Hitachi Virtual Storage Platform E Series

SVOS RF 9.8.2

System Administrator Guide

This document describes the management software for the VSP E series storage systems (for example, Maintenance Utility, Device Manager - Storage Navigator) and provides instructions for setting up and administering the storage systems.

MK-97HM85028-16
May 2022

© 2018, 2022 Hitachi, Ltd. All rights reserved.

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

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

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

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

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

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

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

Hitachi and Lumada are trademarks or registered trademarks of Hitachi, Ltd., in the United States and other countries.

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, Lotus, MVS, OS/390, PowerHA, PowerPC, RS/6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

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

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

Copyright and license information for third-party and open source software used in Hitachi Vantara products can be found at https://www.hitachivantara.com/en-us/company/legal.html or https://knowledge.hitachivantara.com/Documents/Open_Source_Software.

Contents

Preface

This document describes the management software for the storage systems and provides instructions for performing system administration tasks for these storage systems. This document also provides instructions for configuring and using the Hitachi Device Manager - Storage Navigator (HDvM - SN) software.

Please read this document carefully to understand how to use the software described in this manual, and keep a copy for reference.

Intended audience

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

Readers of this document should be familiar with the following:

- Data processing and RAID storage systems and their basic functions.
- The *Hardware Guide* for your storage system.
- The operating system and web browser software on the management client.

Product version

This document revision applies to the following product versions:

- VSP E series: 93-06-4*x* or later
- SVOS RF 9.8.2 or later

Release notes

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

Changes in this revision

- Added SMI-S support for VSP E590 and VSP E790 (Using the SMI-S function on the HDvM - SN management client (on page 114)).
- Added system option modes (SOMs) 1201 and 1273 (System option modes (on page 330)).

Document conventions

This document uses the following typographic conventions:

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

Convention	Description
	[a | b] indicates that you can choose a, b, or nothing. { a | b } indicates that you must choose either a or b.

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

Icon	Label	Description
	Note	Calls attention to additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Important	Highlights information that is essential to the completion of a task.
	Caution	Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash).
	CAUTION	Warns the user of a hazardous situation that, if not avoided, could result in major or minor injury.
	WARNING	Warns the user of a hazardous situation which, if not avoided, could result in death or serious injury.

Conventions for storage capacity values

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

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

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

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

Accessing product documentation

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

Getting help

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

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

Comments

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

Thank you!

Chapter 1: Overview of system administration

System administration of the Hitachi Virtual Storage Platform E series (VSP E series) storage systems involves initial setup and configuration of the management client and storage system and ongoing tasks such as adding users, managing software licenses, and monitoring storage system events and alerts.

System administration tasks and workflow

After storage system installation is complete, the first system administration task is to configure the management client for the storage system. The management client is the computer used to log in to and manage the storage system. The management client is LAN-attached to the storage system and communicates with the service processor (SVP) or with the controllers if the storage system does not have an SVP. You can configure the management client and storage system for secure communications (SSL), and you can set up user authentication and authorization for the management software.

When configuration of the management client is complete, you can perform the initial configuration of the storage system. Initial storage system configuration includes tasks such as entering the storage system information (name, location, contact information), setting the date and time, creating a login message, and setting up the syslog server for the audit logs.

After initial setup and configuration of the management client and storage system are complete, the storage system is ready for use. The ongoing system administration activities include the following:

- Adding users and managing users and user groups
- Managing resource groups
- Monitoring storage system events and alerts
- Managing software licenses

Management tools for system administration

The storage systems support several management tools for system administration, including software that is embedded on the controllers of the storage system and software that is installed on a server connected to the storage system. These management tools are accessed from a management (SSH) client on the management LAN for the storage system.

Maintenance utility

The maintenance utility, which is embedded on the controllers, displays storage system information and allows you to perform basic configuration and administration

tasks on the storage system, including initial setup (for example, date and time, network settings), user administration, software license management, and audit log settings. You can access and log in to the maintenance utility directly from the management client. In addition, you can access the maintenance utility by launching it from Hitachi Storage Advisor Embedded, Hitachi Device Manager - Storage Navigator, or Hitachi Ops Center Administrator.

Hitachi Storage Advisor Embedded (HSAE)

The HSAE software allows you to easily configure storage system resources such as volumes and pools and perform daily operations such as backing up data and monitoring. You can perform operations by using the HSAE web-based user interface or by using REST API, executed automatically as scripts or incorporated into business applications.

Embedded Command Control Interface (CCI)

The embedded CCI software, also on the controllers, enables you to perform storage system configuration and provisioning operations by issuing commands to the storage system. You can access embedded CCI from an SSH client on the management LAN. When the SSH client connects successfully, the CCI user session is created.

Hitachi Device Manager - Storage Navigator (HDvM - SN)

HDvM - SN runs on the service processor (SVP) for the storage system. HDvM - SN displays detailed information about the storage system and allows you to perform configuration, administration, and data management operations. You can log in to HDvM - SN directly from the management client, or you can access HDvM - SN by launching it from Hitachi Ops Center Administrator.

Command Control Interface (CCI)

CCI enables you to perform data management operations (replication, protection) as well as storage system configuration and provisioning operations by issuing commands directly to the storage system. CCI provides powerful command-line control and advanced functionality for your storage system. CCI commands can be used interactively or in scripts to automate and standardize storage administration functions.

Hitachi Ops Center Administrator

Ops Center Administrator reduces the complexity of managing storage systems by simplifying the setup, management, and maintenance of storage resources. Ops Center Administrator has intuitive graphical user interfaces and recommended configuration practices to streamline system configurations and storage management processes.

REST APIs

REST-based APIs extend operations, enabling integration with existing toolsets and automation templates to further simplify and consolidate management tasks. For details about API integration solutions, contact your Hitachi Vantara representative.

Chapter 2: Accessing the storage system

Initial setup and configuration of the storage system includes configuring the management client to access the storage system. The management client is LAN-attached to the storage system and communicates with the service processor (SVP) or with the controllers if the storage system does not have an SVP.

Note:

- VSP E990 supports the physical and virtual SVP with full functionality (Device Manager - Storage Navigator, KMIP, and so on).
- VSP E1090, VSP E790, and VSP E590 support only the virtual SVP and only for enabling and administering VVOL/VASA, SMI-S, and KMIP operations.

Initial setup of the management client

The management client is the computer used to log in to and manage your storage system. The management client is LAN-attached to the storage system and communicates with the service processor (SVP) or with the controller if your storage system does not have an SVP. If your storage system is equipped with an SVP, you can use Hitachi Device Manager - Storage Navigator (HDvM - SN) as well as other management software such as Hitachi Ops Center Administrator to manage your storage system. If your storage system does not have an SVP, you can use the Maintenance Utility and other embedded tools such as Hitachi Storage Advisor Embedded (HSAE) to manage your storage system.

Workflow for setting up the management client

Before you can start managing the storage system, you must set up a management client to use the management software for your storage system. Perform the following tasks to set up the management client for use of Device Manager - Storage Navigator (HDvM - SN).

1. Confirm that the management client meets the hardware and software requirements for running HDvM - SN (Requirements for management clients (on page 20)).
2. Configure the management client to connect through a firewall (Connecting through a firewall (on page 23)).
3. Set up IPv4/IPv6 communications on the management client (Setting up IPv4/IPv6 communications (on page 24)).
4. Register the primary SVP host name on the management client (Registering the SVP host name (on page 25)).
5. Configure the web browser on the management client (Configuring the web browser on the management client (on page 25)).

6. For a management client running Windows, add the SVP to the trusted sites zone (Adding your SVP to the trusted sites zone for Windows Server computers (on page 26)).
7. Enable JavaScript for Windows (Enabling JavaScript for Windows (on page 27)).
8. Install Captive Bundle Application on the SVP (Installing Captive Bundle Application (CBA) on the SVP (on page 28)). CBA is required to use HDvM - SN with Adobe® AIR® from HARMAN™.
9. Install Storage Device Launcher on the management client (Installing Storage Device Launcher on the management client (on page 29)). Storage Device Launcher is required to use HDvM - SN with Adobe AIR from HARMAN.
10. Configure the management client for the HDvM - SN secondary window (Configuring the management client for the HDvM - SN secondary window (on page 39)).

Requirements for management clients

The Device Manager - Storage Navigator administrator is responsible for setting up management clients. Device Manager - Storage Navigator runs on supported versions of the Windows and UNIX/Linux operating systems. If you use a physical or virtual server running on Windows as a management client, you must configure the server to run Device Manager - Storage Navigator.

General requirements

- The management client must be connected to the network via LAN. Device Manager - Storage Navigator connects to the SVP through a TCP/IP network.
- Use category 5e or 6a LAN cable for LAN connections when the transfer speed is 1 Gbps. Maximum cable length is 328 feet (100 meters). For assistance, contact customer support.
- Several storage systems can be managed by one management client. Device Manager - Storage Navigator must be set up for each storage system.
- A maximum of 32 management clients (Device Manager - Storage Navigator) can access the same storage system at the same time.

Requirements for Windows-based management clients

The management client must meet hardware and software requirements to run Device Manager - Storage Navigator (HDvM - SN) in a Windows® environment.

Hardware requirements for the management client (Windows)

Item	Requirement
Processor (CPU)	Pentium 4 640 3.2 GHz or better (Not dependent on a specific CPU vendor and processor family. Core2Duo E6540 2.33 GHz or better is recommended.)

Item	Requirement
Memory (RAM)	2 GB or more Recommended: 3 GB
Available storage space	500 MB or more (+ 80 MB for each managed storage system) When HDvM - SN is using Adobe® AIR® from HARMAN™, an additional 80 MB of free space is required for each storage system managed by HDvM - SN.
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-TX 1000BASE-T

Software requirements for the management client (Windows)

Set the locale of the HDvM - SN management client to either English or Japanese. The storage management software and SVP software installed on the SVP support only English and Japanese.

On a Windows management client, you can use HDvM - SN with Adobe AIR from HARMAN. The following table specifies the requirements for using HDvM with AIR. The combinations and versions of operating system, architecture, browser, and TLS specified below are fixed requirements. Using other combinations or versions might produce unpredictable results such as the inability to use the HDvM - SN windows.

Note: Use software that is supported by the manufacturer. Behavior is not guaranteed for software whose support period has expired.

Requirements for using HDvM with AIR from HARMAN

Operating system	Architecture	Web browser	TLS
Windows 10	64 bit	Microsoft Edge 92.0 or later[1] Google Chrome 63.0 or later Internet Explorer 11.0[2, 3]	TLS1.2 TLS1.2 must be enabled. AIR does not support TLS1.3.
Windows 8.1	64 bit	Microsoft Edge 92.0 or later[1] Google Chrome 48.0 or later Internet Explorer 11.0[2, 3]	

Notes:

1. Microsoft Edge is supported on the SVP with firmware version 93-05-04/xx or later.

Operating system	Architecture	Web browser	TLS
2. Use Microsoft Edge or Google Chrome instead of Internet Explorer because Microsoft plans to end support for Internet Explorer in June, 2022. **3.** Only the latest version of Internet Explorer that runs on each operating system is supported according to Microsoft® Support Policy.			

Note: Some Device Manager - Storage Navigator operations are performed through the HDvM - SN secondary window that runs within Java.

Requirements for UNIX/Linux-based management clients

The management client must meet hardware and software requirements to run Device Manager - Storage Navigator (HDvM - SN) in a UNIX® or Linux® environment.

Hardware requirements for the management client (UNIX/Linux)

Item	Requirement
Processor (CPU)	Pentium 4 640 3.2 GHz or better (Recommended: Core2Duo E6540 2.33 GHz or better)
Memory (RAM)	2 GB or more Recommended: 3 GB
Available storage 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-TX 1000BASE-T

Software requirements for the management client (UNIX/Linux)

Set the locale of the HDvM - SN management client to either English or Japanese. The storage management software and SVP software installed on the SVP support only English and Japanese.

The following table specifies the software requirements for using HDvM - SN in a UNIX or Linux environment. The combinations of operating system, architecture, browser, and Java Runtime Environment described below are fixed requirements. Using other combinations or versions might produce unpredictable results such as the inability to use the HDvM - SN windows.

Operating system	Architecture	Browser	Java Runtime Environment (JRE)
Red Hat Enterprise Linux 7.4	64 bit	Google Chrome 63.0 or later	JRE 8.0 Update 152
		Google Chrome 63.0 or later	OpenJDK 11.0.1+13
		Firefox 58.0 or later*	JRE 8.0 Update 152
		Firefox 58.0 or later*	OpenJDK 11.0.1+13
Red Hat Enterprise Linux 7.5	64 bit	Google Chrome 69.0 or later	JRE 8.0 Update 171
		Google Chrome 69.0 or later	OpenJDK 11.0.1+13
		Firefox 60.0 or later*	JRE 8.0 Update 171
		Firefox 60.0 or later*	OpenJDK 11.0.1+13
* IPv6 HTTPS connection from Firefox is not supported.			

Connecting through a firewall

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

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

The following table shows the type of the protocol and the port used. When accessing the management GUI directly from the SVP without using the management client, it is not necessary to register ports of protocols other than RMI, SLP, and SMI-S in the table below.

Caution: Do not set firewall for ICMP configuration. If you do, alert notifications might not occur. To disable the settings, contact the administrator who manages the firewall.

Note: If you change the port numbers used by the SVP, the firewall is set with the changed port numbers.

Protocol	Port number	Direction of communication
HTTP	80	From the Device Manager - Storage Navigator web client to the SVP

Protocol	Port number	Direction of communication
HTTPS	443	
RMI	1099	
RMI (SSL)	5443	
RMI	51099	
RMI	51100-51355	
SLP	427	
SMI-S	5989-6244	

Setting up IPv4/IPv6 communications

You should assign the SVP the same type of IP addresses (IPv4 or IPv6) as those used on the storage system. You must also configure the client computers with the same IP version that you assign to the SVP. In addition, use the same communication options for the management client and the SVP. If the SVP uses IPv6, you must configure the management clients to use IPv6 for communication.

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

Configuring IPv6 communication in Windows 7

If the SVP uses IPv6, you must configure Windows 7 management clients to use IPv6 for communication.

Procedure

1. Select **Control Panel** > **Network and Sharing Center** > **Manage network connections**.
2. Right-click the network where the SVP resides, and then click **Properties** in the pop-up menu.

   If the User **Account Control** dialog box opens click **Continue**. Otherwise, the **Networking** dialog box opens.
3. In the **Networking** dialog box, clear the **Internet Protocol Version 4 (TCP/IPv4)** check box.
4. Click **OK** to save the changes and close the dialog box.

Configuring IPv6 communication in Solaris 10

If the SVP uses IPv6 and you plan to use Device Manager - Storage Navigator (HDvM - SN) in a web browser, you must configure Solaris 10 management clients to use IPv6 for

communication. If you plan to run HDvM - SN using Adobe AIR, you do not need to perform this task.

Procedure

1. Start a command window or system console.
2. Execute the following command:

```
ifconfig network-interface-name inet down
```

Registering the SVP host name

You must register the SVP host name before you can complete any of the following tasks.

Note: If the SVP High Reliability Kit is installed, the storage system has two SVPs: the primary SVP, and the standby SVP that can be used if the primary SVP becomes unavailable. You must register the primary SVP host name.

- Specifying a host name instead of an IP address when accessing Device Manager - Storage Navigator.
- Obtaining the public key certificate for SSL-encrypted communication from the CA (Certificate Authority). You must register the server name as the host name to the DNS server or the hosts file. The server name is entered in the certificate as a common name.

  Enter the SVP host name and IP address in the DNS server or hosts file of the management client. You can register any host name to the DNS server or the hosts file, but there are restrictions on the characters you can use for the host name.
- Registering the IP address and host name of the SVP to the DNS server that manages the network to which the SVP is connected.
- Entering the IP address and host name of the SVP to the hosts file of the management client. The general directory of the hosts file is:
  - For Windows: `C:\Windows\System32\drivers\etc\hosts`
  - For UNIX: `/etc/hosts`

Caution: If the host name listed in the hosts file is also listed in the CCI configuration definition file, CCI must be restarted.

Configuring the web browser on the management client

Configure the web browser on the Hitachi Device Manager - Storage Navigator (HDvM - SN) management client as described below.

Web browser settings

- The browser must allow first-party, third-party, and session cookies.
- The pop-up blocker and plug-ins must be disabled.
- The browser must be configured to use TLS 1.2.

- Settings for Microsoft Edge:
  - Enable cookies (**Settings** > **Cookies and site permissions** > **Manage and delete cookies and site data** > **Allow sites to save and read cookie data (recommended)**).
  - Allow pop-ups (**Settings** > **Cookies and site permissions** > **Pop-ups and redirects** > **Add**, and then enter the IP address or host name of the SVP).
- Settings for Windows Server 2016, Windows Server 2012 Update, Windows Server 2012 R2 Update, Windows Server 2012, and Windows 8.1, JavaScript must be enabled. For details, see Enabling JavaScript for Windows (on page 27).
- Settings for Windows Server and Internet Explorer:
  - Configure Internet Explorer so it does not save encrypted pages to disk (**Tools** > **Internet Options** > **Advanced** > **Do not save encrypted pages to disk**).
  - Register the URL of the SVP in Internet Explorer (**Tools** > **Internet Options** > **Security**).
  - For Windows Server 2012, set the IE security level for the trusted sites to **Medium-high** (**Tools** > **Internet Options** > **Security** > **Trusted sites** > **Security level for this zone**).
- For the Japanese version of Firefox, the browser must be configured to use the C locale (default system language) by using the X Server Emulator.

  In a B Shell, enter the following command:

  ```
  LANG=C
  export LANG
  ```

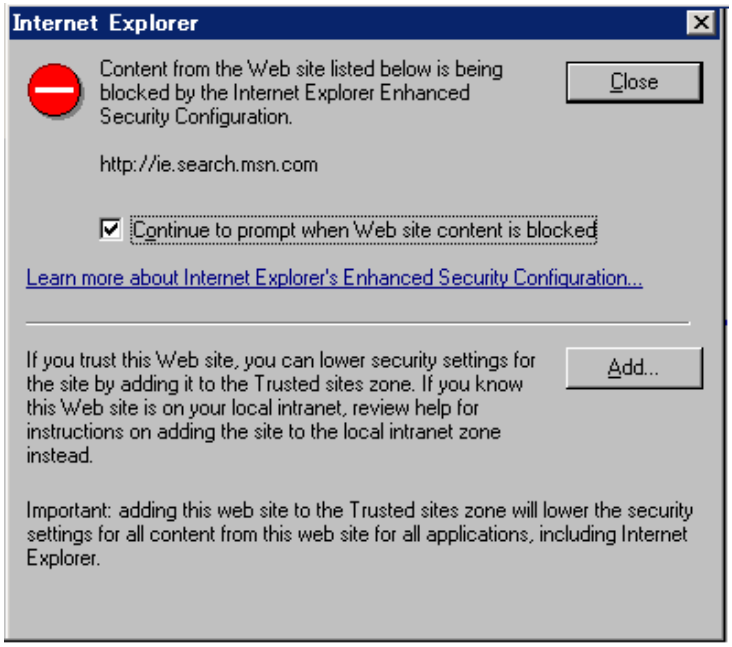
  In a C Shell, enter the following command:

  ```
  setenv LANG C
  ```

Adding your SVP to the trusted sites zone for Windows Server computers

If you are using Device Manager - Storage Navigator on a Windows Server computer, the following message may appear during login. If it does, you must add the SVP to the trusted sites zone.

The message below may appear differently depending on the Windows version you are using.



Procedure

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.

Enabling JavaScript for Windows

You must enable JavaScript if you use any of the following Windows versions:

- Windows Server 2016
- Windows Server 2012 R2 Update
- Windows Server 2012 Update
- Windows 10
- Windows 8.1

Note: This setting is required when you use Device Manager - Storage Navigator in a browser and when you use Device Manager - Storage Navigator with Adobe AIR.

Procedure

1. In Edge, enable the **Allow** setting for JavaScript:
   a. Open the **Settings** window (click the Settings and more icon (···), and then click **Settings** from the drop-down menu).

b. Select **Cookies and site permissions** in the left pane, and then click **JavaScript** in the right pane.
c. In the right pane, set **Allow (recommended)** to enabled.
d. Exit and then restart Edge.

2. In Internet Explorer, enable the **Active scripting** security setting:
   a. Open the **Internet Options** window (**Tools** > **Internet Options**).
   b. Click the **Security** tab, and then click **Custom Level**.
   c. On the **Security Settings - Internet Zone** window, set **Active scripting** to **Enable**, and then click **OK**.
   d. Click **YES** on the **Warning** dialog box, and then click **OK**.
   e. Exit and then restart Internet Explorer.

Installing Captive Bundle Application (CBA) on the SVP

Captive Bundle Application (CBA) is the application on the SVP that enables HDvM - SN to run with Adobe AIR from HARMAN. Before you can use HDvM - SN with AIR, you must install CBA on the SVP. If you are using one SVP to manage multiple storage systems, you must install CBA for each storage system.

Before you begin

- You must have the serial number of the storage system. The serial number is displayed in S/N in the Storage Device List window on the SVP.

Procedure

1. Close all HDvM - SN sessions connected to the storage system for which you are installing CBA.
2. Log in to the SVP.
3. Open a command prompt on the SVP with administrator permissions.
4. Move the current directory to the folder containing the `MappCbaUpload.bat` batch file (for example, `C:\MAPP\wk\Supervisor\MappIniSet`).
5. Run the batch file specifying the storage system serial number and the CBA file (with absolute path) as arguments as follows:

   ```
   MappCbaUpload.bat serial-number CBA-file
   ```

   For example:

   ```
   MappCbaUpload.bat 400102 C:\temp\CBA-file-name
   ```

6. When the completion message is displayed, press any key to exit the processing.
7. Close the command prompt window.

Next steps

After installing Captive Bundle Application (CBA) on the SVP, you need to install Storage Device Launcher on the management client. For instructions, see Installing Storage Device Launcher on the management client (on page 29).

Installing Storage Device Launcher on the management client

The Storage Device Launcher application is required to run Hitachi Device Manager - Storage Navigator (HDvM - SN) with Adobe AIR from HARMAN. Storage Device Launcher is included in the Web Console Launcher setup file on the SVP. Use the following procedure to download and install Storage Device Launcher on the management client.

Caution: If you use other management software to access HDvM - SN (for example, Hitachi Ops Center Administrator), install Storage Device Launcher as a user with administrator permissions on the management client.

Note: If you are using one management client to access multiple storage systems, you only need to install Storage Device Launcher on the management client once.

Before you begin

- You must have the model identification number of the storage system. The model identification number is the same as the folder name of the SVP firmware installation directory.

  Example: `C:\Mapp\wk\936000400001`

  - In this example, the 12-digit character string `936000400001` is the model identification number. The last 6 digits indicate the serial number of the storage system.
  - `C:\Mapp` is the default installation directory for the SVP firmware. The location of the installation directory depends on the conditions specified when the SVP firmware was installed.

  If multiple storage systems are registered on the SVP, you can use the model identification number of any storage system whose SVP firmware version supports AIR.

Procedure

1. Download the Web Console Launcher setup file for Windows from the SVP to the management client.
   - If you can log in to HDvM - SN by using a web browser, click **Tool** > **Download** in the HDvM - SN menu bar, and then download the Web Console Launcher setup file for Windows (`WCLauncher_win.zip`).
   - If you cannot log in to HDvM - SN by using a web browser, open the download the Web Console Launcher setup file as follows:
     a. Open a web browser on the management client, and enter the following URL:

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

```
number-of-storage-system
```

If you changed the port number of the protocol HTTPS from the initial value (443 by default), specify the following URL:

```
https://IP-address-or-host-name-of-SVP:port-number-of-protocol-HTTPS/
sanproject/ToolDownload/serial-number-of-storage-system
```

Note: If the SVP firmware version is earlier than 93-02-02/xx, enter the following URL instead:

```
https://IP-address-or-host-name-of-SVP(:port-number-of-
protocol-HTTPS)/dev/storage/model-identification-number/htdocs/
tool/tooldownload.html
```

After the download page opens, go to step (c).

b. In the authentication window, enter the user name and password.

c. Download the Web Console Launcher setup file for Windows (`WCLauncher_win.zip`).

2. Expand the downloaded Web Console Launcher setup file.

Make sure to expand the setup file in a folder or directory that meets the following requirements:

- Use only 1-byte alphanumeric characters for the expanded folder or directory name.
- Use an expanded folder (excluding directly under C: drive) that can be accessed (Read/Write) by management client users who do not have administrator permissions.
- If you are installing Storage Device Launcher two or more times on the same management client, expand the setup file each time in the same folder or directory (the one used for the initial installation). If you expand the setup file in a different folder or directory from the first installation, other users will not be able to run Storage Device Launcher.

Note: If a security warning or a window blocking the operation is displayed, do not expand the setup file. Change the properties of the setup file as follows and then expand the file:

a. Right-click `WCLauncher_win.zip`, and then click **Properties**.

b. In **Security**, select **Unblock**, and then click **OK**.

3. Install Storage Device Launcher as follows:
   - If you are logged in to the management client with administrator permissions, right-click `WCLauncher_win\WCLauncher\Setup_SDLauncher.bat`, and run it by selecting **Run as Administrator**.
   - If you are not logged in to the management client with administrator permissions:
     a. Right-click `WCLauncher_win\WCLauncher\Setup_SDLauncher.bat`, and then click **Create Shortcut**.
     b. Move the created shortcut onto the desktop.
4. Open `WCLauncher_win\WCLauncher\log\Setup.log` with a text editor, and confirm that "completed" is displayed.

Caution: Do not move or delete the `WCLauncher_win` folder after Storage Device Launcher installation is complete. This folder contains files required for running Storage Device Launcher.

Next steps

After installing Storage Device Launcher on the management client, you can log in to HDvM - SN using AIR. For instructions, see Logging in to HDvM - SN by using AIR (on page 34).

Logging in to HDvM - SN in a browser

There are three ways to log in to Device Manager - Storage Navigator (HDvM - SN) running in a web browser:

- If you are an administrator, you can log in to HDvM - SN with a one-time-only initial login.
- If you are a superuser, you can log in first to HDvM - SN to create other user accounts.
- If you are a HDvM - SN user or administrator, you can log in normally.

Note:

- If you cannot log in three times with the same user ID, HDvM - SN stops responding for one minute. This is for security purposes and is not a system failure.
- The operations (roles) and resource groups that the logged-in user can access are determined when the user logs in. If the roles or resource allocations are changed while the user is logged in, the changes will take effect the next time the user logs back in.

Initial superuser login

When you log in to the storage system for the first time, you must log in as the superuser (includes all permissions) so you can set up the other user accounts.

Important:

- To prevent unauthorized use of the superuser account, you must change the password for the superuser account immediately after the initial login.
- To prevent unauthorized access to the functions available to service representatives, you must create user accounts that do not have the "Support Personnel (Vendor Only)" role and that have limited access to individual tools. Users that have the "Support Personnel (Vendor Only)" role can perform the same operations as service representatives.

Use the following procedure to log in for the first time by using Device Manager - Storage Navigator.

Procedure

1. Contact customer support to obtain the superuser ID and password.
2. Start a web browser on the management client.
3. In the web browser, enter the URL for your SVP:

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

   If you changed the port number of the HTTP protocol from the initial value (443), specify the following URL:

   ```
   https://IP-address-or-host-name-of-SVP:port-number-of-the-protocol/
   ```

4. The following actions might be required to open the login window, depending on your environment:
   - If a message indicates that the enhanced security configuration is enabled on the management client, select **In the future, do not show this message** and then click **OK**.
   - If the SVP is configured to support SSL-encrypted communication and security messages appear, make sure the certificate is correct and follow the instructions in the dialog box.
   - If a message indicates that certain websites are blocked, you need to add the SVP to the trusted sites zone (see Adding your SVP to the trusted sites zone for Windows Server computers (on page 26)).
5. Type the superuser ID and password, and then click **Login**.
6. If the **Security Information** dialog box appears, click **Yes**.

   After you log in, the Device Manager - Storage Navigator main window opens. You can navigate using the menu, tree, or General Tasks.
7. **Important:** Change the superuser password immediately after you log in to prevent unauthorized use of the superuser account. To change the password, click **Settings** > **User Management** > **Change Password**.

Logging in to as a user

Use the following procedure to log in to Device Manager - Storage Navigator (HDvM - SN).

Procedure

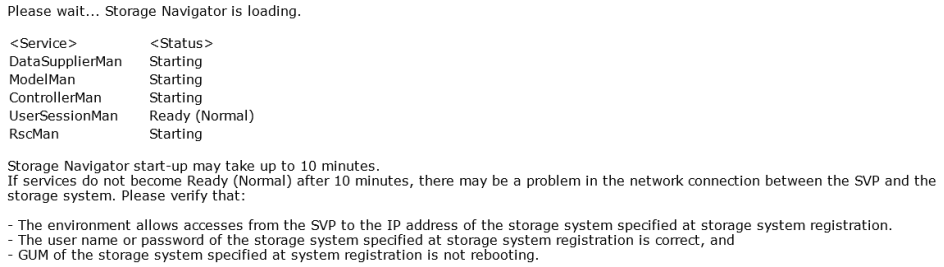
1. Start a web browser on the management client.
2. In the web browser, specify the following URL:

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

   If you changed the port number of the HTTP protocol from the initial value (443), specify the following URL:

   ```
   https://IP-address-or-host-name-of-SVP:port-number-of-the-protocol-HTTPS/
   ```

   If the HDvM - SN loading window is displayed, wait until the service status changes to **Ready (Normal)**. At that time, the login window is displayed automatically. The following is an example of the loading window.

   
   Please wait... Storage Navigator is loading.

<Service>	<Status>
DataSupplierMan	Starting
ModelMan	Starting
ControllerMan	Starting
UserSessionMan	Ready (Normal)
RscMan	Starting

   Storage Navigator start-up may take up to 10 minutes.
   If services do not become Ready (Normal) after 10 minutes, there may be a problem in the network connection between the SVP and the storage system. Please verify that:

   - The environment allows accesses from the SVP to the IP address of the storage system specified at storage system registration.
   - The user name or password of the storage system specified at storage system registration is correct, and
   - GUM of the storage system specified at system registration is not rebooting.

3. The following actions might be required to open the login window, depending on your environment:
   - If a message indicates that the enhanced security configuration is enabled on the management client, select **In the future, do not show this message** and then 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 in the dialog box.
   - If a message indicates that certain web sites are blocked, you need to add the SVP to the trusted sites zone (see Adding your SVP to the trusted sites zone for Windows Server computers (on page 26)).
   - If multiple storage systems are connected, a window that allows selection of the storage system is displayed. Select the storage system you want to connect.
   -
4. When the Storage Device List window opens*, select the storage system.

   * When there is only one SVP in the Storage Device List whose service status is Ready, the Storage Device List window does not appear.

   The HDvM - SN login window appears.

Note: If the window displaying "Please wait ... Storage Navigator is loading" remains open and you cannot log in, the IP address of the SVP might have changed. To update the IP address in the Storage Device List, click **SVP IP Address** (upper right corner of **Storage Device List** window), click **Change SVP IP Address**, and enter the IP address. Then click **Start Service**.

5. Type the user ID and password, and then click **Login**.
6. If the **Security Information** dialog box appears, click **Yes**.

Result

After you log in, the HDvM - SN main window opens. You can navigate using the menu, tree, or General Tasks. For instructions on performing operations on the storage system using Device Manager - Storage Navigator, see the applicable user guide (for example, *Hitachi Universal Replicator User Guide*).

Logging in to HDvM - SN by using AIR

When you log in to HDvM - SN by using Adobe AIR from HARMAN for the first time, Captive Bundle Application (CBA) is downloaded from the SVP to the management client. CBA is the application that enables HDvM - SN to run with AIR. The downloaded file size is about 30 MB. If the CBA version on the SVP is updated later, the new CBA version will be downloaded automatically to the management client.

Use the following procedure to log in to HDvM - SN by using AIR for the first time.

Note:

- When you log in to HDvM - SN locally on the SVP, HDvM - SN starts by using AIR except when the following condition is met. When the OS running on the SVP is one of the following, HDvM - SN starts in a web browser:
  - Windows Server 2012 (including R2)
  - Windows Server 2016 (Server with Desktop Experience)
  - Windows Server 2019 (Server with Desktop Experience)
- When the SVP software version is one of the following, make sure to use Microsoft Edge or Google Chrome as a web browser. In other cases, use Google Chrome.
  - Versions beginning with 93-05: 93-05-04-xx/xx and later
  - Versions beginning with 93-04: 93-04-04-xx/xx and later
  - Versions beginning with 93-03: 93-03-23-xx/12 and later

Before you begin

- Storage Device Launcher must be installed on the management client.
- CBA must be installed on the SVP.
- You must be logged in to the management client as the user who installed Storage Device Launcher.

Procedure

1. Open the HDvM - SN login dialog box.

   You can open the HDvM - SN login dialog box by running Storage Device Launcher on the management client or by opening a web browser and running Storage Device Launcher on the SVP.

   - To open the HDvM - SN login dialog box by running Storage Device Launcher:

     a. If you are logged in to the management client with administrator permissions, on the desktop or start menu, right-click the **Storage Device Launcher** batch file, and then run it by selecting **Run as Administrator**.

        If you are not logged in to the management client with administrator permissions, on the desktop run the shortcut for the Storage Device Launcher batch file.

        Note: If a security warning or a window blocking the operation is displayed, do not run Storage Device Launcher. Change the properties of the batch file (right-click `SDLauncher.bat`, click **Properties**, and then select **Unblock** in **Security**), and then run the file.

     b. Enter the IP address or host name of the SVP.

     c. Specify 443 for the HTTPS port number, and then click **Connect**.

        If a security warning message is displayed, verify that the security certificate is correct, and then follow the instructions in the dialog box.

   - To open the HDvM - SN login dialog box by opening a web browser and running Storage Device Launcher on the SVP:

     a. Start the web browser on the management client with administrator permissions.

     b. Enter the following URL in the web browser:

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

        If the HTTPS port number was changed from the default (443), also specify the new port number as follows:

        ```
        sdlauncher://IP-address-or-host-name-of-SVP:HTTPS-port-number/
        ```

> **Note:** If a security warning or a window blocking the operation is displayed, do not run the file. Change the properties of the batch file (right-click `SDLauncher.bat`, click **Properties**, and select **Unblock** in **Security**), and then run the file.

c. If a warning message appears and the login window does not open:

   For Microsoft Edge: If the message "This site is trying to open SDLauncher.bat." appears, click **Open** in the pop-up window to start Storage Device Launcher.

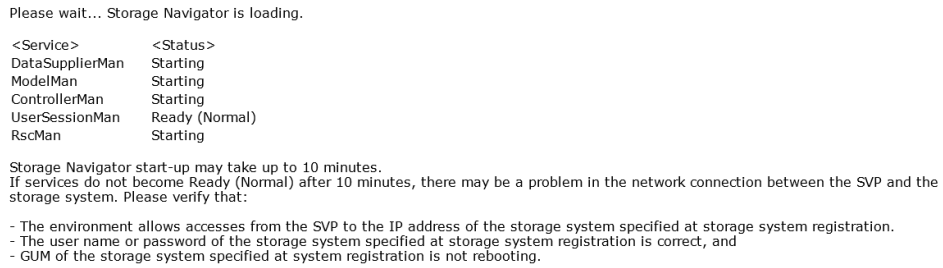
   For Internet Explorer: If a security warning message is displayed, verify that the security certificate is correct, and then follow the instructions in the dialog box.

2. Wait about 10 seconds for the CBA file to be downloaded to the management client.

   If you are using one management client to access multiple storage systems, CBA is downloaded for each storage system.

   When the download is complete, the HDvM - SN login dialog box opens. You can close the web browser.

   If the Device Manager - Storage Navigator loading window is displayed, wait until the service status changes to **Ready (Normal)**. At that time, the login window is displayed automatically. The following is an example of the loading window.


Please wait... Storage Navigator is loading.

<Service>	<Status>
DataSupplierMan	Starting
ModelMan	Starting
ControllerMan	Starting
UserSessionMan	Ready (Normal)
RscMan	Starting

Storage Navigator start-up may take up to 10 minutes.
If services do not become Ready (Normal) after 10 minutes, there may be a problem in the network connection between the SVP and the storage system. Please verify that:

- The environment allows accesses from the SVP to the IP address of the storage system specified at storage system registration.
- The user name or password of the storage system specified at storage system registration is correct, and
- GUM of the storage system specified at system registration is not rebooting.

> **Note:** The following actions might be required to open the login window, depending on your environment:
>
> - If a message indicates that the enhanced security configuration is enabled on the management client, select **In the future, do not show this message**, and then click **OK**.
> - If the SVP is configured to support SSL-encrypted communication and security messages appear, make sure the certificate is correct and follow the instructions in the dialog box.
> - If a message indicating that the site is trying to open SDLauncher.bat, click **Open** in the pop-up window, and then start Storage Device Launcher.

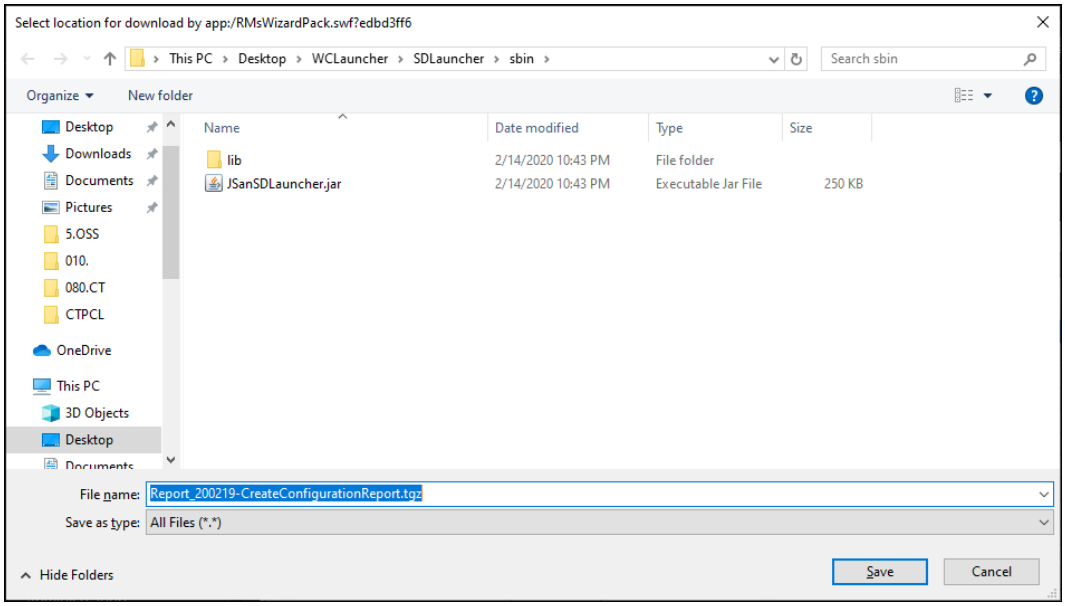
3. Enter the user name and password, and then click **Login**.

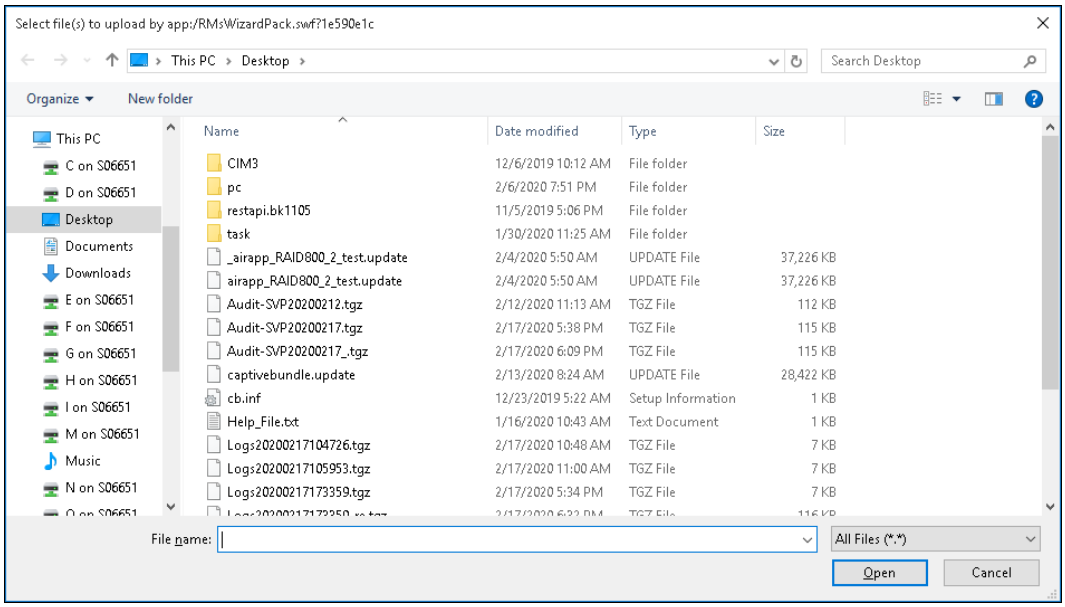
   If the **Security Information** dialog box opens, click **Yes**.

   When the storage system configuration information is finished loading, the HDvM - SN main window opens.

Download/Upload window for HDvM - SN with AIR

When you use Device Manager - Storage Navigator (HDvM - SN) with Adobe AIR, a character string that depends on the Adobe AIR environment is displayed in the title of the window used for selecting a file to be downloaded or uploaded.





Launching the maintenance utility

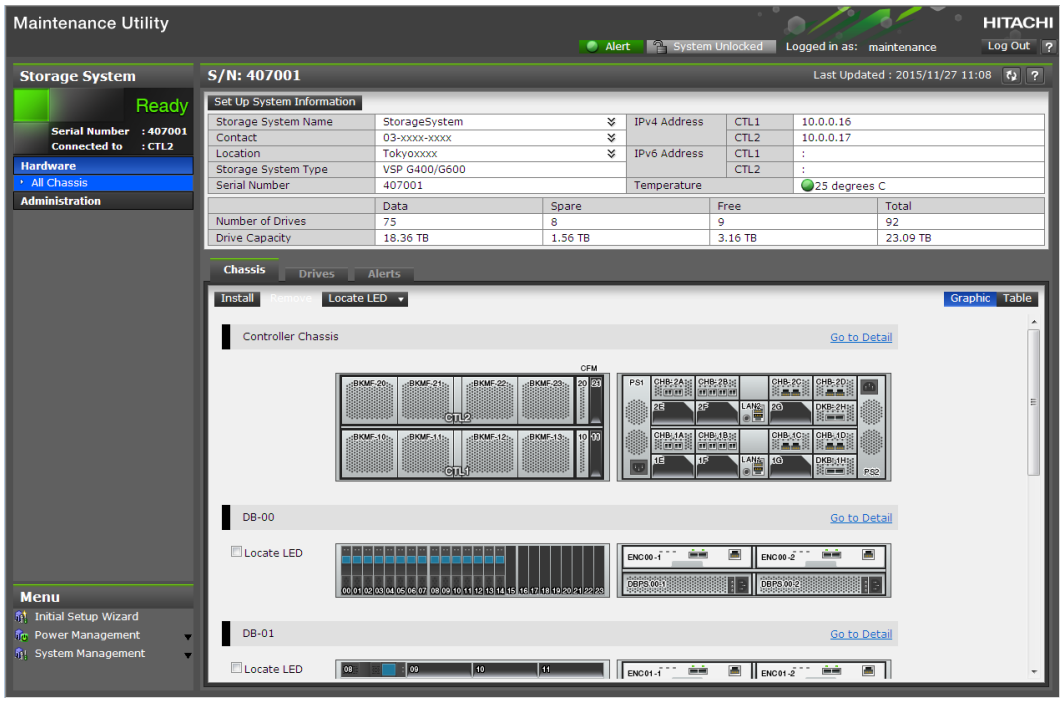
The o configure the storage system and perform maintenance operations,

You can access the maintenance utility in several ways depending on whether your storage system has an SVP. The maintenance utility opens on a separate browser tab.

- Log in to Hitachi Device Manager - Storage Navigator, and then select the Maintenance Utility menu.
- Log in to Storage Advisor Embedded, click the Settings icon (top right), and then select Maintenance Utility.

Note:

- Click ? in the window to see the help menu for the description of the Maintenance Utility.
- To display the help, the settings for enlarging and reducing the display might not be reflected in the help window, depending on the type or version of your browser.



Changing the administrator password

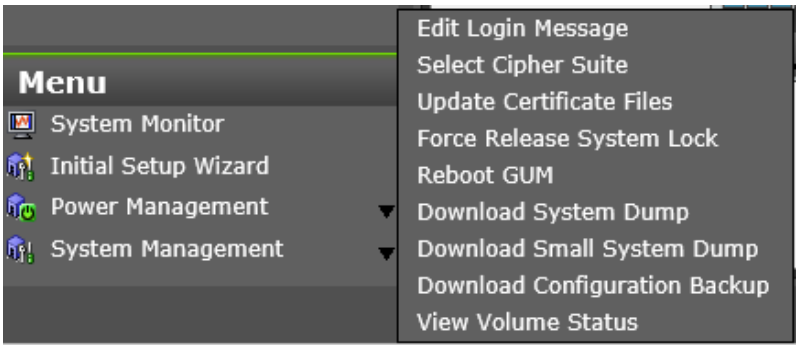
You can change the administrator password using the maintenance utility.

Before you begin

- Before changing the password of a user account specified by the registered storage system in the **Storage Device List** window, click Stop Service for the registered storage system. After changing the password of the user account, click Edit and set the new password, then click Start Service for the storage system.

Procedure

1. In the maintenance utility **Menu** navigation tree, click **System Management**.



2. Click **Change Password**.
3. Enter your current password and a new password. Enter the password again in the **Re-enter Password** field.
4. Click **Finish**.

Configuring the management client for the HDvM - SN secondary window

If you plan to use any of the following functions, you must configure the management client for use of the Device Manager - Storage Navigator (HDvM - SN) secondary window:

- Login Message function
- Data Retention Utility
- Server Priority Manager

The Device Manager - Storage Navigator (HDvM - SN) secondary window runs within the Java Runtime Environment (JRE) on the management client. The secondary window is disabled by default in HDvM - SN and must be enabled by using HDvM - SN or Web Console Launcher (when Java 11 or later is installed on the HDvM - SN management client). If the secondary window is not enabled, the functions listed above are not accessible in HDvM - SN.

Restrictions for using the HDvM - SN secondary window

- When you open the secondary window, Microsoft Edge displays the following message in the upper right of the browser window: `<file name>.jnlp was blocked because this type of file can harm your device.`

  Click **Other actions > Save** in the message window, save the object file, and then open the file. You can continue the operation even though a Java security warning is displayed when you open the file.

- When you open the secondary window, Google Chrome displays the following message in the lower left of the browser window: `This type of file can harm your computer. Are you sure you want to download <file name>.jnlp?` . Click **Save** in the message window and save the object file. Then open the file. You can continue the operation even though a Java security warning is displayed when you open the file.

- The `SJsvlSNStartServlet (<serial number>).jnlp` file is saved in the download folder and duplicated every time you open the secondary window (because it is not overwritten or deleted automatically). To prevent shortage of capacity, delete extraneous downloaded `SJsvlSNStartServlet (<serial number>).jnlp` files periodically.

  - To confirm the download location in Microsoft Edge, follow **Settings** > **Downloads** > **Location**.
  - To confirm the download location in Google Chrome, follow **Chrome Menu** > **Settings** > **Show advanced settings** > **Downloads**.

- When you are using Google Chrome, do not click **Discard** in the message window. If you do, you will not be able to use HDvM - SN for a while until error (20020-108000) appears. When error (20020-108000) appears, click **OK** to close the error, and then continue working in HDvM - SN.

  If you don't want to wait for the error to appear, you can close Chrome and then log in to HDvM - SN again.

  The error also appears if you do not click **Save** or if you do not open the saved file for some time.

Enabling the HDvM - SN secondary window

The HDvM - SN secondary window runs within the Java Runtime Environment (JRE) on the management client. The secondary window is disabled by default in HDvM - SN and must be enabled by using HDvM - SN, or by using Web Console Launcher when Java 11 or later is installed on the HDvM - SN management client. If the secondary window is not enabled, the functions listed above are not accessible in HDvM - SN.

Before you begin

- Required role: Storage Administrator (View Only)

Procedure

1. From the **Settings** menu, click **Environmental Settings** > **Edit Information Display Settings**.

   The **Edit Information Display Settings** window opens.
2. In **Secondary window**, click **Enable**.
3. Click **Apply**.

Using Web Console Launcher to enable the secondary window (Java 11 or later)

When Java 11 or later is installed on the Device Manager - Storage Navigator (HDvM - SN) management client, you must download and execute Web Console Launcher to enable the HDvM - SN secondary window. The setup file that you download contains the following applications:

- Web Console Launcher: This application is required to enable the HDvM - SN secondary window when HDvM - SN is running on a web browser with Java 11 or later installed.
- Storage Device Launcher: This application is required to start HDvM - SN in the Adobe AIR environment. Storage Device Launcher is contained only in the setup file for Windows.

When the HDvM - SN secondary window is opened, you must enable the .jnlp file included in the setup file.

Note: You must perform the following procedure each time the SVP firmware is upgraded.

Procedure

1. From the Menu bar, click **Tool** > **Download**.
2. Download the Web Console Launcher tool for Windows or UNIX.
3. Expand and execute the download file by the following OS method:

   Windows: Expand the file, right click `WCLauncher\Setupwin.bat` and execute it by selecting **Run as Administrator**. This associates the downloaded .jnlp file with Web Console Launcher.

   UNIX: Enter `tar zxvf WCLauncher_unix.tgz` to expand the file, and then enter `sudo shsetupunix.sh` in the expanded directory to execute it.

   Note: When you execute Web Console Launcher, Java8 is disabled.

Next steps

Each time you open the HDvM - SN secondary window with Java 11 or later, you must enable the .jnlp file using Web Console Launcher.

Caution: Do not delete or move the `WCLauncher_win` folder. This folder contains files required to run Web Console Launcher.

Handling a security warning when opening the HDvM - SN secondary window

If a security warning appears when you open the HDvM - SN secondary window, take the following actions to dismiss the warning and continue to the HDvM - SN secondary window.

For Microsoft Edge

1. Click **Advanced**, and then click **Continue to *<IP-address-or-host-name>* (unsafe)**.
2. When the message for downloading the `jnlp` file is displayed (upper right of the window), click **Open** or **Save as**, and save the `jnlp` file.

   When the message `<file name>.jnlp was blocked because this type of file can harm your device` is displayed in the upper right, click **Other actions** > **Save** to save the file.
3. After the file is saved, open the file. If a security warning is displayed, click **Continue**.

   The application is downloaded.
4. When the security warning for running the application is displayed, select to allow the risk and run the application, and then click **Run**.

   The HDvM - SN secondary window starts.
5. Close the warning dialog box.

   If the tab "There is a problem with this website's security certificate" remains open, close this tab and continue operations.

For Internet Explorer

1. Click **Continue to this website (not recommended)**.
2. If a message for downloading the `jnlp` file is displayed (bottom of the window), select to open the file.
3. If a message indicating that the web site is trying to open the web contents by using an old program is displayed in the Internet Explorer security dialog box, select to open the web contents by using the old program.

   If a security warning is displayed, click **Continue**.

   The application is downloaded.
4. When the security warning for running the application is displayed, select to allow the risk and run the application, and then click **Run**.

   The HDvM - SN secondary window starts.
5. Close the warning dialog box.

   If the tab "There is a problem with this website's security certificate" remains open, close this tab and continue operations.

Disabling use of Flash Player with HDvM - SN

If desired, you can disable use of Flash Player with HDvM - SN after you start using HDvM - SN with Adobe AIR.

The default setting (Enabled or Disabled) for use of Flash Player with HDvM - SN depends on the storage system model:

- VSP E1090: Disabled
- VSP E590, VSP E790, VSP E990: Enabled

Use the following procedure to disable use of Flash Player with HDvM - SN. When multiple storage systems are managed by using one SVP, you must disable use of Flash Player for each storage system.

Procedure

1. Close all HDvM - SN sessions connected to the storage system on which this operation is performed.
2. Log in to the SVP.
3. Open a command prompt on the SVP with administrator permissions.
4. Move the current directory to the folder containing the `MappFlashDisable.bat` batch file (for example, `C:\MAPP\wk\Supervisor\MappIniSet`), and then run the batch file specifying the storage system serial number* as the argument. For example:

   ```
   MappFlashDisable.bat 400102
   ```

   * The storage system serial number is displayed in **S/N** in the **Storage Device List** window on the SVP.
5. When the completion message appears, press any key to continue the processing.
6. Close the command prompt window.

Requirements for the management PC

The management PC is the PC on which embedded management tools such as Hitachi Storage Advisor Embedded (HSAE) are used for managing the storage system. To use HSAE, maintenance utility, and embedded CLI on a PC, the following requirements must be satisfied.

Hardware requirements for the management PC

Item	Specifications
Processor (CPU)	▪ Minimum: Pentium 4 640 3.2 GHz or better (not dependent on CPU vendor and processor family) ▪ Recommended: Core2Duo E6540 2.33 GHz or better
Memory (RAM)	▪ Minimum: 2 GB ▪ Recommended: 3 GB
Available storage space	▪ Minimum: 500 GB
Monitor	▪ True Color 32-bit or better ▪ Resolution: 1280 x 1024 or better
Keyboard and mouse	Required
Ethernet LAN card for TCP/IP network	▪ 100BASE-TX ▪ 1000BASE-T

Software requirements for the management PC

OS	Architecture	Browser	Other software
Windows server 2019[1]	64 bit	▪ Microsoft Edge[2] ▪ Internet Explorer 11[3] Do not use Google Chrome. Google Chrome does not support Windows Server 2019.	SSH terminal software
Windows server 2016	64 bit	▪ Microsoft Edge[2] ▪ Google Chrome[5] ▪ Internet Explorer 11[3]	
Windows 10[4]	32 bit / 64 bit		
Windows 8.1	32 bit / 64 bit		
Red Hat Enterprise Linux 7.4	64 bit	Mozilla Firefox[6] Do not use Google Chrome. Google Chrome does not support Red Hat Enterprise Linux 7.4.	

OS	Architecture	Browser	Other software
Red Hat Enterprise Linux 7.5	64 bit	Mozilla Firefox[6] Do not use Google Chrome. Google Chrome does not support Red Hat Enterprise Linux 7.5.	

Notes:

1. Requires DKCMAIN firmware version 93-04-01-x0/00 or later.
2. When you use Microsoft Edge, disable the pop-up blocker of the browser. Also, disable the Sleeping Tabs feature, or add Hitachi Storage Advisor Embedded (HSAE) to the sites that are not to be in sleep state (so that the HSAE session will not be disabled when a certain time passes in sleep state).

   Only the latest version of Microsoft Edge active on each OS is supported, according to Microsoft support policy.
3. When you use Internet Explorer, disable Compatibility View and the pop-up blocker. Also, enable Web Storage (DOM Storage).

   According to Microsoft support policy:

   - Only the latest version of Internet Explorer active on each OS is supported.
   - Support for Internet Explorer 11 will end in 2022. Change to using another browser before the support ends. For details, see the Microsoft website.
4. Do not perform unnecessary operations on the Windows 10 command prompt. There is a report that the processing executed on the command prompt stopped in the middle and the prompt did not return.
5. When you use Google Chrome, disable the pop-up blocker of the browser. Also, enable Web Storage (DOM Storage).

   Use the latest version.

   If you need to change the language setting, change the locale of the browser.
6. When you use Mozzila Firefox, disable the pop-up blocker of the browser.

   Use the latest version.

   If you need to change the language setting, change the locale of the browser.

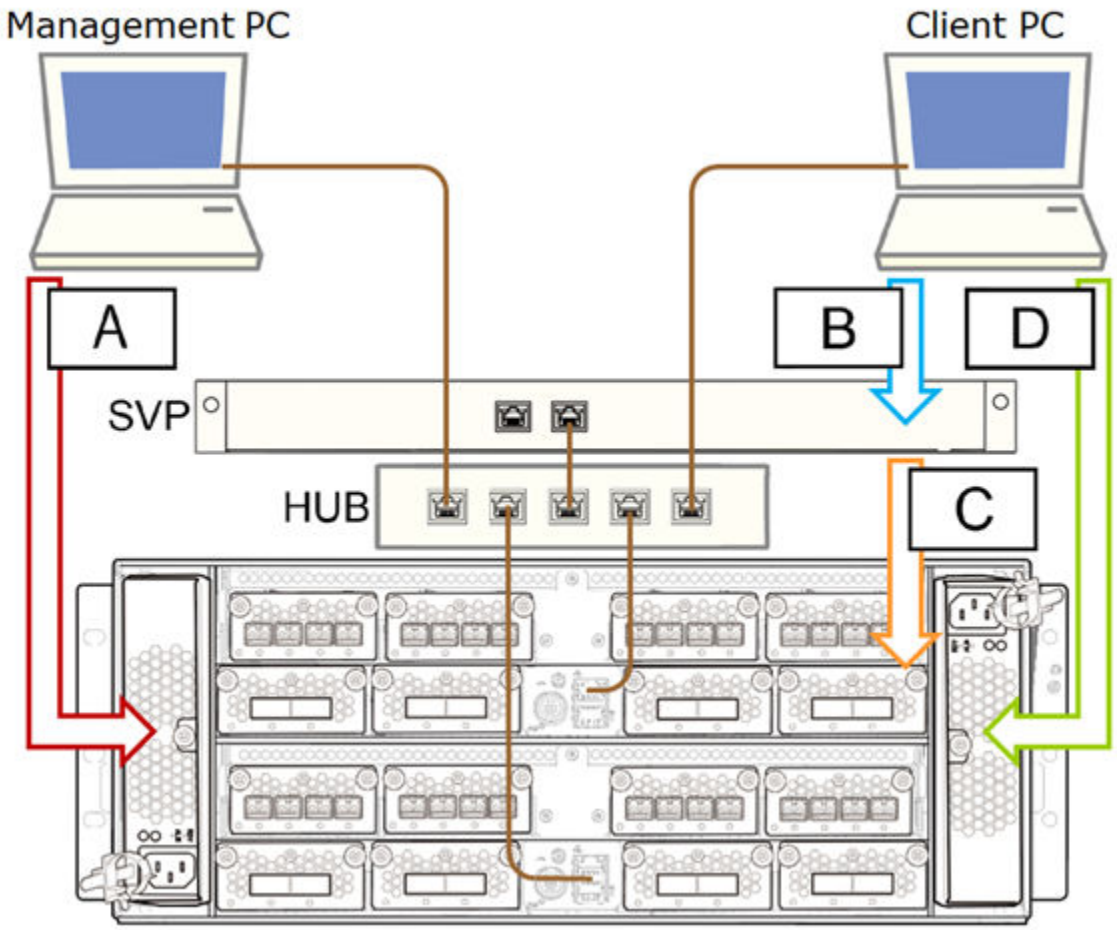
Chapter 3: Setting up SSL security for the management client

You can use a Secure Sockets Layer (SSL) certificate to create a secure, encrypted connection between the storage system and the management client.

SSL encryption of the storage system

The storage systems can use SSL encryption for all connection paths, as shown in the following figure and table. The encryption protocol used for SSL encryption is TLS version 1.2.

Note: The cipher suites for RSA key exchange used by SSL communication are set to enabled by default.



- A: Path between the management client and the storage system.
- B: Path between the SVP and the management client.
- C: Path between the SVP and the storage system.
- D: Path between the management client and the storage system.

Management model	Path	Description	Cipher suites
Using embedded interfaces	A	Between management PC and storage system	▪ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_RSA_WITH_AES_256_GCM_SHA256

Management model	Path	Description	Cipher suites
			▪ TLS_RSA_WITH_AES_256_CBC_SHA256 ▪ TLS_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_RSA_WITH_AES_128_CBC_SHA256 If TLS_RSA_WITH_AES_128_CBC_SHA256 is selected, you can use the following cipher suites: ▪ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_RSA_WITH_AES_256_CBC_SHA256
Using Device Manager - Storage Navigator	B	Between the SVP and client PC	▪ TLS_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_RSA_WITH_AES_256_CBC_SHA256 ▪ TLS_RSA_WITH_AES_256_CBC_SHA ▪ TLS_PSK_WITH_AES_256_CBC_SHA ▪ TLS_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_RSA_WITH_AES_128_CBC_SHA256 ▪ TLS_RSA_WITH_AES_128_CBC_SHA ▪ TLS_PSK_WITH_AES_128_CBC_SHA
	C	Between the SVP and the storage system	▪ TLS_RSA_WITH_AES_128_CBC_SHA256 ▪ TLS_RSA_WITH_AES_128_CBC_SHA ▪ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
	D	Between the client PC and storage system	▪ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_RSA_WITH_AES_256_CBC_SHA256 ▪ TLS_RSA_WITH_AES_256_GCM_SHA256 ▪ TLS_RSA_WITH_AES_128_CBC_SHA256 ▪ TLS_RSA_WITH_AES_128_GCM_SHA256

Management model	Path	Description	Cipher suites
			If TLS_RSA_WITH_AES_128_CBC_SHA256 is selected, you can use the following cipher suites: ▪ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_RSA_WITH_AES_256_CBC_SHA256 ▪ TLS_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_RSA_WITH_AES_128_CBC_SHA256 If TLS_RSA_WITH_AES_128_CBC_SHA256 is not selected, you can use the following cipher suites: ▪ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

Note: When the TLSv1.0/1.1 communication is disabled, pages might not appear properly depending on the TLS settings of browsers. Perform the following TLS settings of browsers:

- Using Internet Explorer: Click **Tool > Internet Option**, go to the **Advanced** tab, and then select **Use TLS 1.2**.
- Using Firefox: Enter a about:config into the address bar, open the configuration editor (about: config page), and set the value of `security.tls.version.max` to **3**.
- Using Google Chrome: Click **Chrome menu > Settings > Show advanced settings > Advanced settings**, and then select **Use TLS 1.2**.

To prevent a man-in-the middle attack, the SSL encryption on path B (between the SVP and storage system) verifies the validity of the connection by using the certificate that was uploaded to the SVP in advance and by using the certificate of the storage system. The same certificate must be uploaded to the SVP and the storage system.

Note:

- If a certificate for the SVP or the storage system is changed, the SVP does not operate normally. Upload the certificate to the storage system before uploading the certificate to the SVP.
- Different certificates can be used to connect to the SVP and web server.

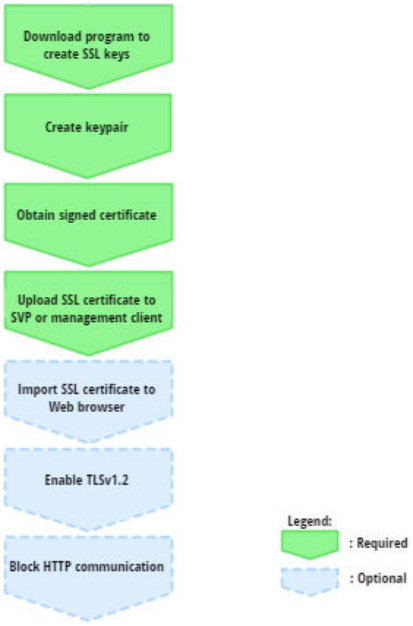
Table 1

Certificate	Upload destination	Comments
A signed certificate of SSL encryption between the SVP and client PC	SVP	N/A
For connecting to the SVP*	SVP and storage system	If a certificate for the SVP or the storage system was uploaded, the SVP will not operate normally.
For connecting to the web server*	SVP and storage system	If a certificate for the SVP or storage system was uploaded, the SVP will not operate normally.
* You can use the same certificate for connecting to the SVP and connecting to the web server.		

Setting up SSL communications

Before you enable SSL encryption, you must create a private key and a public key to establish a secure communication session.

The following figure shows the procedure to set up SSL communication. Unless otherwise noted, all steps are required. Note that creation of private and public keys requires a dedicated program. You can download a program for creating private and public keys from the OpenSSL website (http://www.openssl.org/).



Setting up SSL encryption using Device Manager - Storage Navigator

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

SSL communication can be established between the management client and the SVP using the protocols and port numbers specified in the following table.

Protocol	Port Number
HTTPS	443
RMI	1099
RMI	51100-51355 When a storage system is registered, an unused port number in this range is automatically allocated, and a firewall is set. The allocated port number is used when the storage system starts.
SMI-S	5989-6244 When a storage system is registered, an unused port number in this range is automatically allocated, and a firewall is set. The allocated port number is used when the storage system starts.

Protocol	Port Number
HTTPS (raidinf)	5443

SSL communication can be established between the following servers and the SVP:

- Key management server
- External authentication or authorization server
- Hitachi Ops Center server
- Hitachi Command Suite server

Note: To enable SSL, the private and public key pair and SVP server certificate must be valid. If either the keys or the certificate is expired, the user cannot connect to the SVP.

Note: The extended profile fields in the X.509 certificate support the following items as specified in RFC5280:

- BasicConstraints
- KeyUsage
- SubjectKeyIdentifier

In addition, if you use a key management server (KMS) and an external authentication or authorization server for VSP E series with DKCMAIN firmware version 93-06-22 or later, the following extensions are also supported:

- Authority Key Identifier
- Certificate Policies
- Subject Alternative Name
- Name Constraints
- Policy Constraints
- Extended Key Usage
- Inhibit anyPolicy

Do not use an extension other than those listed above.

Note: To add the Secure attribute to cookies using Device Manager - Storage Navigator, you must block HTTP communication. For details, see Blocking HTTP communication to the SVP (on page 65).

Note: Device Manager - Storage Navigator supports HTTP Strict Transport Security (HSTS) with a max range of 31,536,000 seconds (1 year). To enable HSTS, you must use the security certificate issued by a trusted root certificate authority for your Device Manager - Storage Navigator domain. HSTS is valid for one year (31,536,000 seconds), and it is renewed automatically every time the HSTS header is sent to the browser. The security certificate to use is determined by the browser. For details, contact your browser vendor.

Note: If HSTS is enabled on a Web application on a server you wish to install Device Manager - Storage Navigator, use a domain that is written to the security certificate specific to each application. If you use the same domain, the HSTS settings are applied to all Web applications that use the domain, and all connections are switched to https. If you have an application that can be accessed only through http, you cannot establish the connection.

Creating a keypair

To enable SSL, you must create a keypair consisting of a public and a private key on the management client. The instructions use Windows 8.1 as an example.

Creating a private key using the OpenSSL command

A private key is required to create an SSL keypair. The following procedure for Windows systems creates a private key file called `server.key` in the `c:\key` folder.

Before you begin

Ensure that OpenSSL is stored in `C:\Mapp\OSS\apache\bin\openssl` on the SVP. (You do not need to install OpenSSL.) If not, download and install `openssl.exe` from http://www.openssl.org/ to the `C:\openssl` folder.

Note: `C:\Mapp` indicates the installation directory for the storage management software and SVP software. Specify `C:\Mapp` for the installation directory if another directory is specified for the installation directory.

Procedure

1. When you install OpenSSL, if the read-only attribute is set, release it from the `c:\openssl` folder. (This step is not necessary if you use OpenSSL on the SVP.)
2. Open a command prompt with administrator permissions.
3. Move the current directory to the folder to which the key file is output (such as `c:\key`), and execute the following command.

   When OpenSSL is installed:

   ```
   C:\key>c:\openssl\bin\openssl genrsa -out server.key 2048
   ```

   When using OpenSSL on the SVP:

   ```
   C:\key>c:\Mapp\OSS\apache\bin\openssl genrsa -out server.key 2048
   ```

Creating a public key using the OpenSSL command

A public key, which has the file extension `.csr`, is required to create an SSL keypair. The following procedure is for the Windows operating system.

Before you begin

Download `openssl.exe` from the OpenSSL website or determine to use OpenSSL on the SVP.

Procedure

1. Open a command prompt with administrator permissions.
2. Execute the following command:

   When OpenSSL is installed:

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

   When using OpenSSL on the SVP:

   ```
   C:\Key>c:\Mapp\OSS\apache\bin\openssl req -sha256 -new -key
   server.key -config c:\Mapp\OSS\apache\conf\openssl.cnf -out
   server.csr
   ```

   Note: `C:\Mapp` indicates the installation directory for the storage management software and SVP software. Specify `C:\Mapp` for the installation directory if another directory is specified for the installation directory.

   Note: This command uses SHA-256 as a hash algorithm.

   - Use SHA-256 for the hash algorithm. Do not use MD5 or SHA-1 for the hash algorithm due to its low security level.
   - When you use OpenSSL on the SVP, do not change the contents of `c:\Mapp\OSS\apache\conf\openssl.cnf`.

3. 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 SVP or GUM. The name you entered here is used as the server name (host name). To obtain a signed and trusted certificate, ensure that the server name is the same as the host name.
   - Email Address

- Challenge password (optional)
- Company name (optional)

Example

The following example shows the contents of a command window when you create a public key.

```
......++++++
..++++++
is 65537 (0x10001)
C:\key>c:\openssl\bin\openssl req -sha256 -new -key server.key -config c
You are about to be asked to enter information that will be incorporated into your
certificate request. What you are about to enter is what is called a Distinguished
Name or a DN.
\openssl\bin\openssl.cfg -out server.csr
For some fields there will be a default value.
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:JP
State or Province Name (full name) [Some-State]:Kanagawa
Locality Name (eg, city) []:Odawara
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Hitachi
Organization Unit Name (eg, section) []:ITPD
Common Name (eg, YOUR name) []:192.168.0.1
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

Obtaining a signed certificate

After creating a private key and public key, obtain a signed public key certificate file. You can use any of these methods to obtain a signed certificate file.

- Create a certificate by self-signing. See Obtaining a self-signed certificate (on page 56).
- Obtain a certificate from the certificate authority that is used by your company.
- Request an official certificate from an SSL certificate authority. See Obtaining a signed and trusted certificate (on page 56).

Note:

When you send a request to a certificate authority, specify the SVP or GUM as the host name.

Hitachi recommends that self-signed certificates be used only for testing encrypted communication.

Obtaining a self-signed certificate

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

When OpenSSL is installed:

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

When using OpenSSL on the SVP:

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

Note: C:\Mapp indicates the installation directory for the storage management software and SVP software. Specify C:\Mapp for the installation directory if another directory is specified for the installation directory.

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

This command 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.

Obtaining a signed and trusted certificate

To obtain a signed and trusted certificate, you must obtain 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. Use of this certificate results in higher reliability in exchange for greater cost and requirements. The signed and trusted certificate is the signed public key.

Before uploading the SSL certificate

Before uploading the SSL certificate to the SVP or management client, perform the following tasks:

- If the passphrase is set, an SSL certificate cannot be applied for the SVP. You must release the passphrase for the SSL certificate before applying the SSL certificate to the SVP. For instructions, see Releasing an SSL certificate passphrase (on page 56).
- If you are uploading a created private key and the SSL certificate to the management client, you need to convert the SSL certificate to PKCS#12 format. For instructions, see Converting the SSL certificates to PKCS#12 format (on page 58).

Releasing an SSL certificate passphrase

An SSL certificate cannot be uploaded to the SVP if the passphrase is set. If the passphrase is set, use the following procedure to release the passphrase for the SSL certificate before applying it to the SVP.

Before you begin

- The private key (`server.key` file) must have been created.
- OpenSSL must be installed. In this procedure, it is installed in `C:\openssl`.
- All users must be logged out of Device Manager - Storage Navigator.

Procedure

1. On the SVP, open a command prompt with administrator permissions.
2. Move the current directory to the folder containing the key file (for example, `C:\key`).
3. Execute the following command.

   Caution: Executing this command will overwrite the current key file. To prevent loss of the key file, either back up the key file before executing the following command, or specify a different key file input destination and output destination when executing the following command.

   When OpenSSL is installed:

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

   When using OpenSSL on the SVP:

   ```
   C:\key>c:\Mapp\OSS\apache\bin\openssl rsa -in key-file-input-
   destination -out key-file-output-destination
   ```

   Note: `C:\Mapp` indicates the installation directory for the storage management software and SVP software. If you specified a different installation directory, replace `C:\Mapp` with the specified installation directory.

4. When `Enter pass phrase for server.key:` is displayed, enter the passphrase. The passphrase in the SSL private key is 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
```

Converting the SSL certificates to PKCS#12 format

Uploaded SSL certificates need to be in PKCS#12 format.

If you are uploading a created private key and the SSL certificate to the management client, you need to convert the SSL certificate to PKCS#12 format. If you are not uploading the SSL certificate, conversion is not required.

Before you begin

- You must store a private key and SSL certificate in the same folder.
- In the following procedure:
  - The private key file name is “client.key”.
  - The SSL certificate file name is “client.crt”.
  - The SSL certificate in PKCS#12 format is output to c:\key.
  - If you update SSL certificates in a batch, conversion is not required.

Procedure

1. Open a command prompt with administrator permissions.
2. Enter the following command:

   When OpenSSL is installed:

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

   When using OpenSSL on the SVP:

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

   Note: `C:\Mapp` indicates the installation directory for the storage management software and SVP software. Specify `C:\Mapp` for the installation directory if another directory is specified for the installation directory.

3. Enter a password, which is used when uploading the SSL certificate in PKCS#12 format. You can use up to 128 alphanumeric characters and the following symbols: ! # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
4. The `client.p12` file is created in the `C:\key` folder. This `client.p12` file is the SSL certificate in PKCS#12 format.
5. Close the command prompt.

Uploading the SSL certificate to the SVP or management client

To use SSL-encrypted communication, you must upload the private key and the signed server certificate (public key) to the management client.

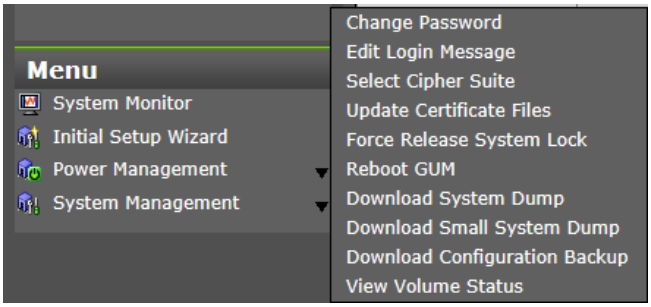
Caution: Back up the SSL certificate file before updating the storage system firmware. When the firmware is updated, the existing SSL certificate file might be deleted and replaced with the default certificate file. If this happens, reinstall the backed-up SSL certificate file.

