses. See Creating user accounts on page 4-13.
Account Status	Account statuses. The following statuses are available: Enable: The user can use the account. Disable: The user cannot use the account or log in to Storage Navigator.
Authentication	Authentication method. The following methods are available: Local: Does not use authentication server. Uses a dedicated password for Storage Navigator. External: Uses authentication server.
Password	Password that the user enters for login. The allowable characters and length of passwords depend on the application that the user uses. See Creating user accounts on page 4-13.
Re-enter Password	Password as above.

Create User confirmation window
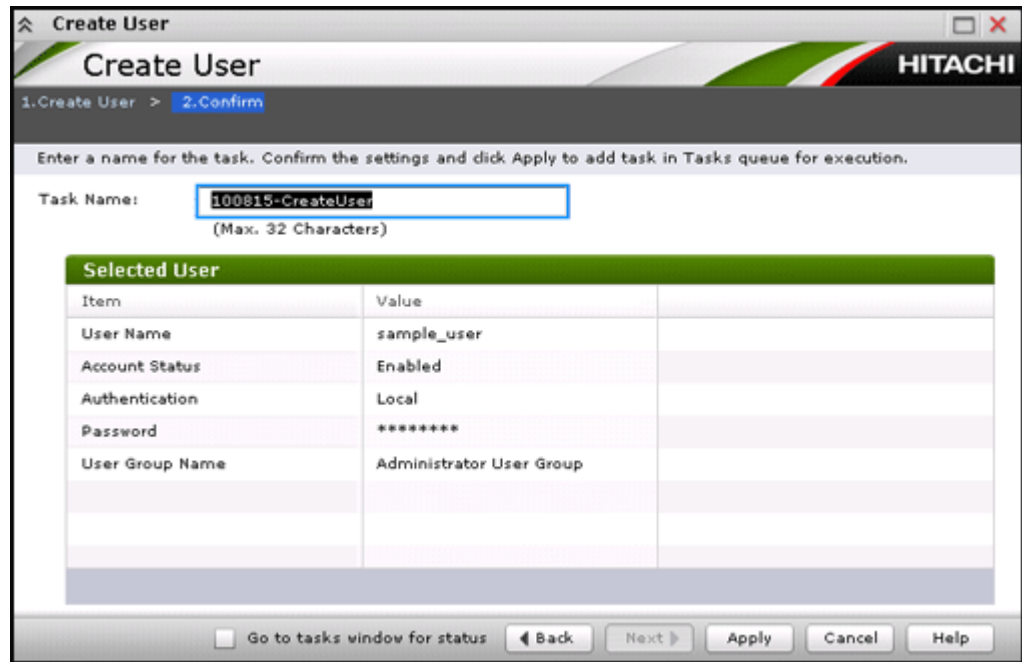
Selected User table

Item	Description
User Name	User name to be created.
Account Status	Account statuses. The following statuses are available:
	Enabled: The user can use the account.
	Disabled: The user cannot use the account or log in to Storage Navigator.
Authentication	Authentication methods. The following methods are available:
	Local: Does not use authentication server. Uses a dedicated password for Storage Navigator.
	External: Uses authentication server.
Password	Password that the user enters for login.
User Group Name	User group name where the user is added.

Change Password wizard

Change Password window

Use this wizard to change the password for yourself or another user.

Setting fields

Item	Description
User Name	Selected user name.
Current Password	Current password of your user account. Required only when you change your own password.
New Password	New password that the selected user enters for login. The allowable characters and length of passwords depend on the application that the user uses. See Creating user accounts on page 4-13.
Re-enter New Password	Same password as above.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Change Password confirmation window

Selected User table

Item	Description
User Name	Selected user name
Current Password	Current password A hyphen (-) indicates no current password is specified.
New Password	New password

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Edit User wizard

Edit User window
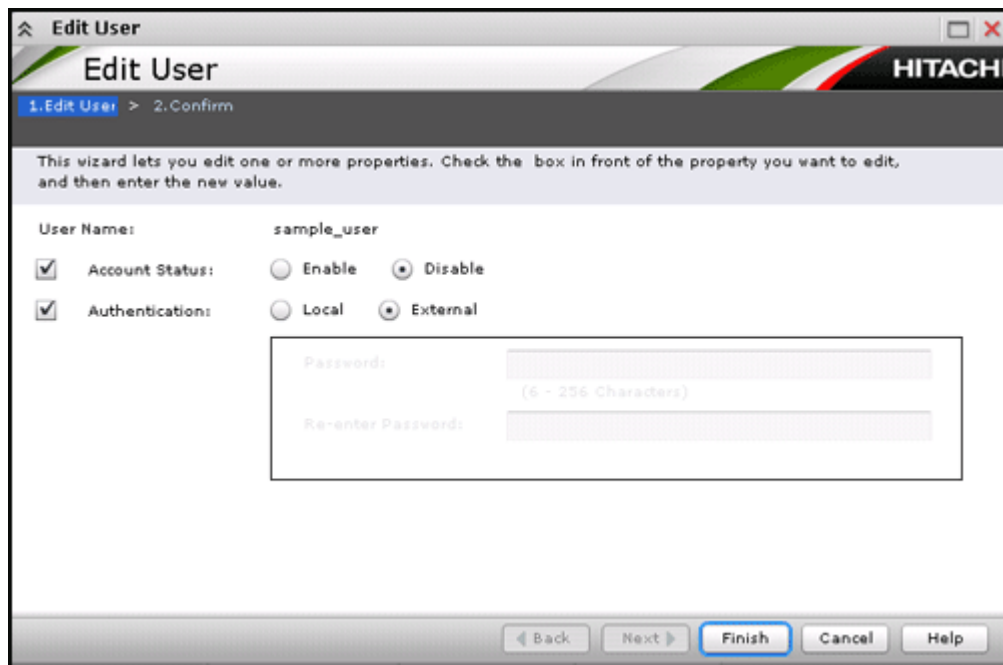
Use this wizard to change the setting for authentication or for the account status.

Setting fields

Item	Description
User Name	Selected user name
Account Status	Account statuses. The following statuses are available: Enable: The user can use the account. Disable: The user cannot use the account or log in to Storage Navigator.
Authentication	Authentication method. The following methods are available: Local: Does not use authentication server. Uses a dedicated password for Storage Navigator. External: Uses authentication server.
Password	Password that the user enters for login. The allowable characters and length of passwords depend on the application that the user uses. See Creating user accounts on page 4-13.
Re-enter Password	Same password as above.

Edit User confirmation window

Selected User table

Item	Description
User Name	Selected user name.
Account Status	Account status. The following statuses are available: Enabled: The user can use the account. Disabled: The user cannot use the account or log in to Storage Navigator.
Authentication	Authentication method. The following methods are available: Local: Does not use authentication server. Uses a dedicated password for Storage Navigator. External: Uses authentication server.
Password	Password that the user enters for login.

Add Users wizard

Add Users window
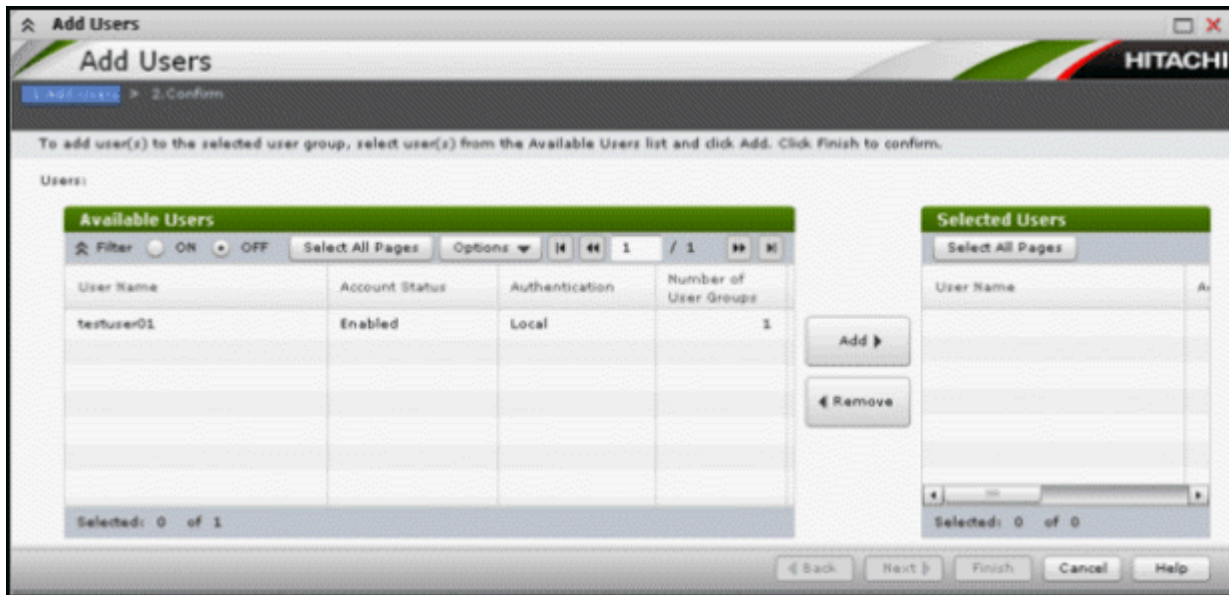
Use this wizard to add the created user accounts to the selected user group.

Available Users table

Lists all the candidate users who do not belong to the selected user group.

Item	Description
User Name	Selected user name
Account Status	Account status. The following statuses are available: Enabled: The user can use the account. Disabled: The user cannot use the account or log in to Storage Navigator.
Authentication	Authentication method. The following methods are available:

Item	Description
	Local: Does not use authentication server. Uses a dedicated password for Storage Navigator.
	External: Uses authentication server.
Number of User Groups	Displays the number of the user groups where the user belongs.

Add button

Adds the selected users in the Available Users list to the Selected Users list.

Remove button

Removes the selected users from the Selected Users list and relocates the selected users to the Available User list.

Selected Users table

Lists users to be added to the user group.

Item	Description
User Name	Selected user name.
Account Status	Account status. The following statuses are available:
	Enabled: The user can use the account.
	Disabled: The user cannot use the account or log in to Storage Navigator.
Authentication	Authentication method. The following methods are available:
	Local: Does not use authentication server. Uses a dedicated password for Storage Navigator.
	External: Uses authentication server.
Number of User Groups	Displays the number of the user groups where the user belongs.

Add Users confirmation window

Selected User Group table

Item	Description
User Group Name	Displays the user group name where the user is added.

Selected Users table

Item	Description
User Name	Selected user name.
Account Status	Account status. The following statuses are available: Enabled: The user can use the account. Disabled: The user cannot use the account or log in to Storage Navigator.
Authentication	Authentication method. The following methods are available: Local: Does not use authentication server. Uses a dedicated password for Storage Navigator. External: Uses authentication server.
Number of User Groups	Displays the number of the user groups where the user belongs.

Remove Users window

Selected User Group table

Item	Description
User Group Name	Displays the name of the user group where the user is removed.

Selected Users table

Item	Description
User Name	Selected user name.
Account Status	Account status. the following statuses are available: Enabled: The user can use the account. Disabled: The user cannot use the account or log in to Storage Navigator.
Authentication	Authentication method. The following methods are available: Local: Does not use authentication server. Uses a dedicated password for Storage Navigator. External: Uses authentication server.
Number of User Groups	Number of user group from which user is removed.

Delete Users window

Selected Users table

Item	Description
User Name	Selected user name.
Account Status	Account status. the following statuses are available: Enabled: The user can use the account. Disabled: The user cannot use the account or log in to Storage Navigator.
Authentication	Authentication method. The following methods are available: Local: Does not use authentication server. Uses a dedicated password for Storage Navigator. External: Uses authentication server.
Number of User Groups	Displays the number of the user groups where the user belongs.

Create User Group wizard

Create User Group window

Use this window to create a new user group.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide
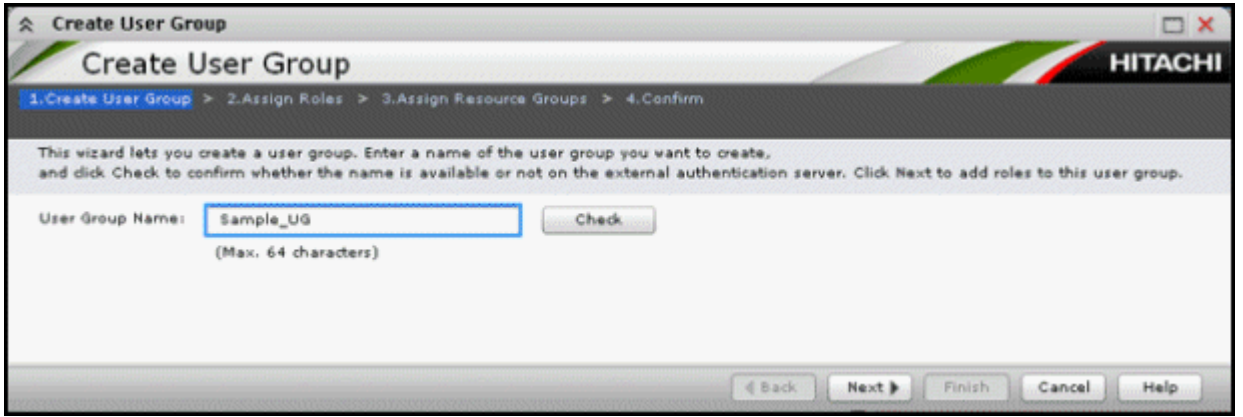
Setting fields

Item	Description
User Group Name	Enter the name of the user group to be created. You can specify ASCII code characters, spaces, and the following symbols: ! # $ % & ' ( ) + - . = @ [ ] ^ _ ` { } ~
Check	Check whether the entered user group name is registered to the authorization server when you use an authorization server.

Create User Group confirmation window

Create User Group table

Item	Description
User Group Name	Displays the name of user groups to be created.

Storage Navigator GUI reference (main windows)

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
Number of Roles	Displays the number of roles that are assigned to the user group to be created.
Number of Resource Groups	Displays the number of resource groups that are assigned to the user group to be created.
Number of Users	Displays the number of users that belong to the user group to be created.
All Resource Groups Assigned	Displays whether all resource groups are assigned. Yes: All resource groups are assigned to the user group. No: All resource groups are not assigned to the user group.

Assigned Roles table

Item	Description
Role	Displays the roles that are assigned the user group to be created.

Assigned Resource Groups table

Item	Description
Resource Group Name (ID)	Displays the name and ID of the resource group assigned to the user group to be created.
Number of User Groups	Displays the number of user groups that are assigned to the resource group.
Number of Parity Groups	Displays the number of parity groups that are assigned to the resource group.
Number of LDEVs	Displays the number of LDEVs that are assigned to the resource group.
Number of Ports	Displays the number of ports that are assigned to the resource group.
Number of Host Groups	Displays the number of host groups that are assigned to the resource group.
Detail	Displays details of the selected resource group.

Selected Users table

This table displays only when users are added to the user group.

Item	Description
User Name	Displays the name of the users that belong to the user group to be created.
Account Status	Displays the account status. The following status are available: Enabled: The user can use the account.

Item	Description
	Disabled: The user cannot use the account or log in to Storage Navigator.
Authentication	Displays the authentication method. The following methods are available:
	Local: Does not use authentication server. Uses a dedicated password for Storage Navigator.
	External: Uses authentication server.
Number of User Groups	Displays the number of user groups where the user belongs.

Edit User Group wizard

Edit User Group window

Use this window to change the name of a user group.

Setting fields

Item	Description
User Group Name	Enter the new name of the user group.
	You can use ASCII code characters, spaces, and the following symbols:

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
	! # $ % & ' ( ) + - . = @ [ ] ^ _ ` { } ~
Check	Check whether the entered user group name is registered to the authorization server when you use an authorization server.

Edit User Group confirmation window

Selected User Group table

Item	Description
User Group Name	Displays the new name of the user group.
Number of Roles	Displays the number of roles that are assigned to the user group.
Number of Resource Groups	Displays the number of resource groups that are assigned to the user group.
Number of Users	Displays the number of users that belong to the user group.
All Resource Groups Assigned	Displays whether all the resource groups are assigned. Yes: All resource groups are assigned to the user group. No: All resource groups are not assigned to the user group.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Delete User Groups window

Selected User Groups table

Item	Description
User Group Name	Displays the new name of the user group.
Number of Roles	Displays the number of roles that are assigned to the user group.
Number of Resource Groups	Displays the number of resource groups that are assigned to the user group.
Number of Users	Displays the number of users that belong to the user group.
All Resource Groups Assigned	Displays whether all resource groups are assigned. Yes: All resource groups are assigned to the user group. No: All resource groups are not assigned to the user group.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Release Lockout window

Use this window to release the lockout status of a user account.

