# Hitachi Virtual Storage Platform Gx00 and Fx00

**SVOS 7.3.1**

## System Administrator Guide

This document provides information and instructions to help you use the maintenance utility and some of the functions in Device Manager - Storage Navigator as needed to perform system administration tasks and change settings for VSP Gx00 models or VSP Fx00 models. It explains the GUI features and provides basic navigation information.

**MK-94HM8016-10**
**December 2017**

# Contents

# Preface

This document provides information and instructions to help you use the maintenance utility and some of the functions in Device Manager - Storage Navigator as needed to perform system administration tasks and change settings for VSP Gx00 models or VSP Fx00 models. It explains the GUI features and provides basic navigation information.

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 operateVSP Gx00 models or VSP Fx00 models systems.

Readers of this document should be familiar with the following:

- Data processing and RAID storage systems and their basic functions.
- Hitachi Virtual Storage Platform G200, G400, G600, G800 or Hitachi Virtual Storage Platform F400, F600, F800 storage systems.
- The operating system and web browser software on the SVP hosting the Device Manager - Storage Navigator software.
- The Windows 7 operating system and the management software on the management server.

## Product version

This document revision applies to the following product versions:

- VSP Gx00 models and VSP Fx00 models: Firmware 83-05-1*x* or later
- SVOS 7.3.1 or later

## Release notes

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

# Changes in this revision

- Added procedure for enabling and disabling TLSv1.0 and TLSv1.1 communications.
- Updated the description of system option modes (SOMs) 15 and 1106.

# Referenced documents

The following documents are referenced in this guide.

- *Performance Guide*, MK-94HM8012
- *Hitachi SNMP Agent User Guide*, MK-94HM8015

# Document conventions

This document uses the following storage system terminology conventions:

| Convention | Description |
|---|---|
| VSP Gx00 models | Refers to all of the following models, unless otherwise noted.<br>▪ Hitachi Virtual Storage Platform G200<br>▪ Hitachi Virtual Storage Platform G400<br>▪ Hitachi Virtual Storage Platform G600<br>▪ Hitachi Virtual Storage Platform G800 |
| VSP Fx00 models | Refers to all of the following models, unless otherwise noted.<br>▪ Hitachi Virtual Storage Platform F400<br>▪ Hitachi Virtual Storage Platform F600<br>▪ Hitachi Virtual Storage Platform F800 |

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:<br>Click **OK**.<br>▪ Indicates emphasized words in list items. |

| Convention | Description |
|---|---|
| *Italic* | ▪ Indicates a document title or emphasized words in text.<br>▪ Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example:<br>`pairdisplay -g group`<br>(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:<br>▪ Variables are not clearly separated from the surrounding text or from other variables. Example:<br>`Status-<report-name><file-version>.csv`<br>▪ 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:<br>[ a \| b ] indicates that you can choose a, b, or nothing.<br>{ a \| b } indicates that you must choose either a or b. |

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

| Icon | Label | Description |
|---|---|---|
|  | Note | Calls attention to important or additional information. |
|  | Tip | Provides helpful information, guidelines, or suggestions for performing tasks more effectively. |
|  | Caution | Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash). |

| Icon | Label | Description |
|---|---|---|
|  | 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<br>Open-systems:<br>▪ OPEN-V: 960 KB<br>▪ Others: 720 KB |
| 1 KB | 1,024 ($2^{10}$) bytes |
| 1 MB | 1,024 KB or $1{,}024^2$ bytes |
| 1 GB | 1,024 MB or $1{,}024^3$ bytes |
| 1 TB | 1,024 GB or $1{,}024^4$ bytes |
| 1 PB | 1,024 TB or $1{,}024^5$ bytes |
| 1 EB | 1,024 PB or $1{,}024^6$ bytes |

# Accessing product documentation

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

# Getting help

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

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

# Comments

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

**Thank you!**

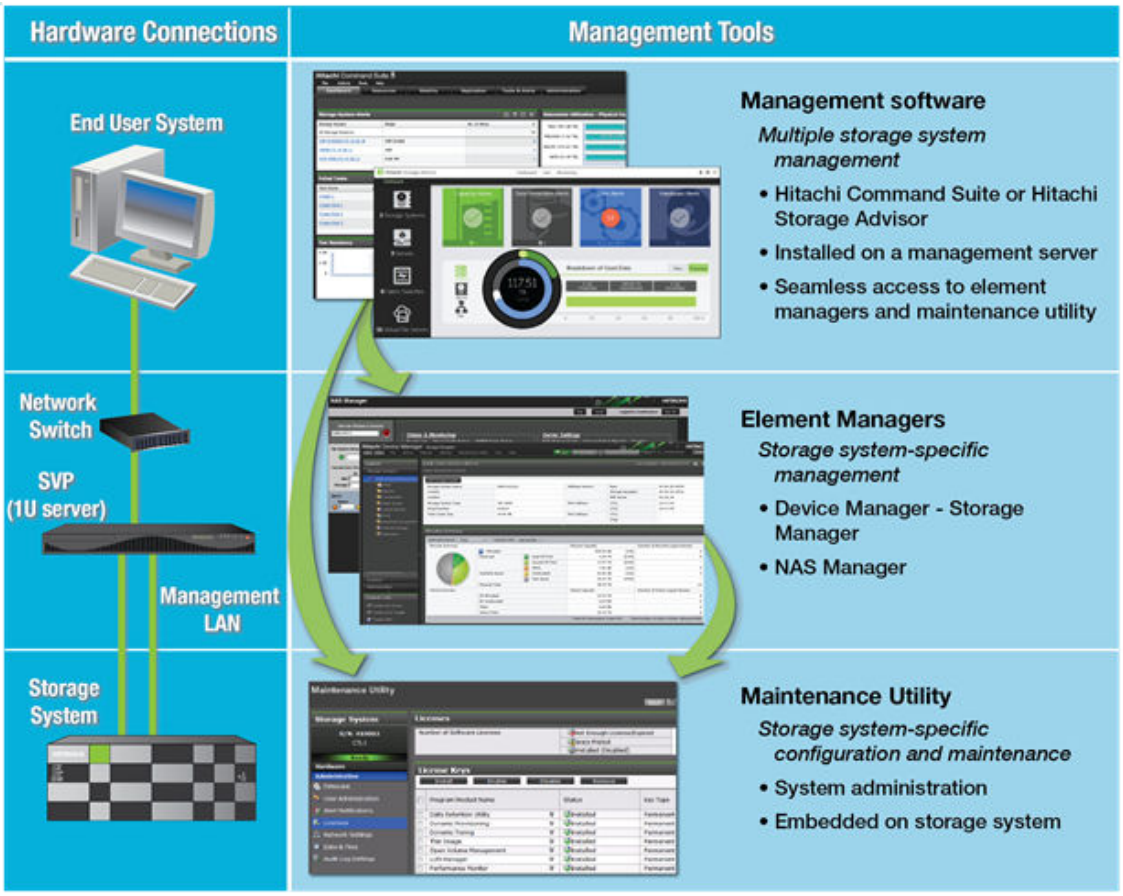
# Chapter 1: System administration overview

This chapter provides a high-level view of system administration tasks for the Hitachi Virtual Storage Platform G200, G400, G600, G800 or Hitachi Virtual Storage Platform F400, F600, F800 storage systems. It describes:

- Software architecture and access to system administration tools from management software (Hitachi Storage Advisor and Hitachi Command Suite).
- System administration tasks for the VSP Gx00 models and VSP Fx00 models storage systems, including some with NAS modules installed to provide native file functionality (VSP G400, G600, G800).

## System management architecture

The following figure shows a high-level view of the storage system management software architecture. It shows the access points that a system administrator can use to configure and manage the system settings.



# Ways to administer the storage system

The system administration tasks described in this guide apply to all VSP Gx00 models and Hitachi Virtual Storage Platform F400, F600, F800 storage systems, including those with NAS modules.

Users with storage systems that do not have NAS modules use Hitachi Storage Advisor (HSA), Device Manager - Storage Navigator, and the maintenance utility to administer block operations. If your storage system includes NAS modules, use NAS Manager to administer file operations, and then use the maintenance utility to verify that the settings are synchronized with block operations.

For more information about administration tasks for file operations, see the following documentation:

- *Storage Subsystem Administration Guide* (MK-92HNAS012)
- *Storage System User Administration Guide* (MK-92HNAS013)
- *File Services Administration Guide* (MK-92HNAS006)
- *Server and Cluster Administration Guide* (MK-92HNAS010)
- *System Access Guide* (MK-92HNAS014)

For more information about HSA, see the following documentation:

- *Hitachi Storage Advisor Getting Started Guide* (MK-94HSA001)
- *Hitachi Storage Advisor RESTful API Reference Guide* (MK-94HSA003)
- *Hitachi Storage Advisor User Guide* (MK-94HSA004)

You can also perform some administration tasks from a command line. For information, see Command Control Interface User and Reference Guide (MK-90RD7010) and the Command Control Interface Command Reference (MK-90RD7009), which you can access from the Documentation page of NAS Manager.

## Overview of Storage Advisor

Hitachi Storage Advisor is a unified software management tool that reduces the complexity of managing storage systems by simplifying the setup, management, and maintenance of storage resources.

Storage Advisor reduces infrastructure management complexities and enables a new simplified approach to managing storage infrastructures. It provides intuitive graphical user interfaces and recommended configuration practices to streamline system configurations and storage management operations. You can leverage Storage Advisor to easily provision new storage capacity for business applications without requiring in-depth knowledge of the underlying infrastructure resource details. It provides centralized management while reducing the number of steps to configure, optimize, and deploy new infrastructure resources.

Some of the key Storage Advisor capabilities include:

- Simplified user experience for managing infrastructure resources. Visual aids enable easy viewing and interpretation of key management information, such as used and available capacity, and guide features to help quickly determine appropriate next steps for a given management task.
- Recommended system configurations to speed initial storage system setup and accelerate new infrastructure resource deployments.

- Integrated configuration workflows with Hitachi recommended practices to streamline storage provisioning and data protection tasks.
- Common, centralized management for supported storage systems.
- A REST-based API to provide full management programmability and control in addition to unified file-based management support.
- Storage Advisor enables automated SAN zoning during volume attach and detach. Optional auto-zoning eliminates the need for repetitive zoning tasks to be performed on the switch.

## Unified management of block storage and file storage

Storage Advisor can be used to onboard and configure both block storage and file storage if NAS modules are included in the chassis of a supported storage system.

### Understand block and file storage

- Block storage:

  In block storage, volumes of storage are created. A server-based operating system can connect to each block of storage and control it as an individual hard drive. Each storage block can be individually formatted with the required file system, such as NTFS or VMFS. Block storage systems are typically deployed in a Storage Area Network (SAN) environment.

  From the dashboard of Storage Advisor, you can discover, register, and onboard a block storage system.

- File storage:

  Storage Advisor supports unified onboarding and configuration of file storage in the form of NAS modules.

  If a supported storage system includes NAS modules, the file storage is automatically added with the block storage. Then file pools and other file resources can be created in the Storage Advisor interface or by using the API.

### Adding block and file storage together

Storage Advisor enables you to add block and file storage in a single step. The only requirements are the service processor (SVP) IP address, user name, and password. When the file storage is added, the cluster is automatically registered in Storage Advisor.

### Unified configuration

Once a storage system is onboarded, all block and file resources can be configured and managed from a single Storage System page. File pool creation workflow incorporates best practices that simplify workflow and enhance usability. The file pools are used to easily create virtual file servers, file systems, and shares and exports. File system creation automatically mounts and formats the new file system.

### Unified reporting

Capacity is reported for all aggregated storage systems in the dashboard.

Capacity is also displayed for each storage system in the Storage System detail page.

Three views of capacity are available: file only, block only, or a unified view of block and file.

## Dashboard

Once a storage system has been onboarded to Storage Advisor, the dashboard displays as soon as you log in. The Storage Advisor dashboard provides the tools to easily configure, manage, and monitor storage systems.


From the Storage Advisor dashboard, you can access managed resources and provision storage in the context of a given storage system or server. The provided templates and configurations make it possible to quickly and easily provision a storage system, without knowing the details of the underlying hardware and software.

The top navigation menu provides access to Jobs and Monitoring pages. Links to the following settings are available, based on the user role:

- Tier Management
- Security Settings
- SNMP Settings
- Change Local Password

The dashboard has three distinct sections:

- **Resource side panel:** The left pane provides quick access to review the configuration of your storage systems, servers, and fabric switches. If the storage system includes NAS modules, virtual file servers can also be accessed.
- **Alert tiles:** Four alert tiles represent various aspects of the health of the storage system. When Storage Advisor detects a problem with a storage system environment, a number appears in the tile. The number indicates the number of alerts for that aspect of the storage system. Click the alert tile to go directly to a summary of the problems.
- **Resource summary:** The middle area, with the information gauge, provides a summary of the capacity allocated from the registered storage systems.

### Resource side panel

The resource side panel enables quick access to storage systems and to servers.

- Click **Storage Systems** to view and add storage systems.

- Click **Servers** to view and add servers.
- Click **Fabric Switches** to view and add fabric switches.
- Click **Virtual File Servers** to view and add virtual file servers. Displays if the storage system includes NAS modules.

### Alert tiles

Across the top of the dashboard are tiles that display alerts for storage capacity, data protection, jobs, and hardware.

If a tile includes a circled check mark, there are no alerts for that part of the storage system, and everything is functioning normally. A number in a red circle within a tile indicates one or more problems with that part of the storage system.

You can click a tile for Capacity Alerts, Data Protection Alerts, or Hardware Alerts to view the summary for the category in the Monitoring tab.

The Jobs Alert tile displays the number of jobs in the last 24 hours with a status of **Failed** or **Success with Errors**.

### Resource summary

The circular information gauge displays capacity metrics for the available storage.

- If the storage systems include file storage, you can click **Block** or **File** next to the information gauge to view a legend and capacity values for either type of storage. Click **Unified** to view a legend and capacity values for both block and file.
- For block-only storage systems, the numerical data for each capacity parameter in the ring is displayed to the left of the information gauge.
- The number in the center of the rings shows the total usable capacity of all storage systems. The total usable capacity is the capacity available from all the parity groups across all storage systems.

  If you do not have any parity groups configured on the storage system, this number is zero and all other data points in the capacity visualization are zero.

  **Note:** To understand uninitialized raw capacities, review the available unused disks on the detail page for each storage system.
- The light grey ring indicates the sum of all pool capacity available across all storage systems. The dark grey indicates the parity group capacity that is not yet allocated to pools.

  If you do not have any pools created, the light grey ring indicates zero. As you create pools, this number increases to eventually become equal to the total usable capacity when you have consumed all parity groups for pool creation.

  **Note:** Allocated to Pools plus Unallocated to Pools equals the Total Usable Capacity in the center of information gauge.
- The light green ring (Thin Used) indicates the storage utilization. As you create volumes on the pools and start consuming capacity, the utilization of thin pools increases and you will notice the value in green starting to increase.

  If Thin Used starts to increase and get closer to your total pool capacity, that indicates that the pools may be starting to fill up.

**Note:** The Thin Free and Thin Used capacities include both Thin and Snap. Thin Used plus Thin Free equals Allocated to Pools.

- Physical capacity allocated to file pools is indicated by medium blue in the File view and by light blue in the Unified view.
- File pool utilization is indicated by light blue in the File view and by medium blue in the Unified view.
- File over-commit capacity is represented by darkest gray in the outer ring of the File view.
- The subscribed capacity of all volumes, as a percentage, is represented by white in the outermost ring in the Block and Unified views. If the white ring extends outside the circle, it indicates oversubscription. Capacity subscription beyond the total available capacity should not be an issue if your capacity utilization is well within the total capacity.
- Physical capacity, or total usable capacity across all parity groups, is represented by dark blue in the outermost ring in the Block and Unified views.

If you notice the total pool capacity (light grey) and Thin used (light green) values getting closer to total capacity, you may be running out of storage on one or more storage systems and may need to add disks to increase storage capacity. Review the information gauge for each storage system to identify which storage system needs additional capacity. In addition, check disks for each storage system to determine if there is unused capacity available for parity group creation.

The right side of the resource summary offers alternate views:

- **Protection:** is the breakdown of data protection metrics including a representation of types of protected, unprotected, and secondary capacity and gauge of the total percentage of capacity protected.
- **Tier Breakdown:** is a visualization of the amount of each tier that is allocated to pools.
- **Savings:** tab displays the following ratios:
  - **Data Reduction:** : The ratio of logical used capacity to the physical used capacity, for all compression and deduplication technologies. It is calculated as follows:
    - For disk-based compression = Capacity 1 / Capacity 2.
    - For controller-based compression = Capacity 3 / Capacity 4.
    - Data reduction savings = Capacity 1 + Capacity 3 / Capacity 2 + Capacity 4.
    - Capacity 1 = logical used capacity of a parity group.
    - Capacity 2 = physical used capacity of a parity group.
    - Capacity 3 = logical used capacity of a pool.
    - Capacity 4 = physical used capacity of a pool.
  - **Capacity Efficiency:** : The ratio of Thin Free plus Thin Used to the physical used capacity. Capacity efficiency is only calculated for volumes on HDP and HDT pools.
    - If disk-based compression is in use, either alone or in combination with controller-based compression, the physical used capacity is that resulting from disk-based compression alone.
    - If only controller-based compression is in use, the physical used capacity is that resulting from controller-based compression.

- If no compression is in use then physical used capacity is the used capacity of the pool(s).