Before you begin

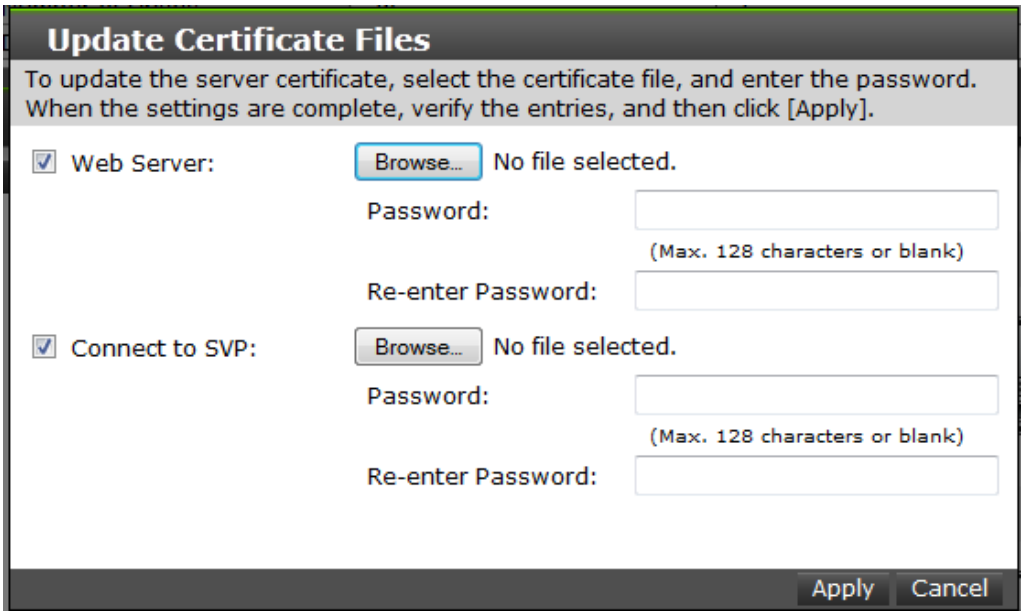
- You must have the Storage Administrator (Initial Configuration) role to perform this task.
- You must be logged in to the SVP or management client.
- A private key (.key file) has been created. Make sure that the file name is `server.key`.
- A signed public key certificate (.crt file) has been acquired. Make sure that the file name is `server.crt`.
- The private key (.key file) must be in PEM format. You cannot use DER format.
- The signed public key certificate (.crt file) must be in X509 PEM format. You cannot use X509 DER format.
- The passphrase for the private key (server.key file) must be released.
- If an intermediate certificate exists, you must prepare a signed public key certificate (server.crt file) in a certificate chain that contains the intermediate certificate.
- The number of tiers of the certificate chain for the certificate to be uploaded must be 5 tiers or less including the root CA certificate.
- The public key of the certificate to be uploaded must be RSA.

Procedure

1. In the maintenance utility **Menu** navigation tree, click **System Management**.



2. Click **Update Certificate Files**.



Note: For storage systems without an SVP, unselect the **Connect to SVP** box.

3. Select the **Web Server** checkbox, then click **Browse.**
4. Browse to the certificate file and click **Open**. The **File Upload** window closes and returns you to the **Update Certificate Files** dialog box.
5. Click **Apply**.

Uploading the signed certificate for SSL communication between the SVP and management client to the SVP

To use a certificate for SSL communications between the SVP and the client PC, you must upload the private key and signed public key certificate to the SVP. Use the following procedure to upload a certificate by using the certificate update tool.

The extended profile fields in the X.509 certificate support the following items as specified in RFC5280:

- BasicConstraints
- KeyUsage
- SubjectKeyIdentifier
- SubjectAltName

Note: When the storage management software is updated, the private key and signed public key certificate might be returned to default. If this happens, you need to upload the private key and signed public key certificate to the SVP again.

Before you begin

- The private key (`server.key` file) must have been created. If the file name is not `server.key`, rename it to `server.key`.
- The signed public key certificate (`server.crt` file) must have been obtained. If the file name is not `server.crt`, rename it to `server.crt`.
- The private key (`server.key` file) and the signed public key certificate (`server.crt` file) must be in X509 PEM format. Do not use a certificate in X509 DER format.
- If an intermediate certificate exists, you must prepare a signed public key certificate (`server.crt` file) in a certificate chain that contains the intermediate certificate.
- The certificate chain for the certificate to be uploaded must have 5 tiers or fewer including the root CA certificate.
- The following GUM firmware version is required to update a certificate file to a certificate file in a certificate chain that contains the intermediate certificate and root CA certificate:
  - 93-02-01-xx/xx or later
- The public key encryption method for the certificate to be uploaded must be RSA.
- All users must be logged out of Device Manager - Storage Navigator.

Procedure

1. On the SVP, start a Windows command prompt as Administrator.
2. Move the current directory to the directory containing the certificate update tool `MappApacheCrtUpdate.bat`.
3. Run the following commands:

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet
   MappApacheCrtUpdate.bat absolute-path-of-the-certificate-file absolute-path-of-the-private-key-file
   ```

   In this command, `C:\MAPP` indicates the installation directory of the storage management software and SVP software. If the installation directory is not `C:\Mapp`, replace `C:\Mapp` with your installation directory.
4. When prompted, press any key to continue.
5. When the processing is complete, you can close the command prompt.

Uploading the certificates for “Connect to SVP” and “Web server” to the storage system

Before uploading the SSL certificate, you must upload and update the certificate for “Connect to SVP” and the certificate for “Web server” that are used for SSL communications between the management client and the storage system and between the SVP and the storage system.

The extended profile fields in the X.509 certificate support the following items as specified in RFC5280:

- BasicConstraints
- KeyUsage
- SubjectKeyIdentifier

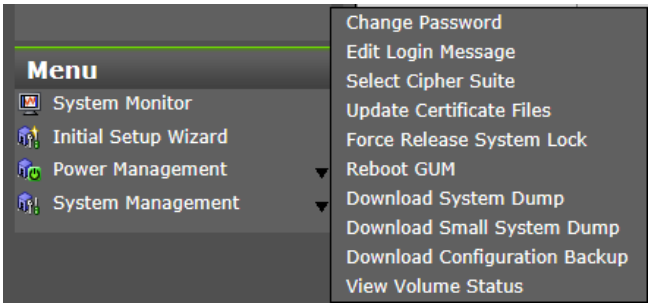
Note: When the storage management software is updated, the private key and signed public key certificate might be returned to default. If this happens, you need to upload the private key and signed public key certificate to the SVP again.

Before you begin

- The certificate files must be in PKCS#12 format.
- If you have a server certificate file and a private key file that are in PEM format, you need to convert the certificates to PKCS#12 format. Also, register the server certificate files before conversion in the SVP.
- If an intermediate certificate exists, you must prepare a signed public key certificate in a certificate chain that contains the intermediate certificate.
- The number of tiers of the certificate chain for the certificate to be uploaded must be 5 tiers or less including the root CA certificate.
- The following GUM firmware version is required to update a certificate file to a certificate file in a certificate chain that contains the intermediate certificate and CA certificate:
  - 93-02-01-xx/xx or later
- The public key encryption method for the certificate to be uploaded must be RSA.

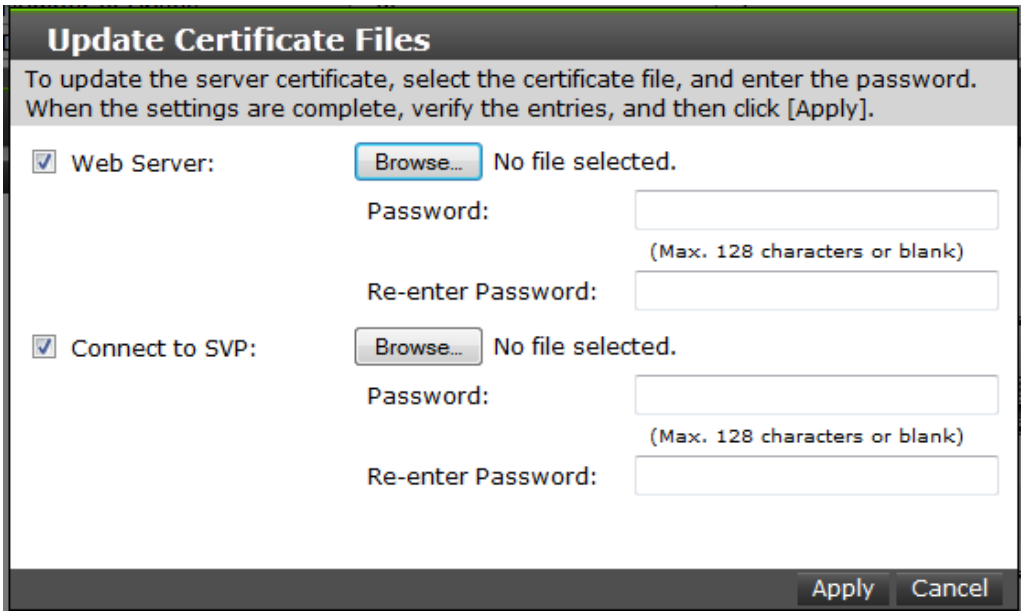
Procedure

1. In the maintenance utility **Menu** navigation tree, click **System Management** > **Update Certificate Files**.



2. Select the check box for the certificate you want to update, and then specify the certificate file.
   - If you are using Hitachi Storage Advisor Embedded, select **Web Server**.

     Note: If the storage system does not have an SVP, make sure to clear (uncheck) the check box for **Connect to SVP**.
   - If you are using Hitachi Device Manager - Storage Navigator, select **Web Server** or **Connect to SVP**.



3. Confirm the settings, and then click **Apply**.
4. When the completion message appears, close the dialog box.

Uploading the certificate for "Connect to SVP" to the SVP

Before using a certificate for SSL communications between the SVP and the storage system, you need to upload the signed public key certificate to the SVP.

The extended profile fields in the X.509 certificate support the following items as specified in RFC5280:

- BasicConstraints
- KeyUsage
- SubjectKeyIdentifier

Before you begin

- The private key for the storage system and the signed public key certificate must be updated in the maintenance utility.
- The signed public key certificate (`server.crt` file) must be in X509 PEM format.
- If an intermediate certificate exists, you must prepare a signed public key certificate (`server.crt` file) in a certificate chain that contains the intermediate certificate.
- The number of tiers of the certificate chain for the certificate to be uploaded must be 5 tiers or less including the root CA certificate.
- The following GUM firmware version is required to update a certificate file to a certificate file in a certificate chain that contains the intermediate certificate and CA certificate:
  - 93-02-01-xx/xx or later
- The public key encryption method for the certificate to be uploaded must be RSA.
- All users must be logged out of Device Manager - Storage Navigator.

Procedure

1. On the SVP, start a Windows command prompt as Administrator.
2. Move the current directory to the directory containing the tool `MappL7SwitchGumSslCrtUpdate.bat`.
3. Run the following commands:

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet
   MappL7SwitchGumSslCrtUpdate.bat absolute-path-of-the-certificate-file
   ```

   In this command, `C:\MAPP` indicates the installation directory of the storage management software and SVP software. If the installation directory is not `C:\Mapp`, replace `C:\Mapp` with your installation directory.
4. When prompted, press any key to continue.
5. When the processing is complete, you can close the command prompt.

Uploading the web server certificate to the SVP

Execute the SSL communication with Device Manager - Storage Navigator installed on the SVP as a client and with the controller of the storage system as a server. Upload the private key and the signed server certificate (public key) to the SVP for using the SSL communication.

The extended profile fields in the X.509 certificate support the following items as specified in RFC5280:

- BasicConstraints
- KeyUsage
- SubjectKeyIdentifier

Use the following procedure to upload the certificate using the certificate update tool.

Before you begin

- The private key for the web server and the signed public key certificate must be updated in the maintenance utility.
- The private key (`server.key` file) and signed public key certificate (`server.crt` file) must be in X509 PEM format or X509 DER format.
- If an intermediate certificate exists, you must prepare a signed public key certificate (`server.crt` file) in a certificate chain that contains the intermediate certificate.
- The number of tiers of the certificate chain for the certificate to be uploaded must be 5 tiers or less including the root CA certificate.
- The GUM firmware version 93-02-01 or later is required to update a certificate file to a certificate file in a certificate chain that contains the intermediate certificate and root CA certificate.
- The public key encryption method for the certificate to be uploaded must be RSA.
- All users must be logged out of Device Manager - Storage Navigator.

Procedure

1. On the SVP, start a Windows command prompt as Administrator.
2. Move the current directory to the directory containing the certificate update tool (`MappSn2GumSslCrtUpdate.bat`).
3. Run the following command:

```
C:\MAPP\wk\Supervisor\MappIniSet\
MappSn2GumSslCrtUpdate.bat r[absolute path of the certificate file]
```

   In this command, `C:\MAPP` indicates the installation directory of the storage management software and SVP software. If the installation directory is not `C:\Mapp`, replace `C:\Mapp` with your installation directory.

4. When prompted, press any key to continue.
5. When the processing is complete, you can close the command prompt.

Next steps

Verify that the uploaded certificate is valid by checking that the Maintenance Utility window opens. For details and instructions, see Checking the web server certificate uploaded to the SVP (on page 70).

Importing the SSL certificate to the Web browser

To allow your Web browser to automatically trust SSL certificates, you can import the SSL certificate into your Web browser.

Consult your Web browser's documentation for instructions to import the SSL certificate to the Web browser.

Blocking HTTP communication to the SVP

You can use the HTTP setting tool to block or allow access to the HTTP communication port as needed.

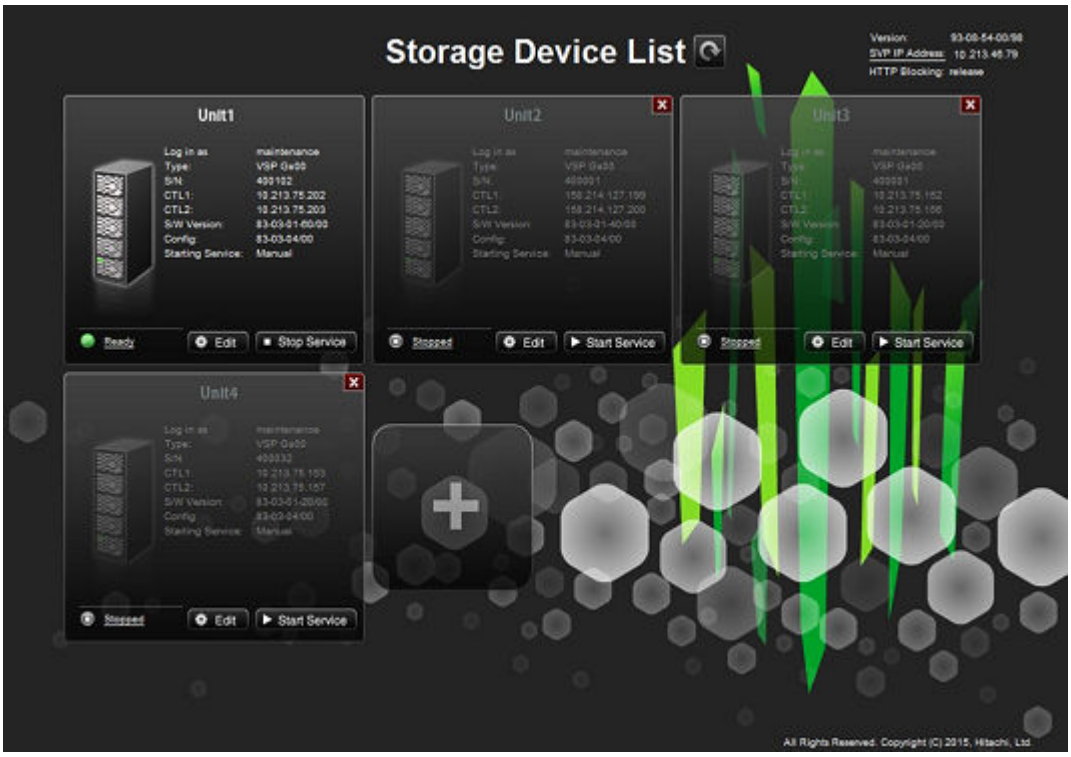
Note: The HTTP communication port is blocked by default on the SVP for VSP E1090.

Before you begin

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

Procedure

1. Verify that HTTP communication is not already blocked by checking **HTTP Blocking** in the **Storage Device List** window on the SVP.
   - **release**: HTTP communication to the SVP is not blocked.
   - **block**: HTTP communication to the SVP is blocked.



The value displayed in **HTTP Blocking** is updated periodically. Wait for a few minutes after changing the setting, or click the refresh button in the **Storage Device List** window.

HTTP Blocking is displayed when the storage management software version is 93-06-01 or later. For software versions that do not display **HTTP Blocking**, connect HDvM - SN using the HTTP protocol from the management client, and then check **HTTP Blocking**.

2. Close all management client sessions on the storage system, including Storage Advisor Embedded, maintenance utility, and HDvM - SN.
3. Open a command prompt window with administrator permissions.
4. Move the current directory to the folder containing the SVP configuration tool (for example, `C:\MAPP\wk\Supervisor\MappIniSet`), and then execute the following command:

   ```
   MappHttpBlock.bat
   ```

5. When the completion message appears, press any key to acknowledge the message and close the message box.
6. Close the command prompt window.

Releasing HTTP communication blocking

If the web server supports SSL (HTTPS), you can use the HTTP setting tool to release a block to the HTTP communication port as needed.

Before you begin

- You must have the Storage Administrator (Initial Configuration) role to perform this task.
- You must be logged into the SVP or management client.

Procedure

1. Close all management client sessions on the storage system, including Storage Advisor Embedded, maintenance utility, and Device Manager - Storage Navigator.
2. Open a command prompt window with administrator permissions.
3. Move the current directory to the folder containing the SVP configuration tool (for example, `C:\MAPP\wk\Supervisor\MappIniSet`), and then execute the following command:

   ```
   MappHttpRelease.bat
   ```
4. When the completion message appears, press any key to acknowledge the message and close the message box.
5. Close the command prompt window.

Managing SSL certificates

When you use encrypted SSL communications to manage your storage system, you can select the desired cipher suite, update a signed certificate, and return an updated certificate to default.

SSL connection protects the User IDs and passwords that are exchanged when users log in to the management client.

Selecting a cipher suite

Cipher suites are part of SSL Version 3 and OSI Transport Layer Security Version 1 Cipher Specifications.

Note: The cipher suites for RSA key exchange used by SSL communication are set to enabled by default.

Caution:

- If you set protocols between the SVP and the storage system, the setting operation on the SVP is also necessary.
- When the storage system is other than VSP E series, if you select either of the following cipher suites, make sure to enable the cipher suites for RSA key exchange on the SVP.
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_128_CBC_SHA

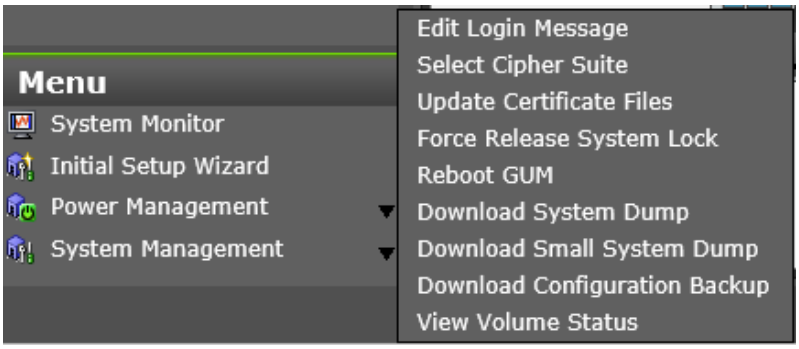
  If you select not to use both these cipher suites, make sure to disable the cipher suites for RSA key exchange on the SVP.
- After you select a cipher suite, the available cipher suites differ, depending on the connection path for SSL communications.

Before you begin

You must have the Storage Administrator (View & Modify) role to complete this procedure.

Procedure

1. In the maintenance utility **Menu** navigation tree, click **System Management**.



2. Click **Select Cipher Suite**.
3. Select the type of communication to use between the management client and the storage system.

   The selections change the encryption level. Higher encryption provides better security but the communication speed is slower. After you select a cipher suite, the available cipher suites differ depending on the connection path for SSL communications.

   - TLS_RSA_WITH_AES_128_CBC_SHA (Prioritize Transmission Speed): This selection provides higher communication speed and lower security.
   - TLS_RSA_WITH_AES_128_CBC_SHA256 (Prioritize Security): This selection provides higher security and lower communication speed.

   If you select either of the following cipher suites, enable the cipher suites for RSA key exchange on the SVP:

   - TLS_RSA_WITH_AES_128_CBC_SHA256
   - TLS_RSA_WITH_AES_128_CBC_SHA

If you do not use either of these cipher suites, disable the cipher suites for RSA key exchange on the SVP.

4. Click **Apply** to save the setting and close the dialog box.

Checking the certificate for SSL communications between the SVP and the management client

You can use a web browser on the management client to check the following information about the certificate for SSL communications between the SVP and the management client:

- Issued to: <name or url>
- Issued by: <name or url>
- Valid from <date> to <date>

Checking the certificate for SSL communications using Internet Explorer

Before you begin

The SVP must be running.

Procedure

1. Launch Internet Explorer on the management client, and then enter the IP address of the SVP.

   `https://IP-address-of-the-SVP`

   If the port number of the HTTPS service on the SVP has been changed from the initial value "443", enter the following in the URL bar:

   ```
   https://IP-address-of-the-SVP:port-number-of-the-HTTPS-service
   ```

2. Select the command bar in Internet Explorer.

   If the command bar is not displayed in an Internet Explorer window, right-click the top edge of the window, and then select **Command bar**.

3. From the command bar, select **Page** > **Properties**, and then click **Certificates**.

   In either of the following cases, the default certificate is used.

   - The following information is displayed in the **General** tab, and “00dc52873fdb5cc76b” is displayed for **Serial number** in the **Details** tab:

     ```
     Issued to: Hitachi.Ltd.
     Issued by: Hitachi.Ltd.
     Valid from 18/14/2014 to 18/04/2024
     ```

   - The following information is displayed in the **General** tab:

     ```
     Issued to: www.example.com
     Issued by: www.example.com
     Valid from DD/MM/YYYY to DD/MM/YYYY
     ```

Note that the valid period differs depending on the SVP software version.

Checking the certificate for SSL communications using Google Chrome

Before you begin

The SVP must be running.

Procedure

1. Launch Google Chrome on the management client, and then enter the IP address of the SVP.

   ```
   https://IP-address-of-the-SVP
   ```

   If the port number of the HTTPS service on the SVP has been changed from the initial value "443", enter the following in the URL bar:

   ```
   https://IP-address-of-the-SVP:port-number-of-the-HTTPS-service
   ```

2. Right-click in a Google Chrome window, select **Inspect**, and then select the **Security** tab.
3. In the **Security overview** area, click **View certificate**.

   In either of the following cases, the default certificate is used.

   - The following information is displayed in the **General** tab, and “00dc52873fdb5cc76b” is displayed for **Serial number** in the **Details** tab:

     ```
     Issued to: Hitachi.Ltd.
     Issued by: Hitachi.Ltd.
     Valid from 18/14/2014 to 18/04/2024
     ```

   - The following information is displayed in the **General** tab:

     ```
     Issued to: www.example.com
     Issued by: www.example.com
     Valid from DD/MM/YYYY to DD/MM/YYYY
     ```

   Note that the valid period differs depending on the SVP software version.

Checking the web server certificate uploaded to the SVP

Procedure

1. Log in to Device Manager - Storage Navigator.
2. In the Device Manager - Storage Navigator main window, click **Maintenance Utility, Hardware** > **Other hardware maintenance**.
3. Check that the **Maintenance Utility** window opens.

If the Maintenance Utility window opens, the certificate for connecting to the web server is valid.

If the error message 20122-207001 is displayed, the certificate uploaded to the SVP and the storage system might not be valid. Take the following actions:

a. Verify that the certificate meets the requirements (see Setting up SSL security for the management client (on page 46)). If not, create a certificate that meets the requirements.
b. Retry the operations. See Uploading the certificates for “Connect to SVP” and “Web server” to the storage system (on page 61).
c. Retry the operations. See Uploading the web server certificate to the SVP (on page 64).

If the error message 20122-207001 is displayed due to a reason other than those listed, see the *Hitachi Device Manager - Storage Navigator Messages Messages* guide.

Updating a signed certificate

To use SSL-encrypted communication, you must update and upload the private key and the signed server certificate (public key) to the management client.

The extended profile fields in the X.509 certificate support the following items as specified in RFC5280:

- BasicConstraints
- KeyUsage
- SubjectKeyIdentifier
- subjectAltName

Important: Before updating a signed certificate, review the following information:

- While the SVP certificate is being updated, tasks that are being run or scheduled to run on Device Manager - Storage Navigator are not executed.
- Certificates for RMI communication are updated asynchronously. The process takes about 2 minutes.
- If the SVP certificate is updated while Ops Center Administrator or Hitachi Command Suite is being set up, the setup operation will fail.
- Updating the SSL certificate might change the system drastically and could lead to SVP failure. Make sure to consider carefully the content of the certificate and private key to be set.
- After the certificate update is complete, the SVP can take 30 to 60 minutes to restart depending on the environment.

Before you begin

- You must have the Storage Administrator (Initial Configuration) role to perform this task.
- You must be logged in to the SVP or management client.
- A private key (`.key` file) has been created. Make sure that the file name is `server.key`.

- The passphrase for the private key (`server.key` file) is released.
- A signed public key certificate (`.crt` file) has been acquired. Make sure that the file name is `server.crt`.
- The private key (`.key` file) must be in PEM format. You cannot use DER format.
- The signed public key certificate (`.crt` file) must be in X509 PEM format. You cannot use X509 DER format.
- The passphrase for the private key (`server.key` file) must be released.

Procedure

1. Close all management client sessions on the storage system, including Storage Advisor Embedded, maintenance utility, and Device Manager - Storage Navigator.
2. Open a command prompt window with administrator permissions.
3. Move the current directory to folder containing the SVP configuration tool (for example, `C:\MAPP\wk\Supervisor\MappIniSet`), and then execute the following command:

   `MappApacheCrtUpdate.bat` *`absolute-path-of-signed-public-key-certification-file absolute-path-of-private-key-file`*

   Note:
   - A space is required between `MappApacheCrtUpdate.bat` and the signed public key certification file path.
   - A space is required between the signed public key certification file path and the private key file path.
4. When the completion message appears, press any key to acknowledge the message and close the message box.
5. Close the command prompt window.

Returning the certificate to default

You can return the certificate that was updated by the procedure in Updating a signed certificate (on page 71) back to default.

Before you begin

- You must have the Storage Administrator (Initial Configuration) role to perform this task.
- You must be logged into the management client.
- A private key (`.key` file) has been created. Make sure that the file name is `server.key`. See Creating a private key using the OpenSSL command (on page 53).
- The passphrase for the private key (`server.key` file) is released.
- A signed public key certificate (`.crt` file) has been acquired. Make sure that the file name is `server.crt`. See Creating a public key using the OpenSSL command (on page 54).
- The private key (`.key` file) must be in PEM format. You cannot use DER format.

- The signed public key certificate (`.crt` file) must be in X509 PEM format. You cannot use X509 DER format. See Obtaining a self-signed certificate (on page 56).
- The extended profile fields in the X.509 certificate support the following items as specified in RFC5280:
  - BasicConstraints
  - KeyUsage
  - SubjectKeyIdentifier
  - subjectAltName
- The passphrase for the private key (`server.key` file) must be released.

Procedure

1. Close all management client sessions on the storage system, including Storage Advisor Embedded, maintenance utility, and Device Manager - Storage Navigator.
2. Open a command prompt window with administrator permissions.
3. Move the current directory to the folder containing the SVP configuration tool (for example, `C:\MAPP\wk\Supervisor\MappIniSet`), and then execute the following command:

   ```
   MappApacheCrtInit.bat
   ```
4. When the completion message appears, press any key to acknowledge the message and close the message box.
5. Close the command prompt window.

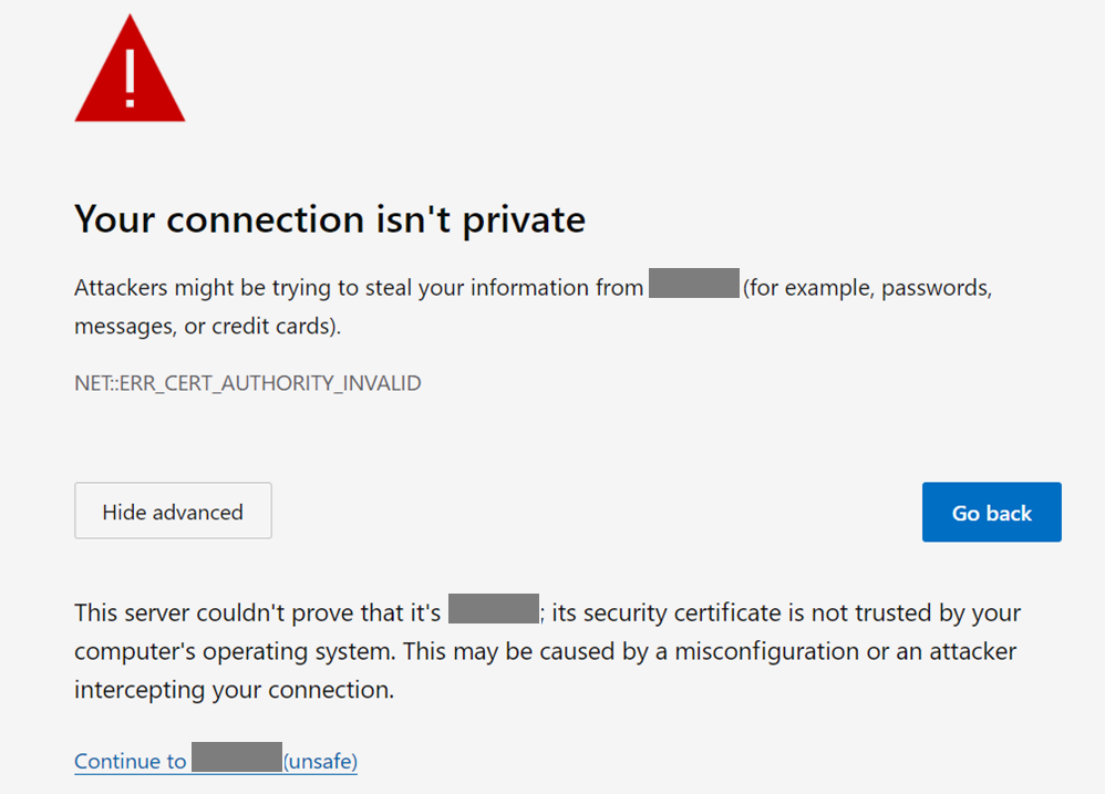
Actions to take when a security warning is displayed

The security warning below might appear during a setting operation using SSL communications. This warning differs depending on the type of web browser.

- For Microsoft Edge:

  Click **Advanced** and then **Continue to <*IP-address-or-host-name*> (unsafe)**.

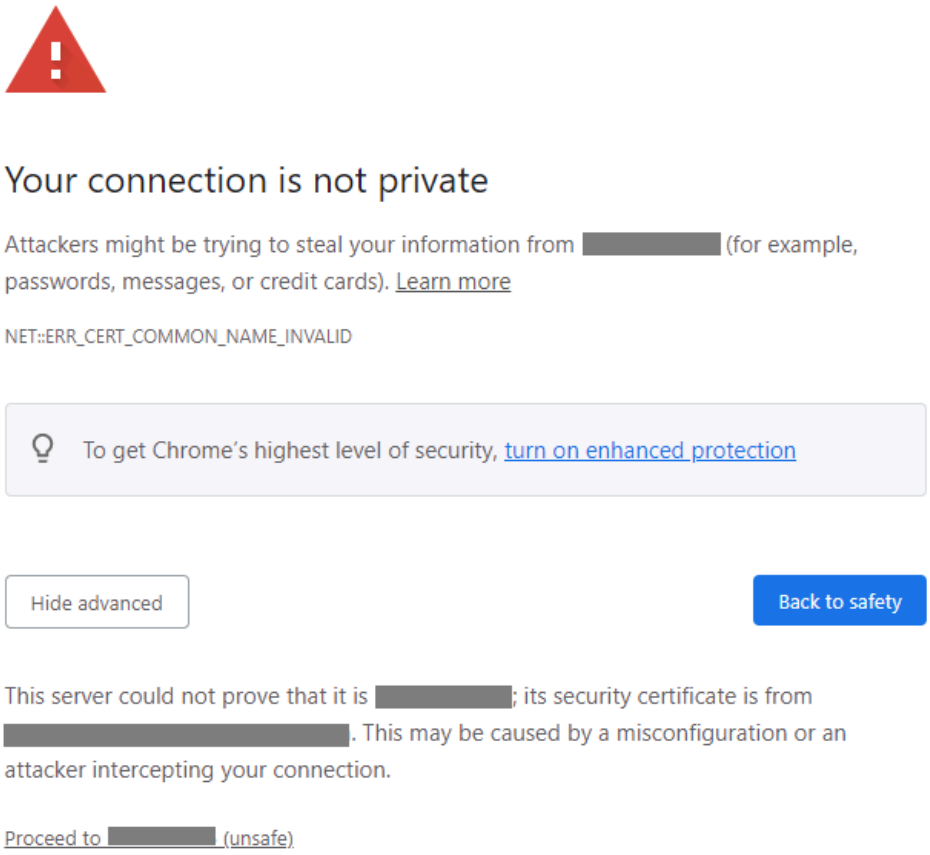
  Example for Microsoft Edge



- For Google Chrome:

  Click **Advanced**, and then click **Proceed to <*IP-address*> (unsafe)**.

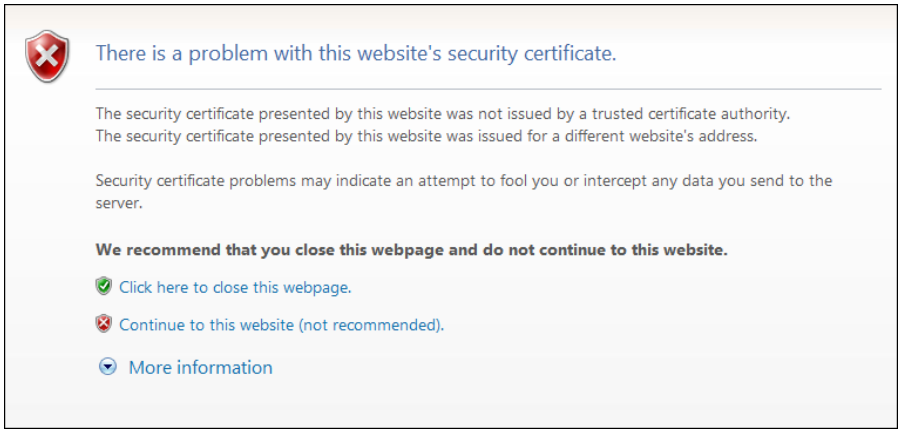
  Example for Google Chrome



- For Internet Explorer:

  Click **Continue to this website (not recommended)**.

  Example for Internet Explorer



When you are using encrypted SSL communications to connect to Device Manager - Storage Navigator, the browser displays a warning message if the security certificate is not issued by a trusted certificate authority. This warning message also appears when the IP address or host name specified in the URL does not match the CN (Common Name) listed in the security certificate.

If this warning message starts to appear after an update of the storage management software, check to see if the SSL certificate returned to the default. If the SSL certificate has returned to the default, install the certificate file that was backed up when the storage management software was updated.

Updating the certificate files

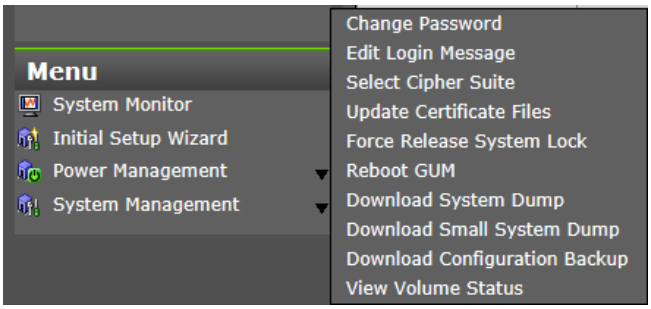
The **Update Certificate Files** window is used to update the certificates that are used for communication between the management client and the storage system.

Before you begin

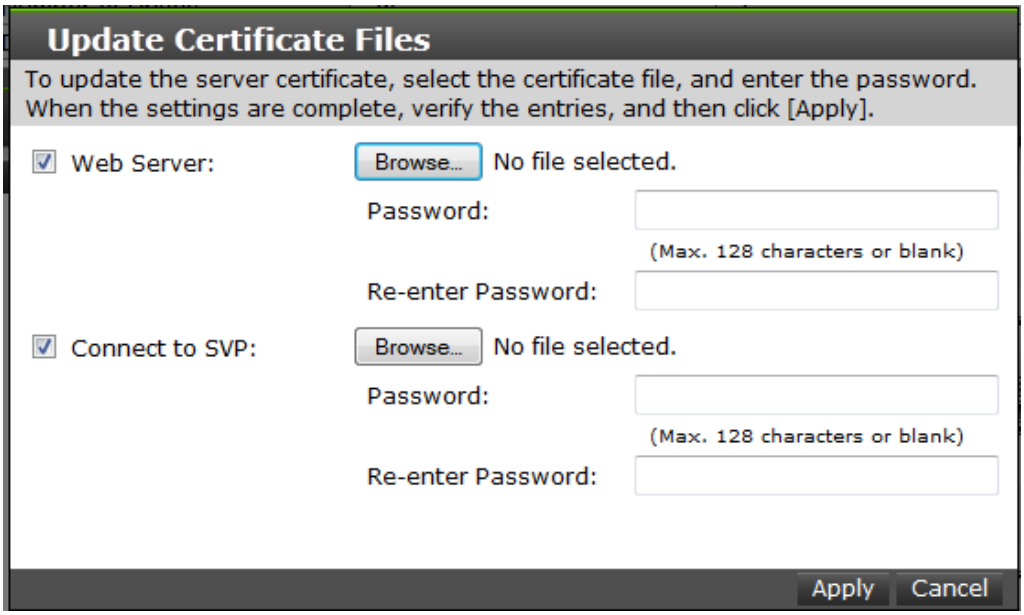
- You must have the Storage Administrator (View & Modify) role to complete this procedure.

Procedure

1. In the maintenance utility **Menu** navigation tree, click **System Management**.



2. Click **Update Certificate Files**.



Note: For storage systems without an SVP, unselect the **Connect to SVP** box.

3. To update the certificate file on the management client:
   a. Select the **Web Server** checkbox, then click **Browse.**
   b. Browse to the certificate file and click **Open**. The **File Upload** window closes and returns you to the **Update Certificate Files** dialog box.
   c. In the Web Server **Password:** field, enter the certificate password.
   d. Enter the password again in the Web Server **Re-enter Password:** field.

   Note: For storage systems without an SVP, continue to step 5.

4. To update the certificate file on the SVP:
   a. Select the **Connect to SVP** checkbox, then click **Browse**.
   b. Browse to the certificate file and click **Open**. The **File Upload** window closes and returns you to the **Update Certificate Files** dialog box.
   c. In the Connect to SVP **Password:** field, enter the certificate password.
   d. Enter the password again in the Connect to SVP **Re-enter Password:** field.
5. Click **Apply** to update the certificates.

Updating SSL certificates for the SVP and storage system in a batch

If only one storage system is registered in the SVP, you can update the following SSL certificates in a batch:

- Signed certificate for SSL communication between the SVP and the management client
- Certificate for connecting to the SVP
- Certificate for connecting to the web server on the storage system

Note: The extended profile fields in the X.509 certificate support the following items as specified in RFC5280:

- BasicConstraints
- KeyUsage
- SubjectKeyIdentifier
- subjectAltName

Before you begin

- Ensure that only one storage system is registered in the SVP.
- A private key for external communication between the SVP and the management client has been created.
- A signed public key certificate for external communication between the SVP and the management client has been acquired.

- A private key for internal communication for connecting to the SVP or web server and a signed public key certificate must be X509 PEM or X509 DER format.
- All users must be logged out of Hitachi Device Manager - Storage Navigator.
- You must have the Security Administrator (View & Modify) role and Support Personnel (User) role to perform this task.

Create the following parameter file (in JSON format) beforehand. Allowed characters when you specify the path to the certificate in the parameter file are alphanumeric characters, spaces, and symbols: - _ . \ / :.

- "user": *"user-name-of-the-account-registered-in-the-storage-system"*
- "password": *"password-of-the-account-registered-in-the-storage-system"*
- "innerConnectionCertPath": *"absolute-path-to-the-public-key-certificate-for-internal-communication"*
- "innerPrivateKeyPath": *"absolute-path-to-the-private-key-for-internal-communication"*
- "outerConnectionCertPath": *"absolute-path-to-the-public-key-certificate-for-external-communication"*
- "outerPrivateKeyPath": *"absolute-path-to-the-private-key-for-external-communication"*

```
{
"user": "someuser",
"password": "password123",
"innerConnectionCertPath": "c:\\sslcert\\innercert.crt",
"innerPrivateKeyPath": "c:\\sslcert\\innercert.key",
"outerConnectionCertPath": "c:\\sslcert\\outercert.crt",
"outerPrivateKeyPath": "c:\\sslcert\\outercert.key"
}
```

Procedure

1. On the SVP, start Windows command prompt as an Administrator.
2. Move the current directory to the directory where the tool exists

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet
   ```

   Note:

   - `C:\Mapp` indicates the installation directory of the storage management software and the SVP software. When the installation directory other than `C:\Mapp` was specified, replace `C:\Mapp` with the specified installation directory.
   - If you specify `--ignore-cert-verification`, the signed certificate for SSL communication between the SVP and the management client is not verified when the certificate is updated. Specify this option immediately after you install HDvM - SN on the SVP or when the certificate has not been normally updated. (You must check the IP address of the GUM on the storage system beforehand.)
   - If you specify `--delete`, the parameter file is automatically deleted after the SSL certificate is updated.

3. Run the following command:

```
mappsslcertupdate.bat
        --file=name-of-the-parameter-file-created-beforehand
```

4. A message appears indicating that the command finished, and then the GUM restarts automatically.
5. Restart the SVP manually.

Administering management software certificates

You can set or delete certificates for management software, including Hitachi Ops Center Administrator and Hitachi Command Suite, that are used to check the server's reliability when SSL communication external authentication is performed.

You cannot register the certificate for both Ops Center Administrator and HCS at the same time. Register one of the certificate for the server you are using to manage the storage system.

Registering management software certificates

To check the server reliability during SSL communication for management software external authentication, upload a public key certificate of the management software to the web server to register the certificate.

Before you begin

- You must be logged into the SVP.
- The private key file on the management software server must be current. Update it if necessary.
- The certificate file must have a .crt extension. Rename the file if necessary.
- The certificate must be in X509 PEM format or X509 DER format.

Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Open a command prompt window with administrator permissions.
3. Move the current directory to the folder containing the SVP configuration tool (for example, `C:\MAPP\wk\Supervisor\MappIniSet`), and then execute the following command:

   `MappHcsCrtEntry.bat` *`absolute-path-of-signed-public-key-certificate-file`*

   If you are using Hitachi Ops Center Administrator, execute the same command.

   Note: A space is required between `MappHcsCrtEntry.bat` and the signed public key certification file path.

4. When the completion message box appears, press any key to acknowledge the message and close the message box.
5. Close the command prompt window.

Deleting management software certificates

You can delete the certificates you registered for the following management software:

- Hitachi Ops Center Administrator
- Hitachi Command Suite (HCS)

After you delete a certificate, server reliability for that certificate is not checked by SSL communication for management software external authentication.

Before you begin

- You must be logged into the SVP.
- The private key file on the management software server must be current. Update it if necessary.
- The certificate file must have a `.crt` extension. Rename the file if necessary.
- The certificate must be in X509 PEM format or X509 DER format.

Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Open a command prompt window with administrator permissions.
3. Move the current directory to the folder containing the SVP configuration tool (for example, `C:\MAPP\wk\Supervisor\MappIniSet`), and then execute the following command:

   ```
   MappHcsCrtDelete.bat
   ```

   Use this command for Ops Center Administrator and for HCS.
4. When the completion message box appears, press any key to acknowledge the message and close the message box.
5. Close the command prompt window.

Using HSTS

HSTS (HTTP Strict Transport Security) is a security mechanism used when the Web server communicates with the Web browser using HTTPS.

Note: If you enable HSTS, you might not connect to Device Manager - Storage Navigator by using HTTP. If the connection does not work by using HTTP, use HTTPS.

Enabling HSTS

HTTP Strict Transport Security (HSTS) is a security mechanism that informs web browsers they can communicate with web servers only through secured HTTPS connections. Use the following procedure to enable HSTS.

Caution: If you enable HSTS, you might not be able to use HTTP for connection to Device Manager - Storage Navigator. In this case, use HTTPS for connection to Device Manager - Storage Navigator.

Procedure

1. On the SVP, open a command prompt with administrator permissions.
2. Move the current directory to the folder containing the setting tool.
3. Execute the following command:

```
cd /d C:\Mapp\wk\Supervisor\MappIniSet
MappHstsEnable.bat
```

Note: `C:\Mapp` indicates the installation directory of the storage management software and SVP software. If you specified a different installation directory, replace `C:\Mapp` with the specified installation directory.

4. When prompted, press any key to continue.
5. To verify that HSTS is enabled, execute the following command:

```
MappHstsState.bat
```

   - If "hsts=on" appears, HSTS is enabled. Press the Enter key, and then go to the next step.
   - If "hsts=off" appears, HSTS is not enabled. Press the Enter key, and then go back to step 3.
   - If a message indicating that the specified file could not be found appears, the HSTS settings failed. Press the Enter key, and then go back to step 3.

6. Close the command prompt window.

Disabling HSTS

To disable HSTS, use the following procedure:

Procedure

1. Open a command prompt with administrator permissions on the SVP.

2. Move the current directory to the folder in which the setting tool is located, and then execute the following command:

```
cd /d C:\Mapp\wk\Supervisor\MappIniSet
MappHstsDisable.bat
```

> **Note:** `C:\Mapp:` indicates the installation directory of storage management software and SVP software. If you specified an installation directory other than `C:\Mapp`, replace `C:\Mapp` with the specified installation directory.

3. When "Press any key to continue ..." appears in the window, press the Enter key.
4. To verify that HSTS is disabled, execute the following command:

   `MappHstsState.bat`

> **Note:**
>
> If "hsts=off" appears, HSTS is disabled. Press the Enter key. If "hsts=on" appears, HSTS is not disabled. Press the Enter key, and then go back to step 2.
>
> If the message indicating that the specified file could not be found appears, the HSTS settings failed. Press the Enter key, and then go back to step 2.

5. Close the command prompt window.

Chapter 4: User authentication and authorization with Device Manager - Storage Navigator

An authentication server enables users to log in to Device Manager - Storage Navigator with the same password as the password they use for other applications. In addition, an authentication server can be configured to work with an authorization server so that user groups registered in the authorization server can be assigned to Device Manager - Storage Navigator users.

Setting up authentication and authorization with Device Manager - Storage Navigator

The following figures show the Device Manager - Storage Navigator login workflow without and with an authentication server. The authentication server must be configured for each user.

Note: If you use the SVP, enable authentication by the SVP and disable external authentication by the maintenance utility. For instructions, see Disabling external authentication by the maintenance utility (on page 105).

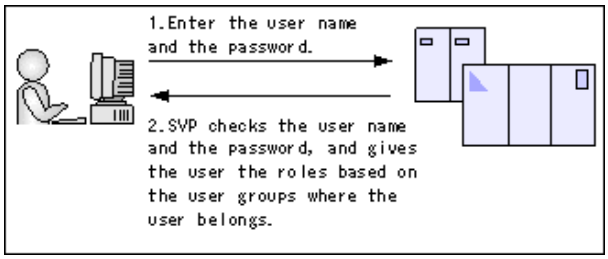


Figure 1 Logging in without an authentication server

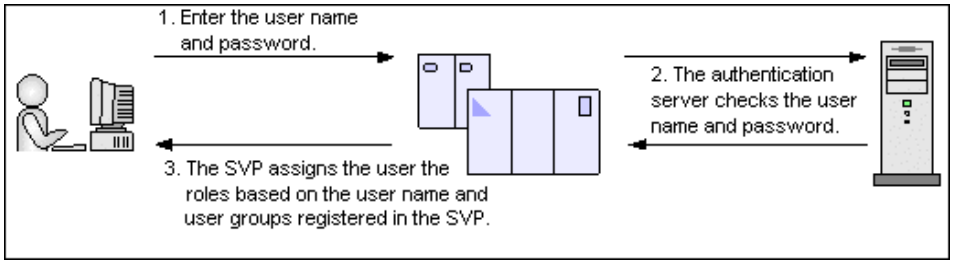
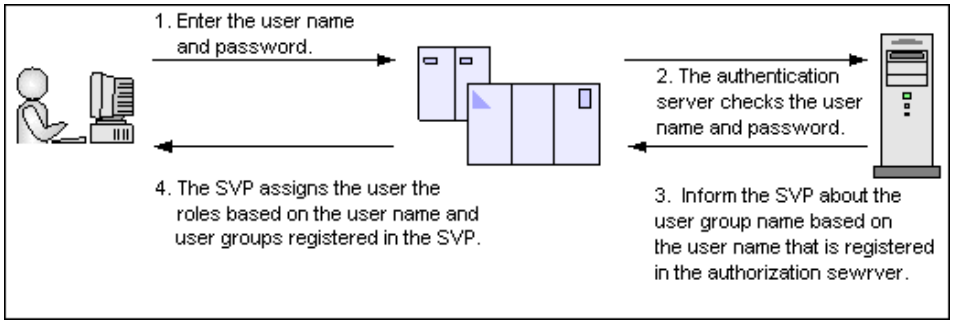


Figure 2 Logging in with an authentication server

The following figure shows the login workflow when an authentication server and an authorization server are used in combination. In this case, the user groups that are registered in the authorization server can be assigned to Device Manager - Storage Navigator users.

Figure 3 Logging in with an authentication server and an authorization server



If you register the information of the authentication server as an SRV record in the DNS server, you can use the authentication server without knowing the host names and port numbers. If you register multiple numbers of 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.

Caution:

- If the affiliated user group registered in the external authentication server and the user group registered locally in the storage system are different, the user group in the storage system has higher priority.
- You cannot create a load balancer between the SVP and the external authentication server.
- If you use external authentication of the SVP, you need to disable external authentication of the maintenance utility.

External authentication requirements using authentication server

Authentication servers support the following protocols:

- LDAPv3 simple bind authentication (Note that Bind DN is used for authentication.)
- RFC 2865-compliant RADIUS with PAP and CHAP authentication
- Kerberos v5

Note: The authentication server must support TLS1.2 as a transfer protocol.

The following root certificate file formats to be set on Device Manager - Storage Navigator are available for LDAP server settings:

- X509 DER format

- X509 PEM format

Note:

The root certificate to be set on Storage Navigator must satisfy the following requirements:

- The extended profile fields in the X.509 certificate support the following items as specified in RFC5280:
  - BasicConstraints
  - KeyUsage
  - SubjectKeyIdentifier
  - Authority Key Identifier
  - Certificate Policies
  - Subject Alternative Name
  - Name Constraints
  - Policy Constraints
  - Extended Key Usage
  - Inhibit anyPolicy

The certificate to be set on the connected server must satisfy the following requirements:

- The extended profile fields in the X.509 certificate support the following items as specified in RFC5280:
  - BasicConstraints
  - KeyUsage
  - SubjectKeyIdentifier
  - Authority Key Identifier
  - Certificate Policies
  - Subject Alternative Name
  - Name Constraints
  - Policy Constraints
  - Extended Key Usage
  - Inhibit anyPolicy
- If you set an IP address as the host name of the server for a configuration file (created in Connecting authentication and authorization servers (on page 104)), make sure to also set the IP address for subjectAltName or Common Name of a certificate (for a secure communication) that is created along with the configuration file.

  However, when using DNS Lookup, make sure to enter the host name of the server in subjectAltName or CommonName.

If the certificate contains both subjectAltName and CommonName, the IP address or the host name that you set for subjectAltName applies.

- If no DNS server is used, the IP address of the authentication server must be specified for the common name of the certificate.
- Check the number of tiers of the certificate chain to be used. The maximum number supported is 5 tiers. Make sure to use a certificate in the certificate chain with no more than 5 tiers.

One of the 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

Caution:

- Two authentication servers (one primary and one secondary) can be connected to a storage system. In this case, the server configurations must be the same, except for the IP address and the port. For the secondary server, use the same configuration settings as the primary server, except for the host name and the port number.
- If you search for a server using information registered in the SRV records in the DNS server, confirm that the following conditions are satisfied. For RADIUS servers, you cannot use the SRV records.

  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.
- Because UDP/IP is used to access the RADIUS server, encrypted communications, including negotiation between processes, are not used. To access the RADIUS server in a secure environment, encryption in the packet level, such as IPsec, is required.

External authorization requirements using authorization server

The authorization server must satisfy the following requirements to work together with the authentication server:

Note: Use an operating system (OS) and software that continue to be supported by the vendor. Operations performed using an OS or software for which vendor support has expired cannot be guaranteed.

Prerequisite OS

- Windows Server 2008*
- Windows Server 2008 R2*
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

* Microsoft support for this operating system has expired. Use an operating system for which Microsoft continues to provide support.

Prerequisite software

- Active Directory

Authentication protocol for user for searching

- LDAP v3 simple bind (Note that Bind DN is used for authentication.)

TLS security settings

- The TLS security settings made in Setting up SSL encryption using Device Manager - Storage Navigator (on page 51) must be supported.

Root certificate file format for Device Manager - Storage Navigator

- X509 DER format
- X509 PEM format

Requirements for root certificate format for Device Manager - Storage Navigator

- If the public key of the certificate to be uploaded is RSA, the key length must not be less than the key length that is set for Minimum Key Length (Key Exchange) in the **TLS Security Settings** dialog box.
- If the public key of the certificate to be uploaded is ECDSA, the public key parameter must be any of the following:
  - ECDSA_P256 (secp256r1)
  - ECDSA_P384 (secp384r1)
  - ECDSA_P521 (secp521r1)

- The signature hash algorithm of the certificate must be SHA-256, SHA-384, or SHA-512.
- The extended profile fields in the X.509 certificate support the following items as specified in RFC5280:
  - BasicConstraints
  - KeyUsage
  - SubjectKeyIdentifier
  - Authority Key Identifier
  - Certificate Policies
  - Subject Alternative Name
  - Name Constraints
  - Policy Constraints
  - Extended Key Usage
  - Inhibit anyPolicy

Requirements for certificate for the connected server

- If the public key of the certificate is RSA, the key length must be 2048 bits or more.
- If the public key of the certificate to be uploaded is ECDSA, the public key parameter must be any of the following:
  - ECDSA_P256 (secp256r1)
  - ECDSA_P384 (secp384r1)
  - ECDSA_P521 (secp521r1)
- The signature hash algorithm of the certificate must be SHA-256, SHA-384, or SHA-512.
- The extended profile fields in the X.509 certificate support the following items as specified in RFC5280:
  - BasicConstraints
  - KeyUsage
  - SubjectKeyIdentifier
  - Authority Key Identifier
  - Certificate Policies
  - Subject Alternative Name
  - Name Constraints
  - Policy Constraints
  - Extended Key Usage
  - Inhibit anyPolicy

When setting a host name for **Primary Host Name** or **Secondary Host Name** in the **Setup Server** window (Settings > User Management > View External Authentication Server Properties > Setup Server), enter the host name of the server in *subjectAltName* or *CommonName* of the server certificate.

- When setting an IP address for **Primary Host Name** or **Secondary Host Name** in the **Setup Server** window (Settings > User Management > View External Authentication Server Properties > Setup Server), enter the IP address of the server in *subjectAltName* or *CommonName* of the server certificate.
- If you set an IP address as the host name of the server for a configuration file (created in Connecting authentication and authorization servers (on page 104)), make sure to also set the IP address for *subjectAltName* or *CommonName* of a certificate (for a secure communication) that is created along with the configuration file.

  When using DNS Lookup to connect to an external authentication server, enter the host name of the server in *subjectAltName* or *CommonName* of the server certificate. If the certificate contains both *subjectAltName* and *CommonName*, the IP address or the host name that you set for *subjectAltName* applies.
- When you perform a certificate revocation check by using CRL, set the URI of the CRL repository for cRLDistributionPoint (CRL distribution point) of the intermediate certificate and server certificate set on the connected server. The CRL repository must be on the network that can be accessed by the SVP so that the SVP can communicate with the CRL repository. If the SVP cannot communicate with the CRL repository, communication with the authorization server fails.
- When you perform a certificate revocation check by using OCSP, correctly set the URI of the OCSP responder for authorityInfoAccess (Authority Information Access) of the intermediate certificate and server certificate set on the connected server. The OCSP responder must be on the network that can be accessed by the SVP so that the SVP can communicate with the OCSP responder. If the SVP cannot communicate with the OCSP responder, communication with the authorization server fails.
- If no DNS server is used, the IP address of the authorization server must be specified for the common name of the certificate.
- Check the number of tiers of the certificate chain to be used. The maximum number supported is 5 tiers. Make sure to use a certificate in a certificate chain with no more than 5 tiers.

Note:

- Acquire the root certificate for the authentication server from the authentication server administrator.
- The certificates has an expiration date. If the certificate expires, you will not be able to connect to the authentication server. Make sure to set the expiration date carefully to prepare the certificate.
- For more information about the certificate management, consult with the authentication server administrator and manage it appropriately.

Note: When using an LDAP server or a Kerberos server as an authentication server, and combining it with an authorization server, use the same host for the authentication and authorization servers.

When a RADIUS server is used as an authentication server, two authentication servers (one primary and one secondary) can be specified, but only one authorization server can be specified.

If you use Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 as an authorization server, the SSL communications cannot be established by using DHE in the default settings. When you use any of these servers as the authorization server, configure the SSL communication settings by using Device Manager - Storage Navigator to disable the cipher suites that use DHE for key exchange.

Creating configuration files

Authentication servers and authorization servers must be configured using configuration files.

Configuration files can be created for LDAP, RADIUS, and Kerberos authentication protocols.

Creating an LDAP configuration file

You can use an LDAP server for authentication on your storage system.

To use an LDAP server for authentication, create a configuration file in UTF-8 encoding. Include information about the authentication server as shown in the following example. Any file name and extension is allowed.

Caution: If you save the configuration file when using the Windows standard Notepad application, specify ANSI for the letter code. If you use an editor other than the memo pad and have the YTF-8 BOM setting, specify No BOM and then save.

```
auth.server.type=ldap
auth.server.name=<server_name>
auth.group.mapping=<value>
auth.ldap.<server_name>.<attribute>=<value>
```

A full example is shown here:

```
auth.server.type=ldap
auth.server.name=PrimaryServer
auth.group.mapping=true
auth.ldap.PrimaryServer.protocol=ldaps
auth.ldap.PrimaryServer.host=ldaphost.domain.local
auth.ldap.PrimaryServer.port=636
auth.ldap.PrimaryServer.timeout=3
auth.ldap.PrimaryServer.attr=sAMAccountName
auth.ldap.PrimaryServer.searchdn=CN=sample1,CN=Users,DC=domain,DC=local
```

```
auth.ldap.PrimaryServer.searchpw=password
auth.ldap.PrimaryServer.basedn=CN=Users,DC=domain,DC=local
auth.ldap.PrimaryServer.retry.interval=1
auth.ldap.PrimaryServer.retry.times=3
auth.ldap.PrimaryServer.domain.name=EXAMPLE.COM
```

The LDAP attributes are defined in the following table.

Attribute	Description	Required / Optional	Default value
auth.server.type	Type of authentication server. Specify `ldap`.	Required	None
auth.server.name	Name of the authentication server (referred to as `<server_name>`). When registering a primary and a secondary server, use a comma to separate the names. The name of the server, including the primary name, secondary name, and the comma (1 byte) must be 64 bytes or less. The name can use all ASCII code characters except for the following: \ / : , ; * ? " < > | $ % & ' ~	Required	None
auth.group.mapping	Information about whether to work together with an authorization server: ▪ `true`: Works together. ▪ `false`: Does not work together.	Optional	False
auth.ldap.<server_name>.protocol	LDAP protocol to use. Specify `ldaps` (uses LDAP over SSL/TLS). Do not specify `starttls` (uses StartTLS).	Required	None

Attribute	Description	Required / Optional	Default value
auth.ldap.<server_name>.host	Host name, an IPv4 address or an IPv6 address of the LDAP server. An IPv6 address must be enclosed in square brackets. To use StartTLS as a protocol, specify a host name. If this value is specified, `auth.ldap.<server_name>.dns_lookup` will be ignored.	Optional[1]	None
auth.ldap.<server_name>.port	Port number of the LDAP server. Must be between 1 and 65,535.[2]	Optional	389
auth.ldap.<server_name>.timeout	Number of seconds before the connection to the LDAP server times out. Must be between 1 and 30.[2]	Required	10
auth.ldap.<server_name>.attr	Attribute name to identify a user (such as a user ID). ▪ Hierarchical model: An attribute name where the value that can identify a user is stored. ▪ Flat model: An attribute name for a user entry's RDN. sAMAccountName is used for Active Directory.	Required	None
auth.ldap.<server_name>.searchdn	DN of the user for searching. If omitted, `[value_of_attr]=[Login_ID],[value_ of _basedn]` is used for bind authentication.[3]	Otional	None
auth.ldap.<server_name>.searchpw	User password that is used for searching. Specify the same password that is registered in the LDAP server.	Required	None

Attribute	Description	Required / Optional	Default value
auth.ldap.<server_name>.basedn	BaseDN for searching for users to authenticate.[3] ▪ Hierarchical model: DN of hierarchy that includes all the targeted users for searching. ▪ Flat model: DN of hierarchy that is one level up from the targeted user for searching.	Required	None
auth.ldap.<server_name>.retry.interval	Retry interval in seconds when the connection to the LDAP server fails. Must be between 1 and 5.[2]	Optional	1
auth.ldap.<server_name>.retry.times	Retry times when the connection to the LDAP server fails. Must be between 0 and 3. Zero means no retry.[2]	Optional	3
auth.ldap.<server_name>.domain.name	Domain name that the LDAP server manages.	Required	None
auth.ldap.<server_name>.dns_lookup	Information about whether to search the LDAP server with the information registered in the SRV records in the DNS server. Specify `false` (Searches with the host name and port number). Do not specify `true` (Searches with the information registered in the SRV records in the DNS server).	Optional	False

Notes:

1. This item can be omitted if `true` is specified for `auth.ldap.<server_name>.dns_lookup`.
2. If the specified value is not valid, the default value is used.
3. To use symbols such as + ; , < = and >, type a backslash (\) before each symbol. When using multiple symbols, each symbol must have a backslash before it. For example, to enter `abc++` in the basedn or searchdn field, type `abc\+\+`.

Attribute	Description	Required / Optional	Default value
	To enter \ , /, or ", type a backslash (\) followed by the ASCII code in hex for the character: ▪ To enter a backslash (\), type `\5c`. ▪ To enter a forward slash (/), type `\2f`. ▪ To enter a quotation mark ("), type `\22`.		

Creating a RADIUS configuration file

You can use a RADIUS server for authentication on your storage system.

To use a RADIUS server for authentication, create a configuration file in UTF-8 encoding. Include information about the authentication server as shown in the following example. Any file name and extension is allowed. If an authorization server is not used, you do not need to define the items for it.

Caution: If you save the configuration file when using the Windows standard Notepad application, specify ANSI for the letter code. If you use an editor other than the memo pad and have the YTF-8 BOM setting, specify No BOM then save.

```
auth.server.type=radius
auth.server.name=server-name
auth.group.mapping=value
auth.radius.server-name.attribute=value
auth.group.domain-name.attribute=value
```

A full example is shown below:

```
auth.server.type=radius
auth.server.name=PrimaryServer
auth.group.mapping=true
auth.radius.PrimaryServer.protocol=PAP
auth.radius.PrimaryServer.host=example.com
auth.radius.PrimaryServer.port=1812
auth.radius.PrimaryServer.timeout=3
auth.radius.PrimaryServer.secret=secretword
auth.radius.PrimaryServer.retry.times=3
auth.radius.PrimaryServer.domain.name=radius.example.com
auth.group.radius.example.com.protocol=ldaps
auth.group.radius.example.com.host=xxx.xxx.xxx.xxx
auth.group.radius.example.com.port=636
auth.group.radius.example.com.searchdn=CN=sample1,CN=Users,DC=domain,DC=local
auth.group.radius.example.com.searchpw=password
auth.group.radius.example.com.basedn=CN=Users,DC=domain,DC=local
```

The attributes are defined in the following tables.

Table 2 RADIUS definition (for authentication server)

Attribute	Description	Required / Optional	Default value
auth.server.type	Type of authentication server Specify `radius`.	Required	None
auth.server.name	Name of the server (referred to as <server_name>) When registering a primary and secondary server, use a comma to separate the names. The name of the server, including the primary name, secondary name, and the comma (1 byte) must be 64 bytes or less. The names can use all ASCII code characters except for the following: \ / : , ; * ? " < > | $ % & ' ~	Required	None
auth.group.mapping	Information about whether to work together with an authorization server ▪ `true`: Works together. ▪ `false`: Does not work together.	Optional	False
auth.radius.*server-name*.protocol	RADIUS protocol to use ▪ PAP: Password authentication protocol that transmits plaintext user ID and password. ▪ CHAP: Challenge-handshake authentication protocol that transmits encrypted password.	Required	None
auth.radius.*server-name*.host	Host name, IPv4 address, or IPv6 address of the RADIUS server An IPv6 address must be enclosed in square brackets.	Required[1]	None
auth.radius.*server-name*.port	Port number of the RADIUS server Must be between 1 and 65,535.	Optional[2]	1,812
auth.radius.*server-name*.timeout	Number of seconds before the connection to the RADIUS server times out Must be between 1 and 30.	Optional[2]	10

Attribute	Description	Required / Optional	Default value
auth.radius.*server-name*.secret	RADIUS secret key used for PAP or CHAP authentication	Required	None
auth.radius.*server-name*.retry.times	Retry times when the connection to the RADIUS server fails Must be between 0 and 3. 0 means no retry.	Optional[2]	3
auth.radius.*server-name*.attr.NASIdentifier	Identifier for the RADIUS server to find SVP Specify this value if the `attr.NAS-Identifier` attribute is used in your RADIUS environment. ASCII codes up to 253 bytes long are accepted.	Optional	None
auth.radius.*server-name*.attr.NAS-IPv4-Address	IPv4 address of the SVP Specify this value if the `attr.NAS-Identifier` attribute is used in your RADIUS environment. ASCII codes up to 253 bytes long are accepted.	Optional	None
auth.radius.*server-name*.attr.NAS-IPv6-Address	IPv6 address of the SVP Specify the value of the `NAS-IPv6-Address` attribute. This value is transmitted to the RADIUS server when the authentication is requested.	Optional	None

Notes:

1. If you query DNS with external authorization, the settings are not required.
2. If the specified value is not applicable, the default value is used.

Table 3 RADIUS definition (for authorization server)

Attribute	Description	Required / Optional	Default value
auth.radius.*server-name*.domain.name	Domain name that the LDAP server manages (referred to as *domain-name*)	Required	None
auth.radius.*server-name*.dns_lookup	Information about whether to search the LDAP server with the information registered in the SRV records in the DNS server	Optional	false

Attribute	Description	Required / Optional	Default value
	Specify `false` (searches with the host name and port number). Do not specify `true` (searches with the information registered in the SRV records in the DNS server).		
auth.group.*domain-name*.protocol	LDAP protocol to use Specify `ldaps` (uses LDAP over SSL/TLS). Do not specify `starttls` (uses StartTLS).	Required	None
auth.group.*domain-name*.host	Host name, IPv4 address, or IPv6 address of the LDAP server. An IPv6 address must be enclosed in square brackets ([ ]).	Optional[1]	None
auth.group.*domain-name*.port	Port number of the LDAP server Must be between 1 and 65535.	Optional[2]	389
auth.group.*domain-name*.searchdn	DN of the user for searching	Required[3]	None
auth.group.*domain-name*.searchpw	User password for searching Specify the same password that is registered in the LDAP server.	Required	None
auth.group.*domain-name*.basedn	Base DN for searching for users to authenticate Specify DN of the hierarchy, including all the users for searching because the targeted users for searching are in lower hierarchy than the specified DN.	Optional[3]	abbr
auth.group.*domain-name*.timeout	Number of seconds before the connection to the LDAP server times out Must be between 1 and 30.	Optional[2]	10
auth.group.*domain-name*.retry.interval	Retry interval in seconds when the connection to the LDAP server fails Must be between 1 and 5.	Optional	1

Attribute	Description	Required / Optional	Default value
auth.group.*domain-name*.retry.times	Retry times when the connection to the LDAP server fails Must be between 0 and 3. 0 means no retry.	Optional[2]	3

Notes:

1. This item can be omitted if `true` is specified for `auth.radius.server-name.dns_lookup`.
2. If the specified value is not valid, the default value is used.
3. To use symbols such as + ; , < = and >, type a backslash (\) before each symbol. When using multiple symbols, each symbol must have a backslash before it. For example, to enter `abc++` in the basedn or searchdn field, type `abc\+\+`.

   To enter a backslash (\), forward slash (/), or quotation mark ("), type a backslash (\) followed by the ASCII code in hex:

   - To enter a backslash (\), type `\5c`.
   - To enter a forward slash (/), type `\2f`.
   - To enter a quotation mark ("), type `\22`.

Creating a Kerberos configuration file

You can use a Kerberos server for authentication on your storage system.

To use a Kerberos server for authentication, create a configuration file in UTF-8 encoding. Include information about the authentication server as shown in the following example. Any file name and extension are allowed. If an authorization server is not used, you do not need to define the items for it.

Caution: If you save the configuration file when using the Windows standard Notepad application, specify ANSI for the letter code. If you use an editor other than the memo pad and have the YTF-8 BOM setting, specify `No BOM` and then save.