Selected Users

Select the user whose lockout status you want to change.

Item	Description
User Name	Displays the name of the user whose account you want to unlock.

Edit Resource Group Assignment wizard

Edit Resource Group Assignment window
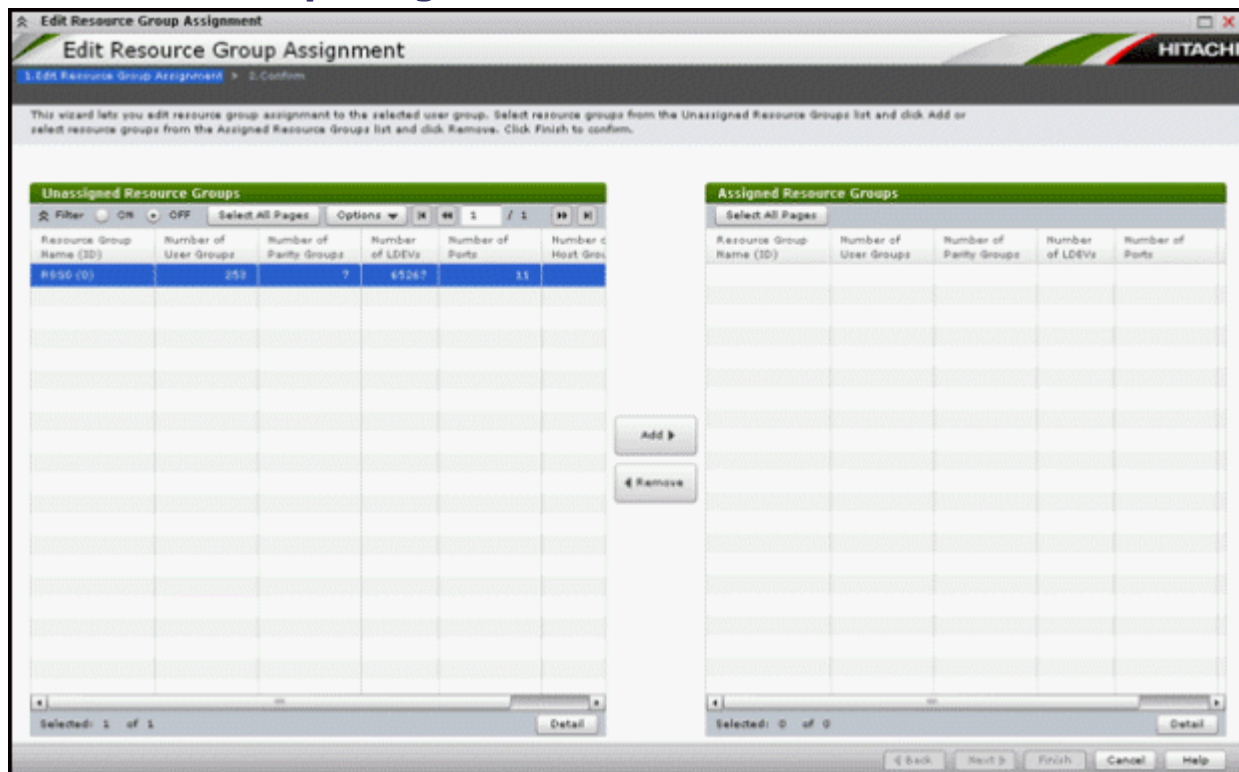
Use this window to assign created resource groups to the user group and to assign created resource groups to the user group in the Create User Group wizard.

Setting fields

These fields display only when resource groups are assigned in the Create User Group wizard.

Item	Description
All Resource Groups Assigned	Displays whether all the resource groups are assigned to the user group.
	This item is set to Yes when the following roles are assigned in the Assign Roles window.
	• Security Administrator (View Only)
	• Security Administrator (View & Modify)
	• Audit Log Administrator (View Only)
	• Audit Log Administrator (View & Modify)
	• Support Personnel
	• User Maintenance

Item	Description
	When this item is set to Yes, Unassigned Resource Groups table, Assigned Resource Groups table, Add button, and Remove button are disabled.

Unassigned Resource Groups table

Lists the resource groups that are not assigned to the user group.

Item	Description
Resource Group Name (ID)	Displays the name and ID of the resource group assigned to the user group to be created.
Number of User Groups	Displays the number of user groups that are assigned to the resource group.
Number of Parity Groups	Displays the number of parity groups that are assigned to the resource group.
Number of LDEVs	Displays the number of LDEVs that are assigned to the resource group.
Number of Ports	Displays the number of ports that are assigned to the resource group.

Item	Description
Number of Host Groups	Displays the number of host groups that are assigned to the resource group.
Detail	Displays the detail of the selected resource group.

Add button

Adds the selected resource groups in the Unassigned Resource Groups list to the Assigned Resource Groups list.

Remove button

Removes the selected resource groups from the Assigned Resource Groups list and relocates the resource groups to the Unassigned Resource Groups list.

Assigned Resource Groups table

Lists the resource groups to be assigned to the user group.

Item	Description
Resource Group Name (ID)	Displays the name and ID of the resource group assigned to the user group to be created.
Number of User Groups	Displays the number of user groups that are assigned to the resource group.
Number of Parity Groups	Displays the number of parity groups that are assigned to the resource group.
Number of LDEVs	Displays the number of LDEVs that are assigned to the resource group.
Number of Ports	Displays the number of ports that are assigned to the resource group.
Number of Host Groups	Displays the number of host groups that are assigned to the resource group.
Detail	Displays the detail of the selected resource group.

Edit Resource Group Assignment confirmation window

Selected User Group table

Item	Description
User Group Name	Displays the new name of the user group.

Assigned Resource Groups table

Item	Description
Resource Group Name (ID)	Displays the name and ID of the resource group assigned to the user group to be created.
Number of User Groups	Displays the number of user groups that are assigned to the resource group.
Number of Parity Groups	Displays the number of parity groups that are assigned to the resource group.
Number of LDEVs	Displays the number of LDEVs that are assigned to the resource group.
Number of Ports	Displays the number of ports that are assigned to the resource group.
Number of Host Groups	Displays the number of host groups that are assigned to the resource group.
Detail	Displays the detail of the selected resource group.

Edit Role Assignment wizard

Edit Role Assignment window

Use this window to add roles to the user group and to assign roles to the user group in the Create User Group wizard.

Unassigned Roles table
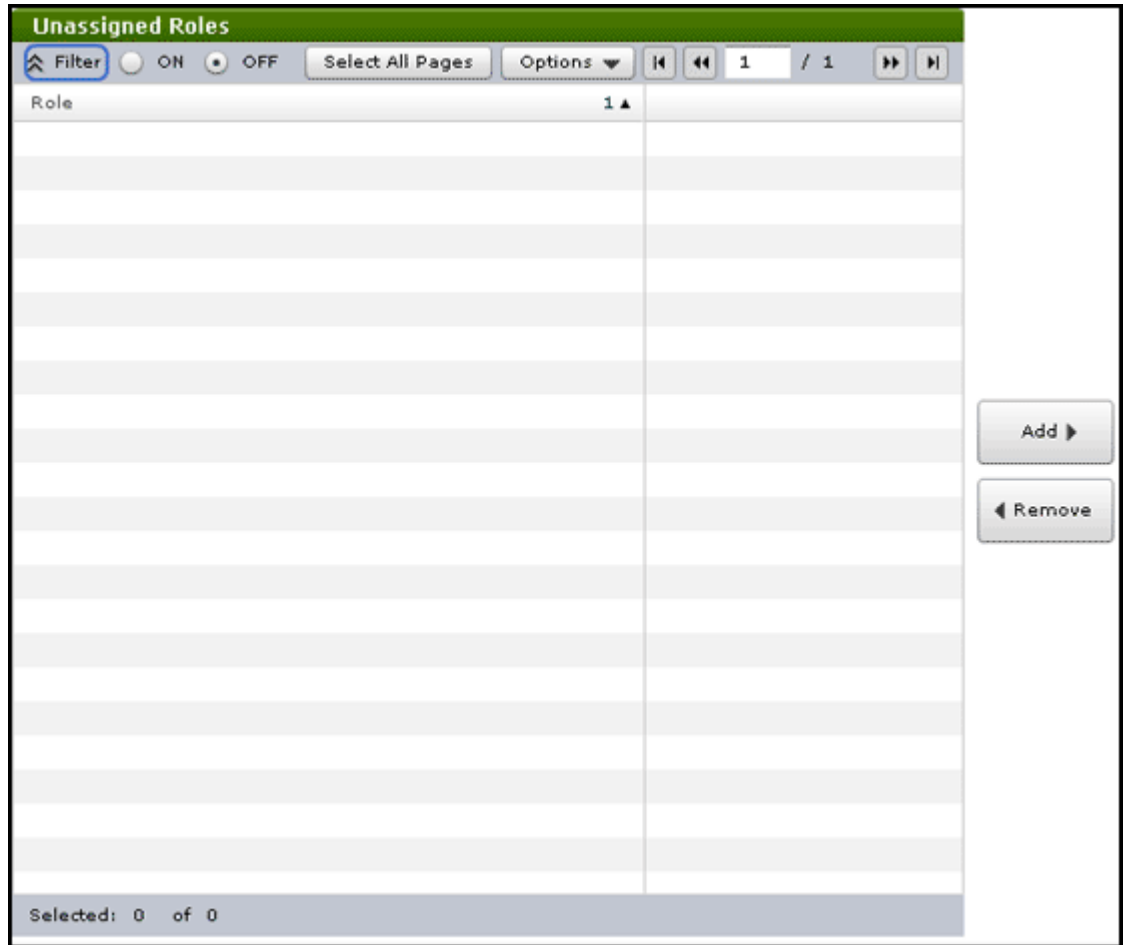
Lists roles that are not assigned to the user group.

Item	Description
Role	Displays roles.

Add button

Adds the selected roles in the Unassigned Roles list to the Assigned Roles list.

Remove button

Removes the selected roles from the Assigned Roles list and relocates the selected roles to the Unassigned Roles list.

Assigned Roles table

Lists roles to be assigned to the user group.

Item	Description
Role	Displays roles.

Edit Role Assignment confirmation window

Selected User Group table

Item	Description
User Group Name	Displays the new name of the user group.
All Resource Groups Assigned	Displays whether all the resource groups are assigned. Yes: All the resource groups are assigned to the user group. No: All the resource groups are not assigned to the user group.

Assigned Roles

Item	Description
Role	Displays the roles that are assigned to the user group.

Alerts window

Displays the list of alerts (SIM) that occurred in storage system.

Summary

Item	Description
Number of Uncompleted Alerts	Displays the number of alerts that are not authenticated yet. • Acute: Displays total number of Acute level alerts that are not authenticated yet. • Serious: Displays total number of Serious level alerts that are not authenticated yet. • Moderate: Displays total number of Moderate level alerts that are not authenticated yet. • Service: Displays total number of Service level alerts that are not authenticated yet. • Total: Total number of above is displayed.

Alerts table

Item	Description
Error Code	Displays reference code of SIM. For details about reference code, contact the Hitachi Data Systems customer support. About errors that need to be solved, see Checking alerts on page 8-3.
Date	Displays the date when alerts occurred.
Error Level	Displays error level of alerts. • *Service:* No need to deal with immediately. Errors that are dealt with within periodical maintenance. • *Moderate:* No need to deal with immediately. Errors that are dealt with within periodical maintenance. • *Serious:* Contact the Hitachi Data Systems customer support. Take adequate measure as instructed, report and solve the problem. • *Acute:* Contact the Hitachi Data Systems customer support. Take adequate measure as instructed, report and solve the problem.
Status	If status alert remains, Uncompleted is displayed. If alert is removed by SVP, Completed is displayed.
Detail	Displays the details of alert that is selected in the list.

Alert Properties window

Displays details of alert (SIM) that occurred in storage system.

When you select multiple alerts in **Alert** window, click **back** and **Next** button to change alert that is displayed.

Alert Properties table

Item	Description
Error Code	Displays reference codes of SIM. For details about reference codes, contact the Hitachi Data Systems customer support. About errors that need to be solved, see Checking alerts on page 8-3.
Date	Displays the date when alerts occurred.
Error Level	Displays error level of alerts.

Item	Description
	• ![Service icon] *Service:* No need to deal with immediately. Errors that are dealt with within periodical maintenance. • ![Moderate icon] *Moderate:* No need to deal with immediately. Errors that are dealt with within periodical maintenance. • ![Serious icon] *Serious:* Contact the Hitachi Data Systems customer support. Take adequate measure as instructed, report and solve the problem. • ![Acute icon] *Acute:* Contact the Hitachi Data Systems customer support. Take adequate measure as instructed, report and solve the problem.
Status	If status alert remains, Uncompleted is displayed. If alert is removed by SVP, Completed is displayed.
Error Section	Displays overview of the error where the alert occurred.
Error Detail	Displays more detail on the error.
Location	Displays where the error occurred. It differs according to the error code.

LDAP Properties window

This window displays when you select **Disable** or **LDAP** in External Authentication.

LDAP Properties table

Item	Description
DNS Lookup	Displays whether to search for the LDAP server using the information registered in the SRV records in the DNS server. • Enable: Performs the search using information registered in the SRV records in the DNS server. • Disable: Performs the search using the host name and the port number.
Authentication Protocol	Displays the LDAP protocol to use.
External User Group Mapping	Displays whether to connect an authentication server to an authorization server.

Item	Description
	• Enable: Connects an authentication server to an authorization server. • Disable: Does not connect an authentication server to an authorization server.
Primary Host Name	Displays the host name of the LDAP server.
Primary Port Number	Displays the port number of the LDAP server.
Domain Name	Displays the domain name that the LDAP server manages.
User Name Attribute	Displays the attribute name to identify a user, such as a user ID.
Base DN	Displays the Base DN for searching for users to authenticate.
Search User's DN	Displays the DN of the user for searching.
Password	Displays asterisks (*) to mask the password of the user for searching.
Timeout	Displays the number of seconds before connection to the LDAP server times out.
Retry Interval	Displays the retry interval in seconds when the connection to the LDAP server fails.
Number of Retries	Displays the retry times when the connection to the LDAP server fails.
Secondary Host Name	Displays the host name of the secondary LDAP server.
Secondary Port Number	Displays the port number of the secondary LDAP server.
Setup Server	Displays the Setup Server window.