## *Analyzing data in the dashboard*

The dashboard is a visual display of the important information needed to analyze the overall capacity utilization and health of your storage system. It provides visual indicators such as total usable capacity, current utilization, data protection summary, and monitoring alerts.

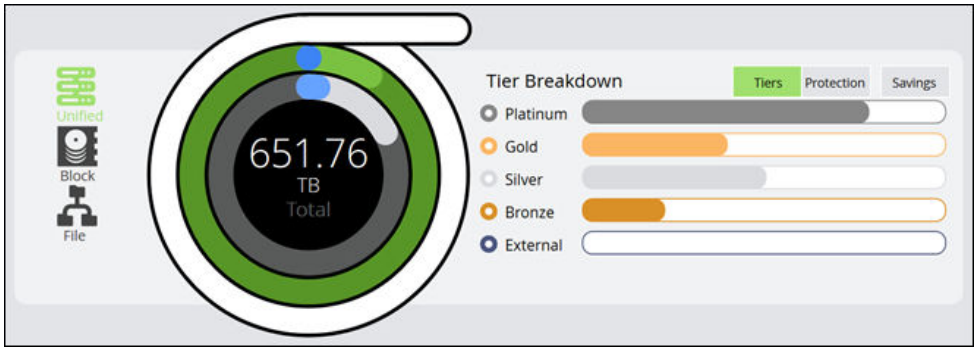
### Analyzing data shown in alert tiles

The alert tiles collectively present the health of the storage system environment. In one glance you can verify that the overall health is sound if you see no alerts on the alert tiles. This means that there are no capacity or hardware issues in the environment, no failed jobs in the last 24 hours and that the data protection is working without any issues.

If there are any alerts, you can drill down to the relevant alert page to investigate the cause. Storage Advisor provides alerts for capacity utilization, hardware, data protection, and jobs status.

### Analyzing data in the information gauge

The information gauge provides a visual indication of the total capacity of all storage systems managed by Storage Advisor.




The capacity indicated in the center of the ring is the total usable capacity available via the configured parity groups. After you add a storage system and configure parity groups, the total capacity indicator will show the capacity from the newly added storage system. The Thin Used capacity (light green ring) indicates the total capacity that is currently being used. If the usage is around 70-80% of the total capacity, you may receive capacity alerts based on the thresholds set by your storage administrator. The default thresholds are 70% and 80%, and can be changed during pool creation.

The light grey ring that provides a sum of capacities of all pools in the systems should be closer to 100% capacity. This would mean that you are using your entire parity group capacity by allocating it to pools. If the Thin Used capacity ring (light green) nears the total capacity (light grey ring) then you may run out of pool capacity soon. In such a case, expand the pool to consume more capacity.

If you notice that the total pool capacity (light grey ring) and Thin used (light green ring) values are getting closer to total capacity, you may be running out of disk capacity on one or more storage systems and would need to add disk space to increase storage capacity. Before adding disk space:

- Review the information gauge for each storage system to identify which storage system needs additional capacity.
- Review unused disks for each storage system to determine if any raw unused capacity is available for parity group creation.

Capacity subscription beyond the total available capacity should not be an issue if your thin capacity utilization is well within the total capacity.

### Analyzing tier metrics

As parity groups are created, the various disk types become categorized into tiers. The tiers and corresponding disk types are shown below.

**Table 1 Tier definitions**

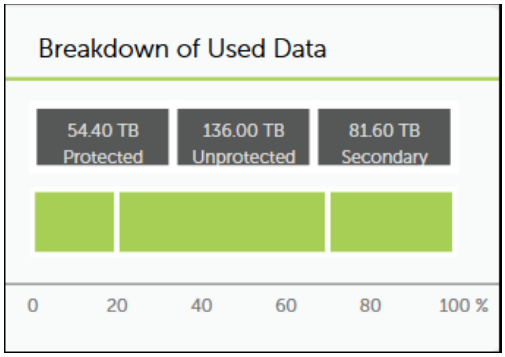
| Tier | Disk type |
|---|---|
| Platinum | SSD, FMD, and FMD DC2 |
| Gold | SAS 15 k |
| Silver | SAS 10 k |
| Bronze | SAS 7.2 k |

**Note:** Adding all tier capacities together equals the Total Usable Capacity in the center of the information gauge.

### Analyzing data protection metrics

The balance of your protected primary volumes and secondary volumes depends on the number of copies you have chosen to maintain, and also on the type of the data protection technology being used. If you choose to set aside more volumes for data protection, then the overall usable capacity may be affected. On the other hand, if you have a large amount of unprotected data, you may want to consider data protection options.

**Note:** These data protection capacity numbers are based on oversubscribed allocations and as a result will correlate with the overall oversubscription percentage, not the usable capacity numbers represented in the rest of the information gauge.



### Inventory and resource information

The inventory pages display details about the storage system resources in Storage Advisor. These resources include storage systems, servers, ports, and pools, volumes, parity groups, external parity groups (if the storage system has external storage), and replication groups. If the storage system has NAS modules, resources will also include file pools, virtual file servers, file systems, and shares and exports. Common actions can be performed on the inventory pages, such as the following:

- You can select one or more resources and delete them.

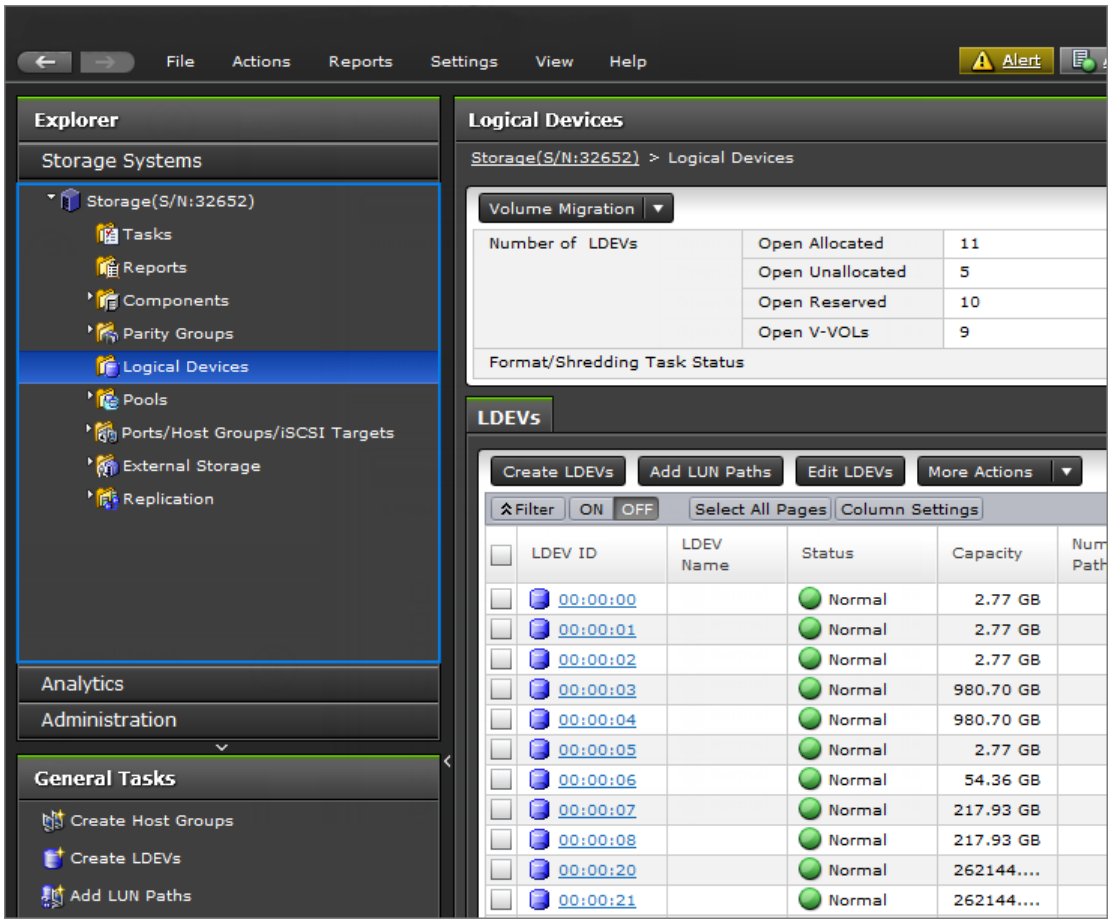
  When you delete a storage system, you disassociate it from Storage Advisor. When you delete a pool or volume, the resource is de-provisioned and removed from the storage system.
- When a parity group is deleted, it is removed from the storage system and the disks used to create the parity group are no longer in use. You can delete the parity group if you want to reconfigure the storage system with some other RAID configuration or simply decommission the array. If the parity group is in use by a pool, the parity group deletion will fail.
- You can select one or more of the same type of resources and update their properties. The properties that can be updated depend on the type of resource.
- You can click a particular resource to see more details about it on its resource detail page.
  - When you delete a block pool, the parity groups used by the pool will no longer be in In Use status. The pool volumes on these parity groups will be formatted and the parity group will eventually be in Available status.
  - When you delete a volume, the pool subscription will go down. Volume deletion will fail if the volume participates in data protection or is attached to a server.
  - When you delete a file pool, the underlying related block pool is deleted.
  - When you delete a server, the server is disassociated from Storage Advisor. You will no longer be able to provision volumes to the server (or its WWNs). Server deletion will fail if it has volumes attached to it.

## Device Manager - Storage Navigator

Device Manager - Storage Navigator (HDvM - SN) is the application used to configure the storage system. It is factory-installed and runs on the service processor (SVP) connected to the storage system.

You can access Device Manager - Storage Navigator from the management software to perform additional system administration tasks on your storage system besides those available in the maintenance utility. In addition, you can easily access advanced storage configuration options while performing management operations with the management software.

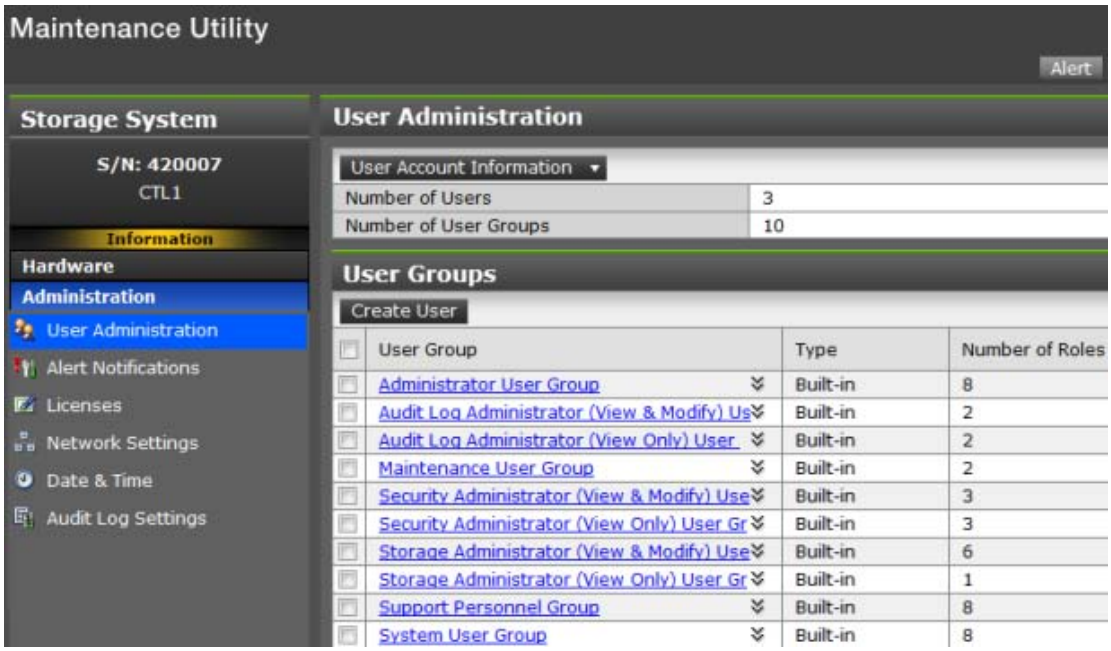
In addition to the information in this guide, the HDvM - SN online help has procedures for setting up and managing the storage system.




## Maintenance utility

The maintenance utility allows you to perform administration tasks on VSP Gx00 models or VSP Fx00 models. You can access this tool from either HDvM - SN, SMU, or the management software.

You can use the maintenance utility to configure settings such as licenses, syslog, alerts, and network configuration. As shown in the following figure, these settings are available from the **Administration** navigation tree.



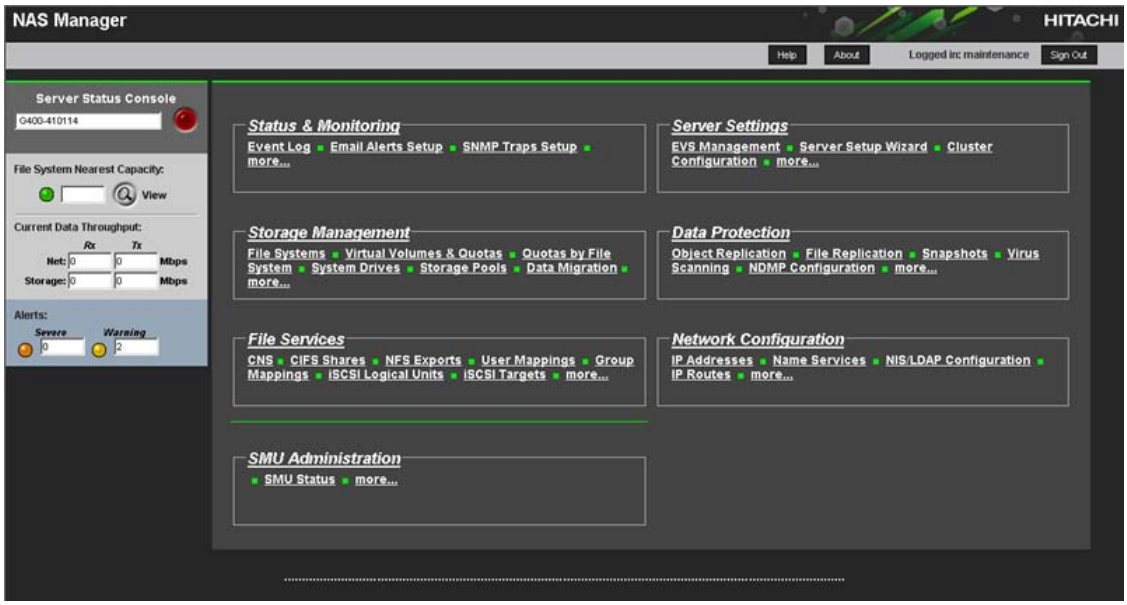

The maintenance utility online help provides procedural information for supported storage system administration tasks. Links to storage system tasks, search functions, and a glossary are included.

**Note:** Self-service features that are used to install and remove hardware components and to update the firmware are currently available for use only by customer support personnel or by authorized service providers.

## NAS Manager

NAS Manager is the element manager for NAS modules. It is a factory-installed application running on the NAS module.

NAS Manager provides a web-based interface for managing stand-alone or clustered servers and their attached storage systems. This tool allows you to perform most administrative tasks from any client on the network using a network browser. To access NAS Manager, point your browser to the following URL: `https://<unified-management-IP-address>:20443`. You can also access NAS Manager from a command line interface. For information, see the *Command Line Reference*, which is accessible through the **Documentation** page of NAS Manager or the *NAS Platform System Access Guide*.


NAS Manager
HITACHI
Help
About
Logged in: maintenance
Sign Out
Server Status Console
G400-410114
File System Nearest Capacity:
View
Current Data Throughput:
Rx
Tx
Net:
Storage:
Mbps
Alerts:
Severe
Warning
Status & Monitoring
Event Log ▪ Email Alerts Setup ▪ SNMP Traps Setup ▪ more...
Server Settings
EVS Management ▪ Server Setup Wizard ▪ Cluster Configuration ▪ more...
Storage Management
File Systems ▪ Virtual Volumes & Quotas ▪ Quotas by File System ▪ System Drives ▪ Storage Pools ▪ Data Migration ▪ more...
Data Protection
Object Replication ▪ File Replication ▪ Snapshots ▪ Virus Scanning ▪ NDMP Configuration ▪ more...
File Services
CNS ▪ CIFS Shares ▪ NFS Exports ▪ User Mappings ▪ Group Mappings ▪ iSCSI Logical Units ▪ iSCSI Targets ▪ more...
Network Configuration
IP Addresses ▪ Name Services ▪ NIS/LDAP Configuration ▪ IP Routes ▪ more...
SMU Administration
▪ SMU Status ▪ more...

# Chapter 2: Preparing your management software

Use the information in this chapter to prepare the management software you want to use to administer your storage system.

## Configuring Storage Advisor

Storage Advisor is deployed on a virtual machine and accessed by a client computer.

After installing Storage Advisor on a virtual machine, you must perform the following tasks:

- Change the root password
- Log into Storage Advisor
- Generate and install a signed SSL certificate

For more details about configuring Storage Advisor, see *Hitachi Storage Advisor Getting Started Guide*.

## Configuring Device Manager - Storage Navigator

To configure the storage system using Hitachi Device Manager - Storage Navigator, set up a client computer, and then log in to Hitachi Device Manager - Storage Navigator.

### Setting up a management client

Before running Device Manager - Storage Navigator on a management client, certain web browser guidelines must be observed. Some guidelines apply to all browsers, while other are specific to Internet Explorer and servers running Windows.