```
auth.server.type=kerberos
auth.group.mapping=<value>
auth.kerberos.<attribute>=<value>
auth.group.<realm name>.<attribute>=<value>
```

A full example is shown below:

```
auth.server.type=kerberos
auth.group.mapping=true
auth.kerberos.default_realm=example.com
```

```
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=10
auth.group.example.com.protocol=ldaps
auth.group.example.com.port=636
auth.group.example.com.searchdn=CN=sample1,CN=Users,DC=domain,DC=local
auth.group.example.com.searchpw=password
auth.group.example.com.basedn=CN=Users,DC=domain,DC=local
```

The Kerberos attributes are defined in the following table.

Table 4 Kerberos definition (for authentication server)

Attribute	Description	Required / Optional	Default value
auth.server.type	Type of authentication server. Specify `kerberos`.	Required	None
auth.group.mapping	Information about whether to work together with an authorization server: ▪ `true`: Works together. ▪ `false`: Does not work together.	Optional	false
auth.kerberos.default_realm	Default realm name	Required	None
auth.kerberos.dns_lookup.kdc	Switch that determines which information registered in the SRV records in the DNS server to use when searching the Kerberos server. Specify `false` (searches with the host name and port number). Do not specify `true` (searches with the information registered in the SRV records in the DNS server).	Optional	false
auth.kerberos.clockskew	Acceptable range of the difference in time between the SVP and the Kerberos server where the SVP is operating. Must be between 0 and 300 seconds.	Optional[1]	300

Attribute	Description	Required / Optional	Default value
auth.kerberos.timeout	Number of seconds before the connection to the RADIUS server times out. Must be between 1 and 30. When 0 is specified, the connection does not time out until a communication error occurs.	Optonal[1]	10
auth.kerberos.realm_name	Realm identifier name (referred to as <realm_name>) Any name to distinguish the information of Kerberos server in each realm. Duplicate names cannot be used. If you register multiple names, use a comma to separate the names.	Optional[2]	None
auth.kerberos.<realm _name>.realm	Realm name set to the Kerberos server.	Optional[2]	None
auth.kerberos.<realm_name>.kdc	Host name, the IPv4 address, and port number of the Kerberos server. Specify these in the format of `<Host name or IP address>[:Port number]`.	Optional[2]	None

Notes:

1. If the specified value is not valid, the default value is used.
2. This item can be omitted if `true` is specified for `auth.kerberos.dns_lookup_kdc`.

Table 5 Kerberos definition (for authorization server)

Attribute	Description	Required / Optional	Default value
auth.group.<realm_name>.protocol	LDAP protocol to use. Specify `ldaps` (uses LDAP over SSL/ TLS).	Required	None

Attribute	Description	Required / Optional	Default value
	Do not specify `starttls` (uses StartTLS).		
auth.group.<realm_name>.port	Port number of the LDAP server. Must be between 1 and 65535.	Optional[1]	389
auth.group.<realm_name>.searchdn	DN of the user for searching.	Required[2]	None
auth.group.<realm_name>.searchpw	Password of the user for searching. Specify the same password that is registered in the LDAP server.	Required	None
auth.group.<realm_name>.basedn	BaseDN when the search for users begins. When searching, specify the hierarchy DN, including all the users, because the targeted user for the search is in a lower hierarchy than the specified DN.	Optional[2]	abbr
auth.group.<realm_name>.timeout	Number of seconds before the connection to the LDAP server times out. Must be between 1 and 30 seconds. When 0 is specified, the connection does not time out until a communication error occurs.	Optional[1]	10

Attribute	Description	Required / Optional	Default value
auth.group.<realm_name>.retry.interval	Retry interval in seconds when the connection to the LDAP server fails. Must be between 1 and 5.	Optional[1]	1
auth.group.<realm_name>.retry.times	Retry times when the connection to the LDAP server fails. Must be between 0 and 3. 0 means no retry.	Optional[1]	3

Notes:

1. If the specified value is not valid, the default value is used.
2. To use symbols such as + ; , < = and >, type a backslash (\) before each symbol. When using multiple symbols, each symbol must have a backslash before it. For example, to enter `abc++` in the basedn or searchdn field, type `abc\+\+`.

   To enter a backslash (\) , forward slash (/), or quotation mark ("), type a backslash followed by the ASCII code in hex:

   - To enter a backslash (\), type `\5c`.
   - To enter a forward slash (/), type `\2f`.
   - To enter a quotation mark ("), type `\22`.

Connecting two authentication servers

Two authentication servers can be connected to a storage system. 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:

Note: For RADIUS servers, you cannot use the SRV records.

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.

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.

Connecting authentication and authorization servers

To use an authentication server and an authorization server, you must create configuration files and configure your network. Detailed setting information is required for the authentication server and the authorization server, especially for creating a configuration file.

Before you begin

- 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, obtain certification for the LDAP server files.
- Contact your network administrator for information about the network settings.

Procedure

1. Create a configuration file. The items to specify depend on the protocol you use.
2. Log in to the SVP and store the following files in an easily accessible location.
   - Certificate (for secure communication)
   - Configuration file
3. Open the Windows command prompt on the SVP.
4. Move the current directory to the folder containing the SVP configuration tool (for example, `C:\MAPP\wk\Supervisor\MappIniSet`), and then execute the following command specifying the configuration file path and the certificate file path:

   ```
   MappSetExAuthConf "C:\auth\auth.properties" "C:\auth\auth.cer"
   ```
5. When the confirmation message appears, press **y** to delete the files.

   If you do not delete these files now when prompted, delete them manually.

Note: If the authentication server and the authorization server are unusable even after you make the settings, the network or the configuration file settings might have a problem. Contact the server administrator or the network administrator.

Next steps

After you complete the settings and verify that you can use the authentication and authorization servers, back up the connection settings for the authentication server.

Disabling external authentication by the maintenance utility

If you use the SVP, enable authentication by the SVP, and also disable external authentication by the maintenance utility.

Use the following procedure to disable external authentication server by the maintenance utility.

Procedure

1. Log in to the maintenance utility.
2. Click **Administration** > **External Authentication** > **Set Up Server** > **Disable**.
3. When the confirmation window appears, click **Apply**.
4. When the completion message appears, click **Close**.

Chapter 5: Configuring the storage system

Initial storage system configuration includes tasks such as entering the storage system information (name, location, contact information), setting the date and time, creating a login message, configuring SMI-S on the SVP, and setting up the syslog server for the audit logs.

Note:

- VSP E990 supports the physical and virtual SVP with full functionality (Device Manager - Storage Navigator, SMI-S, and so on).
- VSP E1090, VSP E790, and VSP E590 support only the virtual SVP and only for enabling and administering VVOL/VASA, SMI-S, and KMIP operations.

Setting storage system information

You can set the name, contact information, and location of the storage system.

Caution: When changing a setting more than once, ensure that the current setting is complete before changing it again. Otherwise, only the new change will be applied, and the result might be different from what you expected.

Before you begin

- You must have the Storage Administrator (Initial Configuration) role to complete this procedure.

Procedure

1. In the Device Manager - Storage Navigator **Storage Systems** tree, select the storage system.
2. From **Settings**, click **Environmental Settings** > **Edit Storage System**.
3. Enter the items that you want to set.

   You can enter up to 180 alphanumeric characters (ASCII codes) excluding several symbols (\ , / ; : * ? " < > | & % ^). Do not use a space at the beginning or the end.
4. Click **Finish**.
5. In the **Confirm** window, check the settings and enter a task name in **Task Name**.
6. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Tasks** window opens to show the status of the task.

Changing the date and time

You can change the date and time for the controller clock and the SVP clock.

Note: The SVP supports Simple Network Time Protocol version 4 (SNTPv4) for date and time synchronization.

Regularly (preferably every day) check whether the time is synchronized with the NTP server. SIM reference code "7ffa00" is output if synchronization fails.

Changing the controller clock settings

Complete the following steps to change the date and time on the storage system controller.

Caution:

- If you change the system date and time when the currently set date and time is after the real time, the configuration information might not be backed up. To prevent this from happening, move the existing backup file to another folder and then change the system date and time.
- The date and time cannot be changed while a different user is accessing the storage system.
- If you use the SVP, make sure to also update the system date and time on the SVP.
- To use the NTP server, make sure to use the port number 123 for communications between the storage system and the NTP server. Therefore, configure the network settings between the storage system and the NTP server so that the communications using the port number 123 are established.

Before you begin

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

Procedure

1. In the maintenance utility **Administration** tree, select **Date & Time**.

   The current settings are displayed.
2. Click **Set Up**.
3. Change the settings as needed, and either click **Apply** to save them, or click **Cancel** to close the window without saving the changes.

Changing the SVP clock and time zone settings

If your configuration includes an SVP for external management servers, you need to ensure that the clock and the time zone settings on the SVP match those of the controller clock.

Note: The SVP supports Simple Network Time Protocol version 4 (SNTPv4) for date and time synchronization.

Before you begin

- The management client must be connected to the LAN 2 port on the SVP.
- The management client must have already established a remote desktop connection with the SVP. Note that the connection cannot be established when you use Remote Desktop Session Host.
- If storage systems are registered in the Storage Device List, click Stop Service for all registered storage systems in the Storage Device List window before changing the SVP clock settings.

Procedure

1. Log in to the management client that is connected to the SVP.
2. On the Windows 8.1 desktop, click **Start** > **Control Panel**.
3. Click **Clock, Language, and Region**.
4. Click **Date and Time**.
5. Click **Change date and time**.
6. In the **Date and Time Settings** window, set the date and time, and then click **OK** to save the settings.
7. Click **Change time zone**.
8. In the **Time Zone Settings** window, select the time zone, and then click **OK**.

Note: If you do not restart the background service, the time zone change is not reflected. When the time zones remain different between the SVP and the storage system, this condition can cause error conditions.

Changing network communication settings

Use the following procedure to change the network settings on the management client for communicating with the SVP.

Procedure

1. In the maintenance utility, click **Administration** to expand the **Administration** navigation pane.
2. Click **Network Settings**.
3. In the **Network Settings** window, click **Set Up Network Settings**.

   The **Network Settings** dialog box displays the current settings for the Mac address, IPv4 and IPv6 settings, and the network connection mode for controllers 1 and 2. It also displays the current settings for the maintenance port and the storage system internal network.
4. Change the settings as needed.

   If you set items for DNS server, register the following items to the DNS server:

   - host name: localhost
   - IP address: 127.0.0.1

If you set the protocol to both IPv4 and IPv6 and then switch only to IPv4 or IPv6, the **Network Settings** window displays settings for both IPv4 and IPv6. To verify the protocol settings, click **Set Up Network Settings**. The selected protocol is displayed in the dialog box, and the IP address of the invalid protocol is displayed in gray.

5. Click **Apply** to apply your changes.

Changing network permissions

This procedure explains how to block or allow HTTP blocking.

Procedure

1. In the maintenance utility, click **Administration** to expand the **Administration** navigation pane.
2. Click **Network Settings**. The **Network Settings** window displays the current network settings and permissions.
3. In the **Network Settings** window, click **Set Up Network Permissions**.
4. To enable HTTP blocking, click **Enable**. To disable HTTP blocking, click **Disable.**
5. Click **Apply**. The dialog box closes and returns you to the **Network Settings** window.

Configuring cloud connection settings

To connect the storage system to Ops Center Clear Sight, you need to configure firewall settings and cloud connection settings, including the organization code from Ops Center Clear Sight and proxy server settings, by using the **Set Up Cloud Connection Settings** window.

Note:

- **Cloud connector technology**

  Enabling cloud connector technology allows storage system configuration changes to be performed remotely.

- **Proxy server**

  The storage system supports only HTTP proxy with basic authentication.

- **Firewall**

  The direction of communication between the storage system and Ops Center Clear Sight goes from the storage system to Clear Sight, not from Clear Sight to the storage system. If you are using a firewall, you need to configure the firewall as shown below to communicate from the storage system to Ops Center Clear Sight.

  cloudconnector.hitachivantara.com:

Destination	Protocol	Port number
cloudconnector.hitachivantara.com	HTTPS	443
us-west-2.amazonaws.com	HTTPS	443

Setting up cloud connection

Use this procedure to configure your cloud connection settings for Ops Center Clear Sight.

Procedure

1. In the maintenance utility, click **Administration** to expand the Administration navigation pane, and then click **Cloud Connection Settings**.
2. In the **Cloud Connection Settings** window, click **Set Up Cloud Connection Settings**.
3. In the **Set Up Cloud Connection Settings** window, enter the desired settings.

Option	
Organization Code	Specify the organization code obtained from Ops Center Clear Sight. You can enter a character string of 8 alphanumeric characters excluding spaces.
Proxy	Select whether to set a proxy server. ▪ **Enable**: A proxy server is set. ▪ **Disable**: A proxy server is not set.

Option	
Server Settings	Specify the settings for the proxy server. ▪ **Identifier**: Enter the host name of the proxy server. You can enter up to 255 alphanumeric characters and symbols excluding " # & ' * + , / : ; < = > ? [\ ] ^ { | } and spaces. ▪ **IPv4**: Enter the IPv4 address of the proxy server. ▪ **IPv6**: Enter the IPv6 address of the proxy server. ▪ **Port Number**: Enter the port number of the proxy server.
Authentication	Select whether to set the authentication function. ▪ **Enable**: The authentication function is set. ▪ **Disable**: The authentication function is not set. ▪ **User Name**: Enter a user name used for authentication. You can enter up to 255 alphanumeric characters and symbols excluding : (colon). ▪ **Password**: Enter a password for the user name used for authentication. You can enter up to 255 alphanumeric characters and symbols.

4. Confirm the settings, and then click **Apply**.
5. When the completion message appears, click **Close**.

Clearing cloud connection settings

Use this procedure to clear your cloud connection settings for Ops Center Clear Sight.

Procedure

1. In the maintenance utility, click **Administration** to expand the Administration navigation pane, and then click **Cloud Connection Settings**.
2. In the **Cloud Connection Settings** window, click **Clear Cloud Connection Settings**.
3. In the **Clear Cloud Connection Settings** window, confirm the item to be cleared, and then click **Apply**.
4. When the completion message appears, click **Close**.

Changing advanced system settings

You can change alert display settings and data acquisition settings in advanced system settings.

Before you begin

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

Procedure

1. In the Device Manager - Storage Navigator main menu, click **Settings** > **Environmental Settings** > **Edit Advanced System Settings**.
2. Select the desired advanced system settings, and then click **Enable** to enable the selected settings or **Disable** to disable the selected settings.

Setting	Description
Hide alert information	If you enable this setting, the **Alert** window in the Device Manager - Storage Navigator main window does not open.
Refresh forcibly after Apply	If you enable this advanced system setting, after settings changes are applied to the storage system, the configuration information for the storage system is always updated to the latest information.
Disable data polling	If you enable this advanced system setting, polling stops.
Disable retry of data updating	If you enable this advanced system setting, retry does not occur even if data cannot be acquired.
Enable Storage Navigator 2 All Function	If you enable this advanced system setting, the restrictions on login from Device Manager - Storage Navigator's login window are cleared, including the restrictions on the users who can log in and on the functions available after login. When enabling or disabling this advanced system setting, log in again.
Manage differential bitmaps in DP pool at pair create operations for 4TB or less TC/UR/GAD pairs	When enabled, the differential data is maintained in a pool with which a DP-VOL that has the user capacity (up to 4,194,304 MB) is linked when a new TC/UR/GAD pair is created using the DP-VOL. Note that differential data is maintained, regardless of this setting, in a pool linked with the DP-VOL that has the user capacity (greater than 4,194,304 MB) when a new pair using the DP-VOL is created. For details about this setting, see the *Hitachi TrueCopy® User Guide*, *Hitachi Universal Replicator User Guide*, or *Global-Active Device User Guide*.
Manage differential bitmaps in DP pool at pair create operations for 4TB or less TC/UR/GAD pairs	When enabled, the differential data is maintained in a pool with which a DP-VOL that has the user capacity (up to 4,194,304 MB) is linked when a new TC/UR/GAD pair is created using the DP-VOL. Note that differential data is maintained, regardless of this setting, in a pool linked with the DP-VOL that has the user capacity (greater than 4,194,304 MB) when a new pair using the DP-VOL is created. For details about this setting, see the *Hitachi TrueCopy® User Guide*, *Hitachi Universal Replicator User Guide*, or *Global-Active Device User Guide*.

Setting	Description
Enable reboot of background service	Enable this setting only when requested. If you enable this setting, the SVP starts monitoring of the background service process (RMIServer). When either of the following values exceeds its threshold value, the background service process for managing configuration information is restarted: ▪ The amount of memory used in the background service process. ▪ Time elapsed after the background service process is started.
Disable cache of the PP Info	Enable this setting only when requested.
Notify an alert when tier relocation is suspended by system	If you enable this setting, when tier relocation is suspended by the system, an alert is issued to users. For details about an alert (SIM) to be issued, see the Troubleshooting chapter of the *Provisioning Guide for Open Systems* or *Provisioning Guide for Mainframe Systems*.

3. Click **Finish**.
4. In the confirmation window, check the settings and enter a task name in **Task Name**.
5. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Tasks** window opens to display the status of the task.
6. After you have enabled or disabled the desired advanced system settings, log off Device Manager - Storage Navigator and then log in again.

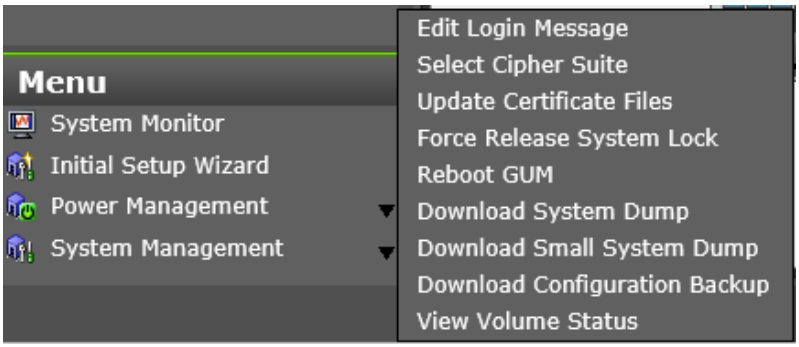
Creating a login message

Before you begin

You must have the Storage Administrator (View & Modify) role to complete this procedure.

Procedure

1. In the maintenance utility **Menu** navigation tree, click **System Management**.



2. Click **Edit Login Message**.
3. Enter a message to be displayed at the time of login. The message can contain up to 2,048 characters. A line break is counted as one character.
4. Click **Apply** to save the message and close the dialog box.

Using the SMI-S function on the HDvM - SN management client

VSP E series storage systems with a physical or virtual SVP support the SMI-S function developed by SNIA. Administrators can use the SMI-S function by using SMI-S compliant management software on the HDvM - SN management client.

Requirements for SMI-S support:

- A physical or virtual SVP with the following SVP firmware version:
  - VSP E990: 93-02-01 or later
  - VSP E1090: 93-06-21 or later
  - VSP E590, VSP E790: 93-06-41 or later
- TLS version 1.2
- Valid signed SMI-S certificate

  If the SMI-S certificate is expired, upload a new signed certificate to the SMI-S provider.

Using the SMI-S function

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

Procedure

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

   When the user accesses the SMI-S function with the read-only access authority, the user account must belong to one of the following built-in user groups:

   - Storage Administrator (Remote Copy)

2. In the management software program, enter the following storage system information:
   - **IP Address** of the SVP
   - **Protocol**: specify **HTTPS**
   - **Port**: **5989**

     Note: The allocation method of the port numbers to be used varies depending on the SVP software versions.
   - **Namespace**:**root/hitachi/smis** or **interop**

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.

Important: When the storage management software is updated, the private key and signed public key certificate might be returned to default. If this happens, you need to upload the private key and signed public key certificate to the SVP again.

Before you begin

Ensure that the following items have been completed:

- You must have the Storage Administrator (View & Modify) role to perform this task.
- A private key (`.key` file) must have been created. Change the file name to `server.key` unless the file is already named that. See Creating a private key using the OpenSSL command (on page 53).
- The passphrase for the private key (`server.key` file) is released.
- A signed public key certificate (`.crt` file) has been acquired. Change the file name to `server.crt` unless the file is already named that. See Creating a public key using the OpenSSL command (on page 54).
- The private key (`.key` file) is in PEM format. (You cannot use the DER format.)
- The signed public key certificate (`.crt` file) is in X509 PEM format. (You cannot use the X509 DER format.) See Obtaining a self-signed certificate (on page 56).

  The extended profile fields in the X.509 certificate support the following items as specified in RFC5280:
  - BasicConstraints
  - KeyUsage
  - SubjectKeyIdentifier
  - SubjectAltName
- If an intermediate certificate exists, prepare a signed public key certificate (`server.crt` file) that has a certificate chain that includes the intermediate certificate.

- The number of tiers of the certificate chain for the certificate to be uploaded must be 5 tiers or less including the root CA certificate.
- The public key encryption method for the certificate to be uploaded must be RSA.

Procedure

1. Log in to the SVP.
2. Close all Device Manager - Storage Navigator sessions on the SVP.
3. On the SVP, start Windows command prompt as an Administrator.
4. Move the current directory to the directory where the tool `MappApacheCrtUpdate.bat` exists (for example, `C:\MAPP\wk\Supervisor\MappIniSet`), and then execute the following command:

```
MappApacheCrtUpdate.bat <absolute-path-of-signed-public-key-certification-file>
<absolute-path-of-private-key-file>
```

Note:

- A space is required between `MappApacheCrtUpdate.bat` and the signed public key certification file path.
- A space is required between the signed public key certification file path and the private key file path.

5. When the completion message appears, press any key to acknowledge the message and close the message box.
6. Close the command prompt window.

Uploading an SMI-S provider configuration file

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

Before you begin

- Ensure that the SMI-S provider configuration file has already been created. If the configuration is not already named array-setting-01.properties, rename it to that name.
- You must have the Storage Administrator (View & Modify) role to perform this task.
- A private key (.key file) has been created. Make sure that the file name is server.key.
- A signed public key certificate (.crt file) has been acquired. Make sure that the file name is server.crt.
- The signed public key certificate (.crt file) must be in X509 PEM format. You cannot use X509 DER format.

- The extended profile fields in the X.509 certificate support the following items as specified in RFC5280:
  - BasicConstraints
  - KeyUsage
  - SubjectKeyIdentifier
  - subjectAltName
- If an intermediate certificate exists, prepare a signed public key certificate (server.crt file) that has a certificate chain that includes the intermediate certificate.
- The number of tiers of the certificate chain for the certificate to be uploaded must be 5 tiers or less including the root CA certificate.
- The public key encryption method for the certificate to be uploaded must be RSA.
- The passphrase for the private key (server.key file) is released.
- SMI-S provider service has been stopped.

Note: If the ResourceGroup parameter is set, theVVolForSnapshot parameter and the PoolIDForSnapshot parameter are not valid.

Procedure

1. On the SVP, start Windows command prompt as an Administrator.
2. Move the current directory to the directory where the tool `MappSmisConfUpload.bat` exists. Execute the following command:

```
cd /d C:\Mapp\wk\Supervisor\MappIniSet
MappSmisConfUpload.bat serial-number-of-storage-system absolute-path-of-SMI-S-provider-configuration-file
```

Note: `C:\MAPP` indicates the installation directory of the storage management software and the SVP software. When the installation directory other than `C:\Mapp` was specified, replace `C:\Mapp` with the specified installation directory.

3. The completion message appears. Press any key to continue.
4. Close the command prompt.

Note: To reflect the update of the certificate, you need to start the SMI-S provider service.

Returning an SMI-S provider configuration file to default

You can return a configuration file uploaded to the SMI-S provider to default.

Before you begin

- You must have the Storage Administrator (View & Modify) role to perform this task.
- SMI-S provider service has been stopped.

Procedure

1. On the SVP, start Windows command prompt as an Administrator.
2. Move the current directory to the directory where the tool `MappSmisConfInit.bat` exists. Execute the following command:

```
cd /d C:\Mapp\wk\Supervisor\MappIniSet
MappSmisConfInit.bat serial-number-of-storage-system
```

> **Note:** `C:\MAPP` indicates the installation directory of the storage management software and the SVP software. When the installation directory other than `C:\Mapp` was specified, replace *C:\Mapp* with the specified installation directory.

3. The completion message appears. Press any key to continue.
4. Close the command prompt.

> **Note:** To reflect the update of the certificate, you need to start the SMI-S provider service.

Sending SMI-S artificial indication

You can send an SMI-S artificial indication to determine whether the communication between the listeners and the SMI-S provider succeeds or fails.

Before you begin

- SMI-S Provider software application must be installed.
- The network environment is configured so that the computer on which the listener application operates is connected to the SVP.
- The listeners are subscribed to the SMI-S provider.
- The user specified for the parameter must have the following roles:
  - Storage Administrator (Initial Configuration)
  - Storage Administrator (System Resource Management)
  - Storage Administrator (Provisioning)
  - Storage Administrator (Performance Management)
  - Storage Administrator (Local Copy)
  - Storage Administrator (Remote Copy)
- The services of the SMI-S provider should be running.

Procedure

1. On the SVP, start Windows command prompt as an Administrator.

2. Move the current directory to the directory where the tool `MappSmisArtificialIndicate.bat` exists. Execute the following command:

```
cd /d C:\Mapp\wk\Supervisor\MappIniSet
MappSmisArtificialIndicate.bat serial-number-of-storage-system username password
```

> **Note:** `C:\MAPP` indicates the installation directory of the storage management software and the SVP software. When the installation directory other than `C:\Mapp` was specified, replace `C:\Mapp` with the specified installation directory.

3. The SMI-S artificial indication result message appears. Press any key to continue.
4. Close the command prompt.

SMI-S provider startup setting

You can enable or disable the SMI-S provider service by performing the SMI-S provider startup setting.

> **Note:** To use the SMI-S function, the SMI-S provider service must be enabled. If the service is set to disable by the startup setting, the SMI-S function cannot be used because the service does not start.

> **Caution:** The port number used for the SMI-S provider is automatically assigned when the SMI-S provider service is enabled. When you re-enable the SMI-S provider service after it was disabled, the port number that was in use before the service was disabled is not assigned, and a new port number is assigned instead. Therefore, when you re-enable the SMI-S provider service, make sure to set the newly assigned port number for the management client.

Procedure

1. Stop the SMI-S provider service on the SVP.
2. On the SVP, open a Windows command prompt as an Administrator.
3. Execute the following command:

```
C:\Mapp\wk\Supervisor\SMI\SetServiceStartupType.bat Serial-number-of-storage-system Startup-type
```

   Specify **`enable`** or **`disable`** for *`Startup-type`*.

   `C:\MAPP` indicates the installation directory of the storage management and SVP software. If a different installation directory was specified, replace `C:\Mapp` with the specified installation directory.

4. When the completion message appears, press any key to continue.
5. Close the command prompt.

> **Note:** The startup setting is reflected the next time the service is started in each storage system.

Configuring audit logs

The audit log files contain records of the operations performed on the storage system, including the user who performed the operation and the date and time, as well as the storage system behaviors resulting from the operations. For storage systems with an SVP, the audit log files are stored in the SVP or in the storage system depending on the type of log. For storage systems without an SVP, the audit log files are stored in the storage system. To access the collected log files, you must configure the storage system to transfer the log files to the syslog server and export an audit log file before you can view an audit log for the storage system.

Setting up a syslog server

Use the following procedure to set up a syslog server for your storage system.

Before you begin

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

Procedure

1. In the maintenance utility, expand the **Administration** tree, and then select **Audit Log Settings**.
2. Click **Set Up Syslog Server**.
3. In the **Set Up Syslog Server for Audit Logs** window:
   a. Select the desired **Transfer Protocol**.
   b. Enable or disable the **Primary Server**.
   c. Enable or disable the **Secondary Server**.
   d. Enter the **Location Identification Name**.
   e. Enable or disable the **Retry**. If enabled, enter the desired retry interval.
   f. Enable or disable the **Output Detailed Information**.
4. When are finished specifying the syslog server settings, click **Apply** to save the settings and close the window.

Exporting audit log files overview

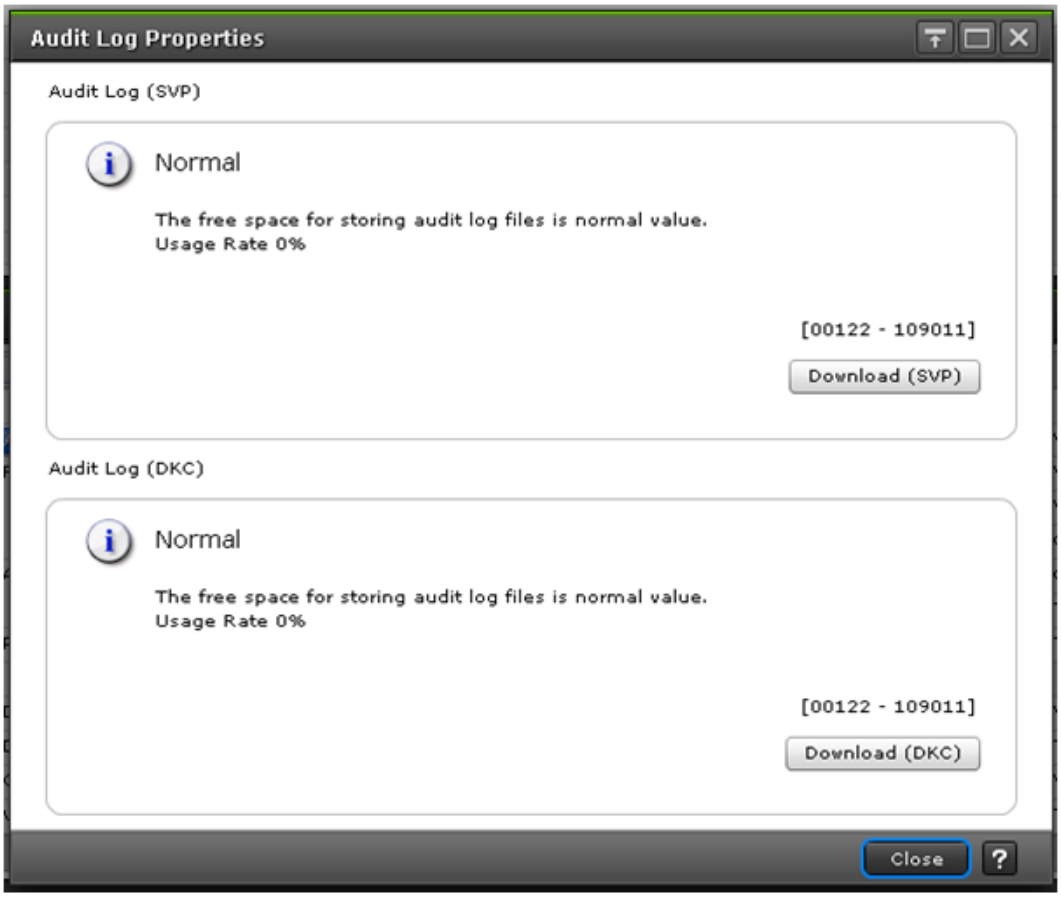
You can export audit log files stored in the SVP using Hitachi Device Manager - Storage Navigator or files stored in the storage system using the maintenance utility.

Exporting audit log files stored in the SVP

Procedure

1. In the main window, click **Audit Log** on the menu bar.
   The icons on the menu bar show the accumulated status of the audit log files.

2. From the **Audit Log Properties** window, click **Download (SVP)** to export logs operated by the Device Manager - Storage Navigator client computer (SVP window). Click **Download (DKC)** to export commands sent from a host or computers using CCI or logs of events on encryption keys.
   The preparation message appears.



Item	Description
Usage Rate	Indicates how much of storage capacity of the non-transfer audit logs is used in comparison to the maximum storage capacity.
Download (SVP)	Audit logs of the following contents or type are exported: ▪ Operation set by the client PC ▪ Operation logs of encryption keys for encrypting stored data ▪ Execution logs of Remote Maintenance API

3. Click **OK**.
   A window opens where you can specify the export destination.
4. Specify the export destination and file name, and then click **Save**.
5. Click **Close**.

Exporting audit log files stored in the storage system

You can export audit logs from either the controller or the GUM located on the controller.

The storage system has two controllers, so to get audit logs for the complete system, you must log-in to the maintenance utility on each controller to export the audit log individually.

Before you begin

You must have the Audit Log Administrator (View Only) role to perform this task.

Procedure

1. In the maintenance utility under Administration menu, select **Audit Log Settings**.
2. Click **Export Audit Log** in the **Audit Log Settings** window to select **GUM** or **DKC**.
3. Click **OK**.

   Note: If the certificate is not valid during an HTTPS connection, the security warning message is displayed. Make sure to take the following actions within 30 seconds. The audit logs cannot be exported after 30 seconds. Go back to step 2.

   - Microsoft Edge: Click **Advanced** and then **Continue to <*IP-address-or-host-name*> (unsafe)**.
   - Google Chrome: Click **Advanced**, and then click **Proceed to <*IP-address*> (unsafe)**.
   - Internet Explorer: Click **Continue to this website (not recommended)**.
4. Save the file to the folder containing audit logs.

   Note: If you change the location identification name of a syslog server, the location identification name on new audit logs could be changed retroactively.

   Note: If you change the UTC time zone setting of the storage system, the times recorded on new audit logs could be changed retroactively.

Send test message to syslog server

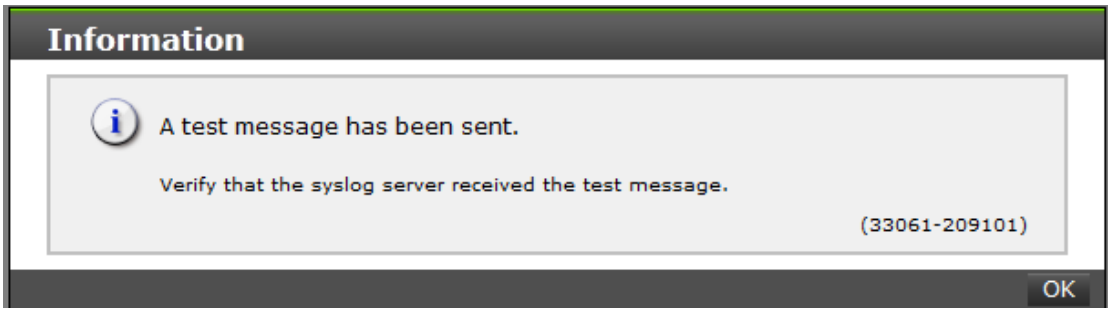
Use the following procedure to send a test audit log message to the syslog server.

Before you begin

You must have the Audit Log Administrator (View Only) role to perform this task.

Procedure

1. In the maintenance usage **Administration** tree, select **Audit Log Settings**.
2. Click **Send Test Message to Syslog Server**. The following message box opens:



3. Click **OK** to close the message box. Check the syslog server messages and verify that the test message was received and is on the server.

Backing up and restoring the HDvM - SN configuration files

The HDvM - SN configuration files for your storage system are stored on the SVP. You can maintain a current backup of these HDvM - SN configuration files, and then if the SVP needs to be replaced, you can restore the backed up HDvM - SN configuration files onto the new SVP.

Configuration items that are included in the backup

The following configuration information can be backed up and restored. Before you create backup files, ensure that these settings are correct.

- HDvM - SN environment parameters
- Authentication server connection settings
- Key management server connection settings
- Password policy for backing up the encryption keys on the management client
- Display settings for each HDvM - SN user (customized table width)
- HDvM - SN login warning messages
- Settings for automatically deleting tasks from the HDvM - SN **Tasks** window
- HDvM - SN task information
- SMI-S application settings
- SSL certification for HTTPS/SMI-S/RMI
- Port numbers used on the SVP
- RSA key exchange settings
- Settings for blocking HTTP communication to the SVP

  This information can be backed up and restored with SVP firmware version 93-01-02-xx/00 or later.
- Settings for enabling and disabling use of Flash Player

  This information can be backed up and restored with SVP firmware version 93-02-01-xx/00 or later.

Configuration items that are not included in the backup

The following table lists the configuration information that is not included in the backup and describes how to back up and restore each item.

Configuration information	Action
Configuration reports for the storage system	Download and then store the HDvM - SN configuration reports. For instructions, see Downloading and viewing the HDvM - SN configuration reports (on page 209).
Settings for blocking HTTP communication to the SVP	Reapply the settings. For instructions, see Blocking HTTP communication to the SVP (on page 65). This information can be backed up and restored with SVP firmware version 93-01-02-xx/00 or later.
Refresh time intervals for the HDvM - SN **Tasks** window	The refresh time interval settings apply only to the user currently logged in. Users must reapply their settings for the refresh time interval.
Audit log files stored in the SVP	Export and then store the audit log files. For instructions, see Exporting audit log files stored in the SVP (on page 120).
Monitoring data stored by Performance Monitor	Store the monitoring data. For details, see the *Performance Guide*.
CCI configuration information	Store the CCI configuration definition files. For details, see the *Command Control Interface Installation and Configuration Guide*.
Settings for enabling or disabling use of Flash Player	Reapply the settings. For instructions, see Disabling use of Flash Player with HDvM - SN (on page 43). This information can be backed up and restored with SVP firmware version 93-02-01-xx/00 or later.

Backing up HDvM - SN configuration files

You can make backup copies of the various Device Manager - Storage Navigator (HDvM - SN) configuration files by downloading them to a folder that you specify. You can then use the backup configuration files to restore one or more of the files to the existing SVP if necessary or to configure a new SVP.

Before you begin

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

Procedure

1. Stop all storage services running on the SVP.
2. Open a command prompt window with administrator permissions.
3. Move the current directory to the folder containing the SVP configuration tool (for example, `C:\MAPP\wk\Supervisor\MappIniSet`), and then execute the following command:

   `MappBackup.bat` *`absolute-path-of-backup-file`*

   Make sure to include the first 8 digits of the SVP firmware version (for example, 93050100) when you specify the file name. If you need to restore a configuration file, you must use a backup file that was created with the same SVP firmware version as the target SVP.

   Note:

   - The backup file must be in `.tgz` format. Use a tool that supports `tar` and `gzip` to extract the data from the `.tgz` file.
   - A space is required between the `.bat` file and the path to the backup file.

     If you do not specify a folder in which to save the file, the system automatically creates a default file in the following location:

     `SVP-root``\wk\Supervisor\MappIniset\Logs`*`yyyyMMddHHmmss`*`.tgz`

     where *yyyyMMddHHmmss* is the year, month, date, and time that the file was created.
4. When the backup confirmation message is displayed, enter **y** to continue.
5. When the completion message is displayed, click any key to continue.
6. Close the command prompt window.
7. Save the backup file to another computer or to an external memory device such as a USB flash drive.

Restoring HDvM - SN configuration files

You can use a backup copy of a Device Manager - Storage Navigator configuration file to restore the active configuration file if it becomes necessary, for example, to configure a replacement SVP.

Caution: When you restore a configuration file, make sure the backup file has the same SVP firmware version as the target SVP. If you use a backup file with a different version as shown in the following table, special care might be required.

SVP firmware version of the backup file	SVP firmware version on the target SVP
93-02-03-xx/00 or later	93-02-02-xx/00 or earlier

If the services on the storage system do not work correctly after the restore operation with the combination of firmware versions listed in the table, you must perform either of the following operations after the restore operation is complete:

- When a signed certificate is set: Update the signed certificate for the SSL communication between the SVP and the management client.
- When a signed certificate is not set: Return the certificate for the SSL communication between the SVP and the management client to default.

Before you begin

- The storage systems registered in the SVP you backed up must be registered in the new SVP.
- The SVP must be configured so that the service does not start automatically when starting the system.

Procedure

1. Stop all storage services running on the SVP.
2. Copy the backup file to any folder in the SVP.
3. Open a command prompt window with administrator permissions.
4. Move the current directory to the folder containing the SVP configuration tool (for example, `C:\MAPP\wk\Supervisor\MappIniSet`), and then execute the following command:

   `MappRestore.bat` *`absolute-path-of-backup-file`*

   Note:
   - The backup file must be in `.tgz` format.
   - A space is required between `MappRestore.bat` and the path to the backup file.
5. When the completion message is displayed, click any key to continue.
6. Close the command prompt.
7. Reassign a port number for each storage system registered in the Storage Device List.
8. Reboot the SVP.

   It usually takes about 10 minutes to complete the startup process.

Preventing errors while using virus detection programs on the SVP

Running virus detecting programs on an SVP* that has Device Manager - Storage Navigator installed might cause operation errors while using Device Manager - Storage Navigator.

To prevent errors caused by virus detection programs, exclude the Device Manager - Storage Navigator installation directory from the real-time virus scan target in your virus detection program.

Note: `C:\MAPP` indicates the installation directory of the storage management software and the SVP software. When the installation directory other than `C:\Mapp` was specified, replace `C:\Mapp` with the specified installation directory.

Perform virus scans regularly on the excluded directory during periods when Device Manager - Storage Navigator is not in use or when the service stops.

Note: *Including standard virus detection programs installed on the operating system such as Windows Defender.

Forcing the system lock to release

When performing configuration and maintenance operations, the storage system might automatically lock itself and release the system when the operations are completed. If the storage system does not unlock itself, you can unlock the system using Force Release System Lock in the maintenance utility.

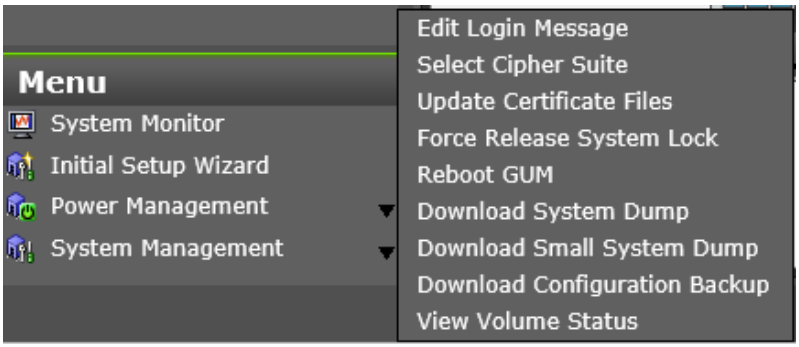
Caution: Before using this feature, ensure that releasing the system lock will not cause system problems due to processes that are currently running. Releasing the system lock can terminate a process before it completes and possibly leave the system in an unknown state. Check with any users that are logged on. Wait until their processes are complete before releasing the system lock.

Before you begin

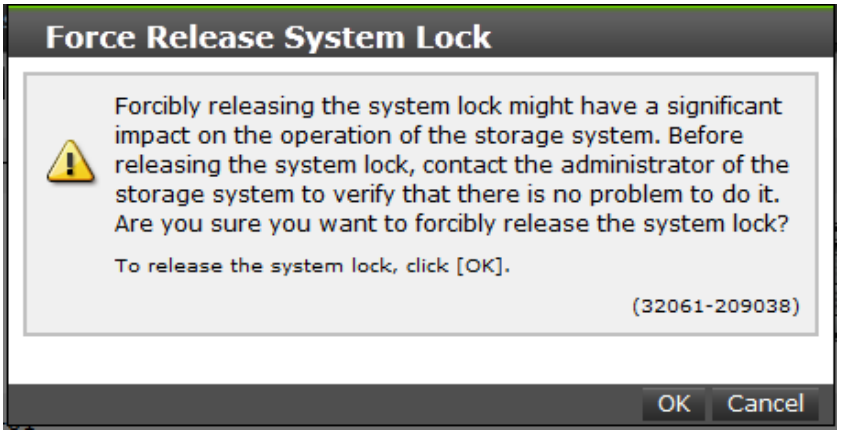
You must have the Storage Administrator (View & Modify) role to complete this procedure.

Procedure

1. In the maintenance utility **Menu** navigation tree, click **System Management**.



2. Click **Force Release System Lock**.
3. A warning message is displayed. Verify that releasing the lock will not cause data loss or other problems. To release the system lock, click **OK**. Click **Cancel** to close the dialog box without releasing the system lock.



Chapter 6: Managing users and user groups

You can create and modify users by assigning them roles, permissions, and groups using Storage Navigator or the maintenance utility.

User administration overview

Device Manager - Storage Navigator provides a rich set of user administration, roles and permissions, and access control features. Administrators can manage users by groups and set up access control by defining who can access what storage resources. For storage systems that do not have an SVP, the maintenance utility provides basic user management capabilities, such as creating, modifying, and deleting user accounts.

You can create and manage users locally or configure the storage system to authenticate users with an existing authentication server, such as LDAP. If you create user accounts in Device Manager - Storage Navigator, you can use the authentication server to allocate user groups to users by configuring the same user group names on the storage system and the authentication server. If you create user accounts in the maintenance utility, users can be authenticated by the authentication server, but user groups are allocated to users based on the configuration in the maintenance utility.

Effective user administration involves the following activities:

1. Understanding roles and permissions: See Roles and permissions (on page 130).
2. Creating user groups: See Creating a new user group (on page 135).
3. Creating users and assigning them to user groups: See Creating user accounts (on page 138).
4. Creating resource groups and assigning them to user groups: See Managing resource groups (on page 155).

User groups

Device Manager - Storage Navigator provides several built-in user groups with predefined permissions based on the available roles. You can use these groups to begin managing user permissions and access control immediately. Or you can create your own user groups tailored to meet your unique requirements.

Consider the following when setting up user groups:

- When a user is assigned to multiple user groups, 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.
- You can create two user accounts that are used by the same user playing two roles. For example, you can create user_1 and user_2 that are used by the same person, but user 1 is a security administrator that has access to all resource groups and user_2 is a storage administrator that has access to only one of the resource groups.
- All user groups, except for the Storage Administrator groups, have access to all resources in the storage systems (All Resource Groups Assigned is automatically set to Yes).
- If you deleted all the roles except the Storage Administrator, you will need to add all required resource groups to the user group because the Storage Administrator role does not have access to all resources by default. See Changing assigned resource groups (on page 137).
- All user groups must have resource groups assigned in order to perform operations on the storage system.

Roles and permissions

The following table lists all of the available user roles and shows the permissions that each role provides to the users. Custom user roles are not supported.

Important: The Support Personnel group and the Support Personnel (Vendor Only) role contain permissions to perform maintenance on the storage system. Assign this role only to the accounts used by support personnel from vendors responsible for maintenance.

The roles for Hitachi Storage Advisor Embedded users are:

- Storage Administrator (Initial Configuration)
- Storage Administrator (System Resource Management)

  This role is not required when the DKCMAIN firmware version is 93-06-3x or earlier.
- Storage Administrator (Provisioning)
- Storage Administrator (Local Backup Management)
- Storage Administrator (Remote Backup Management)
- Security Administrator (View and Modify)
- Maintenance (User)

Role	Permissions
Security Administrator (View Only)	▪ Viewing information about user accounts and encryption settings ▪ Viewing information about the encryption key in the key SVP

Role	Permissions
	▪ Viewing information about the external authentication by the maintenance utility ▪ Viewing information about the cloud connection settings
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 SVP ▪ Viewing and changing the password policy for backing up encryption keys on the management client ▪ Connection to the external server ▪ Backing up and restoring connection configuration to the external server ▪ Configuring the certificate used for the SSL communication ▪ Configuring the fibre channel authentication (FC-SP) ▪ Configuring resource groups ▪ Editing virtual management settings ▪ Setting reserved attributes for global-active device ▪ Configuring external authentication by the maintenance utility ▪ Setting up and clearing the cloud connection settings
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 (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 updating Device Manager - Storage Navigator window by clicking Refresh All

Role	Permissions
Storage Administrator (System Resource Management)	▪ Configuring settings for CLPR ▪ Configuring settings for MP unit ▪ Deleting tasks and releasing exclusive locks of resources ▪ Configuring LUN security ▪ Configuring Server Priority Manager ▪ Configuring tiering policies
Storage Administrator (Provisioning)	▪ Configuring caches ▪ Creating parity groups ▪ Configuring volumes, pools, and virtual volumes ▪ Formatting and shredding volumes ▪ Configuring external volumes ▪ Configuring Dynamic Provisioning ▪ Configuring host groups, paths, and WWN ▪ Configuring Volume Migration except splitting Volume Migration pairs when using CCI ▪ Configuring access attributes for volumes ▪ Configuring LUN security ▪ Creating and deleting quorum disk used with global-active device ▪ Creating and deleting global-active device pairs ▪ Editing virtual management settings ▪ Setting reserved attributes for global-active device.
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 CCI
Storage Administrator (Remote Copy)	▪ Remote copy operations in general ▪ Performing operations on existing global-active device pairs (pair creation and pair deletion are not allowed)
Support Personnel (Vendor Only)	Normally, this role is for service representatives. ▪ Configuring the SVP

Role	Permissions
Support Personnel (User)	▪ Viewing storage system status ▪ Installing OS security patches ▪ Updating operating systems ▪ Performing basic maintenance

Built-in user groups

You can assign users to one or more built-in user groups and custom user groups. You cannot change roles or resource groups set to the built-in groups, but you can create custom user groups according to the needs of your storage environment.

The following table shows all the built-in groups, and their built-in roles and resource 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)	All Resource Groups Assigned

Built-in group	Role	Resource group
	▪ Storage Administrator (Performance Management) ▪ Storage Administrator (Local Copy) ▪ Storage Administrator (Remote Copy)	
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
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)	All Resource Groups Assigned

Built-in group	Role	Resource group
	▪ Storage Administrator (Provisioning) ▪ Storage Administrator (Performance Management) ▪ Storage Administrator (Local Copy) ▪ Storage Administrator (Remote Copy) ▪ Support Personnel	

Creating a new user group

You can customize a user group, as long as it supports your storage system.

This section explains how administrators can create a user group.

A user group name consists of 1 to 64 characters including alphanumeric characters, spaces, and the following symbols:

! # $ % & ' ( ) + - . = @ [ ] ^ _ ` { } ~

The system can support a maximum of 32 user groups, including the nine built-in user groups.

Before you begin

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

Procedure

1. In the **Administration** tree, select **User Groups**.
2. In the **User Groups** tab, click **Create User Groups** 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**. 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** to finish and confirm settings.

   Click **Next** to add another user.
10. Check the settings and enter a task name in **Task Name**.
11. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Tasks** window opens to show the status of the task.

Changing a user group name

You can change the name of a user group by using Hitachi Device Manager - Storage Navigator.

Before you begin

- You must have the 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 **Administration** tree, select **User Groups**.
2. In the **User Groups** tab, select the user group.
3. Click **More Actions** > **Edit User Group**.
4. In the **Edit User Group** window, enter a new user group name.
5. If you use an authorization server, click **Check** and verify that the entered user group name is registered in the authorization server.
6. Click **Finish**.
7. In the **Confirm** window, check the settings and enter a task name in **Task Name**.
8. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Tasks** window opens to display the status of the task.

Changing user group permissions

You can change the permissions that are assigned to user groups by using Hitachi Device Manager - Storage Navigator.

Before you begin

- You must have the Security Administrator (View & Modify) role to perform this task.
- The permissions of a built-in group cannot be changed.

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, select **User Groups**.
2. In the **User Groups** tab, select the user group whose permission you want to change.
3. Click the **Roles** tab.
4. Click **Edit Role Assignment**.
5. In the **Edit Role Assignment** window, change roles to be assigned to the user group.
   - Select roles to add, and then click **Add**.
   - Select a role to remove, and then click **Remove**.
6. Click **Finish**.
7. In the **Confirm** window, check the settings and enter a task name in **Task Name**.

8. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Tasks** window opens.

Changing assigned resource groups

You can change the resource groups that are assigned to user groups by using Hitachi Device Manager - Storage Navigator.

Before you begin

- You must have the 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 a user group that has All Resource Groups Assigned set to Yes
- You cannot change resource groups of a built-in group.

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, select **User Groups**.
2. On the **User Groups** tab, select a user group to change the resource group.
3. Select the **Resource Groups** tab.
4. Click **Edit Resource Group Assignment** to open the **Edit Resource Group Assignment** window.
5. In the **Edit Resource Group Assignment** window, change resource groups to be assigned to the user group.
   - Select the resource group to add, and click **Add**.
   - Select the resource group to remove, and click **Remove**.
6. Click **Finish**.
7. In the **Confirm** window, check the settings and enter a task name in **Task Name**.
8. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Tasks** window opens to display the status of the task.

Deleting a user group

You do not have to retain a user group for the life of the project. You can delete it at any time by using Hitachi Device Manager - Storage Navigator.

Before you begin

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

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, select **User Groups**.

2. In the **User Groups** tab, select the user-created user groups that you want to delete.
3. Click **More Actions** > **Delete User Groups**.
4. Check the settings, then click **Apply**.

User accounts

When adding a new user, you need to add it to a user group with desired permissions. You can use one of the built-in user group or a custom user group.

For more information about roles, permissions, and user groups, see Roles and permissions (on page 130).

You will need to use the local administrator account created during the initial setup step, or create administrator accounts using the procedures described in this chapter as needed to access the storage system temporarily when the management software is not available.

Important:

- Create more than one user account in case the system administrator is not available when the management software becomes unavailable, or when someone else needs to access the system. This is also helpful if multiple users need to access Device Manager - Storage Navigator to use storage features that are not available in the management software.
- Create user accounts that do not have the "Support Personnel (Vendor Only)" role to prevent unauthorized access to the functions available to service representatives. Users that have the "Support Personnel (Vendor Only)" role can perform the same operations as service representatives.

Creating user accounts

When you create a user account, you register the user to the applicable user groups with appropriate permissions. The storage system supports a maximum of 20 user accounts, including the built-in user accounts. To prevent unauthorized access to the storage system, users must change their password immediately after logging in for the first time.

Important: After the user accounts have been created, back up the user account information. If a controller failure or other problem occurs, recover from the failure and then restore the backup file. You will be able to use the user account information again after the backup file is restored.

The following tables specify the character requirements for logging in to Device Manager - Storage Navigator and CCI.

Table 6 User name and password for Device Manager - Storage Navigator

Item	Length in characters	Characters that can be used
User name	1-256	▪ Alphanumeric characters ▪ The following symbols: # $ % & ' * + - . / = ? @ ^ _ ` { | } ~
Password	6-256	▪ Alphanumeric characters ▪ All symbols

Table 7 User name and password for logging in to CCI

Item	Length in characters	Characters that can be used
User name	1-63	▪ Alphanumeric characters ▪ The following symbols: - . @ _ When CCI is installed on a UNIX computer, forward slashes (/) can also be used.
Password	6-63	▪ Alphanumeric characters ▪ The following symbols: , - . @ _: When CCI is installed on a Windows computer, back slashes (\) can also be specified. When CCI is installed on a UNIX computer, forward slashes (/) can also be used.

Before you begin

- You must have the Security Administrator (View & Modify) role to perform this task.
- You or an authorized technical support representative can log in to Device Manager - Storage Navigator and CCI with user accounts that are created in Device Manager - Storage Navigator.

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, select **User Groups**.

2. On the **User Groups** tab, select a user group to which to add a user. This is dependent on which permissions you want to give to the user.

   Support representatives must have the Support Personnel (Vendor Only) role to log in.
3. On the **Roles** tab, confirm that the displayed permissions are appropriate for the user.

   The roles for Hitachi Storage Advisor Embedded users are:

   - Storage Administrator (Initial Configuration)
   - Storage Administrator (Provisioning)
   - Storage Administrator (Local Backup Management)
   - Security Administrator (View and Modify)
   - (VSP E series) Maintenance (User)
4. On the **Users** tab, click **Create**.
5. Enter the user 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 Device Manager - Storage Navigator.
7. To use an authentication server, select **External**. To authenticate users with only Device Manager - Storage Navigator, select **Local**.
8. If you select **Local**, enter the password for this user account in two places.

   You can use all alphanumeric characters and symbols for the password. The password must be between 6 and 256 characters.
9. Click **Finish**.
10. In the **Confirm** window, check the settings.
11. Click **Apply**. The task is now registered. If **Go to tasks window for status** is checked, the **Tasks** window opens to display the status of the task.

Changing your initial HDvM - SN password

When the system administrator adds users to HDvM - SN, each user is assigned a user ID and an initial password. When you log in to HDvM - SN for the first time using your initial password, you must change your password to prevent unauthorized access to the storage system.

Procedure

1. Log in to Device Manager - Storage Navigator with the user ID and password given to you by the administrator.
2. Click **Settings** > **User Management** > **Change Password**.
3. Enter your initial password and your new password on the **Change Password** window, and then click **Finish**.
4. In the confirmation window:
   a. Enter a task name or accept the default task name.
   b. If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status**.
   c. Click **Apply**.

Changing user passwords

You can change or reissue passwords for other users by using Device Manager - Storage Navigator.

Caution: When using management software (for example, Ops Center, Hitachi Command Suite), you need to change information, such as passwords, registered in the software. For details, see the documentation for the software product.

Caution: Before changing the password of a user account specified by the registered storage system in the **Storage Device List** window, click Stop Service for the registered storage system. After changing the password of the user account, click Edit and set the new password, then click Start Service for the storage system.

Before you begin

- Security administrators with View & Modify roles can change user passwords on Device Manager - Storage Navigator.
- If the target user has a local user account for Device Manager - Storage Navigator, the security administrator can use Device Manager - 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 Device Manager - Storage Navigator.

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, select **User Groups**.
2. On the **User Groups** tab, select the user group to which the user belongs.
3. On the **User** tab, select the user whose password you want to change.
4. In the **User** tab, click **Change Password**.
5. In the **Change Password** dialog box, specify a new password for the user in the two password fields.
6. Click **Finish**.
7. In the **Confirm** window, check the settings and enter a task name in **Task Name**.
8. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Tasks** window opens to show the status of the task.

Changing user permissions

You can change user 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.

Before you begin

- You must have the 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 account can belong to up to 8 user groups.
- A user group can contain a maximum of 20 user accounts, including the built-in user accounts.

Adding a user

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, select **User Groups**.
2. On the **User Groups** tab, select the user group that has the role you want the user to have, and then add or remove users.

   To add users to the selected groups:

   a. Click **Add Users**.

   b. In the **Add Users** window, select a user and click **Add**.

   To remove users from the selected groups:

   a. In the **Remove Users** window, select one or more users.

   b. Click **More Actions > Remove Users**.
3. Click **Finish**.
4. In the **Confirm** window, check the settings. If the **Task Name** field is empty, enter a task name.
5. Click **Apply**. The task is now registered. If you selected the **Go to tasks window for status** check box, the **Tasks** window opens to show the status of the task.

Enabling and disabling user accounts

To allow or prevent a user from logging in to Device Manager - Storage Navigator, follow the steps below.

Caution: Do not select any user account used to connect to a storage system that is registered in the Storage Device List window. For details, see the Hardware Reference Guide for your storage system.

Before you begin

- Log into an account that is different from the user whose account that you want to disable.
- You must have the Security Administrator (View & Modify) role to perform this task.

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, click **User Groups**.
2. On the **User Group** tab, select the user group.
3. On the **Users** tab, select a user.
4. Click **Edit User**.

5. Click the **Account Status** check box.
6. Click **Finish**.
7. In the **Confirm** window, check the settings.
8. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Tasks** window opens to show the status of the task.

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.

Caution: Do not select any user account used to connect to a storage system that is registered in the **Storage Device List** window. For details, see the Hardware Reference Guide for your storage system.

Before you begin

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

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, select **User Groups**.
2. On the **User Groups** tab, click a user group to which a user belongs.
3. On the **Users** tab, select the user whose account you want to delete.
4. Click **More Actions** > **Delete Users**.
5. In the **Delete Users** window, select the user to be deleted, then click **Finish.**
6. In the Confirm window, check the settings.
7. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Tasks** window opens to show the status of the task.

Unlocking a user account

A user account is automatically locked after three unsuccessful login attempts to Device Manager - Storage Navigator or Command Control Interface. The account is locked for 60 seconds. If necessary, you can release the locked status before the lock times out.

Before you begin

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

Procedure

1. In the **Administration** tree, select **User Groups**.
2. On the **User Groups** tab, click a user group to which the locked-out user belongs.
3. On the **User** tab, select the user you want to unlock.
4. On the **User** tab, click **More Actions** > **Release Lockout**.
   The **Release Lockout** window opens.
5. Specify a task name, and then click **Apply**.

Managing users using the maintenance utility

You can create, modify, and delete users in the storage systems without an SVP or Device Manager-Storage Navigator using the maintenance utility.

You can perform the following user administration tasks using the maintenance utility:

- Create, modify, and delete user accounts
- Back up and restore the user account information

Required roles

Administrators can control what maintenance utility operation windows are available for a user by registering the user with the appropriate roles.

The following table lists the required roles for using specific maintenance utility operation windows.

Maintenance utility operation window	Required role name
Initial Setting Wizard	Storage Administrator (Initial Configuration)
Set Up System Information	Storage Administrator (Initial Configuration)
Firmware	Support Personnel or User Maintenance*
User Administration	Security Administrator (View & Modify)
External authentication setting	Security Administrator (View & Modify)
System Monitor	93-03-2*x* or later: Not needed 93-03-1*x* or earlier: Support Personnel or User Maintenance*
Alert Notifications	Storage Administrator (Initial Configuration)
Set Up Date & Time	Storage Administrator (Initial Configuration)
Set Up Network Settings	Storage Administrator (Initial Configuration)
Cloud Connection Settings	Security Administrator (View & Modify)
Licenses	Storage Administrator (Initial Configuration)
Audit Log Settings	Audit Log Administrator (View & Modify)
Turn on/off Locate LEDs	Support Personnel or User Maintenance*
Power on Storage System	Support Personnel or User Maintenance*
Power off Storage System	Support Personnel or User Maintenance*
Edit UPS Mode	Support Personnel or User Maintenance*

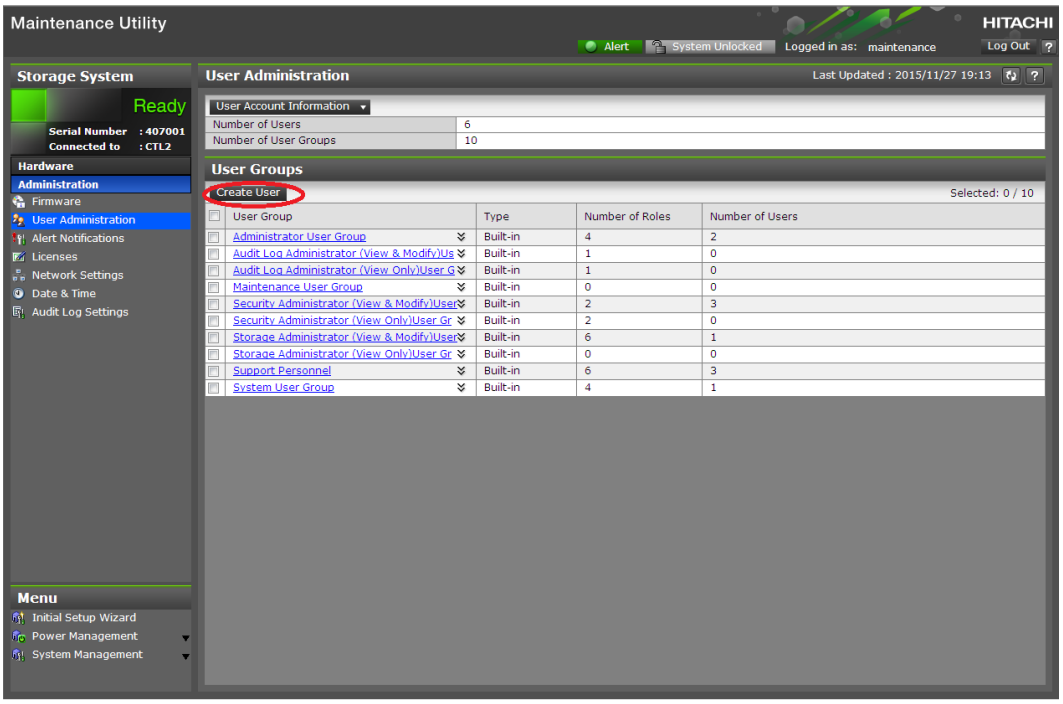
Maintenance utility operation window	Required role name
Edit Login Message	Storage Administrator (Initial Configuration)
Select Cipher Suite	Security Administrator (View & Modify)
Update Certificate Files	Security Administrator (View & Modify)
Force Release System Lock	Storage Administrator (Initial Configuration)
Reboot GUM	Support Personnel or User Maintenance
View Volume Status	Support Personnel or User Maintenance*
Change Password	No role is required.
Boot System Safe Mode	Support Personnel*
Alert Display	Support Personnel or User Maintenance*
Alert Display Related to FRU	Support Personnel or User Maintenance*
Administration Menu	N/A
Power Management	N/A
System Management	N/A
Resetting GUM	N/A
* *Support Personnel* means operations performed by service personnel. *User Maintenance* means operations performed by the user.	

Setting up user accounts

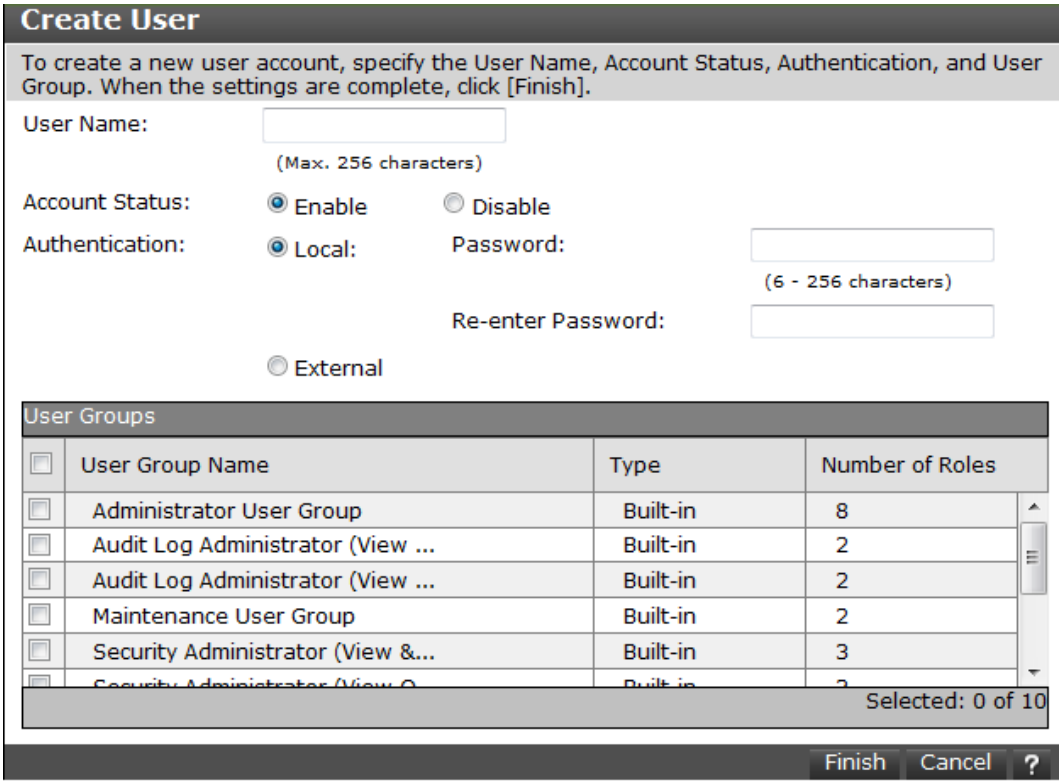
You can create up to 20 users, including the built-in user.

Procedure

1. In the Maintenance Utility window, click **Administration** > **User Administration**.
2. In the **User Groups** tab, click **Create User**.



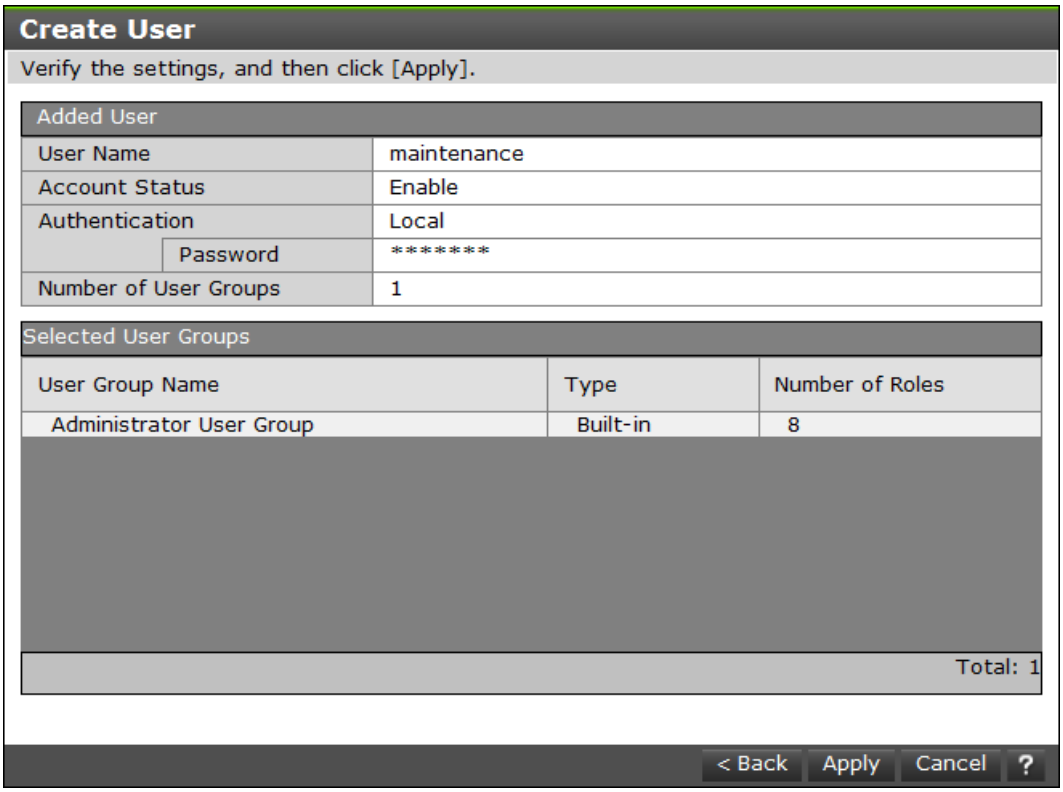
3. Create a new user account. Specify the **User Name**, **Account Status**, **Authentication**, and **User Group**. Click **Finish**.



Item	Description

User Name	Create a user name. You can enter up to 256 one-byte alphanumeric characters and some symbols (! # $ % & ' * + - . / = ? @ ^ _ ` { | } ~).
Account Status	The following statuses are available: Enable: User can use the account. Disable: User cannot use the account or log in to the storage management software.
Authentication	The following methods are available: Local: Does not use authentication server. Uses a dedicated password for storage management software. External: Uses an authentication server.

4. Confirm the settings, and then click **Apply**.



5. When the completion message appears, click **Close**.

Disabling user accounts

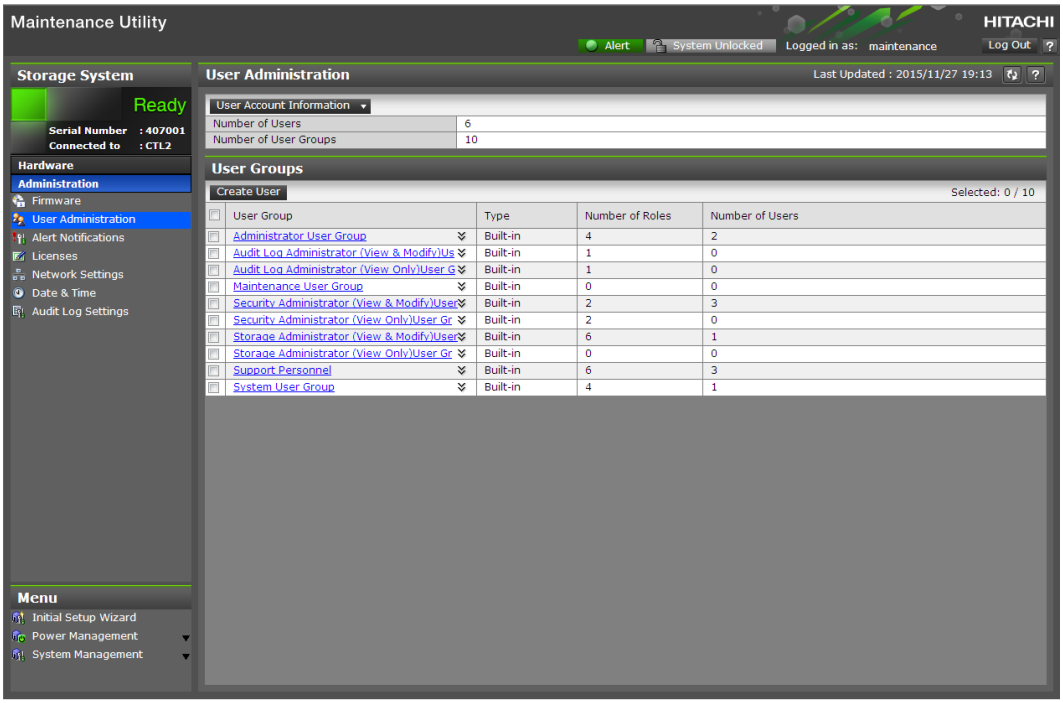
You can disable user accounts by changing the **Account Status** to Disable.

Observe the following guidelines:

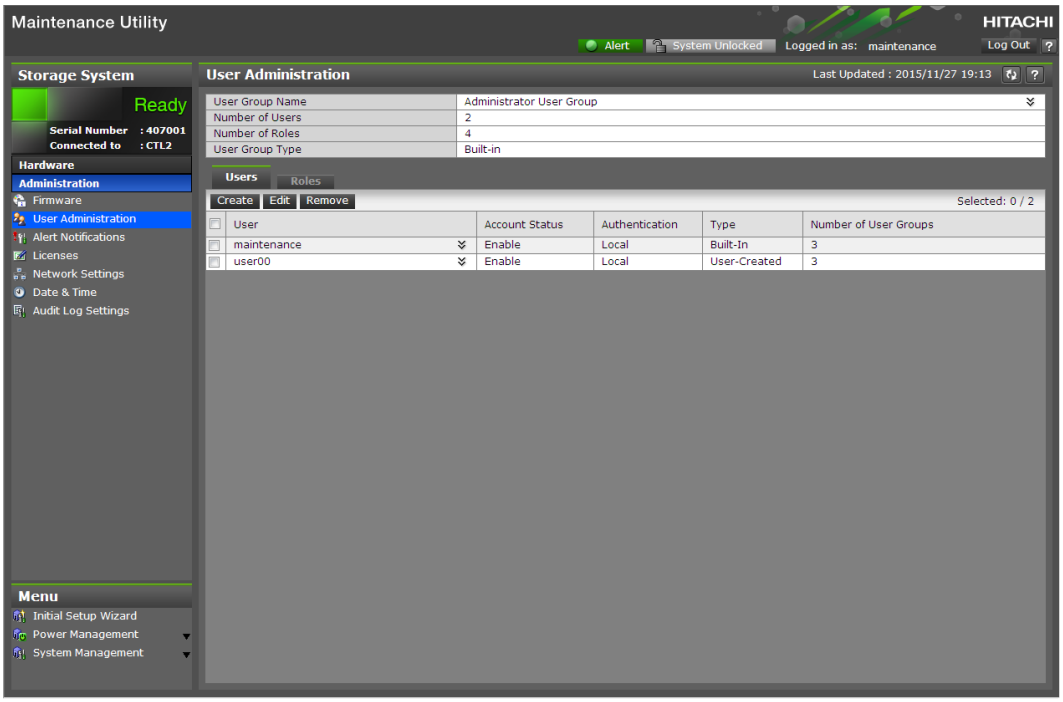
- Log into an account that is different from the user account that you want to disable (you cannot disable the current login user account).
- To disable the user account specified by the registered storage system in the **Storage Device List** window, click Stop Service for the registered storage system. After disabling the user account, click Edit to enable the user account.

Procedure

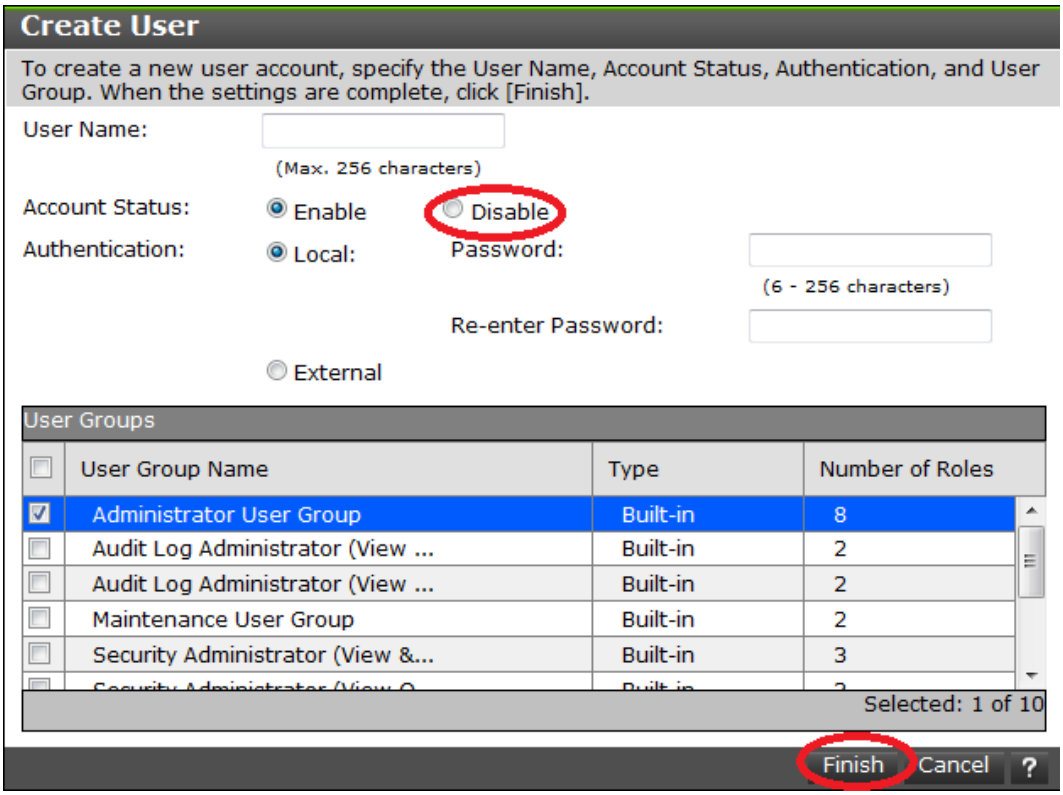
1. In the Maintenance Utility window, click **Administration** > **User Administration**.
2. In the **User Groups** tab, click the user group belonging to the user.



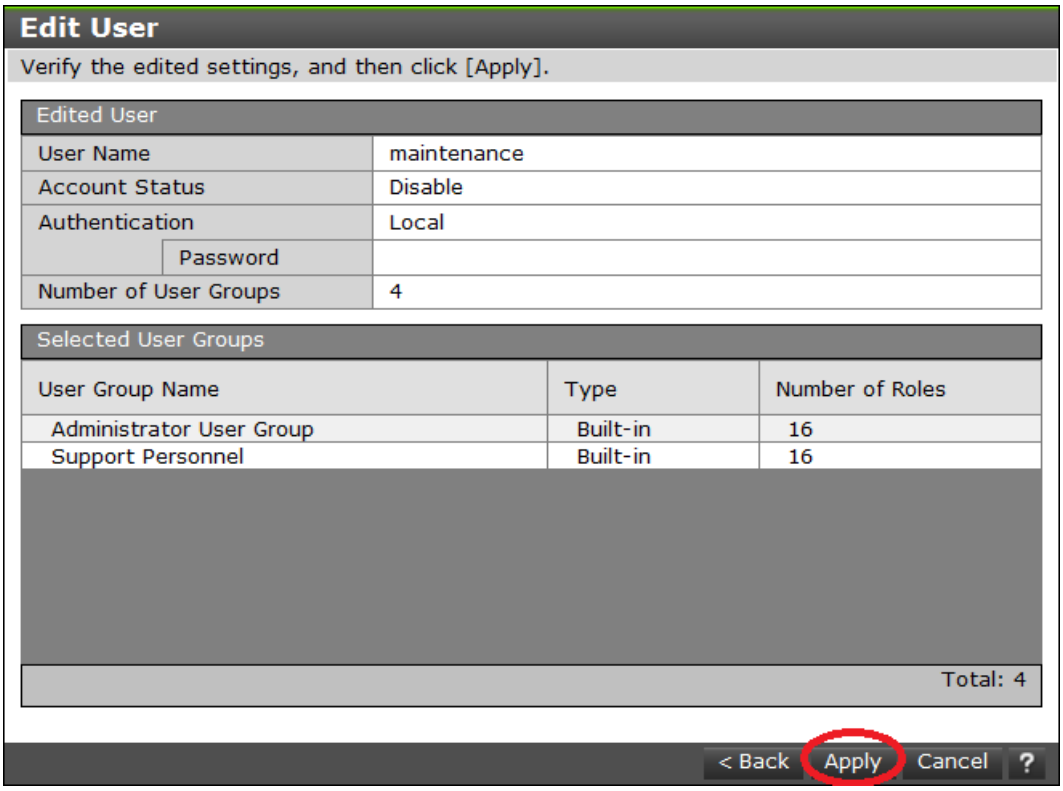
3. Click the **Users** tab, and then select the user account to disable.



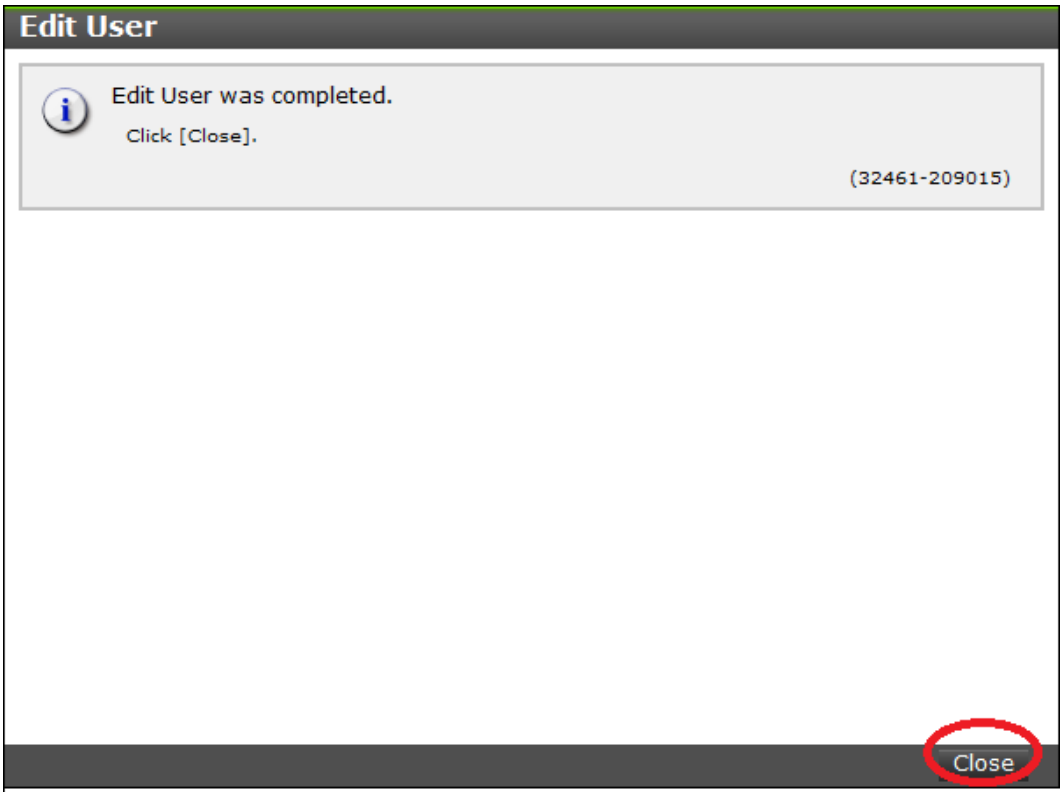
4. Click **Edit**.
5. For **Account Status**, click **Disable**, and then click **Finish**.



6. Confirm the settings, and then click **Apply**.



7. When a completion message appears, click **Close**.



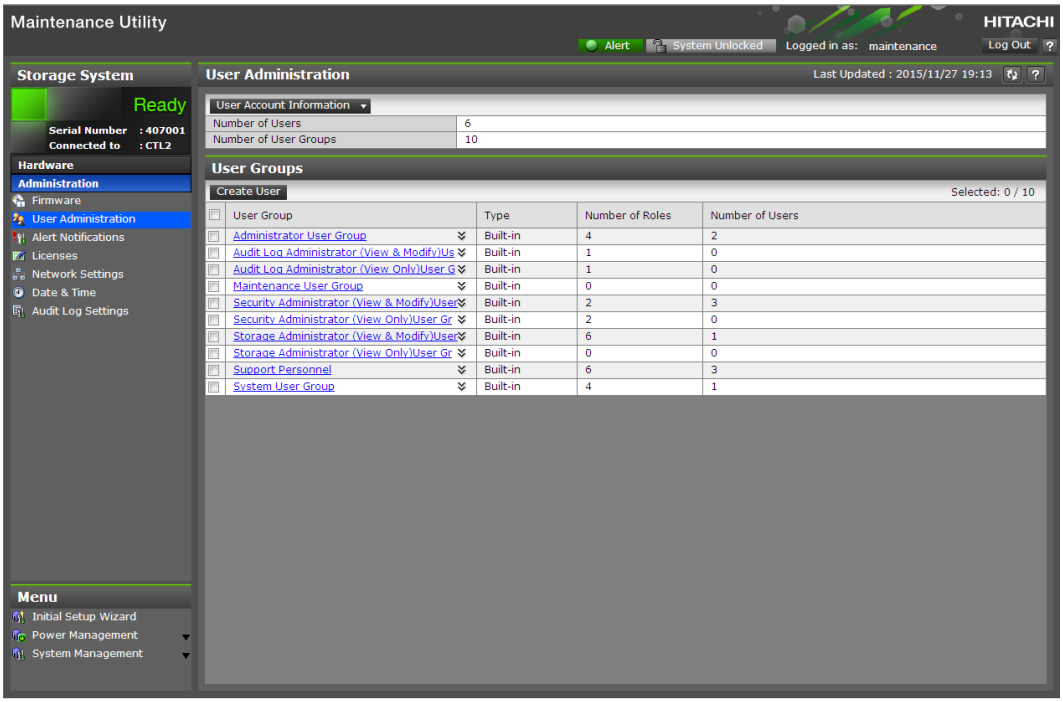
Deleting user accounts

Security administrators can remove a user account when the account is no longer in use. Built-in user accounts cannot be deleted. If deleting the current login user account, you can continue the storage management software operation until you log out.

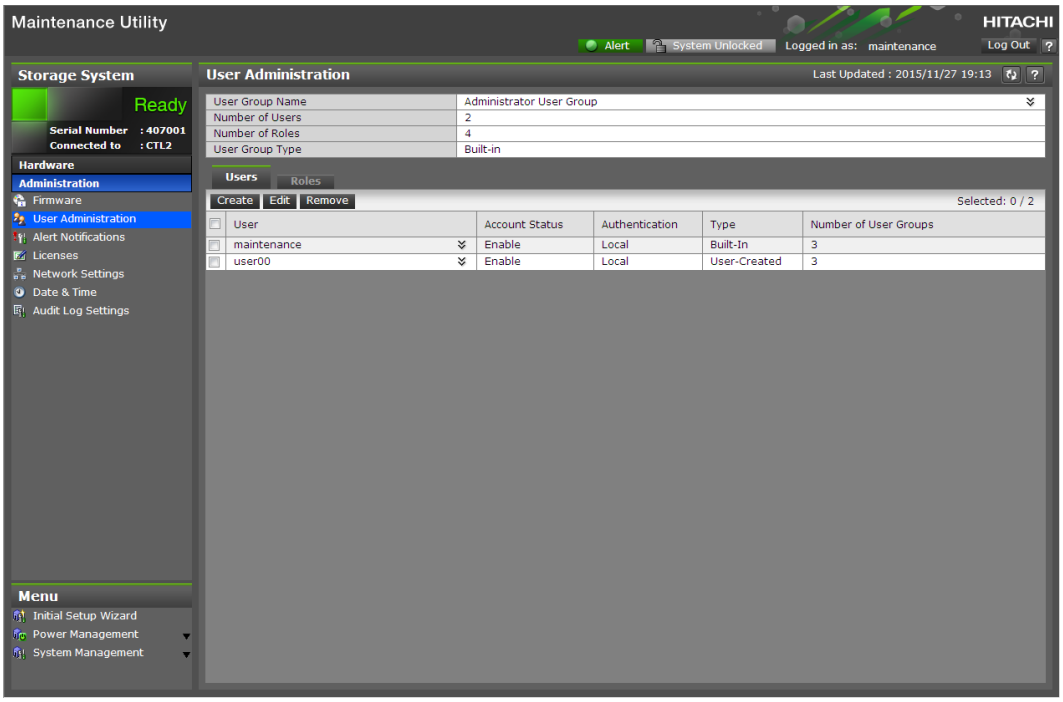
Note: To delete the user account specified by the registered storage system in the **Storage Device List** window, click **Stop Service** of the registered storage system. After deletion, click Edit to enable the user account.

Procedure

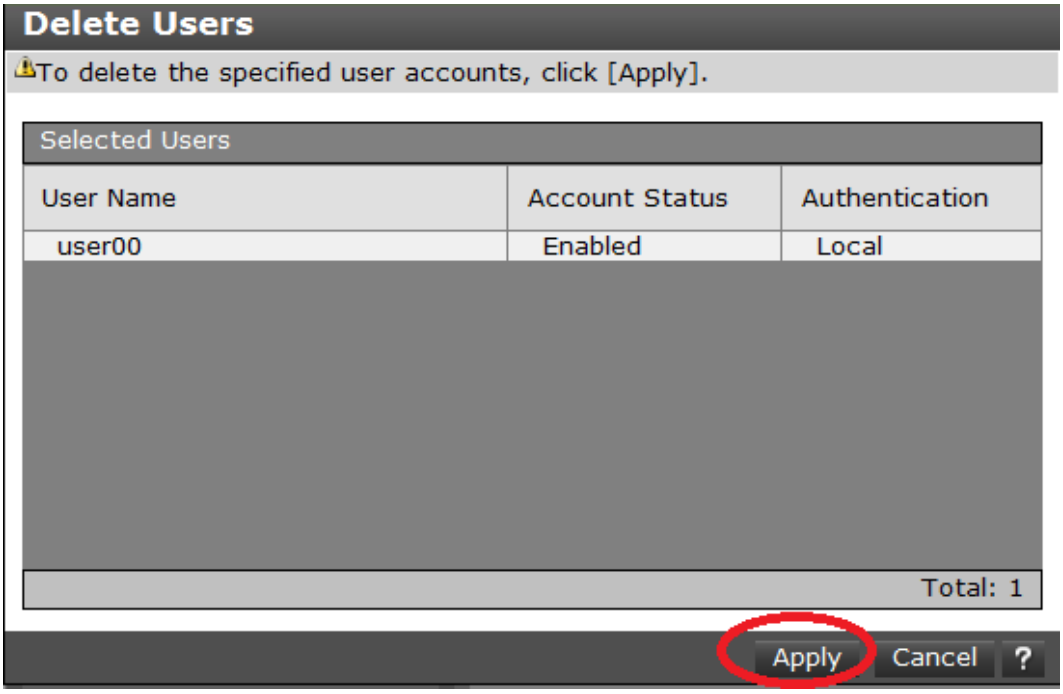
1. In the **Maintenance Utility** window, click **Administration** > **User Administration**.
2. In the **User Groups** tab, select the user group belonging to the user.



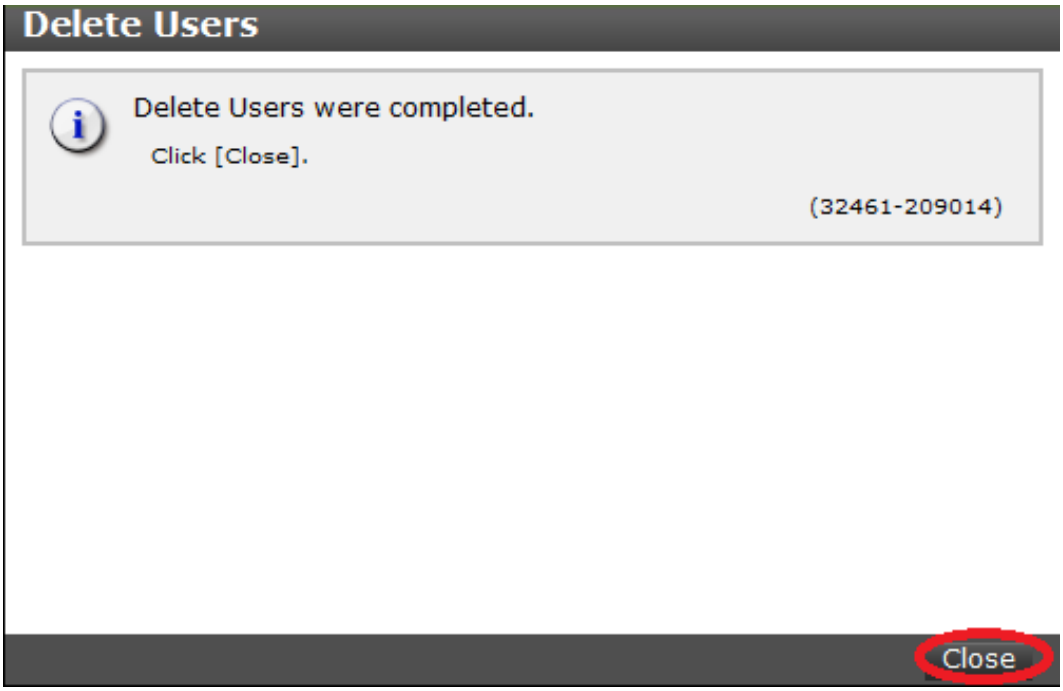
3. Click the **Users** tab, and then select the user to remove.



4. Click **Remove**.
   The **Confirm** window opens.
5. In the **Confirm** window, confirm the settings, and then click **Apply**.



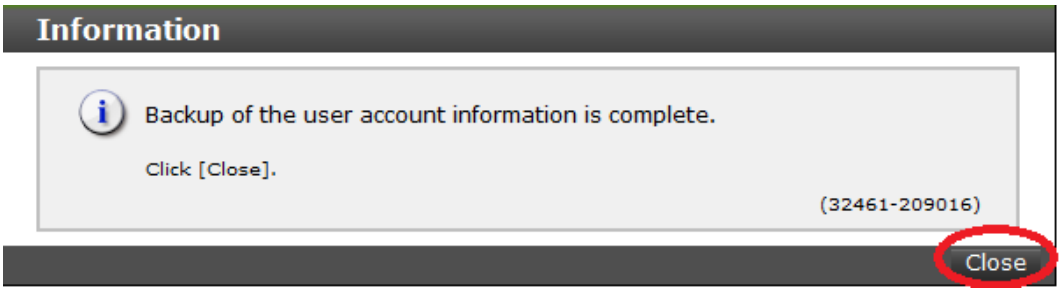
6. At the completion message, click **Close**.



Backing up user accounts

Procedure

1. In the **Maintenance Utility** window, click **Administration** > **User Administration**.
2. In the **User Administration** window, click **User Account Information** > **Backup**.
3. Specify a storage destination and a file name in the displayed window and download the file.
4. When the following message appears, click **Close**.

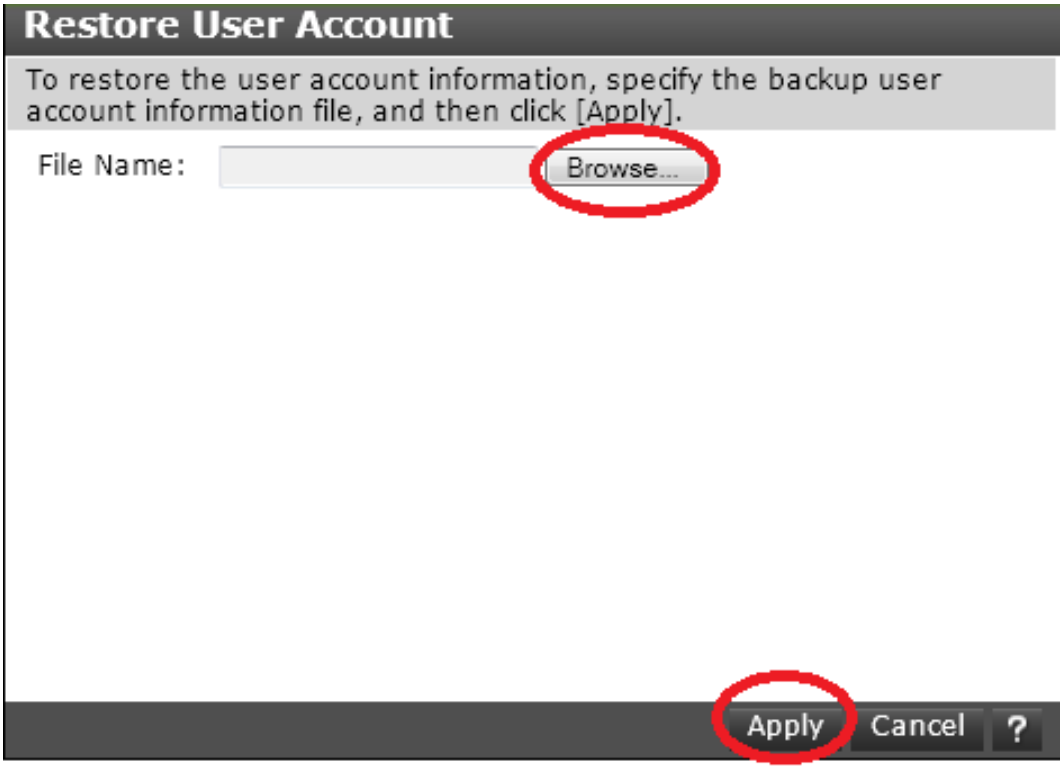


Restoring user account information

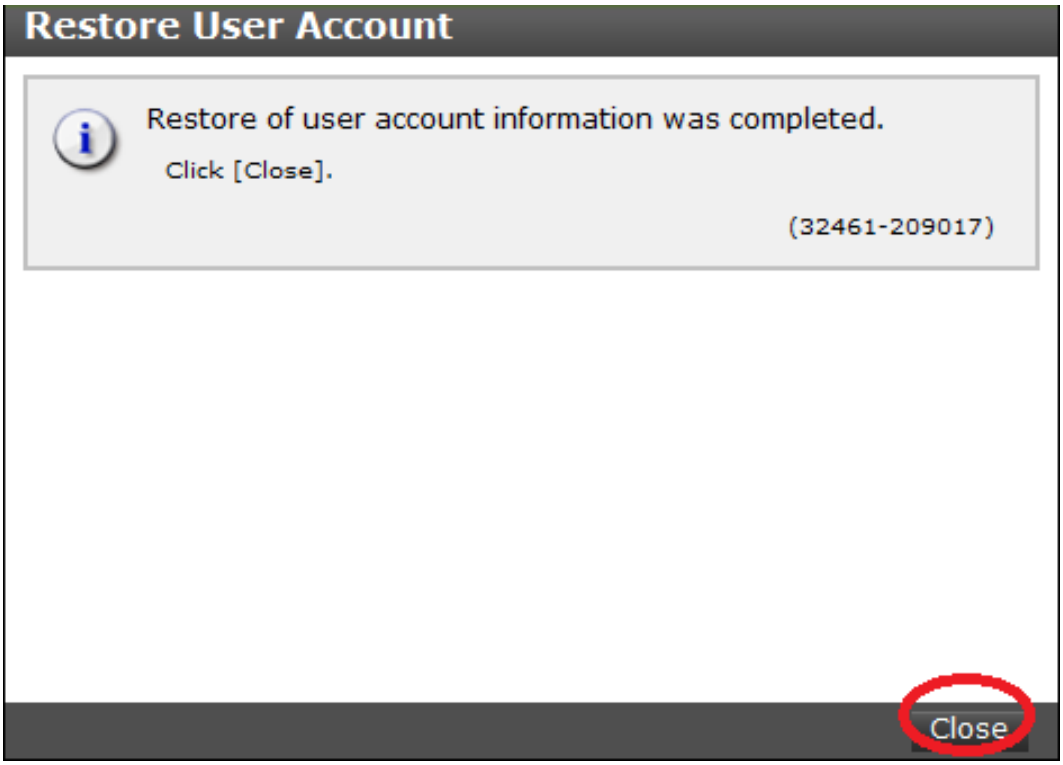
Procedure

1. In the **Maintenance Utility** window, click **Administration** > **User Administration**.
2. In the **User Administration** window, click **User Account Information** > **Restore**.

3. In the **Restore User Account** window, specify the file to be restored, and then click **Apply**.



4. When a completion message appears, click **Close**.



Changing the administrator password

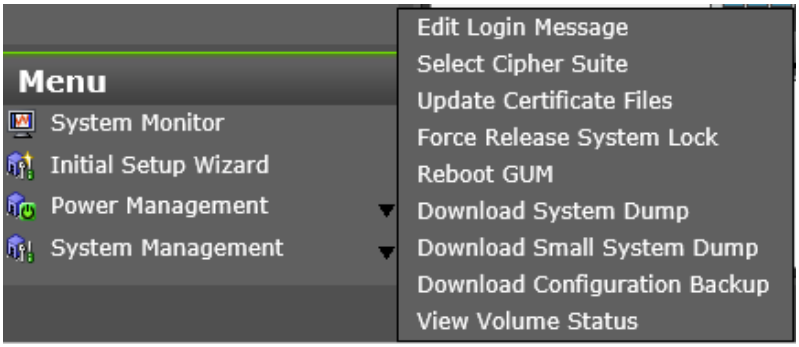
You can change the administrator password using the maintenance utility.

Before you begin

- Before changing the password of a user account specified by the registered storage system in the **Storage Device List** window, click Stop Service for the registered storage system. After changing the password of the user account, click Edit and set the new password, then click Start Service for the storage system.

Procedure

1. In the maintenance utility **Menu** navigation tree, click **System Management**.



2. Click **Change Password**.
3. Enter your current password and a new password. Enter the password again in the **Re-enter Password** field.
4. Click **Finish**.

Managing resource groups

You can divide a provisioned storage system into resource groups that allow you to manage the storage system as multiple virtual private storage systems. Configuring resource groups involves creating resource groups, moving storage system resources into the resource groups, and assigning resource groups to user groups.

About resource groups

A storage system can connect to multiple hosts and be shared by multiple divisions in a company or by multiple companies. Many storage administrators from different organizations can access the storage system. Managing the entire storage system can become complex and difficult. Potential problems are that private data might be accessed by other users, or a volume in one organization might be accidentally destroyed by a storage administrator in another organization.

To avoid such problems, use Hitachi Resource Partition Manager software to set up resource groups that allow you to manage one storage system as multiple virtual private storage systems. The storage administrator in each resource group can access only their assigned resources. Resource groups prevent the risk of data leakage or data destruction by another storage administrator in another resource group.

The following resources can be assigned to resource groups.

- LDEV IDs
- Parity groups
- External volumes
- Ports
- Host group IDs
- iSCSI target IDs

Note:

Before you create LDEVs, you can reserve the desired number of LDEV IDs and assign them to a resource group for future use. You can also reserve and assign host group IDs and iSCSI target IDs in advance because the number of host groups or iSCSI targets per port is limited.

meta_resource

The meta_resource group is the resource group consisting of the resources that exist on the storage system (other than external volumes) before Resource Partition Manager is installed. By default, all existing resources initially belong to the meta_resource group to ensure compatibility with older software when a system is upgraded to include Resource Partition Manager.

Resource lock

When a task is being processed on a resource, all of the resource groups assigned to the logged-on user are locked for exclusive access. When a resource is locked, a status indicator appears on the Device Manager - Storage Navigator status bar. To view information about the locked resource, click Resource Locked.

Note: Opening a Device Manager - Storage Navigator secondary window (such as **Basic Information Display**) or performing an operation from the service processor (SVP) locks all of the resource groups in the storage system.

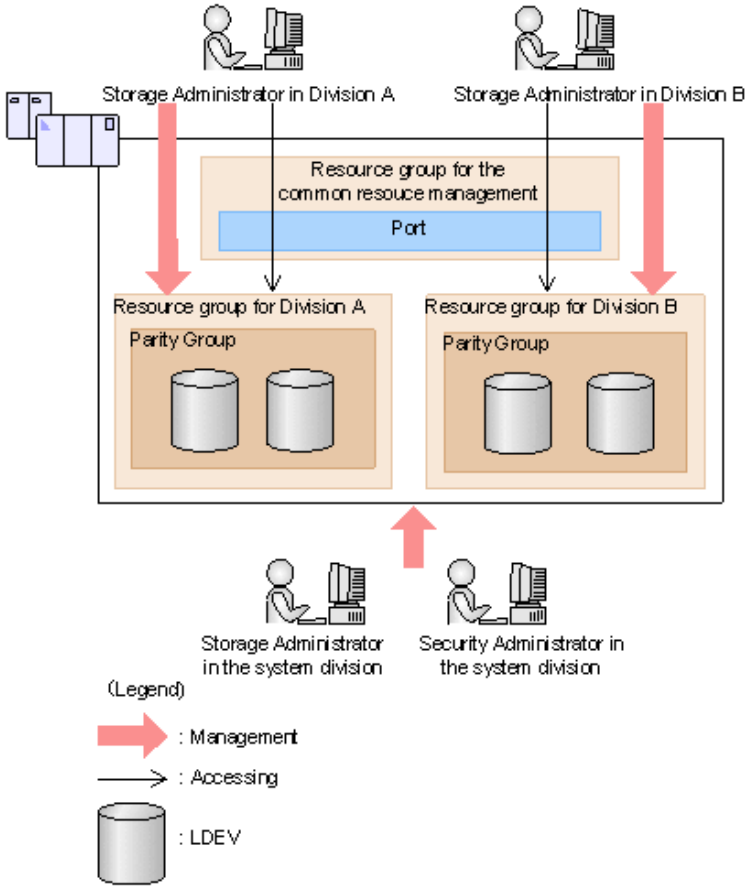
Examples

The following examples illustrate how you can configure resource groups on your storage system.

Resource groups sharing a port

If you have a limited number of ports, you can still operate a storage system effectively by sharing ports using resource groups.

The following example shows the system configuration of an in-house division providing virtual private storage system for two divisions. Divisions A and B each use their own assigned parity group, but share a port between the two divisions. The shared port is managed by the system division.



The Security Administrator in the system division creates resource groups for each division in the storage system and assigns them to the respective divisions. The Storage Administrator in Division A can manage the resource groups for Division A but cannot access the resource groups for Division B. In the same manner, the Storage Administrator in Division B can manage the resource groups for Division B but cannot access the resource groups for Division A.

The Security Administrator creates a resource group for managing the common resources, and the Storage Administrator in the system division manages the port that is shared between Divisions A and B. The Storage Administrators in Divisions A and B cannot manage the shared port belonging to the resource group for common resources management.

Configuration workflow for resource groups sharing a port

1. The system division forms a plan about the resource group creation and assignment of the resources.

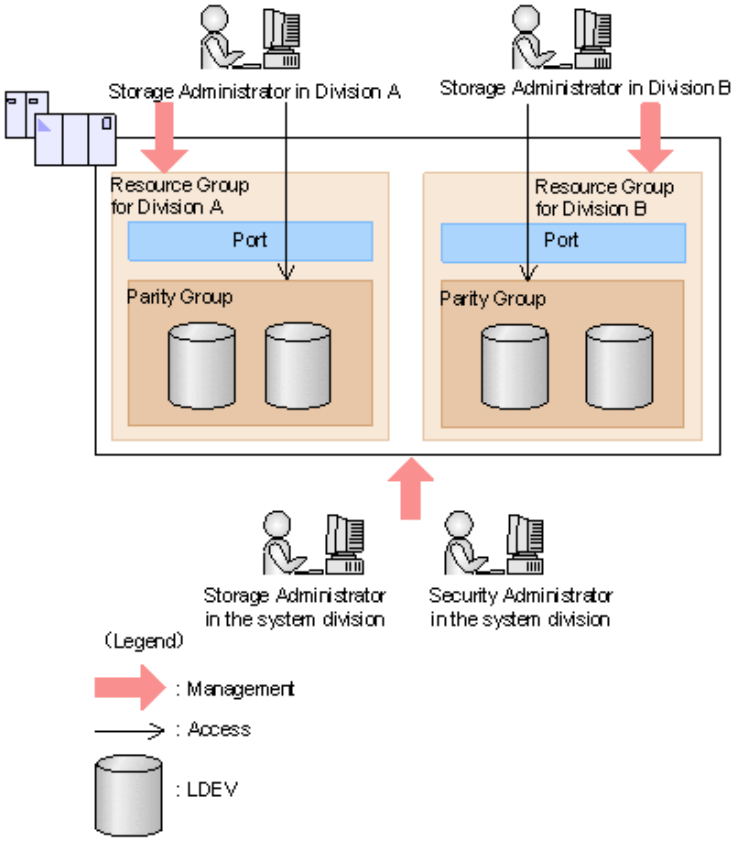
2. The Security Administrator creates the resource groups.
3. The Security Administrator creates the user groups.
4. The Security Administrator assigns the resource groups to the user groups.
5. The Storage Administrator in the system division sets a port.
6. The Security Administrator assigns resources to the resource groups.
7. The Security Administrator assigns the Storage Administrators to the appropriate user groups.

After the above procedures, the Storage Administrators in Divisions A and B can manage the resource groups assigned to their own division.

Resource groups not sharing ports

If you assign ports to each resource group without sharing, performance can be maintained on a different port even if the bulk of I/O is issued from one side port.

The following shows a system configuration example of an in-house system division providing the virtual private storage system for two divisions. Divisions A and B each use individual assigned ports and parity groups. In this example, they do not share a port.



The Security Administrator in the system division creates resource groups for each division in the storage system and assigns them to the respective divisions. The Storage Administrator in Division A can manage the resource groups for Division A but cannot access the resource groups for Division B. In the same manner, the Storage Administrator in Division B can manage the resource groups for Division B but cannot access the resource groups for Division A.

Configuration workflow for resource groups not sharing a port

1. The system division forms a plan about creating resource groups and the assigning resources to the groups.
2. The Security Administrator creates the resource groups.
3. The Security Administrator creates the user groups.
4. The Security Administrator assigns the resource groups to user groups.
5. The Storage Administrator in the system division sets ports.
6. The Security Administrator assigns resources to the resource groups.
7. The Security Administrator assigns each Storage Administrator to each user group.

After the above procedures, the Storage Administrators in Divisions A and B can access the resource groups allocated to their own division.

Resource group assignments

All resource groups are normally assigned to the Security Administrator and the Audit Log Administrator.

Each resource group has a designated Storage Administrator who can access only their assigned resources and cannot access other resources.

All resource groups to which all resources in the storage system belong can be assigned to a user group. Configure this in Device Manager - Storage Navigator by setting All Resource Groups Assigned to Yes.

A user who has All Resource Groups Assigned set to Yes can access all resources in the storage system. For example, if a user is a Security Administrator (with View & Modify privileges) and a Storage Administrator (with View and Modify privileges) and All Resource Groups Assigned is Yes on that user account, the user can edit the storage for all the resources.

If allowing this access becomes a problem with security on the storage system, then register the following two user accounts and use these different accounts for different purposes.

- A user account for a Security Administrator where All Resource Groups Assigned is set to Yes.
- A user account for a Storage Administrator who does not have all resource groups assigned and has only some of the resource groups assigned.

Resource group rules, restrictions, and guidelines

Rules

- The maximum number of resource groups that can be created on a storage system is 1023.

If you are providing a virtual private storage system to different companies, you should not share parity groups, external volumes, or pools if you want to limit the capacity that can be used by each user. When parity groups, external volumes, or pools are shared between multiple users, and if one user uses too much capacity of the shared resource, the other users might not be able to create an LDEV.

Creating resource groups

When you create a resource group, you enter a name and assign the desired resources (parity groups, LDEVs, ports, host groups, and iSCSI targets) to the new group. You can create more than one resource group at a time.

Before you begin

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

Procedure

1. In the **Explorer** pane, expand the **Storage Systems** tree, click the **Administration** tab, and then select **Resource Groups**.
2. In the **Explorer** pane, expand the **Storage Systems** tree, and then click the **Administration** tab.
3. Select **Resource Groups**, and then click **Create Resource Groups**.
4. In the **Create Resource Groups** window, enter the name for the new group, select the desired resources for the new group, and click **Add** to add the new group to list of resource groups to be added.

   Naming guidelines:

   - A resource group name can use alphanumeric characters, spaces, and the following symbols: ! # $ % & ' ( ) + - . = @ [ ] ^ _ ` { } ~
   - The characters in a resource group name are case-sensitive.
   - Duplicate occurrences of the same name are not allowed.
   - You cannot use the following names: `meta_resource`

5. Repeat the previous step for each new resource group to be added. If you need to remove a group from the list of resource groups to be added, select the group, and click **Remove**.

   Note: The maximum number of resource groups that can be created on a storage system is 1023.

6. When you are finished configuring new resource groups in the **Create Resource Groups** window, click **Next**.
7. Enter a task name or accept the default, and then click **Submit**.

   If you select **View task status**, the **Tasks & Alerts** tab opens.

Adding resources to a resource group

You can add resources to, remove resources from, and rename existing resource groups.

Note the following restrictions for editing resource groups:

- Only resources allocated to meta_resource can be added to resource groups.
- Resources removed from a resource group are returned to meta_resource.

- No resource can be added to or removed from meta_resource.
- The name of the meta_resource group cannot be changed or used for any resource group other than the meta_resource group.
- The system does not allow duplicate names.
- LDEVs with the same pool ID or journal ID cannot be added to multiple resource groups or partially removed from a resource group. For example, if two LDEVs belong to the same pool, you must allocate both to the same resource group. You cannot allocate them separately.

  You cannot partially remove LDEVs with the same pool ID or journal ID from a resource group. If LDEV1 and LDEV2 belong to the same pool, you cannot remove LDEV1 leave only LDEV2 in the resource group.

  Use the sort function to sort the LDEVs by pool ID or journal ID. Then select the IDs and add or remove them all at once.
- Host groups that belong to the initiator port cannot be added to a resource group.
- To add or delete DP pool volumes, you must first add or delete DP pools.

Before you begin

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

Procedure

1. In the **Explorer** pane, click the **Administration** tab, and then select **Resource Groups**.
2. Select the desired resource group (check the box next to the name of the resource group) to display the resource information for the resource group.
   - To change the name of the selected resource group, click **Edit Resource Group**, and enter the new name.
   - To add resources to the selected resource group, select the **Parity Groups**, **LDEVs**, **Ports**, or **Host Groups / iSCSI Targets** tab, click **Add Resources**, and follow the instructions on the **Add Resources** window.
   - To remove resources from the selected resource group, select the **Parity Groups**, **LDEVs**, **Ports**, or **Host Groups / iSCSI Targets** tab, select the resources to be removed, and then click **Remove Resources**.
3. Enter a task name or accept the default, and then click **Submit**.

   If you select **View task status**, the **Tasks & Alerts** tab opens.

Deleting resource groups

You can delete a resource group only when the resource group does not contain any resources and is not assigned to any user groups.

The following resource groups cannot be deleted:

- `meta_resource`
- A resource group that is assigned to a user group

- A resource group that has resources assigned to it
- Resource groups included in different resource groups cannot be removed at the same time.

Before you begin

The Security Administrator (View & Modify) role is required to perform this task.

Procedure

1. In the **Explorer** pane, expand the **Storage Systems** tree, click the **Administration** tab, select **Resource Groups**.
2. Click the check box of a **Resource Group Name**.
3. Click **Delete Resource Groups**.
4. Enter a task name or accept the default, and then click **Submit**.

   If you select **View task status**, the **Tasks & Alerts** tab opens.

Resource access requirements for Device Manager - Storage Navigator operations

When you log on to Device Manager - Storage Navigator, your user access privileges determine the resources you can view and the operations you can perform. User access privileges are determined by the user groups to which a user belongs and the resources assigned to those user groups. To perform an operation on the storage system, you must have access to the resources (for example, volumes, pools, ports) that are required for the operation.

These tables specify the resource access requirements for Device Manager - Storage Navigator operations.

Access requirements for Data Retention Utility

This table specifies the resource access requirements for Data Retention Utility operations.

Operation name	Condition
Set access attributes	The specified LDEV must be assigned to users.

Access requirements for Dynamic Provisioning and Dynamic Tiering

This table specifies the resource access requirements for Dynamic Provisioning and Dynamic Tiering operations.

Operation name	Condition
Create LDEVs	If DP-VOLs are created, these items must be assigned to the Storage Administrator group that is permitted to manage them. ▪ LDEV ID ▪ Pool-VOL of the pool
Delete LDEVs	If DP-VOLs are deleted, these items must be assigned to the Storage Administrator group that is permitted to manage them. ▪ LDEV ID ▪ Pool-VOL of the pool
Create pools Expand pools	Volumes to be specified as pool-VOLs must be assigned to the Storage Administrator group permitted to manage them. All the volumes that are specified when creating a pool must belong to the same resource group.
Edit pools Delete pools	Pool-VOLs of the specified pool must be assigned to the Storage Administrator group permitted to manage them.
Expand V-VOLs	You can expand only the DP-VOLs that are assigned to the Storage Administrator group permitted to manage them.
Reclaim zero pages Stop reclaiming zero pages	You can reclaim or stop reclaiming zero pages only for the DP-VOLs that are assigned to the Storage Administrator group permitted to manage them.

Access requirements for Encryption License Key

This table specifies the resource access requirements for Encryption License Key operations.

Operation name	Condition
Edit encryption keys	When you specify a parity group and open the **Edit Encryption** window, the specified parity group and LDEVs carved from the parity group must be assigned to the Storage Administrator group permitted to manage them. When you open the **Edit Encryption** window without specifying a parity group, more than one parity group and LDEVs carved from the parity group must be assigned to the Storage Administrator group permitted to manage them.

Access requirements for global-active device

This table specifies the resource access requirements for global-active device operations.

Operation name	Condition
Edit Ports	Specified ports must be assigned to the user.
Add Remote Connection	Specified ports must be assigned to the user.
Edit Remote Connection Options	Operation can be performed with no conditions.
Create Pairs	Primary volumes must be assigned to the user. Ports of remote paths that are connected with the primary volume in the remote storage must be assigned to the user.
Split Pairs	Specified primary volumes or secondary volumes must be assigned to the user.
Resync Pairs	Primary volumes must be assigned to the user.
Delete Pairs	Specified volumes must be assigned to the user. If primary volumes are specified, the ports of remote paths that are connected with the primary volume in the remote storage must be assigned to the user.
Edit Pair Options	Primary volumes must be assigned to the user.
Add Remote Paths	Specified ports must be assigned to the user.
Remove Remote Paths	Specified ports must be assigned to the user.
Edit Remote Connection Options	Ports of remote paths that are connected to a specified remote storage must be assigned to the user.
Remove Remote Connections	Ports of remote paths that are connected to a specified remote storage must be assigned to the user.
Force Delete Pairs	Specified primary volumes or secondary volumes must be assigned to the user.
Add Quorum Disks	LDEVs to be set as quorum disks must be assigned to the user.
Remove Quorum Disks	LDEVs set as quorum disks to be deleted must be assigned to the user.

Access requirements for LUN Manager

These tables specify the resource access requirements for LUN Manager operations.

For Fibre Channel

Operation name	Condition
Add LUN paths	When you specify host groups and open the **Add LUN Paths** window, the specified host groups must be assigned to the Storage Administrator group permitted to manage them. When you specify LDEVs and open the **Add LUN paths** window, the specified LDEVs must be assigned to the Storage Administrator group permitted to manage them.
Delete LUN paths	When you specify a host group and open the **Delete LUN Paths** window, the specified host group must be assigned to the Storage Administrator group permitted to manage them. When you specify LDEVs and open the **Delete LUN Paths** window, the specified LDEVs must be assigned to the Storage Administrator group permitted to manage them. When selecting the Delete all defined LUN paths to above LDEVs check box, the host groups of all the alternate paths in the LDEV displayed on the Selected LUNs table must be assigned to the Storage Administrator group permitted to manage them.
Edit host groups	The specified host groups and ports must be assigned to the Storage Administrator group permitted to manage them.
Add hosts	The specified host groups must be assigned to the Storage Administrator group permitted to manage them.
Edit hosts	The specified host group must be assigned to the Storage Administrator group permitted to manage them. When you select the Apply same settings to the HBA WWN of all ports check box, all the host groups where the specified HBA WWNs are registered must be assigned to the Storage Administrator group permitted to manage them.
Remove hosts	When you select the Remove hosts from all host groups containing the hosts in the storage system check box, all the host groups where the HBA WWNs displayed in the Selected Hosts table are registered must be assigned to the Storage Administrator group permitted to manage them.
Edit ports	The specified port must be assigned to the Storage Administrator group permitted to manage them.
Create alternative LUN paths	The specified host groups and all the LDEVs where the paths are set to the host groups must be assigned to the Storage Administrator group permitted to manage them.

Operation name	Condition
Copy LUN paths	The specified host groups and the LDEVs where the paths are set must be assigned to the Storage Administrator group permitted to manage them.
Edit command devices	LDEVs where the specified paths are set must be assigned to the Storage Administrator group permitted to manage them.
Edit UUIDs	The specified LDEV must be assigned to the Storage Administrator group permitted to manage them.
Delete UUIDs	The specified LDEV must be assigned to the Storage Administrator group permitted to manage them.
Create host groups	When you open the **Create Host Groups** window by specifying host groups, the specified host groups must be assigned to the Storage Administrator group permitted to manage them.
Delete host groups	The specified host groups and all the LDEVs where the paths are set to the host groups must be assigned to the Storage Administrator group permitted to manage them.
Release Host-Reserved LUNs	LDEVs where the specified paths are set must be assigned to you.

For iSCSI

Operation name	Condition
Add LUN paths	When you specify host groups and open the **Add LUN Paths** window, the specified iSCSI target must be assigned to the Storage Administrator group permitted to manage them. When you specify LDEVs and open the **Add LUN paths** window, the specified LDEVs must be assigned to the Storage Administrator group permitted to manage them.
Delete LUN paths	When you specify an iSCSI target and open the **Delete LUN Paths** window, the specified iSCSI target must be assigned to the Storage Administrator group permitted to manage them. When you specify LDEVs and open the **Delete LUN Paths** window, the specified LDEVs must be assigned to the Storage Administrator group permitted to manage them. When selecting the Delete all defined LUN paths to above LDEVs check box, the iSCSI target of all the alternate paths in the LDEV displayed on the Selected LUNs table must be assigned to the Storage Administrator group permitted to manage them.

Operation name	Condition
Add hosts	The specified iSCSI target must be assigned to the Storage Administrator group permitted to manage them.
Edit hosts	The specified iSCSI target must be assigned to the Storage Administrator group permitted to manage them. When you select the Apply same settings to the HBA WWN of all ports check box, all the iSCSI targets where the specified HBA WWNs are registered must be assigned to the Storage Administrator group permitted to manage them.
Remove hosts	The specified iSCSI target must be assigned to the Storage Administrator group permitted to manage them.
Edit ports	The specified port must be assigned to the Storage Administrator group permitted to manage them.
Create alternative LUN paths	The specified iSCSI target and all the LDEVs where the paths are set to the iSCSI target must be assigned to the Storage Administrator group permitted to manage them.
Copy LUN paths	The specified iSCSI target and the LDEVs where the paths are set must be assigned to the Storage Administrator group permitted to manage them.
Edit command devices	LDEVs where the specified paths are set must be assigned to the Storage Administrator group permitted to manage them.
Edit UUIDs	The specified LDEV must be assigned to the Storage Administrator group permitted to manage them.
Delete UUIDs	The specified LDEV must be assigned to the Storage Administrator group permitted to manage them.
Release Host-Reserved LUNs	LDEVs where the specified paths are set must be assigned to you.
Create iSCSI targets	When you open the **Create iSCSI targets** window by specifying iSCSI targets, the specified iSCSI targets must be assigned to the Storage Administrator group permitted to manage them.
Edit iSCSI targets	The specified iSCSI targets and ports must be assigned to the Storage Administrator group permitted to manage them.
Delete iSCSI targets	The specified iSCSI targets and all the LDEVs where the paths are set to the iSCSI targets must be assigned to the Storage Administrator group permitted to manage them.

Access requirements for Performance Monitor

This table specifies the resource access requirements for Performance Monitor operations.

Operation name	Condition
Add to ports	The specified ports must be assigned to the Storage Administrator group permitted to manage them.
Add new monitored WWNs	
Edit WWNs	

Access requirements for ShadowImage

This table specifies the resource access requirements for ShadowImage operations.

Operation name	Condition
Create pairs	Both primary volume and secondary volumes must be assigned to the Storage Administrator group permitted to manage them.
Split pairs	Primary volumes must be assigned to the Storage Administrator group permitted to manage them.
Suspend pairs	
Resynchronize pairs	
Release pairs	

Access requirements for Thin Image

This table specifies the resource access requirements for Thin Image operations.

Operation name	Condition
Create LDEVs	If LDEVs for Thin Image are created, these items must be assigned to the Storage Administrator group that is permitted to manage them. ▪ LDEV ID ▪ Pool VOL of the pool

Operation name	Condition
Delete LDEVs	If LDEVs for Thin Image are deleted, these items must be assigned to the Storage Administrator group that is permitted to manage them. ▪ LDEV ID ▪ Pool VOL of the pool
Create pools Expand Pool	Volumes that are specified when creating or expanding pools must be assigned to the Storage Administrator group that is permitted to manage them. All the volumes that are specified when creating pools must belong to the same resource group.
Edit Pools Delete Pools	Pool-VOLs of the specified pools must be assigned to the Storage Administrator group that is permitted to manage them.
Create pairs	Both primary volumes and secondary volumes must be assigned to the Storage Administrator group that is permitted to manage them.
Split pairs	Primary volumes must be assigned to the Storage Administrator group that is permitted to manage them.
Suspend pairs	
Resynchronize pairs	
Release pairs	

Access requirements for TrueCopy

This table specifies the resource access requirements for TrueCopy operations.

Operation name	Condition
Edit Ports	Specified ports must be assigned to the user.
Add Remote Connection	Specified ports must be assigned to the user.
Edit Remote Connection Options	Operation can be performed with no conditions.
Create Pairs	Primary volumes must be assigned to the user. Ports of remote paths that are connected with the primary volume in the remote storage must be assigned to the user.
Split Pairs	Specified primary volumes or secondary volumes must be assigned to the user.

Operation name	Condition
Resync Pairs	Primary volumes must be assigned to the user.
Delete Pairs	Specified volumes must be assigned to the user. If primary volumes are specified, the ports of remote paths that are connected with the primary volume in the remote storage must be assigned to the user.
Edit Pair Options	Primary volumes must be assigned to the user.
Add Remote Paths	Specified ports must be assigned to the user.
Remove Remote Paths	Specified ports must be assigned to the user.
Edit Remote Connection Options	Ports of remote paths that are connected to a specified remote storage must be assigned to the user.
Remove Remote Connections	Ports of remote paths that are connected to a specified remote storage must be assigned to the user.
Force Delete Pairs	Specified primary volumes or secondary volumes must be assigned to the user.

Access requirements for Universal Replicator

This table specifies the resource access requirements for Universal Replicator operations.

Operation name	Condition
Edit Ports	Specified ports must be assigned to the user.
Add Remote Connection	Specified ports must be assigned to the user.
Add Remote Paths	Specified ports must be assigned to the user.
Create Journals	All LDEVs that are specified when creating a journal must belong to the same resource group. Volumes to be assigned to a journal must be assigned to the user.
Assign Journal Volumes	Volumes to be assigned to a journal must be assigned to the user. All volumes to be assigned to a journal must belong to a same resource group to which the existing journal volumes belong.
Assign MP Unit	Journal volumes must be assigned to the user.
Edit Remote Connection Options	Operation can be performed with no conditions.

Operation name	Condition
Create Pairs	Journal volumes for pair volumes and primary volumes must be assigned to the user. Ports of remote paths that are connected with the primary volume in the remote storage must be assigned to the user.
Split Pairs	Specified primary volumes or secondary volumes must be assigned to the user.
Split Mirrors	All data volumes configured to a mirror must be assigned to the user.
Resync Pairs	Primary volumes must be assigned to the user.
Resync Mirrors	All data volumes configured to a mirror must be assigned to the user.
Delete Pairs	Specified volumes or secondary volume must be assigned to the user. Ports of remote paths that are connected with the primary volume in the remote storage must be assigned to the user.
Delete Mirrors	All data volumes configured to a mirror must be assigned to the user.
Edit Pair Options	Primary volumes must be assigned to the user.
Force Delete Pairs	Specified volumes must be assigned to the user.
Edit Journal Options	All data volumes consisting of the specified journal must be assigned to the user. Journal volumes must be assigned to the user.
Edit Mirror Options	All data volumes configuring the specified journal must be assigned to the user. Journal volumes must be assigned to the user.
Remove Journals	Journal volumes must be assigned to the user.
Edit Remote Connection Options	Ports of remote paths that are connected to a specified remote storage must be assigned to the user.
Remove Remote Paths	Specified ports must be assigned to the user.
Move LDEVs to other resource groups	When you move LDEVs used for journal volumes to other resource groups, you must specify all the journal volumes of the journal to which the LDEVs belong.
Assign Remote Command Devices	Journal volumes must be assigned to the user.

Operation name	Condition
	Specified remote command devices must be assigned to the user.
Release Remote Command Devices	Journal volumes must be assigned to the user. Specified remote command devices must be assigned to the user.

Access requirements for Universal Volume Manager

This table specifies the resource access requirements for Universal Volume Manager operations.

Operation name	Condition
Add external volumes	When creating an external volume, a volume is created in the resource group where the port belongs. When you specify a path group and open the **Add External Volumes** window, all the ports that compose the path group must be assigned to the Storage Administrator group permitted to manage them.
Delete external volumes	The specified external volume and all the LDEVs allocated to that external volume must be assigned to the Storage Administrator group permitted to manage them.
Disconnect external storage systems	All the external volumes belonging to the specified external storage system and all the LDEVs allocated to those external volumes must be assigned to the Storage Administrator group permitted to manage them.
Reconnect external storage systems	All the external volumes belonging to the specified external storage system and all the LDEVs allocated to those external volumes must be assigned to the Storage Administrator group permitted to manage them.
Disconnect external volumes	The specified external volumes and all the LDEVs allocated to those external volume must be assigned to the Storage Administrator group permitted to manage them.
Reconnect external volumes	The specified external volumes and all the LDEVs allocated to those external volumes must be assigned to the Storage Administrator group permitted to manage them.
Edit external volumes	The specified external volumes must be assigned to the Storage Administrator group permitted to manage them.

Operation name	Condition
Assign MP Unit	The specified external volumes and all the ports of the external paths connecting the external volumes must be assigned to the Storage Administrator group permitted to manage them.
Disconnect external paths	Ports of the specified external paths and all the external volumes connecting with the external path must be assigned to the Storage Administrator group permitted to manage them. When you specify By Ports, all the external paths connecting with the specified ports and all the external volumes connecting with the external paths must be assigned to the Storage Administrator group permitted to manage them. When you specify By External WWNs, all the ports of the external paths connecting to the specified external WWN and all the external volumes connecting with those external paths must be assigned to the Storage Administrator group permitted to manage them.
Reconnect external paths	Ports of the specified external paths and all the external volumes connecting with those external paths must be assigned to the Storage Administrator group permitted to manage them. When you specify By Ports, all the external paths connecting with the specified ports and all the external volumes connecting with the external paths must be assigned to the Storage Administrator group permitted to manage them. When you specify By External WWNs, all the ports of the external paths connecting to the specified external WWN and all the external volumes connecting with those external paths must be assigned to the Storage Administrator group permitted to manage them.
Edit external WWNs	All the ports of the external paths connecting to the specified external WWN and all the external volumes connecting with the external paths must be assigned to the Storage Administrator group permitted to manage them.
Edit external path configuration	Ports of all the external paths composing the specified path group and all the external volumes that belong to the path group must be assigned to the Storage Administrator group permitted to manage them.

Access requirements for Virtual LUN

This table specifies the resource access requirements for Virtual LUN operations.

Operation name	Condition
Create LDEVs	When you specify a parity group and open the **Create LDEVs** window, the parity group must be assigned to the Storage Administrator group permitted to manage them. When you create an internal or external volumes, the parity groups to which the LDEVs belong and the IDs of the new LDEVs must be assigned to the Storage Administrator group permitted to manage them.
Delete LDEVs	When deleting an internal or external volume, the deleted LDEV and parity groups where the LDEV belongs must be assigned to the Storage Administrator group permitted to manage them.
Edit LDEVs	The specified LDEV must be assigned to the Storage Administrator group permitted to manage them.
Restore LDEVs	When you specify LDEVs and open the **Restore LDEVs** window, the specified LDEVs must be assigned to the Storage Administrator group permitted to manage them. When you specify a parity group and open the **Restore LDEVs** window, the specified parity group and all the LDEVs in the parity group must be assigned to the Storage Administrator group permitted to manage them.
Block LDEVs	When you specify LDEVs and open the **Block LDEVs** window, the specified LDEVs must be assigned to the Storage Administrator group permitted to manage them. When you specify a parity group and open the **Block LDEVs** window, the specified parity group and all the LDEVs in the parity group must be assigned to the Storage Administrator group permitted to manage them.
Format LDEVs	When you specify LDEV and open the **Format LDEVs** window, the specified LDEV must be assigned to the Storage Administrator group permitted to manage them. When you specify a parity group and open the **Format LDEVs** window, the specified parity group and all the LDEVs in the parity group must be assigned to the Storage Administrator group permitted to manage them.
Delete Parity Groups	When deleting a parity group, the parity group to be deleted must be assigned to the Storage Administrator group permitted to manage them.
Format Parity Groups	When you specify a parity group and open the **Format Parity Groups** window, the specified parity group must be assigned to the Storage Administrator group permitted to manage them.

Access requirements for Virtual Partition Manager

This table specifies the resource access requirements for Virtual Partition Manager operations.

Operation name	Condition
Migrate parity groups	When you specify virtual volumes, the specified LDEV must be assigned to the Storage Administrator group permitted to manage them. When you specify a parity group, the specified parity group must be assigned to the Storage Administrator group permitted to manage them.

Access requirements for Volume Migration

This table specifies the resource access requirements for Volume Migration operations.

Operation name	Condition
Migrate volumes	The specified source volume and target volume must be assigned to the Storage Administrator group permitted to manage them.

Access requirements for Volume Shredder

This table specifies the resource access requirements for Volume Shredder operations.

Operation name	Condition
Shred LDEVs	When you specify LDEVs and open the **Shred LDEVs** window, the specified LDEVs must be assigned to the Storage Administrator group permitted to manage them. When you specify a parity group and open the **Shred LDEVs** window, the specified parity group and all the LDEVs in the parity group must be assigned to the Storage Administrator group permitted to manage them.

Access requirements for Server Priority Manager

This table specifies the resource access requirements for Server Priority Manager operations.

Operation name	Conditions
Set priority of ports (attribute/ threshold/upper limit)	The specified ports must be assigned to the Storage Administrator group permitted to manage them.
Release settings on ports by the decrease of ports	
Set priority of WWNs (attribute/upper limit)	
Change WWNs and SPM names	
Add WWNs (add WWNs to SPM groups)	
Delete WWNs (delete WWNs from SPM groups)	
Add SPM groups and WWNs	
Delete SPM groups	
Set priority of SPM groups (attribute/ upper limit)	
Rename SPM groups	
Add WWNs	
Delete WWNs	
Initialization	All ports must be assigned to the Storage Administrator group permitted to manage them.
Set threshold	

Chapter 7: Monitoring alerts and events

Use alert notifications to monitor the storage system for changes in configuration or status.

Alert notifications overview

You can view alert email messages, Syslog messages, and SNMP trap messages using Device Manager - Storage Navigator or using the maintenance utility.

Email

Check your email to view alerts sent by email. Alerts that are reported through email are the same as the SIM information that is displayed in the Alert window or reported through an SNMP trap.

Syslog

Check the messages on the Syslog server to view alert information sent there.

SNMP traps

To view SNMP trap information, use SNMP Manager in Device Manager - Storage Navigator. For information about using SNMP traps, see the *SNMP Agent User Guide*.

The SNMP Agent is mounted on each controller (CTL). The SNMP Agent on each CTL sends traps to the SNMP Manager. When you use SNMP v3 protocol, you need to register the SNMP Engine ID for each CTL in the SNMP Manager. The SNMP Engine ID is displayed on the SNMP tab of the Alert Notifications window of the maintenance utility.

Note:

- Storage system failure information is sent from the management port on CTL1 or CTL2 via the management LAN. If either of the CTLs stops due to a failure, failure information is sent from the management port on the normal CTL. Therefore, make sure to connect the management ports on both CTL1 and CTL2 to the management LAN. If the management port on only one CTL is connected to the management LAN, failure information might not be reported correctly.
- If a communication failure occurs, a maximum of 256 failure information sets might not be reported. However, when the communication failure is resolved, the failure information is reported within about 5 minutes.

Alert notification email

The following example shows an alert notification email that is sent from the storage system to the mail server.

```
VSP E990 Report
//HM900 //VSP ////////////////////////////
//e-Mail Report
////////////////////////////
Date : 20/04/2021
Time : 00:20:00
Machine : VSP E990(Serial# 400102)
RefCode : 7fffff
Detail: This is Test Report.
```

The following table describes the components of an alert notification email.

Component	Item in the example	Description
Title	VSP E990 Report	*product-name-of-the-storage-system* Report

Additional information	//HM900 //
	VSP ////////////////////////////
	//e-Mail Report
	////////////////////////////
		The information set in Setting up email notifications (on page 183)
		Nothing appears if no information is set.

Date	Date : 20/04/2021	The date when the error occurred
Time	Time : 00:20:00	The time when the error occurred
Hardware identification	Machine : VSP E990 (serial# 400102)	*storage-system-name-set-in-Storage-Navigator*(serial# *serial-number*)
Failure code	RefCode : 7fffff	The reference code that appears in the alert window
Failure detail	Detail: This is Test Report.	Information of failure locations that need maintenance Information of a maximum of eight failure locations appears. Each information item includes the following items: action code, assumed failure part, and location.

Syslog message

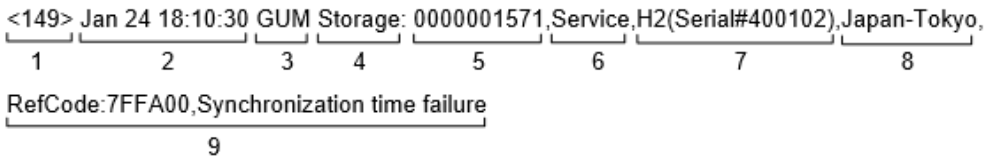
The following examples show Syslog messages that are sent from the storage system to the syslog server.

Note: The contents of a syslog message differ depending on whether the message is for alert notification or for audit log. The contents of a syslog message for alert notification are shown here. For details about the contents of a syslog message for audit log, see the *Hitachi Audit Log User Guide*.

You can use the maintenance utility to select either of the following message formats: RFC3164-compliant or RFC5424-compliant.

For details, see Syslog settings (on page 184)

Syslog file format (RFC3164-compliant)



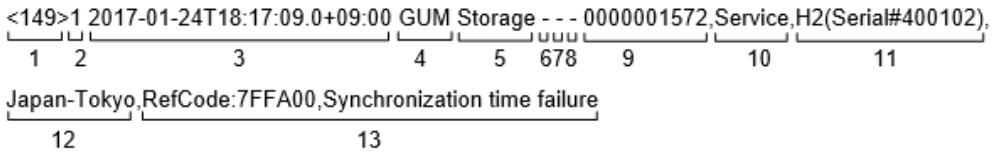
No.	Item	Description
1	Priority	The priority of a syslog message is determined according to the following formula, enclosed by angle brackets (< >): *Priority* = 8 × *Facility* + *Severity* *Facility* is 18 (fixed). *Severity* depends on the type of log information: ▪ 3: Error (abnormal end) ▪ 4: Warning (partially abnormal end, or an operation was canceled before it could be completed) ▪ 5: Notice (normal end) For example, if *Severity* is 3 (Error), <147> is output as the priority value.
2	Date, time[1]	The date and time in the format of "*MMM DD HH*:*MM*:*SS*" ▪ *MMM*: first three letters of the month (Jan to Dec) ▪ *DD*: date If *DD* is a single digit (for example, 1), it is displayed as " 1" (with a blank space before "1") and not as "01". ▪ *HH*: hour ▪ *MM*: minute ▪ *SS*: second

No.	Item	Description
3	Detected location	"GUM" (fixed)
4	Program name	"Storage" (fixed)
5	Message identification	The serial number (0000000000 to 4294967295)
6	Event type	Any of the following event category names. (The event category corresponds to *Severity*.) ▪ Acute *Severity* is 3 (Error). ▪ Serious *Severity* is 3 (Error). ▪ Moderate *Severity* is 4 (Warning). ▪ Service *Severity* is 5 (Notice).
7	Hardware identification[2]	The storage system name and serial number
8	Related information	The location identification information set in the Syslog tab in the maintenance utility
9	Detailed information	The SIM reference code and failure information that are displayed in the alert window

Notes:

1. A date and time being set on SVP are output as log data. If a failure, such as a SVP failure and a LAN failure, occurs in the storage system, the date and time may be output of the accumulated date and time since January 01, 1970.
2. While the controller model is being upgraded, information before upgrade might be output. While the controller model is being downgraded, information before downgrade might be output.

Syslog file format (RFC5424-compliant)



No.	Item	Description
1	Priority	The priority of a syslog message is determined according to the following formula, enclosed by angle brackets (< >): *Priority* = 8 × *Facility* + *Severity* *Facility* is 18 (fixed). *Severity* depends on the type of log information: ▪ 3: Error (abnormal end) ▪ 4: Warning (partially abnormal end, or an operation was canceled before it could be completed) ▪ 5: Notice (normal end) For example, if *Severity* is 3 (Error), <147> is output as the priority value.
2	Version	"1" (fixed)
3	Date, time[1]	The date, time, and the time difference between UTC (Coordinated Universal Time) and the local time in the format of "*YYYY-MM-DD*T*hh*:*mm*:*ss*.*s*±*hh*:*mm*" ▪ *YYYY*: year, *MM*: month, *DD*: date ▪ *hh*: hour, *mm*: minute, *ss*.*s*: second in one decimal place ▪ ±*hh*:*mm*: hours and minutes of the time difference. "Z" is written instead of "± *hh*:*mm*" when there is no time difference between UTC and the local time, such as "2018-12-26T23:06:58.0Z".
4	Detected location	"GUM" (fixed)
5	Program name	"Storage" (fixed)
6	Process name	"-" (fixed.)
7	Message ID	"-" (fixed.)
8	Structured data	"-" (fixed.)
9	Message identification	The serial number (0000000000 to 4294967295)
10	Event type	Any of the following event category names. (The event category corresponds to *Severity*.) ▪ Acute *Severity* is 3 (Error). ▪ Serious *Severity* is 3 (Error).

No.	Item	Description
		▪ Moderate *Severity* is 4 (Warning). ▪ Service *Severity* is 5 (Notice).
11	Hardware identification[2]	The storage system name and serial number
12	Related information	The location identification information set in the Syslog tab in the maintenance utility
13	Detailed information	The SIM reference code and failure information that are displayed in the alert window

Notes:

1. A date and time being set on SVP are output as log data. If a failure, such as a SVP failure and a LAN failure, occurs in the storage system, the date and time may be output of the accumulated date and time since January 01, 1970.
2. While the controller model is being upgraded, information before upgrade might be output. While the controller model is being downgraded, information before downgrade might be output.

SNMP message

SNMP data is sent from a storage system to the SNMP agent. The following table describes an example of event details that are contained in SNMP data.

Component	Example	Description
TRAP type	raideventUsermoderate	Failure level
eventTrapSerialNumber	400001	Serial number of the product
eventTrapNickname	HM900	Product name
eventTrapREFCODE	7d0201	The reference code that appears in the alert window
eventTrapPartsID	dkcHWEnvironment	Failure location
eventTrapDate	2020/01/07	The date the SNMP Agent received the SNMP data
eventTrapTime	16:31:19	The time the SNMP Agent received the SNMP data

Component	Example	Description
eventTrapDescription	"LAN error(CTL1-CTL2)"	Information of the failure locations that need maintenance

Setting up email notifications

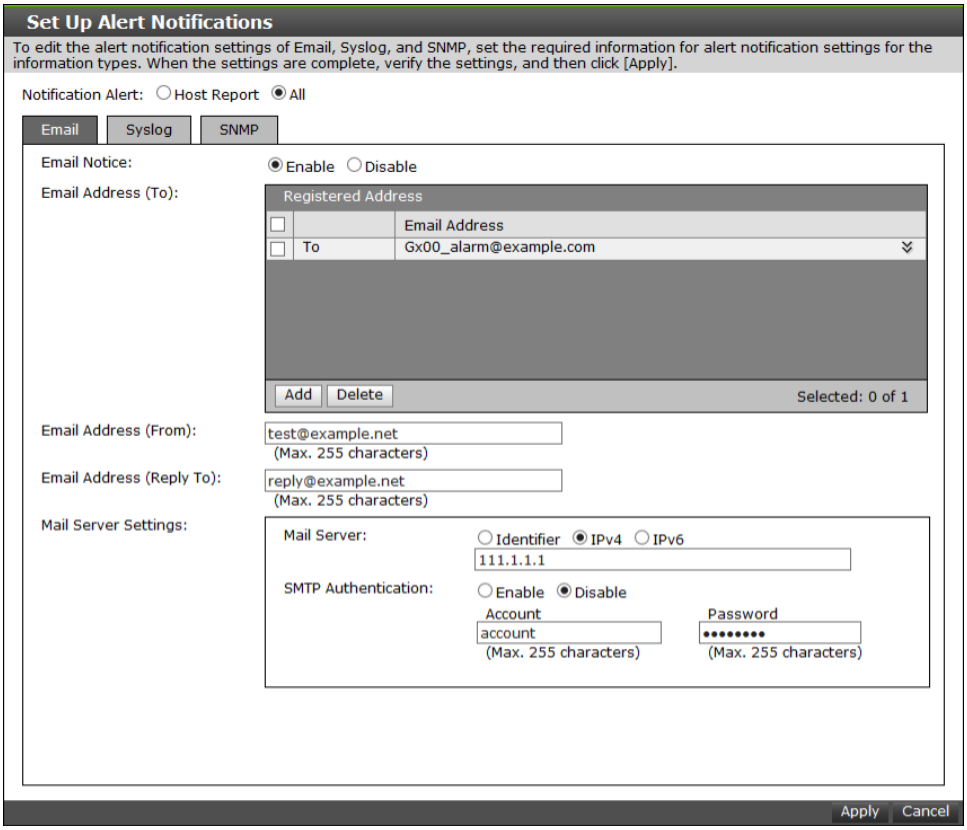
For details about the format of alert notification emails, see Alert notification email (on page 178).

Before you begin

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

Procedure

1. In the maintenance utility **Administration** pane, select **Alert Notifications**.
2. To send email notices, click **Enable**, next to **Email Notice**. Click **Disable** to not send email notices.



3. Click **Add** to add an email address to the list of registered addresses.

4. Enter the email address and then use the pull-down menu to select the type of address: **To**, **Cc**, or **Bcc.**
5. Click **OK** to save the email address and close the dialog box.
6. Enter an email address in **Email Address (From)**.
7. Enter an email address in **Email Address (Reply To:)**.
8. In **Mail Server Settings**, select the mail server type: **Identifier**, **IPv4**, or **IPv6.**
9. To use SMTP authentication, click **Enable**.
10. In **Account**, enter an SMTP account name.
11. In **Password**, enter the SMTP account password.
12. Click **Apply** to save the changes and close the **Set Up Alert Notifications** window.

Note: If SIMs are not transferred through email, verify the settings in the procedure. If all settings are correct, verify the settings and operating conditions of the mail server itself, and the operating conditions of the Management LAN.

Syslog settings

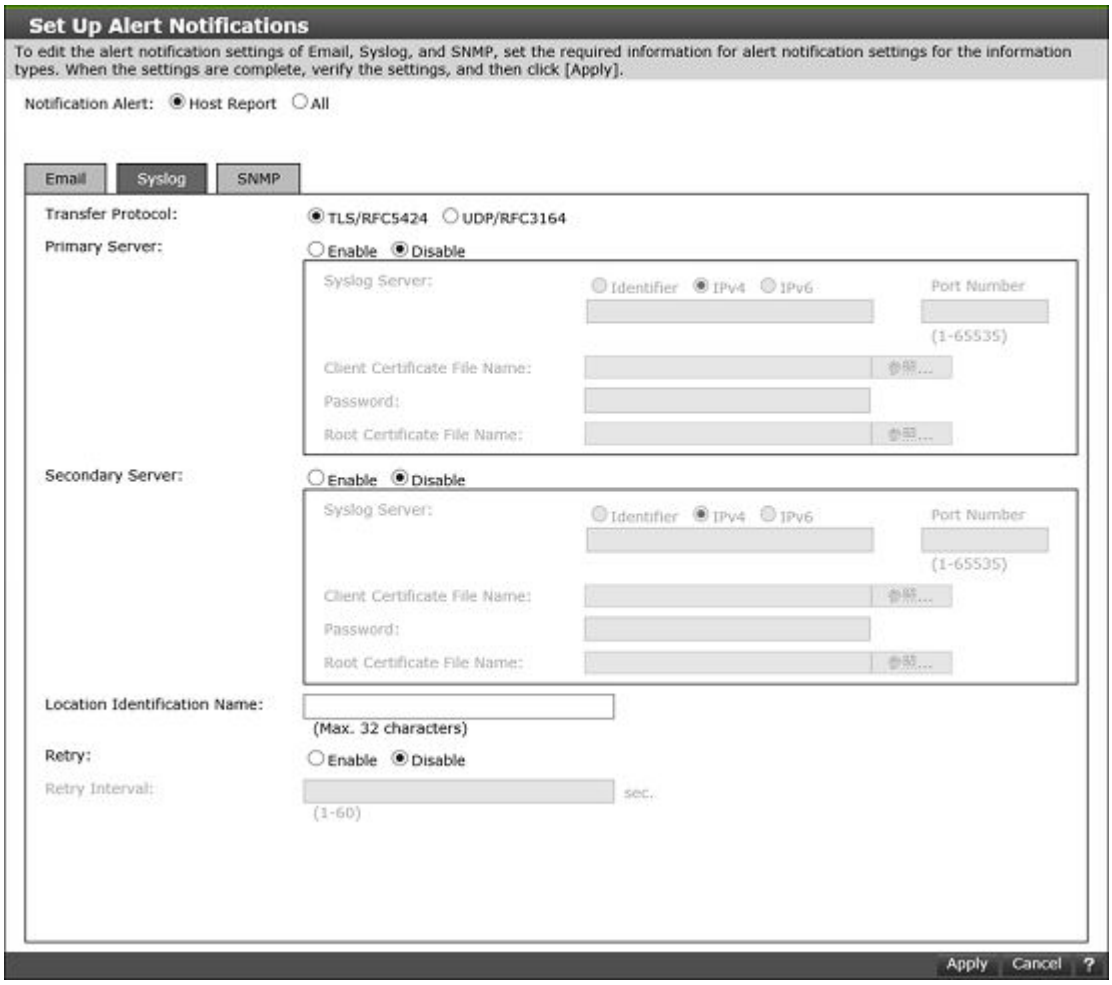
For details about the format of alert notifications sent to the syslog server, see Syslog message (on page 179).

Before you begin

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

Procedure

1. Click the **Syslog** tab.



2. Select the type of transfer protocol to use.
3. In **Primary Server**:
   a. Click **Enable** to use the server or **Disable** not to use it.
   b. Select the type of IP address to use for the server: **IPv4** or **IPv6**.
   c. In **Client Certificate File Name**, click **Browse** to select a client certificate file.
4. In **Secondary Server**:
   a. Click **Enable** to use the server or **Disable** not to use it.
   b. Select the type of IP address to use for the server: **IPv4** or **IPv6**.
   c. In **Client Certificate File Name**, click **Browse** to select a client certificate file.
5. In **Location Identification Name**, enter a name to use to identify the server.
6. To set up an automatic attempt to reconnect to the server in case of communication failure, in **Retry**, click **Enable**. Click **Disable** to not use this feature.
7. If you enabled retry, in **Retry Interval**, enter the number of seconds that the system will wait between retry attempts.

Note: If SIMs are not transferred to the Syslog server, verify the settings in the procedure. If all settings are correct, verify the settings and operating conditions of the Syslog server itself, and the operating conditions of the Management LAN.

SNMP settings

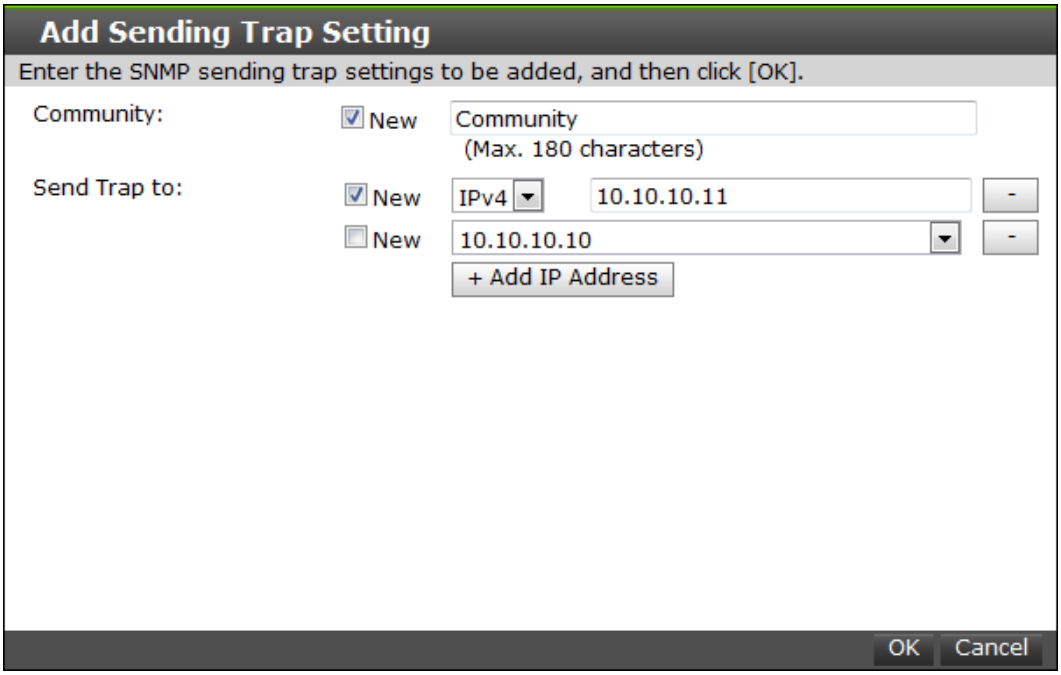
For details about the format of SNMP messages sent to the SNMP Manager, see SNMP message (on page 182).

Before you begin

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

Procedure

1. Click the **SNMP** tab.
2. In **SNMP Agent**, click **Enable** to use the agent or **Disable** not to use it.
3. In **Trap Destination**, click the type of address to send the SNMP trap information: **Community** or **Public.**
4. Click **Add** to add an SNMP trap address.



5. In **Community**, create a new community name or select an existing one.
6. In **Send Trap to**, enter a new IP address or select an existing one.
7. Click **OK** to save the information and close the dialog box.

Reporting failure information about storage systems

You can report failure information (SIM) about storage systems through Syslog, SNMP trap, and email. Failure information reported through email is the same as SIM displayed on the **Alert** window or reported through SNMP trap. For SNMP trap, the user needs to access the SNMP Manager to check for failure. However, for report through Syslog or email, the user has only to check Syslog or email to know about the occurrence of failure. For methods of notification with SNMP traps, see the *SNMP Agent User Guide*.

Requirements of the Syslog transfer protocol (TLS/RFC5424)

The Syslog transfer protocol (TLS/RFC5424) requires the following:

- Syslog server that supports TLS (TLS 1.2 or later)
- Syslog server certificate
  - Do not use any items other than the following items (that are specified in RFC5280) for the extended profile fields in the X.509 certificate:
    - BasicConstraints
    - KeyUsage
    - SubjectKeyIdentifier
    - SubjectAltName
  - The number of tiers of the certificate chain must be 5 tiers or fewer.
- Client certificates

  The following table lists and describes the certificates that can be uploaded to the SVP.

  Note:
  - Consult the Syslog server administrator for details about these certificates and appropriately manage the certificates.
  - Be careful about the expiration date of certificates. If a certificate is expired, you will not be able to connect to the Syslog server.
  - Ask the Syslog server administrator for the root certificate of the Syslog server. Also, convert the client certificate signed by the Certificate Authority (CA) of the Syslog server to PKCS#12 format.
  - Contact the Syslog server administrator for the password set for the PKCS#12-format client certificate.

Certificate type	Format	Requirements
Syslog server root certificate	X.509	Any items other than the following items (that are specified in RFC5280) must not be used

Certificate type	Format	Requirements
		for the extended profile fields in the X.509 certificate: ▪ BasicConstraints ▪ KeyUsage ▪ SubjectKeyIdentifier
Client certificate	PKCS#12	▪ If an intermediate certificate exists, you must prepare a signed public key certificate in a certificate chain that contains the intermediate certificate. ▪ The number of tiers of the certificate chain for the certificate to be uploaded must be 5 tiers or fewer including the root CA certificate. ▪ The public key of the certificate to be uploaded must be RSA. ▪ The IP addresses or host names of GUM(CTL1) and GUM(CTL2) must be set for Common Name and Subject Alternative Name in the client certificate. If an intermediate certificate is provided by a certificate authority, set the intermediate certificate on the Syslog server.

Obtaining a client certificate for the Syslog protocol

You must obtain a client certificate from the SVP to enable the Syslog protocol.

Procedure

1. Create a private key (.key file). See Creating a private key using the OpenSSL command (on page 53).
2. Create a public key (.csr file). See Creating a public key using the OpenSSL command (on page 54).
3. Send the new key to the Syslog server Certificate Authority for signature to obtain a certificate. The certificate is used as the client certificate.

Caution:

- If the certificate expires, you cannot connect to the Syslog server.
- If an intermediate certificate is provided by the certificate authority, set the intermediate certificate on the Syslog server.

4. Open a Windows command prompt, and then set the current directory to the directory where the PKCS#12 format client certificate is output.
5. Store the private key (`.key` file) and client certificate in this folder, and then execute the command below.

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

   Where

   - Folder to which the PKCS#12 format client certificate is output: `C:\key`
   - File name of the private key: `client.key`
   - File name of the client certificate: `client.crt`
6. Set the password.

   The password can have up to 128 characters. You can use alphanumeric characters and the following 31 symbols:

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

Configuring syslog notification for SIMs

You can be notified in syslog format when storage system failures occur.

Note: If no alert is sent to the Syslog server after you perform this procedure, check and correct the settings as described in the following procdure. If the settings are correct, check the settings and operating status of the Syslog server and the operating status of the management LAN.

Before you begin

- You must have the Storage Administrator (Initial Configuration) role to perform this task. See Roles and permissions (on page 130).
- You must have a server that supports syslogs.
- If a firewall is used, a port must be opened to transfer syslogs.

Note: In any of the following steps, if you enter an invalid character or do not enter required information, a message box displays, asking you to reenter the information.

Procedure

1. In the **Maintenance Utility** menu, select **Alert Notifications**.
2. Click **Set Up** on the **Alert Notifications** window. The **Set Up Alert Notifications** window displays.

3. For **Notification Alert**, select one of the following:

   Host Report: Sends alerts only of SIMs that report to hosts.

   All: Sends alerts of all SIMs.

   The alert notification destination is common to Syslog, SNMP, and Email.

4. Select the **Syslog** tab.
5. In **Transfer Protocol**, select the protocol for Syslog transfer.
6. To transfer Syslog to the primary server and alternative secondary server, select **Enable** and set the following items:
   - IP Address or host name
   - Port Number

   Set the following items only when you select **TLS/RFC5424** in **Transfer Protocol**:
   - Client Certificate File Name
   - Password
   - Root Certificate File Name
7. Enter a name in **Location Identification Name** for identification for the storage system.
8. If you select **TLS/RFC5424** in **Transfer Protocol**, select **Enable** for **Retry** and then specify the retry interval.
9. Click **Apply**. When the completion message is displayed, click **OK**.

Configuring email notification

You can configure the required information to notify storage system failure (SIM) by email.

Note: If no alert is sent to the Syslog server after you perform this procedure, check and correct the settings as described in the following procdure. If the settings are correct, check the settings and operating status of the Syslog server and the operating status of the management LAN.

Before you begin

- You must have a Storage Administrator account with an Initial Configuration role to perform this task.
- You must have a mail server that supports the Simple Mail Transfer Protocol (SMTP). The SVP uses PLAIN or LOGIN of SMTP authentication (SMTP-AUTH) to connect to the mail server. CRAM-MD5 and DIGEST-MD5 of SMTP-AUTH are not supported.
- If a firewall is used, port 25 must be released because port 25 is used for communication between the SVP and the mail server.

Procedure

1. In the **Maintenance Utility** menu, select **Alert Notifications**.
2. Click **Set Up** on the **Alert Notifications** window. The **Set Up Alert Notifications** window displays.

3. Click **Settings > Environmental Settings > Edit Alert Settings**. The **Edit Alert Settings** window opens.
4. For **Notification Alert**, select one of the following:

   Host Report: Sends alerts only of SIMs that report to hosts.

   All: Sends alerts of all SIMs.

   Alert destinations are common to Syslog, SNMP, and Email.
5. On the **Email** tab, for **Mail Notice** select **Enable**.
6. In the **Email Settings** table, set the email destination address and attributes (To, Cc, Bcc).

   This field is required when you select **Enable** in Mail Notice.

   - To add an email address, click **Add**. On the **Add Email Address** window, set the email address and attributes.
   - To delete an email address, select the email address to be deleted, and then click **Delete**. You can select more than one email address.
7. Enter the email source address (required) and return address (optional).
8. Enter the email server information.
9. In **SMTP Authentication**, select **Enable** to use SMTP authentication. Select **Disable** to not use SMTP authentication. If you select Enable, enter an account and password for SMTP authentication.
10. Click **Apply**. A completion message box displays. Click **OK**.
11. If necessary, click **Email Test Send** to test the settings.
12. Check that the test email has been received.

    For a test email example and explanation, see **Example of test email**, below.
13. Click **Finish**. The **Confirm** window opens.
14. In the **Confirm** window, check the settings and enter a task name in **Task Name**.
15. Click **Apply**. The task is registered. If the **Go to tasks window for status** check box is checked, the **Task** window opens.

Sending a test email message

Procedure

1. Click the **Email** tab.

   The **Email** tab displays the current settings for the mail server, SMTP authentications, and email addresses.
2. Click **Send Test Email**.

   A completion notice is displayed.
3. Click **OK** to acknowledge the notice and close the message. Verify that the log *(Detailed data: "RefCode: 7FFFFF, This is Test Report.")* has been transferred to the Syslog server.

Example of a test email message