RADIUS Properties
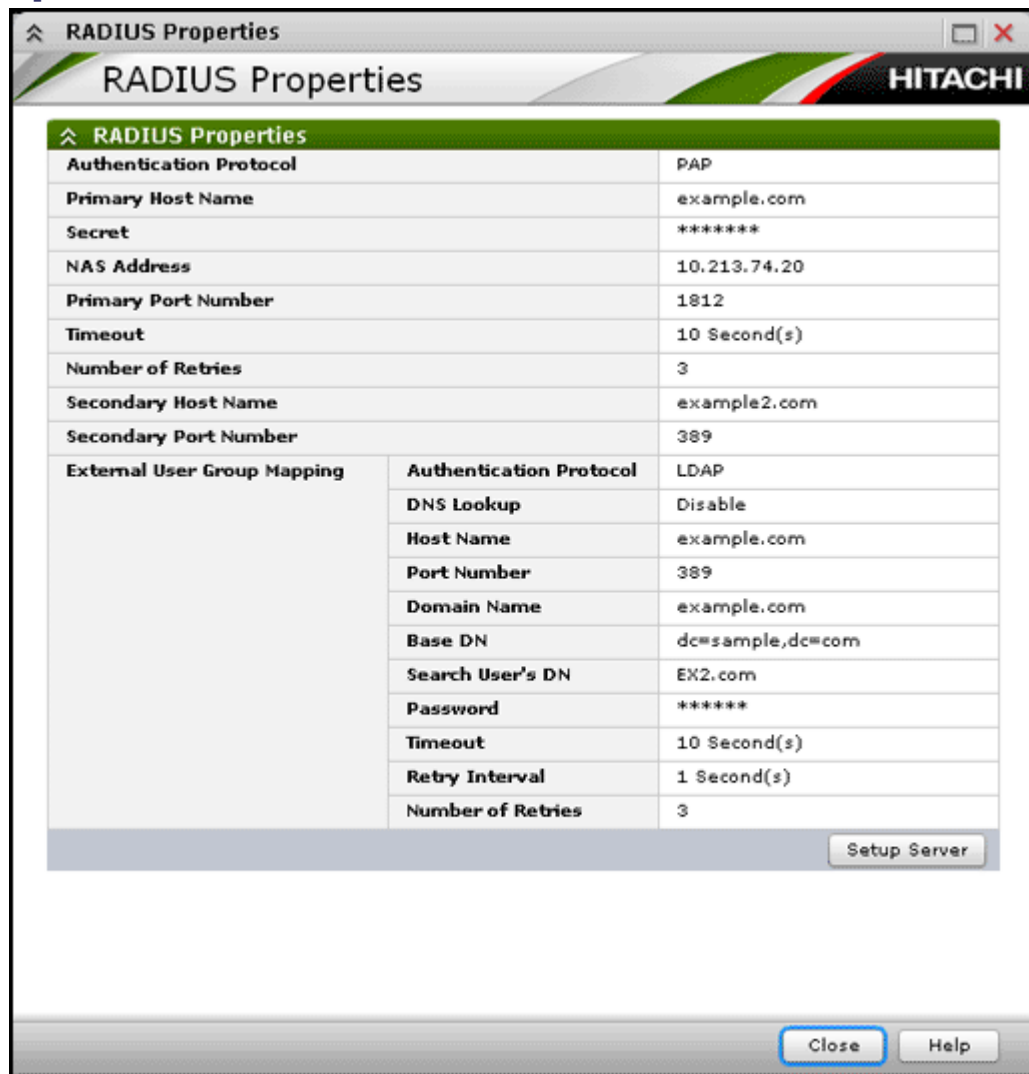
This window displays when you select **RADIUS** in External Authentication.

RADIUS Properties table

Item	Description
Authentication Protocol	Displays the RADIUS protocol to use. • PAP: Password authentication protocol that transmits plaintext user ID and password. • CHAP: Challenge-handshake authentication protocol that transmits encrypted password.
Primary Host Name	Displays the host name, the IPv4 address, or the IPv6 address of the RADIUS server.
Secret	Displays asterisks (*) to mask the RADIUS secret key used for the PAP or CHAP authentication.
NAS Address	Displays the identifier for the RADIUS server to find SVP.

Storage Navigator GUI reference (main windows)

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
Primary Port Number	Displays the port number of the RADIUS server.
Timeout	Displays the number of seconds before connection to the RADIUS server times out.
Number of Retries	Displays the retry times when the connection to the RADIUS server fails.
Secondary Host Name	Displays the host name, the IPv4 address, or the IPv6 address of the secondary RADIUS server.
Secondary Port Number	Displays the port number of the secondary RADIUS server.
External User Group Mapping - Authentication Protocol	Displays the LDAP protocol to use.
External User Group Mapping - DNS Lookup	Displays whether to search for the LDAP server using the information registered in the SRV records in the DNS server. • Enable: Performs the search using information registered in the SRV records in the DNS server. • Disable: Performs the search using the host name and the port number.
External User Group Mapping - Host Name	Displays the host name, the IPv4 address, or the IPv6 address of the LDAP server.
External User Group Mapping - Port Number	Displays the port number of the LDAP server.
External User Group Mapping - Domain Name	Displays the domain name of the LDAP server.
External User Group Mapping - Base DN	Displays a base DN to search for users to authenticate.
External User Group Mapping - Search User's DN	Displays the DN of the user for searching.
External User Group Mapping - Password	Displays asterisks (*) to mask the password of the user for searching.
External User Group Mapping - Timeout	Displays the number of seconds before connection to the LDAP server times out.
External User Group Mapping - Retry Interval	Displays the retry interval in seconds when the connection to the LDAP server fails.
External User Group Mapping - Number of Retries	Displays the retry times when the connection to the LDAP server fails.
Setup Server	Displays the Setup Server window.

Kerberos Properties
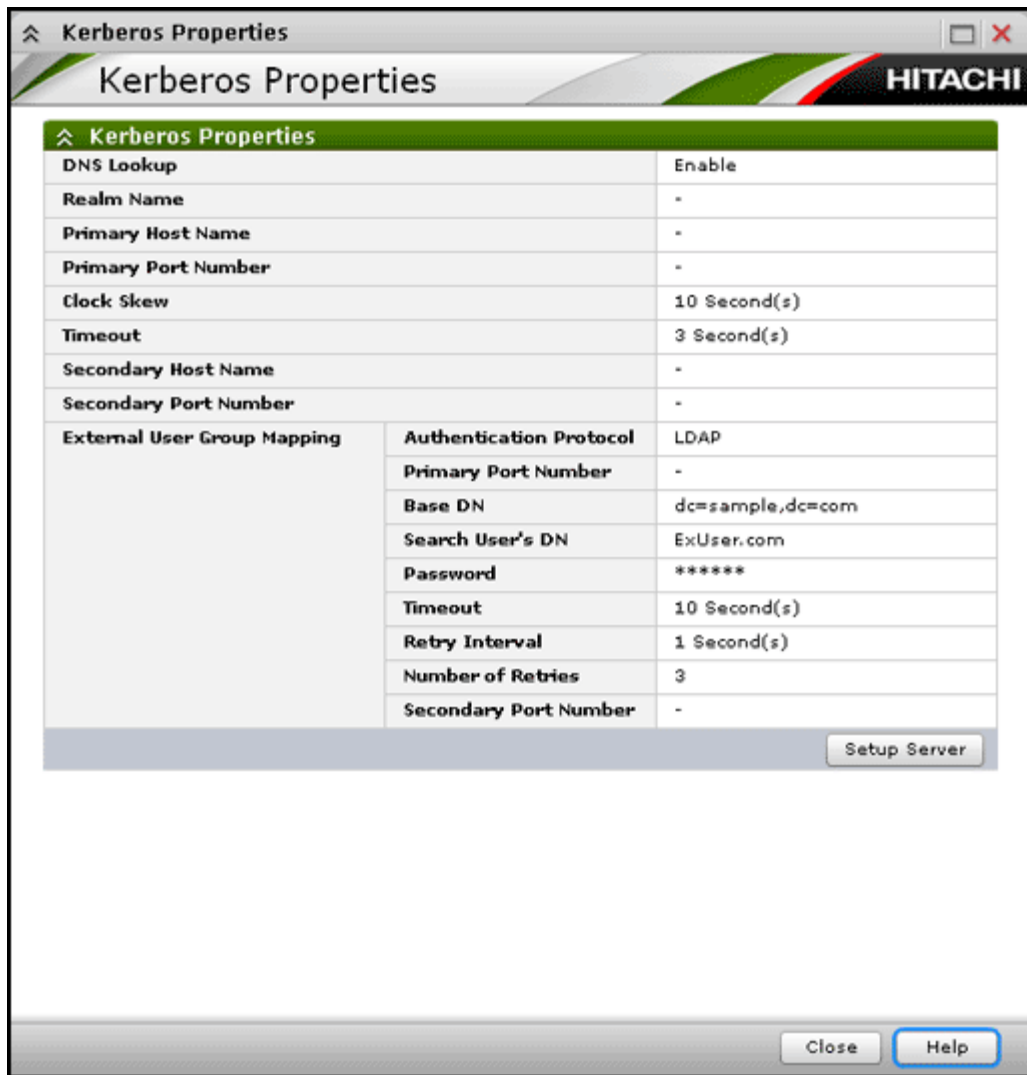
This window displays when you select **Kerberos** in External Authentication.

Kerberos Properties table

Item	Description
DNS Lookup	Displays whether to search for the Kerberos server using the information registered in the SRV records in the DNS server. • Enable: Performs the search using information registered in the SRV records in the DNS server. • Disable: Performs the search using the host name and the port number.
Realm Name	Displays the default realm name.
Primary Host Name	Displays the name of the Kerberos server.
Primary Port Number	Displays the port number of the Kerberos server.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
Clock Skew	Displays the acceptable range of time difference between the SVP and the Kerberos server.
Timeout	Displays the number of seconds before connection to the Kerberos server times out.
Secondary Host Name	Displays the name of the secondary Kerberos server.
Secondary Port Number	Displays the port number of the secondary Kerberos server.
External User Group Mapping - Authentication Protocol	Displays the LDAP protocol to use.
External User Group Mapping - Primary Port Number	Displays the port number of the LDAP server.
External User Group Mapping - Base DN	Displays a base DN to search for users to authenticate.
External User Group Mapping - Search User's DN	Displays the DN of the user for searching.
External User Group Mapping - Password	Displays asterisks (*) to mask the password of the user for searching.
External User Group Mapping - Timeout	Displays the number of seconds before connection to the LDAP server times out.
External User Group Mapping - Retry Interval	Displays the retry interval in seconds when the connection to the LDAP server fails.
External User Group Mapping - Number of Retries	Displays the retry times when the connection to the LDAP server fails.
External User Group Mapping - Secondary Port Number	Displays the port number of the secondary LDAP server.
Setup Server	Displays the Setup Server window.

Setup Server wizard

Select Authentication Server window
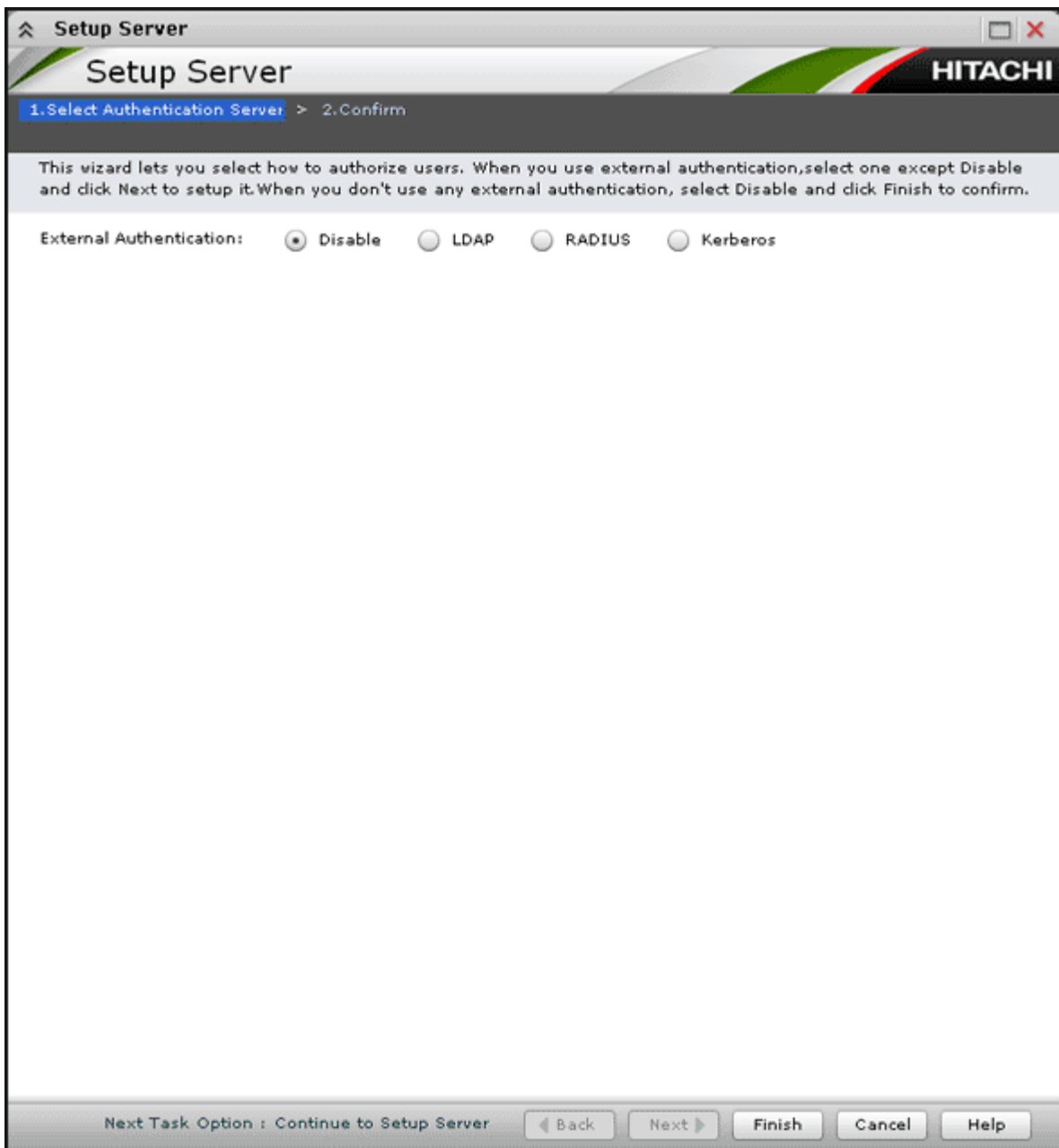
This window displays when you select Server Setup from the LDAP, RADIUS, or Kerberos properties window

Setting field

Item	Description
External Authentication	Select the type of authentication server. • Disable: Does not use any authentication server. Users are authenticated with user information registered in the SVP. • LDAP: Users are authenticated with user information registered in the LDAP server. • RADIUS: Users are authenticated with user information registered in the RADIUS server. • Kerberos: Users are authenticated with user information registered in the Kerberos server. When you select **Disable**, click **Finish** to open the confirm window. When you select **LDAP**, **RADIUS**, or **Kerberos**, click **Next** to open the Setup Server window.

Disable authentication server setup window

This window displays when you select **Disable** in Select Authentication Server window.

Selected Server table

Item	Description
External Authentication	Displays the type of the authentication server. • Disable: Does not use any authentication server. Users are authenticated with user information registered in the SVP.

Item	Description
	• LDAP: Users are authenticated with user information registered in the LDAP server. • RADIUS: Users are authenticated with user information registered in the RADIUS server. • Kerberos: Users are authenticated with user information registered in the Kerberos server.

Setup Server for LDAP

Setup Server for LDAP window

This window displays when you select **LDAP** in Select Authentication Server window.

Setting fields

Item	Description
Certification File Name	Specify a certification file. Click **Browse** to find the file.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
DNS Lookup	Specify whether to search for the LDAP server using the information registered in the SRV records in the DNS server. • Enable: Performs the search using information registered in the SRV records in the DNS server. • Disable: Performs the search using the host name and the port number.
Authentication Protocol	Specify an LDAP protocol to use. Available protocols are as follows. • LDAP over SSL/TLS • STARTTLS If you select **Enable** in DNS Lookup, you cannot select LDAP over SSL/TLS.
External User Group Mapping	Specify whether to connect an authentication server to an authorization server. • Enable: Connects an authentication server to an authorization server. • Disable: Does not connect an authentication server to an authorization server.
External User Group Mapping - Host Name	Specify a host name of the LDAP server. ASCII code characters, hyphens (-), and periods (.) can be specified. If you select **Enable** in DNS Lookup, this item is disabled.
External User Group Mapping - Port Number	Specify a port number of the LDAP server. If you select **Enable** in DNS Lookup, this item is disabled.
External User Group Mapping - Domain Name	Specify a domain name that the LDAP server manages. You can specify ASCII code characters, hyphens (-), and periods (.).
External User Group Mapping - User Name Attribute	Specify an attribute name to identify a user, such as a user ID. You can specify ASCII code characters and the following symbols: ! # $ % & ' ( ) * + , -. / : ; < = > ? @[\ ] ^ _` {	} ~ • Hierarchical model Specify an attribute name where the value that can identify a user is stored. • Flat model Specify an attribute name for a user entry's RDN.
External User Group Mapping - Timeout	Specify the number of seconds before connection to the LDAP server times out.
External User Group Mapping - Retry Interval	Specify a retry interval in seconds when the connection to the LDAP server fails.
External User Group Mapping - Number of Retries	Specify retry times when the connection to the LDAP server fails.