#### Requirements for management clients

The Device Manager - Storage Navigator administrator is responsible for setting up management clients.

The administrator's responsibilities include:

- Ensuring that Device Manager - Storage Navigator management clients run on supported versions of Windows and UNIX/Linux operating systems.
- Verifying that management clients can access and use Device Manager - Storage Navigator.

- Configuring the server if you use a physical or virtual server running on Windows as a management client.

### General requirements

- An SVP, required for system maintenance, must be connected to the storage system. Device Manager - Storage Navigator connects to the SVP through a TCP/IP network.
- 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 SVP concurrently.
- Use thinnet coaxial cable for twisted-pair LAN connections. Maximum cable length is 607 feet (185 meters). For assistance, contact the customer support.

### Requirements for Windows-based computers

**Note:** The combinations of operating system, architecture, browser, Java Runtime Environment, and Adobe Flash Player described below are fixed requirements. Using other combinations or versions might produce unpredictable results such as the inability to operate program windows. Therefore, contact customer support to use other combinations or versions.

**Hardware requirements**

| Item | Requirement |
|---|---|
| Processor (CPU) | Pentium 4 640 3.2 GHz or better<br>(Recommended: Core2Duo E6540 2.33 GHz or better) |
| Memory (RAM) | 2 GB or more<br>Recommended: 3 GB |
| Available storage space | 500 MB or more |
| Monitor | True Color 32-bit or better<br>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<br>1000BASE-T |

**Software requirements**

| Operating system | Architecture | Browser | Java Runtime Environment (JRE) | Adobe Flash Player |
|---|---|---|---|---|
| Windows 7 SP1 | 32 bit or 64 bit | Internet Explorer 11.0 | JRE 7.0 Update 67 | 14.0 |
| Windows 8.1 | 32 bit or 64 bit | Internet Explorer 11.0 | JRE 7.0 Update 67 | 14.0 |
| | | Google Chrome 48.0 or later | JRE 8.0 Update 71 | 20.0 |
| Windows 8.1 | 64 bit | Internet Explorer 11.0 | JRE 7.0 | 20.0 |
| | 64 bit | Internet Explorer 11.0 | JRE 7.0 | 21.0 |
| | 64 bit | Google Chrome | JRE 7.0 or later | Installed as a plug-in of Web browser |
| Windows 10 | 64 bit | Internet Explorer 11.0 | JRE 7.0 | 20.0 |
| | 64 bit | Internet Explorer 11.0 | JRE 7.0 | 21.0 |
| | 64 bit | | JRE 7.0 or later | Installed as a plug-in of Web browser |
| Windows Server 2008 R2 (SP1) | 64 bit | Internet Explorer 11.0 | JRE 7.0 Update 67 | 14.0 |
| Windows Server 2012 SP1 | 64 bit | Internet Explorer 10.0 | JRE 7.0 Update 67 | 14.0 |
| Windows Server 2012 R2 SP1 | 64 bit | Internet Explorer 11.0 | JRE 7.0 Update 67 | 14.0 |
| Windows Server 2016 | 64 bit | Internet Explorer 11.0 | JRE 8.0 Update 111 | 24.0 |

**Notes:**

- 
- If the SVP supports Internet Protocol Version 6 (IPv6), you can specify IPv6 addresses.
- Use Adobe Flash Player with the same architecture (32 bit or 64 bit) as the browser.
- Only the latest version of Internet Explorer active on each OS is supported, according to Microsoft support policy.
- The management client must be restarted after enabling Adobe Flash Player.

**Note:** To use Device Manager - Storage Navigator secondary windows, first install Java Runtime Environment (JRE).

## *Requirements for UNIX/Linux-based computers*

**Note:** The combinations of operating system, architecture, browser, Java Runtime Environment, and Adobe Flash Player described below are fixed requirements. Using other combinations or versions might produce unpredictable results such as the inability to operate program windows. Therefore, contact customer support to use other combinations or versions. To see the latest platform listed in the applicable product documents, visit our web site from the following URL: https://knowledge.hds.com/Documents.

### Hardware requirements

| Item | Requirement |
|---|---|
| Processor (CPU) | Pentium 4 640 3.2 GHz or better<br>(Recommended: Core2Duo E6540 2.33 GHz or better) |
| Memory (RAM) | 2 GB or more<br>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<br>1000BASE-T |

### Software requirements

| Operating system | Architecture | Browser | Java Runtime Environment (JRE) | Adobe Flash Player |
|---|---|---|---|---|
| Solaris 10 | 32 bit | Firefox 3.6.28 | JRE 6.0 Update 20 | 10.3 |
| | | Firefox 31 | JRE 7.0 Update 67 | 11.2 |
| Red Hat Enterprise Linux AS version 6.2 | 64 bit | Firefox 3.6.28 | JRE 6.0 Update 20 | 10.3 |
| | | Firefox 35 | JRE 7.0 Update 67 | 11.2 |

| Operating system | Architecture | Browser | Java Runtime Environment (JRE) | Adobe Flash Player |
|---|---|---|---|---|
| **Notes:**<br>▪ IPv6 HTTPS connections from Firefox are not supported.<br>▪ Use Adobe Flash Player with the same architecture (32 bit or 64 bit) as the browser.<br>▪ Device Manager - Storage Navigator supports Firefox 3.6.28, but the maintenance utility does not. | | | | |

**Note:**

To use Device Manager - Storage Navigator secondary windows, first install Java Runtime Environment (JRE).

### Setting up TCP/IP for 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.

For details about setting up the SVP, see the *Hardware Installation and Reference Guide* for your storage system.

### Configuring the web browser

To configure the client web browser, note the following:

- The browser must allow first-party, third-party, and session cookies.
- Pop-up blocker and plug-ins must be disabled.
- The management client must be connected to the network via LAN.
- The version of Adobe Flash Player specified in the management client requirements must be installed.

Consult your browser's documentation for instructions.

## Device Manager - Storage Navigator secondary windows

The Device Manager - Storage Navigator secondary window runs within the Java Runtime Environment (JRE). The secondary window opens when you select a menu on the Device Manager - Storage Navigator main window. The following functions and software applications use secondary windows:

- Authentication function of LUN Manager
- Login Message function
- Data Retention Utility
- Server Priority Manager

To use the Device Manager - Storage Navigator secondary window, you must enable it in advance. For details about enabling the secondary window, see Enabling the Device Manager - Storage Navigator secondary window (on page 37) . By default, this setting is disabled. When disabled, these functions and software applications do not appear in the menu on the Device Manager - Storage Navigator main window.

Google Chrome shows the message "This type of file can harm your computer. Are you sure you want to download `<file name>.jnlp`?" when you open the secondary window.

Click Save in the message window and save the object file. Then open the file. Continue the operation though Java security warning is displayed when you open the file.

**Note:**

`SJsvlSNStartServlet (<serial number>).jnlp` is saved in the download folder. This file is duplicated every time you open the second window because this file is not overwritten or deleted automatically. Delete extraneous downloaded `SJsvlSNStartServlet (<serial number>).jnlp` files periodically to prevent shortage of disc capacity. To confirm the download location, follow Chrome Menu > Settings > Show advanced settings > Downloads.

**Note:**

Do not click Discard in the message window, or you will be unable to operate for a while until the error (20020-108000) appears. Click OK to close the error and operate again.

If you don't want to wait for the error to appear, close Chrome and log in to Device Manager - Storage Navigator again.

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

## Requirements for using HDvM - SN secondary windows

This topic describes the configuration prerequisites for using Device Manager - Storage Navigator secondary windows.

### *Installing and configuring JRE*

JRE must be installed and configured in a Windows or Unix environment. You can download JRE from http://www.oracle.com/technetwork/java/index.html.

*Path setting (UNIX)*

Verify that JRE is installed correctly by opening the ControlPanel.html file. It is located in the JRE root directory. If the file opens, JRE is installed correctly.

*Configuring JRE*

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

### Enabling the Device Manager - Storage Navigator secondary window

The Device Manager - Storage Navigator secondary window must be enabled before it can be used.

#### Before you begin

- You must have Storage Administrator (View Only) role to perform this task.
- Install and configure JRE.

#### Procedure

1. From the Settings menu, click **Environmental Settings** > **Edit Information Display Settings**. The **Edit Information Display Settings** window opens.
2. In the Secondary window field, click **Enable**.
3. Click **Apply**.

## Logging in to Device Manager - Storage Navigator

You can log in to Device Manager - Storage Navigator in different ways.

If you are an administrator, you can log in to Device Manager - Storage Navigator with a one-time only initial login.

If you are a super-user, you can log in first to Device Manager - Storage Navigator to create other user accounts.

If you are a Device Manager - Storage Navigator and storage system user or administrator, you can log in normally.

### Initial superuser login

Follow these instructions to log in as a superuser.

When logging on to Device Manager - Storage Navigator for the first time, you must log on as a superuser to set up additional user accounts.

The superuser account has a built-in ID, which includes all permissions, and a default password.

#### Procedure

1. Call your local service representative to obtain the superuser ID and default password.
2. In your web browser, specify the URL for your SVP:

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

   To change the port number of the protocol from the initial value (443), specify the following URL:

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

3. Log in with the superuser ID and password.

4. To prevent unauthorized use of the superuser account, change the password immediately after you log in. Click **Settings** > **User Management** > **Change Password** to change your password.

   After you log in, the Device Manager - Storage Navigator main window opens. You can navigate using the menu, tree, or General Tasks. Precise instructions for performing an operation can be found in the software user guides. Also, see Appendixes D through G, which describe the screens in the GUI.

## Normal login

By logging in, you can manage users and licenses, create a login message, or edit advanced system settings.

### Procedure

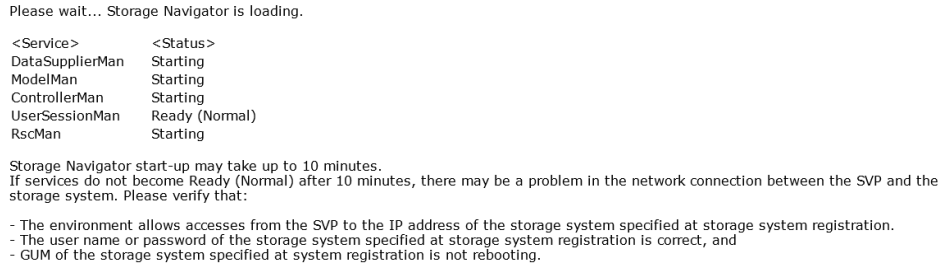
1. In your web browser, specify the following URL:

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

   If you changed the port number of the protocol HTTP 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 loading window displays in Device Manager - Storage Navigator, wait until the service status changes to **Ready (Normal)**. At that time, the login window displays 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 |

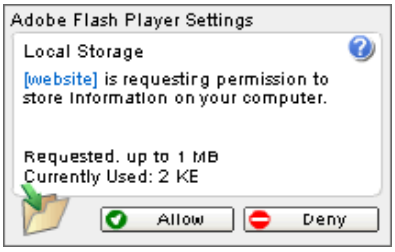
   Storage Navigator start-up may take up to 10 minutes.
   If services do not become Ready (Normal) after 10 minutes, there may be a problem in the network connection between the SVP and the storage system. Please verify that:

   - 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.

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

   - If a message indicates that the enhanced security configuration is enabled on the management client, select **In the future, do not show this message** and click **OK**.
   - If the SVP is set to support SSL-encrypted communication and security messages appear, make sure the certificate is correct and follow the instructions in the dialog box.
   - If a message indicates that certain web sites are blocked, follow instructions in Adding your SVP to the trusted sites zone for Windows Server computers (on page 39).
   - If multiple storage systems are connected, a window which allows selection of the storage system is displayed. Select the storage system you want to connect.

3. When the Storage Device List window opens, select the storage system. The Device Manager - Storage Navigator login window appears.
4. Type the user ID and password.
5. Click **Login**.
6. If the **Security Information** dialog box appears, click **Yes**.
7. If a local storage area pop-up dialog box of Adobe Flash Player Setting appears, click **Allow** to open the Device Manager - Storage Navigator main window. The cache function of Adobe Flash Player optimizes the process of Device Manager - Storage Navigator. Denial of the request might delay the processing speed of Device Manager - Storage Navigator.




After you log in, the Device Manager - Storage Navigator main window opens. You can navigate using the menu, tree, or General Tasks. Precise instructions for performing an operation can be found in the software user guides. Also, see Appendixes D through G, which describe the screens in the GUI.

**Note:** If login fails three times with the same user ID, Device Manager - Storage Navigator stops responding for one minute. This is for security purposes and is not a system failure. Wait, then try again. The roles and resource groups for each user are set up ahead of time and will be available to you when you log in to Device Manager - Storage Navigator. If the roles or resource allocations for your username are changed after you log in, the changes will not be effective until you log out and log back in again. When you use a web browser for a long period of time, memory is heavily used. We recommend closing or logging out of Device Manager - Storage Navigator after you are finished using it.

## Changing your password

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

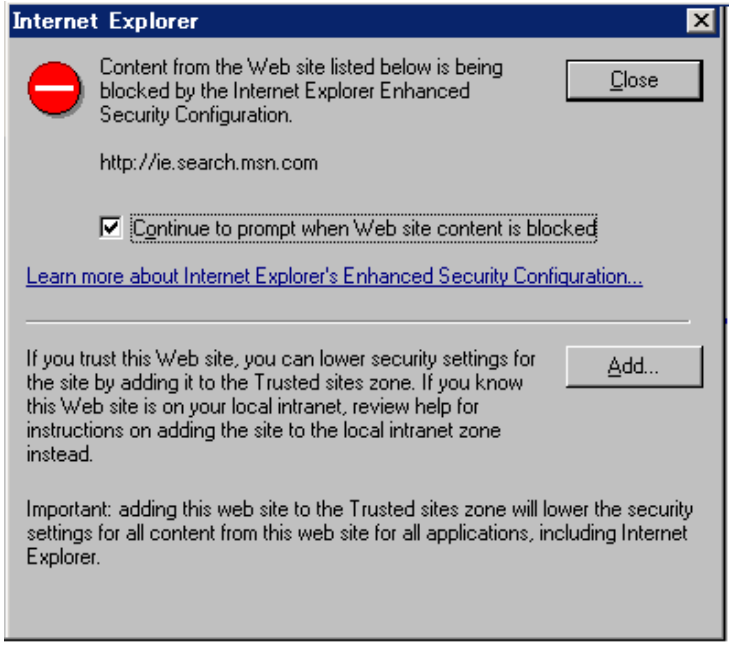
### Procedure

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** to change your password.

## 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

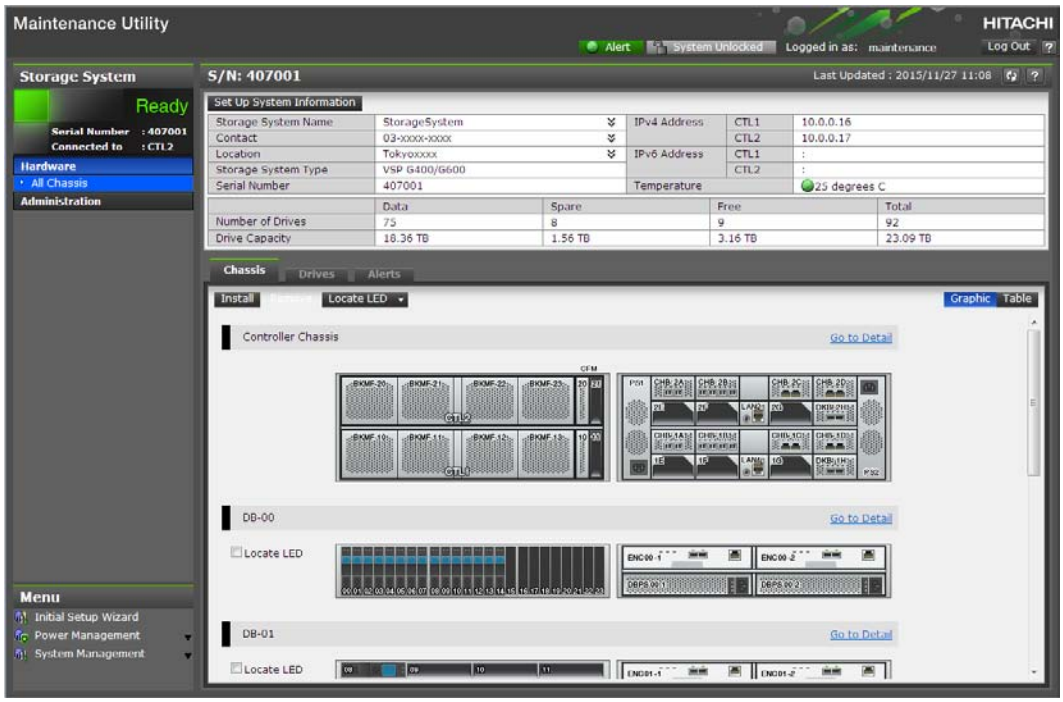
1. Click **Add** in the message dialog box. The **Trusted Sites** dialog box opens.
2. In **Add this web site to the zone**, enter the URL of the SVP that you want to log in to. For example, if the host name is `host01`, the URL is `http://host01`. If the IP address is `127.0.0.1`, the URL is `http://127.0.0.1`.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

## Accessing the maintenance utility

To configure the storage system using the maintenance utility, start the maintenance utility from Hitachi Device Manager - Storage Navigator or the management software.