```
Subject: VSP E990 Report
DATE : 24/10/2020
TIME : 10:09:30
Machine : Hitachi Virtual Storage Platform Ex00 (Serial# 400001)
RefCode : 7fffff
Detail: This is Test Report.
```

The field definitions in the test email message are listed in the following table.

Item	Description
Subject	Email title (name of the storage system) + (report)
DATE	Date when a system failure occurred
TIME	Time when a system failure occurred
Machine	Name and serial number of the storage system
RefCode	Reference code. The same code as the one reported by SNMP traps.
Detail	Failure details. The same information as the one reported by SNMP traps.

For reference codes and failure details, see the *SIM Reference Guide*.

Sending a test Syslog message

Procedure

1. Click the **Syslog** tab.
   The **Syslog** tab displays the current settings for the primary and secondary servers.
2. Click **Send Test message to the Syslog Server**.
   A completion notice appears.
3. Click **OK** to acknowledge the notice and close the message. Verify that the log *(Detailed data: "RefCode: 7FFFFF, This is Test Report.")* has been transferred to the Syslog server.

Sending a test SNMP trap

Procedure

1. Click the **SNMP** tab.
   The **SNMP** tab displays the current settings for the storage system name, contact, location, SNMP trap, and SNMP manager.

2. Click **Send Test SNMP Trap**.

   A completion notice displays.
3. Click **OK** to acknowledge the notice and close the message.

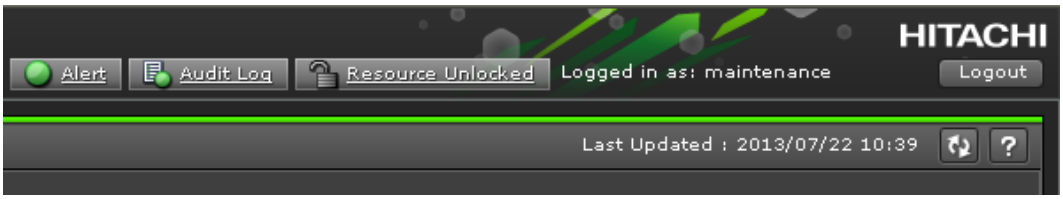
Monitoring SIM alerts in Device Manager - Storage Navigator

The Alert icon at the top of the Device Manager - Storage Navigator main window indicates whether service information messages (SIMs) have been issued by the storage system. Use the following procedure to

Procedure

1. In the Device Manager - Storage Navigator main window, click **Alert**.

   The **Alerts** window opens.



2. To check the details of an alert, select and right-click the row for that alert, and then click **Detail** in the pop-up menu.
3. If the following SIM reference codes appear, you must resolve the error (*xxx* indicates the pool ID):
   - For Thin Image: 601*xxx*, 602*xxx*, 602fffff, and 624000
   - For Dynamic Provisioning: 620*xxx*, 621*xxx*, 622*xxx*, 624000, 625000, and 626*xxx*.

   For details about how to resolve the error, see the *Hitachi Thin Image User Guide* or the *Provisioning Guide for Open Systems*.

Checking storage system alerts by using the maintenance utility

When a notification consisting of information about the detection of a failure in the storage system is sent via Health Status, an email message, or an SNMP trap message, you can check the alert information by using the maintenance utility, and then take appropriate action.

Before you begin

The logged-in user must be registered in the Maintenance user group (a built-in user group).

Procedure

1. In the navigation bar, click **Settings** and then select **Maintenance Utility** to open the maintenance utility.
2. Click the **Alerts** tab to display the list of alerts.

3. Check the alerts and then take appropriate action based on the notification information.

   Tip: For details about alerts, see the Provisioning Guide.

4. In the maintenance utility, click **Log Out**.

Using the Windows event log

Some failure information is output to the Windows event log.

Monitoring the system log using the Windows event log

You can manage the Windows error information by outputting failure information to the event log.

Before you begin

- The storage system status in the storage device list must be READY.

Procedure

1. Open a Windows command prompt with administrator permissions in SVP.
2. Execute the following command to move the current directory:

   ```
   cd /d C:\Mapp\wk\model-identification-number\DKC200\mp\pc
   ```

   - The default installation directory is `C:\Mapp:`*<installation-directory-of-SVP>*

     Note:

     - `C:\Mapp` indicates the installation directory of Device Manager - Storage Navigator. If you specified another directory, replace `C:\Mapp:` with the specified installation directory.
     - Without moving the current directory, failure information is not output to the Windows event log if you execute the batch file in step 3.

   - *model-identification-number*: Use the format *<First 2 digits of firmware version><model-name><serial-number>*, where *<model-name>* is 6000 for VSP E990 and 8000 for VSP E1090.

     For example, for a VSP E990 that has the serial number 400102, the value is 936000400102.

3. Execute the following batch file:

```
eventlog.bat action monitoring-period
```

   - *action*: Specify one of the following:

     0: Stop outputting failure information

     1: Start outputting failure information

     when this parameter is omitted, 0 is set.
   - *monitoring-period*: If you specified 1 for *action*, specify the monitoring period, from 5 to 720 minutes.
   - A space is required between `eventlog.bat` and *action*.
   - A space is required between *action* and *monitoring-period*.
   - The command prompt is displayed if the command finishes without any errors.

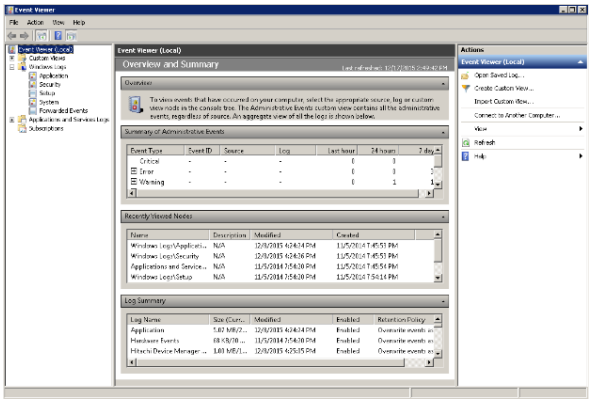
4. Close the command prompt.

Viewing the system log in the Event Viewer

You can view the Windows event log which is output to the SVP.

Procedure

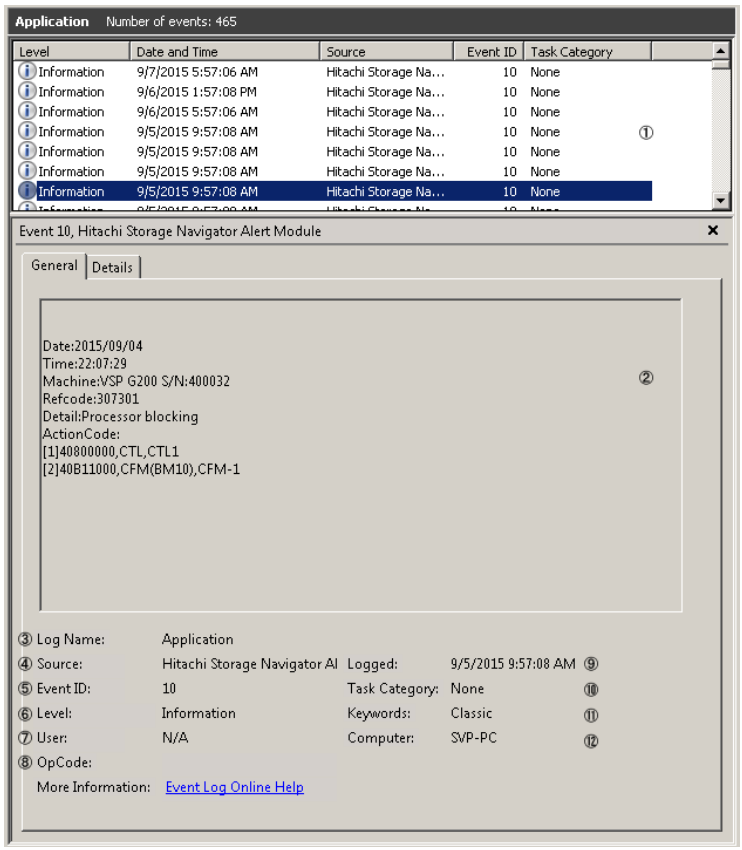
1. From the Windows start menu, click **Control Panel** > **System and Security** > **Administrative Tools** > **Event Viewer**.
2. Click **Windows Logs** > **Application** in the left pane.



Output example

The storage system delivers a report after you send failure information to the event log.

The storage system failure information looks similar to the following example.



#	Item	Description
1	Overview of the event info	Displays the overview of the event information
2	Detail of the event info	Displays the selected information Date: Date of the event occurrence Time: Time of the event occurrence Machine: Model name and serial number of the storage system Refcode: Reference code* Detail: Detailed failure information* ActionCode: Includes action code, expected failure parts, and location. A maximum of 8 failure information can be shown.
3	Log name	Displays the log type This is always displayed as "Application"

#	Item	Description
4	Source	Displays the name of the application which issued the event This is always displayed as "Hitachi Storage Navigator Alert Module"
5	Event ID	Displays the event ID This is always displayed as "10"
6	Level	Displays the event alert level ▪ Error: Acute or Serious ▪ Warning: Moderate ▪ Information: Service
7	User	This is always displayed as "N/A"
8	OpCode	This is always displayed as blank
9	Logged	Displays the date and time when the event log was registered
10	Task category	This is always displayed as "None"
11	Keywords	This is always displayed as "Classic"
12	Computer	Displays the computer name on which the event occurred
*For reference code, failure details, and alert level, see the *SIM Reference Guide*.		

Events that do not affect the operation of the storage system

Occurrence of the following events does not affect the operation of the storage system:

Note: These events can be ignored.

Event	Timing of occurrence of event
Log type: Application Source: Application Error Event ID: 1000 Level: Error	This event might occur at the following timing: ▪ When the storage management software is updated ▪ When the SVP is shut down or rebooted

Event	Timing of occurrence of event

Application on which an error occurs:
`DkcMan.exe`
Module in which an error occurs:
`ntdll.dll orjvm.dll`
Exception code: *0xc0000005*	

Log type: Application
Source: Application Error
Event ID: 1000
Level: Error
Application on which an error occurs:
`KickJava.exe`
Module in which an error occurs:
`SVPCMN32.dll`
Exception code: *0xc0000005*
	This event might occur when the service of the storage system is stopped.

Log type: Application Source: Application Error Event ID: 1000 Level: Error Application on which an error occurs: MpcL7Comm.exe Module in which an error occurs: MpcL7Mem.dll Exception code: 0xc0000005	This event might occur at the following timing: ▪ When the services on the storage system stop ▪ When the storage management software is updated ▪ When the SVP is shut down or rebooted
Log type: Application Source: Application Error Event ID: 1000 Level: Error Application on which an error occurs: RestPush_Base.exe Module in which an error occurs: jvm.dll Exception code: 0xc0000005 or 0xc000041d	This event might occur when the service of the storage system is stopped.

Chapter 8: Managing license keys

Accessing software functionality for your storage system requires a license key.

License key types and prerequisite software

License key types

The following table lists and describes the types of license keys.

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 and buy)	120 days	Not required
Emergency	For emergency use	30 days	Not required
* When you log in to Device Manager - Storage Navigator, a warning message appears if 45 days or fewer remain before the license expires.			

When you install a license key, it is automatically enabled and the timer on the license starts at that time. To preserve time on a term key license, you can disable the license without uninstalling it. When you need to use the software again, you can re-enable the license.

You can use software with licensed capacity for a term key by installing a term key and overwriting a permanent key as long as the term key is valid. If the term key expires while the system is being used and the capacity needed for the operation is insufficient, operations that you can perform are limited. In this case, a SIM that indicates the term key expiration (reference code 7ff7*xx*) is output on the Alerts tab in the Storage Systems window.

Note: When you need to enable a license key, install the prerequisite software first, and then enable the key. If you install the software after you enable the key, the software will install correctly but will be disabled.

Prerequisite software

The following table lists the software products that have prerequisite software. The prerequisite software must be installed before you can install the software product. If the prerequisite software becomes unusable during operations, the software product also becomes unusable.

Software product	Prerequisite software
Universal Replicator	TrueCopy
Remote Replication Extended	Universal Replicator
Server Priority Manager	Performance Monitor
Dynamic Tiering	Dynamic Provisioning
Thin Image	Dynamic Provisioning
Active flash	Dynamic Tiering
Dedupe and compression	Dynamic Provisioning

Using the permanent key

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

- If insufficient license capacity is installed, Not Enough License displays in the status field of the **License Keys** window, and the software application is not enabled.
- If the capacity of the usable volume exceeds the licensed capacity while the storage system is running (for example, when an LDEV is additionally installed), Grace Period displays in the status field of the **License Keys** window. You can continue to perform the same operations, but the deficient amount of license capacity must be purchased within 30 days.

Using the term key

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

- If insufficient license capacity is installed, Not Enough License or Grace Period displays in the status field of the **License Keys** window.
- You can enable or disable the term key for each software application. 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 installation date.
- The number of effective days is decremented by one day when the date changes.

  For example, if the term key is set to be enabled for 150 days during 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 software application is not used, you can prevent the unnecessary shortening 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 Keys** window, and the software application is disabled.

Using the temporary key

You can use the temporary key for trial purposes. The effective term is 120 days from the time of installation of the temporary key. The effective term is not increased even if the temporary key is reinstalled during the effective term.

If you uninstall the temporary key, even though the effective term remains, Temporary is displayed in the status field, Not Installed is displayed in the Key Type field, and the remaining days of the effective term are displayed in the Term (Days) field of the **License Keys** window.

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

Using the emergency key

You can use the emergency key if the license key cannot be purchased, or 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 software application 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 software application after using the temporary key for trial purposes, you can restore the changed configuration to the original status by temporarily enabling the software application with the emergency key.

Caution:

- If an emergency key is installed for a software application for which a permanent or term key is installed, the effective term of the license key is 30 days. However, because the emergency key can be reinstalled during the effective term, the effective term can be restored to 30 days.
- In other scenarios, the emergency key can be installed only once.

For details about software bundles for your storage system, contact customer support.

Cautions on license capacities in license-related windows

License capacities are displayed not only in license-related windows but also in the **Pools** window and the **Replication** window.

When you install or overwrite a temporary key or an emergency key for an installed software application, the license capacity before the overwrite installation is displayed as Permitted (TB) in license-related windows. However, Unlimited (license capacity for the temporary key or emergency key) is displayed as Licensed Capacity in the **Pools** window and the **Replication** window.

For example: You install a term key that has a license capacity of 5 TB for Compatible FlashCopy®, and when the term expires, you use an emergency key. In license-related windows, 5 TB is displayed in the Permitted (TB) field. However, in the **Licensed Capacity** field in a **Replication** window, Unlimited (capacity of the emergency key) is displayed.

Estimating licensed capacity

The licensed capacity is volume capacity that you are licensed to use with the software application. You must estimate the amount of capacity that you want to use with the software application before you purchase the permanent key or the term key.

Software and licensed capacity

The following table describes the three types of licensed capacity: used capacity, mounted capacity, and unlimited capacity. The type you select depends on the software application.

Caution: 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 happens, you must purchase an additional license within 30 days to increase the capacity to match the new volume size. For instructions on calculating pool capacity, see the *Provisioning Guide*.

Table 8 Licensed capacity types

Type	Description
Used capacity	The licensed capacity is calculated by using one of the following capacities: ▪ Normal volumes (volumes) ▪ External volumes mapped to the storage system ▪ Pools
Mounted capacity / usable capacity	The licensed capacity is estimated by using the capacity of all the volumes in the storage system.
Unlimited capacity	You can use the software regardless of the volume capacity.

The following table lists the software bundles and specifies the licensed capacity type for each bundle.

Table 9 Software bundle licensed capacity for VSP E series

Software bundle	Licensed capacity
Base Package	Used capacity or mounted capacity
Advanced Package	Used capacity or mounted capacity
Remote Data Protection	Used capacity or mounted capacity
Global-active device	Used capacity or mounted capacity

Calculating licensed capacity for a normal volume

A normal volume is a volume that is not blocked or protected. For OPEN-V volumes, the licensed capacity of a volume is the same as the capacity specified when creating the volume.

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
```

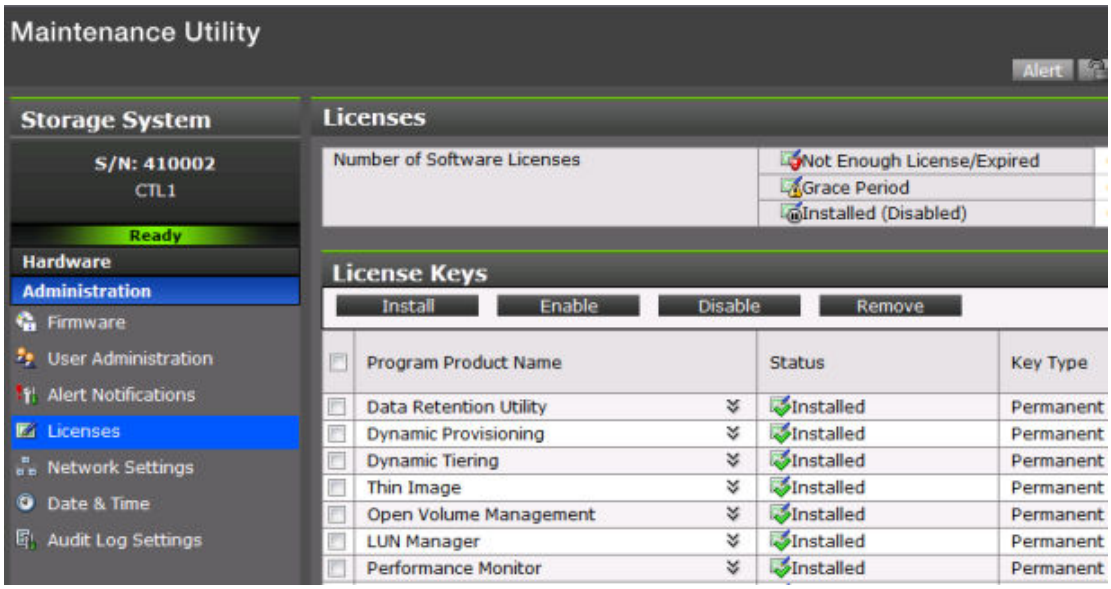
Calculating pool capacity

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, or global-active device, the license capacity of ShadowImage, TrueCopy, Universal Replicator, or global-active device is calculated by 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 *Provisioning Guide*.

Managing licenses

Use the Licenses window in the maintenance utility to install and uninstall block license keys.



Caution: 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 *Provisioning Guide*.

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

Installing a license key

Before you can use a software product such as Thin Image, you must first install the license key on your storage system. Use the following procedure to install a license key using maintenance utility.

Before you begin

- Prepare the license key code or the license key file for the software product to be registered.

Procedure

1. In the navigation bar, click (**Settings**), and then select **Licenses**.
2. In the maintenance utility, click **Install**.
3. Specify the license key code or the license key file, and register the license key.

   Tip: For more information, refer to Help in the maintenance utility.
4. In the list of license keys, confirm that the status of the software product has changed to **Installed**.

Enabling a license

You can enable a license that is in disabled status.

Before you begin

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

Procedure

1. From the **Maintenance Utility** menu, click **License Keys** to open the **License Keys** window.
2. Select the license to enable. You can select from one to all of the licenses listed in the window at the same time.
3. Click **Enable** to display the **License Keys** window.
4. Check the settings and click **Apply.**

Disabling a license

You can disable a license that is in enabled status.

Before you begin

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

Procedure

1. From the **Maintenance Utility** menu, click **License Keys** to open the **License Keys** window.
2. Select the license to disable. You can select from one to all of the licenses listed in window the at the same time.
3. Click **Disable** to display the **License Keys** window.
4. Click **Finish**.

5. Check the settings and click **Apply**.

Removing a software license

You can remove (uninstall) a software license that is in disabled status.

Note: If the key type is other than Permanent, the license key file used for installation cannot be used after the license key is uninstalled. To reinstall the license key after uninstalling it, contact customer support to reissue the license key file.

Before you begin

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

Procedure

1. In the maintenance utility **Administration** tree, click **License Keys**.
2. In the **License Keys** window, select the license to uninstall. You can select from one to all of the licenses listed in the window at the same time.
3. In the **License Keys** window, click **Uninstall Licenses**.
4. Check the settings, and then click **Apply**.

   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 then uninstall the software.

Removing a Data Retention Utility license

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

Procedure

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.
3. Change the settings so that the logical volumes are usable as S-VOLs.
4. Uninstall the Data Retention Utility.

Examples of license information

The following table provides examples of license information displayed in the **License Keys** table of the maintenance utility.

Note: When using Volume Migration, you do not need to install the license key. The function of Volume Migration is available regardless of the license key status displayed in the maintenance utility.

License key status (example)	Status	Key type	Licensed capacity	Term (Days)
Not installed	Not installed	blank	Blank	Blank
Installed with the permanent key	Installed	permanent	Permitted	-
Installed with the term key and set to Enabled	Installed	term	Permitted	Number of remaining days before expiration
Installed with the term key and set to Disabled	Installed (Disabled)	term	Permitted	-
Installed with the temporary key.	Installed	temporary	-	Number of remaining days before expiration
Installed with the emergency key.	Installed	emergency	-	Number of remaining days before expiration
A temporary key was installed, but has expired.	Expired	temporary	-	Number of remaining days before expiration
A term key or an emergency key was installed, but has expired.	Not installed	blank	Blank	Blank
Installed with the permanent key or the term key, but the licensed capacity was insufficient.	Not Enough License	permanent or term	Permitted and Used	-
Installed with the permanent or term key, and then LDEVs are added, but the license capacity was insufficient.	Grace Period	permanent or term	Permitted and Used	Number of remaining days before expiration
Installed with the temporary key, and then reinstalled with the permanent key, but the license capacity was insufficient.	Installed	temporary	Permitted and Used	Number of remaining days before expiration

License key status (example)	Status	Key type	Licensed capacity	Term (Days)
Installed with the permanent or term key, then reinstalled with the emergency key.	Installed	emergency	Permitted and Used	Number of remaining days before expiration

License key expiration

If the license key for software-A expires, the license key for software-B is also disabled if software-B requires an enabled software-A. In this scenario, Installed (Disabled) is shown for software-B in the Status column of the **License Keys** table. 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 Keys** table and manually change the status of software-B back to Installed.

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.

Chapter 9: Managing Device Manager - Storage Navigator storage system reports

Device Manager - Storage Navigator can generate a standard set of reports that provide views of various aspects of the storage system. In addition to these views, you can generate custom reports for specific areas of the system. These include a summary of the system data and configuration, ports, channel adapters, and disk adapters. You can save reports in CSV files or HTML files. Tables in the HTML version of the configuration reports are sortable.

Before making changes to a storage system, create reports of your storage system's physical configurations and logical settings. Make a similar report after the changes, and then compare the reports to verify that new settings were made as intended.

Downloading and viewing the HDvM - SN configuration reports

Use the following procedure to download configuration reports created on HDvM - SN to the management client.

Note:

- If you want to view configuration reports created with SVP firmware version earlier than 93-05-04/*xx*, use a web browser other than Microsoft Edge.
- If you use Google Chrome and the SVP firmware version is earlier than 93-05-04/*xx*, specify the Start Option `--allow-file-access-from-files`.
- If you use Google Chrome, the window used to specify the folder in which the report will be saved might not appear when downloading the report. In this case, click **Chrome Menu > Settings > Show advanced settings**, and then under **Privacy** clear the check box for **Protect you and your device from dangerous sites**.
- If you use Firefox and you want to view configuration reports created on HDvM - SN with SVP firmware version earlier than 93-05-04/*xx*, use Firefox version 67.0 or earlier.

Before you begin

- Users can view the reports that they created.
- Users who have the Storage Administrator (Initial Configuration) role can view all reports.

Procedure

1. Expand the **Storage Systems** tree, and then click **Reports**.
2. Specify the report to download.
3. Click **Download Reports**.

   Note: A character string that depends on the AIR environment is displayed in the title of the download window.
4. Specify the folder in which to save the `.tgz` file.
5. Extract the downloaded `.tgz` file.
6. Display the report.
   - For HTML reports, open the file *extracted-folder*`\html\index.html`.

     The following warning message might appear when you open the HTML file: An ActiveX control on this page might be unsafe to interact with other parts of the page. Do you want to allow this interaction? This message appears when the program embedded in the report accesses a local file. Click **Yes** to continue the operation.
   - For CSV reports, open the CSV file in the folder *extracted-folder*`\csv`.

Viewing configuration reports in the Reports window

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

Note:

- If you use Microsoft Edge, open the Settings window (click the ··· icon, and then click **Settings**), and then set **Allow sites to be reloaded in Internet Explorer mode** to disabled.
- If you use Google Chrome with an old version of SVP firmware, specify the Start Option `--allow-file-access-from-files`.
- If you use Internet Explorer, in the **Compatibility View Settings** dialog box clear the check box for **Display intranet sites in Compatibility View**, and then delete the IP address or host name of the SVP, if any, from **Websites you've added to Compatibility View**.

Procedure

1. Expand the **Storage Systems** tree, and then click **Reports**.
2. Click the name of the report to display.

   The report is displayed in the **Reports** window.
3. In the **Reports** window, click the name of the report in the list at the left, and then view the report at the right.

Creating configuration reports

You can create and store up to 20 configuration reports for each storage system. There are two types of reports:

- Configuration Reports, which are generated in HTML format
- Detail Configuration Reports, which are generated in CSV format

Before you begin

- You must have the Storage Administrator (Initial Configuration) role to create a configuration report.
- Verify that there are less than 20 reports listed on the **Reports** window. If there are already 20 reports, you must delete one or more existing reports before you can create a new report.

Procedure

1. If CCI has been used to create parity groups or LDEVs, click **File** > **Refresh All** to update the configuration information before creating a configuration report.
2. In the Device Manager - Storage Navigator main menu, click **Reports** > **Configuration Report** > **Create Configuration Report**.
3. In the **Create Configuration Report** window, specify a task name or accept the default task name (***yymmdd*-CreateConfigurationReport**).

   This task name is used as the report name in the **Reports** window.
4. In the **Selected Reports** table, select the desired report type: **Configuration Reports** (HTML) or **Detail Configuration Reports** (CSV).
5. If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status** (selected by default).
6. Click **Apply** to create the selected report.

   The create configuration report process takes approximately 10 minutes to complete.

   When the process is complete, the new report is displayed on the **Reports** window. If necessary, click **Refresh** to update the list of reports.

Deleting configuration reports

You can delete a configuration report when you no longer need it, or to make room in the **Reports** window when the number of reports is near the limit (20).

Caution: Do not perform Device Manager - Storage Navigator or CCI operations while you are deleting configuration reports. If you perform such operations, deletion of configuration reports might fail.

Before you begin

- You must have the Storage Administrator (Initial Configuration) role to delete a configuration report.

Procedure

1. Expand the **Storage Systems** tree, and then click **Reports**.
2. In the **Reports** window, select the report to delete, and then click **Delete Reports**.
3. In the **Delete Reports** window, specify a task name or accept the default task name (***yymmdd*-DeleteReports**).
4. If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status** (selected by default).
5. Click **Apply**.

Downloading dump files

Use the Dump tool to download dump files onto a management client. The downloaded dump files can be used to:

- Troubleshoot the system. Use the Dump tool to download dump files from the SVP and give it to the support personnel.
- Check system configuration. First, click File > Refresh All to update the configuration information, and then use the Dump tool to download the dump files.
- Before deleting the storage management software and the SVP software. Collect the dump files of the SVP system information.

Types of dump tools:

- Normal Dump tool (file name: `Dump_Normal.bat`): Use the Normal Dump tool to obtain the `Dump_Normal.bat` file. The `Dump_Normal.bat` file includes all information about the SVP and the minimum information about the storage system. Select this when you have a less serious problem such as incorrect display.
- Detail Dump tool (file name: `Dump_Detail.bat`): Use the Detail Dump tool to obtain the `Dump_Detail.bat` file. The `Dump_Detail.bat` file includes all information about the storage system in addition to the Normal Dump data. Select this when Device Manager - Storage Navigator has a serious problem (for example, HDvM - SN does not start) or when you need to determine if the storage system has a problem.
- Initial Analysis Dump tool (file name: `Dump_MoreRapid.bat`): Use the Initial Analysis Dump tool to obtain the `Dump_MoreRapid.bat` file. The `Dump_MoreRapid.bat` file includes the minimum dump data required to perform the initial dump analysis of SSBs and SIMs. Select this when you must start the initial analysis of the problem as soon as possible if a failure occurs. This dump tool is available for SVP firmware version 93-06-21-*xx* or later.

Before you begin

- You must be logged into the SVP.
- HDvM - SN must be running.
- The configuration information must be refreshed by selecting File > Refresh All in HDvM - SN.
- All other users (including the SVP user) must stop using the Dump tool.
- Stop all maintenance operations.
- Dump tools from other storage systems must not be used during the process.
- The installation directory of Storage Navigator must be excluded from the real time virus scan targets by the virus detection program.

Note:

If the error is in regards to HDvM - SN starting up, collect information about the SVP using the Dump tool, without HDvM - SN running.

Procedure

1. Close all HDvM - SN sessions on the SVP.
2. Open a Windows command prompt with administrator permissions.
3. Move the current directory to the folder where the tool is available. (For example: `<SVP-root-directory>\DKC200\mp\pc`).
4. Specify the output destination of the dump file and execute `Dump_Detail.bat`, `Dump_Normal.bat`, or `Dump_MoreRapid.bat`.

   For example, if you are storing the result of `Dump_Detail.bat` to `C:\Result_832000400001`, enter the following:

```
C:\MAPP\wk\832000400001\DKC200\mp\pc>Dump_Detail.bat C:\Result_832000400001
```

Note:

- A space is required between `Dump_Detail.bat` and `C:\Result`.
- The dump file name is `hdcp.tgz`. To manage dump files by storage systems, we recommend adding a serial number to the output folder name. For example, if the serial number is 832000400001, the folder name should be `C:\Result_832000400001`.
- A folder under the network drive cannot be specified as the output destination.
- When the tool is being executed, `Executing` is displayed in the command prompt. When the execution is completed, the following is displayed:

  ```
  zSv_AutoDump.exe is completed.
  ```

  zSv_AutoDump.exe is completed." might not be displayed even after the completion of the tool execution due to the heavy load on the SVP or other cause. If it is not displayed even after 20 minutes, check whether a dump file is output in the output folder for the dump file. When a dump file is output, see the date and time of the file update to confirm that the file is created after 20 minutes have passed since the start time of execution of the dump tool. When no dump file is output, close the command prompt and execute the dump tool again.

  Note: If the execution fails, `zSv_AutoDump.exe is failed` is displayed.
- You cannot specify the folders under the network drive as the output folder.
- The dump file capacity might become approximately 3 GB depending on the usage of the storage system.
- If "zSv_AutoDump.exe is failed." is displayed when you run the dump tool, the installation directory of HDvM - SN might not be excluded from the real-time virus scan target in the virus detection program. Exclude the installation directory from the virus scan target.

5. A completion message box displays. Press any key to acknowledge the message and close the message box.

   `hdcp.tgz`: This is the dump file. Give this file to the maintenance personnel. If you save too many dump files in the SVP storage, space might not be available. Therefore, move the dump file outside of SVP storage.

   `zSv_AutoDump.log`: This is the log file of the dump tool. If the dump file is not output, give this log file to the maintenance personnel. If the dump file is output, delete the log file.

   `DumpResult.txt`: This is the collection results file. The results are displayed in the following catagories:

DKC dump
Collection result of the DKC dump data

Dump of GUM of CTRL1
Collection result of the GUM (CTL1) dump data

Dump of GUM of CTRL2
Collection result of the GUM (CTL2) dump data

exist is displayed if the collection was successful. *not exist* is displayed if the collection has failed.

6. Close the Windows command prompt.

Collecting dump files manually

You can collect dump files manually if the dump tool is unavailable or is causing an error in the dump files.

Note:

- `installDir` indicates the installation directory of the storage management software and the SVP software (for example, `C:\Mapp`).
- `%USERPROFILE%` indicates the installation login user of the SVP (for example, `C:\Users\<user name>`).
- `%WINDIR%` indicates the Windows folder in the system drive (for example, `C:\Windows`).
- [Storage system number]□□□(Example) When the storage system number is 832000400001, the folder name is as follows:. `<installDir>\wk\832000400001\DKC200\mp\pc\*.trc`
- Note that some files do not exist depending on the operating environment.

Files to collect manually:

- <installDir>¥wk¥supervisor¥dkcman¥log¥*.*
- installDir>¥wk¥supervisor¥dkcman¥cnf¥*.*
- <installDir>¥wk¥supervisor¥rmiserver¥log¥*.*
- <installDir>¥wk¥supervisor¥rmiserver¥cnf¥*.*
- <installDir>¥wk¥supervisor¥sdlist¥log¥*.*
- <installDir>¥wk¥supervisor¥mappiniset¥logs¥MappIniSet¥*.*
- <installDir>¥wk¥supervisor¥mappiniset¥mpprt¥cnf
- <installDir>¥wk¥supervisor¥assist¥log¥*.*
- <installDir>¥wk¥supervisor¥assist¥cfg¥*.*
- <installDir>¥wk¥supervisor¥assist¥dat¥*.*
- <installDir>¥wk¥supervisor¥assist¥history¥*.*
- <installDir>¥wk¥supervisor¥comweb¥logs¥*.*
- <installDir>¥wk¥supervisor¥microsetup¥log¥*.*
- <installDir>¥wk¥supervisor¥portmanager¥cnf¥*.*
- <installDir>¥wk¥supervisor¥portmanager¥logs¥PortManager¥*.*
- <installDir>¥wk¥supervisor¥restapi¥data
- <installDir>¥wk¥supervisor¥restapi¥logs
- <installDir>¥wk¥supervisor¥restapi¥build.json
- <installDir>¥wk¥supervisor¥restapi¥version.json
- <installDir>¥wk¥supervisor¥system¥log¥*.log
- <installDir>¥wk¥[Storage system number]¥DKC200¥mp¥pc¥*.trc
- <installDir>¥wk¥[Storage system number]¥DKC200¥mp¥pc¥*.dmp
- <installDir>¥wk¥[Storage system number]¥DKC200¥mp¥pc¥*.dbg
- <installDir>¥wk¥[Storage system number]¥DKC200¥mp¥pc¥*.dmb
- <installDir>¥wk¥[Storage system number]¥DKC200¥mp¥pc¥*.ini
- <installDir>¥wk¥[Storage system number]¥DKC200¥mp¥pc¥*.inf
- <installDir>¥wk¥[Storage system number]¥DKC200¥san¥SN2¥SN2Files ¥logs¥*.*
- <installDir>¥wk¥[Storage system number]¥DKC200¥san¥SN2¥SN2¥logs ¥*.*
- <installDir>¥wk¥[Storage system number]¥DKC200¥san¥cgi-bin¥utility ¥log¥*.*
- <installDir>¥wk¥[Storage system number]¥DKC200¥others¥commdata¥*.*
- <installDir>¥wk¥[Storage system number]¥DKC200¥config¥*.cfg
- ¥wk¥[Storage system number]¥SMI\logs*.*
- <installDir>¥OSS¥apache¥logs¥*.log

- `<installDir>¥OSS¥apache¥logs¥ssl¥*.log`
- `<installDir>¥OSS¥jetty¥logs¥*.log`
- `%USERPROFILE%¥AppData¥LocalLow¥Sun¥Java¥Deployment¥log`
- `%WINDIR%¥system32¥config¥SysEvent.Evt`
- `%WINDIR%¥system32¥config¥SecEvent.Evt`
- `%WINDIR%¥system32¥config¥AppEvent.Evt`
- `%WINDIR%¥minidump¥*.dmp`
- `%WINDIR%¥System32¥Winevt¥Logs¥Application.evtx`
- `%WINDIR%¥System32¥Winevt¥Logs¥Security.evtx`
- `%WINDIR%¥System32¥Winevt¥Logs¥System.evtx`
- `%WINDIR%¥system32¥drivers¥etc¥HOSTS*`
- `%WINDIR%¥system32¥drivers¥etc¥services*`
- `%WINDIR%¥minidump¥*.`

Collecting performance information of the SVP

If the following performance problems occur in the SVP, collect the performance information of the SVP and dumps using the performance information collection tool, and then send them to the maintenance personnel:

- Slow operation of the SVP
- High CPU usage rate of the SVP
- Slow operation of the Storage Device List or the Device Manager - Storage Navigator

Caution: The tool used in this procedure collects the performance information of the SVP. This tool is installed in the directories corresponding to the serial numbers of all storage systems registered in the Storage Device List. Although this tool does not collect performance information of individual storage systems, it can collect dump files for the storage system corresponding to the directory used to run the tool. Therefore, for the storage systems other than that storage system, see Downloading dump files (on page 212) and Collecting dump files manually (on page 215) to collect the dump files, and then pass them to maintenance personnel.

Use the following procedure to collect performance information of the SVP by using the performance information collection tool. Collection of performance information takes about 30 minutes, and then the dump files are automatically collected.

Before you begin

- Any performance problem of the SVP must be occurring.
- You must be logged into the SVP.
- Device Manager - Storage Navigator must be running.

- All other users (including the SVP user) must stop using the performance information collection tool.
- All maintenance operations must be stopped.
- Performance information collection tools from other storage systems must not be used during the process.
- The installation directory of the Device Manager - Storage Navigator must be excluded from the real time virus scan targets by the virus detection program.

For the virus detection program settings, see Preventing errors while using virus detection programs on the SVP (on page 127).

Note: If the error is in regards to Device Manager - Storage Navigator starting up, collect information about the SVP using the performance information collection tool without Device Manager - Storage Navigator running. If some tools are running, performance of the SVP might be further degraded.

Procedure

1. On the SVP, open a command prompt window with administrator permissions.
2. Move the current directory to the directory in which the tools are installed.

   For example, if the model identification number of the storage system is 932000400001, the directory in which the tool is installed is `C:\Mapp\wk\932000400001\DKC200\mp\pc`. In this case, enter the following:

   ```
   cd /d C:\Mapp\wk\932000400001\DKC200\mp\pc
   ```

   Note: `C:\MAPP` indicates the installation directory of the storage management software and the SVP software. When the installation directory other than `C:\Mapp` was specified, replace `C:\Mapp` with the specified installation directory.

3. Run the performance information collection tool `GetSVPPerfInfo.bat` by specifying the output folder of the performance information and dump files. In the command prompt, enter the following:

   ```
   GetSVPInfo.bat output-directory
   ```

   For example, when you want to output the performance information and dump files of the SVP to `C:\Result_932000400001`, enter the following command:

   ```
   GetSVPPerfInfo.bat C:\Result_932000400001
   ```

   If you do not specify output directory, the performance information and dump files are output to the following folders:

   ```
   C:\Mapp\wk\932000400001\DKC200\tmp\PerfLog
      C:\Mapp\wk\932000400001\DKC200\tmp\PerfLog
   ```

   In this example, `932000400001` is the model identification number of the registered storage system.

Note:

- When you enter the command, a space is required between the `.bat` file of the tool and the output directory.
- A directory under the network drive cannot be specified as the output destination.
- Do not click or close the command prompt window while running the tool.
- When the tool is being executed, `Executing…` is displayed in the command prompt.
- The tool automatically starts collecting dumps after collection of the performance information finishes.
- Both performance information and system information of the SVP are collected. Do not click **Cancel** on the dialog box that opens while system information is collected. The dialog box closes automatically after collection of system information finishes.
- When all processes are complete, `SVP Performance Information tool is completed.` is displayed in the command prompt.

4. Check the dump files that were output.

   The following files are output:

   - `CounterResult_`*`YYYYMMDDhhmmss`*`.blg` : Windows performance monitor log
   - `ProcessList_`*`YYYYMMDDhhmmss`*`.csv` : Information of the processes running on the SVP
   - `Sysinfo_`*`YYYYMMDDhhmmss`*`.txt` : System information of the SVP
   - `hdcp.tgz`
   - `zSv_AutoDump.log`
   - `DumpResult.txt`

5. Close the command prompt.
6. An OS failure might cause a failure of collecting dumps. If the output result of the tool in step 4 is not output, collect the dump files manually.
7. Send all of the files that were output to the maintenance personnel.

Chapter 10: Troubleshooting

Troubleshooting for Device Manager - Storage Navigator involves identifying the cause of the error condition and resolving the problem.

General troubleshooting

If you have a problem with Device Manager - Storage Navigator, check the following items. If you cannot resolve an error condition, contact customer support.

- Check the cabling and the LAN. Verify that both the management client and LAN cabling are firmly attached, and that the LAN is operating properly.
- Close any programs on the management client that are not responding. If necessary, reboot the management client and restart a Device Manager - Storage Navigator web client session.
- Clear the Java and web browser caches to solve the problem. To clear the Java cache, click Delete the temporary files in the **General** dialog box of the Java Control Panel.
- Check for other general error conditions. For a complete list of Device Manager - Storage Navigator error codes, see the *Hitachi Device Manager - Storage Navigator Messages*.
- Check the alert icon. Confirm the severity level of the storage system alert by clicking Alert in the Device Manager - Storage Navigator main window.

Collecting network trace

If an abnormal event occurs on a network connecting to the SVP, you can use the network trace collection tool to capture the packets to and from the SVP. The network trace collection tool is supported by the following SVP firmware versions:

- 93-06-22 or later
- 93-06-02 to 93-06-20
- 93-05-05 to 93-05-20

Caution:

- When you are asked by maintenance personnel to collect network trace, you can agree with collecting network trace and sending the collected information to maintenance personnel. If you do not agree with this, contact maintenance personnel.

  Note that information about all packets to and from the SVP through the network is collected while this tool is running. Be careful when handling collected information.
- While the network trace collection tool is running, the network interface card (NIC) link on the SVP might be momentarily down. There is no problem with this link-down event because it is caused by the `netsh trace` command (Windows standard command) that is used internally by the tool.
- Do not perform other maintenance operations while using the network trace collection tool.

Before you begin

- You must be able to reproduce the abnormal event on the network while the network trace collection tool is running. Make sure that you can reproduce the event on the SVP before running the tool. If you are not able to reproduce the event, contact maintenance personnel.
- You must have 8 GB of capacity for storing the network trace and dump files that are output by the dump tool.

Procedure

1. On the SVP, start a Windows command prompt as Administrator.
2. Move the current directory to the folder where the tool is available.

   Example: *<SVP-root-directory>*`\DKC200\mp\pc`
3. Run the network trace collection tool (`GetNetTrace.bat`) and specify the output destination of the network trace and dump files.

   For example, to store the network trace and dump files to `C:\Result_934000600001`, enter the following command to run the tool:

   ```
   GetNetTrace.bat C:\Result_934000600001
   ```

Note:

- A space is required between `GetNetTrace.bat` and the output destination.
- You cannot specify a folder under a network drive as the output destination.
- Do not click on or close the command prompt window while the tool is running. If you accidentally close the window, restart the SVP.
- While the tool is running, `Executing...` is displayed in the command prompt.

When the message `Do you want to stop the network tracing session? (Y) :` is displayed, do not respond to this message until after you have reproduced the network event.

4. Reproduce the network event.
5. After the network event has been reproduced, stop the network tracing session by entering `Y` (uppercase) in response to the message `Do you want to stop the network tracing session?(Y):`.

   Caution: You must stop the network tracing session soon after the network event has been reproduced. If the tool remains running for one hour or more after the network event was reproduced, the network trace might be lost.

   When you stop the network tracing session, the dump tool automatically starts, collects the dump files, and stops. When the dump tool stops, `Network Trace tool END.` is displayed in the command prompt.
6. Confirm that the following files were output to the specified destination folder:
   - `SVP_NetTrace.etl`: Network trace log
   - `SVP_NetTrace.cab`: Log for related information regarding network trace log. This file might not be output.
   - `hdcp.tgz`: Dump file
   - `zSv_AutoDump.log`: Log file of the dump tool
   - `DumpResult.txt`: Collection results file

   In some cases the dump tool might fail to collect files due to an OS problem. If these result files were not output, you can collect the dump files manually. For details, see Collecting dump files manually (on page 215).
7. Close the command prompt.
8. Send all files output by the tool to maintenance personnel.

Displaying alerts

You can check if the failure (SIM) is reported or not in the storage system by checking the alert in the Device Manager - Storage Navigator main window.

Procedure

1. In the Device Manager - Storage Navigator main window, click **Alert**. The **Alerts** window opens.
2. On the **Alerts** tab, click **DKC** or **GUM (CTL1)**, or **GUM (CTL2)** to check alert information.
3. Click the alert ID link to check the detailed information for each alert.

   The error information displays in the **Alert Detail** window.

Login errors

The following table lists login errors and provides recommended actions for each error condition.

Error condition	Probable cause / Recommended action
Failed to login is displayed.	Check that the user name and password are correct. If you forget your password, log in with the Security Administrator (View & Modify) and set a new password. To confirm that the SVP and the storage system can communicate normally, check the following: ▪ LAN cabling is correct and connections are in place. ▪ IP address of SVP and IP address of GUM are in the same network. ▪ There is no duplicate IP address in the network to which SVP and GUM belong. ▪ GUM is pingable from SVP. When you are using an external authentication server such as LDAP, check the following: ▪ The authentication server has been started. ▪ The authentication server can be accessed from the SVP via the network ▪ The user account has been established on the authentication server ▪ The connection information for the authentication server that has set on the SVP is correct. ▪ The authentication server certificate that is used in Connecting authentication and authorization servers (on page 104) meets the requirements and the prerequisites for the certificate. If this problem occurs again, verify the requirements for the authentication server and the certificate (see Setting up authentication and authorization with Device Manager - Storage Navigator (on page 83)).

Error condition	Probable cause / Recommended action
	Check whether the user account is registered. If the user account is not registered, perform one of the following operations: ▪ Reboot the GUM of CTL2. ▪ Restore the user account. ▪ Register the user account again. If the symptom recurs even after you correct the above settings, use the dump tool to collect HDvM - SN normal dump files to some recording media and then contact customer support.
The HDvM - SN window is not displayed.	▪ Make sure the URL of the desired SVP is registered to the Trusted sites section of the Internet Options dialog box ▪ Make sure that the browser uses TLS 1.2.
HDvM - SN does not start even with repeated attempts.	Close all the web browser windows and then clear the web browser cache. Use the Task Manager to check for "hung" or duplicate processes.
A network error occurred when you logged in to HDvM - SN.	Close all dialog boxes and log in to the HDvM - SN again. If the same error occurs, check the network environment.
Internet Explorer cannot display the webpage is displayed.	▪ Ensure that the network device is enabled. ▪ Ensure that the proxy server settings are correct if you use proxy for the network connection.
An error occurred during SVP processing is displayed.	▪ If the web browser is set up to use a proxy server, disable the proxy server. ▪ If a proxy server is not used in the web browser, wait a few minutes, update the screen, and log in again.
The login to a storage system from the Hitachi Command Suite server fails.	If you change your password for a storage system, you need to change the information registered in Hitachi Command Suite. For details, see the section describing how to change storage system settings in the *Hitachi Command Suite User Guide*.

Error condition	Probable cause / Recommended action
	If Hitachi Command Suite does not support these four cipher suites, enable RSA key exchange on the SVP: ▪ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 Check the number of tiers of the certificate chain to be used in Hitachi Command Suite. The maximum number supported is 5 tiers. Make sure to use a certificate in a certificate chain with no more than 5 tiers.
The window in gray appears and the login dialog box is not displayed during startup of HDvM - SN that can run in the Adobe AIR environment.	Enable the TLS settings of Internet Options for the web browser.
When starting HDvM - SN running in an Adobe AIR environment, the display goes gray and the login window does not open.	Make sure that the TLS setting is enabled for the browser.
The login window does not open for HDvM - SN running on a web browser.	Internet Explorer 11 might be used with Adobe Flash Player whose version is 10.0 or earlier. Confirm the version of Adobe Flash Player. If you use Microsoft Edge, install Storage Device Launcher and run HDvM - SN in an Adobe AIR environment because Microsoft Edge does not support Adobe Flash Player.

No-response errors

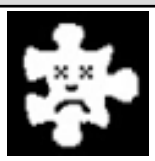
The following table lists no-response errors in Device Manager - Storage Navigator and provides the probable cause and recommended actions for each error.

Error condition	Probable cause / Recommended action
The error 20121-107022 occurs when using Device Manager - Storage Navigator (HDvM - SN).	An unsupported locale might be set for the SVP. Make sure that the correct locale is set for the SVP. To set the locale, see the Hardware Reference Guide for your storage system.
The following error occurs when using Device Manager - Storage Navigator: ▪ 20121-107024	The SVP web server might have been restarted. Close HDvM - SN, wait 10 minutes, and then restart HDvM - SN.
Error (20121-107096) occurs repeatedly while you are using Device Manager - Storage Navigator.	A timeout error may have occurred in Adobe AIR. Close the HDvM - SN window. Click X in the corner of the browser window or click the window and press **Alt**+**F4**.
The following errors occur when using Device Manager - Storage Navigator: ▪ 20121-107024 ▪ 20121-107025 ▪ 20121-107096 ▪ 20121-107097	This error may occur if the load to the management client is high, or if you start multiple instances of HDvM - SN by using multiple tabs in a tab browser or multiple browsers. Close the other applications which cause the high load, or make sure to start only one HDvM - SN
▪ The application errors 20020-108000 and 10-6027 occur when you click the Device Manager - Storage Navigator menu. ▪ The application error 10-6027 occurs when you click the Device Manager - Storage Navigator menu.	Retry the operations on HDvM - SN. If the problem occurs again, take the following actions: ▪ The port number might not be reassigned after restoring the SVP configuration files. Retry the assignment of the port number. ▪ Java might have not started because Java takes a while to start from the management client. Close all other applications being used, and then retry the operations on HDvM - SN. ▪ The version of HDvM - SN recognized by the management client might not match the version installed on the SVP. Close all the browser windows and then clear the browser cache. ▪ The management client might have entered standby or hibernate mode. Restart HDvM - SN. ▪ 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 the browser cache, contact your network administrator.

Error condition	Probable cause / Recommended action
	▪ Java content might be disabled in the web browser using the JRE 7.0 Update 10 or later. Enable Java content in the web browser and then restart the browser. ▪ The JRE used by the secondary window might not support the protocols or cipher suites used in TLS communications. Check whether your JRE supports the protocols and cipher suites used in TLS communications. If not, install a new JRE that supports these protocols and cipher suites. If none of the above actions solves the problem, save the HDvM - SN dump file and send it to customer support. Then restart the web browser.
Device Manager - Storage Navigator does not respond. Device Manager - Storage Navigator may hang in the following cases: ▪ The HDvM - SN 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. ▪ 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. ▪ The login window does not appear and the white screen continues. ▪ You clicked the cross mark  or Close, however the window cannot be closed.	Close the web browser and reopen it. When using the HDvM - SN secondary window, exit HDvM - SN by pressing **Ctrl**+**Alt**+**Shift**+**D** all at once. If you close the web browser but you cannot exit HDvM - SN, reboot the management client or restart HDvM - SN after forcibly closing HDvM - SN as follows: ▪ In Windows: Exit the web browser, and then use the Task Manager to terminate `msedge.exe` (for Microsoft Edge), `iexplorer.exe` (for Internet Explorer), or `chrome.exe` (for Google Chrome). ▪ In UNIX: Exit the web browser, and then terminate firefox-bin with the kill command. ▪ If the problem continues, restart the SVP.
A network error occurred. There is no response to any operation even after 30 minutes.	Restart the management client. An operation can take over 30 minutes depending on the use condition. For example, when several HDvM - SN web clients are running, an operation might take a long time.
An internal error occurs, or a web browser ended abnormally.	Close all dialog boxes, and then log in to HDvM - SN again. If the same error occurs, restart the management client.

Error condition	Probable cause / Recommended action
During a Device Manager - Storage Navigator operation, the web browser suddenly disappears.	Restart the management client.
An error (1-4011) occurs while you are using Device Manager - Storage Navigator.	The clock time of the management client may have been changed. Log in to HDvM - SN again.
The management client reboots on its own.	Restart the management client.
A Device Manager - 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 HDvM - SN.
A Device Manager - Storage Navigator window is incorrectly closed 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 HDvM - SN. If you cannot log in, wait for one minute and try again.
When you log out of Device Manager - Storage Navigator, a Microsoft Edge or Internet Explorer error occurs.	The probable causes are as follows: ▪ Microsoft Edge or Internet Explorer has not been updated. Action: Install the latest updates. ▪ Microsoft Edge or Internet Explorer may be configured incorrectly. Action: Re-install Microsoft Edge or Internet Explorer.
When you click File > Refresh All or Refresh in the Device Manager - Storage Navigator main window, the percentage of progress remains 99%.	The probable causes are as follows: ▪ Another application such as Command Control Interface may be changing configuration. The window will be updated shortly after the configuration change ends. ▪ Volume Migration operations, Quick Restore operations or Thin Image operations may be in progress. The window will be updated shortly after the operations end.

Error condition	Probable cause / Recommended action
One of the following errors occurred during a Device Manager - Storage Navigator operation in the main window ▪ 20123-107027 ▪ 20123-108004 ▪ 00002-058578 ▪ 00003-002003 ▪ xxxxx-065740 ▪ xxxxx-068800 where xxxxx indicates any code.	▪ 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 data may not be matched if a communication error occurs between the storage system and SVP. Wait a few minutes and then click File > Refresh All to reload the configuration information. Then run HDvM - SN again. If a configuration change operation was performed, check that all the configuration changes that caused the error were applied, and then set the settings that were not applied again. When using Encryption License Key, do the following: ▪ If a failure (00002-058578) occurs when you set the Encryption Environment for the first time from the **Edit Encryption Environmental Settings** window, do the following: **1.** Wait a few minutes and then click File > Refresh All to reload the configuration information. **2.** Initialize the Encryption Environment Settings. **3.** Set the Encryption Environment again. ▪ If a failure (00002-058578) occurs when you set the Encryption Environment again from the **Edit Encryption Environmental Settings** window, do the following: **1.** Wait a few minutes and then click File > Refresh All to reload the configuration information. **2.** Set the Encryption Environment again.
The Device Manager - Storage Navigator window turns white and the icon shown below displays in the center of the web browser when you use Device Manager - Storage Navigator. Icon in Internet Explorer: 	Restart the management client.

Error condition	Probable cause / Recommended action
Icon in Google Chrome: 	
Operations cannot be performed due to a problem with the Device Manager - Storage Navigator main window. For example, tables are not displayed correctly or some buttons are not displayed. Logging out and back in does not solve the problem.	The HDvM - SN window setting information may have been saved with an incorrect value. Click Settings > Environmental Settings > Reset View to Settings in the HDvM - SN main window to clear the window setting information. Then click any button in the HDvM - SN window and check that it operates correctly. You do not need to log out and back in.
Device Manager - Storage Navigator closes automatically when operating the IPv6 address setting from Device Manager - Storage Navigator.	When the symptom occurs, the resource group status remains locked. Open the **Resource Lock Properties** window and release the locked resource group caused by the symptom. Suspend other operations when releasing the resource group, as other resource groups are also released the lock.
The error 20122-208003 occurred when using HDvM - SN.	A problem might have occurred with the storage system connection, or user account information which is used for the storage system connection might have changed. Configure the user account information specified for the registered system of the **Storage Device List** window. For details, see the Hardware Reference Guide for your storage system.
A pop-up block message appears when Microsoft Edge is used.	In Microsoft Edge settings, pop-ups might be blocked. Change the settings in Edge to allow pop-ups for the SVP.
An error message "Error: 290-6125 A permission error occurred." is displayed during login on the Tool Panel dialog box, and the login cannot be performed.	Restart your web browser. If this problem occurs again, verify that the cookie settings for your web browser are enabled. In Internet Explorer (**Internet Options > Privacy tab > Advanced**), verify the following settings: ▪ **Accept** is selected for First-party Cookies. ▪ **Accept** is selected for Third-party Cookies. ▪ **Always allow session cookies** is checked.

Error condition	Probable cause / Recommended action
	In Microsoft Edge (**Settings > Cookies and site permissions > Cookies and data stored**), verify that **Allow sites to save and read cookie data (recommended)** is turned on to unblock cookies.
A security warning repeatedly appears while you perform HDvM - SN operations.	The SVP certificate might have been updated. Log out from HDvM - SN. The security warning window may not respond for a while, but it will be automatically closed in about two minutes. Log in to HDvM - SN again.
The window displaying "Please wait ... Storage Navigator is loading" remains open and you cannot log in.	The IP address of the SVP might have changed. To update the IP address in the Storage Device List, click SVP IP Address (upper right corner of **Storage Device List** window), click Change SVP IP Address, and enter the IP address. Then click Start Service.

Incorrect display errors

The following table lists incorrect display errors and provides the probable cause and recommended action for each error condition.

Error condition	Probable cause / Recommended action
A question mark or icon is displayed in a table or other area of the window.	▪ When a question mark appears in the **Tier Properties** window, see the topic describing this window in the *Provisioning Guide*. If the problem persists, contact customer support. ▪ When a 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 persists, contact customer support. ▪ If a question mark or icon appears in another window, update the window. If the question mark or icon remains after you update the window, contact customer support.
The product name, vendor name, and function name displayed in HDvM - SN are incorrect.	Contact customer support.

Error condition	Probable cause / Recommended action
A part of the HDvM - SN window is not displayed.	You might be using the zoom-in and zoom-out function of the web browser. Do not use this web browser function when using HDvM - SN.
The display on HDvM - SN's main window is not updated to the latest information. "Last Updated" on HDvM - SN's main window is not updated.	Volume Migration operations, Quick Restore operations, or Thin Image operations might be in progress. The window will be updated shortly after the operations end.
The Maintenance Utility window is not displayed.	▪ Make sure that the browser uses TLS 1.2. ▪ If the storage system is registered by using the host name, you need Windows setting on the SVP. Add, to the DNS suffix, the domain names of the hosts that are set for CTL1 and CTL2.
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: ▪ Increase the resolution so that more areas of the table can be shown. ▪ Use the zoom in or zoom out function of your browser to adjust the viewing area. **Note:** Text might become too small. If you still cannot solve the problem, contact customer support.
The Maintenance Utility window is displayed incorrectly in Internet Explorer. ▪ A specific window is not displayed. ▪ No response if you click the button.	Set the **Maintenance Utility** window out of Compatibility View by first confirming "Compatibility View" in the Address bar of Internet Explorer, and then setting Compatibility View to OFF. If "Compatibility View" is not displayed (prior to IE11): **1.** Select Tool > Compatible View Settings in Internet Explorer. **2.** Uncheck the Display intranet sites in Compatibility View and Display all websites in Compatibility View checkboxes. **3.** Click Close.
The message "Unable to launch the application" appears on the secondary window, then operation ends abnormally.	Perform the following: **1.** If the current JRE (Client) version is JRE 7, update to JRE 8 or later. **2.** Confirm that Use TLS 1.2 for Java is enabled. If Use TLS 1.2 is disabled, change the TLS settings for Java to enabled.

Error condition	Probable cause / Recommended action
A pop-up block message appears when Microsoft Edge is used.	In Microsoft Edge settings, pop-ups might be blocked. Change the settings in Microsoft Edge on the SVP to allow pop-ups.

UNIX operation errors

The following table lists UNIX operation errors:

Error condition	Probable cause / Recommended action

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 Device Manager - Storage Navigator on the Japanese version of Firefox, log out of Device Manager - Storage Navigator, and then log in to Device Manager - Storage Navigator again. Enter the following commands using the X Server Emulator.
	▪ B Shell:
	`LANG=C`
	`export LANG`
	▪ C Shell:
	`setenv LANG C`

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

Storage Device Launcher errors

Error condition	Probable cause / Recommended action
Installation of Storage Device Launcher failed with error message “CPU Address Width”.	The storage management software and SVP software installed on the SVP support only English and Japanese. Set the locale of the HDvM - SN management client to either English or Japanese.

Error condition	Probable cause / Recommended action
▪ Storage Device Launcher cannot start. Or a message appears asking if you have entered the name correctly because `..\..\bundle\jre_win\bin\javaw` cannot be found. ▪ HDvM - SN that can run in the Adobe AIR environment cannot start from a web browser.	After installing Storage Device Launcher, the `WCLauncher_win` folder used for the installation might have been deleted or moved. If the `WCLauncher_win` folder remains, restore it to the location where it was installed. Or, reinstall Storage Device Launcher in the new location to which it has been moved. If you cannot find the `WCLauncher_win` folder, download the setup file and reinstall Storage Device Launcher. For details, see Installing Storage Device Launcher on the management client (on page 29). Check the number of tiers of the certificate chain that is used in Hitachi Command Suite. The maximum number supported is 5 tiers for VSP E series. Make sure to use a certificate in the certificate chain with no more than 5 tiers.

HDvM - SN secondary window blocked

If you cannot open the HDvM - SN secondary window on a Windows PC, the default browser might not be set to one of the supported browsers (Edge, Google Chrome, Internet Explorer). Set the default browser to one of the supported browsers, and then retry the operation.

If Java 7 Update 55 or later or Java 8 Update 5 or later is installed on the management client, execution of the Device Manager - Storage Navigator secondary window application might be blocked. In this case, use the following procedure to change the Java security settings.

Procedure

1. Check the version and update information of Java installed in your management client. 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 **Exception Site List**, specify the URL of the SVP as follows, and then click **Add**.

   `http://`*`IP-address-of-SVP`* or `https://`*`IP-address-of-SVP`*
7. Click **OK**.
8. Select the **Advanced** tab.
9. For **Perform signed code certificate revocation checks on**, select **Do not check (not recommended)**, and then click **OK**.
10. Close the **Control Panel**.

Troubleshooting secondary windows

The following tables list error conditions in the Device Manager - Storage Navigator (HDvM - SN) secondary window and provide recommended actions to resolve the errors.

- Java application errors (on page 236)
- No response errors (on page 242)
- Incorrect display errors (on page 244)
- Other secondary window errors (on page 246)

Java application errors

Error condition	Probable cause / recommended action
When you click the HDvM - SN 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 HDvM - SN. 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 Microsoft Edge or Internet Explorer, you can open the window by clicking the HDvM - SN 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. If none of the above actions solve the problem, reinstall the JRE.
When you click the HDvM - SN 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 management client, 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.
When you click the HDvM - SN menu, a message appears asking you to save a `.jnlp` file.	Perform the following to save the encrypted page:

Error condition	Probable cause / recommended action
	1. Open the Windows **Internet Options** window (**Control Panel** > **Network and Internet** > **Internet Options**). 2. In the Internet Properties dialog box, select the **Advanced** tab, clear the check box for **Do not save encrypted pages to disk**, and then click OK.
When you click the HDvM - SN menu, a message regarding the web browser (for example, "How do you want to open this website?") appears. One minute later, the application error (20020-108000) occurs.	The web browser for HDvM - SN operations might not be set as the default browser on the HDvM - SN web client. Set the default browser to one of the supported browsers.
▪ The application errors (20020-108000 and 10-6027) occur when you click the HDvM - SN menu. ▪ The application error (10-6027) occurs and HDvM - SN terminates when you click the HDvM - SN menu.	If the problem continues after you perform the operation multiple times, see the probable causes listed below. For Windows: Exit all applications using Java, and then terminate the javaw.exe and javaws.exe applications through Task Manager. ▪ Java on the HDvM - SN web client might have failed to start due to timeout. Close all other applications and perform the HDvM - SN operation again. ▪ The version of HDvM - SN recognized by the management client might not match the version installed on the SVP. Close all the windows of your web browser and then clear the Java and web browser cache. ▪ The management client might have entered standby or hibernate mode. Restart the management client. ▪ 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 management client might be blocked by a firewall or some kind of device.

Error condition	Probable cause / recommended action
	Check the firewall settings and contact your network administrator. If none of the above actions solve the problem, save the dump file, the Java trace file and the log file on the management client, and report to customer support. Then restart HDvM - SN.
When you click the HDvM - SN menu, the system does not respond.	If the problem continues after you perform the operation multiple times, close all the HDvM - SN windows and clear the Java and web browser caches.
The application error (1-7050) occurs when you click the HDvM - SN menu.	The version of HDvM - SN recognized by the management client might not match the version installed on the SVP. 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.
Java console is grayed out and does not start when you try to open the HDvM - SN secondary window (Java application).	Restart the management client, or terminate the HDvM - SN process with one of the following methods: ▪ 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.
A message box remains displayed when opening the HDvM - SN secondary window (Java application). The HDvM - SN secondary window does not appear for a long time.	Restart the management client, or terminate the HDvM - SN process with one of the following methods: ▪ 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.

Error condition	Probable cause / recommended action
A message remains displayed when the HDvM - SN 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. Do the same settings on the Network Settings displayed in the General tab of the Java Control Panel.
If you open the Java console dialog box by selecting the Java icon on the system tray while opening the HDvM - SN secondary window (Java application), the browser and Java console may stop responding.	Do not open the Java console dialog box while opening the HDvM - SN secondary window. If the browser and Java console stop responding, restart the management client.
When you click the HDvM - SN 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. Restart the management client, or terminate the HDvM - SN process with one of the following methods: For example: ▪ You might have clicked Exit on the **Security Warning** window. ▪ You might have clicked Cancel on the **Warning - Security** window. Close all the HDvM - SN windows and clear the Java and web browser caches. If the problem continues after you clear both Java and web browser caches, save the HDvM - SN dump file and the Java trace file, and send them to HDvM - SN.