Item	Description
External User Group Mapping - Base DN	Specify a base DN to search for users to authenticate. Available characters: Alphanumeric characters (ASCII characters) and all symbols. • Hierarchical model Specify a DN of hierarchy that includes all the targeted users for searching. • Flat model Specify a DN of hierarchy that is one level up of the targeted user for searching. You can enter alphanumeric characters and all symbols. Note, however, that when you enter symbols like the following, you need to use a backslash to escape for each symbol: + ; , < = > \ / " In some cases, you may need to use a backslash and an ASCII character to escape. • \->\5c (hexadecimal) • / -> \2f (hexadecimal) • "->\22 (hexadecimal)
External User Group Mapping - Search User's DN	Search for a user by specifying a DN. Available characters: Alphanumeric characters (ASCII characters) and all symbols. If you specify sAMAccountName in External User Group Mapping - User Name Attribute, or if you select Enable in External User Group Mapping, this item must be specified. You can enter alphanumeric characters and all symbols. Note, however, that when you enter symbols like the following, you need to use a backslash to escape for each symbol: + ; , < = > \ / " In some cases, you may need to use a backslash and an ASCII character to escape. • \->\5c (hexadecimal) • / -> \2f (hexadecimal) • "->\22 (hexadecimal)
External User Group Mapping - Password	Search for a user by specifying his password. Search for a user by specifying his password. Specify the same password that is registered in the LDAP server. You can specify ASCII code characters and the following symbols: ! # $ % & ' ( ) * + - . = @ \ ^ _ | If you specify sAMAccountName in External User Group Mapping - User Name Attribute, or if you select Enable in External User Group Mapping, this item must be specified.
External User Group Mapping - Re-enter Password	Re-enter the password of the user group you are searching for to confirm your entry. You can specify ASCII code characters and the following symbols:

Storage Navigator GUI reference (main windows)

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
	! # $ % & ' ( ) * + - . = @ \ ^ _ |
	If you enter any password in External User Group Mapping - Password, you must specify this item.
Secondary Server	Specify whether to use a secondary LDAP server. • **Enable**: Uses a secondary LDAP server. • **Disable**: Does not use a secondary LDAP server. If you select Enable in DNS Lookup, this item is disabled.
Secondary Server - Host Name	Specify a host name of the secondary LDAP server. You can specify ASCII code characters, hyphens (-), and periods (.). If you select **Disable** in Secondary Server, this item is disabled.
Secondary Server -Port Number	Specify a port number of the secondary LDAP server. If you select **Disable** in Secondary Server, this item is disabled.
Test User Name	Specify a user name for a server connection test. You can specify ASCII code characters and the following symbols: ! # $ % & ' * + - . / = ? @ ^ _ `{ | } ~
Password	Specify a password of the user name for a server connection test. You can specify ASCII code characters and the following symbols: ! # $ % & ' ( ) * + , -. / : ; < = > ? @[\ ] ^ _` { | } ~
Server Configuration Test	Click **Check** to conduct a server connection test for the authentication server and the authorization server based on the specified settings.
Server Configuration Test - Result	Displays a result of the server connection test for the authentication server and the authorization server.

LDAP setup server confirmation window

Selected Server table

Item	Description
External Authentication	Displays the type of the authentication server. • Disable: Does not use any authentication server. Users are authenticated with user information registered in the SVP. • LDAP: Users are authenticated with user information registered in the LDAP server.

Storage Navigator GUI reference (main windows)

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
	• RADIUS: Users are authenticated with user information registered in the RADIUS server.
	• Kerberos: Users are authenticated with user information registered in the Kerberos server.

Setup Server table

Item	Description
Certification File Name	Displays the certification file.
DNS Lookup	Displays whether to search for the LDAP server using the information registered in the SRV records in the DNS server. • Enable: Performs the search using information registered in the SRV records in the DNS server. • Disable: Performs the search using the host name and the port number.
Authentication Protocol	Displays the LDAP protocol.
External User Group Mapping	Displays whether to connect an authentication server to an authorization server. • Enable: Connects an authentication server to an authorization server. • Disable: Does not connect an authentication server to an authorization server.
Primary Host Name	Displays the host name of the LDAP server.
Primary Port Number	Displays the port number of the LDAP server.
Domain Name	Displays the domain name that the LDAP server manages.
User Name Attribute	Displays the attribute name to identify a user.
Base DN	Displays the base DN for searching for users to authenticate.
Search User's DN	Displays the DN of a user for searching.
Password	Displays asterisks (*) to mask the password of the user for searching.
Timeout	Displays the number of seconds before connection to the LDAP server times out.
Retry Interval	Displays the retry interval in seconds when the connection to the LDAP server fails.
Number of Retries	Displays the retry times when the connection to the LDAP server fails.
Secondary Host name	Displays the host name of the secondary LDAP server.
Secondary Port Number	Displays the port number of the secondary LDAP server.

Setup Server for RADIUS

Setup Server RADIUS window

This window displays when you select **RADIUS** in Select Authentication Server window.

Setting fields

Item	Description
Authentication Protocol	Specify a RADIUS protocol to use. • PAP: Password authentication protocol that transmits plaintext user ID and password. • CHAP: Challenge-handshake authentication protocol that transmits encrypted password.
Host Name	Specify a name of the RADIUS server. You can specify ASCII code characters, hyphens (-), and periods (.).
Secret	Specify a RADIUS secret key used for the PAP authentication or the CHAP authentication. You can specify ASCII code characters and the following symbols: ! # $ % & ' ( ) * + - . = @ \ ^ _ |
Re-enter Secret	Re-enter the RADIUS secret key to confirm your entry. You can specify ASCII code characters and the following symbols: ! # $ % & ' ( ) * + - . = @ \ ^ _ |
NAS Address	Specify an identifier for the RADIUS server to find SVP. • To specify a host name, select **Identifier** and enter the host name. You can specify ASCII code characters and the following symbols: ! " # $ % & ' ( ) * + , - . / ; : < > = ? @ [\ ] ^ _ { } ~ • To specify an IPv4 address, select IPv4 and enter 4 numbers (0-255). For example: *XXX.XXX.XXX.XXX* (X indicates a digit) Specify only numbers. Do not specify any periods. • To specify an IPv6 address, select IPv6 and enter 8 hexadecimal numbers (0-FFFF). For example: *YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY* (Y indicates a hexadecimal digit) Enter 0 to omit a segment.
Port Number	Specify a port number of the RADIUS server.
Timeout	Specify the number of seconds before connection to the RADIUS server times out.
Number of Retries	Specify the retry times when the connection to the RADIUS server fails.
Secondary Server	Specify whether to use a secondary RADIUS server and a secondary LDAP server. • Enable: Uses secondary servers. • Disable: Does not use secondary servers.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
Secondary Server - Host Name	Specify a name of the secondary RADIUS server. You can specify ASCII code characters, hyphens (-), and periods (.). If you select Disable in Secondary Server, this item is disabled.
Secondary Server - Port Number	Specify a port number of the secondary RADIUS server. If you select Disable in Secondary Server, this item is disabled.
External User Group Mapping	Specify whether to connect an authentication server to an authorization server. • Enable: Connects an authentication server to an authorization server. • Disable: Does not connect an authentication server to an authorization server.
External User Group Mapping - Certification File Name	Specify a certification file. Click **Browse** to find the file. If you select **Disable** in External User Group Mapping, this item is disabled.
External User Group Mapping - DNS Lookup	Specify whether to search for the LDAP server using the information registered in the SRV records in the DNS server. • Enable: Performs the search using information registered in the SRV records in the DNS server. • Disable: Performs the search using the host name and the port number. If you select **Disable** in External User Group Mapping, this item is disabled.
External User Group Mapping - Authentication Protocol	Specify an LDAP protocol to use. Available protocols are as follows. • LDAP over SSL/TLS • STARTTLS If you select **Enable** in **DNS Lookup**, you cannot select LDAP over SSL/TLS. If you select **Disable** in External User Group Mapping, this item is disabled.
External User Group Mapping - Host Name	Specify a host name of the LDAP server. You can specify ASCII code characters, hyphens (-), and periods (.). If you select **Enable** in **DNS Lookup**, or if you select **Disable** in External User Group Mapping, this item is disabled.
External User Group Mapping - Port Number	Specify a port number of the LDAP server. If you select **Enable** in DNS Lookup, or if you select **Disable** in External User Group Mapping, this item is disabled.
External User Group Mapping - Domain Name	Specify a domain name of the LDAP server. You can specify ASCII code characters, hyphens (-), and periods (.). If you select **Disable** in External User Group Mapping, this item is disabled.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description

External User Group Mapping - Base DN	Specify a base DN to search for users to authenticate.
	
	Available characters: Alphanumeric characters (ASCII characters) and all symbols.
	
	• Hierarchical model
	
	    Specify a DN of hierarchy that includes all the targeted users for searching.
	
	• Flat model
	
	    Specify a DN of hierarchy that is one level up of the targeted user for searching.
	
	You can enter alphanumeric characters and all symbols. Note, however, that when you enter symbols like the following, you need to use a backslash to escape for each symbol:
	
	+ ; , < = > \ / "
	
	In some cases, you may need to use a backslash and an ASCII character to escape.
	
	• \->\5c (hexadecimal)
	• / -> \2f (hexadecimal)
	• "->\22 (hexadecimal)

External User Group Mapping - Search User's DN	Search for a user by specifying a DN Available characters: Alphanumeric characters (ASCII characters) and all symbols. If you specify sAMAccountName in External User Group Mapping - User Name Attribute, or if you select Enable in External User Group Mapping, this item must be specified. You can enter alphanumeric characters and all symbols. Note, however, that when you enter symbols like the following, you need to use a backslash to escape for each symbol: + ; , < = > \ / " In some cases, you may need to use a backslash and an ASCII character to escape. • \->\5c (hexadecimal) • / -> \2f (hexadecimal) • "->\22 (hexadecimal)
External User Group Mapping - Password	Search for a user by specifying his password. Specify the same password that is registered in the LDAP server. You can specify ASCII code characters and the following symbols: ! # $ % & ' ( ) * + - . = @ \ ^ _ | If you select Disable in External User Group Mapping, this item is disabled.
External User Group Mapping - Re-enter Password	Re-enter the password of the user you are searching for to confirm your entry. You can specify ASCII code characters and the following symbols: ! # $ % & ' ( ) * + - . = @ \ ^ _ | If you enter any password in External User Group Mapping - Password, you must specify this item.

Item	Description
	If you select **Disable** in External User Group Mapping, this item is disabled.
External User Group Mapping - Timeout	Specify the number of seconds before connection to the LDAP server times out. If you select **Disable** in External User Group Mapping, this item is disabled.
External User Group Mapping - Retry Interval	Specify a retry interval in seconds when the connection to the LDAP server fails. If you select **Disable** in External User Group Mapping, this item is disabled.
External User Group Mapping - Number of Retries	Specify retry times when the connection to the LDAP server fails. If you select **Disable** in External User Group Mapping, this item is disabled.
Test User Name	Specify a user name for a server connection test. You can specify ASCII code characters and the following symbols: ! # $ % & ' * + - . / = ? @ ^ _ ` {	} ~
Password	Specify a password of the user name for a server connection test. You can specify ASCII code characters and the following symbols: ! # $ % & ' ( ) * + , -. / : ; < = > ? @[\ ] ^ _` {	} ~
Server Configuration Test	Click **Check** to conduct a server connection test for the authentication server and the authorization server based on the specified settings.
Server Configuration Test - Result	Displays a result of the server connection test for the authentication server and the authorization server.

RADIUS setup server confirmation window

Selected Server table

Item	Description
External Authentication	Displays the type of the authentication server. • Disable: Does not use any authentication server. Users are authenticated with user information registered in the SVP. • LDAP: Users are authenticated with user information registered in the LDAP server. • RADIUS: Users are authenticated with user information registered in the RADIUS server.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
	• Kerberos: Users are authenticated with user information registered in the Kerberos server.

Setup Server table

Item	Description
Authentication Protocol	Displays the RADIUS protocol to use. • PAP: Password authentication protocol that transmits plaintext user ID and password. • CHAP: Challenge-handshake authentication protocol that transmits encrypted password.
Primary Host Name	Displays the name of the RADIUS server.
Secret	Displays asterisks (*) to mask the RADIUS secret key used for the PAP authentication or the CHAP authentication.
NAS Address	Displays the identifier for the RADIUS server to find SVP.
Primary Port Number	Displays the port number of the RADIUS server.
Timeout	Displays the number of seconds before connection to the RADIUS server times out.
Number of Retries	Displays the retry times when the connection to the RADIUS server fails.
Secondary Host Name	Displays the name of the secondary RADIUS server.
Secondary Port Number	Displays the port number of the secondary RADIUS server.
External User Group Mapping - Certification File Name	Displays the certification file.
External User Group Mapping - Authentication Protocol	Displays the LDAP protocol to use.
External User Group Mapping - DNS Lookup	Displays whether to search for the LDAP server using the information registered in the SRV records in the DNS server. • Enable: Performs the search using information registered in the SRV records in the DNS server. • Disable: Performs the search using the host name and the port number.
External User Group Mapping - Host Name	Displays the host name of the LDAP server.
External User Group Mapping - Port Number	Displays the port number of the LDAP server.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
External User Group Mapping - Domain Name	Displays the domain name of the LDAP server.
External User Group Mapping - Base DN	Displays a base DN to search for users to authenticate.
External User Group Mapping - Search User's DN	Displays the DN of the user for searching.
External User Group Mapping - Password	Displays asterisks (*) to mask the password of the user for searching.
External User Group Mapping - Timeout	Displays the number of seconds before connection to the LDAP server times out.
External User Group Mapping - Retry Interval	Displays the retry interval in seconds when the connection to the LDAP server fails.
External User Group Mapping - Number of Retries	Displays the retry times when the connection to the LDAP server fails.

Setup Server for Kerberos

Setup Server Kerberos window

This window displays when you select **Kerberos** in Select Authentication Server window.

Setting fields

Item	Description
DNS Lookup	Specify whether to search for the Kerberos server using the information registered in the SRV records in the DNS server.

Item	Description
	• Enable: Performs the search using information registered in the SRV records in the DNS server. • Disable: Performs the search using the host name and the port number.
Realm Name	Specify a default realm name. You can specify ASCII code characters and hyphens (-).
Host Name	Specify a host name of the Kerberos server. You can specify ASCII code characters, hyphens (-), and periods (.). If you select Enable in DNS Lookup, this item is disabled.
Port Number	Specify a port number of the Kerberos server. If you select Enable in DNS Lookup, this item is disabled.
Clock Skew	Specify an acceptable range of time difference between the SVP and the Kerberos server.
Timeout	Specify the number of seconds before connection to the Kerberos server times out.
Secondary Server	Specify whether to use a secondary Kerberos server. • Enable: Uses the secondary server. • Disable: Does not use the secondary server. If you specify Enable in DNS Lookup, this item is disabled.
Secondary Server - Host Name	Specify a name of the secondary Kerberos server. You can specify ASCII code characters, hyphens (-), and periods (.). If you select Enable in DNS Lookup, or if you select Disable in Secondary Server, this item is disabled.
Secondary Server - Port Number	Specify a port number of the secondary Kerberos server. If you select Enable in DNS Lookup, or if you select Disable in Secondary Server, this item is disabled.
External User Group Mapping	Specify whether to connect an authentication server to an authorization server. • Enable: Connects an authentication server to an authorization server. • Disable: Does not connect an authentication server to an authorization server.
External User Group Mapping - Certification File Name	Specify a certification file. Click **Browse** to find the file. If you select Disable in External User Group Mapping, this item is disabled.
External User Group Mapping - Authentication Protocol	Specify an LDAP protocol to use. Available protocols are: • LDAP over SSL/TLS • STARTTLS If you select Enable in DNS Lookup, you cannot select LDAP over SSL/TLS.