**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.




## Starting from Hitachi Command Suite

### Procedure

1. Start Hitachi Command Suite.
2. In the **Hitachi Command Suite** main window, click the **Resources** tab, and then click **Storage Systems** from the tree view.
3. Expand the tree, and then right-click a storage system and click **Other Functions**.
4. In Hitachi Device Manager - Storage Navigator, click the **Maintenance Utility** menu, and then click **Hardware** to start the maintenance utility.

## Starting from Hitachi Device Manager - Storage Navigator

### Procedure

1. Launch a web browser from the console PC connected to the SVP, and then start Device Manager - Storage Navigator.
2. Enter the following URL in the address field of your browser, and then press **Enter**:
   `http://[IP address of SVP]/module/sn2/0/index.do`
3. In the **Storage Device List** window, click the picture of the registered storage system.
4. Log in to Device Manager - Storage Navigator.
5. On the **Maintenance Utility** menu, click **Hardware**.
6. Select the menu for the part that needs to be replaced (see the following table).

| Menu | Replace part |
|---|---|
| Cache Memory replacement/installation for CTL1 | Cache memory installed on controller 1. |
| Cache Memory replacement/installation for CTL2 | Cache memory installed on controller 2. |
| Other hardware maintenance | Component other than a controller, fan, and LAN blade. |

# Accessing a storage system without management software

You can use the administrator account created during the initial setup to use HDvM - SN temporarily to access the storage system. You can then perform critical storage management operations during a planned maintenance activity or an unexpected downtime on the management server.

### Before you begin

- You must have an administrator login account with permissions equal to or higher than Administrator User Group has. For information about creating user accounts, see Creating user accounts (on page 77) in this manual, and the *Hardware Reference Guide* for your system model.
- Adobe Flash Player must be configured on the client to use HDvM - SN.

**Note:** To obtain the administrator login information, contact customer support.

### Procedure

1. Start a web browser.
2. Enter the following URL:
   - For the VSP G200 storage system, enter:

     `https://`*`IP-address-or-host-name-of-the-SVP`*`/dev/storage/8320004`*`XXXXX`*`/emergency.do` (where the model number is '8320004' and '4*XXXXX*' indicates the system serial number)
   - For VSP G400, G600 and VSP F400, F600 storage systems, enter:

     `https://`*`IP-address-or-host-name-of-the-SVP`*`/dev/storage/8340004`*`XXXXX`*`/emergency.do` (where the model number is '8340004' and '4*XXXXX*' indicates the system serial number)
   - For VSP G800 and VSP F800 storage systems, enter:

     `https://`*`IP-address-or-host-name-of-the-SVP`*`/dev/storage/8360004`*`XXXXX`*`/emergency.do` (where the model number is '8360004' and '4*XXXXX*' indicates the system serial number)
3. The following actions might be required to open the login dialog box, depending on your environment:

- If a message indicates that the enhanced security configuration is enabled on the computer, select **In the future, do not show this message** and click **OK**.
- If the SVP is set to support SSL-encrypted communication and security messages appear, make sure the certificate is correct and follow the instructions in the dialog box.
- If a messages indicates that certain web sites are blocked, make sure you have added the SVP to the trusted sites zone.

4. Enter a user ID and password for the account.
5. Click **Log In**.
6. If the Security Information dialog box appears, click **Yes**.
7. If an Adobe Flash Player local storage area pop-up dialog box appears, click **Allow** to open the Device Manager - Storage Navigator main window.

   The cache function of Adobe Flash Player optimizes the process of Device Manager - Storage Navigator. Denial of the request might reduce processing speed.

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

# Chapter 3: Configuring the storage system

When configuring the storage system, you must set storage system information, set up security, and register the SVP.

This chapter provides information about configuring the storage system.

## System administration tasks at a glance

The following table summarizes key system administration tasks. The tool used to perform these tasks depends on whether the storage system contains NAS modules.

**Table 2 System administration tasks at a glance**

| Task | Block-only storage systems (no NAS modules installed) | Block and file storage systems (NAS modules installed) |
|---|---|---|
| Set IPv4 and IPv6 network settings and set HTTP blocking | Maintenance utility<br><br>See Changing network communication settings (on page 49) | IP addresses cannot be added, deleted, or modified in the NAS Manager. To change these addresses, use the maintenance utility. |
| Set system clock (date and time) | Maintenance utility<br><br>See Changing the date and time (on page 48) | NAS Manager<br><br>See Changing the system date and time of the NAS Modules (on page 55) |
| Configure audit log settings | Maintenance utility<br><br>See Audit log settings (on page 199) | NAS Manager<br><br>See the *File Services Administration Guide* (MK-92HNAS006) and the *Server and Cluster Administration Guide* (MK-92HNAS010) |
| Configure alert notifications | Maintenance utility<br><br>See Alert notifications (on page 177) | NAS Manager<br><br>See the *Server and Cluster Administration Guide* (MK-92HNAS010) |
| Changing link aggregation | N/A | NAS Manager<br><br>See the *Network Administration Guide* (MK-92HNAS008) |

| Task | Block-only storage systems (no NAS modules installed) | Block and file storage systems (NAS modules installed) |
|---|---|---|
| Change administrator password | Maintenance utility<br>See Configuring the storage system (on page 45) | NAS Manager<br>See the *Network Administration Guide* (MK-92HNAS008) |
| Edit the login message | Maintenance utility<br>See Configuring the storage system (on page 45) | NAS Manager<br>See the *Network Administration Guide* (MK-92HNAS008) |
| Select the SSL cipher suite | Maintenance utility<br>See Configuring the storage system (on page 45) | NAS Manager<br>See the *Network Administration Guide* (MK-92HNAS008) |
| Update certificate files | Maintenance utility<br>See Configuring the storage system (on page 45) | NAS Manager<br>See the *Network Administration Guide* (MK-92HNAS008) |
| Force the system lock to release | Maintenance utility<br>See Configuring the storage system (on page 45) | NAS Manager<br>See the *Network Administration Guide* (MK-92HNAS008) |
| User administration - add, manage, and delete storage system users | Device Manager - Storage Navigator<br>See Managing users, user groups, and accounts (on page 75) | NAS Manager<br>See User Administration for NAS Manager (on page 130) |
| Manage user groups | Device Manager - Storage Navigator<br>See Managing users, user groups, and accounts (on page 75) | NAS Manager<br>See User Administration for NAS Manager (on page 130) |

| Task | Block-only storage systems (no NAS modules installed) | Block and file storage systems (NAS modules installed) |
|---|---|---|
| Registration | Device Manager - Storage Navigator to register the service processor host name.<br>See Registering the primary SVP host name (on page 51) | NAS Manager to register the service.<br>See the *Server and Cluster Administration Guide* (MK-92HNAS010) |
| Change storage system information | Device Manager - Storage Navigator<br>See Setting storage system information (on page 52) | N/A |
| Manage SSL certificates: create keypairs, obtain, update, and return certificates, verify and release passphrases | Device Manager - Storage Navigator<br>See Managing HCS certificates (on page 145) | N/A |
| Manage HCS certificates | Device Manager - Storage Navigator<br>See Managing HCS certificates (on page 145) | N/A |
| Manage HDvM - SN configuration files | Device Manager - Storage Navigator<br>See Backing up HDvM - SN configuration files (on page 52) | NAS Manager<br>See the *Server and Cluster Administration Guide* (MK-92HNAS010) |
| Manage authorization and authentication servers | Device Manager - Storage Navigator<br>See Setting up authentication and authorization (on page 157) | N/A |
| Create LDAP, RADIUS, and Kerberos configuration files | Device Manager - Storage Navigator<br>See Authentication server protocols (on page 158) | NAS Manager<br>See the *Server and Cluster Administration Guide* (MK-92HNAS010) |

| Task | Block-only storage systems (no NAS modules installed) | Block and file storage systems (NAS modules installed) |
|---|---|---|
| Installing licenses | Maintenance utility<br>See License keys (on page 187) | NAS Manager<br>See License keys (on page 187) |
| Enabling and disabling licenses | Maintenance utility<br>See License keys (on page 187) | NAS Manager<br>See License keys (on page 187) |
| Removing licenses | Maintenance utility<br>See License keys (on page 187) | NAS Manager<br>See License keys (on page 187) |

# System administration using the maintenance utility

## Changing the date and time

To keep the date and time on the storage system controller, the SVP, and NAS modules in sync, you must change the date and time settings on all. This section includes procedures to change all settings.

### Changing the controller clock settings

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

#### 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 settings

Complete the following steps to change the Windows 7 date and time on the SVP.

#### Before you begin

- The management console is connected to the LAN 2 port on the SVP.

- The console has established a remote desktop connection with the SVP.
- The management utility window is displayed on the console.

**On the management console that is connected to the SVP:**

### Procedure

1. On the Windows 7 desktop, click **Start** > **Control Panel**.
2. Click **Clock, Language, and Region.**
3. Click **Date and Time.**
4. Click **Change date and time.** The Date and Time Settings window opens.
5. Set the date and time, then click **OK** to save the settings and close the window.

## Enabling IPv6 communication

You can use IPv6 to set communication between the management client and the SVP.

You should assign the SVP the same type of IP addresses (IPv4 or IPv6) that are 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 both the management client and the SVP.

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.

The following topics provide brief instructions on configuring IPv6 communication.

**Note:** If the SVP uses IPv6, you must configure management clients to use IPv6 for communication. Consult your operating system's documentation for instructions.

### Changing network communication settings

This procedure explains how to configure a management client to use IPv6 for communication with an SVP.

#### 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 Settings**.

   The **Network Settings** dialog box displays the current settings for the Mac address, IPv4 and IPv6 settings, and the network connection mode for both 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 and click **Apply**.

   The dialog box closes and returns you to the **Network Settings** window.

### 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.

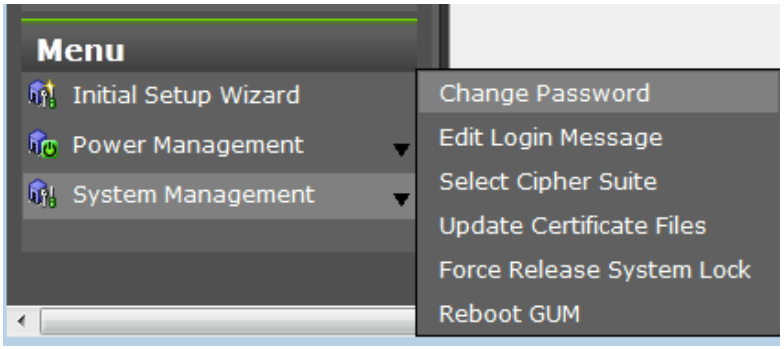
## Creating a login message

#### 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.

## Forcing the system lock to release

When a user locks the system, other users cannot log in or access the system. This feature can be used to ensure that no changes to the system can be made while maintenance or upgrade procedures are in process.

**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

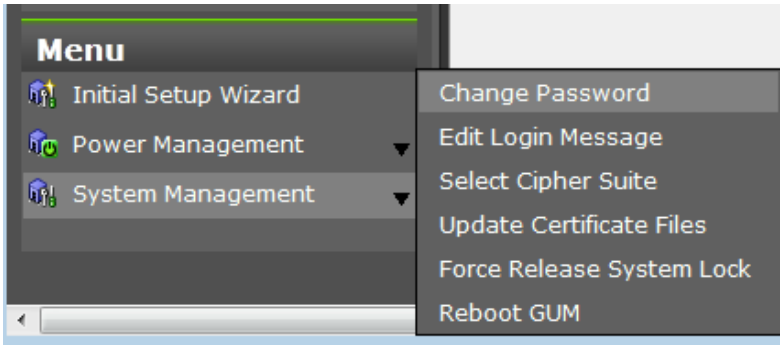
logged on. Wait until their processes are complete before releasing the system lock.

### Before you begin

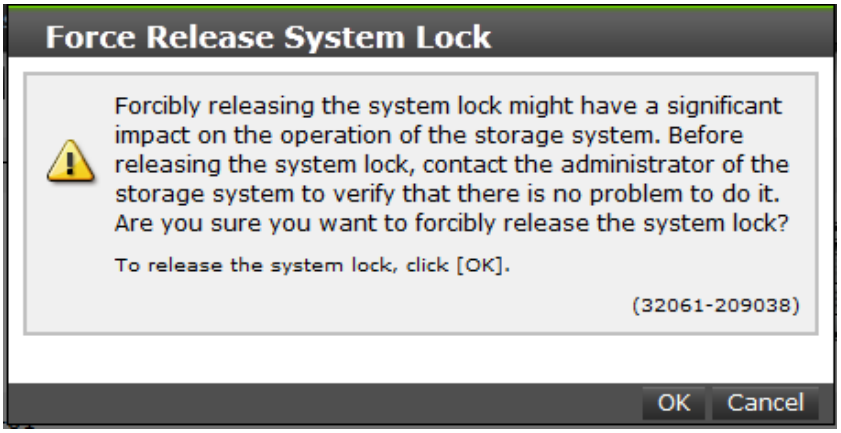
You must have the Storage Administrator (View & Modify) role to complete this procedure.

### 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.




## Registering the primary SVP host name

You must register the primary SVP host name before completing any of the following tasks.

- Specify a host name instead of an IP address when accessing Device Manager - Storage Navigator.
- Obtain 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 the 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 letters you can use for the host name.

- **DNS setting:** You must register the IP address and host name of the SVP to the DNS server that manages the network to which the SVP is connected.
- **Hosts file setting:** You must enter 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:
  - **Windows 7:** `C:\Windows\System32\drivers\etc\hosts`
  - **UNIX:** `/etc/hosts`

# System administration using Device Manager - Storage Navigator

## 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.

### 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 **Task** window opens to show the status of the task.

## Backing up HDvM - SN configuration files

Before replacing an SVP, you must make a backup copy of the Device Manager - Storage Navigator configuration files on the SVP. You can then use the backup copy to restore the configuration file if it becomes necessary, or to configure a replacement SVP if one fails.

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

- Device Manager - Storage Navigator environment parameters
- Authentication server connection settings
- Key management server connection settings
- Password policy when backing up the management client encryption key

- Display settings (table width) for each Device Manager - Storage Navigator user
- Device Manager - Storage Navigator login warning messages
- Device Manager - Storage Navigator task information
- SMI-S application settings
- SSL certification for HTTPS/SMI-S/RMI

### Before you begin

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

### Procedure

1. Stop all services running on the storage system.
2. Open a command prompt window with administrator permissions.
3. In the folder where the .bat file is located, execute the following command:

   `C:\MAPP\wk\Supervisor\MappIniSet>MappBackup.bat` *`absolute-path-of-backup-file`*

   **Note:**
   - The backup file must be in .tgz format.
   - A space is required between .bat file and the path to the backup file.
4. A completion message displays. Click any key to continue.
5. Close the command prompt window.

   **Tip:**
   - 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.
   - The backup file is compressed and uses the .tgz format. Use a tool that supports tar and gzip to extract the data from the .tgz file.
6. Save the backup file to another computer or external memory device such as a USB flash memory or hard drive.

## Restoring HDvM - SN configuration files

You can use a saved copy of a configuration file to restore the active configuration file if it becomes necessary, or to configure a replacement SVP if one fails.

### Before you begin

- The storage systems registered in the SVP you backed up are registered in a new SVP.
- The services on the storage system are stopped.

- The SVP is configured so that the service does not start automatically when starting the system. See the Hardware Reference Guide for your storage system model for information about the SVP configuration method.

### Procedure

1. Copy the backup file to any folder in the SVP.
2. Open a command prompt window with administrator permissions.
3. In the folder where the .bat file is located, enter
   `C:\MAPP\wk\Supervisor\MappIniSet>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.
4. A completion message displays.
5. Type a key to close the message, and then close the command prompt.
6. Set the service to run automatically when starting the SVP.
7. Reboot the SVP. It takes about 10 minutes to complete the startup process.

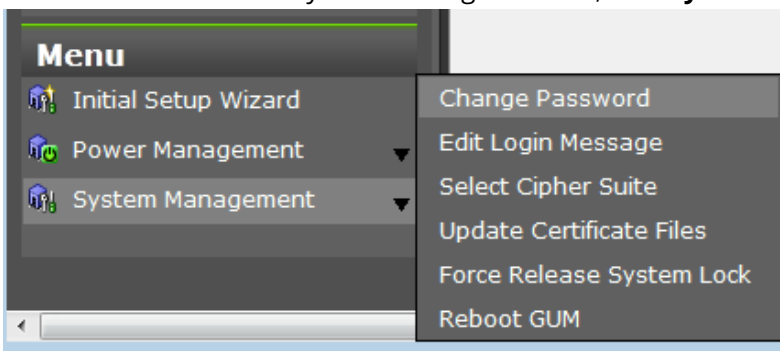
# Changing the administrator password

### 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**.

# System administration using NAS Manager

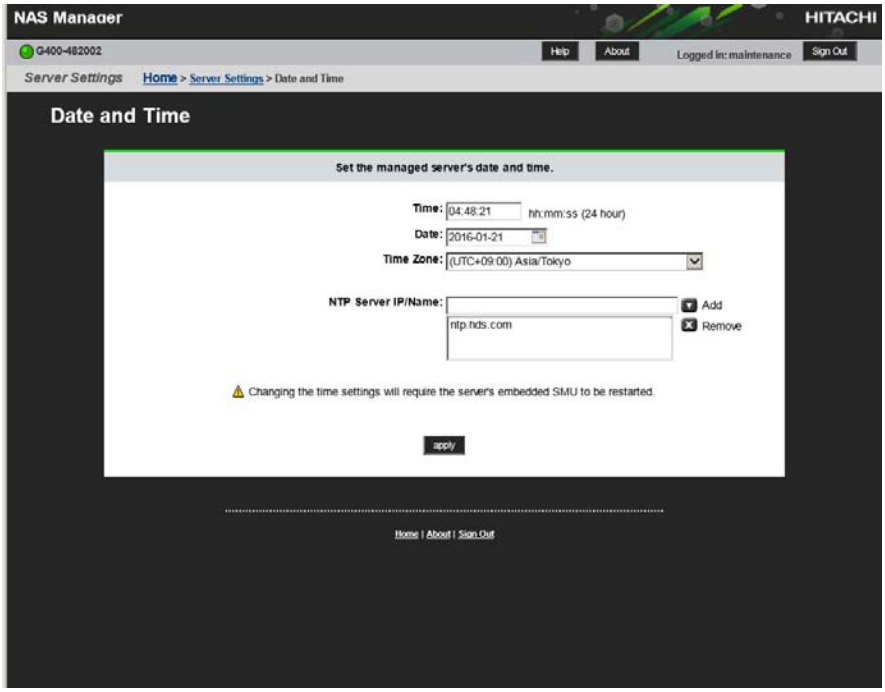
## Changing the system date and time of the NAS modules

When the system date and time are set by NAS Manager, they are also reflected in the system date and time of the storage system.