Error condition	Probable cause / recommended action
The following message displays in HDvM - SN. ▪ 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 HDvM - SN. If the problem continues, the cause may be one of the following: ▪ The version of HDvM - SN recognized by the management client might not match the version installed on the SVP. 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.
In Microsoft Edge, the following pop-up window appears when you open the HDvM - SN secondary window: "Microsoft Edge 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 might be enabled. Disable third-party browser extensions as follows: 1. Open the Windows **Internet Options** window (**Control Panel** > **Network and Internet** > **Internet Options**). 2. In the Internet Properties dialog box, select the **Advanced** tab, clear the check box for **Enable third-party browser extensions** under **Browsing**, and then click OK.
In Internet Explorer, the following pop-up window appears when you open the HDvM - SN 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.
In Internet Explorer, an application error (10-6027) occurs when you open the HDvM - SN secondary window.	The SmartScreen Filter function might be enabled when you use Internet Explorer 8.0 or later. Turn off SmartScreen Filter as follows:

Error condition	Probable cause / recommended action
	1. In the Windows menu bar, click Safety > SmartScreen Filter > Turn Off SmartScreen Filter. 2. Restart Internet Explorer.
In Microsoft Edge, the following message appears at the upper right of the browser window when you open the HDvM - SN secondary window: `<file name>.jnlp was blocked because this type of file can harm your device.`	Open the HDvM - SN secondary window after performing the following procedure: 1. Click **Other actions > Save** to save the file. 2. After the file is saved, open the file. (Ignore the Java security warning.)
When you open the HDvM - SN secondary window, an error (22252-005002) occurs.	This problem might occur when the SVP firmware is updated. Download WCLauncher again. If this problem occurs again, collect the HDvM - SN dump files, the Java logs and trace files, and the WCLauncher logs, and then contact customer support.
When you try to open the HDvM - SN secondary window, *`filename`*`.jnlp` is opened by an application other than `WCLauncher.bat`, and the HDvM - SN secondary window cannot be opened.	The .jnlp extension might be associated with an application other than WCLauncher.bat. To associate the .jnlp extension with WCLauncher.bat on Windows 10, perform the following procedure. If you are using another OS, follow the setting method for the OS. After that, open the HDvM - SN secondary window. 1. Save *`filename`*`.jnlp` that is opened when the HDvM - SN secondary window is opened. 2. Right-click *`filename`*`.jnlp` that was saved in step 1, and then click **Open with > Choose another app**.

Error condition	Probable cause / recommended action
	3. In the "How do you want to open this file?" window, select WCLauncher.bat. If WCLauncher.bat is not displayed, click **Look for another app on this PC** and select the following WCLauncher.bat: *installation-directory-of-Web Console Launcher* \WCLauncher\WCLauncher.bat Make sure that you use the Web Console Launcher that you installed in Using Web Console Launcher to enable the secondary window (Java 11 or later) (on page 41). **4.** Select **Always use this app to open .jnlp files**, and then click **OK**.

No response errors

Error condition	Probable cause / recommended action
HDvM - SN hangs and does not respond. HDvM - SN may hang in the following cases: ▪ When you move a window displayed in front of the HDvM - SN secondary window, the area behind the window remains gray and does not go back to normal for a long period of time. ▪ The entire HDvM - SN secondary window goes gray and does not go back to normal for a long period of time.	From the HDvM - SN secondary window, press **Ctrl**+**Alt**+**Shift**+**D** all at once to exit HDvM - SN. If you cannot exit HDvM - SN, reboot the management client or restart HDvM - SN after finishing HDvM - SN forcibly by the following way. ▪ 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.

Error condition	Probable cause / recommended action
When you click Refresh All or Refresh in the HDvM - SN secondary window, it displays the message "Loading" for a long time.	The probable causes are: ▪ Another application such as Command Control Interface may be changing configuration. The window will be updated shortly after the configuration change ends. ▪ Volume Migration operations, Quick Restore operations or Thin Image operations may be in progress. The window will be updated shortly after the operations end.
Error 110-67005 occurred during a HDvM - SN operation on the secondary window.	The probable causes are: ▪ 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 data may not be matched if a communication error occurs between the storage system and the SVP. Wait a few minutes and then click File > Refresh All to reread the configuration information. Then launch Device Manager - Storage Navigator again.
While you are using a HDvM - SN secondary Window, it closes unexpectedly and error 20020-108000 occurs.	Start the HDvM - SN secondary window from the HDvM - SN main window again. If this error occurs repeatedly, close all the HDvM - SN windows, and then clear the Java and web browser caches.
The web browser closes abnormally	This problem can occur if a Mozilla process keeps running after Mozilla stops responding. Delete the "java_vm" and "mozilla" processes and continue with HDvM - SN operations.

Error condition	Probable cause / recommended action
One of the following sets of errors occurred when using HDvM - SN: ▪ 20121-107024 and 10-6027 ▪ 20020-108000 and 10-6027 ▪ 10-6027	The probable causes are: ▪ The SVP may have been restarted. Close HDvM - SN, wait 10 minutes, and then restart it. ▪ The version of HDvM - SN recognized by the management client might not match the version installed on the SVP. Close all the browser windows and then clear the browser cache. ▪ The management client might be in standby or hibernate mode. Restart HDvM - SN. ▪ 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 the browser cache, contact your network administrator. ▪ Restart the web browser If none of the above actions solve the problem, save the HDvM - SN dump file and send it to customer support.

Incorrect display errors

Error condition	Probable cause / recommended action
Only the Exit button and the Refresh and Refresh All commands are effective when accessing the SVP from HDvM - SN.	The SVP might not be ready to perform some write processes from the other system. Wait a few minutes and then click File > Refresh. If the SVP is not restored, click Refresh All.
Only the Exit button and the Refresh All command are effective when accessing the SVP from the HDvM - SN.	An error may have occurred in the SVP. Click File > Refresh All. If the SVP is not restored, log in to HDvM - SN again.
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.

Error condition	Probable cause / recommended action
	Make sure that all the required software options are installed. If they are installed, do one of the following: ▪ Click File > Refresh. ▪ Click File > Refresh All. ▪ Log in to HDvM - SN again.
When you switch windows from one window to the HDvM - SN window, the HDvM - SN window is not displayed.	Close all windows, and then log in to HDvM - SN again.
The items in a list are not synchronized with a scroll bar.	Click the scroll buttons  or  above and below the scroll bar.
The focus disappears from the edit box.	Close all dialog boxes, and then log in to HDvM - SN again.
The web browser does not display correctly, because some GUI items such as labels and icons cannot be loaded properly.	Log out of HDvM - SN, and then log in again. If this error occurs before you log in to the HDvM - SN, close all dialog boxes and then log in to HDvM - SN.
The characters are unreadable because they are overlapped or garbled.	Log out of HDvM - SN, and then log in again.
The characters are garbled in a window where a tree is displayed.	Click File > Refresh.
Even though you have clicked Apply to change storage system settings, the new settings are not displayed in HDvM - SN.	Click File > Refresh.
The dialog box that says Loading... stays open for a long period of time.	A HDvM - SN message dialog box other than the dialog box that says Loading... might be displayed behind this window. Press **Alt**+**Tab** 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 customer support.

Error condition	Probable cause / recommended action
The following information does not display in HDvM - SN windows: ▪ Information on the storage system, such as ports or HDDs ▪ Information configured with another management client	Click File > Refresh. If the problem continues, close all HDvM - SN windows, and then clear the Web browser caches.
The HDvM - SN secondary window does not display.	▪ In the Java Control Panel, click the Temporary Internet Files section. In the Disk Space area, enter 1 MB, and then click Delete Files. ▪ Click Security > Java Control Panel. 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 redo the web browser settings.

Other secondary window errors

Error condition	Probable cause / recommended action
If you click in a HDvM - SN secondary window while a dialog box is open, the dialog box disappears behind the HDvM - SN secondary window.	Click the dialog box again.
An error occurs because a digital signature or security certificate has expired.	You can continue using HDvM - SN even though the digital signature for the HDvM - SN Java application is expired.
You specify IPv6 communication addresses when you start HDvM - SN, but IPv6 is not being used. Instead, IPv6 is being used and IPv4 addresses are output to audit logs for operations on the HDvM - SN secondary window.	IPv4 has higher priority when both IPv4 communication and IPv6 communication can be used. As a result, IPv4 may be used when you specify IPv6 communication addresses. Also, IPv4 addresses may appear in audit logs.

Clearing Java caches

When an error occurs on Device Manager - Storage Navigator, clear the Java and web browser caches to solve the problem. To clear the Java cache, click Delete the temporary files in the **General** dialog box of the Java Control Panel.

Saving Java log and trace files

Before you contact your service representative, save the detail dump files collected using the Dump tool, and the Java log and trace file on your management client, 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 userID\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

Clearing the browser cache and Java memory

If an error occurs in Device Manager - Storage Navigator, try clearing the web browser cache to solve the problem. For instructions, see the documentation for the browser.

Reboot Jetty periodically to ensure that Device Manager - Storage Navigator starts up and runs well. When Jetty is rebooted at regular intervals, memory is released from Java programs, and the necessary memory capacity is secured for startup of Device Manager - Storage Navigator.

Firefox web browser problems on UNIX

Note the following when using Firefox web browser on UNIX:

- If a Mozilla process or a Firefox web browser process becomes unavailable, Device Manager - Storage Navigator performance is affected. Delete the abnormal process and continue with Device Manager - Storage Navigator operations.
- When using Device Manager - 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 Device Manager - Storage Navigator with Firefox, movements of the focus may differ from movements of the focus in Internet Explorer. For example:

- When the Device Manager - 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.

In Firefox, when you click Logout at the upper right corner of the Device Manager - Storage Navigator main window, the Device Manager - Storage Navigator login window appears after you logout. With Internet Explorer, the window closes after the logout.

Troubleshooting the SMI-S function

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 customer support.

The SMI-S certificate might have expired when you receive a storage system. If so, you must upload a new signed certificate to the SMI-S provider.

The following tables list SMI-S error conditions and provide recommended action to resolve the error condition.

SMI-S artificial indication errors

Error condition	Probable cause / Recommended action
The user ID or the password is not valid. (00190 77302)	User ID or password is invalid. Enter the correct user ID or password, and then retry the operation.
An error occurred during the listener information acquisition. (00190 77303)	▪ An error occurred during the listener information acquisition. Check the number of tiers of the certificate chain to be used. The maximum number supported is 5 tiers. Make sure to use a certificate in a certificate chain with no more than 5 tiers. If this problem occurs again, collect Device Manager - Storage Navigator normal dump file using the dump tool.
No listeners are subscribed to the provider. (00190 77304)	The listeners are not subscribed to the SMI-S provider. Have the listeners subscribe to the provider, and retry.
The artificial indication cannot be sent to some listeners. (00190 77305)	The artificial indication cannot be sent to some listeners. Use the dump tool to collect and save Device Manager - Storage Navigator normal dump files. Then contact customer support.
A time-out error occurred. (00190 77306)	Send the artificial indication again. If this problem persists, use the dump tool to collect Device Manager - Storage Navigator normal dump files to some recording media and then contact customer support.
An internal error occurred. (00190 77307)	Use the dump tool to collect Device Manager - Storage Navigator normal dump files to some recording media and then contact customer support.

SMI-S provider errors

Error condition	Probable cause / Recommended action

The following response was received from the SMIS provider:
`Return Value : 4(Failed)`
`ErrorMessage : Could not find FCPort with CtrlID:`
`<Port Number> on device <Serial Number>`
	Stop the service for the storage system on the Storage Device List, and then start the service again. For details about how to stop and start the service for the storage system, see the *Hardware Reference Guide* for your storage system.

Error condition	Probable cause / Recommended action
The HostGroup information referenced by using Device Manager - Storage Navigator cannot be referenced from the SMI-S provider.	Stop the service for the storage system on the Storage Device List, and then start the service again. For details about how to stop and start the service for the storage system, see the *Hardware Reference Guide* for your storage system.

Other errors

The following table lists other errors that occur in Device Manager - Storage Navigator (HDvM - SN) and provides recommended actions for resolving the errors.

Error condition	Probable cause / Recommended action
▪ Error about insufficient capacity when creating an LDEV with sufficient capacity. ▪ Operation error about an LDEV that does not exist when creating a pair for an LDEV that does exist.	Configuration information displayed in HDvM - SN and controller configuration information might not match. Click File > Refresh All in the Device Manager - Storage Navigator main window to reload configuration information. If the problem persists, contact customer support.
The firmware on the SVP is upgraded or downgraded.	▪ Close all HDvM - SN windows, and then clear the browser cache. Even when you are not sure that the firmware on the SVP is upgraded or downgraded, clear the browser cache. ▪ An item added to the table by upgrading or downgrading the SVP firmware is placed on the right edge of the table. Move the column to a more appropriate location if necessary.
The HDvM - SN service stopped unexpectedly and then it is restarting. Troubleshooting code: TRSTNA000007	Wait for 3 minutes. If the error condition does not resolve after waiting for 3 minutes, stop the storage system by Storage Device List and restart it. If the HDvM - SN service does not recover, restart the SVP. If the HDvM - SN service does not recover after restarting the SVP, stop the service by Storage Device List, and update the storage management software and SVP software. If the HDvM - SN service does not recover after updating the storage management software and SVP software, change the virtual memory settings, and then restart the SVP. If the HDvM - SN service still does not recover, uninstall HDvM - SN, install HDvM - SN again, and then register the storage system.

Error condition	Probable cause / Recommended action
HDvM - SN processing is temporarily delayed.	Internal processing (for example, configuration change, P.P. check, operational information acquisition) might be running on the SVP.
Installing of signed SSL certificate fails.	The passphrase for the SSL certificate might be set. Release the passphrase. If needed, see Releasing an SSL certificate passphrase (on page 56).
The message "34062-203102 The storage system is busy." appears during the Syslog settings to send alert notification messages or audit log files.	This error occurs while the HDvM - SN service status is Ready. Take actions by following the error message, and then retry the Syslog settings. If this problem occurs again, take either of the following actions, and then retry the settings: ▪ Stop the HDvM - SN service, and then restart the service. ▪ Restart the SVP.
An error (0002-009000) occurs while you are using HDvM - SN.	Another management client might be changing the HDvM - SN settings. Close all windows, check that maintenance personnel are not using the storage system, and then log in to HDvM - SN again. If other than above, restart the SVP, and then log in to HDvM - SN again.
A message is displayed indicating that the exclusive setting cannot be released, a different user is using the resource, or a different user is locking the resource.	Take the following actions: ▪ This operation cannot be performed while a different user is changing the configurations. Wait for a while, and then retry the operation. ▪ This operation might not be performed while a task is running. Wait for a while, and then retry the operation. If a task is waiting to run, suspend the task so that the waiting task does not run. In other cases, ask the storage administrator to perform Force Release System Lock. After the system lock is forcibly released, retry the operation. If this problem persists, restart the SVP.
In the **Operation Lock Properties** window, Locked is displayed for system lock status and Unlocked is displayed for resource group status.	Restart the SVP, and then log in to HDvM - SN again.
Failed in the certification of the user. appears when you create a configuration report of a storage system and try to view it in a browser.	Close the tab of the configuration report or the window, and then open it again.

Error condition	Probable cause / Recommended action
	If the problem cannot be solved, take the following actions: ▪ If you log in to HDvM - SN from the SVP, download the configuration report. For details, see Downloading and viewing the HDvM - SN configuration reports (on page 209). ▪ If you log in to HDvM - SN from the management client, address mismatch of SSL certificates between the SVP and the management client might have occurred. To reconfigure SSL communication, see Setting up SSL communications (on page 50). If the SSL communication cannot be reconfigured immediately (for example, you do not have permission), you can also download and verify the configuration report. For details, see Downloading and viewing the HDvM - SN configuration reports (on page 209). Otherwise, you can display the configuration report by logging in to HDvM - SN using HTTP. **Note:** You cannot connect HDvM - SN that operates on Adobe AIR by using HTTP (only HTTPS connection is available).
HDvM - SN operation is slow, although the hardware requirements for the SVP are satisfied.	Verify that no anti-virus software runs on the SVP. For more information, see Preventing errors while using virus detection programs on the SVP (on page 127).
You cannot resolve an error condition.	1. Log in to the SVP. 2. In the SVP, use the dump tool to copy the HDvM - SN detailed dump files onto recording media. 3. When using the HDvM - SN secondary window, obtain the Java log and trace files. When using Web Console Launcher, collect the log in *<installation-directory-for-Web-Console-Launcher>*\WCLauncher\log. 4. Contact customer support.
When you open the Tool Panel dialog box while Microsoft Edge Developer Tools is open, an error message is displayed on the Developer Tools console.	Change the Microsoft Edge browser setting as follows: 1. Open the Settings window (click the Settings and more icon (···), and then click **Settings** from the drop-down menu). 2. In the **Settings** window, click **Default browser** in the left pane of the window. 3. In the right pane, set **Allow sites to be reloaded in Internet Explorer mode** to disabled.
When you open the window for updating the firmware, a window for one of the following	Forcibly release the system lock, and then update the firmware again. Note that the system lock can be forcibly released even if

Error condition	Probable cause / Recommended action
messages appears, and the firmware cannot be updated: ▪ 32061 208061, 33361 203116 ▪ 30162 205057, 33361 203116 "The firmware is being updated."	System Unlocked is displayed as the status at the upper right of the Maintenance Utility window.
Edit is clicked, but error "21041-007018" occurs and the storage system information cannot be changed.	The Storage Device List might not have been started with administrator permissions. ▪ End the Storage Device List, and then start it with administrator permissions. ▪ If an error still occurs after starting the Storage Device List with administrator permissions, restart the SVP and restart the Storage Device List with administrator permissions.
Start Service or Stop Service is clicked, but error "21041-007019" occurs. Otherwise, storage systems cannot be deleted from the Storage Device List.	The Storage Device List might not have been started with administrator permissions. ▪ End the Storage Device List, and then start it with administrator permissions. ▪ If an error still occurs after starting the Storage Device List with administrator permissions, restart the SVP and restart the Storage Device List with administrator permissions.
A storage system is clicked in a Storage Device List window, the login window for Storage Navigator is not opened.	The Storage Device List might not have been started with administrator permissions. ▪ End the Storage Device List, and then start it with administrator permissions. ▪ If an error still occurs after starting the Storage Device List with administrator permissions, restart the SVP and restart the Storage Device List with administrator permissions.
An error (21443-200026) occurs while installing the storage management software or the SVP software.	The port number of the port number key name "RestAPIServerStop" might be the same as the port number of other software. Use the following procedure to install the software again: **1.** Check whether the port number of "RestAPIServerStop" is the same as the port number of another application. **2.** If the port numbers are the same, change the port number of "RestAPIServerStop" or the port number of the other software. **3.** Install the software again.
An error (21443-200017) occurs while removing the storage management software.	This error occurs when the command prompt is running and the folder of the current directory of the command prompt is to be deleted.

Error condition	Probable cause / Recommended action
	Move the current directory of the command prompt to a folder that is not subject to deletion, or close the command prompt. Then remove the storage management software again. After removal is done again, a message indicating that the storage management software or SVP software is not installed might be output. Perform one of the following: ▪ Reinstall the software as follows: **1.** From Internet Explorer, remove the storage management software and the SVP software installation folder. **2.** Install the storage management software and SVP software. ▪ Remove the software completely as follows: **1.** From Internet Explorer, remove the installation folder of storage management software and the SVP software. **2.** Install the storage management software and SVP software. **3.** Remove the storage management software and the SVP software.
An error (21041-007006) or (21041-007008) occurs when you click Apply on the **Add System** window.	The connection between the SVP and the storage system has failed. Make sure that the following conditions are satisfied: ▪ The storage system is running. ▪ The Management LAN is working properly. ▪ The IP address or the host name of the storage system is correct. If you want to create a device icon when the running storage system is not connected to the Management LAN, select Manual and then enter the values for the required fields.
After the server certificate for the syslog server, the key management server, or the external authentication server is set, you cannot communicate with the server.	▪ Verify that the server certificate satisfies the requirements and prerequisites. If not, set a server certificate that satisfies the requirements and prerequisites. ▪ Check the number of tiers of the certificate chain to be used. The maximum number supported is 5 tiers for VSP E series. Make sure to use a certificate in the certificate chain with no more than 5 tiers.
In Microsoft Edge, the following pop-up window appears when you open the HDvM - SN secondary window:	Third-party browser extensions might be enabled. Disable third-party browser extensions as follows: **1.** Open the Windows **Internet Options** window (Control Panel > Network and Internet > Internet Options). **2.** In the **Internet Properties** dialog box, select the **Advanced** tab, clear the check box for **Enable third-party browser extensions** under **Browsing**, and then click **OK**.

Error condition	Probable cause / Recommended action
"Microsoft Edge 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."	
In Microsoft Edge, the following message appears at the upper right of the browser window when you open the HDvM - SN secondary window: `<file name>.jnlp` was blocked because this type of file can harm your device.	Open the HDvM - SN secondary window after performing the following procedure: **1.** Click **Other actions > Save** to save the file. **2.** After the file is saved, open the file. (Ignore the Java security warning.)
In the maintenance utility, when a firmware update window opens, a message prompting you to save the `jnlp` file appears. `<file name>.jnlp` was blocked because this type of file can harm your device.	For Microsoft Edge and Google Chrome: Click **Other actions > Save** to save the file. Internet Explorer: Configure Internet Explorer so it saves encrypted pages to disk (click **Tools > Internet Options > Advanced**, and then clear **Do not save encrypted pages to disk**).
The window displaying "Please wait ... Storage Navigator is loading" remains open and you cannot log in.	The IP address of the SVP might have changed. To update the IP address in the Storage Device List, click SVP IP Address (upper right corner of **Storage Device List** window), click Change SVP IP Address, and enter the IP address. Then click Start Service.

Appendix A: Examples of Device Manager - Storage Navigator storage configuration reports

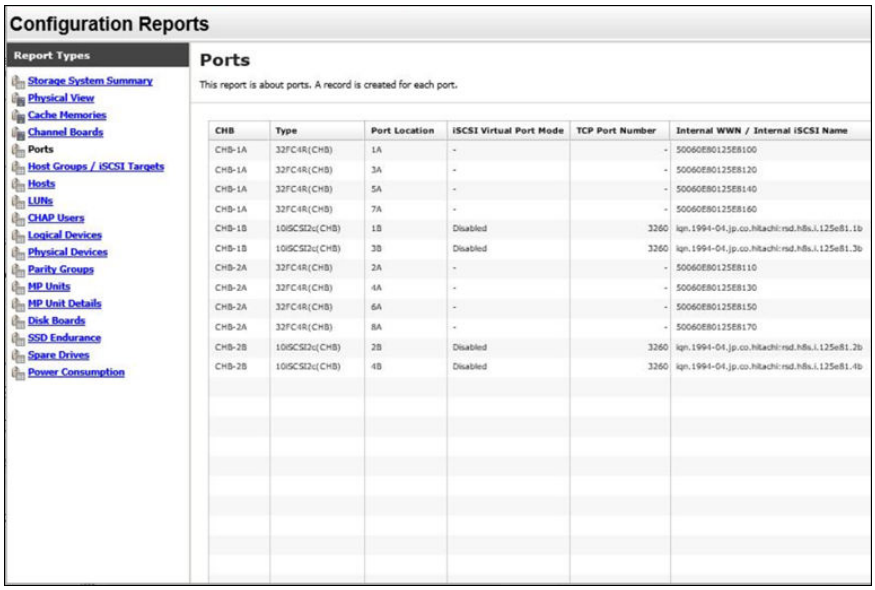
The Device Manager - Storage Navigator can show configuration reports for your storage system in table, graph, and CSV formats.

The following examples show various storage configuration reports in table, graph, and CSV formats.

Report examples: table view

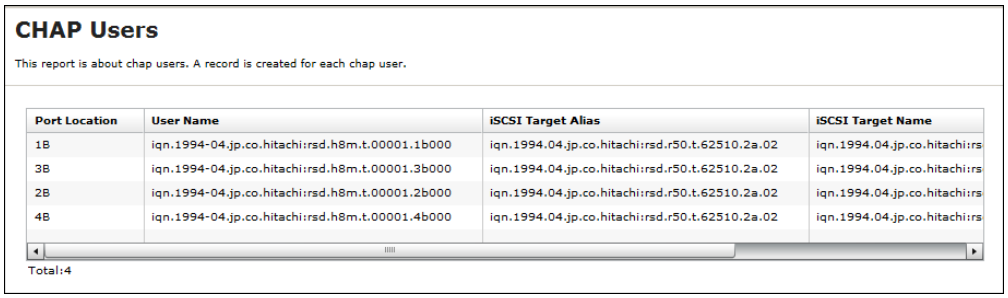
Some Device Manager - Storage Navigator reports appear in table format.

The following figure provides examples of reports in table format. The icons are displayed before the names of the reports in table view. If the icons are not displayed correctly, update the window. To sort data in table reports, click any column header.



CHAP Users report

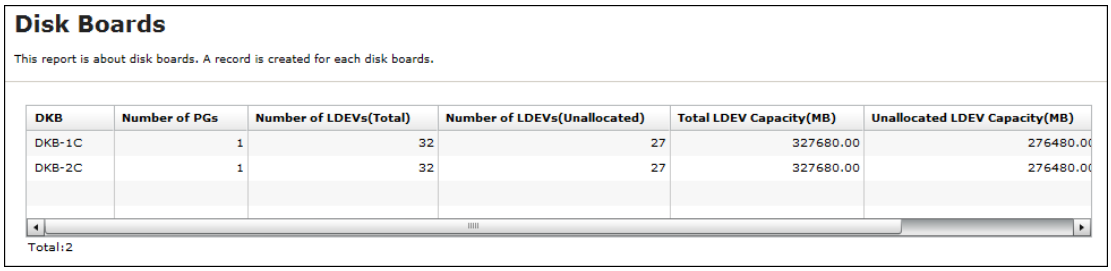
The following figure shows an example of a CHAP Users report. The table following the figure describes the items in the report.



Item	Description
Port Location	Name of the port
User Name	Name of the CHAP user for authentication
iSCSI Target Alias	Alias of the iSCSI target
iSCSI Target Name	Name of the iSCSI target

Disk Boards report

The following figure shows an example of a Disk Boards report. The table following the figure describes the items in the report.

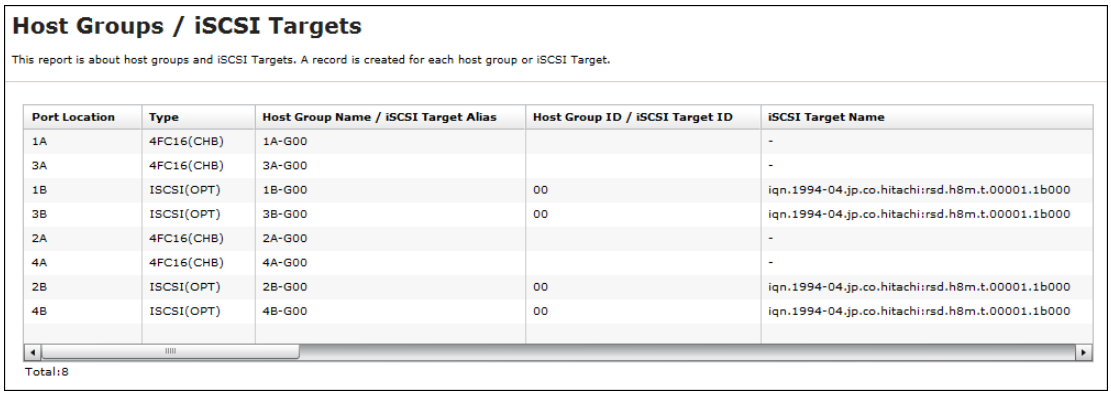


Item	Description
DKB	Location of the disk board. ▪ "External" is displayed when the storage system has an external storage system. ▪ "External (FICON DM)" is displayed when the storage system has volumes for FICON DM.
Number of PGs	The number of the parity groups that the disk board controls. ▪ If "DKB" is "External", this item indicates the number of parity groups mapped to external volumes. ▪ If "DKB" is "External (FICON DM)", this item indicates the number of parity groups mapped to volumes for FICON DM.

Item	Description
Number of LDEVs (Total)	The number of the logical volumes belonging to the parity groups that the disk board 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 board.
Total LDEV Capacity (MB)	Total capacity of the logical volumes belonging to the parity groups that the disk board 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 board.

Host Groups / iSCSI Targets report

The following figure shows an example of a Host Groups / iSCSI Targets report. The table following the figure describes the items in the report.



Host Groups / iSCSI Targets

This report is about host groups and iSCSI Targets. A record is created for each host group or iSCSI Target.

Port Location	Type	Host Group Name / iSCSI Target Alias	Host Group ID / iSCSI Target ID	iSCSI Target Name
1A	4FC16(CHB)	1A-G00		-
3A	4FC16(CHB)	3A-G00		-
1B	ISCSI(OPT)	1B-G00	00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
3B	ISCSI(OPT)	3B-G00	00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
2A	4FC16(CHB)	2A-G00		-
4A	4FC16(CHB)	4A-G00		-
2B	ISCSI(OPT)	2B-G00	00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
4B	ISCSI(OPT)	4B-G00	00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000

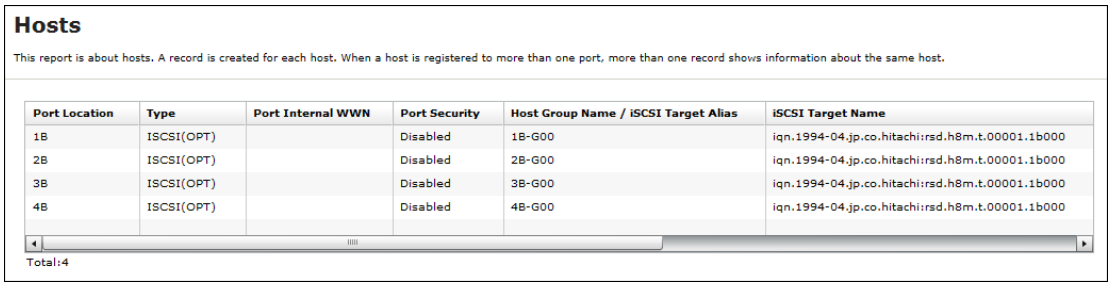
Total:8

Item	Description
Port Location	Name of the port
Type	Type of the host group
Host Group Name / iSCSI Target Alias	Name of the host group / alias of the iSCSI target
Host Group ID / iSCSI Target ID	Number of the host group / ID of the iSCSI target
iSCSI Target Name	Name of the iSCSI target
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

Item	Description
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 boards 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
Authentication : Method	iSCSI target method authentication settings ▪ CHAP ▪ None ▪ Comply with Host Setting
Authentication : Mutual CHAP	Enable or disable the iSCSI target mutual CHAP ▪ Enabled ▪ Disabled
Authentication : User Name	Authenticated iSCSI target user name
Authentication : Number of Users	The number of authenticated users registered in the iSCSI target
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

The following figure shows an example of a hosts report. The table following the figure describes the items in the report. When a host is registered to more than one port, more than one record shows information about the same host.



Hosts

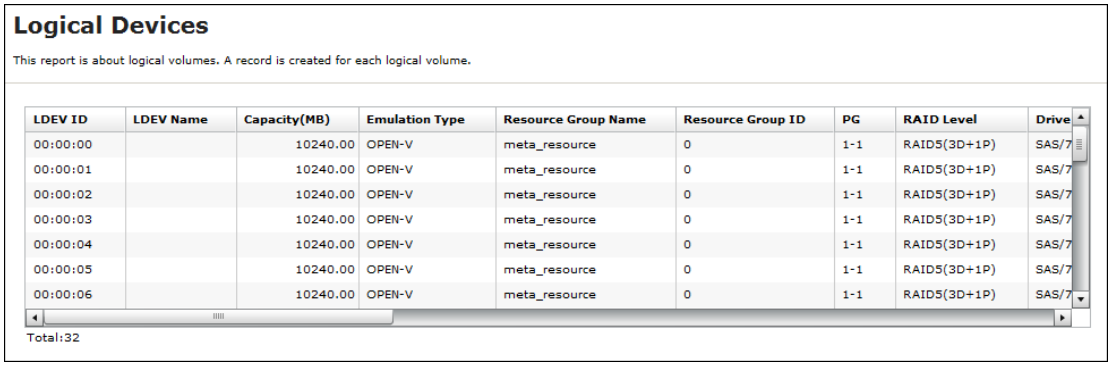
This report is about hosts. A record is created for each host. When a host is registered to more than one port, more than one record shows information about the same host.

Port Location	Type	Port Internal WWN	Port Security	Host Group Name / iSCSI Target Alias	iSCSI Target Name
1B	ISCSI(OPT)		Disabled	1B-G00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
2B	ISCSI(OPT)		Disabled	2B-G00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
3B	ISCSI(OPT)		Disabled	3B-G00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
4B	ISCSI(OPT)		Disabled	4B-G00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000

Total:4

Item	Description
Port Location	Name of the port
Type	Port type
Port Internal WWN	Port WWN
Port Security	Port security setting
Host Group Name / iSCSI Target Alias	Name of the host group / alias of the iSCSI target
iSCSI Target Name	Name of the iSCSI target
Host Mode	Host mode of the host group
Host Mode Option	Host group host mode option. When more than one host mode option is specified, they are separated by semicolons (;)
Host Name	Name of the host that can access the LU path through the port
HBA WWN / iSCSI Name	Host WWN (16-digit hexadecimal) or host iSCSI name

Logical Devices report



Logical Devices

This report is about logical volumes. A record is created for each logical volume.

LDEV ID	LDEV Name	Capacity(MB)	Emulation Type	Resource Group Name	Resource Group ID	PG	RAID Level	Drive
00:00:00		10240.00	OPEN-V	meta_resource	0	1-1	RAID5(3D+1P)	SAS/7
00:00:01		10240.00	OPEN-V	meta_resource	0	1-1	RAID5(3D+1P)	SAS/7
00:00:02		10240.00	OPEN-V	meta_resource	0	1-1	RAID5(3D+1P)	SAS/7
00:00:03		10240.00	OPEN-V	meta_resource	0	1-1	RAID5(3D+1P)	SAS/7
00:00:04		10240.00	OPEN-V	meta_resource	0	1-1	RAID5(3D+1P)	SAS/7
00:00:05		10240.00	OPEN-V	meta_resource	0	1-1	RAID5(3D+1P)	SAS/7
00:00:06		10240.00	OPEN-V	meta_resource	0	1-1	RAID5(3D+1P)	SAS/7

Total:32

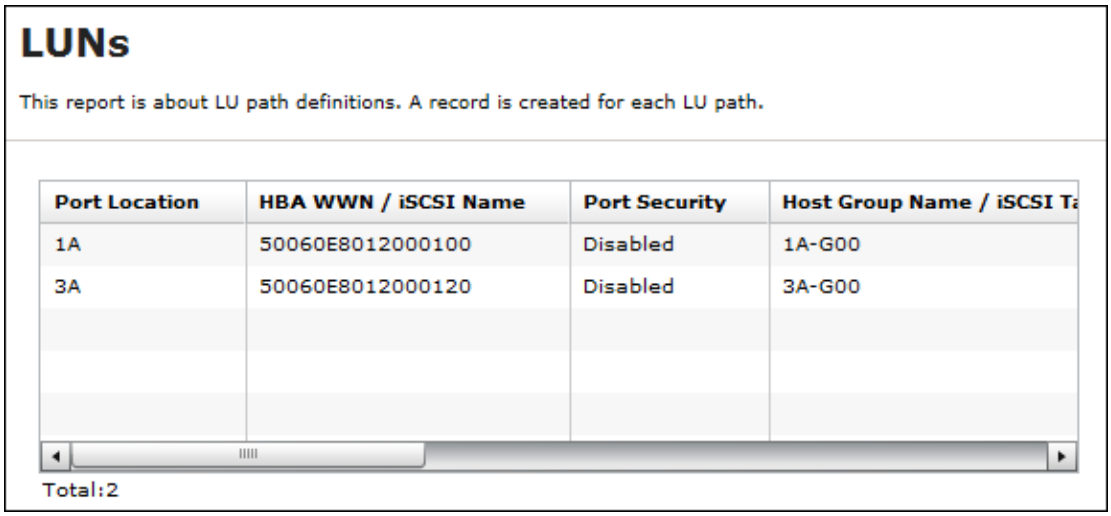
Item	Description
LDEV ID	The logical volume number

Item	Description
LDEV Name	The logical volume name
Capacity (MB)	Capacity of the logical volume
Emulation Type	Emulation type of the logical volume
Resource Group Name	Name of the resource group to which the LDEV belongs
Resource Group ID	ID of the resource group to which the LDEV belongs
PG	Number of the parity group to which the LDEV belongs. ▪ If the number starts with "E" (for example, E1-1), the parity group contains external volumes. ▪ If the number starts with "M" (for example, M1-1), the parity group contains FICON DM volumes. A hyphen (-) is displayed for Dynamic Provisioning and Thin Image V-VOLs.
RAID Level	RAID level of the parity group to which the LDEV belongs*
Drive Type/Interface	Type and interface of the drives in the parity group to which the logical volume belongs For VSP E1090, this item is displayed as "Drive Type/Interface/RPM".
Drive Type-Code	Type code of the drives in the parity group to which the logical volume belongs*
Drive Capacity	Capacity of the drives in the parity group to which the LDEV belongs*
PG Members	Drive locations of the parity group to which the LDEV belongs*
Allocated	Information about whether the host can access the LDEV: ▪ `Y`: The host can access the volume. ▪ `N`: The host cannot access the volume.
SSID	SSID of the LDEV
CVS	Information about whether the LDEV is a custom-size volume
OCS	Oracle checksum
Attribute	Attribute of the LDEV
Provisioning Type	Provisioning type of the LDEV

Item	Description
Pool Name	▪ For V-VOLs of 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 to which the logical volume belongs is displayed. ▪ When neither of the above is displayed, the pool name is blank.
Pool ID	ID of the pool indicated by "Pool Name". A hyphen (-) is displayed for volumes other than pool-VOLs or V-VOLs.
Current MPU	Number of the MP unit that currently controls the LDEV
Setting MPU	Number of the MP unit that you specified to control the LDEV
Command Device: Security	Indicates whether Security is specified as the attribute for the command device. A hyphen (-) is displayed when "Attribute" is not "CMDDEV".
Command Device: User Authentication	Indicates whether User Authentication is specified as the attribute for the command device. A hyphen (-) is displayed when "Attribute" is not "CMDDEV".
Command Device: Device Group Definition	Indicates whether Device Group Definition is specified as the attribute for the command device. A hyphen (-) is displayed when "Attribute" is not "CMDDEV".
Encryption	Indicates whether the parity group to which the LDEV belongs is encrypted: ▪ For internal volumes: Enabled (encrypted) or Disabled (not encrypted) ▪ For external volumes: blank
ALUA Mode	Indicates whether the ALUA mode is enabled: ▪ Enabled: ALUA mode is enabled. ▪ Disabled: ALUA mode is disabled.
T10 PI	Indicates the T10 PI attribute set for the LDEV: ▪ Enabled ▪ Disabled ▪ Blank if the emulation type is not OPEN-V
RPM	Revolutions-per-minute (RPM) (unit: krpm) of the drive in the parity group to which the LDEV belongs. A hyphen (-) is displayed when the drive type is not HDD.* This item is output only when the firmware version is 93-05-02 or later. For VSP E1090, this item is displayed between Interface and Drive Type-Code.
* A hyphen (-) is displayed if the LDEV is an external volume.	

LUNs report

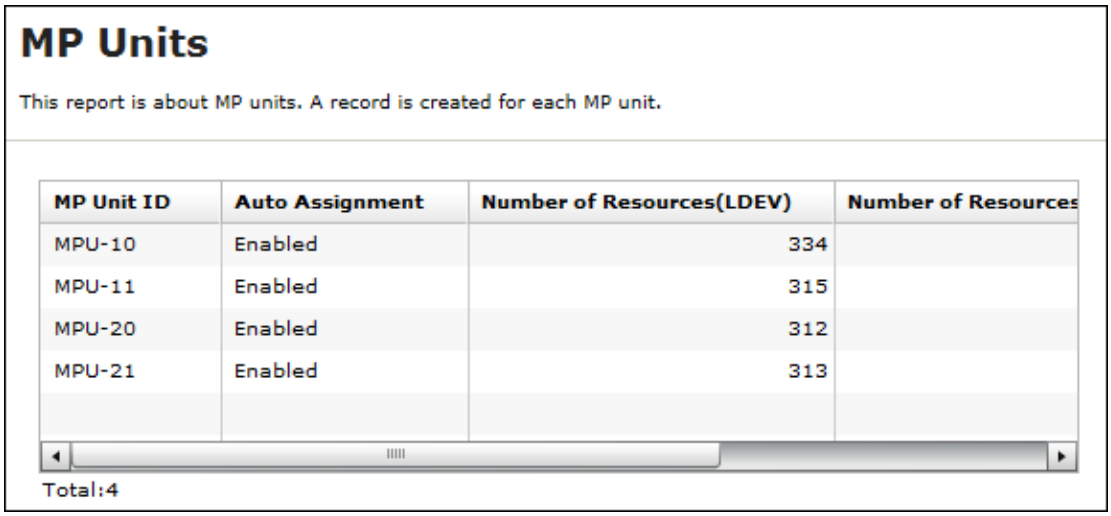
The following figure shows an example of an LU path definitions report. A record is created for each LU path. The table following the figure describes the items in the report.



Item	Description
Port Location	Name of the port
Internal WWN / Internal iSCSI Name	Port WWN (16-digit hexadecimal) or port iSCSI name
Port Security	Name of the type of security of the port
Host Group Name / iSCSI Target Alias	Name of the host group or alias of the iSCSI target
iSCSI Target Name	Name of the iSCSI target
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
Asymmetric Access State	Asymmetric access status: ▪ Active/Optimized: Prioritized ▪ Active/Non-Optimized: Lower priority

MP Units report

The following figure shows an example of an MP units report. The table following the figure describes the items in the report.



MP Units

This report is about MP units. A record is created for each MP unit.

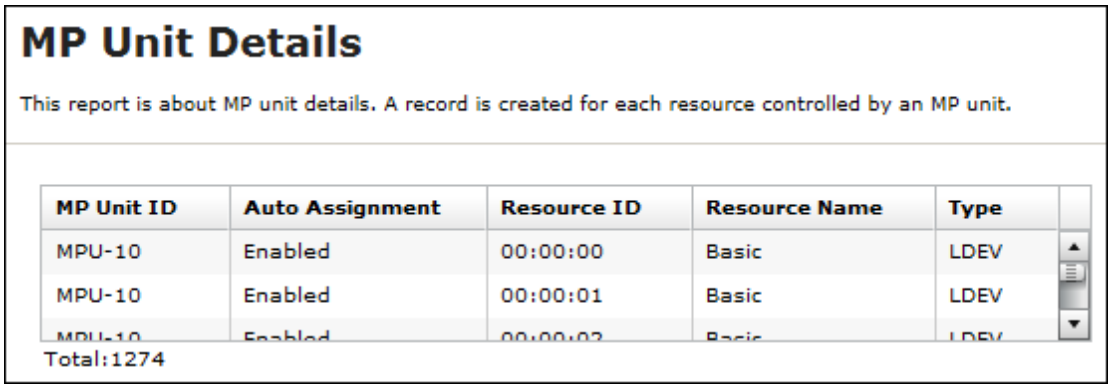
MP Unit ID	Auto Assignment	Number of Resources(LDEV)	Number of Resources
MPU-10	Enabled	334	
MPU-11	Enabled	315	
MPU-20	Enabled	312	
MPU-21	Enabled	313	

Total:4

Item	Description
MP Unit ID	MP unit ID
Auto Assignment	Auto assignment attribute for the MP unit
Number of Resources (LDEV)	Number of LDEVs that the MP unit controls
Number of Resources (Journal)	Number of journals that the MP unit controls
Number of Resources (External Volume)	Number of external volumes that the MP unit controls (includes volumes for FICON DM)
Number of Resources (Total)	The total number of resources that the MP unit controls. It is the total of Number of Resources (LDEV), Number of Resources (Journal), and Number of Resources (External Volume).

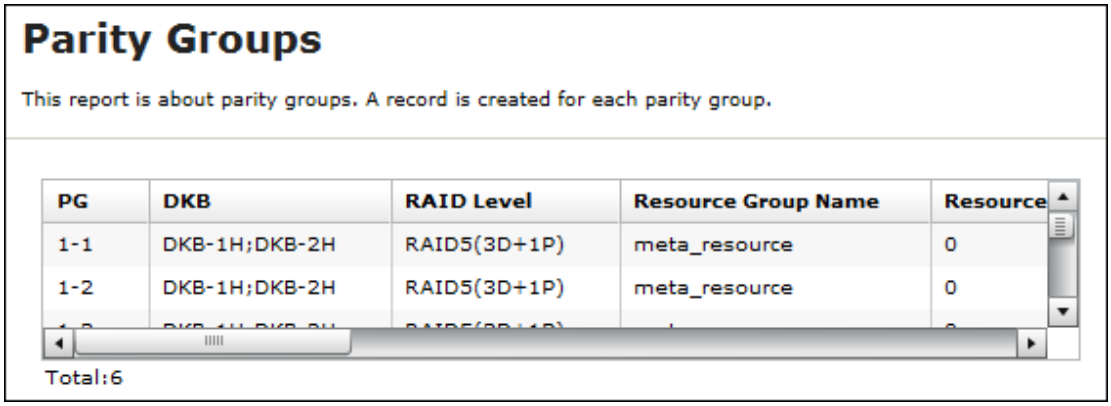
MP Unit Details report

The following figure shows an example of an MP unit details report. The table following the figure describes the items in the report.



Item	Description
MP Unit ID	MP unit 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. A hyphen (-) displays for journal volumes or external volumes.
Type	The type of the resource that the MP unit controls

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 (Hitachi Universal Volume Manager User Guide). ▪ If the number starts with "M" (for example, M1-1), the parity group contains volumes for FICON DM.
DKB	Name of the disk board that controls the parity group[1]
RAID Level	RAID level of the parity group[1]
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
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 ▪ The type code of the first drive in the parity group. ▪ If the parity group contains external volumes, the drive type code displays the vendor, the model, and the serial number of the storage system. ▪ Separated by semicolons (;) if multiple drive types are set.
Drive Type/Interface	(VSP E590, VSP E790, VSP E990) Drive type and interface of the drives in the parity group to which the LDEV belongs[1] For VSP E1090 this item is displayed as "Drive Type/Interface/RPM".
Drive Type/ Interface/RPM	(VSP E1090) Drive type, drive control name, and revolutions-per-minute (RPM) (unit: krpm) of the drives in the parity group to which the LDEV belongs[1] A hyphen (-) is displayed instead of the RPM when the drive type is not HDD.
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[1,2]

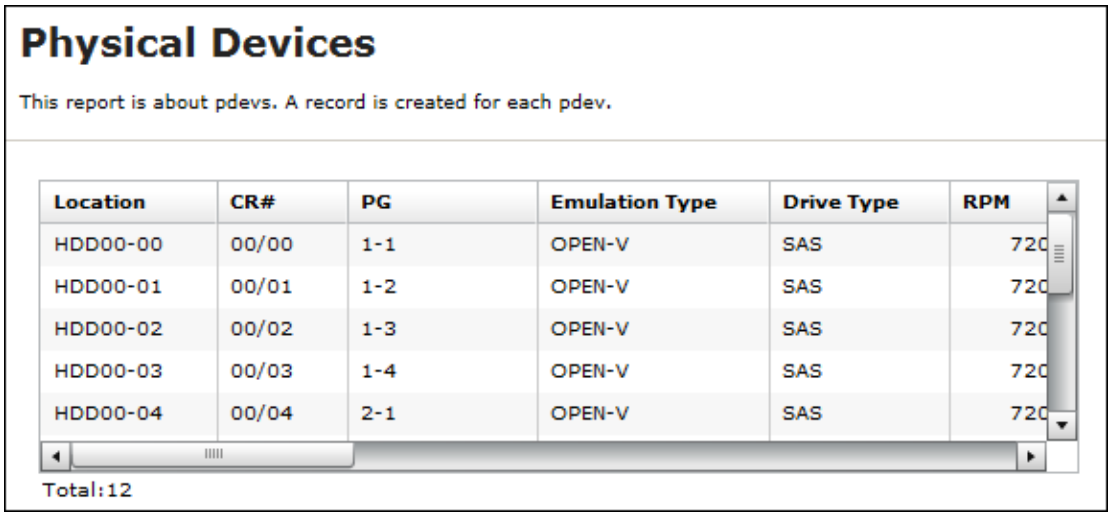
Item	Description
RAID Concatenation #1	The number indicating a parity group #1 connected to this parity group[1,2]
RAID Concatenation #2	The number indicating a parity group #1,2 connected to this parity group[1,2]
Encryption	Indicates whether the parity group is encrypted. ▪ For internal volumes: Enabled (encrypted) or Disabled (not encrypted) ▪ For external volumes: A hyphen (-) is displayed.
RPM	Revolutions-per-minute (RPM) (unit: krpm) of the drives in the parity group.[1] A hyphen (-) is displayed when the drive type is not HDD. This item is output only when the firmware version is 93-05-02 or later.

Notes:

1. A hyphen is displayed if the parity group contains external volumes.
2. A hyphen is displayed if the parity group is not connected with another parity group or if the parity group contains external volumes including volumes for FICON DM.

Physical Devices report

The following figure shows an example of part of a Physical Devices report. The actual report includes more columns of information. A record is created for each physical device.



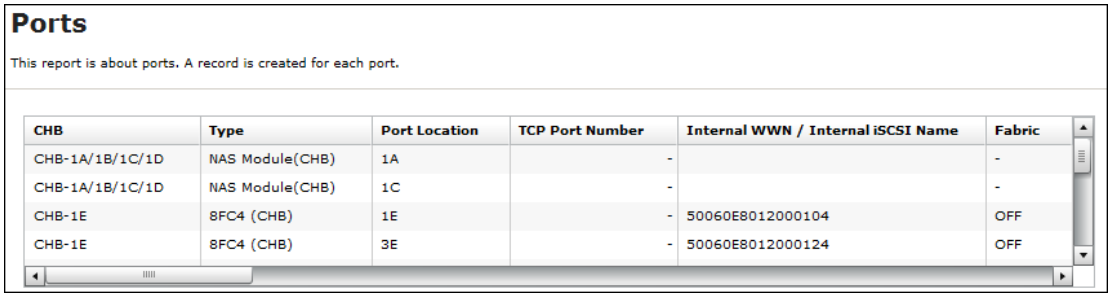
Item	Description
Location	Name of physical devices
CR#	C# and R# to define physical devices Output as "XX/YY"

Item	Description
PG	Parity group of physical devices
Emulation Type	Parity group of physical devices
Drive type	Drive type of physical devices (for example, SAS, SSD)
Interface	Revolutions-per-minute (RPM) (unit: rpm) of the drives of the physical devices A hyphen (-) is displayed when the drive type is not HDD.
Drive Type-Code	Type code of the drive in the parity group. Output example: SLR5B- M200SS;SFB5A-M200SS; (if multiple drive types are set)
Drive Size	Drive size (inches) (for example, 2.5, 3.5)
Drive Capacity	Physical drive capacity (GB or TB)
Drive Version	Firmware version of the drive
DKB1*	Name of the DKB1 which controls the physical devices
DKB2*	Name of the DKB2 which controls the physical devices
DKB3*	Name of the DKB3 which controls the physical devices This item is output only for VSP E990 and VSP E1090.
DKB4*	Name of the DKB4 which controls the physical devices This item is output only for VSP E990 and VSP E1090.
Serial Number#	Serial product number of the physical devices
RAID Level	RAID level of the physical devices (for example, RAID1(2D+2D), RAID6(6D +2P))
RAID Concatenation#0	Number indicating a parity group #0 connected to this parity group Output example: 2-1, 3-1, 4-1
RAID Concatenation#1	Number indicating a parity group #1 connected to this parity group Output example: 2-1, 3-1, 4-1
RAID Concatenation#2	Number indicating a parity group #2 connected to this parity group Output example: 2-1, 3-1, 4-1
Resource Group Name	Name of resource group to which the parity group of physical devices belong
Resource Group ID	ID (0 to 1023 binary)

Item	Description
Encryption	Enable or disable status of the parity group to which the physical devices belong ▪ Enabled: Encryption is enabled. ▪ Disabled: Encryption is disabled.
RPM	Revolutions-per-minute (RPM) (unit: rpm) of the drives of the physical devices A hyphen (-) is displayed when the drive type is not HDD. This item is output only when the firmware version is 93-05-02 or later. For VSP E1090, this item is displayed between **Interface** and **Drive Type-Code**.
* The number of DKBs that control the physical devices depends on the storage configuration, such as the connected DB type. The name of DKB is output in the order from DKB1. A hyphen (-) is displayed if no DKBs are output.	

Ports report

The following figure shows an example of a Ports report. The Ports report includes several more columns of information that are described below but not shown here.



Item	Description
CHB	Name of the channel board
Type	Package type of the channel board
Port Location	Name of the port on the channel board
iSCSI Virtual Port Mode	Mode of the iSCSI virtual port
TCP Port Number	Port number to use for a socket (decimal)
Internal WWN / Internal iSCSI Name	Port WWN (16-digit hexadecimal) or iSCSI name of the port

Item	Description
Fabric	One of the Fibre topology settings indicating the setting status of the Fabric switch A hyphen (-) is displayed for mainframe ports.
Connection Type	Fibre topology setting: ▪ Point to Point ▪ FC-AL A hyphen (-) is displayed for mainframe ports.
IPv4 : IP Address	IPv4 address of the port Output example: 192.168.0.100
IPv4 : Subnet Mask	IPv4 subnet mask of the port Output example: 255.255.255.0
IPv4 : Default Gateway	IPv4 default gateway of the port Output example: 255.255.255.0
IPv6 : Mode	IPv6 settings of the port (enabled or disabled)
IPv6 : Link Local Address	IPv6 link local address of the port (16-digit hexadecimal)
IPv6 : Global Address	IPv6 global address of the port. Output example: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal)
IPv6 : Global Address 2	IPv6 global address 2 of the port. Output example: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal)
IPv6 : Assigned Default Gateway	Assigned IPv6 default gateway
Selective ACK	Selective ACK mode (enabled or disabled)
Ethernet MTU Size (Byte)	MTU settings (binary) Output example: 1,500
Keep Alive Timer	iSCSI keep alive timer (0 to 64,800) (sec)
VLAN : Tagging Mode	Tagging mode of VLAN (enabled or disabled)
VLAN : ID	Number of VLAN set to the port (1 to 4,094)
CHAP User Name	User name for the CHAP authentication
iSNS Server : Mode	iSNS mode settings (on or off)

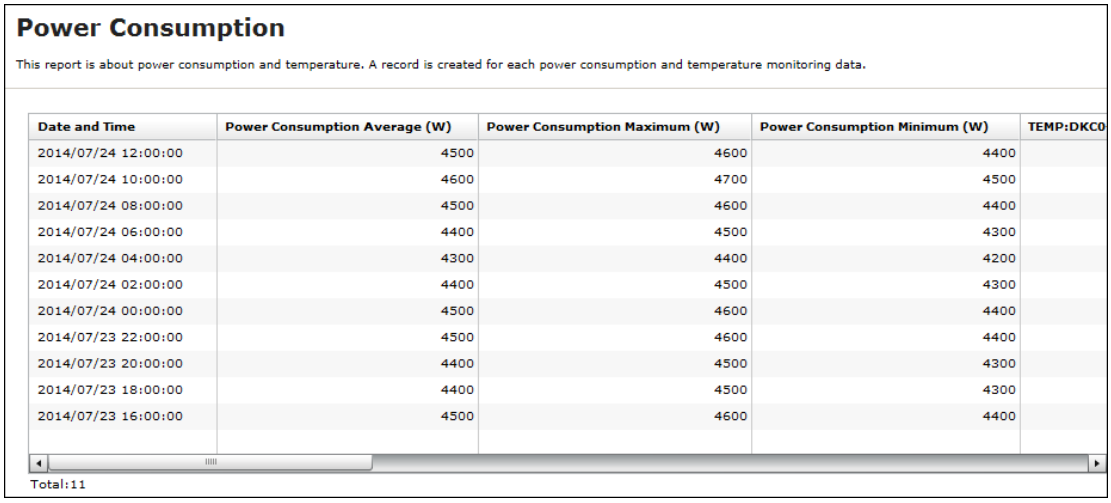
Item	Description
iSNS Server : IP Address	IP address of the iSNS server (30 to 65,535)
iSNS Server : TCP Port Number	Number of the TCP port used in iSNS (binary)
Address (Loop ID)	Fibre port address and Loop ID of the port A hyphen (-) is displayed for mainframe ports.
Port Security	Security of the port (enabled or disabled) A hyphen (-) is displayed for mainframe ports.
Speed	Data transfer speed of the port A hyphen (-) is displayed for mainframe ports.
SFP Data Transfer Rate	Maximum transfer rate of SFP which the mounted package supports. Output example: 32G
T10 PI Mode	Indicates whether the T10 PI mode can be applied to the port. ▪ Enabled ▪ Disabled ▪ Blank: The port type is a Fibre port other than 16FC2(CHB). ▪ - (hyphen): iSCSI port
Resource Group Name	Name of the resource group to which the port belongs
Resource Group ID	ID of the resource group to which the port belongs (0 to 1023)
Number of Hosts	Number of hosts registered to the port A hyphen (-) is displayed for mainframe ports.
Number of LUNs	Number of LU paths defined to the port A hyphen (-) is displayed for mainframe ports.
Number of LDEVs	Number of logical volumes that can be accessed through the port A hyphen (-) is displayed for mainframe ports.
Number of PGs	Number of parity groups having the logical volumes that can be accessed through the port A hyphen (-) is displayed for mainframe ports.
Number of DKBs	Number of disk boards controlling the parity group that contains the logical volumes that can be accessed through the port A hyphen (-) is displayed for mainframe ports.

Power Consumption report

The following figure shows an example of a power consumption report. A record is created every two hours for each power consumption and temperature monitoring data. The table following the figure describes the items in the report.

Note:

- If the storage system is turned off, no records are created. If the system is in maintenance mode or if the SVP is rebooted, up to 2 hours of records could be lost.
- If a failure occurs in the storage system, the correct information might not be output.
- If the power and temperature information cannot be acquired due to a unit or network failure, a hyphen(-) is displayed.
- For unimplemented DBs, the temperature information is blank.



Power Consumption

This report is about power consumption and temperature. A record is created for each power consumption and temperature monitoring data.

Date and Time	Power Consumption Average (W)	Power Consumption Maximum (W)	Power Consumption Minimum (W)	TEMP:DKC0
2014/07/24 12:00:00	4500	4600	4400	
2014/07/24 10:00:00	4600	4700	4500	
2014/07/24 08:00:00	4500	4600	4400	
2014/07/24 06:00:00	4400	4500	4300	
2014/07/24 04:00:00	4300	4400	4200	
2014/07/24 02:00:00	4400	4500	4300	
2014/07/24 00:00:00	4500	4600	4400	
2014/07/23 22:00:00	4500	4600	4400	
2014/07/23 20:00:00	4400	4500	4300	
2014/07/23 18:00:00	4400	4500	4300	
2014/07/23 16:00:00	4500	4600	4400	

Total:11

Item	Description
Date and Time	Date and time when the power or temperature information was recorded.
Power Consumption Average (W)	Average of the power consumption
Power Consumption Maximum (W)	Maximum of the power consumption
Power Consumption Minimum (W)	Minimum of the power consumption
TEMP:DKC0-Cluster1 Average (°C)	Average temperature of DKC0:CL1
TEMP:DKC0-Cluster1 Maximum (°C)	Maximum temperature of DKC0:CL1
TEMP:DKC0-Cluster1 Minimum (°C)	Minimum temperature of DKC0:CL1
TEMP:DKC0-Cluster2 Average (°C)	Average temperature of DKC0:CL2

Item	Description
TEMP:DKC0-Cluster2 Maximum (°C)	Maximum temperature of DKC0:CL2
TEMP:DKC0-Cluster2 Minimum (°C)	Minimum temperature of DKC0:CL2

Example of Power Consumption report for VSP E590 or VSP E790 (for DB50)

Item for DB50	Description
Date and Time	Date and time when the power or temperature information was recorded.
TEMP:DB50-DBPS50-1 Average (°C) TEMP:DB50-DBPS50-1 Maximum (°C) TEMP:DB50-DBPS50-1 Minimum (°C) TEMP:DB50-DBPS50-2 Average (°C) TEMP:DB50-DBPS50-2 Maximum (°C) TEMP:DB50-DBPS50-2 Minimum (°C)	Average temperature, maximum temperature, and minimum temperature of the DB for the two-hour period. Outputs in the following format: TEMP:DB*XX*-DBPS*XX*-*CL* Average, Maximum, or Minimum (°C) where ▪ DB*XX*: DB location number The display format of the DB location number differs depending on the type and mount location of the DB: • DB*XX*: DBS/DBL/DB60 location number (decimal) (50 to 61) • DB*XX&YY*: DBS2 location number (decimal) (50&51, or 52&53) ▪ DBPS*XX*-*CL*: DBPS location number • *XX*: *XX* in the DB location number (decimal) (00, or 50 to 61) • *CL*: DBPS number (1 or 2)

Example of Power Consumption report for VSP E990 (for DB01)

Item for DB01	Description
Date and Time	Date and time when the power or temperature information was recorded.
TEMP:DB01-DBPS01-1 Average (°C)	Average temperature, maximum temperature, and minimum temperature of the DB for the two-hour period. Outputs in the following format:

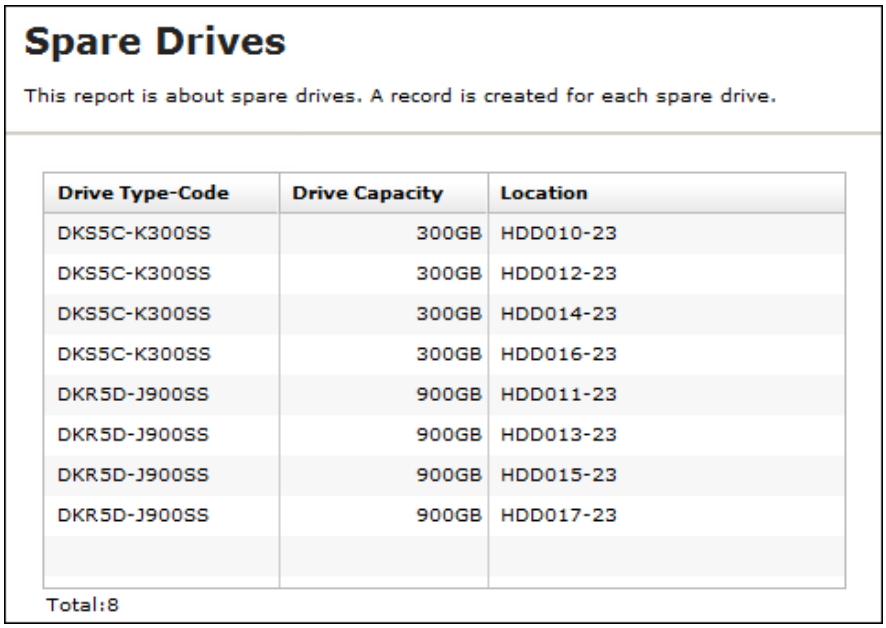
Item for DB01	Description
TEMP:DB01-DBPS01-1 Maximum (°C)	TEMP:DB*XX*-DBPS*XX*-*CL* Average, Maximum, or Minimum (°C) where ▪ *XX*: DB number (00 to 03) ▪ *CL*: Cluster number (1 or 2)
TEMP:DB01-DBPS01-1 Minimum (°C)	
TEMP:DB01-DBPS01-2 Average (°C)	
TEMP:DB01-DBPS01-2 Maximum (°C)	
TEMP:DB01-DBPS01-2 Minimum (°C)	

Example of Power Consumption report for VSP E1090 (for DB69)

Item for DB01	Description
Date and Time	Date and time when the power or temperature information was recorded.
TEMP:DB69-DBPS69-1 Average (°C)	Average temperature, maximum temperature, and minimum temperature of the DB for the two-hour period. Outputs in the following format: TEMP:DB*XX*-DBPS*XX*-*CL* Average, Maximum, or Minimum (°C) where ▪ DB*XX*: DB location number The display format of the DB location number differs depending on the type and mount location of the DB: ▫ DB*XX*: DBN location number (decimal) (00 to 03), DBS, DBL, DB60 location number (decimal) (00 to 61) ▫ DB*XX*&*YY*: DBS2 location number (decimal) (00&01, 02&03, 50&51, or 52&53) ▪ DBPS*XX*-*CL*: DBPS location number • *XX*: DB location number (decimal) (00 to 69) • *CL*: DBPS number (1 or 2)
TEMP:DB69-DBPS69-1 Maximum (°C)	
TEMP:DB69-DBPS69-1 Minimum (°C)	
TEMP:DB69-DBPS69-2 Average (°C)	
TEMP:DB69-DBPS69-2 Maximum (°C)	
TEMP:DB69-DBPS69-2 Minimum (°C)	

Spare Drives report

The following figure shows an example of a spare drives report. The table following the figure describes the items in the report.



Spare Drives

This report is about spare drives. A record is created for each spare drive.

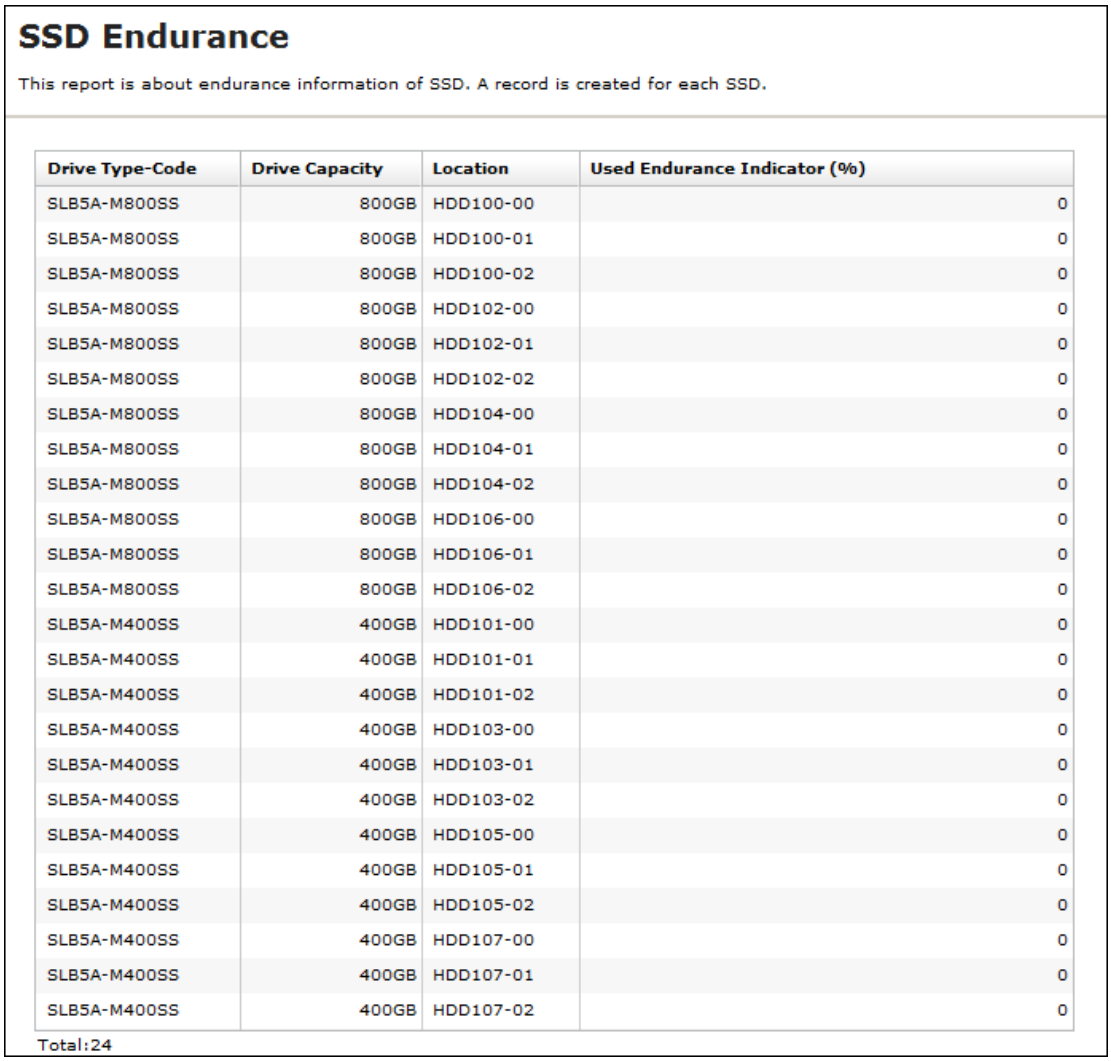
Drive Type-Code	Drive Capacity	Location
DKS5C-K300SS	300GB	HDD010-23
DKS5C-K300SS	300GB	HDD012-23
DKS5C-K300SS	300GB	HDD014-23
DKS5C-K300SS	300GB	HDD016-23
DKR5D-J900SS	900GB	HDD011-23
DKR5D-J900SS	900GB	HDD013-23
DKR5D-J900SS	900GB	HDD015-23
DKR5D-J900SS	900GB	HDD017-23

Total:8

Item	Description
Drive Capacity	Capacity of the spare drive
Drive Type-Code	Type code of the spare drive
Location	Location of the spare drive

SSD Endurance report

The following figure shows an example of an SSD endurance report. The table following the figure describes the items in the report.



SSD Endurance

This report is about endurance information of SSD. A record is created for each SSD.

Drive Type-Code	Drive Capacity	Location	Used Endurance Indicator (%)
SLB5A-M800SS	800GB	HDD100-00	0
SLB5A-M800SS	800GB	HDD100-01	0
SLB5A-M800SS	800GB	HDD100-02	0
SLB5A-M800SS	800GB	HDD102-00	0
SLB5A-M800SS	800GB	HDD102-01	0
SLB5A-M800SS	800GB	HDD102-02	0
SLB5A-M800SS	800GB	HDD104-00	0
SLB5A-M800SS	800GB	HDD104-01	0
SLB5A-M800SS	800GB	HDD104-02	0
SLB5A-M800SS	800GB	HDD106-00	0
SLB5A-M800SS	800GB	HDD106-01	0
SLB5A-M800SS	800GB	HDD106-02	0
SLB5A-M400SS	400GB	HDD101-00	0
SLB5A-M400SS	400GB	HDD101-01	0
SLB5A-M400SS	400GB	HDD101-02	0
SLB5A-M400SS	400GB	HDD103-00	0
SLB5A-M400SS	400GB	HDD103-01	0
SLB5A-M400SS	400GB	HDD103-02	0
SLB5A-M400SS	400GB	HDD105-00	0
SLB5A-M400SS	400GB	HDD105-01	0
SLB5A-M400SS	400GB	HDD105-02	0
SLB5A-M400SS	400GB	HDD107-00	0
SLB5A-M400SS	400GB	HDD107-01	0
SLB5A-M400SS	400GB	HDD107-02	0

Total:24

Item	Description
Drive Type-Code	Type code of the drive
Drive Capacity	Capacity of the drive
Location	Location of the drive
Used Endurance Indicator (%)	The used endurance of SSD life (0 to 100) The value of this indicator increases due to drive operation associated with internal processing of the storage system, and the host I/O. Even when no data is copied due to a drive failure, the value of this indicator increases because the spare drive also performs internal processing.

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
Software Versions	Version of the following programs. VSP E590, VSP E790: ▪ Main ▪ DKB ▪ ROM BOOT ▪ RAM BOOT ▪ Expander ▪ Config ▪ CFM ▪ HDD ▪ Printout Tool ▪ CHB (iSCSI) ▪ CHB (FC32G) ▪ GUM ▪ CTL_NSW ▪ CTL_eDKBN ▪ DKBN (not supported by VSP E590 or VSP E790) ▪ NSW (not supported by VSP E590 or VSP E790)

Item	Description
	VSP E990: ▪ Main ▪ DKBN ▪ NSW ▪ ROM BOOT ▪ RAM BOOT ▪ Config ▪ CFM ▪ HDD ▪ Printout Tool ▪ CHB (iSCSI) ▪ CHB (FC32G) ▪ GUM ▪ EDKBN VSP E1090: ▪ Main ▪ CHB (iSCSI) ▪ CHB (FC32G) ▪ DKB ▪ DKBN ▪ EDKBN ▪ GUM ▪ ROM BOOT ▪ RAM BOOT ▪ Expander ▪ NSW ▪ Config ▪ CFM ▪ HDD ▪ Printout Tool
Number of CUs	The number of control units in the storage system

Item	Description
Shared Memory Size (GB)	Capacity of shared memory Includes the cache management information (directory)
Cache Size (GB)	Capacity of the cache
Number of DKBs	The number of disk boards on the module
System Options	List of the system options specified for the storage system
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
Free Drive Capacity (GB)	Total capacity of the free drives in the storage system
Volume Capacity (GB)	List of the capacity of the open volumes You cannot sort the list.
Number of LDEVs	List of the numbers of the volumes in the following status. ▪ Allocated ▪ Unallocated ▪ Reserved ▪ V-VOL You cannot sort the list.

Report examples: graphical view

Some Device Manager - Storage Navigator reports appear in graphical format.

The reports described in this topic display as graphics.  icons are displayed before the names of reports in graphical view. If the icons or graphics are not displayed properly, update the window.

Cache Memories report

This report shows cache memory data, including shared memory, main board, and DIMM capacity. The total cache memory is displayed for each module.