Item	Description
	If you select Disable in External User Group Mapping, this item is disabled.
External User Group Mapping - Primary Port Number	Specify a port number of the LDAP server. If you select Enable in DNS Lookup, or if you select Disable in External User Group Mapping, this item is disabled.
External User Group Mapping - Secondary Port Number	Specify a port number of the secondary LDAP server. If you select Disable in Secondary Server, Enable in DNS Lookup, or External User Group Mapping fields, this item is disabled.
External User Group Mapping - Base DN	Specify a base DN to search for users to authenticate. Available characters: Alphanumeric characters (ASCII characters) and all symbols. • Hierarchical model Specify a DN of hierarchy that includes all the targeted users for searching. • Flat model Specify a DN of hierarchy that is one level up of the targeted user for searching. You can enter alphanumeric characters and all symbols. Note, however, that when you enter symbols like the following, you need to use a backslash to escape for each symbol: + ; , < = > \ / " In some cases, you may need to use a backslash and an ASCII character to escape. • \->\5c (hexadecimal) • / -> \2f (hexadecimal) • "->\22 (hexadecimal)
External User Group Mapping - Search User's DN	Search for a user by specifying a DN Available characters: Alphanumeric characters (ASCII characters) and all symbols. If you specify sAMAccountName in External User Group Mapping - User Name Attribute, or if you select **Enable** in External User Group Mapping, this item must be specified. If you select **Disable** in External User Group Mapping, this item is disabled. You can enter alphanumeric characters and all symbols. Note, however, that when you enter symbols like the following, you need to use a backslash to escape for each symbol: + ; , < = > \ / " In some cases, you may need to use a backslash and an ASCII character to escape. • \->\5c (hexadecimal) • / -> \2f (hexadecimal) • "->\22 (hexadecimal)
External User Group Mapping - Password	Search for a user by specifying his password. Specify the same password that is registered in the LDAP server. You can specify ASCII code characters and the following symbols:

Item	Description
	! # $ % & ' ( ) * + - . = @ \ ^ _ |
	If you select Disable in External User Group Mapping, this item is disabled.
External User Group Mapping - Re-enter Password	Re-enter the password of the user you are searching for to confirm your entry.
	You can specify ASCII code characters and the following symbols:
	! # $ % & ' ( ) * + - . = @ \ ^ _ |
	If you enter any password in External User Group Mapping - Password, you must specify this item.
	If you select Disable in External User Group Mapping, this item is disabled.
External User Group Mapping - Timeout	Specify the number of seconds before connection to the LDAP server times out.
	If you select Disable in External User Group Mapping, this item is disabled.
External User Group Mapping - Retry Interval	Specify a retry interval in seconds when the connection to the LDAP server fails.
	If you select Disable in External User Group Mapping, this item is disabled.
External User Group Mapping - Number of Retries	Specify retry times when the connection to the LDAP server fails.
	If you select Disable in External User Group Mapping, this item is disabled.
Test User Name	Specify a user name for a server connection test.
	You can specify ASCII code characters and the following symbols:
	! # $ % & ' * + - . / = ? @ ^ _ ` { | } ~
Password	Specify a password of the user name for a server connection test.
	You can specify ASCII code characters and the following symbols:
	! # $ % & ' ( ) * + , -. / : ; < = > ? @[\ ] ^ _` { | } ~
Server Configuration Test	Click **Check** to conduct a server connection test for the authentication server and the authorization server based on the specified settings.
Server Configuration Test - Result	Displays a result of the server connection test for the authentication server and the authorization server.

Kerberos setup server confirmation window

Selected Server table

Item	Description
External Authentication	Displays the type of the authentication server. • Disable: Does not use any authentication server. Users are authenticated with user information registered in the SVP. • LDAP: Users are authenticated with user information registered in the LDAP server. • RADIUS: Users are authenticated with user information registered in the RADIUS server.

Item	Description
	• Kerberos: Users are authenticated with user information registered in the Kerberos server.

Setup Server table

Item	Description
DNS Lookup	Displays whether to search for the Kerberos server using the information registered in the SRV records in the DNS server. • Enable: Performs the search using information registered in the SRV records in the DNS server. • Disable: Performs the search using the host name and the port number.
Realm Name	Displays the default realm name.
Primary Host Name	Displays the name of the Kerberos server.
Primary Port Number	Displays the port number of the Kerberos server.
Clock Skew	Displays the acceptable range of time difference between the SVP and the Kerberos server.
Timeout	Displays the number of seconds before connection to the Kerberos server times out.
Secondary Host Name	Displays the name of the secondary Kerberos server.
Secondary Port Number	Displays the port number of the secondary Kerberos server.
External User Group Mapping - Certification File Name	Displays the certification file.
External User Group Mapping - Authentication Protocol	Displays the LDAP protocol to use.
External User Group Mapping - Primary Port Number	Displays the port number of the LDAP server.
External User Group Mapping - Base DN	Displays a base DN to search for users to authenticate.
External User Group Mapping - Search User's DN	Displays the DN of the user for searching.
External User Group Mapping - Password	Displays asterisks (*) to mask the password of the user for searching.
External User Group Mapping - Timeout	Displays the number of seconds before connection to the LDAP server times out.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
External User Group Mapping - Retry Interval	Displays the retry interval in seconds when the connection to the LDAP server fails.
External User Group Mapping - Number of Retries	Displays the retry times when the connection to the LDAP server fails.
External User Group Mapping - Secondary Port Number	Displays the port number of the secondary LDAP server.

Edit SIM Syslog Server Settings wizard

Edit SIM Syslog Server Settings window

Use this window to configure syslog servers so that storage system failures will be reported to syslogs when SIMs occur.

Setting fields

Item	Description
Primary Server	Specify whether SIMs are reported to syslogs in the primary server. • Enable: SIMs are reported to syslogs in the primary server. • Disable: SIMs are not reported to syslogs in the primary server.
Primary Server - IP Address	Specify an IP address of the primary syslog server. You can specify an IPv4 address or an IPv6 address. • To specify an IPv4 address, select IPv4 and enter 4 numbers (0-255). For example: XXX.XXX.XXX.XXX (X indicates a digit) • To specify an IPv6 address, select IPv6 and enter 8 hexadecimal numbers (0-FFFF). For example: YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY (Y indicates a hexadecimal digit)
Primary Server - Port Number	Enter a port number of the primary syslog server. The default port number is displayed. You can also specify any port number.
Secondary Server	Specify whether SIMs are reported to syslogs in the secondary server. • Enable: SIMs are reported to syslogs in the secondary server. • Disable: SIMs are not reported to syslogs in the secondary server.
Secondary Server - IP Address	Specify an IP address of the secondary syslog server. You can specify an IPv4 address or an IPv6 address. • To specify an IPv4 address, select IPv4 and enter 4 numbers (0-255). For example: XXX.XXX.XXX.XXX (X indicates a digit) • To specify an IPv6 address, select IPv6 and enter 8 hexadecimal numbers (0-FFFF). For example: YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY (Y indicates a hexadecimal digit)
Secondary Server - Port Number	Enter a port number of the secondary syslog server. The default port number is displayed. You can also specify any port number.
Location Identification Name	Specify any name to identify the storage system that notifies the syslog server of SIMs. Up to 32 letters and numbers of ASCII code characters and the following symbols can be specified: ! " # $ % & ' ( ) = - ~^ | \ { } [ ] @ ` : ; * + _ ? / < > . You cannot specify commas (,) and spaces.

Item	Description
Send a test message	If this is checked, test SIMs are reported to syslogs as you configure the servers.

Edit SIM Syslog Server Settings confirmation window

Syslog Server table

Item	Description
Primary Server - SIM Transfer	Displays whether SIMs are reported to syslogs in the primary server. • Enable: SIMs are reported to syslogs in the primary server. • Disable: SIMs are not reported to syslogs in the primary server.
Primary Server - IP Address	Displays an IP address of the primary syslog server.
Primary Server - Port Number	Displays a port number of the primary syslog server.
Secondary Server- SIM Transfer	Displays whether SIMs are reported to syslogs in the secondary server.

Storage Navigator GUI reference (main windows)

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
	• Enable: SIMs are reported to syslogs in the secondary server. • Disable: SIMs are not reported to syslogs in the secondary server.
Secondary Server - IP Address	Displays an IP address of the secondary syslog server.
Secondary Server - Port Number	Displays a port number of the secondary syslog server.
Location Identification Name	Displays a name to identify the storage system that notifies the syslog server of SIMs.
Send a test message	Displays whether test SIMs are reported to syslogs. • Yes: Test SIMs are reported to syslogs. • No: Test SIMs are not reported to syslogs.

Storage Navigator GUI reference (main windows)

Storage Navigator GUI reference (secondary windows)

This appendix describes the Storage Navigator secondary windows.

Storage Navigator secondary window
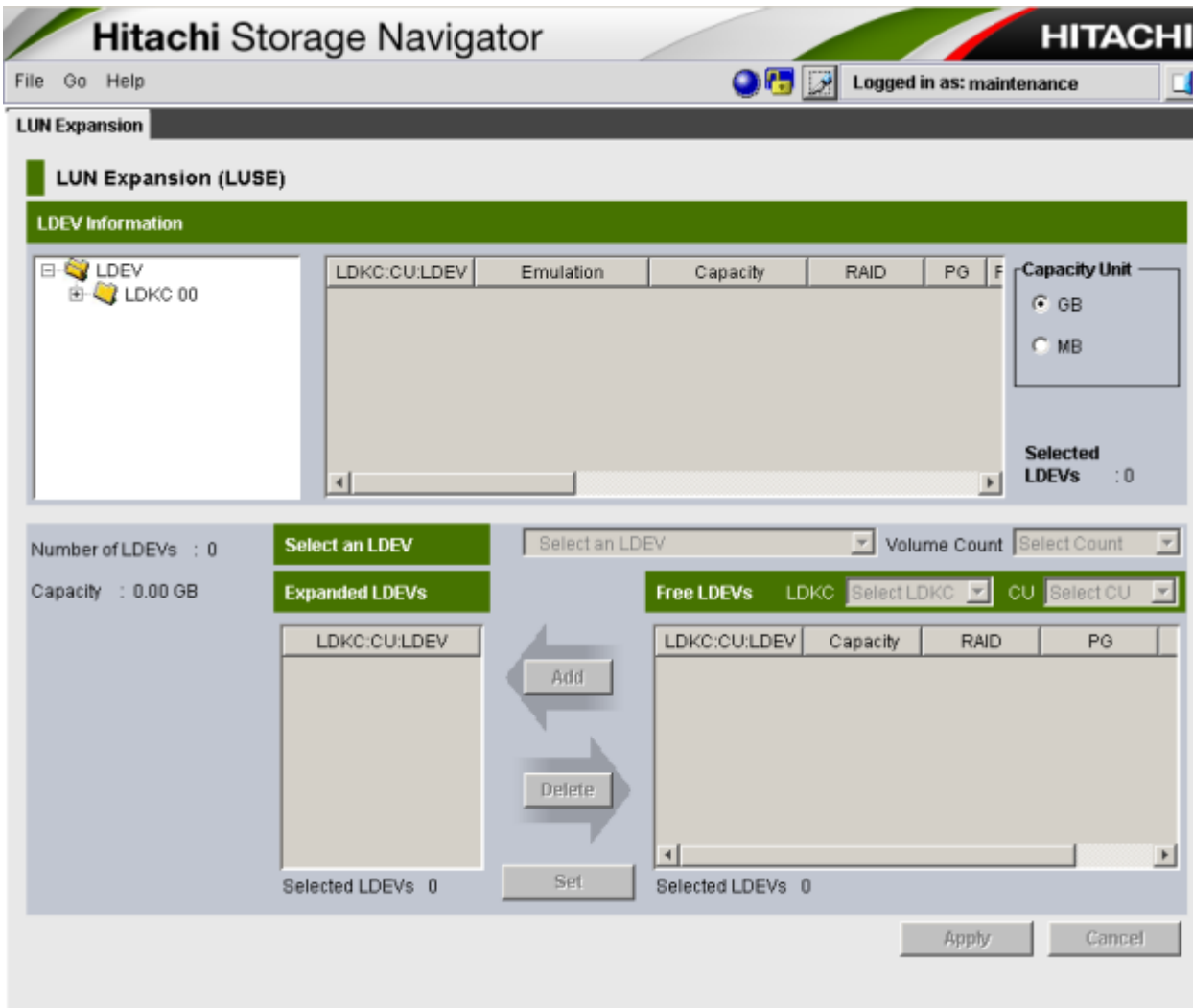
The Storage Navigator secondary window is reset when you do any of the following:

- Click **Apply** or **Cancel**.
- Click **Refresh** or **Refresh All** on the **File** menu.
- Switch tabs.

Item	Description
Title bar	Provides information about the connected storage system. • IP indicates the IP address of the SVP. • S/N indicates the serial number. • D/N indicates the device name specified in the Edit storage system window.
File > Basic Information	Opens the Basic Information Display dialog box, which provides the basic configuration information on the storage system.

Item	Description
File > Refresh All	Updates the information on the SVP. All information displayed on the Storage Navigator secondary window is reacquired from the storage system. We recommend that you use this command only when error recovery is required. • Takes time until the processing has been completed. • While updating, other users are not allowed to perform any operation on the Storage Navigator windows. Maintenance of the storage system or the SVP operation by the service personnel is not allowed, either. • Available only for the user with Storage Administrator (Initial Configuration) role. • Available only when the user is in Modify mode. • The information may not display correctly if SVP maintenance is in progress. • Try this command if the configuration information displayed on the Storage Navigator differs from the actual configuration information that can be recognized from the host.
File > Refresh	Displays the latest information on Storage Navigator. The information might not display correctly when the exclusive lock is effective or SVP maintenance is in progress.
File > Close	Closes the Storage Navigator secondary window
Go	Indicates software names
Help > About	Opens the About dialog box to show the version of the storage system.
Normal Warning Abnormal	Indicates the storage system error status by color (blue: normal, yellow: warning, red: abnormal) according to the host SIM status. If the SIM occurs but is not reported to the host, the status remains the same.
Unlocked Locked	Indicates the current operational mode of Storage Navigator. If all logged in users are currently working in the view mode, the blue unlocked-shaped icon () appears. If any user is working in the Modify mode, the red locked-shaped icon () appears. Note: The operational status might not be displayed correctly when the exclusive lock is effective or SVP maintenance is in progress.
View Modify	Allows users to switch the operation mode between Modify and View. The button always shows the current user operation mode. To change the modes, click the button. You cannot switch to the Modify mode while any other user is operating in the Modify mode. Make sure to confirm the exclusive lock icon before switching to the Modify mode.
Reset	Reset the remaining time for the Modify mode. Appears only when you are in Modify mode.
Logged in as	Shows the user ID of the currently logged-in user.

Item	Description
Logout	Closes the Storage Navigator secondary window.
Apply	Implements all the changes or settings displayed in blue bold italics. This button is available only in Modify mode. You can create and store up to 20,000 settings or operations before actually applying them to the storage system. To avoid a possible error, do not apply more than 20,000 settings at a time.
Cancel	Cancels the changes or settings made on the window. This button is available only in Modify mode.
PP Status	Displays the SIM severity level. **PP Status** appears if a SIM occurs related to a software license because the license is expired or the licensed capacity is insufficient. However only the storage administrator with the Storage Administrator role set to Enable will be able to see the display. **PP Status** can display any of the following SIM severity level statuses: • If **PP Status: Normal** appears, no SIM has occurred. If any other status appears, view either the License Key window or the Status window to identify which software has a problem. You may find that you need to consider purchasing the license. • When multiple SIMs occur, only the SIM with the highest severity appears.

Opening Storage Navigator secondary windows

Some Storage Navigator operations are performed through secondary windows that use a Java application. For this reason, whether you are using JRE 5.0 or 6.0, a message might appear and ask if you want to run a Java Application. You might see slightly different dialog boxes depending on your environment and configuration.

To use Storage Navigator, click **Run** in the following dialog box. If you select the **Always trust content from this publisher** option before clicking **Run**, Storage Navigator is always allowed to access the local files and you will not see this dialog box again.
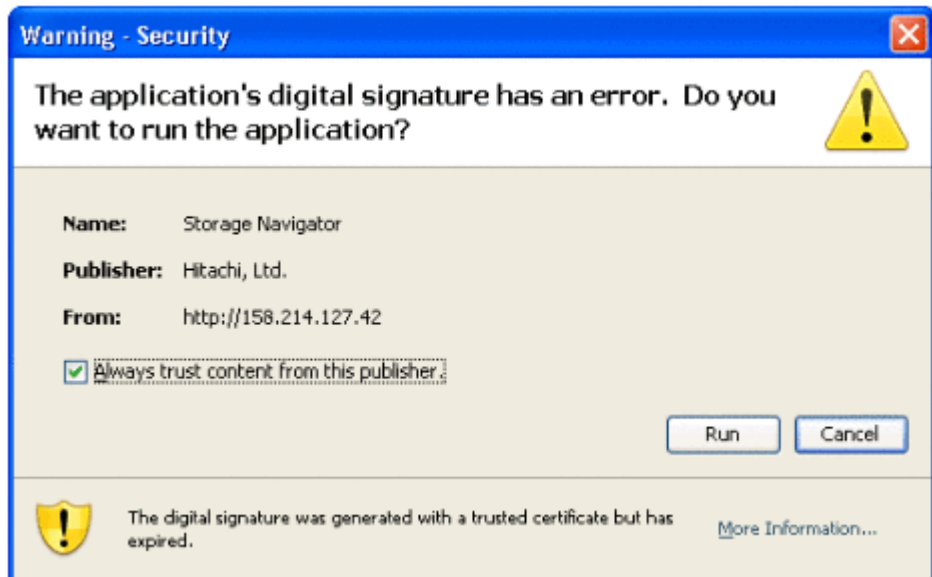
Figure E-1 Warning - Security dialog box when digital signature is expired (for JRE 5.0)

Note: The Storage Navigator digital signature has an expiration date and it might be expired depending on the Storage Navigator version that you use. Even though the digital signature is expired, you can continue using Storage Navigator.