**Tip:** See the *Hitachi NAS Platform Server and Cluster Administration Guide* for more details about changing the system date and time of the NAS modules.

### Procedure

1. Log on to NAS Manager.
2. Click **Server Settings**.
3. In the **Server Settings** window, click **Date and Time**.




4. In the **Date and Time** window, set the time and date.
   **Setting the date and time with the NTP server**:
   a. Select a time zone in **Time Zone** field.
   b. Enter the IP address or the name of the NTP server in **NTP Server IP/Name** field, and then click **add**.
      When using the Active Directory server, enter the IP address or the name of the NTP server.

   **When setting without using the NTP server**:
   a. Enter time in **Time** field.
   b. Enter date in **Date** field.
5. Confirm the settings and click **apply**.

**Tip:** You do not have to enter **Time** and **Date** because the settings are acquired from the NTP server.

6. Click **OK**.
   The window changes to the **Login** window a few minutes later.

# Miscellaneous system administration considerations

## Modifying SVP port numbers

You can change SVP port numbers to any arbitrary number. This is optional. You can also initialize the settings to the original status by initializing the port number.

For SVP firmware 83-03-01-*XX*/00 or later, some ports are automatically assigned unused port numbers.

You can change the automatically assigned port numbers:

- To check automatically assigned port numbers, see Viewing the port number used in SVP (on page 57).
- To change an automatically assigned port number, see Reassigning an automatically assigned port number (on page 61).
- To return a port to its automatically assigned port number, see Initializing and reassigning an automatically assigned port number (on page 62).
- To change the range of port numbers used for automatic assignment, see Changing the range of an automatically assigned port number (on page 62).
- To return the range of port number for automatic assignment to its original range, see Initializing the range of an automatically assigned port number (on page 63).

**Note:** Perform this task only if an SVP port number is used by another application.

You need to verify the effects before you modify an SVP port number. See Effects of changing service processor port number (on page 58).

The following table describes the port number key names and the initial value of the port number.

| Port number key name | Protocol | Initial port number | Corresponding SVP software version |
|---|---|---|---|
| MAPPWebServer | HTTP | 80 | 83-01-20-*XX*/00 or later |
| MAPPWebServerHttps | HTTPS | 443 | 83-01-20-*XX*/00 or later |
| RMIClassLoader | RMI | 51099 | 83-01-20-*XX*/00 or later |
| RMIClassLoaderHttps | RMI (SSL) | 5443 | 83-01-20-*XX*/00 or later |

| Port number key name | Protocol | Initial port number | Corresponding SVP software version |
|---|---|---|---|
| RMIIFRegist | RMI | 1099 | 83-01-20-*XX*/00 or later |
| PreRMIServer | RMI | 51100 | 83-01-20-*XX*/00 or later |
| | | Automatically assigned | 83-03-01-*XX*/00 or later |
| DKCManPrivate | RMI | 11099 | 83-01-24-*XX*/00 or later |
| SLP | SLP | 427 | 83-01-24-*XX*/00 or later |
| SMIS_CIMOM | SMI-S | 5989 | 83-01-20-*XX*/00 or later |
| | | Automatically assigned | 83-03-01-*XX*/00 or later |
| CommonJettyStart | HTTP | 8080 | 83-01-24-*XX*/00 or later |
| CommonJettyStop | HTTP | 8210 | 83-01-24-*XX*/00 or later |
| RestAPIServerStop | HTTP | 9210 | 83-01-24-*XX*/00 or later |
| DeviceJettyStart | HTTP | 8081 | 83-01-24-*XX*/00 or later |
| | | Automatically assigned | 83-03-01-*XX*/00 or later |
| DeviceJettyStop | HTTP | 8211 | 83-01-24-*XX*/00 or later |
| | | Automatically assigned | 83-03-01-*XX*/00 or later |

## Viewing the port number used in SVP

You can view the port number used in SVP.

### Procedure

1. Open the Windows command prompt as administrator on the SVP.
2. In the folder where the .bat file is located, execute the following command:
   `C:\MAPP\wk\Supervisor\MappIniSet>MappPortRefer.bat` *serial-number* (optional)

   **Note:**
   A space is required between .bat file and the serial number.

   If you omitted the serial number, information of every storage system that is registered in the **Storage Device List** window is displayed.

   For the port on which the port number information is not allocated, **Not Defined** is displayed and a completion message displays.

3. Press any key to acknowledge the message and close the message box.
4. Close the Windows command prompt.

## Effects of changing SVP port numbers

Set the firewall settings of the management client according to new SVP port numbers.

The following table describes the effects for each port number.

| Port number key name | Effects | User reference guide on changing the SVP port number |
|---|---|---|
| MAPPWebServer<br>MAPPWebServerHttps | Changes the method to specify URL for Device Manager - Storage Navigator login | See Logging in to Device Manager - Storage Navigator (on page 37) . |
| | In Hitachi Command Suite:<br>You must change the HCS port number to be the same number. | *Hitachi Command Suite Installation and Configuration Guide* |
| RMIClassLoader | When you execute the Export Tool command, you must specify a port number. The port number should be the one you have specified for the -el.dlport operand of the **`java`** command, which was used for downloading the Export Tool. | *Performance Guide* |
| RMIIFRegist | When you execute the Export Tool command, you must specify the IP address and new port number of the SVP for *IP-sub-command*. | *Performance Guide* (Performance Monitor, Server Priority Manager) |
| | In Hitachi Command Suite:<br>You must change the HCS port number to the same number. | *Hitachi Command Suite Installation and Configuration Guide* |
| PreRMIServer | None | None |
| DKCManPrivate | None | None |

| Port number key name | Effects | User reference guide on changing the SVP port number |
|---|---|---|
| SLP | You must change the SMI-S port number to the same number. | *Hardware Reference Guide* for your storage system |
| SMIS_CIMOM | You must change the SMI-S port number to the same number.<br>If the storage system is 83-03-01-*XX*/00 or later, check the port number which is used after registering the storage system. For detail, see Viewing the port number used in SVP (on page 57). | *Hardware Reference Guide* for your storage system |
| CommonJettyStart | None | None |
| CommonJettyStop | None | None |
| RestAPIServerStop | None | None |
| DeviceJettyStart | None | None |
| DeviceJettyStop | None | None |

## Changing the SVP port number

You can change the SVP port number to any arbitrary number. After changing the port number, the SVP will be restarted.

### Before you begin

- Remote desktop connection from the management client to SVP has been performed.
- The range of the available port number is from 1 to 65535. Make sure the new port number is not duplicated with the number used in another application.
- You can enter multiple instances of *port-number-key-name* and *port-number*. For example:

```
MappSetPortEdit.bat MAPPWebServer 81 MAPPWebServerHttps 444
```

- The management file of the SVP port number is stored in the following location:

```
path-to-tool\mpprt\cnf\mappsetportset.properties
```

**Note:**

- Do not change the management file of the port number.
- Close the management file of the port number while executing the command for changing or initializing.
- If the SVP software version of the registered storage system does not support changing the port number, update the SVP software.
- Port numbers 1 to 1023 are reserved for other application programs, so do not use these numbers. If you use these numbers and encounter a problem, change the number to 1024 or higher.
- The following port numbers cannot be used for MAPPWebServer or MAPPWebServerHttps:

  2049, 4045, 6000

### Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Open the Windows command prompt as administrator on the SVP.
3. In the folder where the .bat file is located, execute the following command:

```
C:\MAPP\wk\Supervisor\MappIniSet>MappSetPortEdit.bat port-number-key-name port-number
```

**Note:**

- A space is required between `MappSetPortEdit.bat` and *port-number-key-name*.
- A space is required between *port-number-key-name* and *port-number*.

4. A service restart message box displays, followed by a completion message box. Press any key to acknowledge the message and close the message box.
5. Close the Windows command prompt.

## Initializing the SVP port number

You can initialize the SVP port settings and restore to the original status. After initializing the port number, the SVP will be restarted.

To initialize the automatically assigned port number: See Initializing and reassigning automatically assigned port numbers (on page 62)

### Before you begin

Remote desktop connection from the management client to SVP has been performed.

### Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Open the Windows command prompt on the SVP.

3. In the folder where the .bat file is located, execute the following command:

```
C:\MAPP\wk\Supervisor\MappIniSet>MappSetPortInit.bat
```

4. An initialization confirmation message box displays.
   If you want to continue, enter `Y`, and then press the **Enter** key. If you want to cancel the task, enter `N`, and then press the **Enter** key.
5. A service restart message box displays, followed by a completion message box. Press any key to acknowledge the message and close the message box.
6. Close the Windows command prompt.

## Reassigning an automatically assigned port number

You can reassign the port number that is automatically assigned to the storage system.

If the port number assigned to the storage system is used in another application, the port number is reassigned. Also, if you disabled the automatic assign, this deletes the unnecessary port number that is already assigned.

**Caution:**

- Stop the storage system service before reassigning. If you did not stop before reassigning, stop the storage system service in Storage Device List window, then start the service.
- The port for DeviceJettyStart and DeviceJettyStop that is assigned when starting the storage system service cannot be reassigned.
- If you disable the function which is using the port, this deletes the port number that is already assigned.

### Procedure

1. Logout from Device Manager - Storage Navigator on the storage system that you want to reassign.
2. Stop the service of the storage system that you want to reassign.
3. Open the Windows command prompt as administrator on the SVP.
4. In the folder where the .bat file is located, execute the following command:
   `C:\MAPP\wk\Supervisor\MappIniSet>MappPortManageRenum.bat` *serial-number (optional)*

   **Note:** A space is required between `MappPortManageRenum.bat` and *serial-number*.

   If you omitted the serial number, it is executed for the storage system of 83-03-01-*XX*/00 or later that is registered in the **Storage Device List** window.
5. A confirmation message box displays.
   If you want to continue, enter **Y**, and then press the **Enter** key. If you want to cancel the task, enter **N**, and then press the **Enter** key.
6. Press any key to acknowledge the message and close the message box.
7. Close the Windows command prompt.
8. Start the service of the storage system which is reassigned.

## Initializing and reassigning an automatically assigned port number

You can initialize the port number that is automatically assigned to the storage system.

**Caution:**

- Stop the service of the storage system which has the status Ready in the Storage Device List window before initializing.
- If you did not stop before initializing, execute Reassigning an automatically assigned port number (on page 61).

### Procedure

1. Logout from Device Manager - Storage Navigator.
2. Stop the service of all the storage systems which have the status **Ready** in the **Storage Device List** window.
3. Open the Windows command prompt as administrator on the SVP.
4. In the folder where the .bat file is located, execute the following command:
   `C:\MAPP\wk\Supervisor\MappIniSet>MappPortManageInit.bat`
5. A confirmation message box displays.
   - If you want to continue, enter **Y**, and then press the **Enter** key.
   - If you want to cancel the task, enter **N**, and then press the **Enter** key.
6. Press any key to acknowledge the message and close the message box.
7. Reassign the port number.
   `C:\MAPP\wk\Supervisor\MappIniSet>MappPortManageRenum.bat` *serial-number (optional)*

   **Note:**

   A space is required between `MappPortManageRenum.bat` and *serial-number*.

   If you omitted the serial number, the batch file is run for the storage system of 83-03-01-*XX*/00 or later which is registered in **Storage Device List** window.
8. A confirmation message box displays.
   - If you want to continue, enter **Y**, and then press the **Enter** key.
   - If you want to cancel the task, enter **N**, and then press the **Enter** key.
9. Press any key to acknowledge the message and close the message box.
10. Reassign the port number for all the registered storage systems by executing Steps 7 through 9.
11. Close the Windows command prompt.
12. Start the service of the storage system.

## Changing the range of an automatically assigned port number

You can change the range of the port number that is automatically assigned to the storage system.

### Procedure

1. Open the Windows command prompt as administrator on the SVP.
2. In the folder where the .bat file is located, execute the following command:

   `C:\MAPP\wk\Supervisor\MappIniSet>MappPortRangeSet.bat` *port-number-key-name port-number-range*

   **Note:**
   - A space is required between `MappPortRangeSet.bat` and *port-number-key-name*.
   - A space is required between *port-number-key-name* and *port-number-range*.

   The following table shows the port number key name and initial value of the port number range which can be changed. Port 0 is not assigned.

| Port number key name | Initial value of port number range | Remark |
|---|---|---|
| PreRMIServer | 51100 to 51355 | None |
| SMIS_CIMOM | 5989 to 6244 | None |
| DeviceJettyStart | 48081 to 48336 | None |
| DeviceJettyStop | 48411 to 48666 | None |
| unavailable | 1 to 1023 | Port number that is not used in automatic assign |

   - The valid range of the port number is between 1 and 65535. Use a port number that is not used in another service.
   - Port numbers between 1 and 1023 are reserved for the other applications. If you exclude a number between 1 and 1023 from the setting value of unavailable, the port numbers might not operate normally.
   - The following can be used for the port number range:

     Numbers, space, symbols (, -) and rm
   - You can specify multiple *port-number-key-name* and *port-number-range*.

     For example: `MappPortRangeSet.bat PreRMIServer 51200-55000 SMIS_CIMOM 5989-6244,8000`
3. Press any key to acknowledge the message and close the message box.
4. Close the Windows command prompt.

## Initializing the range of an automatically assigned port number

You can initialize the range of the port number that is automatically assigned to the storage system.

### Procedure

1. Open the Windows command prompt as administrator on the SVP.
2. In the folder where the .bat file is located, execute the following command:
   `C:\MAPP\wk\Supervisor\MappIniSet>MappPortRangeInit.bat`
3. A confirmation message box displays.
   - If you want to continue, enter **Y**, and then press the **Enter** key.
   - If you want to cancel the task, enter **N**, and then press the **Enter** key.
4. Press any key to acknowledge the message and close the message box.
5. Close the Windows command prompt.

# Chapter 4: User administration

This chapter describes various user roles, permissions, and groups available to manage your storage system.

## User administration for maintenance utility

The maintenance utility allows you to set up and manage user accounts.

### Required roles for operating Maintenance Utility

You can control the availability of using each operation window of Maintenance Utility for a user by registering the user in the user group and assigning the user with the appropriate role.