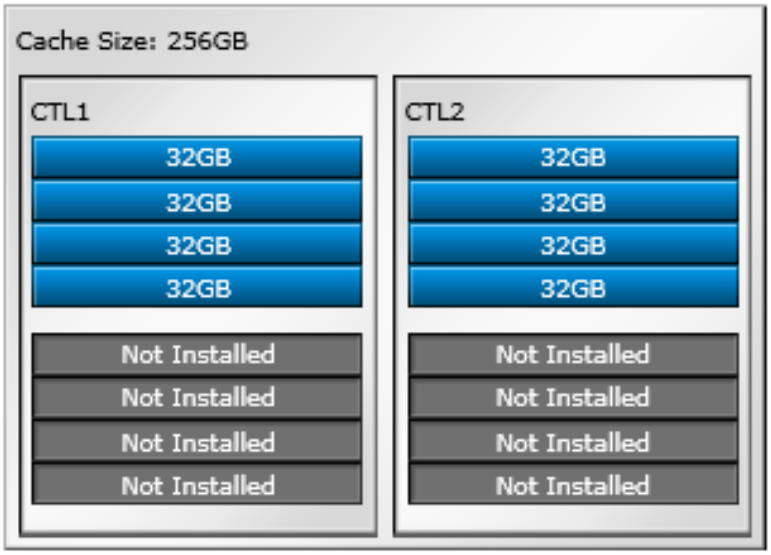


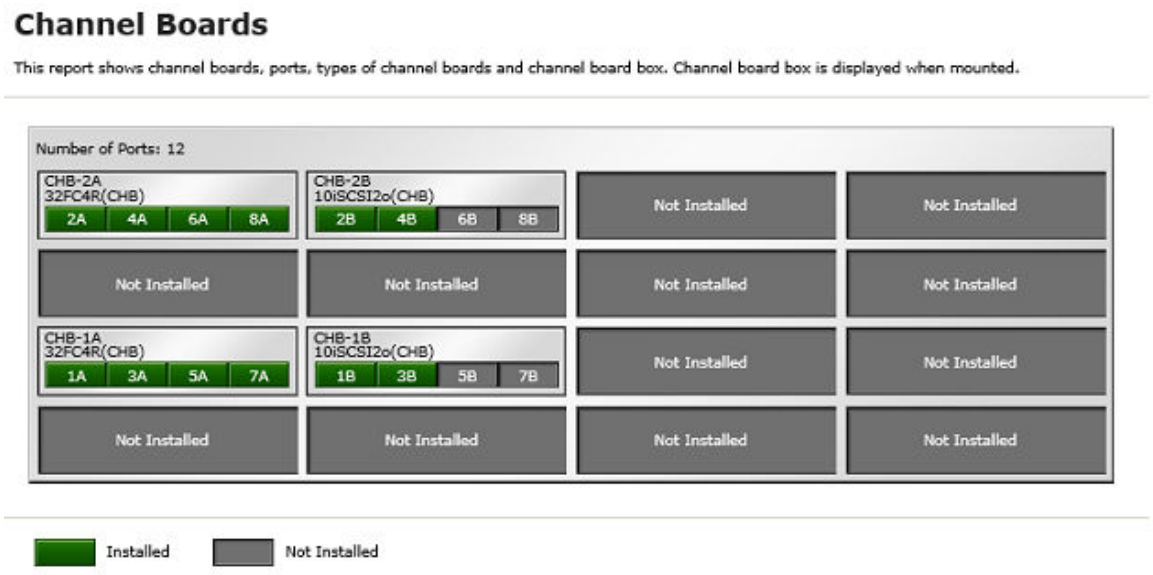
Figure 4 Cache Memories report (VSP E990, VSP E1090)

Channel Boards report

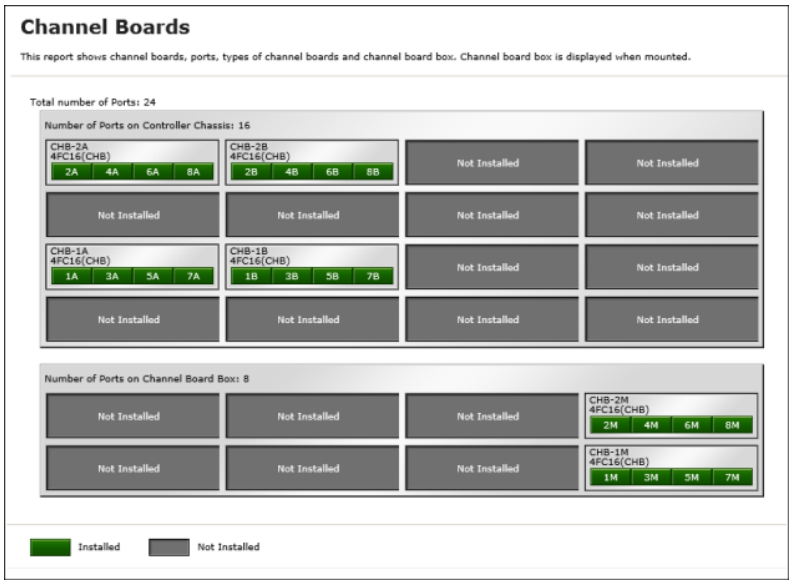
This report shows the channel boards and the ports and types of channel boards for each channel board. The keys show which channel boards are installed (green keys) and which channel boards are not installed (gray keys).

If a PCIe channel board installed in the DKC is connected to a channel board box, the status of the channel board box is displayed.

Channel Boards report (VSP E990, VSP E1090)



Channel Boards report (when a channel board box is connected)



Physical View report

This report shows disk controller chassis and drive boxes, and includes channel boards, disk boards, data drives, spare drives, and free drives.

It also shows the storage system type, serial number, and software version. You can check the legend for disk units, such as SAS, SSD, Spare, Free, or Not Installed.

If a PCIe channel board installed in the DKC is connected to a channel board box, the status of the channel board box is displayed.

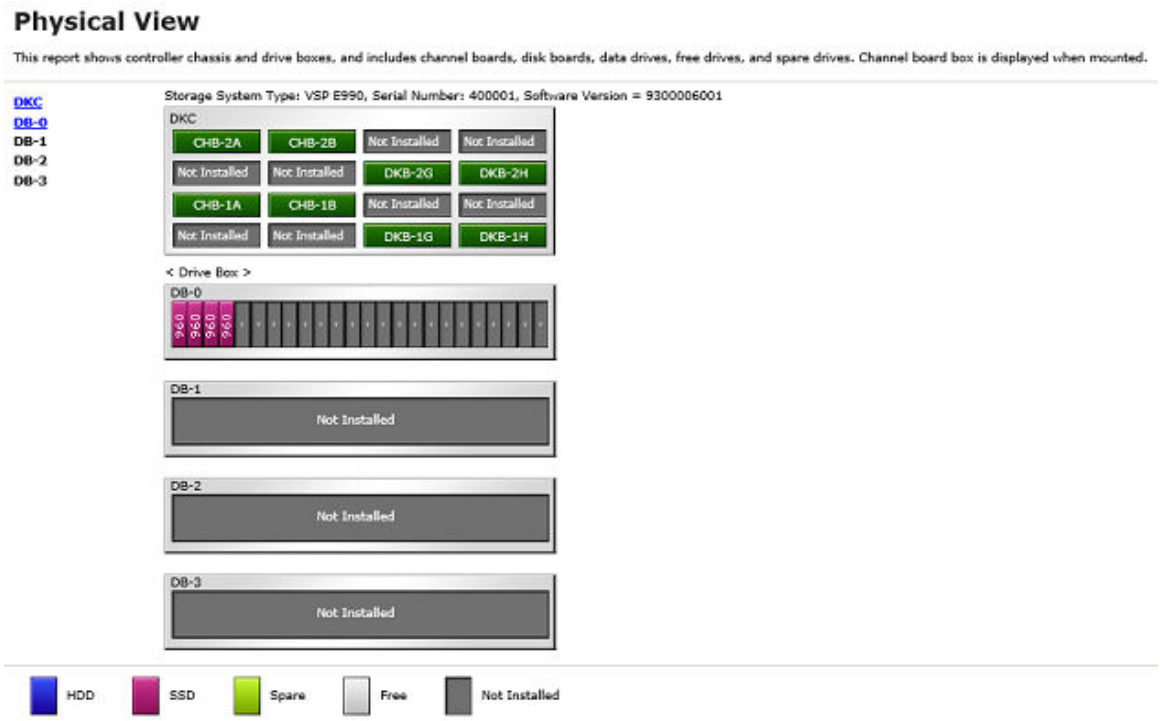


Figure 5 Physical View report

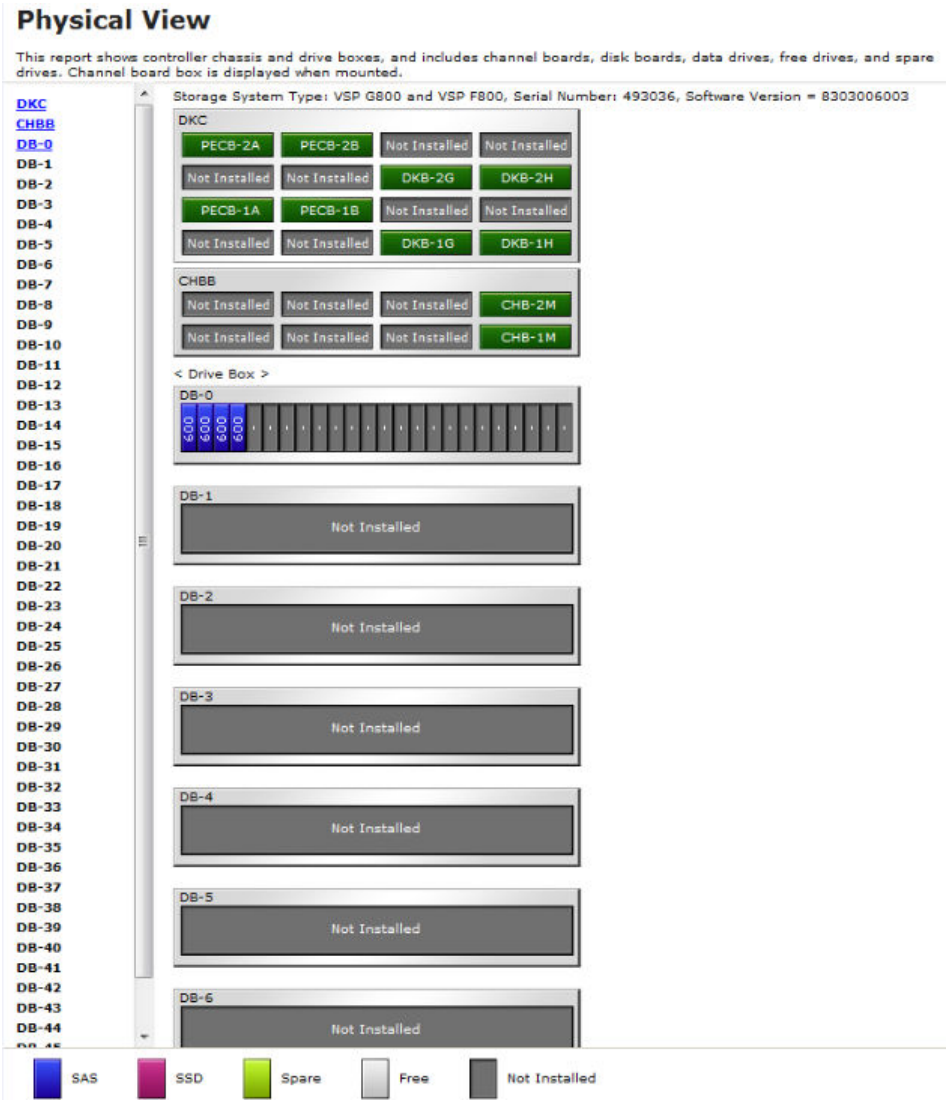


Figure 6 Physical View report (when a channel board box is connected)

Report examples: CSV files

Some Device Manager - Storage Navigator reports appear in CSV format. This topic describes reports that are saved in CSV format.

AllConf.csv

This is the concatenated file of all the csv files.

CacheInfo.csv

This CSV file contains information about the cache memory on the controller board. A record is created for each cache memory.

Item	Content
Location	Name of the cache controller board on which the memory is installed.
CMG#0 Size (GB) CMG#1 Size (GB)	Cache memory capacity in the controller board per CMG (32/64/128/256/ blank). CMG#0 Size and CMG#1 Size are displayed. Depending on the installed number of cache memory (DIMMs), one of the CMG capacities might be blank.
Cache Size (GB)	Total cache memory capacity on the controller board (0 to 512)
SM Size (MB)	The capacity that cannot be used as data cache memory in the total cache memory capacity inside of the controller board: ▪ VSP E590: 0 to 94976 ▪ VSP E790: 0 to 103168 ▪ VSP E990: 0 to 114432 ▪ VSP E1090: 0 to 130048 The capacity per cluster is displayed. Includes the shared memory capacity, cache directory capacity, and the fixed capacity. Fixed capacity is the cache memory capacity that is used for controlling the storage system with the controller board.
CFM#0 Type CFM#1 Type	Type of cache flash module (CFM) in the cluster: BM55, BM5E, BM65, BM6E, BM70, BM7E, blank. The number of CFM differs by model and the number of the displayed items are different. CFM#0 Type and CFM#1 Type are displayed. Depending on the installed CFM number, one of the CFM types might be displayed as blank.

ChapUserInfo.csv

This CSV file contains information about the iSCSI CHAP authenticated user registered to the port in the channel board. A record is created for each target related to the CHAP authenticated user.

Item	Content
Port	Port name
User Name	Name of the CHAP authenticated user[1]
iSCSI Target ID[2]	The iSCSI number of the target (00 to fe, hexadecimal)

Item	Content
Notes: **1.** If the character string contains a comma, the comma is converted to a tab. **2.** For the target information, see the record information with the same iSCSI target ID in IscsiTargetInfo.csv.	

ChaStatus.csv

This CSV file contains information about the status of each channel board (CHB). A record is created for each CHB.

Item	Content
CHB Location	CHB name
PCB Status	Status of this CHB*
Port#00, #01, …, #03	Status of ports on this CHB*
* 1: Normal, 0: Abnormal	

DeviceEquipInfo.csv

This CSV file contains information about equipment and devices that are part of the storage system, including DKC power supply, DB power supply, CHBB power supply, batteries, and BKMF. A record is created for each device.

Item	Content
Device Location	Device location name. For example: ▪ For DKCPS: DKCPS-00 ▪ For DKUPS: DKUPS000-1 ▪ For Battery: BATTERY-1BA ▪ For SVP: SVP-BASIC
Equip Status	Equipment status of the device: ▪ Equipped ▪ Not Equipped

Item	Content
Status	Status of the device: ▪ Normal ▪ Abnormal ▪ Blank if "Equip Status" is Not Equipped
Type	Type of the device: ▪ BKMF ▪ ACLF This item is blank if the device location name is not BKMF.

DkaInfo.csv

This CSV file contains information about disk boards (DKBs). A record is created for each DKB.

Item	Content
DKB Location	DKB name
Package Type	DKB type ▪ Unencryption DKB (2Port) ▪ Unencryption DKBN (2Port) ▪ Encryption EDKB (2Port) ▪ Encryption EDKBN (2Port) The supported DKB types differ depending on the storage system model.

DkaStatus.csv

This CSV file contains information about the status of disk boards (DKBs). A record is created for each DKB.

Item	Content
DKB Location	DKB name
PCB Status	Status of this DKB[1]
BECON#00	Status of BECON[1]

Item	Content
BEPORT#0000 to #0001	Status of BEPORT on this DKB[1] Items are output in the format BEPORT#*XXYY*, where: ▪ *XX*: BE controller number (2-digit hexadecimal) ▪ *YY*: BE port number (2-digit hexadecimal)
Notes: **1.** 1: Normal, 0: Abnormal	

DkcInfo.csv

This CSV file contains information about the DKC. A record is created for each module.

When Module #1 is not installed, the record for Module #1 is not created.

Item	Content
Storage System Type	Storage system type Output example: `VSP E990`
Serial Number #	Serial product number (decimal, from 400001 to 499999)
IP Address	IP address Output example: `xxx.xxx.xxx.xxx` (decimal, 0 to 255)
Subnet Mask	Subnet mask Output example: `xxx.xxx.xxx.xxx` (decimal, 0 to 255)
Number of CUs	Number of CUs (decimal, 0 to 255)
Number of DKBs	Number of DKBs (decimal, 0 to 8) Zero (`0`) is sometimes displayed if no drives are installed.
Configuration Type	Configuration type Output example: `PCM`
Model	Storage system model (for example, MH4)

DkuTempAveInfo.csv

This CSV file contains information about DB temperature for every two hours. A record is DB temperature information obtained from the environment monitor. A record output to the first line shows the latest temperature information. Because DB temperature information is measured by DBPS, items are displayed in this unit.

DkuTempAveInfo.csv shows the average temperature as DB temperature data. The maximum number of items depends on the storage system model:

- VSP E590 and VSP E790 with DBS2: 21
- VSP E590 and VSP E790 without expansion drive box: 17
- VSP E990: 9
- VSP E1090 with DBS2: 73
- VSP E1090 with DBN: 9
- VSP E1090 without expansion drive box: 65

The DB temperature data displayed in DkuTempAveInfo.csv (average temperature only), DkuTempMaxInfo.csv (maximum temperature only), and DkuTempMinInfo.csv (minimum temperature only) is the same value as the DB temperature data for DkuTempInfo.csv.

If the system is in maintenance mode or the SVP is rebooted, the data that is output every two hours might not contain data for the period. If a failure occurs in the storage system, the correct information might not be output.

Item	Description
Date	Year, month, and date when temperature data was acquired in the format: *YYYY*/*MM*/*DD hh*:*mm*:*ss*
DB00 DBPS001 Temperature average	Average temperature (°C) for the two-hour period of DB00 DBPS001
DB47 DBPS472 Temperature average	Average temperature (°C) for the two-hour period of DB47 DBPS472 For VSP E590 andVSP E790, this item shows up to DB61 DBPS612. For VSP E990, this item shows up to DB03 DBPS032. For VSP E1090, this item shows up to DB69 DBPS692.

Note: An item name is displayed as DB*xx* DBPS*xxy*. The names are listed in ascending order of the DB number. See DkuTempInfo.csv (on page 288) for locations and values for DB*xx* and DBPS*xxy*.

DkuTempInfo.csv

This CSV file contains information about DB temperature for every two hours. A record is DB temperature information obtained from the environment monitor. A record output to the first line shows the latest temperature information. Because DB temperature information is measured by DBPS, items are displayed in this unit.

DkuTempInfo.csv shows the average temperature, maximum temperature, and minimum temperature as DB temperature data. The maximum number of items depends on the storage system model:

- VSP E590 and VSP E790 with DBS2: 61
- VSP E590 and VSP E790 without expansion drive box: 49
- VSP E990: 25
- VSP E1090 with DBS2: 217
- VSP E1090 with DBN: 25
- VSP E1090 without expansion drive box: 193

The DB temperature data displayed in DkuTempAveInfo.csv (average temperature only), DkuTempMaxInfo.csv (maximum temperature only), and DkuTempMinInfo.csv (minimum temperature only) is the same value as the DB temperature data for DkuTempInfo.csv.

If the system is in maintenance mode or the SVP is rebooted, the data that is output every two hours might not contain data for the period. If a failure occurs in the storage system, the correct information might not be output.

An item name is displayed as DB*xx* DBPS*xxy*. The names are listed in ascending order of the DB number.

Item	Description
Date	Year, month, and date when temperature data was acquired in the format: *YYYY*/*MM*/*DD hh*:*mm*:*ss*
DB00 DBPS001 Temperature average	Average temperature (°C) for the two-hour period of DB00 DBPS001
DB00 DBPS001 Temperature maximum value	Maximum temperature (°C) for the two-hour period of DB00 DBPS001
DB00 DBPS001 Temperature minimum value	Minimum temperature (°C) for the two-hour period of DB00 DBPS001
DB47 DBPS472 Temperature average	Average temperature (°C) for the two-hour period of DB47 DBPS472 ▪ VSP E590 and VSP E790, this item shows up to DB61 DBPS612. ▪ For VSP E990, this item shows up to DB03 DBPS032. ▪ For VSP E1090, this item shows up to DB69 DBPS692.

Item	Description
DB47 DBPS472 Temperature maximum value	Maximum temperature (°C) for the two-hour period of DB47 DBPS472 ▪ VSP E590 and VSP E790, this item shows up to DB61 DBPS612. ▪ For VSP E990, this item shows up to DB03 DBPS032. ▪ For VSP E1090, this item shows up to DB69 DBPS692.
DB47 DBPS472 Temperature minimum value	Minimum temperature (°C) for the two-hour period of DB47 DBPS472 ▪ VSP E590 and VSP E790, this item shows up to DB61 DBPS612. ▪ For VSP E990, this item shows up to DB03 DBPS032. ▪ For VSP E1090, this item shows up to DB69 DBPS692.

The following tables list DB*xx* and DBPS*xxy*: *xx* values, where

- *xx* is a value from 00 to 61 for VSP E590 and VSP E790.
- *xx* is a value from 00 to 03 for VSP E990.
- *xx* is a value from 00 to 69 for VSP E1090.

DB #	0	1	2	… (omitted)	46	47
xx	00	01	02	...	46	47
DB*xx*	DB00	DB01	DB02	...	DB46	DB47
DB*xxy*	DBPS00y	DBPS01y	DBPS02y	...	DBPS46y	DBPS47y

The following table lists the DBPS*xxy: y* values (where DB# is 0 and *xx* is 00)

DB#	0	
y	1	2
DBPS*xxy: y*	DBPS001	DBPS002

DkuTempMaxInfo.csv

This CSV file contains information about DB temperature for every two hours. A record is DB temperature information obtained from the environment monitor. A record output to the first line shows the latest temperature information. Because DB temperature information is measured by DBPS, items are displayed in this unit.

DkuTempMaxInfo.csv shows the maximum temperature as DB temperature data. The maximum number of items depends on the storage system model:

- VSP E590 and VSP E790 with DBS2: 21
- VSP E590 and VSP E790 without expansion drive box: 17
- VSP E990: 9
- VSP E1090 with DBS2: 73
- VSP E1090 with DBN: 9
- VSP E1090 without expansion drive box: 65

The DB temperature data displayed in DkuTempAveInfo.csv (average temperature only), DkuTempMaxInfo.csv (maximum temperature only), and DkuTempMinInfo.csv (minimum temperature only) is the same value as the DB temperature data for DkuTempInfo.csv.

If the system is in maintenance mode or the SVP is rebooted, the data that is output every two hours might not contain data for the period. If a failure occurs in the storage system, the correct information might not be output.

An item name is displayed as DB*xx* DBPS*xxy*. The names are listed in ascending order of the DB number. See DkuTempInfo.csv (on page 288) for locations and values for DB*xx* and DBPS*xxy.*.

Item	Description
Date	Year, month, and date when temperature data was acquired in the format: *YYYY*/*MM*/*DD hh*:*mm*:*ss*
DB00 DBPS001 Temperature maximum value	Maximum temperature (°C) for the two-hour period of DB00 DBPS001
DB47 DBPS472 Temperature maximum value	Maximum temperature (°C) for the two-hour period of DB47 DBPS472 For VSP E590 and VSP E790, this item shows up to DB61 DBPS612. For VSP E990, this item shows up to DB03 DBPS032. For VSP E1090, this item shows up to DB69 DBPS692.

DkuTempMinInfo.csv

This CSV file contains information about DB temperature for every two hours. A record is DB temperature information obtained from the environment monitor. A record output to the first line shows the latest temperature information. Because DB temperature information is measured by DBPS, items are displayed in this unit.

DkuTempMinInfo.csv shows the minimum temperature as DB temperature data. The maximum number of items depends on the storage system model:

- VSP E590 and VSP E790 with DBS2: 21
- VSP E590 and VSP E790 without expansion drive box: 17
- VSP E990: 9
- VSP E1090 with DBS2: 73
- VSP E1090 with DBN: 9
- VSP E1090 without expansion drive box: 65

The DB temperature data displayed in DkuTempAveInfo.csv (average temperature only), DkuTempMaxInfo.csv (maximum temperature only), and DkuTempMinInfo.csv (minimum temperature only) is the same value as the DB temperature data for DkuTempInfo.csv.

If the system is in maintenance mode or the SVP is rebooted, the data that is output every two hours might not contain data for the period. If a failure occurs in the storage system, the correct information might not be output.

Item	Description
Date	Year, month, and date when temperature data was acquired in the format: *YYYY*/*MM*/*DD hh*:*mm*:*ss*
DB00 DBPS001 Temperature minimum value	Minimum temperature (°C) for the two-hour period of DB00 DBPS001
DB47 DBPS472 Temperature minimum value	Minimum temperature (°C) for the two-hour period of DB47 DBPS472 ▪ For VSP E590, VSP E790, this item shows up to DB61 DBPS612. ▪ For VSP E990, this item shows up to DB03 DBPS032. ▪ For VSP E1090, this item shows up to DB69 DBPS692.

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 about external volumes, see the *Hitachi Universal Volume Manager User Guide*.

Item	Content
VDEV#	Virtual device number to which the external volume is mapped
Characteristic1	Identification number of the external volume If the character string contains a comma, the comma is converted to a tab.
Characteristic2	Extended information for identifying the external volume
Device	Product name reported to the host by the external volume If the character string contains a comma, the comma is converted to a tab.
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 ▪ Enabled: Asynchronously ▪ Disabled: Synchronously
ECC Group	Number of parity group to which the external volume is mapped. If the number starts with "E" (for example, E1-1), the parity group contains external volumes. Range of values: E1-1 to E16384-4096
Current MPU	Number and name of a current MP unit controlling the parity group to which the external volume is mapped ▪ MPU-10 ▪ MPU-20
Setting MPU	Number and name of an MP unit configured to control the external volume indicated by ECC Group ▪ MPU-10 ▪ MPU-20
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

Item	Content
Path Mode	Mode which indicates how the paths between local and external storage systems operate ▪ Multi ▪ Single ▪ ALUA
Port	Name 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 This item is blank when the "Package Type" is iSCSI.
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 with the highest priority.
Status	Status of the path between storage systems. ▪ Normal ▪ Blocked
IO TOV	I/O timeout value for the external volume Range of values: 5 to 240
QDepth	The number of Read/Write commands that can be issued to the external volume at a time Range of values: 2 to 128
Resource Group ID (ECC Group)	Resource group ID for the parity group that is mapping external volumes (in decimal format) Range of values: 0 to 1023
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 ▪ Disabled ▪ - (hyphen): Single is specified in Path Mode.

Item	Content
Path Mode on Profile	Path mode on profile information of the external storage system: ▪ Multi ▪ Single
ALUA Settable	Indicates whether ALUA mode can be set as path mode on the external storage system ▪ Yes: ALUA mode can be set ▪ No: ALUA mode cannot be set
ALUA Permitted	Indicates whether ALUA is used as path mode on the local storage system: ▪ Enabled: ALUA mode is used ▪ Disabled: ALUA mode is not used
Target Port Asymmetric Access State	Status of the port on the external storage system when the path mode is ALUA: ▪ Active/Optimized ▪ Active/Non-Optimized ▪ Blank: The path mode is other than ALUA.
Package Type	Type of CHB to which a port of the local storage system connecting to the external storage system belongs: ▪ Output example for FC: 16FC2 (CHB), 32FC4R (CHB) ▪ Output example for iSCSI: 10iSCSI2o (CHB), 10iSCSI2c (CHB)
IP Address	IP address for an iSCSI target of an external storage system ▪ IPv6: *XXXX*:*XXXX*:*XXXX*:*XXXX*:*XXXX*:*XXXX*:*XXXX*:*XXXX* (hexadecimal) ▪ IPv4: *XXX*.*XXX*.*XXX*.*XXX* (decimal) ▪ Blank: The "Package Type" is other than iSCSI.
TCP Port Number	TCP port number (1 through 65535) for the iSCSI target of an external storage system This item is blank when the "Package Type" is other than iSCSI.
iSCSI Target Name	iSCSI target name of an external storage system This item is blank when the "Package Type" is other than iSCSI.

Item	Content
Virtual Port ID	Virtual port number of own storage system to which external storage system is connected. If Virtual Port Mode is Disabled, this column to be blanked.

EnvMonInfo.csv

This CSV file contains information about the power and temperature of the storage system. Power and temperature measurements from the environment monitor are recorded every 2 hours.

No records are created if the storage system is turned off. If the system is in maintenance mode or the SVP is rebooted, up to 2 hours of records could be lost.

If a failure occurs in the storage system, the correct information might not be output.

A hyphen(-) is displayed if the power and temperature information cannot be acquired due to a unit or network failure.

Item	Description
Date	Year, month, and date when record data was acquired for the 2-hour period in the format: *YYYY*/*MM*/*DD HH*:*MM*:*SS*
Electric power average	Average value of electric power (W)
Electric power maximum value	Maximum value of electric power (W)
Electric power minimum value	Minimum value of electric power (W) In the following cases, a lower value might be temporarily displayed: ▪ When the storage system is starting up ▪ Right after replacing storage system parts ▪ During or after microcode/firmware update
DKC0 CLT01 Temperature average	DKC0: Average temperature of CLT01 (°C)
DKC0 CLT01 Temperature maximum value	DKC0: Maximum temperature of CLT011 (°C)
DKC0 CLT01 Temperature minimum value	DKC0: Minimum temperature of CLT01 (°C)

Item	Description
DKC5 CLT52 Temperature average	DKC5 CLT52: Average temperature of CL2 (°C)
DKC5 CLT52 Temperature maximum value	DKC5 CLT52: Maximum temperature of CL2 (°C)
DKC5 CLT52 Temperature minimum value	DKC5 CLT52: Minimum temperature of CL2 (°C)

HduInfo.csv

This CSV file contains information about hard drive boxes (DB). A record is created for each drive box.

Note: Multiple DBs (for example, DB00&01) that are output to **DB Location** are DBs that have multiple DB information internally in one physical DB. For these DBs, one record is output for each DB information set although all records have the same contents. You can also check the **DB Location** output to this CSV in the *Physical View* report.

Example:

```
DB Location,DB Status,Slot Size,DB Type
DB00,Installed,2.5,DBN
DB50&51,Installed,2.5,DBS2
DB50&51,Installed,2.5,DBS2
DB52&53,Installed,2.5,DBS2
DB52&53,Installed,2.5,DBS2
DB54,Installed,3.5,DB60
DB55,Installed,3.5,DB60
DB56,Installed,3.5,DB60
DB57,Installed,3.5,DB60
DB58,Installed,3.5,DB60
DB59,Installed,3.5,DB60
DB60,Installed,3.5,DB60
DB61,Installed,3.5,DB60
```

Item	Description
DB Location	DB location name

Item	Description
DB Status	Information about whether this DB is installed ▪ Installed ▪ Not installed
Slot Size	Slot size (inches) ▪ 2.5 ▪ 3.5 ▪ Blank for DBF (FMD or FMD DC2).
DB Type	DB type ▪ DBS (DB for 2.5-inch drives) ▪ DBL (DB for 3.5-inch drives) ▪ DB60 (dense drive box for 3.5-inch drives) ▪ DBF (DB for FMD or FMD DC2, 2PORT) ▪ DBN (DB for 2.5-inch NVMe drives) ▪ DBS2 (DB for 2.5-inch drives)

IscsiHostInfo.csv

This CSV file contains information about iSCSI Initiator (Host) set to the channel board port. A record is created for each iSCSI Host (Initiator) target.

Item	Content
Port	Port name
iSCSI Name	iSCSI host name
Host Name	Nickname for iSCSI host name
iSCSI Target ID[1]	iSCSI target number (hexadecimal format, 00 to fe)

Notes:

1. For the target information, see the record information with the same iSCSI target ID in IscsiTargetInfo.csv.

IscsiPortInfo.csv

This CSV file contains information about iSCSI information set to the channel board port. A record is created for each iSCSI host (initiator) target.

Item	Content
Port	Port name
IPv4 | IP Address	IPv4 address Output example: *xxx.xxx.xxx.xxx* (decimal)
IPv4 | Subnet Mask	IPv4 subnet mask (decimal) Output example: *xxx.xxx.xxx.xxx* (decimal)
IPv4 | Default Gateway	Port IPv4 default gateway Output example: *xxx.xxx.xxx.xxx* (decimal)
IPv6 | Mode	Port IPv6 settings ▪ Enabled ▪ Disabled
IPv6 | Link Local Address	Port IPv6 link local address ▪ Output example: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal) ▪ Output example: Auto Auto is displayed if the link local address is automatically set. Blank if "IPv6 | Mode" is Disabled.
IPv6 | Global Address	IPv6 global address of the port ▪ Output example: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal) ▪ Output example: Auto Auto is displayed if the global address is automatically set. Blank if "IPv6 | Mode" is Disabled.
IPv6 | Assigned Default Gateway	Port IPv6 assigned default gateway ▪ Output example: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal) Blank if "IPv6 | Mode" is Disabled.
Channel Speed	Data transfer speed of the port (for example, 1G, 10G, Auto)
Security Switch	Port security switch settings ▪ On ▪ Off
TCP Port Number	The number of the port for using socket (1 to 65535)

Item	Content
Ethernet MTU Size (Byte) | MTU	MTU settings ▪ 1500 ▪ 4500 ▪ 9000
Keep Alive Timer (sec.)	Keep alive timer value of iSCSI (30 to 64800) (sec)
Selective ACK	Selective ACK mode ▪ Enabled ▪ Disabled
Delayed ACK	Delayed ACK mode ▪ Enabled ▪ Disabled
Maximum Window Size (KB)	Window scale option settings ▪ 64KB ▪ 128KB ▪ 256KB ▪ 512KB ▪ 1024KB
iSNS Server | Mode	iSNS mode settings ▪ On ▪ Off
iSNS Server | IP Address	IP address of the iSNS server ▪ IPv4: *xxx.xxx.xxx.xxx* (decimal) ▪ IPv6: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal) ▪ Blank if "iSNS Server | Mode" is Off.
iSNS Server | TCP Port Number	Port number of TCP used for iSNS (1 to 65535). Blank if "iSNS Server | Mode" is Off.
VLAN | Tagging Mode	VLAN tagging mode set to the port ▪ On ▪ Off
VLAN | ID	VLAN number set to the port (1 to 4094) Blank if "VLAN | Tagging Mode" is set to Off.

Item	Content
Resource Group ID (Port)	Resource group ID of the port (0 to 1023 in decimal)
Resource Group Name(Port)	Resource group name of the port
iSCSI Name	iSCSI name of the port
CHAP User Name	Authenticated user name of the port
IPv6 | Global Address 2	IPv6 global address 2 of the port ▪ Output example: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal) ▪ Output example: Auto Auto is displayed if the global address 2 is automatically set. Blank if "IPv6 | Mode" is Disabled.
Virtual Port Mode	Virtual port mode of the port ▪ Enabled ▪ Disabled

IscsiTargetInfo.csv

This CSV file contains information about iSCSI target information set to the channel board port. A record is created for each iSCSI target.

Item	Content
Port	Port name
iSCSI Target Alias	iSCSI target alias
iSCSI Target ID	Number of the iSCSI target (00 to fe, hexadecimal)
iSCSI Target Name	Name of the iSCSI target
Host Mode	Host mode set to the iSCSI target (hexadecimal)
Host Mode Option	Host mode option set to the iSCSI target (decimal) Separated with a semicolon (;) if multiple host mode options are set.
Security Switch	Security switch status set to the iSCSI target port ▪ On ▪ Off

Item	Content
Authentication | Method	Authentication method settings of the iSCSI target ▪ CHAP ▪ None ▪ Comply with Host Setting
Authentication | Mutual CHAP	Mutual CHAP authentication function settings of the iSCSI target ▪ Enabled ▪ Disabled
Authentication | User Name	User name set when iSCSI target was authenticated
Resource Group ID (iSCSI Target)	Resource group ID of the iSCSI target (0 to 1023)
Resource Group Name (iSCSI Target)	Resource group name of the iSCSI target

JnlInfo.csv

This CSV file contains information about journals. A record is created for each journal.

Item	Content
JNL#	Journal number (in hexadecimal)
Current MPU	Number and name of MP unit currently controlling the journal (MPU-10, MPU-20)
Setting MPU	Number and name of MP unit configured to control the journal (MPU-10, MPU-20)

LdevCapaInfo.csv

This CSV file contains information about LDEV capacities. A record is created for each of the classifications shown in "Volume Kind".

Item	Content
Volume Kind	The following classifications are output: ▪ Internal OPEN Volumes ▪ External OPEN Volumes ▪ Total OPEN Volumes
Allocated LDEV Capacity (GB)	Allocated LDEV capacity
Unallocated LDEV Capacity (GB)	Unallocated LDEV capacity
Reserved Capacity (GB)	Reserved LDEV capacity
Total Volume Capacity (GB)	Total capacity of "Allocated LDEV Capacity", "Unallocated LDEV Capacity" and "Reserved Capacity"
Free Space (GB)	Free Space
Total Capacity (GB)	Total Capacity The sum of "Total Volume Capacity" and "Free Space"

LdevCountInfo.csv

This CSV file contains information about the number of logical devices (LDEVs). A record is created for each of the classifications shown in "Volume Kind".

Item	Content
Volume Kind	The following classifications are output: ▪ Internal Volumes ▪ External Volumes ▪ Total Volumes
Allocated OPEN LDEVs	Number of allocated open-system volumes (LDEVs)
Unallocated OPEN LDEVs	Number of unallocated open-system volumes (LDEVs)
Reserved OPEN LDEVs	Number of reserved open-system volumes (LDEVs)
V-VOL	Number of virtual volumes This item is output only when "Volume Kind" is Total Volumes. This item is blank when "Volume Kind" is Internal Volumes or External Volumes.

Item	Content
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.

Item	Content
ECC Group	Number of parity group where the LDEV belongs. Output example: *X*-*Y* (decimals) ▪ If the number starts with "E" (for example, E1-1), the parity group contains external volumes. ▪ If "LDEV Type" is Dynamic Provisioning or Thin Image, a hyphen is output.
LDEV#	LDEV number (00:00:00 to 00:fe:ff)
LDEV Name	LDEV name If the character string contains a comma, the comma is converted to a tab.
LDEV Emulation	LDEV emulation type
LDEV Type	LDEV type: ▪ Basic ▪ Dynamic Provisioning ▪ External ▪ Thin Image ▪ ALU

Item	Content
LDEV Attribute	LDEV Attribute: ▪ CMDDEV (Command device) ▪ CMDDEV (Remote command device) If the character string contains a comma, the comma is converted to a tab. ▪ Journal (Journal volume) ▪ Pool (Pool volume) ▪ Quorum disk (used with global-active device) ▪ ALU ▪ SLU ▪ Deduplication system data volume (fingerprint) ▪ Deduplication system data volume (data store) ▪ Nondisruptive migration ▪ Regular (Others)
Volume Size(Cyl)	LDEV capacity (in cylinders) **Note:** This item is not applicable (the output value is not valid).
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: ▪ On: Custom-sized volume ▪ Off: Others
Pool ID	Pool number. This item is blank except in the following cases: ▪ If the 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. Blank if the parity group is not concatenated to another parity group.
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.
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.

Item	Content
ORACLE CHECK SUM	Information about whether this LDEV is an Oracle checksum target. ▪ On ▪ Off
Current MPU	Number of the MP unit currently controlling the LDEV. (MPU-10, MPU-20)
Setting MPU	Number of the MP unit configured to control LDEV. (MPU-10, MPU-20)
Allocated	Information about whether the host can access the LDEV. ▪ Y: The host can access the volume. ▪ N: The host cannot access the volume.
Pool Name	Name of the pool: ▪ If the provisioning type is Dynamic Provisioning, the name of the pool related to the logical volume is displayed. If the character string contains a comma, the comma is converted to a tab. ▪ If the attribute is Pool, the name of the pool to which the logical volume belongs is displayed. If the character string contains a comma, the comma is converted to a tab. ▪ When neither of the above is displayed, the pool name is blank.
CmdDevSecurity	Indicates whether Security is specified as the attribute for the command device. ▪ Enabled: Command device security setting is set. ▪ Disabled: Command device security setting is not set. ▪ Blank: "LDEV Attribute" is not CMDDEV.
CmdDevUserAuth	Indicates whether User Authentication is specified as the attribute for the command device. ▪ Enabled: User authentication setting is set. ▪ Disabled: User authentication setting is not set. ▪ Blank: "LDEV Attribute" is not CMDDEV.

Item	Content
CmdDevDevGrpDef	Indicates whether Device Group Definition is specified as the attribute for the command device. ▪ Enabled: Device group definition setting is set. ▪ Disabled: Device group definition setting is not set. ▪ Blank: "LDEV Attribute" is not CMDDEV.
Resource Group ID (LDEV)	LDEV resource group ID (number in the decimal format)
Resource Group Name (LDEV)	LDEV resource group name (0 to 1,023, decimal)
Encryption	Indicates whether the parity group identified by ECC Group is encrypted. ▪ For internal volumes: Enabled (encrypted) or Disabled (not encrypted) ▪ For external volumes: blank
T10 PI	T10 PI attribute set for the LDEV: ▪ Enabled ▪ Disabled ▪ Blank if "LDEV Emulation" is not OPEN-V.
ALUA Mode	Indicates whether the ALUA mode is enabled. ▪ Enabled: ALUA mode is enabled. ▪ Disabled: ALUA mode is disabled.
Accelerated Compression	Indicates whether accelerated compression is enabled. For internal volumes: ▪ Enabled: accelerated compression is enabled. ▪ Disabled: accelerated compression is disabled. If the parity group with LDEV does not support accelerated compression, a blank space is displayed. Also, for external volumes, a blank is displayed.

LdevStatus.csv

This CSV file contains information about the status of logical devices (LDEVs). A record is created for each LDEV.

Item	Content
VDEV#	Virtual device number in which the LDEV is defined

Item	Content
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 the parity group where the LDEV belongs. ▪ If the number starts with "E" (for example, E1-1), the parity group contains external volumes. ▪ If the type of the LDEV is a Dynamic Provisioning or Thin Image virtual volume, a hyphen is output. Refer to "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 about the cache logical partitioning function, see the *Performance Guide*.

Item	Content
CLPR#	CLPR ID (in decimal)
CLPR Name	CLPR name
Cache Size(MB)	Cache size allocated to this CLPR (in MB)
ECC Group	Number of parity group allocated to this CLPR ▪ If the number starts with "E" (for example, E1-1), the parity group contains external volumes. ▪ If the type of the LDEV is a Dynamic Provisioning or Thin Image virtual volume, a hyphen (-) is output. Refer to "LdevInfo.csv" for information about the LDEV type.

Item	Content
LDEV#(V-VOL)	LDEV number allocated to this CLPR: ▪ VSP E590: 00:00:00 to 00:7f:ff ▪ VSP E790: 00:00:00 to 00:bf:ff ▪ VSP E990: 00:00:00 to 00:fe:ff ▪ VSP E1090: 00:00:00 to 00:fe:ff The type of this LDEV is Dynamic Provisioning, Thin Image, or ALU. This item is blank if no LDEV is assigned to the CLPR ID.

LunInfo.csv

This CSV file contains information about LU path definitions. A record is created for each set of LU path definitions that belongs to a host group. When only the port name (Port) is output, it indicates that no LU path is defined for the port (which is used only for a remote path or an external path). For more information about LU path definitions, see the *Provisioning Guide*.

Item	Description
Port	Port name
Host Group	Host group name If "Package Type" is iSCSI, the iSCSI target alias is output.
Host Mode	Host mode specified for this host group (hexadecimal)
Host Mode Option	Host mode option set for this host group (decimal) If more than one option is specified, the options are separated by semicolons (;). This item is blank when no host mode option has been specified.
LUN#	LUN number for this LU path definition (hexadecimal) This item is blank when no LU path is defined for the host group.
LDEV#	LDEV number for this LU path definition This item is blank when no LU path is defined for the host group.
Command Device	Information about whether the LDEV is a command device: ▪ On: Command Device ▪ On*: Remote Command Device ▪ Off: Others ▪ Blank: No LU path is defined for the host group.

Item	Description
Command Security	Information about whether the command device is secured: ▪ On ▪ Off ▪ Blank: No LU path is defined for the host group.
CVS	Information about whether the LDEV is a custom-sized volume: ▪ On: Customized volume ▪ Off: Other volumes ▪ Blank: No LU path is defined for the host group.
CHB Location	Name of the CHB on which this port is installed Output example: CHB-1D
Package Type	CHB type for CHB Location Output example for Fibre: 32FC4R (CHB) Output example for iSCSI: 10iSCSI2c (CHB)
Resource Group ID (Host Group)	Resource group ID of a host group (0 to 1,023, decimal)
Resource Group Name (Host Group)	Resource group name of a host group
T10 PI Mode	Indicates whether the T10 PI mode can be applied to the port for which the LU path is defined: ▪ Enabled ▪ Disabled ▪ Blank: "Package Type" does not support T10 PI mode.
T10 PI	Information about the T10 PI attribute which is set for the LDEV number of the LU path definition. ▪ Enabled ▪ Disabled ▪ Blank: The LDEV# is blank.
Asymmetric Access State	Asymmetric access status Indicates the asymmetric access status: ▪ Active/Optimized: Prioritized ▪ Active/Non-Optimized: Lower priority ▪ Blank: "Package Type" is iSCSI

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 the *Provisioning Guide*.

Item	Content
Port	Port name
Security Switch	The setting status of the security switch: ▪ On ▪ Off
Port Address	Port address (2-digit hexadecimal number) 00 to ff This item is blank when "Package Type" is iSCSI.
Loop ID	Port address (0 - 125, decimal) This item is blank when "Package Type" is iSCSI.
Fabric	Setting status of the Fabric switch: ▪ On ▪ Off ▪ Blank: "Package Type" is iSCSI.
Connection	Fibre topology setting: ▪ Point to Point ▪ FC-AL ▪ Blank: "Package Type" is iSCSI.
Channel Speed	Channel speed of this port (for example, 4G, 10G, 32G)
WWN	WWN of this port (hexadecimal number) This item is blank when "Package Type" is iSCSI.
CHB Location	CHB on which the port is installed.
Package Type	CHB type for CHB Location Output example for Fibre: 32FC4R (CHB) Output example for iSCSI: 10iSCSI2c (CHB)
T10 PI Mode	Indicates whether the T10 PI mode can be applied to the port: ▪ Enabled ▪ Disabled ▪ Blank: "Package Type" does not support T10 PI mode.

MicroVersion.csv

This CSV file contains information about software versions.

Table 10 Software versions for VSP E590, VSP E790

Item	Content
DKCMAIN	The version of the firmware for the RAID storage system (10 digits)
ROM BOOT	ROM BOOT firmware version (6 digits)
RAM BOOT	RAM BOOT firmware version (6 digits)
Config	Config version (8 digits)
HDD	HDD firmware version (4 digits) Displayed in HDD device type cord: version format. A colon is displayed when no HDDs are installed.
CFM	CFM firmware version (8 digits)
Printout Tool	Printout tool version (*xx-yy-zz-mm/aa*)
CHB(FC32G)	32G FC protocol chip firmware version (8 digits)
CHB(iSCSI)	CHB9(iSCSI) protocol chip firmware version (8 digits)
GUM	GUM firmware version (8 digits)
CTL_NSW	CTL_NSW firmware version (6 digits)
CTL_eDKBN	CTL_eDKBN firmware version (6 digits)
Expander[1]	Expander firmware version (6 digits)
DKB[1]	DKBN firmware version (6 digits)
DKBN[2]	DKBN firmware version (6 digits) (not supported on VSP E590, VSP E790)
NSW[2]	NSW firmware version (6 digits) (not supported on VSP E590, VSP E790)
Notes: **1.** These items are output only when the firmware version is 93-05-02 or later. **2.** These items are output only when the firmware version is 93-06-21 or later.	

Table 11 Software versions for VSP E990

Item	Content
DKCMAIN	The version of the firmware for the RAID storage system (10 digits)
ROM BOOT	ROM BOOT firmware version (6 digits)
RAM BOOT	RAM BOOT firmware version (6 digits)
Config	Config version (8 digits)
HDD	HDD firmware version (4 digits) A colon is displayed for VSP E990.
CFM	CFM firmware version (8 digits)
Printout Tool	Printout tool version (*xx-yy-zz-mm/aa*)
CHB(FC32G)	32G FC protocol chip firmware version (8 digits)
CHB(iSCSI)	CHB9(iSCSI) protocol chip firmware version (8 digits)
GUM	GUM firmware version (8 digits)
DKBN	DKBN firmware version (6 digits)
NSW	NSW firmware version (6 digits)
EDKBN	EDKBN firmware version (6 digits)

Table 12 Software versions for VSP E1090

Item	Content
DKCMAIN	The version of the firmware for the RAID storage system (10 digits)
ROM BOOT	ROM BOOT firmware version (6 digits)
RAM BOOT	RAM BOOT firmware version (6 digits)
Config	Config version (8 digits)
HDD	HDD firmware version (4 digits) Displayed in HDD device type cord: version format. A colon is displayed when no HDDs are installed.
CFM	CFM firmware version (8 digits)
Printout Tool	Printout tool version (*xx-yy-zz-mm/aa*)
CHB(FC32G)	32G FC protocol chip firmware version (8 digits)

Item	Content
CHB(iSCSI)	CHB9(iSCSI) protocol chip firmware version (8 digits)
GUM	GUM firmware version (8 digits)
DKB	DKB firmware version (6 digits)
DKBN	DKBN firmware version (6 digits)
NSW	NSW firmware version (6 digits)
EDKBN	EDKBN firmware version (6 digits)
Expander	Expander firmware version (6 digits)

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.

Item	Content
ECC Group	Number of parity groups of which this MLC (including FMD and FMD DC2) is a component. ▪ If it is a spare drive, Spare Drive is displayed. ▪ If it is a free drive, Free Drive is displayed.
CR#	C# and R# (2-digit hexadecimal numbers), which identify the PDEV Output in the format of "*XX*/*YY*" *XX*: C# *YY*: R#
Device Type-Code	Drive type code of this drive Output example: SLR5A-M800SS
Used Endurance Indicator (%)	The current used endurance of SSD life (0 to 100) The value of this indicator increases due to drive operation associated with internal processing of the storage system, and the host I/O. Even when no data is copied due to a drive failure, the value of this indicator increases because the spare drive also performs internal processing.
History1 (date)	Date on which the used endurance of SSD life was acquired (1 month ago) Output example: *yyyy*/*mm*/*dd*

Item	Content
History1 (%)	The used endurance of SSD life (0 to 100)(1 month ago)
History2 (date)	Date on which the used endurance of SSD life was acquired (2 months ago) Output example: *yyyy*/*mm*/*dd*
History2 (%)	The used endurance of SSD life (0 to 100) (2 months ago)
History3 (%) ... History 119 (%)	Life (0 to 100) (3 months ago ...119 months ago)
History120 (date)	Date on which the used endurance of SSD life was acquired (120 months ago) Output example: yyyy/mm/dd
History120 (%)	The used endurance of SSD life (0 to 100) (120 months ago)

ModePerLpr.csv

This CSV file contains information about system option modes. A record is created for each system option mode.

Item	Content
System Option Mode#	System option mode # (0 to 2047, decimal number)
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 blade or LR.

Item	Content
MPU#/CTL#	MP unit number or CTL number (2-digit hexadecimal number) ▪ For MP unit number: MPU#00 to MPU#01 ▪ For CTL number: CTL#00 to CTL#01

Item	Content
CMG#00-00 to 01 CMG#01-00 to 01	Path status* for the MP unit number with the cache module (CMG#*XX*-*YY*) *XX*: I path, *YY*: CMG#
MPU#00-00 to 01 MPU#01-00 to 01	Path status* and the MP unit for the MP unit number (MPU#*XX*-*YY*) *XX*: I path, *YY*: MPU#
CMG#00-00 to 01 CMG#01-00 to 01	Path status* with the cache module for the CTL number (CMG#*XX*-*YY*) *XX*: I path, *YY*: CMG#
MPU#00-00 to 01 MPU#01-00 to 01	Path status* with the MP unit number for the CTL number (MPU#*XX*-*YY*) *XX*: I path, *YY*: MPU#
* Path status: 1=Normal, 0=Abnormal	

MpPcbStatus.csv

This CSV file contains information about the status of MP Unit. A record is created for each MP unit.

Item	Content
MPU ID	MP unit ID (MPU-10, MPU-20)
Auto Assignment	Information about whether this MP unit is set to be automatically assigned to each resource. ▪ Enabled: Set to be automatically assigned ▪ Disabled: Not set to be automatically assigned
MPU Status	MP unit status: ▪ 1=Normal ▪ 0=Abnormal
MP#00, #01, …, #13	MP status ▪ 1=Normal ▪ 0=Abnormal The number of output items depends on the number of installed MPs: ▪ VSP E590: MP#00,01,…,0b ▪ VSP E790: MP#00,01,…,1f ▪ VSP E990: MP#00,01,…,1b ▪ VSP E1090: MP#00,01,…,1f

PcbRevInfo.csv

This CSV file contains information about revisions of packages such as channel boards (CHBs) and others. A record is created for each package.

Item	Content
Cluster#	Cluster number 1 or 2
Location	Part name
FRU number	Product name of the package or some other name
PK Revision	Revision of the package
Factory	Factory manufacturing the package
Number	Serial number of the package
MAC Address	MAC address of the package This item always remains blank.

PdevCapaInfo.csv

This CSV file contains information about physical device (PDEV) capacities. A record is created for each of the classifications shown in "PDEV Kind".

Item	Content
PDEV Kind	The following four classifications are output: ▪ OPEN System (TB) ▪ Total Capacity (TB) ▪ Number of PDEVs
HDD Drive	HDD drive capacity (TB)
Spare Drive	Spare drive capacity (TB)
SSD Drive	SSD capacity (TB)
Free Drive	Free drive capacity (TB)

PdevInfo.csv

This CSV file contains information about physical devices (PDEVs). A record is created for each PDEV.

Item	Content
ECC Group	Number of parity group of which this PDEV is a component: ▪ Spare Drive: For spare drives ▪ Free Drive: For free drives
Emulation Type	Emulation type for the parity group indicated by "ECC Group" This item is blank when the ECC Group is Spare Drive.
CR#	C# and R# (2-digit hexadecimal numbers that identify the PDEV) Output in the format *XX*/*YY*, where: ▪ *XX*: C# ▪ *YY*: R#
PDEV Location	PDEV location name
Device Type	Drive type (for example, SAS, SSD)
RPM	Revolutions per minute (unit: rpm) This item is blank when the drive type is not HDD.
Interface	Drive control interface (for example, NVMe, SAS)
Device Type-Code	Device type code of this drive (for example, DKR5D-J600SS)
Device Size	Drive size (inches) (for example, 2.5, 3.5) This item is blank when the drive type is FMD.
Device Capacity	Drive capacity (GB or TB)
Drive Version	Drive firmware version
DKB1	Name of the DKB1 controlling the PDEV
DKB2	Name of the DKB2 controlling the PDEV
DKB3	Name of the DKB3 controlling the PDEV This item is output only for VSP E990 and VSP E1090.
DKB4	Name of the DKB4 controlling the PDEV This item is output only for VSP E990 and VSP E1090.
Serial Number #	Serial number of this drive
RAID Level	RAID level of the parity group indicated by "ECC Group" This item is blank when the "ECC Group" is Spare Drive or Free Drive

Item	Content
RAID Concatenation #0	Number of parity group to be concatenated to parity group (#0) identified by "ECC Group" This item is blank when 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" This item is blank when 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" This item is blank when 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 (decimal number)
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 is enabled. ▪ Disabled: Encryption is disabled.
Accelerated Compression	Accelerated compression setting: ▪ Enabled: Accelerated compression is enabled. ▪ Disabled: Accelerated compression is disabled. This item is blank when the parity group with PDEV does not support accelerated compression, or when the ECC Group is Spare Drive.
Automatically manage compressed space of FMD parity group	Indicates whether to manage the compressed area of the FMD parity group automatically. ▪ Enabled: The area is managed automatically. ▪ Disabled: The area is not managed automatically This item is blank when the parity group to which the PDEV belongs does not support accelerated compression.

PdevStatus.csv

This CSV file contains information about the status of physical devices (PDEVs). A record is created for each PDEV.

Item	Content
CR#	C# and R# (2-digit hexadecimal numbers), which identify the PDEV Output in the format *XX*/*YY*, where: ▪ *XX*: C# ▪ *YY*: R#
Pdev Status	PDEV status[1]
Port0 Status	Status of Port 0 on this PDEV[1]
Port1 Status	Status of Port 1 on this PDEV[1]
Pdev Location	Location name of this PDEV
Notes: **1.** 1=Normal, 0=Abnormal	

PECBInfo.csv

This CSV file contains information about the PECB (PCIe channel board) and connecting destination.

For VSP E590 and VSP E790, a hyphen (-) is output for all items.

Item	Content
Location	PECB location name
Status	Whether the PECB is installed ▪ Installed ▪ Not Installed
Type	Destination module type of the PECB ▪ CHBB
Expansion mode	Expansion mode set in the destination module of the PECB

PkInfo.csv

This CSV file contains information about channel boards (CHBs). A record is created for each CHB.

Item	Content
CHB Location	CHB name
Port#	Number of the port installed on the CHB (2-digit hexadecimal number), 00 to ff
Port	Name of port installed on the CHB
Package Type	CHB type indicated on the CHB Location Output examples for FC: 16FC2 (CHB), 32FC4R (CHB) Output examples for iSCSI: 10iSCSI2o (CHB), 10iSCSI2c (CHB)
SFP Kind	Type of SFP (Small Form factor Pluggable): ▪ Short Wave ▪ Long Wave ▪ Blank: The CHB type is iSCSI.
SFP Status	SFP Status: ▪ Normal ▪ Failed ▪ Not Fix ▪ Blank: The CHB type is iSCSI.
Fabric	Fibre topology settings indicating the setting status of the Fabric switch: ▪ On ▪ Off ▪ Blank: The CHB type is iSCSI.
Connection	Fibre topology settings: ▪ Point to Point ▪ FC-AL ▪ Blank: The CHB type is iSCSI.
Port Address	Port address (00 to ff, 2-digit hexadecimal number) This item is blank when the CHB type is iSCSI.
Resource Group ID (Port)	Resource group ID of port (0 to 1023, decimal number)
Resource Group Name (Port)	Resource group name of the port
Port Internal WWN	Port WWN

Item	Content
	This item is blank when the CHB type is iSCSI.
T10 PI Mode	Indicates whether the T10 PI mode can be applied to the port: ▪ Enabled ▪ Disabled ▪ Blank: The CHB does not support T10 PI mode.
SFP Data Transfer Rate	Maximum transfer rate of SFP which the mounted package supports, for example, 10G, 32G. This item is blank when the CHB type is iSCSI.

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 Managing license keys (on page 199).

Item	Content
Program Product Name	Software name
Install	Information about whether the installed license key is enabled: ▪ Enabled: Installed and the software can be used. ▪ Disabled: Installed but the software cannot be used.
Key Type	Installed license key type: ▪ Permanent ▪ Temporary ▪ Emergency ▪ Term ▪ Not Installed: No license key is installed.
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. This item is blank in either of the following cases: ▪ A new license key whose "Key Type" is Temporary or Emergency has been installed. ▪ No license key has been installed.

Item	Content
Expiration Date	Expiration date of the software The format is *mm*/*dd*/*yyyy* (month/day/year). This item is blank in either of the following cases: ▪ The effective term of the license key is unlimited. ▪ No license key has been installed.
Status	License key status of the software: ▪ Installed ▪ Not Enough License ▪ Grace Period ▪ Expired ▪ Not Installed ▪ Installed (Disabled)

SMfundat.csv

This CSV file contains information about SM functions. A record is created for each of the classifications shown in "SM Install Function".

Item	Content
SM Install function	The following classifications are output: **1.** Base **2.** Extension1 **3.** Extension2 **4.** Extension3 **5.** Extension4
Availability	Information about whether the function of "SM Install function" is enabled ▪ Enabled ▪ Disabled

SsdDriveInfo.csv

This CSV file contains information about SSDs. A record is created for each drive.

Item	Content
ECC Group	Number of the parity group to which this SSD belongs ▪ Spare Drive: The SSD is a spare drive. ▪ Free Drive: The SSD is a free drive.
CR#	C# and R# (2-digit hexadecimal numbers that identify the PDEV) Output in the format *XX*/*YY*, where: ▪ *XX*: C# ▪ *YY*: R#
PDEV Location	Drive type code of the PDEV location name for this drive
Device Type-Code	Drive type code Output example: SLR5A-M800SS
Device Capacity	Drive capacity in GB or TB
SSD Device Type	SSD drive type (for example, SSD(RI), MLC, FMD)
Used Endurance Indicator (%)	Used endurance of SSD life (0 to 100)
Used Endurance Indicator Threshold (%)	Drive life threshold (0 to 100)
Used Endurance Indicator Warning SIM (%)	Warning SIM threshold (0 to 100)
FMD Battery Life Indicator Warning SIM (%)	Threshold of battery life warning SIM (0 to 100) This item is blank if the SSD is other than FMD.
FMD Battery Life Indicator (%)	Used battery life (0 to 100) This item is blank if the SSD is other than FMD.

SsidInfo.csv

This CSV file contains information about SSIDs. A record is created for each SSID.

Item	Content
DEV# Start	First LDEV number for the SSID
DEV# End	Last LDEV number for the SSID

Item	Content
SSID	Subsystem ID (hexadecimal)

SysoptInfo.csv

This CSV file contains information about system options.

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. Output example: mode*XXXX* (0 to 2047, decimal number)
Link Failure Threshold	Threshold to notify the link failure (0 to 255, decimal)

WwnInfo.csv

This CSV file contains information about hosts. A record is created for each host.

Item	Content
Port	Port name.

Item	Content
Host Group	Host group name iSCSI target alias is output if the "Package Type" is iSCSI.
Host Mode	Host mode that is set for the host group (hexadecimal)
Host Mode Option	Host mode option that is set for the host group (decimal) Multiple options are separated by semicolons (;). This item is blank when no host mode options have been specified.
WWN	World Wide Name of the host bus adapter registered to the host group (hexadecimal number) This item is blank when no valid WWN has been specified.
Nickname	Nickname of the host This item is blank when no nickname has been specified.
Host Group#	Host group number (00 to fe, hexadecimal number) The iSCSI target ID is output when the "Package Type" is iSCSI.
CHB Location	Name of port installed on the CHB
Package Type	CHB type indicated on the CHB Location Output example for FC: 16FC2 (CHB), 32FC4R(CHB) Output example for iSCSI: 10iSCSI2o (CHB), 10iSCSI2c (CHB)
T10 PI Mode	Indicates whether the T10 PI mode can be applied to the port: ▪ Enabled ▪ Disabled ▪ Blank: "Package Type" does not support T10 PI mode.

Appendix B: SMI-S provider configuration file

To use this SMI-S function you must create a SMI-S provider configuration file. This section describes the SMI-S provider configuration files.

Array-setting-01.properties file

The array-setting-01.properties file is an SMI-S provider user configuration file. This section describes the description format and organization format of SMI-S provider user configuration files and parameters to be defined.

File description format

The format of the array-setting-01.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 array-setting-01.properties file is shown here:

```
# comment line
   parameter1= parameter1_setting_value
  parameter2= parameter2_setting_value
# comment line
```

Parameters defined in user configuration files

The following table describes the parameters can be specified in user configuration files.

All parameters are optional. If no value is specified for a parameter, the default value applies.

Parameter name	Description
ResourceGroup	Specifies the resource groups that the SMI-S provider can use. For details, see ResourceGroup parameter (on page 328).
PullOperationMaxTime	Specifies the timeout value for Pull Operation. This parameter is optional. If the timeout value is not specified, the default value applies. For details, see PullOperationMaxTime parameter (on page 328).

ResourceGroup parameter

Use the ResourceGroup parameter to specify resource groups that the SMI-S provider can use.

All resource groups are specified by default.

Setting up the ResourceGroup parameter

Set up the parameter by using <RangeOfResourceGroupID> and <SingleResourceGroupID> with a comma (,) as a delimiter:

- <RangeOfResourceGroupID>: Specifies a range of resource group IDs
- <SingleResourceGroupID>: Specifies a single resource group ID

<RangeOfResourceGroupID> format

<Start ResourceGroupID>to<End ResourceGroupID>

- <Start ResourceGroupID>: ID of the first resource group in the specified range
- <End ResourceGroupID>: ID of the last resource group in the specified range

<SingleResourceGroupID> format

<ResourceGroupID>

- <ResourceGroupID>: ID of the resource group to be specified

Example

```
ResourceGroup=1to2,4,6to8
```

In this example, resource groups having one of the following resource group IDs are used:

- 1, 2, 4, 6, and 8

PullOperationMaxTime parameter

Use the PullOperationMaxTime parameter to specify the timeout value for the Pull Operation.

Setting up the PullOperationMaxTime parameter

- The setting unit is minute.
- If this parameter is not specified, the default timeout value is 1440 minutes (24 hours).
- Specify a number in the range from 0 to 7200.
- If the timeout value is set to 0, then no timeout is set.
- If the specified number is outside the available range, the timeout value is set to the default value (1440 minutes).

Example

```
PullOperationMaxTime=2000
```

In this example, the timeout value is set to 2000 minutes.

Appendix C: System option modes (SOMs)

System option modes allow the storage system to be configured to specific customer operating requirements.

System option modes

To provide greater flexibility, the storage systems have additional operational parameters called system option modes (SOMs) that allow you to tailor the storage system to your unique operating requirements. You can use the maintenance utility or CCI to set the SOMs.

Caution: Changing the SOM settings on your storage system can have unexpected results. Please contact customer support before changing the SOM settings.

The following table lists and describes the SOMs for DKCMAIN firmware version 93-06-41. Review the SOMs for your storage system, and work with your service representative to ensure that the appropriate SOMs for your operational environment are configured on your storage system.

Note: The SOM information might have changed since this document was published. For the latest SOM information, contact customer support.

Table 13 System option modes for VSP E series

Mode	Category	Description	Default	MCU/RCU
15	Common	This SOM can reduce the host response time to be within about 6 seconds.	ON	-

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** This SOM is used on a storage system where slow or delayed drive response may affect business operations. **2.** When Dynamic Sparing or Auto Correction Mode is used, because host I/Os conflict with copy processing, the I/O watching time is 30 seconds even when this SOM is set to ON. **3.** Even though SOM 15 is set to ON, the function does not apply to SATA or NL-SAS drives. **4.** When SOM 771 or SOM 797 is set to ON, the setting of SOM 771/797 is prioritized for the read I/O watching time. **5.** For additional details about this SOM (interaction with other SOMs, operational details), contact customer support (see SOM015 sheet).		
22	Common	Regarding the correction copy or the drive copy, in case ECCs/LRC PINs are set on the track of copy source HDD, SOM 22 can be used to interrupt the copy processing (default) or to create ECCs/LRC PINs on the track of copy target HDD to continue the processing. **Mode 22 = ON:** If ECCs/LRC PINs (up to 64) have been set on the track of copy source HDD, ECCs/LRC PINs (up to 64) will be created on the track of copy target HDD so that the copy processing will continue. If the number of ECCs/LRC PINs exceeds 64, the corresponding copy processing will be interrupted. **Mode 22 = OFF:** If ECCs/LRC PINs have been set on the track of copy source HDD, the copy processing will be interrupted. (First recover ECCs/LRC PINs by using the PIN recovery flow, and then perform the correction copy or the drive copy again). One of the controlling option for correction/drive copy.	OFF	None
142	Common	When a command issued to a drive turns to time-out, the failure is counted on the failure counter of the drive port. If the failure counter reaches the port blockage threshold, the drive port is blocked. When this SOM is set to ON, the port is blocked when the number of failures reaches the half point of the threshold, which mitigates the occurrence possibility of the host time-out.	ON	-

Mode	Category	Description	Default	MCU/RCU
		Mode 142 = ON (default): The threshold value of blocking a drive port due to command time-out is changed to the half of the normal threshold. **Mode 142 = OFF:** The threshold value of blocking a drive port due to command time-out does not change. **Notes:** **1.** This SOM should always be set to ON. This SOM can be set to OFF only when the customer does not allow to set this SOM to ON for a storage system already in production. **2.** This SOM is effective for the entire storage system.		
144	Common	This mode is intended to detect and block a drive whose response is permanently delayed to keep reliability. **1. Normal response delay detection logic** **Mode 144 = ON:** When a response delay drive is detected, SSB=A4CE and A4DE are logged, the drive with response delay is blocked, and SSB=AE4A and SIM=EF0XXX or EF1XXX are reported. The behavior varies depending on the combinations of SOM settings. For details, contact customer support (see SOM144 sheet). **Mode 144 = OFF:** When a response delay drive is detected, SSB=A4CE and A4DE are logged, and SIM=DFFXXX is reported. The behavior varies depending on the combinations of SOM settings. For details, contact customer support (see SOM144 sheet).	OFF (93-03-01 and later)	-

Mode	Category	Description	Default	MCU/RCU
		2. Early response delay detection logic When the logic that detects a minor drive response delay early, which is enabled or disabled by setting SOM1068 to ON or OFF, detects a drive response delay, the drive with response delay is blocked. SOM144 works with the logic and determines whether to block a drive or not when the logic detects a response delay. **Mode 144 = ON:** When a response delay is detected by the logic, SSB=A4CF and A4DD are logged, the drive with response delay is blocked, and then SSB=AE4A and SIM=EF0XXX or EF1XXX are reported. The behavior varies depending on the combinations of SOM settings. For details, contact customer support (see sheet SOM144). Mode 144 = OFF: When a response delay is detected by the logic, SSB=A4CF is logged and SIM=DFFXXX is reported. The behavior varies depending on the combinations of SOM settings. For details, contact customer support (see sheet SOM144). **3.** Using the mode poses a risk of losing the data at a CM/SM dual failure. If high data reliability is required for the storage system like RAID, data duplication should be realized by the entire system like the configuration where data from host is duplicated on primary and secondary storages. **4.** When the mode is used, the time required for blocking cache memory/shared memory at maintenance is longer than that when the mode is set to OFF so that the maintenance operation may end abnormally if the amount of write pending is large. Therefore, perform the maintenance operation when the amount of write pending is as less as possible. If the maintenance operation ends abnormally, replace the blocked part to recover.		