Note: The following Java versions do not allow the Storage Navigator secondary window to display.

- Java 7 Update 55 or later
- Java 8 Update 5 or later

To start up the window, you need to change Java security settings.

Storage Navigator secondary windows and Modify mode

There is no Modify mode for the Storage Navigator main window. Main window and wizard operations are queued as tasks and performed in order. However, when using a Storage Navigator secondary window, you must be in Modify mode before changing any settings. Secondary window operations are not queued or displayed in the task window.

A secondary window opens when you click a command from the Storage Navigator menu. To make settings in a secondary window, you must change to Modify mode by clicking . Modify mode prohibits other users or programs from changing the storage system setting. As soon as you close the secondary window, Modify mode is released.

Modify mode has a timeout period. If you do not access SVP before the end of the timeout period, Modify mode is released. On some windows, the settings made but not yet applied to the storage system will be canceled.

The secondary window displays the progress bar (shown in the following figure) indicating the remaining time in the timeout period. To extend this period and remain in Modify mode, click **Reset**.

Figure E-2 Modify mode and remaining time in secondary window

The Modify mode default timeout period is 30 minutes, but can be changed by modifying **RMI time-out period for Modify**.

If Modify mode is released due to a timeout, the current window will still be visible, but an error message is returned when you click **Apply**, or when you try to refresh the window through **File** > **Refresh All** or **Refresh View**.

About window

The **About** command provides storage system information.

Item	Description
Storage System Type	Displays the product name of the connected storage system.
Serial Number	Displays the serial number of the connected storage system.
IP Address	Displays the IP address of the connected storage system (SVP).
Storage System Name	Displays the device name of the connected storage system.
Contact	Displays the contact information of the administrator.
Location	Displays the location of the connected storage system.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
Main Version	Displays the version of the microcode installed in the connected storage system.
SVP Version	Displays the version of the Storage Navigator Java application installed in the SVP of the connected storage system. The Java application is downloaded at each time the Storage Navigator computer connects to the SVP, so that the version is always consistent between the Storage Navigator computer and SVP.
RMI Server Version	Displays the version of the RMI server installed in the SVP of the connected storage system.

License Key window

Use the License Key window to install and uninstall software.

Item	Description
License Key list	Lists license keys (software).
Mounted capacity	Displays the capacity of the LDEVs in the storage system. When you install a program product whose license capacity type is Mounted capacity, install license capacity that is at least the same size as the mounted capacity.

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
License Install	Allows you to select one of the following modes for installing a license key: • When **Key Code** mode is selected, use the **Key Code** text box to type the license key code for the selected option to be installed. • When **File** mode is selected, use the **File Name** text box or the **Browse** button to enter the name of the license key file. When you click **Browse**, a dialog box opens allowing you to select the desired license key file. • Select **Available** to update the license status when the license capacity is enough but the license status still displays **Grace Period** or **Not Enough License**. The **Available** button can be used only when the licensed capacity exceeds the mounted (or used) capacity because the LDEVs are reduced, or because the pairs are deleted by a software.
License Status	Allows you to enable or disable a software application. Select a software application, select **Enable** or **Disable**, and click **Set**. • **Enable**: You can use the software. If you enable a software application with the term key, the available days of term key will decease by one day when you set **Enable**. When the setting is applied, **Installed** appears. • **Disable**: You cannot use the software. If you disable a software with the term key, the available days of term key will not lessen when you set **Disable**. When the setting is applied, **Installed (Disabled)** appears.
Install	**Install** appears in the row of the selected software. The software are not actually installed until you click **Apply**.
Remove	**Remove** appears in the row of the selected software. The options are not actually removed until you click **Apply**.
Apply	Implements the settings to the storage system. The status of installed options changes to **Installed**, and the status of uninstalled option changes to **Not Installed**.
Cancel	Cancels the settings.

License Key list

Item	Description
Product Name	The name of the product and icon indicating whether this is available. • : Installed • : Not Installed
Key Type	The license type: • *Permanent* • *Term* • *Temporary* • *Emergency*

Storage Navigator GUI reference (secondary windows)

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
	• *Not Installed* (when no license key is installed)
Permitted Volumes	The column shows the following information: • Unlimited: The capacity is unlimited • Unlimited (*xx.xx*TB): The capacity is unlimited and *xx.xx* indicates the used license capacity. • *XX*TB: *XX* indicates the licensed capacity. • *XX*TB(*xx.xx*TB): *XX* indicates the licensed capacity and *xx.xx* indicates the used license capacity. For example, if this column displays 10 TB (0.52 TB), the licensed capacity is 10 TB and the used license capacity is 0.52 TB. The used license capacity is the capacity used by the program product. Licensed capacities are calculated assuming that 1 KB = 1,024 bytes, 1 MB = 1,024 KB, 1 GB = 1,024 MB, and 1 TB = 1,024 GB.
Term (days)	The number of days remaining before the expiration of a temporary key, an emergency key, or a term key. After the temporary key has expired, the column shows the number of days that remain before you can reinstall the temporary key.
Status	The current status of a software: • *Installed:* The software is available. • *Installed (Disabled):* Installation is complete, but the license is set to disabled. This status might appear if an error occurs after you install software. Resolve the error and enable the license. This status also appears when the license key of this software is installed but the license key of the prerequisite software is expired. • *Not Installed:* The software is not installed. • *Not Enough License:* Installation is complete, but the license capacity is insufficient. *Not Enough License* might remain displayed when the licensed capacity exceeds the mounted capacity after you reduce the number of LDEVs, or when the licensed capacity exceeds the used capacity after you delete pairs or pools. In these cases, you can refresh the license status by using the Available button. • *Grace Period:* The licensed capacity is insufficient because LDEVs are added, or pairs have been created by a software. Also, for a meter key, licensed capacity also becomes insufficient if licensed capacity is consumed and becomes smaller than the used amount. The license expires in 30 days. Please purchase the licenses before the license key expires. *Grace Period* might remain displayed when the licensed capacity exceeds the mounted capacity after you reduce the number of LDEVs, or when the licensed capacity exceeds the used capacity after you delete pairs or pools. In these cases, you can refresh the license status by using the **Available** button. • *Expired*: The term has already expired for the temporary key. When the status is *Expired*, you cannot re-install the temporary key.

Status and icons

License Key status	Icon	Key type	Permitted volume[1]	Term (days)[2]	Status
Not installed.	(Not Installed)	Not Installed	–	–	Not Installed
Installed with the Permanent key.	(Installed)	Permanent	Unlimited or *X* TB	–	Installed
Installed with the Term key and set to enable.	(Installed)	Term	Unlimited or *X* TB	N	Installed
Installed with the Term key and set to disable.	(Not Installed)	Term	Unlimited or *X* TB	–	Installed (Disabled)
Installed with the *Temporary* key.	(Installed)	Temporary	–	N	Installed
Installed with the *Emergency* key.	(Installed)	Emergency	–	N	Installed
A *Temporary* key was installed, but has expired.	(Not Installed)	Temporary	–	N	Expired
A *Term* key or an *Emergency* key was installed, but has expired.	(Not Installed)	Not Installed	–	–	Not Installed
Installed with the *Permanent* key or the **Term** key, but the licensed capacity was insufficient.	(Not Installed)	Permanent or Term	*X* TB	–	Not Enough License
The capacity insufficiency caused by adding LDEVs.	(Installed)	Permanent or Term	*X* TB	N	Grace Period
Installed with the *Temporary* key, and then reinstalled with the *Permanent* key, but the license capacity was insufficient.	(Installed)	Temporary	*X* TB	N	Installed
Installed with the Permanent key, then reinstalled with the *Emergency* key.	(Installed)	Emergency	Unlimited or *X* TB	N	Installed
"–" indicates that nothing appears.					
Notes:					
1. *X* TB indicates a license capacity. (*Y* TB) might appears beside Unlimited or *X* TB, indicating the minimum license capacity.					

License Key status	Icon	Key type	Permitted volume[1]	Term (days)[2]	Status
2. The **Term** column shows the number (N) of days remaining before the license expires.					

Login Message window
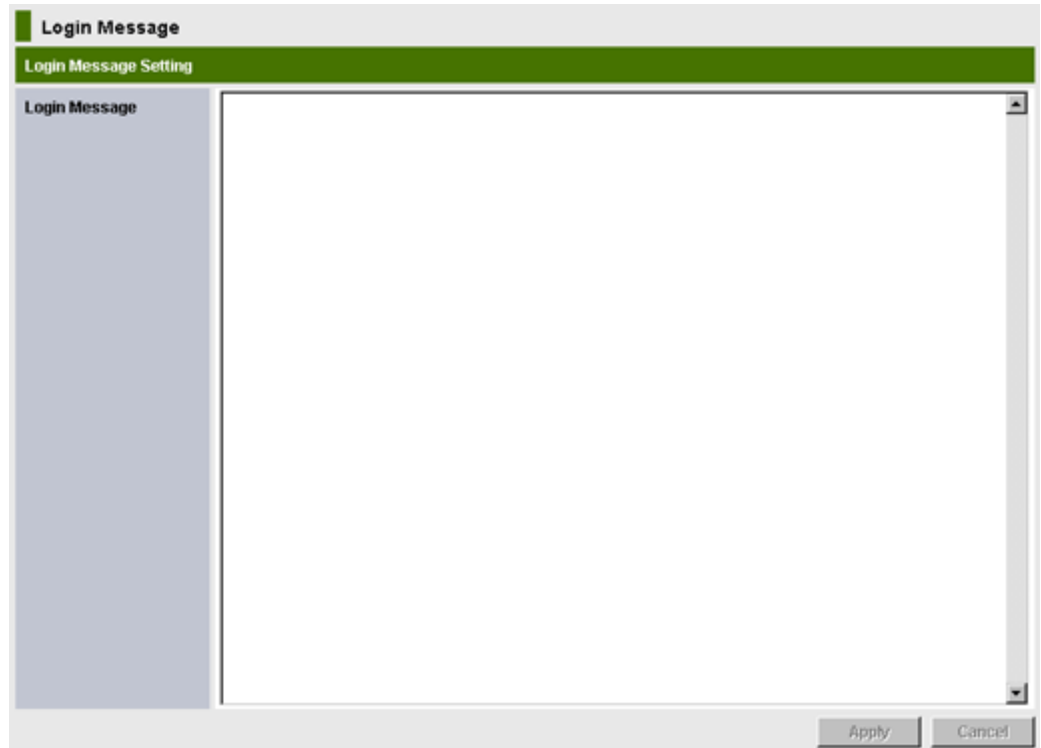
Use the Login Message window to specify the login caution message that appears when Storage Navigator users log in.

Item	Description
Login Message	You can enter alphanumeric characters (ASCII codes) and some symbols. You can enter up to 2,408 letters. The message that you enter in this text box will appear in the Storage Navigator Login window.
Apply	Implements all the changes or settings. This button is available only in Modify mode.
Cancel	Cancels the changes or settings. This button is available only in Modify mode.

Email Information window

Use the Email Information window to configure settings to report storage system failures (SIMs) by email. You can also send a test email from this window.

Item	Description
Mail Notice	Specify whether to report system failures by email. • Enable: Reports system failures by email. • Disable: Does not report system failures by email.
Mail Server	Set an IPv4 address, an IPv6 address, or a host name of the mail server. • To set an IPv4 address, select IPv4 and enter four integers in the range of 0 to 255 (for example, `nnn.nnn.nnn.nnn`, where n is a number). • To set an IPv6 address, select IPv6 and enter eight hexadecimal numbers in the range of 0 to FFFF (for example, `hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh`, where h is a hexadecimal digit). Enter 0 to omit a segment. • To set a host name, select Host Name and enter up to 63 alphanumeric characters (ASCII codes) and symbols, except for the following symbols and a space: " \ ; : , * ? < > | / # & + = [ ] ' { } ^
SMTP-AUTH	Specify whether to use SMTP authentication. • Enable: Uses SMTP authentication. • *Disable:* Does not use SMTP authentication.

Item	Description
Account and Password	Set the account and password for SMTP authentication. Required when SMTP-AUTH is Enable. Enter up to 255 alphanumeric characters and symbols (ASCII codes) for user ID and password, except for the following symbols and a space: " \ ; : , * ? < > | / # & + = [ ] ' { } ^
From Address	Specify an email address of the sender. Enter up to 255 alphanumeric characters (ASCII codes) and symbols: (! # $ % & ` + - * / ' ^ { } _ .).
Return Address	Specify a Reply-To address of email. If you specify this address, replies from the email receivers will be sent to this address. If you omit this address, replies from the email receivers will be sent to From Address. The available values are the same as those of From Address.
To Address	Specify email addresses of the receivers and the attributes (To, Cc, or Bcc). Up to 32 addresses can be specified. The available values are the same as those of From Address.
Test Send	When you click **Test Send**, test emails are sent to the email addresses of the receivers. This button is available only in Modify mode.

Basic Information Display dialog boxes

The Basic Information Display dialog box provides the basic configuration information of the storage system. This dialog box opens separately from Storage Navigator window, so you can configure settings while viewing the dialog box.

To open the Basic Information Display dialog box, open the Storage Navigator secondary window, then click **File** > **Basic Information**.

The information provided in the Basic Information Display dialog box is updated:

- When the tab is clicked on the Basic Information Display dialog box and the displayed dialog box is changed.
- When the Refresh command is selected on the menu bar of the Storage Navigator main window.
- When the tab is clicked on the Storage Navigator windows during the operation of the product option and the displayed window is changed.
- When the Apply button is clicked on the Storage Navigator main window.
- When the operation mode is changed from the View mode to the Modify mode on the Storage Navigator main window.

Common elements

Basic Information Display - IP:158.214.127.175 - S/N:200142 - D/N:StorageSystem -

Basic Information Display dialog box contains the following items:

- The title bar provides *information about the connected storage system.*
  - *IP indicates the IP address of the SVP.*
  - *S/N indicates the serial number.*
  - *D/N indicates the device name specified in the Information window.*
- To view the details about a LUSE volume in LUN or LDEV dialog box, select a LUSE volume, right-click, and select the *Detail Information* command. The detailed information of the LUSE volume appears. Items displayed in the dialog box are the same as the items displayed in the LDEV list.
- LDEV ID column displays the LDKC number, the CU number, and the LDEV number. These numbers are separated by colons (:). The following symbols might appear at the end of the LDEV number:
  - # (e.g., 00:00:01#) indicates that the LDEV is an external volume.
  - V (e.g., 00:00:01V) indicates that the LDEV is a Thin Image virtual volume.
  - X (e.g., 00:00:01X) indicates that the LDEV is a Dynamic Provisioning virtual volume.