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[1] |
| User Administration | Security Administrator (View & Modify) |
| Alert Notifications | Storage Administrator (Initial Configuration) |
| Set Up Date & Time | Storage Administrator (Initial Configuration) |
| Set Up Network Settings | Storage Administrator (Initial Configuration) |
| Licenses | Storage Administrator (Initial Configuration) |
| Audit Log Settings | Audit Log Administrator (View & Modify) |
| Turn on/off Locate LEDs | Support Personnel or User Maintenance[1] |

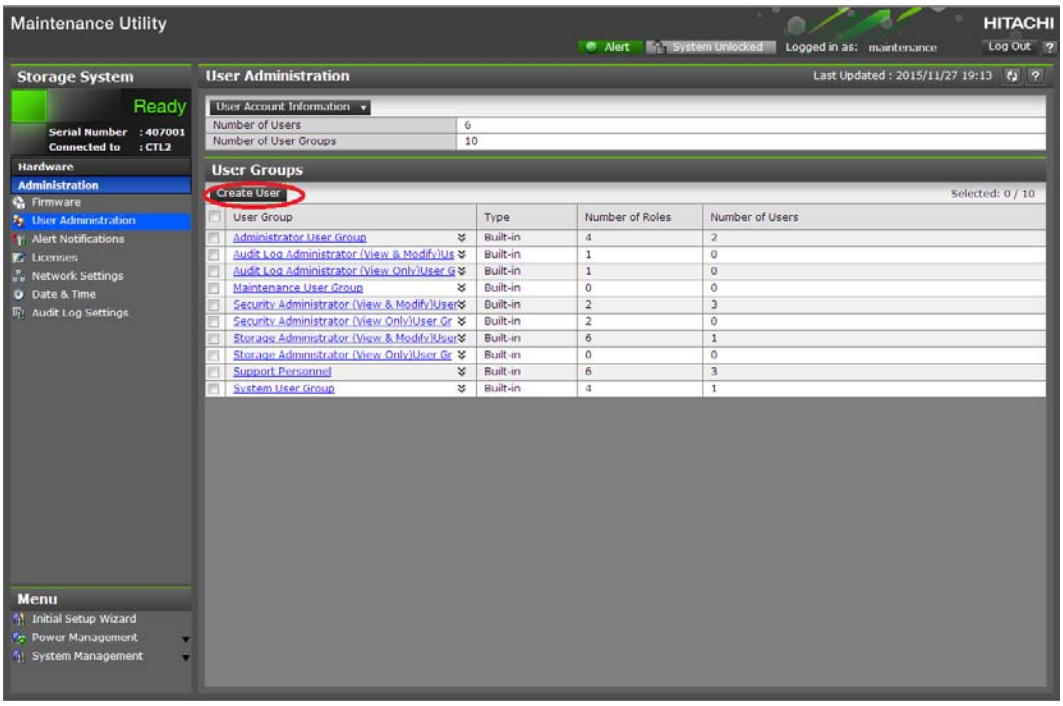
| Maintenance Utility operation window | Required role name |
|---|---|
| Power on Storage System | Support Personnel or User Maintenance[1] |
| Power off Storage System | Support Personnel or User Maintenance[1] |
| Edit UPS Mode | Support Personnel or User Maintenance[1] |
| Edit Login Message | Storage 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 |
| Change Password | No role is required. |
| Boot System Safe Mode | Support Personnel[1] |
| Alert Display | Support Personnel or User Maintenance[1] |
| Alert Display Related to FRU | Support Personnel or User Maintenance[1] |
| Administration Menu | N/A |
| Power Management | N/A |
| System Management | N/A |
| Resetting GUM | N/A |
| **Notes:**<br>1. *Support Personnel* means operations performed by the service personnel. *User Maintenance* means operations performed by the user | |

## Setting up user accounts

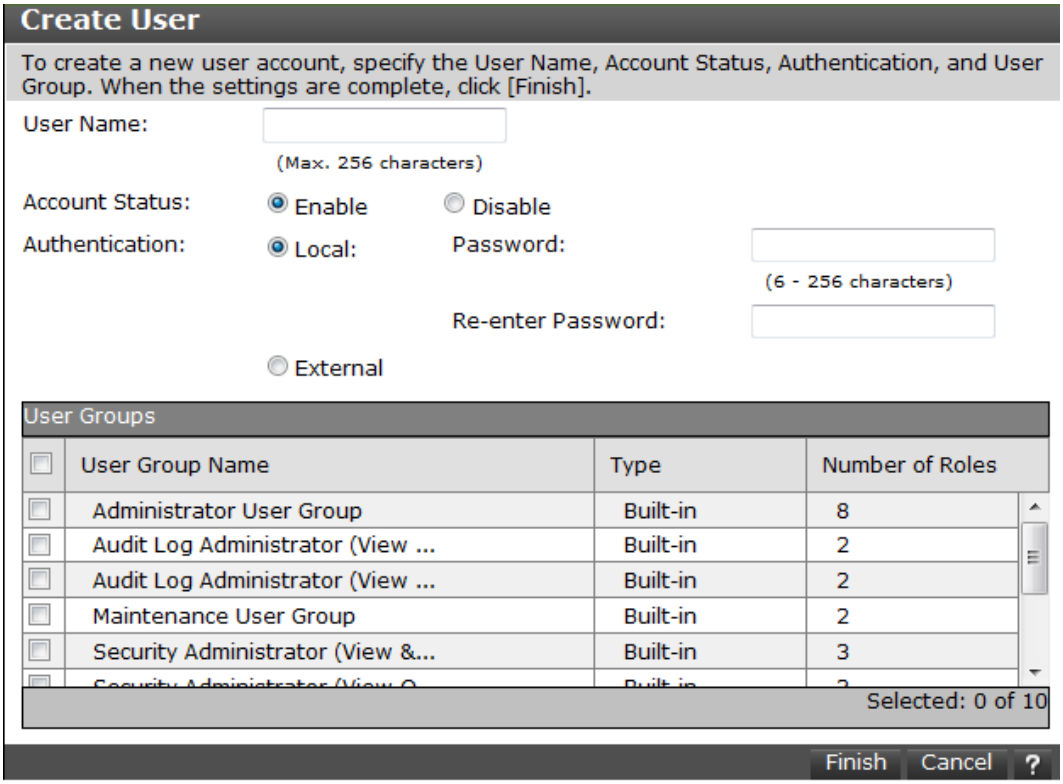
You can create up to 20 users, including the built-in user.

### Procedure

1. In the Maintenance Utility window, click **Administration** > **User Administration**.
2. In the **User Groups** tab, click **Create User**.



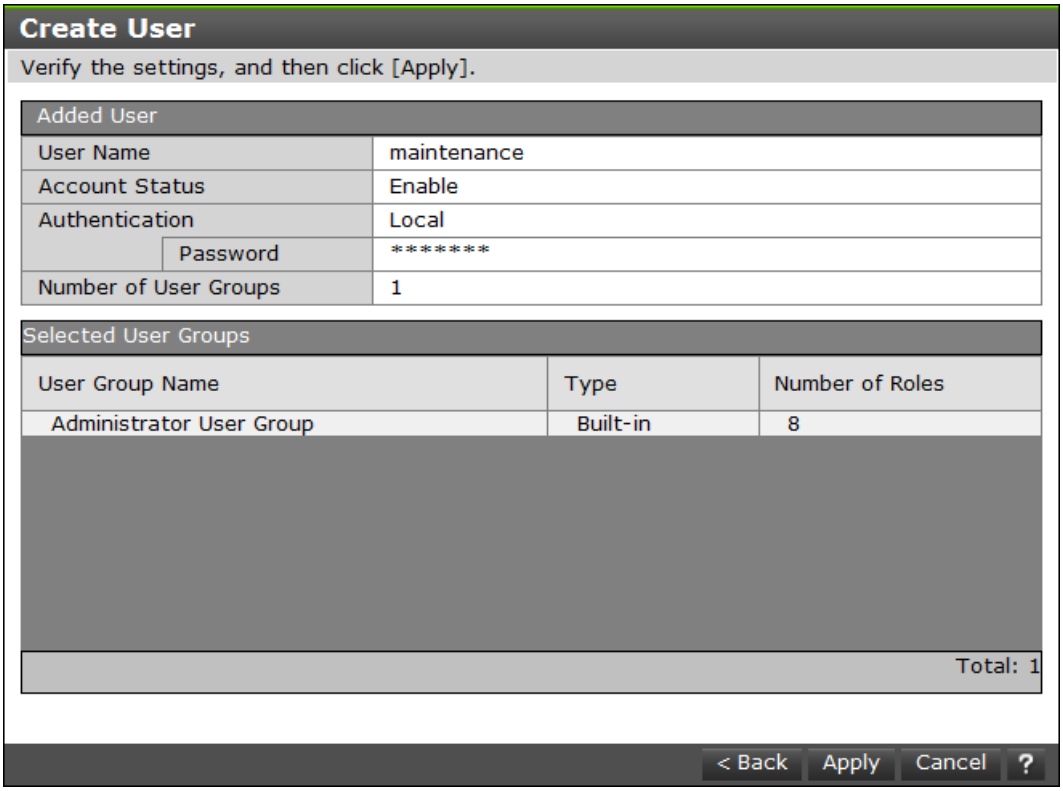

3. Create a new user account. Specify the **User Name**, **Account Status**, **Authentication**, and **User Group**. Click **Finish**.




| Item | Description |
|---|---|
| User Name | |

| | |
|---|---|
| Account Status | The following statuses are available:<br>Enable: User can use the account.<br>Disable: User cannot use the account or log in to the storage management software. |
| Authentication | The following methods are available:<br>Local: Does not use authentication server. Uses a dedicated password for storage management software.<br>External: Uses an authentication server. |

4. Confirm the settings, and then click **Apply**.




5. When the completion message appears, click **Close**.

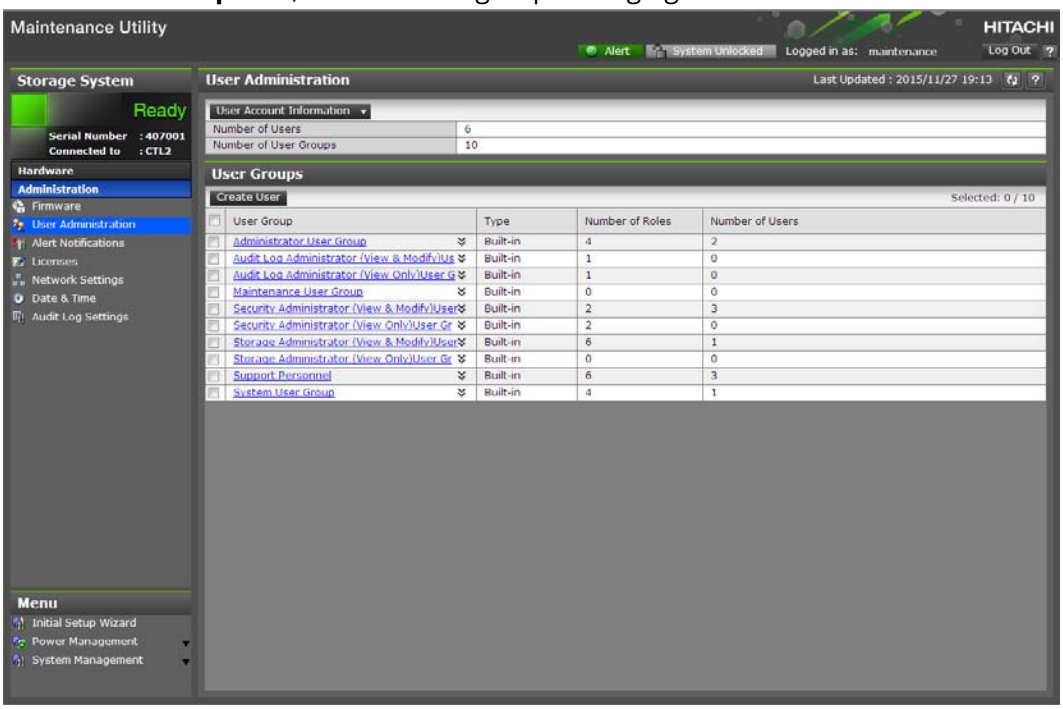
## Disabling user accounts

Observe the following guidelines:

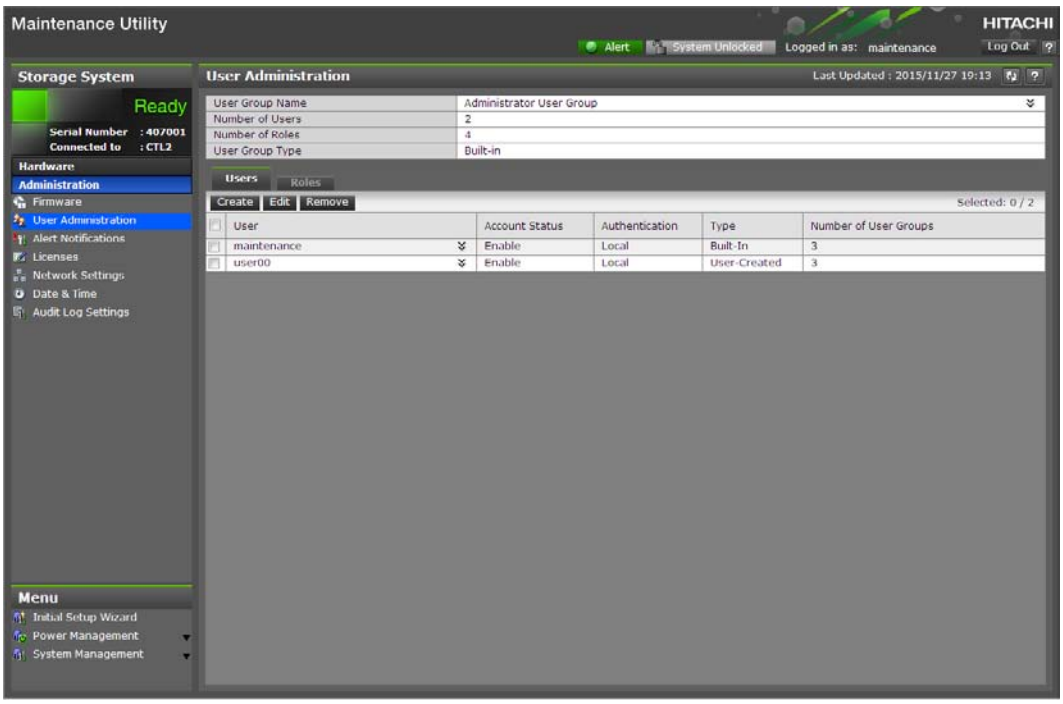
- Log into an account that is different from the user account that you want to disable (you cannot disable the current login user account).
- To disable the user account specified by the registered storage system in the **Storage Device List** window, click Stop Service for the registered storage system. After disabling the user account, click Edit to enable the user account.

## Procedure

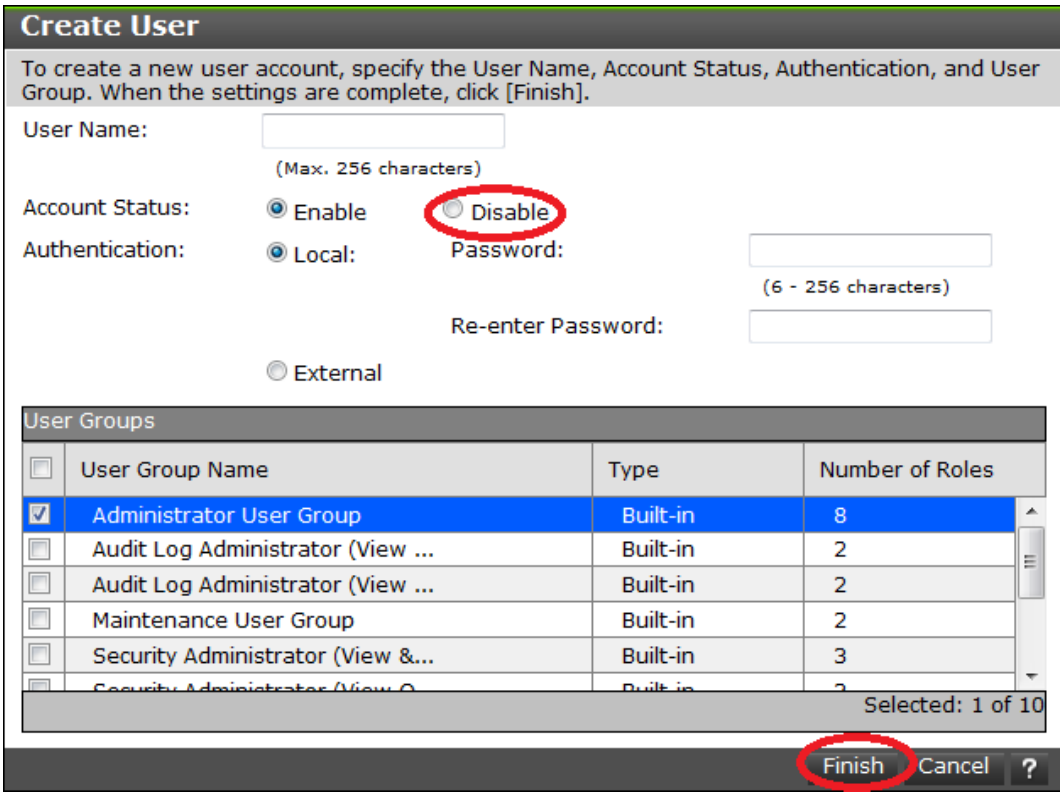
1. In the Maintenance Utility window, click **Administration** > **User Administration**.
2. In the **User Groups** tab, click the user group belonging to the user.