Mode	Category	Description	Default	MCU/RCU
		5. When setting the function to each LDEV is desired, see “WR Through” function on the System Option window. See 2.13 *System option* in the SVP section of the Maintenance Manual. Also, follow the above (1) even when the “WR Through” is used. **Note:** The mode is applied if a stable host response is prioritized by separating a drive whose response is permanently delayed at early stage when the drive delay is detected. To apply the mode, note that separating the drive causes decrease in redundancy.		
164	Common	**Mode 164 = ON:** When CM/SM is blocked or in transition to blockade status, the write-through operation and I/O multiple-operation prevention are not performed. However, the write through operation and I/O multiple-operation prevention during power supply failure mode commanded from HP-UX are performed. **Mode 164 = OFF:** Write through operation and IO multiple-operation prevention are performed when CM/SM is blocked or in transition to blockade status.	OFF	--

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** Data is not secured at the failure on both sides of CM/SM. Recovery from all volume backups is required. **2.** Determine whether to set the mode to ON or OFF on the following basis: **OFF:** The mode is set to OFF to secure the data even when a CM/SM dual failure occurs. As the write through works for data assurance at CM/SM one-side blockage, make sure to design a system where performance degradation such as I/O response is acceptable in a configuration where data from host is duplicated on primary and secondary storages. **ON:** The mode is set to ON to prioritize maintaining the performance over data assurance as a single storage system when a CM/SM dual failure occurs. When the mode is set to ON, the data may be lost at the CM/SM dual failure. If high data reliability is required for the storage system like RAID, data duplication should be realized by the entire system like a configuration where data from host is duplicated on primary and secondary storages.		
310	Common	**Mode 310 = ON:** The monitoring timer for MP hang-up is 6 seconds and returning a response to the host within 8 seconds is guaranteed. **Mode 310 = OFF:** The monitoring timer for MP hang-up is 8 seconds. **Notes:** **1.** This SOM applies to a site where strict host response performance is required. **2.** If a hardware failure occurs when this SOM is set to ON, the time until MPB blockage is determined is shorter than usual.	OFF	-
448	Universal Replicator	**Mode 448 = ON:** After a physical path failure (such as path disconnection) is detected, a mirror is split (suspended) one minute after the detection. On the MCU side, the mirror is suspended one minute after read journal commands from the RCU stop. On the RCU side, the mirror is suspended one minute after read journal commands fail.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Mode 448 = OFF: After a physical path failure (such as path disconnection) is detected, a mirror is split (suspended) if the path is not restored within the path monitoring time set by the mirror option. **Notes:** **1.** The mode is applied when a user requires to suspend the pair one minute after a communication error between UR MCU and RCU is detected. **2.** When SOM 449 is set to ON, SOM 448 does not function.		
449	Universal Replicator	This mode is used to enable and disable detection of communication failures between the MCU and RCU. The default setting is ON. **Mode 449 = ON:** When a physical path failure is detected, the pair is not suspended. On the MCU side, checking read journal command disruption from the RCU is disabled, and monitoring read journal command failures is disabled on the RCU side. **Mode 449 = OFF:** When a physical path failure is detected, the pair is suspended after the path monitoring time set by the mirror option has passed or after one minute. Detecting communication failures between the MCU and RCU is enabled. When this mode is set to OFF, SOM 448 can be enabled. **Notes:** **1.** This SOM is applied when disabling the detection of communication failures between the MCU and RCU in UR configuration is required. **2.** When this SOM is set to ON, SOM 448 does not work. **3.** This SOM setting is not changed by microcode upgrade. **4.** This SOM is not effective for remote paths between an Initiator port on the MCU and a Target port on the RCU. **5.** While a path from the RCU to MCU is disconnected, if the UR pair remains in Suspending or Deleting status, recover it in accordance with the procedure in Recovery from UR Failure in TROUBLE SHOOTING section of Maintenance Manual.	ON	MCU

Mode	Category	Description	Default	MCU/RCU
454	Virtual Partition Manager	CLPR (function of Virtual Partition Manager) partitions the cache memory in the storage system into multiple virtual cache and assigns the partitioned virtual cache for each use. If a large amount of cache is required for a specific use, it can minimize the impact on other uses. The CLPR function works as follows depending on whether SOM 454 is set to ON or OFF. **Mode 454 = OFF:** The amount of the entire destage processing is periodically determined by using the highest workload of all CLPRs (*a). (The larger the workload is, the larger the amount of the entire destage processing becomes.) *a: (Write Pending capacity of CLPR#x of concerned MPB) ÷ (Cache capacity of CLPR#x of concerned MPB), x=0 to 31 CLPR whose value above is the highest of all CLPRs Because the destage processing would be accelerated depending on CLPR with high workload, when the workload in a specific CLPR increases, the risk of host I/O halt would be reduced. Therefore, set SOM 454 to OFF in most cases. **Mode 454 = ON:** The amount of the entire destage processing is periodically determined by using the workload of the entire system (*b). (The larger the workload is, the larger the amount of the entire destage processing becomes.) *b: (Write Pending capacity of the entire system of concerned MPB) ÷ (Cache capacity of the entire system of concerned MPB) **Caution:** Because the destage processing would not be accelerated even if CLPR has high workload, when the workload in a specific CLPR increases, the risk of host I/O halt would be increased. Therefore, set SOM 454 to ON only when a CLPR has constant high workload and the I/O performance in a CLPR with low workload has higher priority than host I/O halt in the CLPR with high workload.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** When this SOM is set to ON, even if there is an overloaded CLPR (CLPR with large Write Pending capacity), the amount of destage processing would not increase easily. Therefore TOV(MIH) may occur in the overloaded CLPR. Set this SOM to ON only when the overloaded state of a specific CLPR would not affect other CLPRs. When the UR function is used, if user volumes and journal volumes are defined in different CLPRs, when the CLPR to which the journal volumes are assigned overflows, the user volumes become inaccessible. Therefore it is recommended to set this SOM to OFF. **2.** Because the destage processing will have a lower priority in the overloaded CLPR, the overloaded state of the overloaded CLPR is not removed, and TOV(MIH) might occur.		
457	Universal Volume Manager	High-speed LDEV format for external volumes. **Mode 457 = ON:** The high-speed LDEV format for external volumes is available by SOM 457 to ON. When SOM 457 is ON, if you select an external volume group and perform an LDEV format, any write processing on the external logical units will be skipped. **Mode 457 = OFF:** High-speed LDEV format for external volumes is not available. **Notes:** ▪ If the LDEV is not written with data “0” before performing the function, the LDEV format might fail. ▪ After the format processing, make sure to set SOM 457 to OFF.	OFF	Both
459	ShadowImage	When the S-VOL of an SI/SIz pair is an external volume, the transaction to change the status from SP-PEND to SPLIT is as follows: **Mode 459 = ON:** When suspending an SI pair: Waits for the copy data in cache memory to completely destage to the external volume S-VOL before changing the pair status to SUSPEND.	ON	-

Mode	Category	Description	Default	MCU/RCU
		Mode 459 = OFF: When suspending an SI pair: The status changes to SUSPEND as soon as all of the delta data is copied to S-VOL cache. The status does not wait for cache to destage to the S-VOL external volume.		
467	ShadowImage Universal Volume Manager Volume Migration	For the following features, the current copy processing slows down when the percentage of “dirty” data is 60% or higher, and it stops when the percentage is 75% or higher. Mode 467 is provided to prevent the percentage from exceeding 60%, so that the host performance is not affected. ▪ SI ▪ UVM ▪ Volume Migration **Mode 467 = ON:** Copy overload prevention. Copy processing stops when the percentage of “dirty” data reaches 60% or higher. When the percentage falls below 60%, copy processing restarts. **Mode 467 = OFF:** Normal operation. The copy processing slows down if the dirty percentage is 60% or larger, and it stops if the dirty percentage is 75% or larger. **Caution:** This SOM must always be set to ON when using an external volume as the secondary volume of any of the applicable replication products.	ON	-

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** It takes longer to finish the copy processing because it stops for prioritizing the host I/O performance. **2.** This SOM supports background copy only. The processing to copy the pre-update data to the S-VOL, which occurs when overwriting data to uncopied slots of P-VOL in Split processing or reading or writing data to uncopied slots of S-VOL, is not supported. **3.** Check the write pending rate of each CLPR per MP unit. Even though there is some free cache capacity in the entire system, if the write pending rate of an MP unit to which pairs* belong exceeds the threshold, the copy operation is stopped. *Applies to pairs of SI, SIz, FCv2, FCSE, and Volume Migration.		
471	Thin Image	Since the SIM-RCs generated when the Thin Image pool usage rate exceeds the threshold value can be resolved by users, these SIM-RCs are not reported to the maintenance personnel. This SOM is used to report these SIM-RCs to maintenance personnel. The SIM-RCs reported by setting the SOM to ON are: 601xxx (Pool utilization threshold exceeded), 603000 (SM space warning). **Mode 471 = ON:** These SIM-RCs are reported to maintenance personnel. **Mode 471 = OFF:** These SIM-RCs are not reported to maintenance personnel. **Note:** Set this SOM to ON when it is required to inform maintenance personnel of these SIM-RCs.	OFF	-
474	Universal Replicator	UR initial copy performance can be improved by issuing a command from CCIto execute a dedicated script consisting of UR initial copy (Nocopy), UR suspend, TC Sync initial copy, TC Sync delete, and UR resync. **Mode 474 = ON:** For a suspended UR pair, a TC (Sync) pair can be created with the same P-VOL/S-VOL so that UR initial copy time can be reduced by using the dedicated script.	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		Mode 474 = OFF: For a suspended UR pair, a TC (Sync) pair cannot be created with the same P-VOL/S-VOL. For this, the dedicated script cannot be used. If the P-VOL and S-VOL are both DP-VOLs, initial copy performance might not improve with SOM 474 set to ON. This is because with DP-VOLs, not all areas in a volume are allocated for UR; therefore not all areas in the P-VOL are copied to the S-VOL. With less than the full amount of data in the P-VOL being copied, the initial copy completes in a shorter time, which might not be improved with SOM 474.		

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** Set this SOM for both primary and secondary storage systems. **2.** When this SOM is set to ON: ▪ Execute all pair operations from CCI. ▪ Use a dedicated script. ▪ Initial copy operation is prioritized over update I/O. Therefore, the processing speed of the update I/O slows down. **3.** If this SOM is set to ON, the processing speed of update I/O slows down by about 15 µs per command, version downgrade is disabled, and Take Over is not available. **4.** If this SOM is not set to ON for both sides, the behavior is as follows: ▪ OFF in primary and secondary storage systems: Normal UR initial copy performance. ▪ ON in the primary storage system/OFF in the secondary storage system: TC Sync pair creation fails. ▪ OFF in the primary storage system/ON in the secondary storage system: The update data is copied to the S-VOL synchronously. **5.** While this SOM is set to ON, make sure not to perform microcode downgrade to an unsupported version. **6.** While this SOM is set to ON, make sure not to perform the Take Over function. **7.** This SOM cannot be applied to a UR pair that is the second mirror in a URxUR multi-target configuration, URxUR cascade configuration, or 3DC multi-target or cascading configuration of three UR sites. If applied, TC pair creation is rejected with SSB=CBED output. **8.** Before setting SOM 474 to ON, make sure that SOM 1091 is set to OFF. If SOM 1091 is set to ON, set it to OFF first, and then set SOM 474 to ON.		

Mode	Category	Description	Default	MCU/RCU
506	Universal Replicator	This SOM is used to enable Delta Resync with no host update I/O by copying only differential JNL instead of copying all data. The UR Delta Resync configuration is required. **Mode 506 = ON:** ▪ Without update I/O: Delta Resync is enabled. ▪ With update I/O: Delta Resync is enabled. **Mode 506 = OFF:** ▪ Without update I/O: Total data copy of Delta Resync is performed. ▪ With update I/O: Delta Resync is enabled. **Note:** Even when SOM 506 is set to ON, the Delta Resync may fail and only the total data copy of the Delta Resync function is allowed if the necessary journal data does not exist on the primary storage system used for the Delta Resync operation.	ON	Both
556	Open	Prevents an error code from being set in the 8 - 11th bytes in the standard 16-byte sense byte. **Mode 556 = ON:** An error code is not set in bytes 8 - 11 in the standard 16-byte sense byte. **Mode 556 = OFF:** An error code is set in bytes 8 - 11 in the standard 16-byte sense byte.	OFF	Both
589	Universal Volume Manager	When this SOM is ON, the frequency of progress update of disconnection is changed. **Mode 589 = ON:** For each external volume, progress is updated only when the progress rate is 100%. **Mode 589 = OFF:** Progress is updated when the progress rate exceeds the previous level. **Notes:** **1.** Set this SOM to ON when disconnecting an external volume while the specific host IO operation is online and its performance requirement is severe. **2.** Whether the disconnecting status for each external volume is progressed or not cannot be confirmed on Device Manager - Storage Navigator (It indicates “-“until just before the completion and at the last it changes to 100%).	OFF	Both

Mode	Category	Description	Default	MCU/RCU
689	TrueCopy Global-active device	Allows you to slow the initial copy and resync operations when the write-pending rate on the RCU exceeds 60%. **Mode 689 = ON:** The initial copy and resync copy operations are slowed down when the Write Pending rate on RCU exceeds 60%. If the CLPR write pending rate where the initial copy target secondary volume belongs to is not over 60% but that of MP PCB where the S-VOL belongs to is over 60%, the initial copy operation is slowed down. **Mode 689 = OFF:** The initial copy and resync copy operations are not slowed down when the Write Pending rate on RCU exceeds 60% (the same as before). **Notes:** **1.** This SOM can be set online. **2.** The micro-programs on both MCU and RCU must support this SOM. **3.** This SOM should be set when requested by the user. **4.** Setting this SOM to ON is recommended when GAD is installed, as the performance degradation is more likely to occur due to active-active I/Os. **5.** If the write-pending status remains at 60% or higher on the RCU for a long time, it takes extra time for the initial copy and resync copy to be completed due to the slower copy operations. **6.** If the write pending rate of CLPR to which the initial copy target S-VOL belongs is not over 60% but that of MP PCB to which the S-VOL belongs is over 60%, the initial copy operation is slowed down.	OFF	Both
690	Universal Replicator	This SOM is used to prevent Read JNL or JNL Restore when the Write Pending rate on RCU exceeds 60% as follows: ▪ When CLPR of JNL-Volume exceeds 60%, Read JNL is prevented. ▪ When CLPR of Data (secondary)-Volume exceeds 60%, JNL Restore is prevented.	OFF	RCU

Mode	Category	Description	Default	MCU/RCU
		Mode 690 = ON: Read JNL or JNL Restore is prevented when the Write Pending rate on RCU exceeds 60%. **Mode 690 = OFF:** Read JNL or JNL Restore is not prevented when the Write Pending rate on RCU exceeds 60% (the same as before). **Notes:** **1.** This SOM can be set online. **2.** This SOM should be set per customer's requests. **3.** If the Write Pending status long keeps 60% or more on RCU, it takes extra time for the initial copy to be completed by making up for the prevented copy operation. **4.** If the Write Pending status long keeps 60% or more on RCU, the pair status may become Suspend due to the JNL-Vol being full.		
701	Universal Volume Manager	Issues the Read command at the logical unit discovery operation using UVM. **Mode 701 = ON:** The Read command is issued at the logical unit discovery operation. **Mode 701 = OFF:** The Read command is not issued at the logical unit discovery operation.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** When the external storage is TagmaStore USP/NSC and the Open LDEV Guard attribute (VMA) is defined on an external device, set this SOM to ON. **2.** When this SOM is set to ON, it takes longer time to complete the LU discovery. The amount of time depends on external storages. **3.** With this SOM OFF, if searching for external devices with VMA is set, the VMA information cannot be read. **4.** When this SOM is set to ON while the following conditions are met, the external volume is blocked: ▪ An external volume to which Nondisruptive migration (NDM) attribute is set exists. ▪ The external volume is reserved by the host **5.** As the VMA information is TagmaStore USP/NSC-specific, this SOM does not need to be ON when the external storage is other than TagmaStore USP/NSC. **6.** Set this SOM to OFF when an external volume to which nondisruptive migration (NDM) attribute is set exists.		
704	ShadowImage Volume Migration	To reduce the chance of MIH, this SOM can reduce the priority of ShadowImage, Volume Migration, or Resync copy internal IO requests so that host IO has a higher priority. This SOM creates new work queues where these jobs can be assigned with a lower priority. **Mode 704 = ON:** Copy processing requested is registered into a newly created queue so that the processing is scheduled with lower priority than host I/O. **Mode 704 = OFF:** Copy processing requested is not registered into a newly created queue. Only the existing queue is used.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** Apply this SOM when the load of host I/O to an ECC that uses ShadowImage or Volume Migration is high and the host I/O processing is delayed. **2.** If the PDEV is highly loaded, the priority of Read/Write processing made by ShadowImage, Volume Migration, or Resync may become lower. As a consequence the copy speed may be slower.		
721	Common	When a parity group is uninstalled or installed, the following operation is performed according to the setting of SOM 721. **Mode 721 = ON:** When a parity group is uninstalled or installed, the LED of the drive for uninstallation is not illuminated, and the instruction message for removing the drive does not appear. Also, the windows other than that of parity group, such as DKA or DKU, are unavailable to select. **Mode 721 = OFF:** When a parity group is uninstalled or installed, the operation is as before: the LED of the drive is illuminated, and the drive must be unmounted and remounted. **Notes:** **1.** When the RAID level or emulation type is changed for the existing parity group, this SOM should be applied only if the drive mounted position remains the same at the time of the parity group uninstallation or installation. **2.** After the operation using this SOM is completed, this SOM must be set back to OFF; otherwise, the LED of the drive to be removed will not be illuminated at subsequent parity group uninstalling operations.	OFF	-
725	Universal Volume Manager	This SOM determines the action that will be taken when the status of an external volume is Not Ready. **Mode 725 = ON:** When Not Ready is returned, the external path is blocked and the path status can be automatically recovered (Not Ready blockade). Note that the two behaviors, automatic recovery and block, may be repeated.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		When the status of a device is Not Ready blockade, Device Health Check is executed after 30 seconds. **Mode 725 = OFF:** When Not Ready is returned three times in three minutes, the path is blocked and the path status cannot be automatically recovered (Response error blockade). **Notes:** **1.** Applying this SOM is prohibited when USP V/VM is used as an external storage system and its external volume is DP-VOL. **2.** Applying this SOM is recommended when the above condition (1) is not met and SUN storage is used as an external storage. **3.** Applying this SOM is recommended when the above condition (1) is not met and EMC CX series or Fujitsu Fibre CAT CX series is used as an external storage. **4.** Applying this SOM is recommended if the above condition (1) is not met and a maintenance operation such as firmware update causing controller reboot is executed on the external storage side while a storage system other than Hitachi product is used as an external storage system. **5.** While USP V/VM is used as an external storage system and its volume is DP-VOL, if some Pool-VOLs constituting the DP-VOL are blocked, external path blockade and recovery occurs repeatedly. **6.** When a virtual volume mapped by UVM is set to pool-VOL and used as DP-VOL in local storage system, this SOM can be applied without problem.		
729	Dynamic Provisioning Data Retention Utility	When a DP pool is full, if any write operation is requested to the area where the page allocation is not provided, this SOM can enable the DRU Protect attribute for the target DP-VOL. **Mode 729 = ON:** Set the DRU Protect attribute for the target DP-VOL when any write operation is requested to the area where the page allocation is not provided at a time when the DP pool is full. (Not to set in the case of Read request.)	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Mode 729 = OFF: Do not set the DRU Protect attribute for the target DP-VOL when any write operation is requested to the area where the page allocation is not provided at a time when DP pool is full. For details, contact customer support (see SOM729 & 803 sheet). **Notes:** **1.** This SOM is applied when: ▪ The threshold of pool is high (for example, 95%) and the pool may be full. ▪ File system is used. ▪ Data Retention Utility is installed. **2.** Since the Protect attribute is set for V-VOL, the Read operation cannot be allowed as well. **3.** When Data Retention Utility is not installed, the desired effect is not achieved. **4.** Protect attribute can be released from the **Data Retention** window of Device Manager - Storage Navigator after releasing the full status of the pool by adding a Pool-VOL. **5.** The Virtual Volume Protection (VVP) function can be enabled/disabled for each pool. With SOM 729 disabled, VVP is also disabled by default, but you can enable VVP for each pool as needed. With SOM 729 enabled, VVP is also enabled automatically (by default) when you create a new pool. **Caution:** A pool is NOT protected by ANY FUNCTION if you deliberately turn VVP for the pool from ON (default) to OFF, even with SOM 729 enabled. **6.** When HMO 63 or 73 is set to ON, the setting of the HMO is prioritized over the SOM 729 setting, so that the behavior remains the same as when SOM 729 is OFF even when it is set to ON.		
734	Dynamic Provisioning	When exceeding the pool threshold, the SIM is reported as follows:	ON	-

Mode	Category	Description	Default	MCU/RCU
		Mode 734 = ON: A SIM is reported at the time when the pool usage rate exceeds the pool threshold (warning, system, or depletion). Once the pool usage rate falls below the pool threshold, and then exceeds again, the SIM is reported again. If the pool usage rate continues to exceed the warning threshold and the depletion threshold, the SIM (SIM-RC625000) is repeatedly reported every eight (8) hours until the pool usage rate falls below the depletion threshold. **Mode 734 = ON:** A SIM is reported at the time when the pool usage rate exceeds the pool threshold (variable threshold or fixed threshold). Once the pool usage rate falls below the pool threshold, and then exceeds again, the SIM is reported again. If the pool usage rate continues to exceed the variable threshold and the fixed threshold, the SIM (SIM-RC625000) is repeatedly reported every eight (8) hours until the pool usage rate falls below the higher threshold. **Mode 734 = OFF:** A SIM is reported at the time when the pool usage rate exceeds the pool threshold (variable threshold or fixed threshold). Once the pool usage rate falls below the pool threshold, and then exceeds again, the SIM is reported again. The SIM is not reported while the pool usage rate continues to exceed both of the variable threshold and the fixed threshold.		
741	Dynamic Provisioning	This SOM enables to switch over whether to report the following SIM for users to the service personnel: SIM-RC 625000 (DP pool usage rate continues to exceed the threshold) **Mode 741 = ON:** SIM is reported to the service personnel. **Mode 741 = OFF:** SIM is not reported to the service personnel.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** This SOM is set to ON to have SIM for users reported to the service personnel: ▪ For the system where SNMP and E-mail notification are not set. ▪ If Device Manager - Storage Navigator is not periodically activated. **2.** When SOM 734 is turned OFF, SIM-RC625000 is not reported; accordingly the SIM is not reported to the service personnel even though this SOM is ON.		
745	Universal Volume Manager	Enables to change the area where the information is obtained as the Characteristic1 item from SYMMETRIX. **Mode 745 = ON:** ▪ The area where the information is obtained as the Characteristic1 item from SYMMETRIX is changed. ▪ When CheckPaths or Device Health Check (1/hour) is performed, the information of an already-mapped external volume is updated to the one after change. **Mode 745 = OFF:** ▪ The area where the information is obtained as the Characteristic1 item from SYMMTRIX is set to the default. ▪ When CheckPaths or Device Health Check (1/hour) is performed, the information of an already-mapped external volume is updated to the default.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** This SOM is applied when the EMC SYMMETRIX is connected using UVM. **2.** Enable the setting of EMC SCSI Flag SC3 for the port of the EMC SYMMETRIX storage connected with the storage system and disable the setting of Flag SPC2. If the setting of EMC SCSI Flag SC3 is not enabled or the setting of Flag SPC2 is enabled, the effect of this SOM may not be achieved. **3.** If you want to enable this SOM immediately after setting, perform Check Paths on each path one by one for all the external ports connected to the EMC SYMMETRIX storage. But, without doing Check Paths, the display of Characteristic1 can automatically be changed by the Device Health Check to be performed once an hour. If SSB=AD02 occurs and a path is blocked, perform Check Paths on this path again.		
749	Dynamic Provisioning Dynamic Tiering Thin Image	This SOM disables the HDP Rebalance function and the HDT Tier relocation function which allow the drives of all ECC Groups in the pool to share the load. **Mode 749 = ON:** The HDP Rebalance function and the HDT Tier relocation function are disabled. **Mode 749 = OFF:** The HDP Rebalance function and the HDT Tier relocation function are enabled. **Notes:** **1.** This SOM is applied when no change in performance characteristic is desired. **2.** When a pool is newly installed, the load may be concentrated on the installed pool volumes. **3.** When 0 data discarding is executed, load may be unbalanced among pool volumes. **4.** Pool VOL deletion while this SOM is set to ON fails. To delete pool VOLs, set this SOM to OFF.	OFF	-
757	Common	Enables/disables output of in-band audit logs. **Mode 757 = ON:** In-band audit log is not output. **Mode 757 = OFF:** In-band audit log is output.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** Mode 757 applies to the sites where outputting the In-band audit logs is not needed. **2.** When this SOM is set to ON: ▪ There is no access to SM for the In-band audit logs, which can avoid the corresponding performance degradation. ▪ SM is not used for the In-band audit logs. **3.** If outputting the In-band audit log is desired, set this SOM to OFF.		
784	TrueCopy Global-active device	This SOM can reduce the MIH watch time of RI/O for a TC or GAD pair internally so that update I/Os can continue by using an alternate path without MIH or time-out occurrence in the environment where Mainframe host MIH is set to 15 seconds, or Open host time-out time is short (15 seconds or less). This SOM is effective at initial pair creation or Resync operation for TC or GAD. (Not effective by just setting this SOM to ON.) This SOM is applied to TC and GAD. This SOM supports Fibre remote copy paths but not iSCSI. **Mode 784 = ON:** The MIH time of RIO is internally reduced so that, even though a path failure occurs between storage systems in the environment where host MIH time is set to 15 seconds, update I/Os can be processed by using an alternate path promptly, lowering the possibility of host MIH occurrence. **Mode 784 = OFF:** The operation is processed in accordance with the TC or GAD specification.	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** This SOM is applied to the environment where Mainframe host MIH time is set to 15 seconds. **2.** This SOM is applied to the environment where OPEN host time-out time is set to 15 seconds or less. **3.** This SOM is applied to reduce RI/O MIH time to 5 seconds. **4.** This function is available for all the TC and GAD pairs on the storage system, unable to specify the pairs that are using this function or not. **5.** For a TC or GAD pair with this SOM effective (RI/O MIH time is 5 seconds), the setting of RI/O MIH time made at RCU registration (default is 15 seconds, which can be changed within range from 10 to 100 seconds) is invalid. However, RI/O MIH time displayed on Device Manager - Storage Navigator and CCI is not “5 seconds” but is what set at RI/O registration. **6.** If a failure occurs on the switched path between storage systems, Mainframe host MIH or Open server time-out may occur. **7.** If an MP to which the path between storage systems belongs is overloaded, switching to an alternate path delays and host MIH or time-out may occur. **8.** If an RI/O retry occurs due to other factors than RI/O MIH (5 sec), such as a check condition report issued from RCU to MCU, the RI/O retry is performed on the same path instead of an alternate path. If a response delay to the RI/O occurs constantly on this path due to path failure or link delay, host MIH or time-out may occur due to response time accumulation for each RI/O retried within 5 seconds. **9.** Even though this SOM is set to ON, if Mainframe host MIH time or Open host time-out time is set to 10 seconds or less, host MIH or time-out may		

Mode	Category	Description	Default	MCU/RCU
		occur due to a path failure between storage systems. **10.** Operation commands are not available for promptly switching to an alternate path. **11.** This SOM works for the pair for which initial pair creation or Resync operation is executed. **12.** Micro-program downgrade to an unsupported version cannot be executed unless all the TC and GAD pairs are suspended or deleted. **13.** For operational specifications in each combination of MCU and RCU of TC, contact customer support (see SOM784 sheet). **14.** For GAD pairs, this SOM is effective if the microcode version supports GAD. **15.** This SOM does not support iSCSI paths between storage systems. When iSCSI is used for paths between storage systems, the time to switch to an alternate path cannot be reduced. For this, if a failure occurs on a path between storage systems in an environment where host time-out time is short, a time-out may occur on the host side. A time-out may also occur on the host side when a failure occurs on an iSCSI path between storage systems if storage system paths of Fibre and iSCSI coexist in an environment where host time-out time is short so that the configuration where storage system paths of Fibre and iSCSI coexist is not supported too.		
803	Dynamic Provisioning Data Retention Utility	While a DP pool VOL is blocked, if a read or write I/O is issued to the blocked pool VOL, this SOM can enable the Protect attribute of DRU for the target DP-VOL. **Mode 803 = ON:** While a DP pool VOL is blocked, if a read or write I/O is issued to the blocked pool VOL, the DRU attribute is set to Protect. **Mode 803 = OFF:** While a DP pool VOL is blocked, if a read or write I/O is issued to the blocked pool VOL, the DRU attribute is not set to Protect. For more details, contact customer support (see SOM729 & 803 sheet).	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** This SOM is applied when: ▪ A file system using DP pool VOLs is used. ▪ Data Retention Utility is installed. **2.** Because the DRU attribute is set to Protect for the V-VOL, a read I/O is also disabled. **3.** If Data Retention Utility is not installed, the expected effect cannot be achieved. **4.** The Protect attribute of DRU for the DP V-VOL can be released on the **Data Retention** window of Device Manager - Storage Navigator after recovering the blocked pool VOL. **5.** The Virtual Volume Protection (VVP) function can be enabled/disabled for each pool. With SOM 803 disabled, VVP is also disabled by default, but you can enable VVP for each pool as needed. With SOM 803 enabled, VVP is also enabled automatically (by default) when you create a new pool. **Caution:** A pool is NOT protected by ANY FUNCTION if you deliberately turn VVP for the pool from ON (default) to OFF, even with SOM 803 enabled.		
855	ShadowImage Volume Migration	By switching this SOM to ON/OFF when ShadowImage is used with SOM 467 set to ON, copy processing is continued or stopped as follows. **Mode 855 = ON:** When the amount of dirty data is within the range from 58% to 63%, the next copy processing is continued after the dirty data created in the previous copy is cleared to prevent the amount of dirty data from increasing (copy after destaging). If the amount of dirty data exceeds 63%, the copy processing is stopped. **Mode 855 = OFF:** The copy processing is stopped when the amount of dirty data is over 60%. For details, contact customer support (see SOM855 sheet).	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** This SOM is applied when all the following conditions are met ▪ ShadowImage is used with SOM 467 set to ON. ▪ Write pending rate of an MP unit that has LDEV ownership of the copy target is high ▪ Usage rate of a parity group to which the copy target LDEV belongs is low. ▪ ShadowImage copy progress is delayed. **2.** This SOM is available only when SOM 467 is set to ON. **3.** If the workload of the copy target parity group is high, the copy processing may not be improved even if this SOM is set to ON.		
867	Dynamic Provisioning Dynamic Tiering	All-page reclamation (discarding all mapping information between DP pool and DP volumes) is executed in DP-VOL LDEV format. This new method is enabled or disabled by setting this SOM to ON or OFF. **Mode 867 = ON:** LDEV format of the DP-VOL is performed with page reclamation. **Mode 867 = OFF:**LDEV format of the DP-VOL is performed with 0 data writing. **Notes:** **1.** This SOM is applied from factory shipment. **2.** Do not change the setting of this SOM during DP-VOL format. **3.** If the setting of this SOM is changed during DP-VOL format, the change is not reflected to the format of the DP-VOL being executed but the format continues in the same method.	ON	-
896	Dynamic Provisioning Dynamic Tiering Thin Image	This SOM enables or disables the background format function performed on an unformatted area of a DP/DT/TI pool. For information regarding operating conditions, see the *Provisioning Guide*. **Mode 896 = ON:** The background format function is disabled.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Mode 896 = OFF: The background format function is enabled. **Notes:** **1.** This SOM is applied when you need to disable the background format for a DP/DT/TI pool due to a concern of performance degradation of other functions in an environment where a DP-VOL is used by other functions. **2.** When the background format function is enabled, because up to 42 MB/s of ECCG performance is used, local copy performance may degrade by about 10%. Therefore, confirm whether the 10% performance degradation is acceptable or not before enabling the function. **3.** When a Dynamic Provisioning VOL on an external storage system, which is used as an external VOL, is used as a pool VOL, if the external pool on the external storage side becomes full due to the background format, the external VOL may be blocked. If the external pool capacity is smaller than the external VOL capacity (Dynamic Provisioning VOL of external storage system), do not enable the background format function. **4.** If the background format function is disabled by changing this SOM setting, the format progress is initialized and the entire area becomes unformatted.		
899	Volume Migration	In combination with the SOM 900 setting, this SOM determines whether to execute and when to start the I/O synchronous copy change as follows. **Mode 899 = ON:** ▪ SOM 900 is ON: I/O synchronous copy starts without retrying Volume Migration. ▪ SOM 900 is OFF: I/O synchronous copy starts when the threshold of Volume Migration retry is exceeded. (Recommended)	ON	-

Mode	Category	Description	Default	MCU/RCU
		Mode 899 = OFF: ▪ SOM 900 is ON: I/O synchronous copy starts when the number of retries reaches half of the threshold of Volume Migration retry. ▪ SOM 900 is OFF: Volume Migration is retired and I/O synchronous copy is not executed. **Notes:** **1.** This SOM is applied when improvement of Volume Migration success rate is desired under the condition that there are many updates to a migration source volume of Volume Migration. **2.** During I/O synchronous copy, host I/O performance degrades.		
900	Volume Migration	In combination with SOM 899 setting, this SOM determines whether to execute and when to start the I/O synchronous copy change as follows. **Mode 900 = ON:** ▪ SOM 899 is ON: I/O synchronous copy starts without retrying Volume Migration. ▪ SOM 899 is OFF: I/O synchronous copy starts when the number of retries reaches half of the threshold of Volume Migration retry. **Mode 900 = OFF:** ▪ SOM 899 is ON: I/O synchronous copy starts when the threshold of Volume Migration retry is exceeded. (Recommended) ▪ SOM 899 is OFF: Volume Migration is retired and I/O synchronous copy is not executed. **Notes:** **1.** This SOM is applied when improvement of Volume Migration success rate is desired under the condition that there are many updates to a migration source volume of Volume Migration. **2.** During I/O synchronous copy, host I/O performance degrades.	OFF	-
901	Dynamic Tiering	By setting this SOM to ON or OFF, the page allocation method of Tier Level ALL when the drive type of tier1 is SSD changes as follows.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Mode 901 = ON: For tier1 (drive type is SSD), pages are allocated until the capacity reaches the limit. Without consideration of exceeding performance limitation, allocation is done from highly loaded pages until reaching the capacity limit When the capacity of tier1 reaches the threshold value, the minimum value of the tier range is set to the starting value of the lower IOPH zone, and the maximum value of the lower tier range is set to the boundary value. **Mode 901 = OFF:** For tier1 (drive type is SSD), page allocation is performed based on performance potential limitation. With consideration of exceeding performance limitation, allocation is done from highly loaded pages but at the point when the performance limitation is reached, pages are not allocated any more even there is free space. When the capacity of tier1 reaches the threshold value, the minimum value of the tier range is set to the boundary value, and the maximum value of the lower tier range is set to a value of *boundary-value* × 110% + 5 [IOPH]. **Notes:** **1.** This SOM is applied when pages with the maximum capacity need to be allocated to tier1 (drive type is SSD) with Dynamic Tiering. **2.** When Tier1 is SSD while SOM 901 is set to ON, the effect of SOM 897 and 898 to the gray zone of Tier1 and Tier2 is disabled and the SOM 901 setting is enabled instead. In addition, the settings of SOM 897 and 898 are effective for Tier2 and Tier3. **3.** The following is recommended when applying SOM 901. actual I/O value (total number of I/Os of all tiering policies) < performance potential value of Tier1* × 0.6 * The performance potential value of Tier1 displayed on Monitor information by using Dx-ray. For more details about the interactions between SOMs 897, 898, and 901, contact customer support (see SOM897_898_901 sheet).		

Mode	Category	Description	Default	MCU/RCU
904	Dynamic Tiering	By setting this SOM to ON or OFF, the number of pages to be migrated per unit time at tier relocation is changed. **Mode 904 = ON:** The number of pages to be migrated at tier relocation is set to up to one page per second. **Mode 904 = OFF:**No restriction on the number of pages to be migrated at tier relocation (existing specification). **Notes:** **1.** This SOM is applied when the requirement for response time is severe. **2.** The number of pages to be migrated per unit time at tier relocation decreases.	OFF	-
908	Universal Replicator	This SOM can change CM capacity allocated to MPBs with different workloads. **Mode 908 = ON:** The difference in CM allocation capacity among MPBs with different workload is large. **Mode 908 = OFF:** The difference in CM allocation capacity among MPBs with different workload is small (existing operation) .	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** If a CLPR is used by only some MPBs among all the installed MPBs, set this SOM to ON for the CLPR to increase CM capacity allocated to the MPBs that use the CLPR. Example: (a) A CLPR only for UR JNLG. (b) A configuration where MPBs and CLPRs are separately used for Open and Mainframe systems. **2.** Since CM capacity allocated to MPBs with low load is small, the performance is affected by a sudden increase in load. **3.** SOM 908 cannot be used with SOM 933. When SOM 933 is set to ON, the function of SOM 908 is canceled even though SOM 908 is ON. **4.** This SOM is effective for a CLPR. Therefore, when setting this SOM to ON/OFF, select target "LPRXX (XX=00 to 31)". For example, even when CLPR0 is defined (any of CLPR1 to 31 are not defined), select “LPR00” first and then set this SOM to ON/OFF.		
930	Dynamic Provisioning Dynamic Tiering ShadowImage	When this SOM is set to ON, all of the zero data page reclamation operations in processing are stopped. (Also the zero data page reclamation cannot be started.) * Zero data page reclamation by WriteSame and UNMAP functions, and IO synchronous page reclamation are not disabled. **Mode 930 = ON:** All of the zero data page reclamation operations in processing are stopped at once. (Also the zero data reclamation cannot be newly started.) **Mode 930 = OFF:** The zero data page reclamation is performed. For details about interactions with SOM 755, contact customer support (see SOM930 sheet).	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** This SOM is applied when stopping or disabling zero data page reclamation by user request is required. **2.** When this SOM is set to ON, the zero data page reclamation does not work at all. * Zero data page reclamation by WriteSame and UNMAP, IO synchronous page reclamation, program product synchronous page reclamation, and UDSR page reclamation can work. **3.** When downgrading micro-program to a version that does not support this SOM while this SOM is set to ON, set this SOM to OFF after the downgrade. * Because the zero data page reclamation does not work at all while this SOM is set to ON. **4.** When the mode is set to ON, zero data page reclamation by WriteSame function, UNMAP function, I/O synchronous page reclamation, program product synchronous page reclamation, and UDSR page reclamation can work. **5.** This SOM is related to SOM 755.		
937	Dynamic Provisioning Dynamic Tiering	By setting this SOM to ON, HDT monitoring data is collected even if the pool is a DP pool. **Mode 937 = ON:** HDT monitoring data is collected even if the pool is a DP pool. Only Manual execution mode and Period mode are supported. **Mode 937 = OFF:** HDT monitoring data is not collected if the pool is a DP pool	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** This SOM is applied when HDT monitoring data collection is required in DP environment. **2.** When HDT is already used, do not set this SOM to ON. **3.** For HDT monitoring data collection, shared memory for HDT must be installed. For details, contact customer support (see SOM937 sheet). **4.** If monitoring data collection is performed without shared memory for HDT installed, an error is reported and the monitoring data collection fails. **5.** Before removing the shared memory for HDT, set this SOM to OFF and wait for 30 minutes. **6.** Tier relocation with monitoring data collected when this SOM is set to ON is disabled. **7.** When DP is converted into HDT (after purchase of software license), the collected monitoring data is discarded. **8.** Before downgrading the micro-program to an unsupported version, set SOM 937 to OFF and wait for at least 30 minutes.		
972	Common	By setting this SOM, THP Page Size in Inquiry Page E3h is changed. THP Page Size varies depending on the combination of SOM 972 and 973 settings. For details, contact customer support (see SOM972_973 sheet). **Notes:** **1.** This SOM is applied when a delay in host I/O response due to reclamation processing occurs in a customer environment. **2.** Reclamation processing is delayed. **3.** This SOM is to prioritize host I/O response over reclamation processing in VxVM environment, so that the time required for reclamation processing may increase when this SOM is set to ON. For details about the interaction between this SOM and SOM 1069, contact customer support (see SOM1069 sheet).	OFF	-
973	Common	By setting this SOM, THP Page Size in Inquiry Page E3h is changed. THP Page Size varies depending on the combination of SOM972 and 973 settings. For	OFF	-

Mode	Category	Description	Default	MCU/RCU
		details, contact customer support (see SOM972_973 sheet). **Notes:** **1.** This SOM is applied when a delay in host I/O response due to reclamation processing occurs in a customer environment. **2.** When this SOM is set to ON, reclamation processing is delayed. **3.** This SOM is to prioritize host I/O response over reclamation processing in VxVM environment, so that the time required for reclamation processing may increase when this SOM is set to ON. For details about the interaction between this SOM and SOM 1069, contact customer support (see SOM1069 sheet).		
1015	Universal Replicator	When a delta resync is performed in a 3DC multi-target configuration with TC and UR, this SOM is used to change the pair status to PAIR/Duplex directly and then complete the delta resync. If the delta resync fails and all differential data items are copied, the pair status changes to COPY/Pending regardless of the SOM 1015 setting, and then it changes to PAIR/Duplex. When the existing delta resync function is required (pair status changes to COPY/Pending and then to PAIR/Duplex), set this SOM to ON before performing delta resync. If SOM 1015 is set (ON or OFF) while delta resync is being peformed, the setting is not applied. **Mode 1015 = ON:** The pair status changes to COPY/Pending and then to PAIR/Duplex when a delta resync is performed in a 3DC multi-target configuration. **Mode 1015 = OFF:** The pair status changes directly to PAIR/Duplex when a delta resync is performed in a 3DC multi-target configuration. **Notes:** **1.** The pair status changes directly to PAIR/Duplex when this SOM is OFF (default). Set this SOM to ON only when the status change to COPY/Pending and then PAIR/Duplex is required.	OFF	MCU

Mode	Category	Description	Default	MCU/RCU
		2. Set this SOM on the site of TC S-VOL in TC-UR 3DC configuration. If site switch by delta resync might occur, set this SOM on both TC primary and secondary sites. **3.** For microcode versions and storage system models that do not support this SOM, even if this SOM is set to OFF on L site of TC-UR delta configuration, the behavior does not change but the status changes to COPY/Pending and then the delta resync is completed. **4.** Regardless of the remote command device setting, the copy status does not change to COPY/Pending and then the delta resync is completed. **5.** If a delta resync fails, all-data copy works. In this case, the pair status changes to COPY/Pending and then the delta resync is completed even when this SOM is set to OFF. **6.** When this SOM setting is default (OFF), a delta resync operation is completed without pair status change to COPY/Pending. Therefore, if an operation depends on the pair status changing to COPY/Pending, such as running the CCI pairevtwait command, set this SOM to ON. **7.** When this SOM setting is default (OFF) (pair status changes directly to PAIR/Duplex), SIMs and SSBs that are reported due to a pair status change to COPY/Pending are not reported. **8.** If this SOM is set to ON or OFF during delta resync, the setting is not applied. Change this SOM setting before delta resync. **9.** During delta resync, downgrading the microcode to a version that does not support this SOM is disabled in TC-UR delta configuration. If microcode downgrade is disabled (FunctionID:0701) when delta resync is not in process, suspend the UR pair and then retry the microcode replacement.		
1021	Universal Volume Manager	This SOM can enable or disable the auto-recovery for external volumes of an EMC storage system. **Mode 0121 = ON:** An external volume that is blocked due to Not Ready status can be recovered automatically regardless of the type of external storage system.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Mode 1021 = OFF: An external volume that is blocked due to Not Ready status might not be recovered automatically depending on the type of external storage system. **Notes:** **1.** This SOM is applied when the auto-recovery of external volumes that are blocked due to Not Ready status is desired in UVM connection using an ECM storage system as an external storage system. **2.** When this SOM is set to ON and the connected external storage system is not in stable status (such as failure and recovery from failure), a blockage due to Not Ready status and auto-recovery might occur repeatedly.		
1043	Universal Replicator	This SOM disables journal copy. **Mode 1043 = ON:** When the following conditions are met at the UR secondary site, the journal copy is disabled. The following conditions (1) and (2) or (1) and (3) are met: **1.** 4,096 or more journals are accumulated at the secondary site. **2.** The CLPR write pending rate for journal volumes of MP unit for which journal ownership at the RCU is defined is 25% or higher (including the write pending rate for other than journal volumes). **3.** It takes 15 seconds or longer to start restore after journal copy at the RCU. **Note:** Even though the above conditions are met, journal copy is not disabled when all time stamps of the journals accumulated are the same in a consistency group containing multiple journals. **Mode 1043 = OFF:** The journal copy is not disabled. **Notes:** **1.** This SOM applies when one of the following conditions is met: **a.** Multiple journals are registered in a consistency group of CCI.	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		b. Multiple journals are registered in an extended consistency group. **c.** Journals are accumulated at the secondary site, causing the system performance to decrease. **2.** If SOM 690 is set to ON and the Write Pending rate is 60% or higher, the journal copy is disabled regardless of the setting of this SOM. **3.** When the host write speed is faster than the JNL copy speed, the usage rate of the master journal increases. **4.** This SOM is effective within the range of each CLPR. Therefore, an operation target LPRxx (xx= 00 to 31) needs to be selected before setting this SOM to ON/OFF. For example, when setting this SOM only to CLPR0 (even though this SOM is not set to CLPR 1 to 31), select "LPR00" and then set this SOM to ON/OFF. If "System" is selected and then this SOM is set to ON, this SOM is not effective for any of the CLPRs. **5.** Set SOM 1043 to ON when journals are not accumulated at the RCU. If journals have already been accumulated at the RCU, journal copy does not start until the journal usage rate becomes 0%. (If you need to set SOM 1043 to ON while journals are accumulated, set Purge Suspend, and then perform resync.)		
1068	Common	This mode can detect and report a minor drive response delay early by severely checking drives. **Mode 1068 = ON:** Drive response delay is checked and detected with conditions that are more severe than current conditions. When SOM 144 is set to ON, the drive with response delay is blocked. Target drive: HDD, FMD, SSD **Mode 1068 = OFF:** Drive response delay is checked and detected with current conditions. The behavior varies depending on the combinations of SOM settings. For details, contact customer support (see SOM144 sheet).	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** Apply this mode to detect a minor delay in drive response. **2.** When a delay is suspected, a processing to refer to the statistics data and determine the delay works. **3.** If SOM 157 is set to ON, the output prevention status of SSB=A4CE is not cleared in one-day cycle. **4.** When applying this mode only, a SIM for delay detection is reported but the drive is not blocked. To block the drive, SOM 144 also needs to be applied.		
1069	Common	By setting this SOM, the INQUIRY Page E3h field is changed. The field varies depending on the combination of SOMs 972, 973, and 1069. For details, contact customer support (see SOM1069 sheet). **Notes:** **1.** This SOM is applied when the page problem occurs in an environment where Symantec ASL 6.0.5 or higher is used and SOM 972 and/or 973 is set to ON. **2.** When this SOM is set to ON, reclamation processing is delayed. **3.** The priority of setting when SOMs are set at the same time is SOM 1069, 972, and then 973. The setting of higher priority SOM is enabled.	OFF	-
1070	Global-active device	This SOM changes the processing for a group operation with GAD consistency group (CTG). **Mode 1070 = ON:** The status change of all pairs in a consistency group. is performed for 50 msec. **Mode 1070 = OFF:** The status change of all pairs in a consistency group is performed for 1 msec.	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** This SOM is applied when reducing the time to complete status change of all pairs in a consistency group at a group operation (suspension and resync operation) with the GAD CTG function. In a system configuration where host I/O performance is prioritized, do not use this SOM because setting this SOM may affect the host I/O performance. **2.** The MP usage rate increases during status change of all pairs in a consistency group. For details about approximate percentage increase in MP usage rate, contact customer support (see SOM1070 sheet).		
1080	Global-active device Universal Volume Manager	This SOM is intended for a case that multiple external connection paths are connected to a Target port on an external system with a quorum disk and there is a path whose performance degrades. For such a case, this SOM can eliminate impacts on commands run for other external devices that share the Target port with the quorum disk on the external system by setting the time to run a reset command for the Target port to be the same (15 seconds) as that to run other commands for the other external devices. **Mode 1080 = ON:** The time to run the reset command for the quorum disk on the external system is 15 seconds to eliminate the impacts on commands run for the other external devices that share the Target port with the quorum disk on the external system. If a response to ABTS is delayed for 12 seconds or longer, the quorum disk may be blocked. **Mode 1080 = OFF:** The time to run a reset command for the quorum disk when performance of a path degrades is 3 seconds so that a retry is performed by an alternate path to avoid quorum disk blockage.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** This SOM is applied if avoiding impacts on commands for other external devices sharing a Target port on an external system side with a quorum disk is prioritized over preventing quorum disk blockage when a response to ABTS is delayed. The delay is caused due to path performance degradation in a configuration where the Target port is shared between external devices and the quorum disk. **2.** When connection performance degradation occurs, the quorum disk blockage is more likely to occur.		
1083	Dynamic Provisioning Universal Volume Manager	This SOM enables or disables DP-VOL deletion while an external volume associated with the DP-VOL with data direct mapping attribute is not disconnected. **Mode 1083 = ON:** DP-VOL deletion is enabled. **Mode 1083 = OFF:** DP-VOL deletion is disabled. **Notes:** **1.** This SOM is applied when the following conditions are met. ▪ A DP-VOL with data direct mapping attribute is deleted. ▪ The data of external volume with data direct mapping attribute associated with a deletion target DP-VOL with data direct mapping attribute will not be used again. **2.** When SOM 1083 is set to ON, the data of external volumes cannot be guaranteed. **3.** When DP-VOL deletion is performed without disconnecting an external volume, the data of the external volume cannot be guaranteed.	OFF	-
1086	Dynamic Provisioning Universal Volume Manager	This SOM enables or disables the performance improvement for Dynamic Provisioning volumes that are Universal Volume Manager volumes used as pool volumes. **Mode 1086 = ON:** The performance improvement is enabled.	ON	-

Mode	Category	Description	Default	MCU/RCU
		Mode 1086 = OFF: The performance improvement is disabled. **Notes:** **1.** This SOM is applied when the IOPS performance of an external storage system is higher than 80k × the number of installed MPBs, which is the value of IOPS that an entire local storage system sends to an external storage system. **2.** When it is required to set this SOM to OFF, if IOPS sent from the local storage system to the external storage system is higher than 80k × the number of installed MPBs, reduce the IOPS to lower than 80k × the number of installed MPBs, and then set this SOM to OFF. (Otherwise CWP increases and cache is overloaded.)		
1097	Common	This SOM disables the warning LED to blink when specific SIMs are reported. **Mode 1097 = ON:** When SIM=452XXX, 462XXX, 3077XY, 4100XX, or 410100 is reported, the warning LED does not blink. **Mode 1097 = OFF:** When SIM=452XXX, 462XXX, 3077XY, 4100XX, or 410100 is reported, the warning LED blinks. **Note:** This SOM disables the warning LED to blink when specific SIMs are reported.	ON	-
1106	Dynamic Provisioning Dynamic Tiering	This SOM is used to monitor the page usage rate of parity groups defined to a pool, and perform rebalance (the same as the rebalance that works at pool expansion or after 0 data page reclamation) to balance the usage rate if the rate differs significantly among parity groups. On VSP E series, this SOM is used to perform rebalance even when the number of reclaimed pages is 0 after 0 data page reclamation.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Mode 1106 = ON: The rebalance (the same as the rebalance that works at pool expansion or after 0 data page reclamation) (*3) works when one of the following conditions is met: **1.** The usage rate is checked for parity groups in a pool once a day, and the usage rate is not balanced (*1) among parity groups. **2.** After 0 data page reclamation, the number of reclaimed pages is 0 (*2). **Mode 1106 = OFF:** The rebalance does not work even when the usage rate is not balanced. *1: How to determine whether usage rate is unbalanced among parity groups The pool usage rate is determined as unbalanced when there is 25% or more difference between the usage rate of each parity group in the pool and the average. **Note:** The term "page usage rate" refers to the percentage of the number of assigned pages in each PG compared to the total number of pages in the pool. For HDT pools, the term "total number of pages" is the number of pages assigned within each specific tier. Examples: **1.** In an HDP pool, if the usage rates of PG1, PG2, and PG3 are 50%, 40%, and 30% respectively, it is not determined as unbalanced. Because the average parity group usage rate is (50%＋ 40%＋ 30%) / 3 ＝ 40% and the difference in the rate between each parity group and the average is 10% at the maximum. **2.** In an HDP pool, if the usage rates of PG1, PG2, and PG3 are 80%, 40%, and 30% respectively, it is determined as unbalanced. Because the average parity group usage rate is (80%＋ 40%＋ 30%) / 3 ＝ 50% and the difference in the rate between each parity group and the average is 30% at the maximum. **3.** In an HDT pool, if the usage rates of PG1, PG2, and PG3 are 80% (SSD), 40% (SAS15K) and		

Mode	Category	Description	Default	MCU/RCU
		30% (SAS15K), it is not determined as unbalanced, because: ▪ The average parity group usage rate of Tier1 is (80%) / 1 ＝ 80% and the difference in the rate between the parity group and the average is 0%. ▪ The average parity group usage rate of Tier2 is (40%＋ 30%) / 2 ＝ 35% and the difference in the rate between the parity group and the average is 5% at the maximum. *2: Condition for rebalance after 0 data page reclamation When the mode is set to ON, rebalance works even when reclaimed page is 0 at 0 data page reclamation. **Note:** This SOM is applied when balancing the usage rate is required at a customer site where the usage rate is not even.		
1113	Dedupe and Compression	If a problem occurs while the capacity saving function is enabled and the MP usage rate needs to be reduced to identify the failure, use this mode to stop asynchronous processing of host I/Os by the capacity saving function other than garbage collection and de-staging. **Mode 1113 = ON:** The asynchronous processing of host I/Os by the capacity saving function, other than garbage collection and de-staging, is stopped. **Note:** While the capacity reduction processing is not working, the capacity saving rate might degrade. **Mode 1113 = OFF:** The capacity saving function fully works. **Relationship between SOM 1113 and SOM 1112:** When both modes are set to ON, the setting of SOM 1112 is prioritized over that of SOM 1113. When SOM 1112 is set to ON, all asynchronous processing for host I/Os among those related to the capacity saving function are stopped, including garbage collection and de-staging, so that write I/Os to V-VOLs with Compression or Deduplication and Compression set are disabled.	OFF	-
1115	Dedupe and Compression	When LDEV format is performed for a virtual volume with capacity saving (Compression, or Deduplication and Compression, the same hereinafter) enabled,	ON	-

Mode	Category	Description	Default	MCU/RCU
		data is initialized without using metadata regardless of the mode setting. **Mode 1115 = ON:** When LDEV format is performed for a virtual volume with capacity saving enabled, the data is initialized without using the metadata. **Mode 1115 = OFF:** When LDEV format is performed for a virtual volume with capacity saving enabled, normal formatting is performed, but if one of the following conditions is met, the data is initialized without using metadata. ▪ There is a pinned slot. ▪ The capacity saving status is “Failed”. ▪ The virtual volume is blocked (Normal restore cannot be performed). The processing time increases with increase in pool capacity. Estimate of processing time: `Processing time (minutes) = (pool capacity (TB)/40) + 5` If the result of dividing the pool capacity by 40 has decimal places, round it up to the next integer. The processing finishes early if there is less capacity of allocated pages. For example, in the case of a 4-PB pool, normal formatting (SOM 1115 OFF) is faster if the LDEV capacity is 50 GB or less, therefore the performance of LDEV format without using metadata is better.		
1118	Open	This SOM is used to disable the ENC reuse function. **Mode 1118 = ON:** When a failure occurs in the Expander chip mounted on a controller board (CTLS, CTLSE) or an ENC board, the reuse function does not work but SIM=CF12XX is reported and the ENC is blocked. **Mode 1118 = OFF:** When a failure occurs in the Expander chip mounted on a controller board (CTLS, CTLSE) or an ENC board, the reuse function works. If the ENC is reusable, SIM=CF12XX and then CF14XX are reported, and the ENC is reused. If the ENC is not reusable, SIM=CF12XX is reported, and the ENC is blocked.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Note: The ENC reuse function is enabled as default. This SOM is applied when you want to disable the ENC reuse function.		
1169	Dedupe and Compression	(VSP E series) This mode can enable or disable the deduplication processing that works during resync processing from P-VOL to S-VOL by the copy function for DP-VOLs with capacity saving in Inline mode enabled. **Mode 1169 = ON:** Deduplication processing is not performed during resync processing.* **Mode 1169 = OFF:** Deduplication processing is performed during resync processing. * To reduce the capacity consumption in the case that the pool capacity is almost depleted for example, the deduplication processing might be performed during the resync processing. In particular, the following cases apply: ▪ The usage rate exceeds the warning threshold. ▪ Free capacity is smaller than about 240 GB.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** When SOM 1280 is ON, deduplication processing is performed even when SOM 1169 is ON. **2.** If conditions to disable deduplication processing by SOM 1191 are met, deduplication processing is not performed even when SOM 1169 is OFF. For details about the conditions to disable deduplication processing, contact customer support (see SOM1191 sheet). **3.** When SOM 1169 is set to ON, like the post mode, estimating and reserving the capacity of a temporary storing area in the copy target DP volume or pool in advance is necessary. **4.** SOM 1169 is not effective for the initial copy at pair creation, but there are some exceptional cases for SI and VM, such as pair creation using a used volume for S-VOL. In this case, deduplication processing is performed or not performed according to the mode setting. **5.** SOM 1169 is not related to determining whether to perform deduplication processing in synchronization with initial write. For example, the setting of SOM 1169 does not contribute to a reduction in time to migrate data to a newly defined volume.		
1174	Open Universal Volume Manager	This SOM is used to disable a path that is logged in from a host or an external storage system (host path and external path) to be used as an external path. **Mode 1174 = ON:** A path logged in from a host or an external storage system is excluded from the WWN discovery target. **Mode 1174 = OFF:**A path logged in from a host or external storage system is included in the WWN discovery target.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** Apply SOM 1174 when discovery is performed while specifying a universal port that is being logged in from a host or an external storage system. **2.** If SOM 1174 is set to ON, external volumes cannot be created using the paths being logged in from hosts and external storage systems. **3.** If WWN discovery is performed while SOM 1174 is set to ON, the storage system being logged in from hosts and external storage systems are displayed as [Unknown] in the discovery result.		
1191	Dedupe and Compression	When online data migration is performed on volumes whose capacity saving mode is set to Deduplication and Compression and inline, setting SOM 1191 to ON can mitigate the I/O performance degradation caused by the deduplication processing. **Mode 1191 = ON:** Inline deduplication processing is disabled when the average of MP usage rates on the entire storage system is 50% or higher. When SOM 1191 is ON, SOM 1191 applies to the entire storage system. **Mode 1191 = OFF:** Inline deduplication processing is not disabled regardless of the average MP usage rate. **Notes:** **1.** Before setting this mode to ON, estimate the temporary area in a pool and then reserve it in advance. For details, see the Caution* below. **2.** By setting the mode to ON, the inline deduplication processing is disabled when the average MP usage is 50% or higher even though SOM 1280 is set to ON. **3.** When SOM 1169 is set to ON, the inline deduplication at copy processing is disabled regardless of SOM 1191 setting.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		* **Caution:** When SOM 1191 is ON and MP usage (entire storage system) reaches or exceeds 50%, the pool used capacity increases due to consumption of temporary area for post-process deduplication processing. Before enabling this SOM, verify that there is enough pool capacity by using the following conditional expressions, and then set SOM 1191 to ON only when the applicable conditional expression is met: ▪ If SOM 1191 is set to ON during data migration: *pool-capacity* × *depletion-threshold* [%] / 100 > *current-pool-used-capacity* + (*data-capacity-to-be-migrated* × (100 - *estimated-compression-ratio* [%]*) / 100) ▪ If SOM 1191 is set to ON during normal operations: *pool-capacity* × *depletion-threshold* [%] / 100 > *current-pool-used-capacity* + (*data-capacity-to-be-written-to-non-write-area* × (100 - *estimated-compression-ratio* [%]*) / 100) where *estimated-compression-ratio* is the ratio of the estimated compression reduction effect. To convert the compression ratio in the N:1 format to percentage, use the following equation: *compression-ratio* [%] = (1 - 1 ÷ N) × 100 If the estimated compression ratio is not specified, use 0% to calculate.		
1198	TrueCopy Universal Replicator Global-active device	To expand TC, UR, and GAD pair capacity, the difference management method must be changed from shared memory (SM) difference management to hierarchical difference management. This mode is used to enable changing the difference management method by using CCI. The difference management method is changed at the first TC, UR, or GAD pair creation or resync operation after setting this mode.	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		Mode 1198 = ON: The difference management method for volumes of 4 TB or less used in TC, UR, or GAD pairs is changed to hierarchical difference management regardless of SOM 5, SOM 6, and SOM 1199 settings. **Mode 1198 = OFF:** ▪ When SOM 1198 is OFF and SOM 1199 is ON, the difference management method for volumes of 4 TB or less used in TC, UR, or GAD pairs is changed to SM difference management. ▪ When both SOM 1198 and SOM 1199 are OFF, the difference management method is not changed. **Notes:** **1.** Apply this mode when the storage system does not have an SVP and you want to expand the capacity of volumes used in TC, UR, or GAD pairs. **2.** Changing the difference management method can affect the I/O response performance depending on the I/O pattern. **3.** Changing the difference management method can affect the initial copy time depending on the conditions.		
1199	TrueCopy Universal Replicator Global-active device	This mode is used to enable changing the difference management method from hierarchical difference management back to SM difference management if necessary for some reasons after the method was changed to hierarchical difference management by setting SOM 1198 to ON. The difference management method is changed at the first TC, UR, or GAD pair creation or resync operation after setting this mode.	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		Mode 1199 = ON: ▪ When both SOM 1199 and SOM 1198 are ON, the difference management method for volumes of 4 TB or less used in TC, UR, or GAD pairs is changed to hierarchical difference management regardless of SOM 5 and 6 settings. ▪ When SOM 1199 is ON and SOM 1198 is OFF, the difference management method for volumes of 4 TB or less used in TC, UR, or GAD pairs is changed to SM difference management regardless of SOM 5 and 6 settings. **Mode 1199 = OFF:** ▪ When SOM 1199 is OFF and SOM 1198 is ON, the difference management method for volumes of 4 TB or less used in TC, UR, or GAD pairs is changed to hierarchical difference management regardless of SOM 5 and 6 settings. ▪ When both SOM 1199 and SOM 1198 are OFF, the difference management method is not changed. **Notes:** **1.** Apply this mode when the storage system does not have an SVP and you want to expand the capacity of volumes used in TC, UR, or GAD pairs. **2.** Changing the difference management method can affect the I/O response performance depending on the I/O pattern. **3.** Changing the difference management method can affect the initial copy time depending on the conditions.		
1201	Global-active device	This mode is used to select the volume for which failure suspend will occur while allowing the host access to the volume when failures occur on all remote paths between the storage systems while the connection between the quorum disk and either of the primary or secondary storage system is disconnected. You need to set this mode on both the primary and secondary storage systems.	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		Mode 1201 = ON: Failure suspend occurs on the volume of the storage system whose connection with the quorum disk is not disconnected while the host access to the volume is allowed. **Mode 1201 = OFF:** Failure suspend occurs on the primary volume while the host access to the volume is allowed. Apply this SOM when you want to continue operations on the storage system in the normal state, in a case in which a failure occurs on the path to the quorum disk and then a remote path failure occurs. Do not apply this SOM when you want to continue operations on the primary volume.		
1202	Common	This mode can be used to disable the logic of response performance improvement for host I/O during FMD or SSD drive firmware replacement. **Mode 1202 = ON:** ▪ Synchronous read I/Os are disabled. ▪ Read I/Os other than synchronous read are disabled. ▪ Write I/Os are disabled. **Mode 1202 = OFF:** ▪ Synchronous read I/Os can be done by collection read. ▪ Read I/Os other than synchronous read are disabled. ▪ Write: I/Os are disabled. **Notes:** **1.** Apply this mode when changing the behavior back to the previous one is required during FMD and SSD firmware replacement. **2.** When this mode is set to ON, the host I/O performance during FMD or SSD drive firmware replacement may be degraded.	OFF	--
1204	Dynamic Provisioning Dynamic Tiering Thin Image	This mode is intended to improve the page migration performance when the MP usage rate is within the range from 30% to 50%. **Mode 1204 = ON:** When the MP usage rate is within the range 30 to 50%, the processing interval is shortened to improve the page migration throughput.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		Mode 1204 = OFF: There is no change for the processing interval. For details, see sheet SOM 1204. **Notes:** **1.** Apply this mode when the following conditions are met: ▪ The MP usage rate constantly exceeds 30%. ▪ Prioritizing the page migration processing over the I/O processing is required. **2.** When SOM 1204 is set to ON, the operation frequency of the relocation processing increases so that the host I/O response performance is degraded. **3.** When SOM 904 is set to ON, the SOM 904 setting is prioritized. **4.** By setting SOM 1204 to ON, the MP usage rate increases by 3 to 10% due to the asynchronous processing, and the host I/O response may be degraded.		
1205	Dynamic Provisioning Dynamic Tiering Thin Image	Changes the background unmap processing speed for FMC drives. **Mode 1205 = ON:** Background unmap runs at up to 42 MB/s. **Mode 1205 = OFF:** Background unmap runs at up to 10 GB/s. **Notes:** **1.** The mode is applied to prevent the host response performance from being degraded due to background unmap. **2.** When SOM 1122 is set to ON, the SOM 1122 setting is prioritized. **3.** As releasing physical areas runs at the normal speed, the following phenomena may occur,	OFF	-

Mode	Category	Description	Default	MCU/RCU
		though the phenomena are solved immediately after the physical area release is complete: ▪ The used pool capacity does not decrease immediately after DP volume deletion. ▪ The saving ratio seems to be lower temporarily. ▪ The used pool capacity may increase due to rebalance.		
1211	Universal Replicator	This mode is to change the threshold for the write pending rate that is a condition to determine whether to disable journal data copy or not. By setting the mode to ON, the threshold of write pending rate that is a condition to disable journal data copy is changed from 25% to 50%. Journal data copy is disabled when the following conditions (1) and (2), or (1) and (3) are met: **1.** 4096 or more journal data sets are accumulated on RCU. **2.** The write pending rate of a journal volume in an MPB that has the ownership of the journal on RCU exceeds the threshold, 25% (mode OFF) or 50% (mode ON). (Including the write pending rate of those other than the journal volume) **3.** On RCU, it takes 15 seconds or longer to start a restore operation after the copy processing of journals is complete. **Note:** Even when the above conditions are met, if the time stamp of accumulated journal datasets is the same in a configuration where multiple journals are added to a consistency group, journal data copy is not disabled. **Mode 1211 = ON:** The threshold for the write pending rate is 50%. **Mode 1211 = OFF:** The threshold for the write pending rate is 25%.	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		Apply this mode when all of the following conditions are met: **1.** Disabling journal data copy is enabled by meeting one of the following conditions: SOM1043 is set to ON for each CLPR on the secondary site. A configuration where multiple journals are added to a CCI consistency group (open and mainframe). **2.** The write pending rate of a CLPR containing a journal on the secondary site exceeds 25%. The mode is effective for a CLPR. **Notes:** **1.** Though the mode can work on UR/URz RCU, apply it to both MCU and RCU assuming Disaster Recovery operation. **2.** This mode is related to SOM 1043. **3.** If SOM 690 is set to ON and the write pending rate is 60% or higher, journal data copy is disabled regardless of the setting of this mode. **4.** This mode is effective per CLPR. Therefore, select a target LPR xx (xx= 00 to 31), and then set the mode to ON or OFF. For example, when setting the mode to CLPR0 (CLPR 1 to 31 are not defined), select LPR00, and then set the mode to ON or OFF. When setting the mode by selecting System, the mode cannot be enabled for any CLPRs.		
1223	Dynamic Provisioning	This mode is used to disable the mapping consistency check processing that runs at Write Same command. The mapping consistency check processing causes response performance degradation if the transfer length is short, so this mode is available to prevent the performance degradation by disabling the processing. **Mode 1223 = ON:** The mapping consistency check processing does not run at Write Same command. **Mode 1223 = OFF:** The mapping consistency check processing runs at Write Same command.	OFF	--

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** Apply the mode when all the following conditions are met: **a.** The microcode that supports the mode is applied.(93-04-01 and later) **b.** The response time of Write Same command increase about 0.1 msec. **c.** The length of Write Same command is short. (less than 256KiB) **2.** The mode is effective for the entire storage system.		
1224	ShadowImage Thin Image Volume Migration Universal Replicator	The mode can disable or enable ownership migration for an LDEV whose ownership has been migrated to the MPU with P-VOL ownership at pair creation back to the previous MPU at pair deletion. **Mode 1224 = ON:** Ownership migration at program product pair deletion is disabled. **Mode 1225 = OFF:** Ownership migration at program product pair deletion is performed. * Different from other program products, the ownership in an MPU with the journal group ownership is migrated as follows in a UR/URz configuration. ▪ Ownership migration target： LDEV (journal volume, remote CMDDEV) ▪ Timing when ownership migration takes place: Journal volume deletion, journal group deletion from EXCTG, and mirror allocation release **Notes:** **1.** Apply the mode when preventing the MP usage rate increase is required. **2.** Ownerships are in a specific MPU so that I/Os may be concentrated on the MPU. **3.** Ownership migration does not work at pair deletion.	OFF	Both
1251	Common	This mode is used to enable online maintenance for controllers if controller recovery fails due to an I-path failure.	OFF	--

Mode	Category	Description	Default	MCU/RCU
		Mode 1251 = ON: When an error caused by an I-path failure is detected during controller recovery, the recovery is continued. In addition, some MPs of the other controller are forcibly blocked. **Mode 1251 = OFF:** When an error caused by an I-path failure is detected during controller recovery, the recovery is stopped. **Notes:** **1.** Apply the mode when controller recovery fails due to an I-path failure (SSB=3560), and the controller recovery still fails for the same reason even when the controller has been replaced with a new part. **2.** The MP usage rate increases because half of MPs on the controller are blocked. **3.** An error may be returned temporarily to the host because of the MP blockage. **4.** When controller recovery is performed while the mode is set to ON, MPs on the other controller are blocked due to failure.		
1254	Universal Replicator Universal Replicator for Mainframe	This mode is used to prevent the performance of a host I/O to a virtual volume with capacity saving enabled (DRD-VOL) from being degraded due to the copy processing of a replication program product (*) that runs in the background. * Replication program products: ShadowImage (SI), ShadowImage for Mainframe (SIz), Volume Migration (VM), FlashCopy (FC), Thin Image (HTI), TrueCopy (TC), TrueCopy for Mainframe (TCz), global-active device (GAD), Universal Replicator (UR), Universal Replicator for Mainframe (URz). Mode 1254 = ON: ▪ SI/SIz, VM, HTI, TC/TCz, GAD, UR/URz: The background copy processing stops when the WP rate of the copy target CLPR is 35% or higher. ▪ FC: The pace of the background copy is slowed down when the WP rate of the copy target CLPR is 35% or higher.	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		Mode 1254 = OFF: ▪ SI/SIz, VM, FC, HTI: As per the SOM 467 setting ▪ TC/TCz, GAD: As per the SOM 689 setting ▪ UR/URz: As per the SOM 690 setting **Notes:** **1.** Apply this mode when all the following conditions are met: **a.** Preventing the performance of a host write I/O to a DRD-VOL from being degraded due to overload by the background copy processing is required. **b.** It is acceptable that completing the background copy for a volume (*1) belonging to a CLPR whose WP rate is 35% or higher takes extra time equal to the time period during which the WP rate of the copy target CLPR is 35% or higher. **c.** Setting the mode for all CLPRs on the storage system is required. (For per CLPR setting, use SOM 1260.)		

Mode	Category	Description	Default	MCU/RCU
		d. A failure suspension of a UR/URz pair is acceptable (*2). The failure suspension occurs when the mode is set to ON to prioritize the host I/O performance in a UR/URz configuration, if the amount of host I/Os exceeds the amount of journal transfer so that the journal usage increases, and then the journal usage exceeds the threshold. **2.** By setting the mode to ON, the background copy is stopped when the WP rate is 35% or higher regardless of the settings of SOM 467, SOM 689, and SOM 690. **3.** Completing the background copy for a volume (*3) belonging to a CLPR whose WP rate is 35% or higher takes extra time equal to the time period during which the WP rate of the copy target CLPR is 35% or higher. Note that recovering a pair that is suspended due to failure takes longer time too. **4.** When UR/URz is used, if 35% or higher WP rate continues for a long time on RCU, a journal volume becomes full and may be suspended on MCU. To disable the background copy of replication program products other than UR/URz, do not set the mode to ON. Instead of setting the mode to ON, use different CLPRs for the UR/URz S-VOL and the journal volume, and for a DRD-VOL for which preventing performance degradation is required on RCU, and set SOM 1260 to ON for the CLPR of the DRD-VOL only. **5.** Apply the same setting of SOM1260 for the CLPR of UR/URz S-VOL and the CLPR of the journal volume. (Set the mode to ON or OFF for both CLPRs) **6.** When UR/URz is used, if operations are switched to RCU, as the previous MCU becomes RCU, meet the following conditions: **a.** The SOM setting is same for MCU and RCU.		

Mode	Category	Description	Default	MCU/RCU
		b. If different CLPRs are used for the UR/URz S-VOL and the journal volume, and for a DRD-VOL for which preventing performance degradation is required on RCU, use different CLPRs for the UR/URz S-VOL and the journal volume, and for a DRD-VOL for which preventing performance degradation is required on MCU too. **7.** When UR/URz is used, disable Inflow Control. If enabled, it may work because the copy is stopped by setting the mode to ON, resulting in degradation of host write I/O performance. *1: In CLPRs with the mode set to ON, the copy processing does not make progress for not only a DRD-VOL but also a normal volume and a virtual volume with capacity saving disabled. *2: Disable Inflow Control for journals. By setting SOM 1254, the background copy is stopped, the amount of host I/Os exceeds the amount of journal transfer, and the journal usage increases. If Inflow Control is enabled, failure suspension can be prevented, but Inflow Control works when the journal usage exceeds the threshold (80%), resulting in host write performance degradation. *3: Note that in CLPRs with the mode set to ON, the copy processing does not make progress for not only a DRD-VOL but also normal volume and virtual volume with capacity saving disabled.		
1260	Dedupe and Compression ShadowImage Volume Migration TrueCopy Global-active device Universal Replicator	This mode is used to prevent the performance of a host I/O to a virtual volume with capacity saving enabled (DRD-VOL) in the specified CLPR from being degraded due to the copy processing of a replication program product (*) that runs on the background. *: ShadowImage (SI), ShadowImage for Mainframe (SIz), Volume Migration (VM), Compatible FlashCopy® (FC), Thin Image (TI), TrueCopy (TC), TrueCopy for Mainframe (TCz), global-active device (GAD), Universal Replicator (UR), Universal Replicator for Mainframe (URz). **Mode 1260 = ON:**	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		SI/SIz, VM, TI, TC/TCz, GAD, UR/URz: The background copy processing stops when the WP rate of the copy target CLPR is 35% or higher. FC: The pace of the background copy is slowed down when the WP rate of the copy target CLPR is 35% or higher. **Mode 1260 = OFF:** SI/SIz, VM, FC, TI: As per the SOM 467 setting TC/TCz, GAD: As per the SOM 689 setting UR/URz: As per the SOM 690 setting **Notes:** **1.** Apply the mode when all the following conditions are met. ▪ Preventing the performance of a host write I/O to a DRD-VOL from being degraded due to overload by the background copy processing is required. ▪ It is acceptable that completing the background copy for a volume (*1) belonging to a CLPR whose WP rate is 35% or higher takes extra time equal to the time period during which the WP rate of the copy target CLPR is 35% or higher. ▪ Setting the mode per CLPR is required. (Setting for all CLPRs, use SOM 1254)		

Mode	Category	Description	Default	MCU/RCU
		▪ The mode setting for a CLPR of UR/URz S/VOL, and that for a CLPR of a journal volume are the same. (The mode is set to ON or OFF for both CLPRs) ▪ *1: Note that in CLPRs with the mode set to ON, the copy processing does not make progress for not only a DRD-VOL but also a normal volume and a virtual volume with capacity saving disabled. **2.** By setting the mode to ON, the background copy is stopped when the WP rate is 35% or higher regardless of the settings of SOM 467, SOM 689, and SOM 690. **3.** Completing the background copy for a volume (*2) belonging to a CLPR whose WP rate is 35% or higher takes extra time equal to the time period during which the WP rate of the copy target CLPR is 35%. Note that recovering a pair that is suspended due to failure takes longer time too. *2: Note that in CLPRs with the mode set to ON, the copy processing does not make progress for not only a DRD-VOL but also normal volume and virtual volume with capacity saving disabled. **4.** When UR/URz is used, if 35% or higher WP rate continues for a long time on RCU, a journal volume becomes full and may be suspended on MCU. To disable the background copy of replication program products other than UR/URz, use different CLPRs for the UR/URz S-VOL and the journal volume, and for a DRD-VOL for which preventing performance degradation is required on RCU, and set the mode to ON for the CLPR of the DRD-VOL only. **5.** When UR/URz is used, if operations are switched to RCU, as the previous MCU becomes RCU, meet the following conditions: ▪ The SOM setting is same for MCU and RCU.		

Mode	Category	Description	Default	MCU/RCU
		▪ If different CLPRs are used for theUR/URz S-VOL and the journal volume, and for a DRD-VOL for which preventing performance degradation is required on RCU, use different CLPRs for the UR/URz S-VOL and the journal volume, and for a DRD-VOL for which preventing performance degradation is required on MCU too.		
1267	Dynamic Provisioning Dedupe and Compression	This mode is used to control the speed of asynchronous processing of capacity saving. **Mode 1267 = ON:** The asynchronous processing of capacity saving listed below runs at low speed. **Mode 1267 = OFF:** The asynchronous processing of capacity saving listed below runs at normal speed. Asynchronous processing that runs at low speed by setting the mode to ON ▪ Disabling of the capacity saving function ▪ Deletion of LDEVs for which the capacity saving function is enabled ▪ Garbage collection ▪ Asynchronous capacity reduction processing ▪ Compression conversion of compression accelerator ▪ Garbage collection for collecting unnecessary meta data or user data of deduplication system data volume (data store) ▪ Deletion of unnecessary hash data for deduplication ▪ Expansion of meta data area of the capacity saving ▪ Correction of control information when SOM 1208 is set to ON ▪ Health check when SOM 1237 is set to ON	OFF	--

Mode	Category	Description	Default	MCU/RCU
		Notes: **1.** Apply this mode in the following cases: ▪ There is a possibility of drive overload by the asynchronous processing (asynchronous capacity reduction, disabling capacity saving, compression conversion of compression accelerator) that works after the data reduction setting (capacity saving, compression accelerator) is changed. ▪ The drive is overloaded by asynchronous processing of capacity saving. **2.** By setting the mode to ON, the capacity saving ratio may decrease. **3.** When an adaptive data reduction setting change is complete after setting the mode to ON, set the mode to OFF.		

Hitachi Vantara

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

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