  The icons in the LDEV ID column have the following meaning:
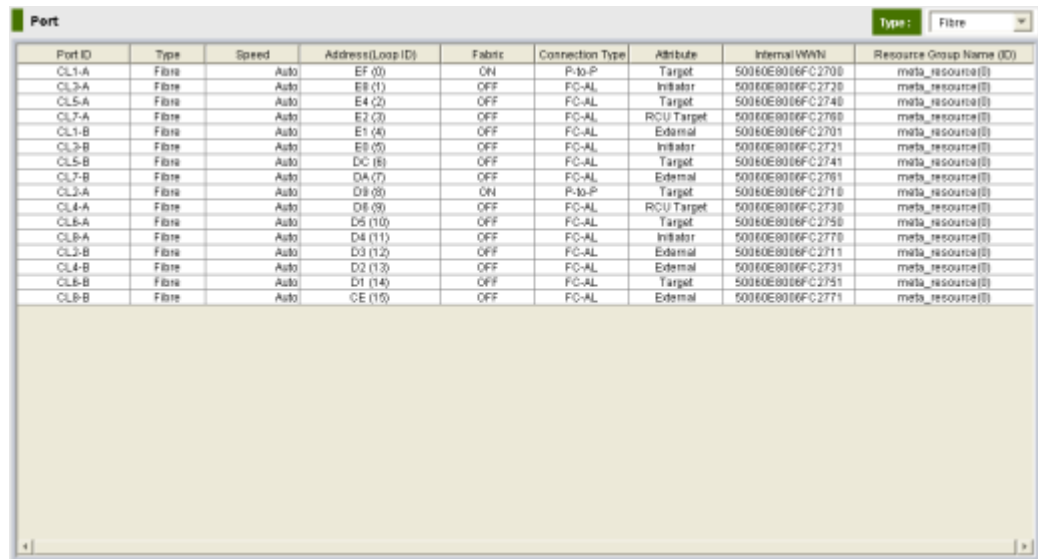
Table E-1 Icons in the LDEV ID column

Icons	Description
	Normal LDEV
	Expanded (LUSE) volume
	Reserved volume of Volume Migration
	Variable-sized volume (CV)
	Secured LDEV

Icons	Description
	Remote command device
	Command device
	Command device to which the command device security is applied

- Use **Export** to save the displayed information as a comma-separated values (CSV) file.
- Use **Close** to close the Basic Information Display dialog box.

Port dialog box

The Port dialog box provides information on ports. The displayed information can be switched using the Type list.

Item	Description
Type	Select a port type to view the port information on the Port list. • Fibre: The information on only the Fibre ports is available.
Port list (when Fibre is selected)	Displays the following when Fibre is selected in Type: • Port ID: Port name. • Type: Type of port. Fibre is displayed. • Speed: Data transfer speed, in Gbps (gigabits per second), for Fibre Channel ports. • Address (Loop ID): Address and Loop ID of port. • Fabric: Indicates whether a Fabric switch is used. ON or OFF is displayed. • Connection Type: Topology. FC-AL or P-to-P is displayed. • Attribute: Port attribute. Initiator, Target, RCU Target, or External is displayed.

Item	Description
	• Internal WWN: WWN of DKC port.
	• Resource Group Name (ID): Name and ID of the resource group where the port is assigned.

LUN dialog box

The LUN dialog box provides information on the volumes.

Item	Description
Port	Select the port for which the information is to be listed.
Port ID	Displays the port name.
Group ID	Displays the group number of the host group.
LUN ID	Displays the LUN number in the decimal (hexadecimal) format. • : Logical volume to which an LU path is defined. • : Expanded LU. • : Remote command device. • : Command device.

Item	Description
	• ![icon]: Command device security.
LDEV ID	From the left the LDKC number, the CU number, and the LDEV number are displayed. For detailed information, see Common elements on page E-14.
Emulation Type	Displays the emulation type. For an expanded volume, such as a LUSE volume, the number of LDEVs configuring the LUSE volume is displayed following the emulation type, for example, OPEN-V*3.
Capacity	Displays Volume capacity. For an expanded volume, such as a LUSE volume, the total capacity of the LDEVs consisting of the LUSE volume is available.
RAID Level	Displays the RAID level.
Number of Paths	Displays the number of LU paths.

LDEV dialog box

The LDEV dialog box provides information about volumes.

Item	Description
CU or PG	Choose which information to display in the *LDEV* list. • If you select LDKC:CU, two lists are available. You can select an LDKC from the list on the left, and a CU from the list on the right. • If you select PG, one list is available. You can select the parity group to display from the list.
CLPR	Displays the CLPR number and CLPR name.
LDEV ID	The LDKC number, the CU number, and the LDEV number. For details about icons, see Table E-1 Icons in the LDEV ID column on page E-14.
MAX LBA	Displays the LDEV size recognized by a host.
Capacity	Displays volume capacity. Volumes are displayed in gigabyte (GB). For an expanded volume, such as a LUSE volume, the capacity of each LDEV is available.
RAID Level	Displays the RAID level.
Internal Volume Information	Displays the hard disk type of internal volume as follows: • Blank indicates SAS drive. • The dollar sign ($) indicates SSD. • A hyphen (-) indicates external volume.
Parity Group ID	Displays the parity group.
Encryption	Shows whether the volume group shown with "ECC Group" is encrypted or not • **Enabled**: The volume is encrypted. • **Disabled**: The volume is not encrypted. • **- (dash)**: This volume is not an internal volume, so encryption information is not displayed.
Number of Paths	Displays the number of LU paths.
Attribute	The attribute set for the volume as follows: • Pool (X): The volume is set as a pool volume (pool-VOL), where X indicates pool ID. • V-VOL: The volume is set as a virtual volume (V-VOL) for Thin Image. • DP-VOL: The volume is set as a virtual volume (V-VOL) for Dynamic Provisioning. • Reserved LDEV: The volume is set as a reserved volume of Volume Migration. • JNL Volume: The volume is set as a journal volume. • Nondisruptive Migration: The volume is set as a nondisruptive migration volume • System Disk: The volume is set as a system disk. • Quorum Disk: The volume is set as a Quorum disk used in High Availability Manager.

Item	Description
External Volume Information	Information on the external volume appears in the format of Vendor/ Product name/ Serial number/ Hard disk type. For an internal volume, "-/-/-/-" appears. For a migration volume, "-/-/-/ " appears. The hard disk type appears as follows: • Blank indicates SAS drives. • An asterisk (*) indicates BD or SATA drive. • The dollar sign ($) indicates SSD. • A hyphen (-) indicates internal volume.
Number of External Paths	Displays the number of LU paths that are set for the external volume.
Cache Mode	Displays the Cache Mode set for the external volume when it was mapped. For an internal volume or a migration volume, a hyphen (-) appears.
Resource Group Name (ID)	Resource Group Name (ID)

LDEV Status dialog box

The LDEV Status dialog box provides information about the status of volumes.

Item	Description
Parity Group list	Allows you to select which disk group to display.
Parity Group ID	A parity group number belonging to the selected disk group.
LDEV Status	A status of all the volumes in the parity group. • *Normal:* All volumes are in a normal status. • *Blocked:* All volumes are in a blocked status. • *Format:* All volumes are being formatted. • *Preparing Quick Format:* All volumes are being prepared for Quick Format. • *Quick Formatting*: Quick Format is in progress. When a parity group contains both the Normal and Normal (Quick Format) statuses, the list also displays Normal (Quick Format). • *Correction Access:* Access attributes of all volumes are being changed. • *Copying:* Data in all volumes is being copied. • *Read Only:* Hosts can only read the volumes. • *Shredding:* The shredding operation is in progress. • *Unknown:* The system does not recognize the status of any volumes. • *Warning:* Some volumes are not in a normal status. • *-:* No volumes in the parity group.
Resource Group Name (ID)	Displays the name and ID of the resource group where the parity group is assigned.
Page Switching area	Displays up to 4,096 parity groups per page. When more parity groups are defined, use the following functions to see the entire list: • *Page Number:* Displays the current page number. It also allows you to display the desired page. • Previous: Displays the previous page. • Next: Displays the next page.
Status area	Displays the status of the disk group that you have selected in the *Parity Group* list. • Normal: All volumes are in a normal status. • Warning: Not all volumes are in a normal status.
Detail	When you select a parity group in the list and click Detail, all the LDEVs in the parity group are displayed in the LDEV list on the right.
LDEV ID	From the left the LDKC number, the CU number, and the LDEV number are displayed.
Status	A status of a volume. • *Normal:* All volumes are in a normal status. • *Blocked:* All volumes are in a blocked status. • *Format:* All volumes are being formatted. • *Preparing Quick Format:* The volume is being prepared for Quick Format.

Item	Description
	• *Quick Formatting:* Quick Format is in progress. • *Correction Access:* The access attribute of the volume is being changed. • *Copying:* Data in all volumes is being copied. • *Read Only:* Hosts can only read the volume. • *Shredding:* The shredding operation is in progress. • *Unknown:* The system does not recognize the status of the volume.
Resource Group Name (ID)	Displays the name and ID of the resource group where the LDEV is assigned.

Tool Panel GUI Reference

This appendix describes the Tool Panel window items

☐ Control Panel

Control Panel

This section describes the Tool Panel windows and controls.

Environment Parameter window

This section describes the Environment Parameter window features and controls.
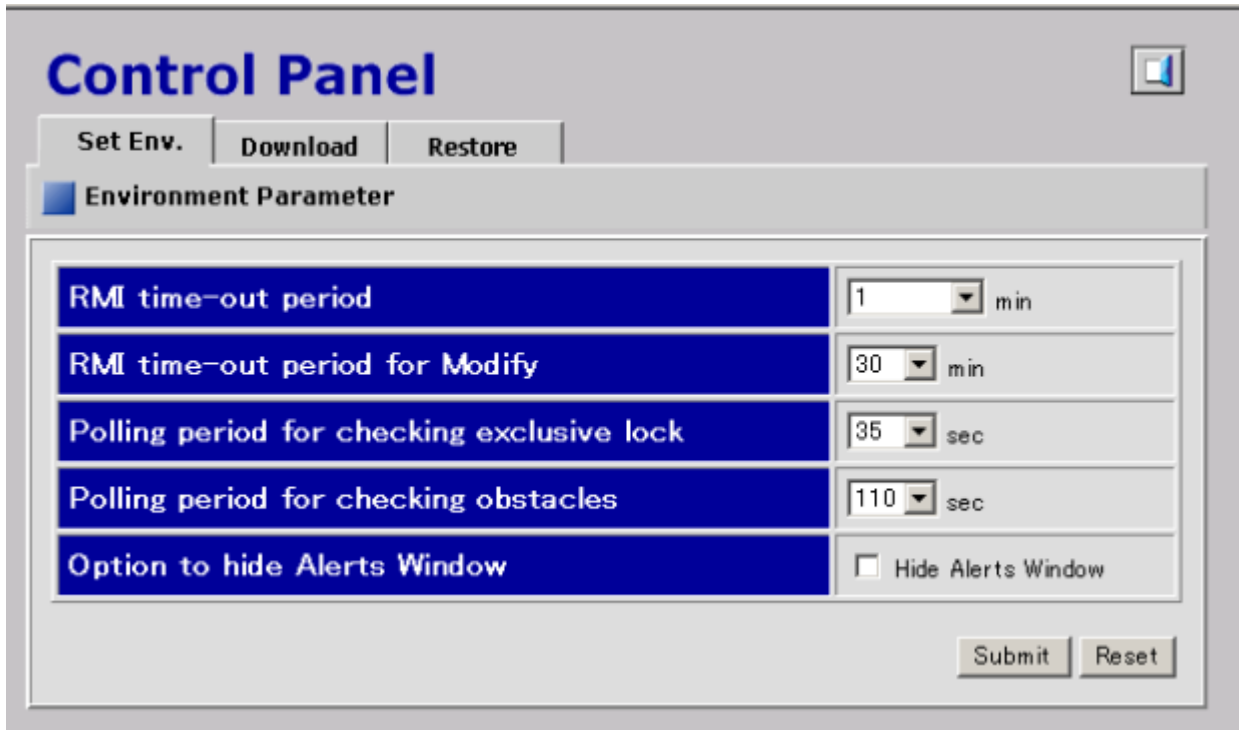
Figure F-1 Environment Parameter window

Item	Description
RMI time-out period	This parameter specifies the time-out period for forcible logout when the user performs no operation for a certain period of time because of a network error, etc.
RMI time-out period for Modify	This parameters specifies the time-out period for forcible release of Modify mode when the use is in Modify mode but does not make any changes that access the RMI server for a certain period of time.
Polling period for checking exclusive lock	This parameter specifies the polling period for monitoring who is changing information while in Modify mode when other users are viewing the storage system information in View mode.
Polling period for checking obstacles	This parameter specifies the time interval to monitor failure within the storage system.
Option to hide Alerts Window	This parameter specifies the whether to display the Alerts window.
Submit	Applies the environment parameters to the storage system.

Tool Panel GUI Reference

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide

Item	Description
Reset	Resets the environment parameter settings

Download File window

This section describes the Download File window features and controls.

Figure F-2 Download File window

Item	Description
Configuration File	Select the checkbox for the file to be downloaded. Downloadable configuration files differ according to the system configuration.
Submit	Downloads the configuration file.
Reset	Cancels downloading the configuration file.

Restore File window

This section describes the Restore File window features and controls.
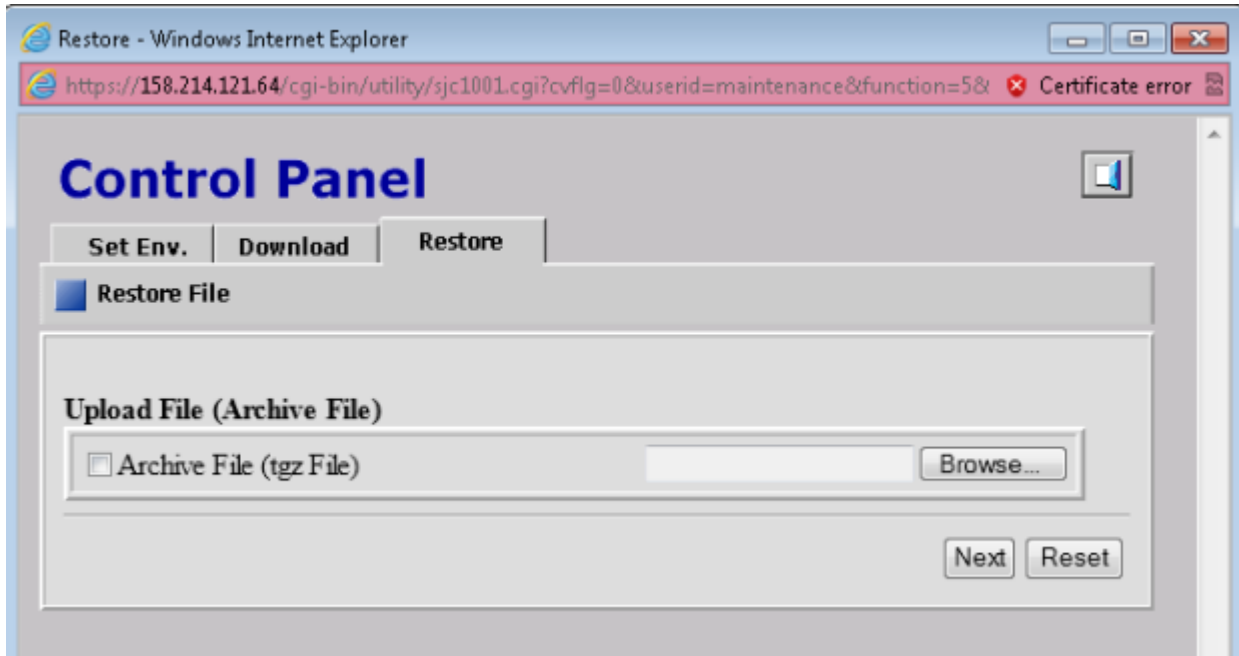
Figure F-3 Restore File window

Item	Description
Upload File (Archive File)	Click **Browse...** and specify the configuration file you want to restore.
Next	Displays a window for confirming the configuration file to be restored.
Reset	Cancels downloading the configuration file.

Download Dump Files window

This section describes the Download Dump Files window features and controls.