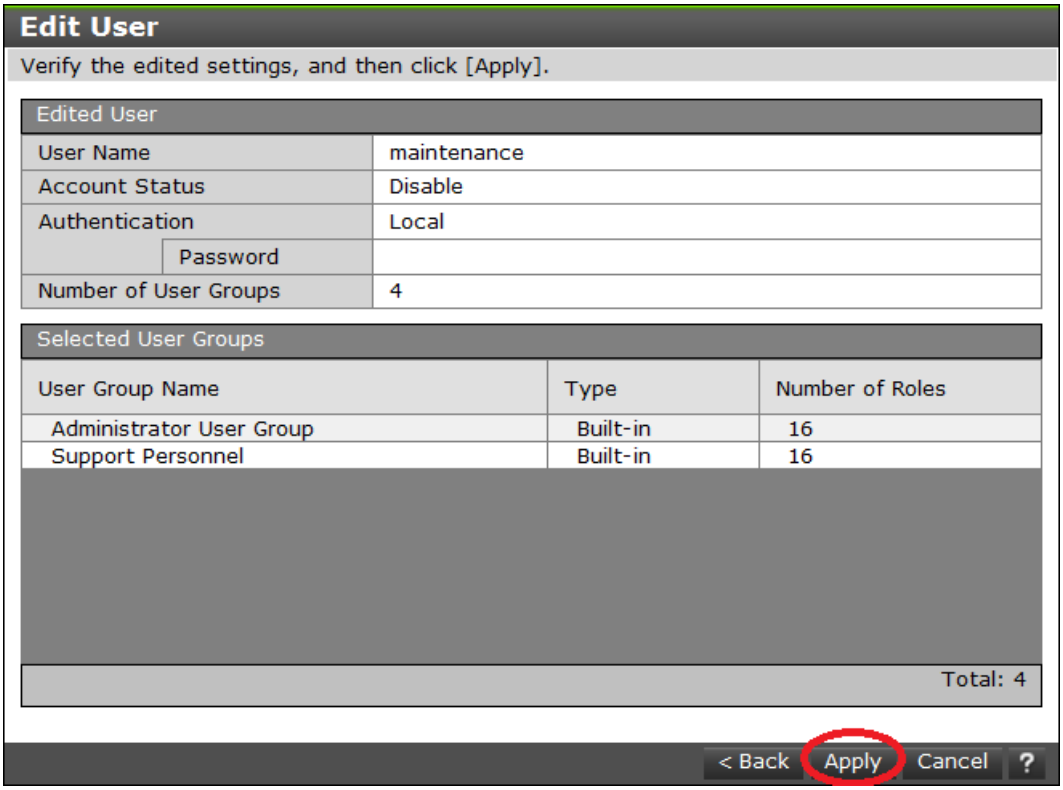

3. Click the **Users** tab, and then select the user account to disable.



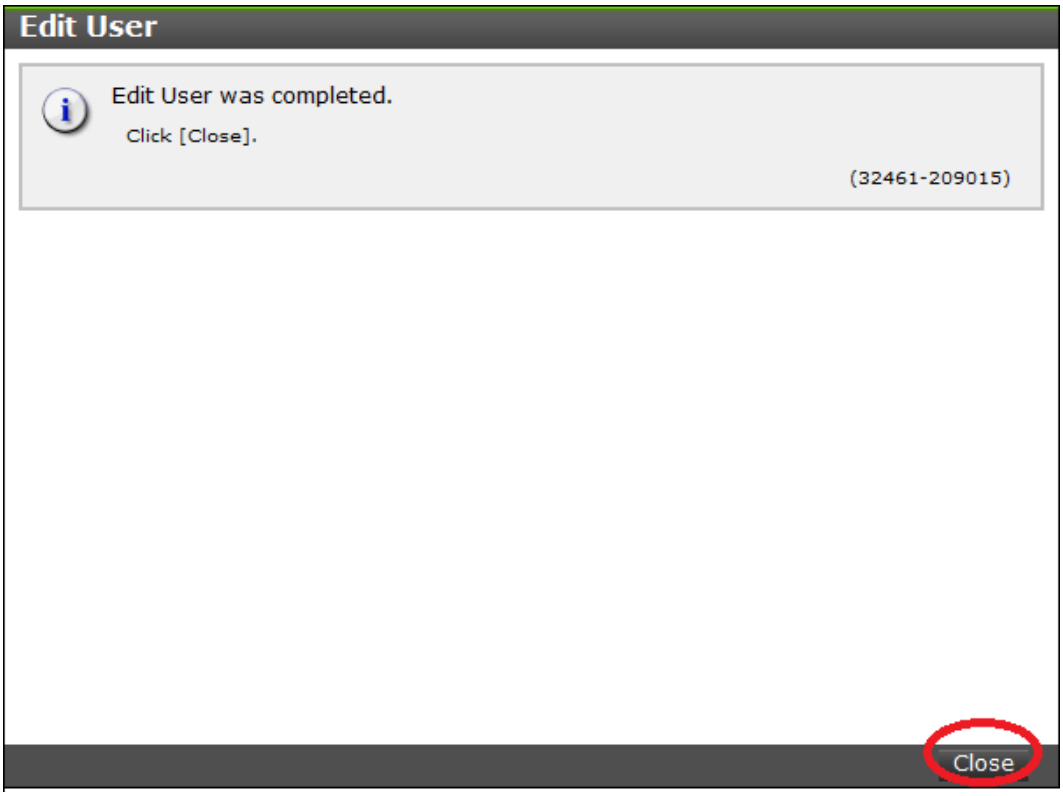

4. Click **Edit**.
5. For **Account Status**, click **Disable**, and then click **Finish**.




6. Confirm the settings, and then click **Apply**.




7. When a completion message appears, click **Close**.



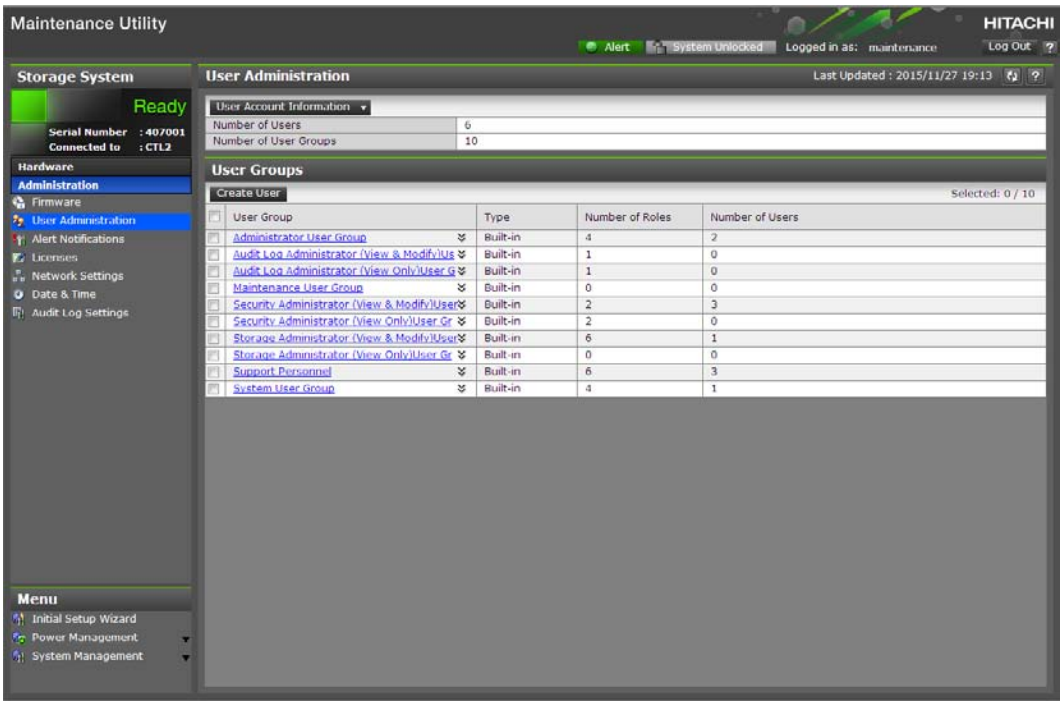

## Removing user accounts

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.

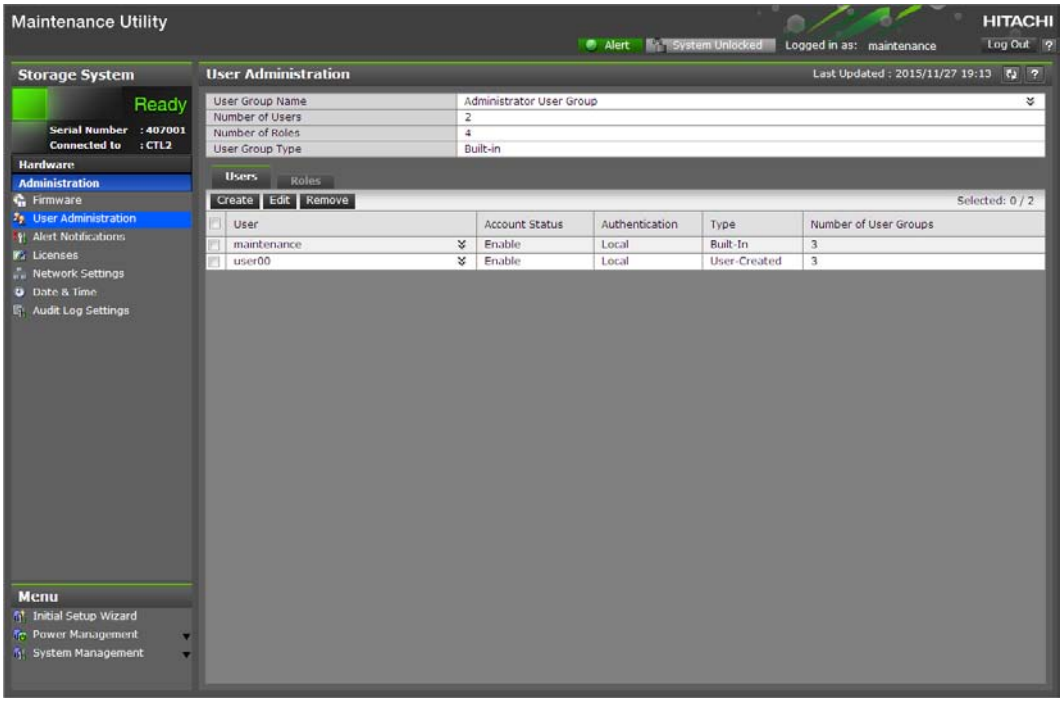
**Note:** To delete the user account specified by the registered storage system in the **Storage Device List** window, click **Stop Service** of the registered storage system. After deletion, click Edit to enable the user account.

### Procedure

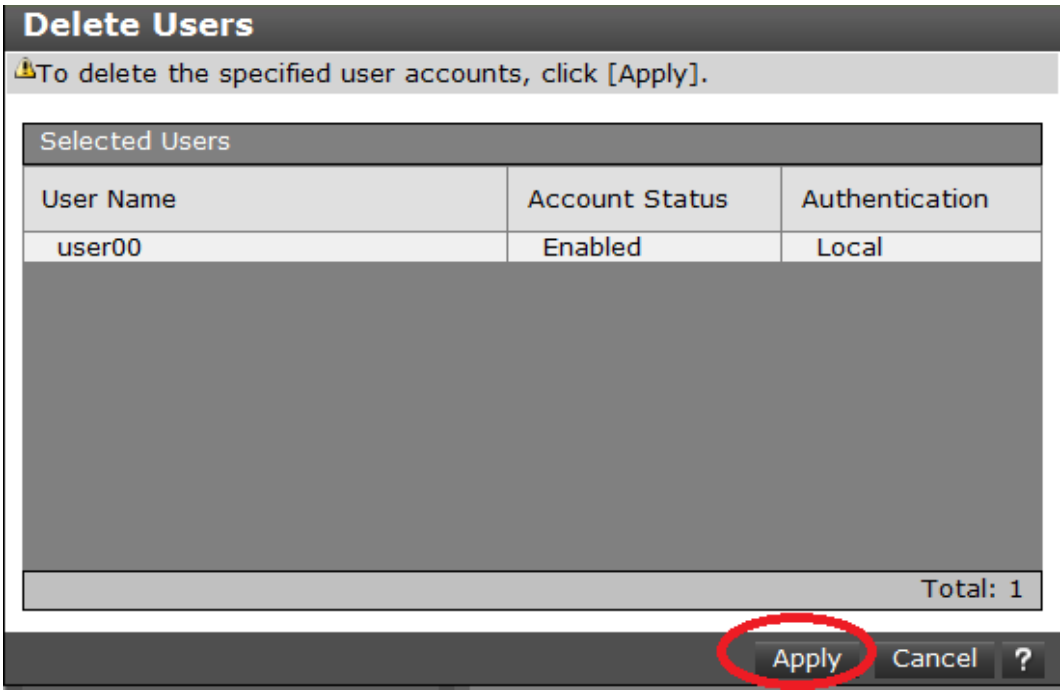
1. In the **Maintenance Utility** window, click **Administration** > **User Administration**.
2. In the **User Groups** tab, select the user group belonging to the user.



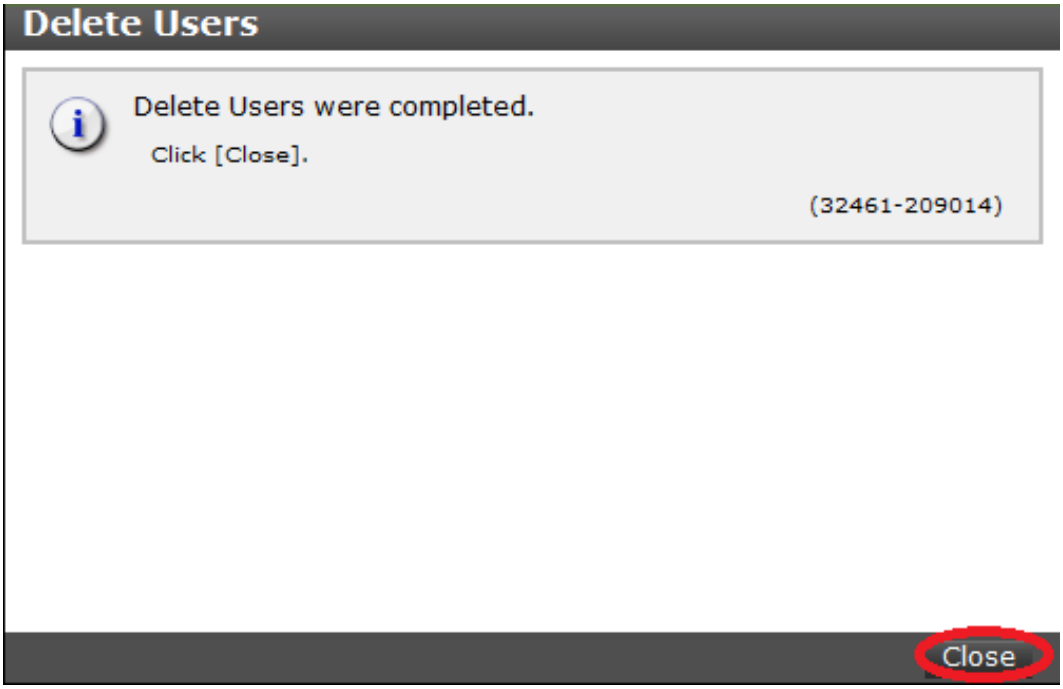

3. Click the **Users** tab, and then select the user to remove.




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**.

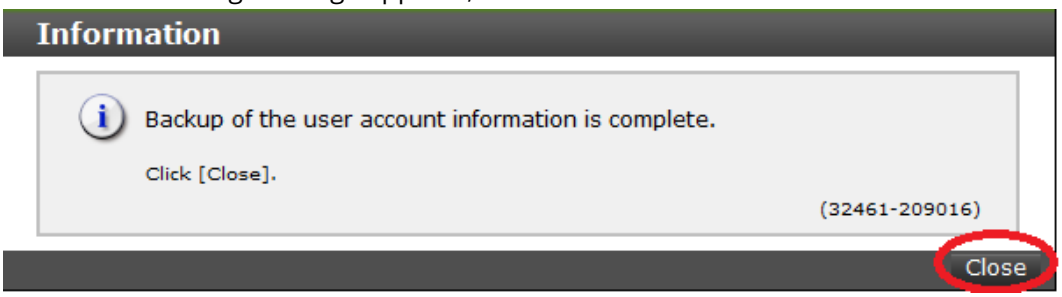



## Backing up user accounts

### Procedure

1. Click **User Account Information** > **Backup**.
2. Specify a storage destination and a file name in the displayed window and download the file.

3. When the following message appears, click **Close**.



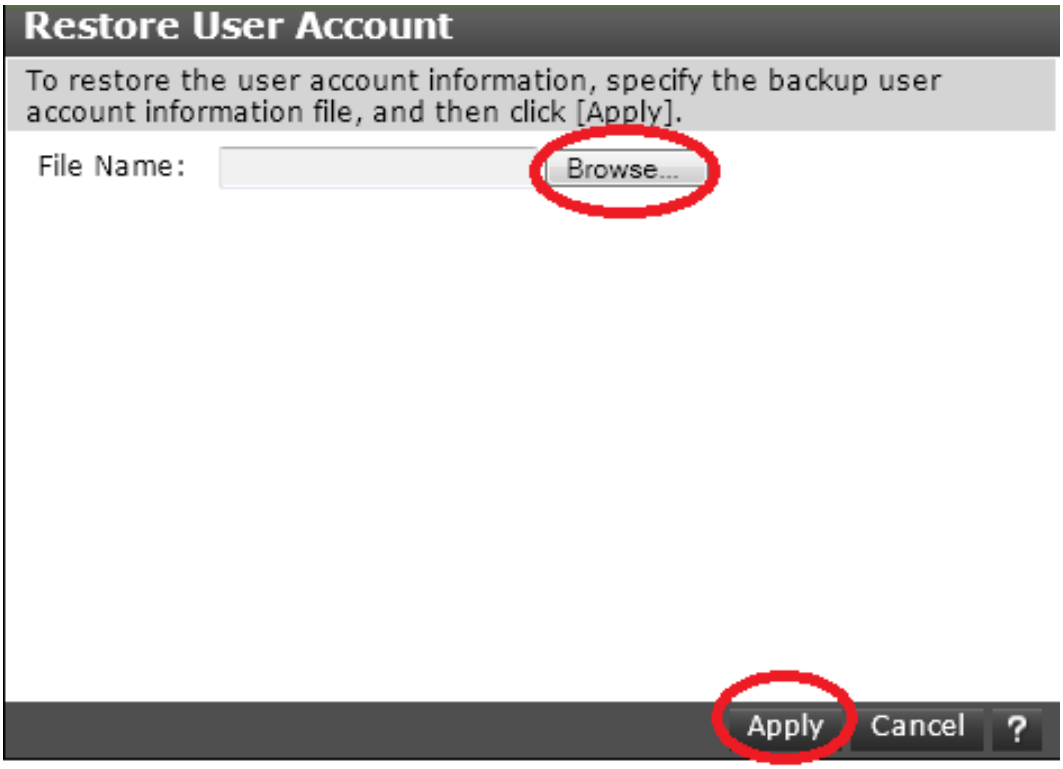

## Restoring user account information

### Procedure

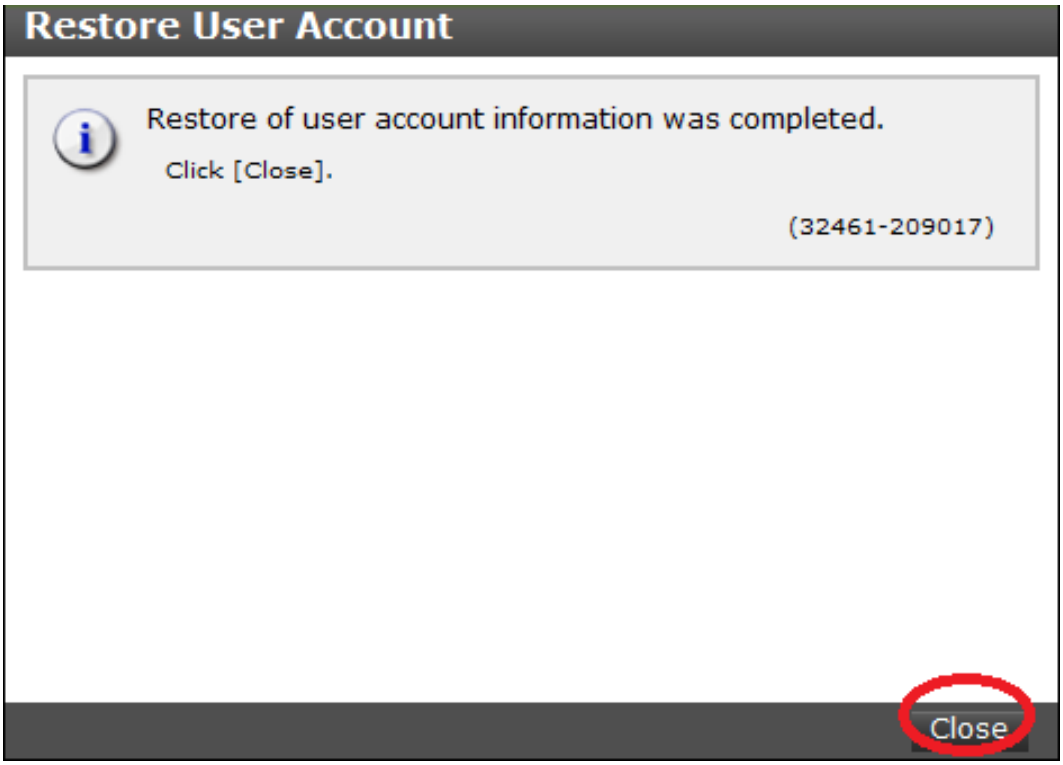
1. Click **User Account Information** > **Restore**

   The **Restore User Account** window opens.