Tool Panel GUI Reference

Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide
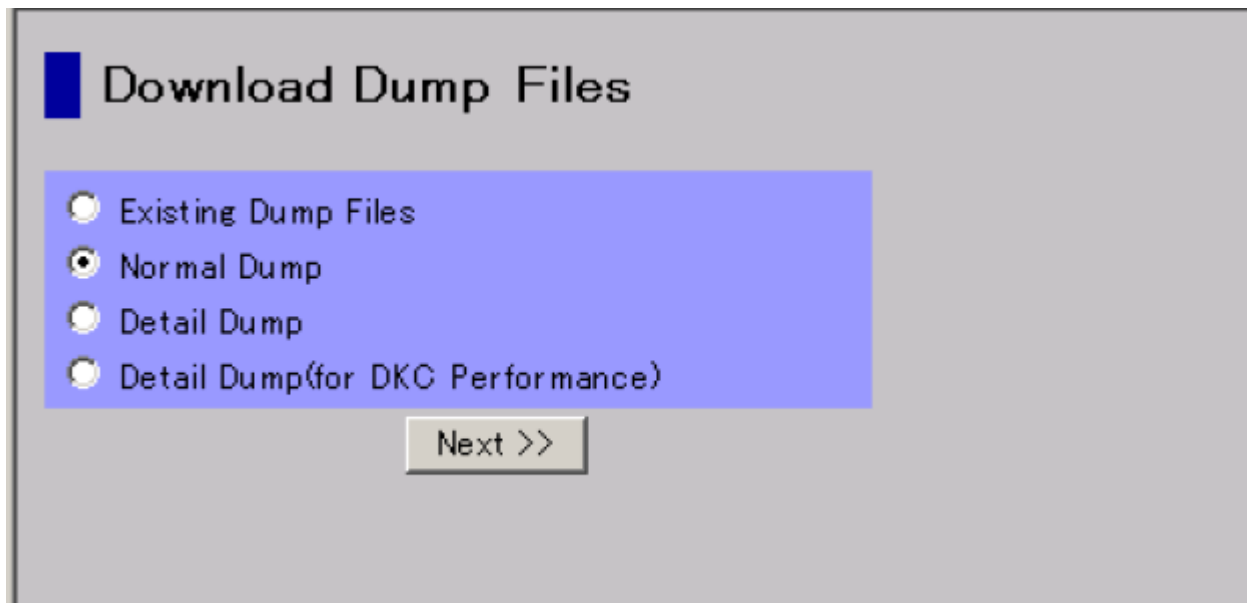
Figure F-4 Download Dump Files window

Item	Description
Existing Dump Files	Select this when you want to re-download a previously downloaded dump file. This item displays only when one or more compressed dump files exist. If you have not downloaded any dump files, this item does not display even though you have acquired dump files via the SVP.
Normal Dump	Contains all information about the SVP and minimum information about the storage system. Select Normal Dump when there is no fatal problem such as a problem with the display of Storage Navigator.
Detail Dump	Contains all information about the storage system in addition to the content of Normal Dump. Select this when you cannot start Storage Navigator or when you check for problems with the storage system.
Detail Dump (for DKC Performance)	Contains information about I/O performance, such as collecting Performance Monitor information in addition to the content of Detail Dump. Select this when you check for problems with the I/O performance.
Next	Displays a dialog box for confirm that the downloading of the dump file can start.

Update Certificate Files window

This section describes the Update Certificate Files window features and controls.
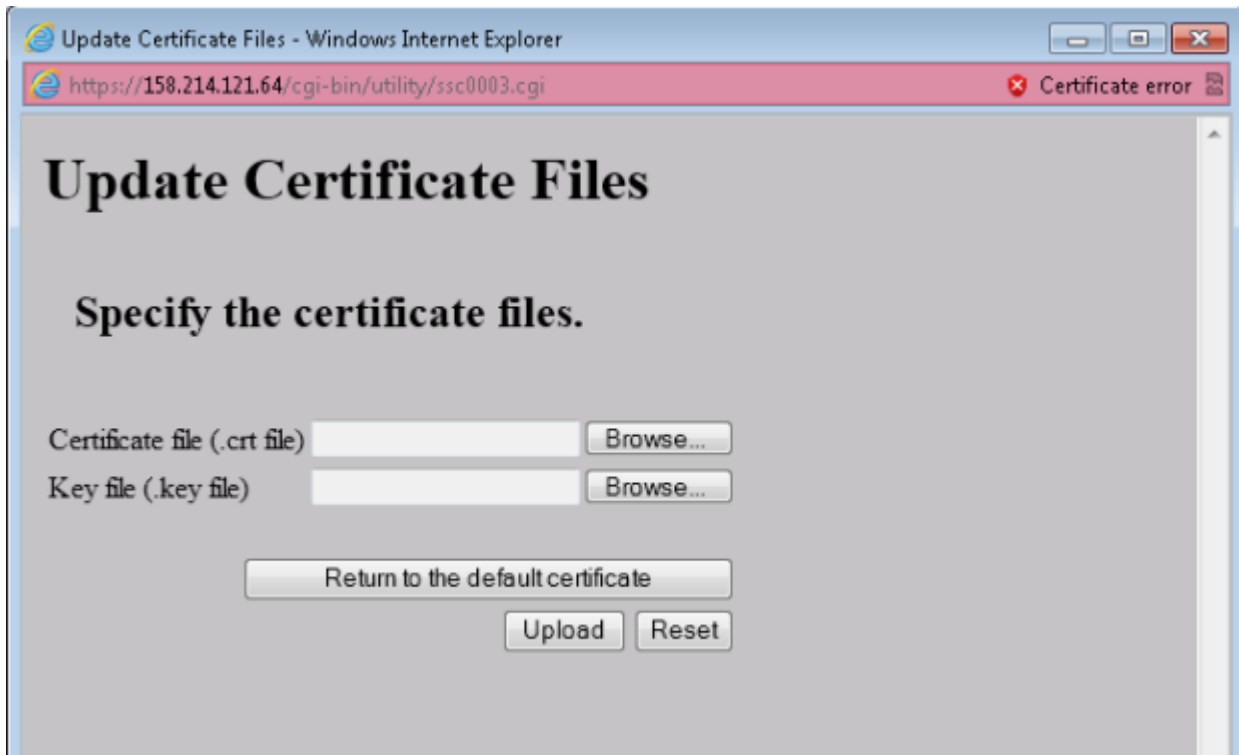
Figure F-5 Update Certificate Files window

Item	Description
Certificate file (.crt file)	Click **Browse...** and specify the certificate (server.crt file).
Key file (.key file)	Click **Browse...** and specify the key file (server.key file).
Return to the default certificate	Returns the certificate to default
Upload	Uploads the SSL certificate.
Reset	Cancels the upload of the SSL certificate.

Update Certificate Files for SMI-S window

This section describes the Update Certificate Files for SMI-S window features and controls.

Figure F-6 Update Certificate Files for SMI-S window

Item	Description
Certificate file (.crt file)	Click **Browse...** and specify the certificate file (server.crt file).
Key file (.key file)	Click **Browse...** and specify the key file (server.key file).
Return to the default certificate	Returns the SMI-S provider certificate to default.
Upload	Uploads the certificate to the SMI-S provider.
Reset	Cancels the upload of the SMI-S provider certificate.

Upload Configuration Files for SMI-S window

This section describes the Upload Configuration Files for SMI-S window features and controls.
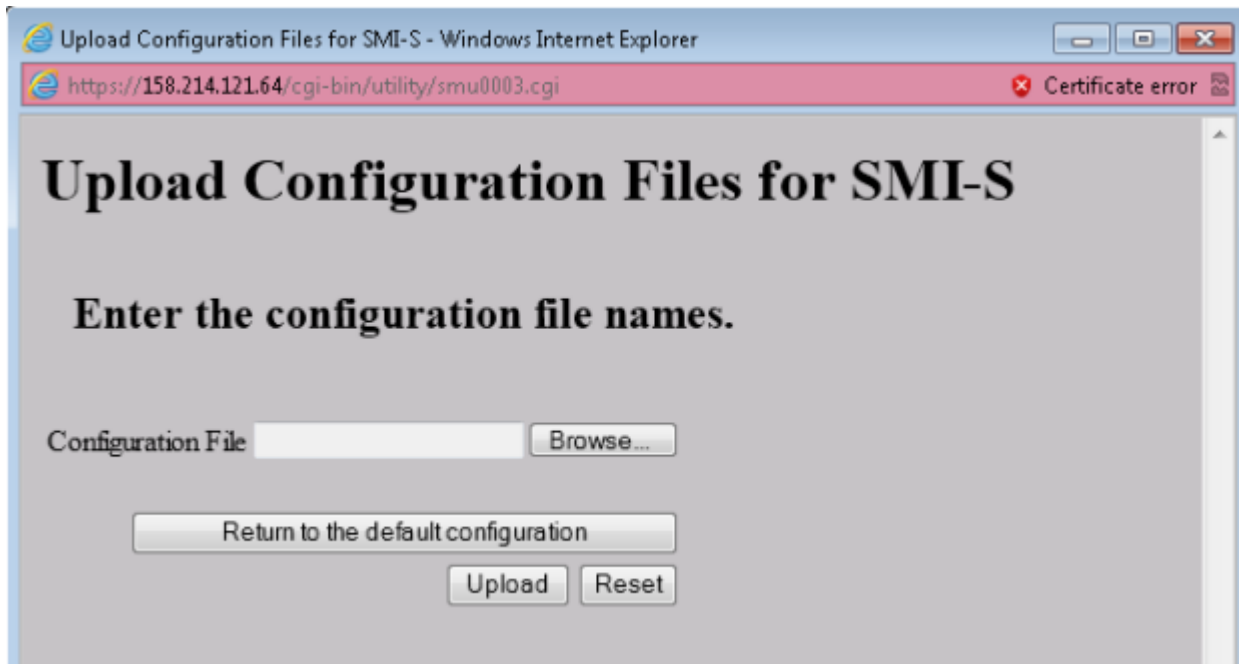
Figure F-7 Upload Configuration Files for SMI-S window

Item	Description
Configuration File	Click **Browse...** and specify the configuration file you want to upload.
Return to the default configuration	Returns the SMI-S provider configuration file to default.
Upload	Uploads the configuration file to the SMI-S provider.
Reset	Cancels the upload of the SMI-S provider configuration file.

Glossary

This glossary defines the special terms used in this document. Click the letter links below to navigate.

A

access attribute
The setting on a logical volume (mainframe or open-systems) that determines whether hosts can read and/or write to the volume.

APLB
active path load balancing

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

B

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

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

C

cache logical partition (CLPR)
> Consists of virtual cache memory that is set up to be allocated to different hosts in contention for cache memory.

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

CCI
> Command Control Interface

CHAP
> challenge handshake authentication protocol

CLPR
> cache logical partition

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

command device
> A dedicated logical volume used only by Command Control Interface to interface with the storage system. Can be shared by several hosts.

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

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

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

COW
> copy-on-write

COW Snapshot
Hitachi Copy-on-Write Snapshot

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

CVS
custom volume size

D

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

DB
drive box

DC
data center

device
A physical or logical unit with a specific function.

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

disk controller (DKC)
The hardware component that manages front-end and back-end storage operations. The term DKC is sometimes used to refer to the entire RAID storage system.

DKC
See *disk controller.*

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

E

emulation
The operation of the Hitachi RAID storage system to emulate the characteristics of a different storage system. For device emulation the mainframe host "sees" the logical

devices on the RAID storage system as 3390-x devices. For controller emulation the mainframe host "sees" the control units on the RAID storage system as 2105 or 2107 controllers.

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

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

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

F

FC
fibre channel; FlashCopy

FC-AL
fibre-channel arbitrated loop

FCP
fibre-channel protocol

FD Dump Tool
Downloads Storage Navigator configuration information onto disk for backup and troubleshooting purposes.

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

FMD
See flash module

H

HBA
host bus adapter

HDD
hard disk drive

host group
A group of hosts of the same operating system platform.

host mode

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

host mode option

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

I

internal volume

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

in-system replication

The original data volume and its copy are located in the same storage system. ShadowImage in-system replication provides duplication of logical volumes; Copy-on-Write Snapshot in-system replication provides "snapshots" of logical volumes that are stored and managed as virtual volumes (V-VOLs).
See also *remote replication*.

J

JNL

journal

journal volume

A volume that records and stores a log of all events that take place in another volume. In the event of a system crash, the journal volume logs are used to restore lost data and maintain data integrity.
In Universal Replicator, differential data is held in journal volumes on until it is copied to the S-VOL.

JRE

Java Runtime Environment

K

keypair

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

Key management server

A server to manage encryption keys. In Hitachi Virtual Storage Platform the user can back up and restore encryption keys on a key management server compliant to Key Management Interoperability Protocol (KMIP).

L

LDAP

lightweight directory access protocol

LDEV

logical device

LDKC

See *logical disk controller (LDKC)* .

license key

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

local copy

See *in-system replication*.

logical device (LDEV)

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

logical disk controller (LDKC)

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

logical partition (LPAR)

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

logical unit (LU)

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

logical volume
    See *volume*.

LU
    See logical unit

LUN
    See logical unit number

LUSE
    Hitachi LUN Expansion; Hitachi LU Size Expansion

M

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

MLC
    Multi-level cell (two cell) flash memory used in solid state drives. Less expensive and slower than SLC (single-level cell) flash memory.

O

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

P

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

parity group
    See *RAID group*.

PAV
    Parallel Access Volume

PDEV
physical device

PG
parity group. See *RAID group*.

physical device
See *device*.

pool
A set of volumes that are reserved for storing Copy-on-Write Snapshot data or Dynamic Provisioning write data.

pool volume (pool-VOL)
A logical volume that is reserved for storing snapshot data for Copy-on-Write Snapshot operations or write data for Dynamic Provisioning.

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

PP
program product

primary volume (P-VOL)
The volume in a copy pair that contains the original data to be replicated. The data on the P-VOL is duplicated synchronously or asynchronously on the secondary volume (S-VOL).
The following Hitachi products use the term P-VOL: Thin Image, Copy-on-Write Snapshot, ShadowImage, TrueCopy, Universal Replicator, Universal Replicator for Mainframe, and High Availability Manager.
See also *secondary volume (S-VOL)*.

prio
priority mode. Used in Cache Residency Manager.

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

Q

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

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

R

RAID
    redundant array of independent disks. A disk array in which part of the physical storage space is used to store user data and parity information, and another part is used to store a duplicate set of user data and parity information. This redundant configuration prevents data loss in case a disk drive within the RAID configuration fails, and enables regeneration of user data in the event that one of the array's member disks or the access path to it fails.

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

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

RCU
    See *remote control unit (RCU)* .

remote copy
    See *remote replication*.

RMI
    Remote Method Invocation

S

SAS
    serial-attached SCSI

secondary volume (S-VOL)
    The volume in a copy pair that is the copy of the original data on the primary volume (P-VOL). The following Hitachi products use the term "secondary volume":Thin Image,

Copy-on-Write Snapshot, ShadowImage, TrueCopy, Universal Replicator, Universal Replicator for Mainframe, and High Availability Manager.
See also *primary volume (P-VOL)* .

service information message (SIM)
SIMs are generated by a HUS VM storage system when it detects an error or service requirement. SIMs are reported to hosts and displayed on Storage Navigator.

Service Processor
The computer in a HUS VM storage system that hosts the Storage Navigator software and is used to configure and maintain the storage system.

severity level
Applies to service information messages (SIMs) and Storage Navigator error codes.

SFP
small form-factor pluggable

shredding
See *volume shredding*.

SIM
See *service information message*

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

SLC
Single-level cell (one cell) flash memory used in solid state drives. More expensive and faster than MLC (multi-level cell) flash memory.

SM
shared memory

SMTP
simple mail transfer protocol

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

SNMP
simple network management protocol

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

SSD
    solid-state drive. Also called flash drive.

SSID
    storage subsystem ID. SSIDs are used for reporting information from the CU to the mainframe operating system. Each group of 64 or 256 volumes requires one SSID, so there are one or four SSIDs per CU image. The user-specified SSIDs are assigned during storage system installation and must be unique to all connected host operating environments.

SSL
    secure socket layer

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 disk
    The volume from which an open-systems host boots.

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

V

VDEV
    See *virtual device (VDEV)* .

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

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

virtual volume (V-VOL)

The secondary volume in a Copy-on-Write Snapshot pair. When in PAIR status, the V-VOL is an up-to-date virtual copy of the primary volume (P-VOL). When in SPLIT status, the V-VOL points to data in the P-VOL and to replaced data in the pool, maintaining the point-in-time copy of the P-VOL at the time of the split operation.

When a V-VOL is used with Dynamic Provisioning, it is called a DP-VOL.

VM

virtual machine; volume migration;

volume

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. A mainframe volume is called a logical volume image (LVI), and an open-systems volume is called a logical unit. (LU).

VSP

Hitachi Virtual Storage Platform

V-VOL

virtual volume

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Index

Index-2

Index-4

Hitachi Data Systems

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

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

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

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

Hitachi Data Systems