2. Specify file names to be restored, and then click **Apply**.




3. When a completion message appears, click **Close**.




# Managing users, user groups, and accounts

You can use the Device Manager - Storage Navigator to create, modify, or delete users, user groups, and accounts.

This chapter describes how to define the users and user groups that will manage your storage system.

## User administration overview

Read and understand the following information before managing users or 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.
- If a user has All Resource Groups Assigned set to Yes, the user can access all the resources in the storage system. For example, if a user is a security administrator and a storage administrator and has all resource groups assigned, the user can edit the storage for all the resources.

  If this is an issue, the recommended solution is to register two user accounts in the storage system and use the two accounts for different purposes.

  - A security administrator user account that has All Resource Groups Assigned set to Yes.
  - A storage administrator user account that has only some of the resource groups assigned.

- For user groups whose roles are other than Storage Administrator, All Resource Groups Assigned is automatically set to Yes. If you delete all the roles except Storage Administrator, reassign resource groups to the user group because All Resource Groups Assigned is automatically set to No.

## Workflow for creating and managing user accounts

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

- If an authentication server is used, connect the management clients to it. An authentication server allows users to log in to Device Manager - Storage Navigator with the same password as the one used for other applications in a system.
- If an authentication server is not used, use a password dedicated to Device Manager - Storage Navigator to log in. Whether to use the authentication server can be specified for each user.
- Review Setting up authentication and authorization (on page 157) for information and instructions.
- Review Managing user groups (on page 84) to understand the user groups and roles you can assign new or existing users.
- Create user accounts and assign permissions. See Creating user accounts (on page 77).
- Change, disable, or delete user passwords and permissions. See Changing user passwords (on page 81).

### Administrator tasks

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

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

#### Procedure

1. Log in to Device Manager - Storage Navigator as a built-in user.

   Use `maintenance` as the user name, and `raid-maintenance` as the password. The built-in user has all permissions.
2. Click **Settings** > **User Management** > **Change Password** to change the password of the built-in user account.
3. Create a user group. Some user groups, such as built-in groups, are available by default.
4. Create a user.
5. If necessary, change the environment parameter.
6. Save the user account information and environment parameter file.
7. Notify the user of the new user name and the password.

### User tasks

#### Procedure

1. Use the user name and password provided by the administrator to log in to Device Manager - Storage Navigator.
2. Click **Settings** > **User Management** > **Change Password** to change the password to your own password.

## Managing user accounts

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.

It is prudent to 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.

### Creating user accounts

You must create a user account and register the account to a user group with appropriate permissions.

#### 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.
- Support representatives must have the Support Personnel (Vendor Only) role to log in.
- The system can support a maximum of 20 user accounts, including the built-in user accounts.

**Table 3 User name and password for Device Manager - Storage Navigator**

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

**Table 4 User name and password for logging in to CCI**

| Item | Length in characters | Characters that can be used |
|---|---|---|
| User name | 1-63 | ▪ Alphanumeric characters<br>▪ The following symbols:[1]<br>- . @ _ |
| Password | 6-63 | ▪ Alphanumeric characters<br>▪ The following symbols:[1]<br>, - . @ _ |

**Note:**

1. When you use a Windows computer, you can also specify a backslash (\). When you use a UNIX computer, you can also specify a slash (/).

### 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.

   The user logging in to NAS Manager must belong to the built-in Administrator group.
3. On the **Roles** tab, confirm that the displayed permissions are appropriate for the user.
4. On the **Users** tab, click **Create User**.
5. Enter a name.
6. Select **Activate** or **Lock** for the account. If you select **Lock**, the user of this account is disabled and cannot log in to Device Manager - Storage Navigator and NAS Manager.
7. To use an authentication server, select **External**. To authenticate users with only Device Manager - Storage Navigator, or to log in to NAS Manager, select **Local**.
8. If you select **Local**, enter the password for this user account in two places.

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

## Character restrictions for user names and passwords

Note the following restrictions for user names and passwords.

A user account created by using Device Manager - Storage Navigator can be used for maintenance utility, CCI, and NAS Manager. It can also be used by maintenance personnel for logins (the Support Personnel role is required).

The number of characters and types of characters that can be used vary between Device Manager - Storage Navigator, CCI, and NAS Manager. If a user uses all three programs, specify a user name and a password that satisfy the following conditions.

| Item | Length in characters | Characters that can be used |
|---|---|---|
| User name | 1-20 | ▪ Alphanumeric (ASCII code) characters<br>▪ The following symbols[1, 3]:<br>- . _ |
| Password | 6-63 | ▪ Alphanumeric (ASCII code) characters<br>▪ The following symbols[1, 2]:<br>- , . : @ _ |

**Note:**

1. If the host on which CCI is installed is running on UNIX, a slash (/) can be specified.
2. If the host on which CCI is installed is running on Windows, a back slash (\) can be specified.
3. Do not specify a user name consisting of periods (.) (..) only, or specify a user name beginning with a hyphen (-). If you specify such names, you cannot log in to NAS Manager.

**Note:** To use NAS Manager after installing NAS modules, users created with DKCMAIN firmware 83-03-2*x* or earlier, must change the password. If you do not change the password, you cannot log in to NAS Manager. Also, if a user name contains more than 20 characters, the user cannot log in to NAS Manager.

**User name and password for Device Manager - Storage Navigator**

| Item | Length in characters | Characters that can be used |
|---|---|---|
| User name | 1-256 | ▪ Alphanumeric (ASCII code) characters<br>▪ The following symbols:<br># $ % & ' * + - . / = ? @ ^ _ ` { \| } ~<br>You cannot use the # symbol when you enter a user name in a screen from the **Tool Panel** dialog box. |

| Item | Length in characters | Characters that can be used |
|---|---|---|
| Password | 6-256 | ▪ Alphanumeric (ASCII code) characters<br>▪ All symbols<br>You cannot use the quotation mark (") or backslash (\) symbols when you enter a password in a screen from the **Tool Panel** dialog box. |

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

**User name and password for logging in to SVP**

| Item | Length in characters | Characters that can be used |
|---|---|---|
| User name | 1-128 | ▪ Alphanumeric (ASCII code) characters<br>▪ The following symbols:<br>! # $ % & ' - . @ ^ _ ` { } ~ |
| Password | 6- 127 | ▪ Alphanumeric (ASCII code) characters<br>▪ All symbols |

**User name and password for logging in to CCI**

| Item | Length in characters | Characters that can be used |
|---|---|---|
| User name | 1-63 | ▪ Alphanumeric (ASCII code) characters<br>▪ The following symbols*:<br>- . @ _ |
| Password | 6- 63 | ▪ Alphanumeric (ASCII code) characters<br>▪ The following symbols*:<br>- , . @ _ |
| *When you use a Windows computer for CCI, you can also specify a backslash (\). When you use a UNIX computer for CCI, you can also specify a slash (/). | | |

**User name and password for logging in to NAS Manager**

| Item | Length in | Characters that can be used |
|---|---|---|
| User name | 1-20 | ▪ Alphanumeric (ASCII code) characters<br>▪ The following symbols*:<br>- . _ |
| Password | 6-256 | ▪ Alphanumeric (ASCII code) characters<br>▪ All symbols:<br>- . _ |
| * Do not specify a user name consisting of periods (.) (..) only, or specify a user name beginning with a hyphen (-). If you specify such names, you cannot log in to NAS Manager. | | |

## Changing user passwords

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

**Caution:** When using Hitachi Command Suite, you need to change information, such as passwords, registered in Hitachi Command Suite. For details, see the section describing how to change storage system settings in the Hitachi Command Suite User Guide.

**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 Changing the administrator password (on page 54).

### 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 **Task** 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 **Task** window opens to show the status of the task.

## Enabling or Disabling user accounts

To allow or prevent a user from logging in to Device Manager - Storage Navigator and NAS Manager, 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 enable or 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.
   - To allow the user to log in to Device Manager - Storage Navigator and NAS Manager, click **Enable**.
   - To prevent the user from logging in to Device Manager - Storage Navigator and NAS Manager, click **Disable**.
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 **Task** 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 **Task** window opens to show the status of the task.

### Releasing a user lockout

If a user attempting to log in to Device Manager - Storage Navigator or Command Control Interface enters an incorrect username or password three times, the system sets the login status to locked, preventing further login attempts 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**.

### Session timeout

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

## Managing user groups

You can use the Device Manager - Storage Navigator to view existing user groups, and to create, modify, or delete them.

Before creating or manipulating user groups, read and understand the following precautions.

- 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.
- If a user has All Resource Groups Assigned set to Yes, the user can access all the resources in the storage system. For example, if a user is a security administrator and a storage administrator taking care of some resources, have all resource groups assigned, and has roles of Security Administrator (View & Modify) and Storage Administrator (View & Modify), the user can edit the storage for all the resources.

  If this is a problem, the recommended solution is to register the following two user accounts in the storage system and use these different accounts for different purposes:

  - A security administrator user account that has All Resource Groups Assigned set to Yes.
  - A storage administrator user account that does not have all resource groups assigned and has only some of the resource groups assigned.

- For the user groups whose roles are other than the Storage Administrator, All Resource Groups Assigned is automatically set to Yes. If you delete all the roles except the Storage Administrator, reassign resource groups to the user group because All Resource Groups Assigned is automatically set to No. To assign resource groups to the user group, see Changing assigned resource groups (on page 92).
- Security settings that affect the entire system is configured by the administrator.
- Resource group 10 is configured by user A.
- Resource group 20 is configured by user B.

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

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

**Notes:**

1. For the user group that is assigned the Security Administrator role, All Resource Groups Assigned is automatically set to Yes.
2. There are a few types of storage administrators. For more information, see Roles (on page 85).

## Roles

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

| Role | Capabilities |
|---|---|
| Security Administrator (View Only) | ▪ Viewing information about user accounts and encryption settings<br>▪ Viewing information about the encryption key in the key SVP |

| Role | Capabilities |
|---|---|
| Security Administrator (View & Modify) | ▪ Configuring user accounts<br>▪ Creating encryption keys and configuring encryption settings<br>▪ Viewing and switching where encryption keys are generated<br>▪ Backing up and restoring encryption keys<br>▪ Deleting encryption keys backed up in the key SVP<br>▪ Viewing and changing the password policy for backing up encryption keys on the management client<br>▪ Connection to the external server<br>▪ Backing up and restoring connection configuration to the external server<br>▪ Configuring the certificate used for the SSL communication<br>▪ Configuring the fibre channel authentication (FC-SP)<br>▪ Configuring resource groups<br>▪ Editing virtual management settings<br>▪ Setting reserved attributes for global-active device |
| 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<br>▪ Configuring settings for SNMP<br>▪ Configuring settings for e-mail notification<br>▪ Configuring settings for license keys<br>▪ Viewing, deleting, and downloading storage configuration reports<br>▪ Acquiring all the information about the storage system and updating Device Manager - Storage Navigator window by clicking Refresh All |
| Storage Administrator (System Resource Management) | ▪ Configuring settings for CLPR<br>▪ Configuring settings for MP unit<br>▪ Deleting tasks and releasing exclusive locks of resources<br>▪ Configuring LUN security<br>▪ Configuring Server Priority Manager<br>▪ Configuring tiering policies |

| Role | Capabilities |
|---|---|
| Storage Administrator (Provisioning) | ▪ Configuring caches<br>▪ Configuring volumes, pools, and virtual volumes<br>▪ Formatting and shredding volumes<br>▪ Configuring external volumes<br>▪ Configuring Dynamic Provisioning<br>▪ Configuring host groups, paths, and WWN<br>▪ Configuring Volume Migration except splitting Volume Migration pairs when using CCI<br>▪ Configuring access attributes for volumes<br>▪ Configuring LUN security<br>▪ Creating and deleting quorum disk used with global-active device<br>▪ Creating and deleting global-active device pairs |
| Storage Administrator (Performance Management) | ▪ Configuring monitoring<br>▪ Starting and stopping monitoring |
| Storage Administrator (Local Copy) | ▪ Performing pair operations for local copy<br>▪ Configuring environmental settings for local copy<br>▪ Splitting Volume Migration pairs when using CCI |
| Storage Administrator (Remote Copy) | ▪ Remote copy operations in general<br>▪ Operating global-active device pairs (except for creation and deletion) |
| Support Personnel (Vendor Only) | Configuring the SVP<br>▪ Normally, this role is for service representatives. |
| Support Personnel (User) | ▪ Viewing storage system status<br>▪ Installing OS security patches<br>▪ Updating operating systems<br>▪ Performing basic maintenance |

## Built-in groups, roles, and resource 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.

For more information about resource groups, see the *Provisioning Guide*.

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)<br>▪ Audit Log Administrator (View & Modify)<br>▪ Storage administrator (Initial Configuration)<br>▪ Storage Administrator (System Resource Management)<br>▪ Storage Administrator (Provisioning)<br>▪ Storage Administrator (Performance Management)<br>▪ Storage Administrator (Local Copy)<br>▪ Storage Administrator (Remote Copy) | All Resource Groups Assigned |
| System | ▪ Security Administrator (View & Modify)<br>▪ Audit Log Administrator (View & Modify)<br>▪ Storage Administrator (Initial Configuration)<br>▪ Storage Administrator (System Resource Management)<br>▪ Storage Administrator (Provisioning)<br>▪ Storage Administrator (Performance Management)<br>▪ Storage Administrator (Local Copy)<br>▪ Storage Administrator (Remote Copy) | All Resource Groups Assigned |
| Security Administrator (View Only) | ▪ Security Administrator (View Only)<br>▪ Audit Log Administrator (View Only)<br>▪ Storage Administrator (View Only) | All Resource Groups Assigned |

| Built-in group | Role | Resource group |
|---|---|---|
| Security Administrator (View & Modify) | ▪ Security Administrator (View & Modify)<br>▪ Audit Log Administrator (View & Modify)<br>▪ Storage Administrator (View Only) | All Resource Groups Assigned |
| Audit Log Administrator (View Only) | ▪ Audit Log Administrator (View Only)<br>▪ Storage Administrator (View Only) | All Resource Groups Assigned |
| Audit Log Administrator (View & Modify) | ▪ Audit Log Administrator (View & Modify)<br>▪ 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)<br>▪ Storage Administrator (System Resource Management)<br>▪ Storage Administrator (Provisioning)<br>▪ Storage Administrator (Performance Management)<br>▪ Storage Administrator (Local Copy)<br>▪ Storage Administrator (Remote Copy) | meta_resource |
| Support Personnel | ▪ Storage Administrator (Initial Configuration)<br>▪ Storage Administrator (System Resource Management)<br>▪ Storage Administrator (Provisioning)<br>▪ Storage Administrator (Performance Management)<br>▪ Storage Administrator (Local Copy)<br>▪ Storage Administrator (Remote Copy)<br>▪ Support Personnel | All Resource Groups Assigned |

## Verifying the roles available to a user group

You can use Device Manager - Storage Navigator to verify the roles that are available to use with any user group.

### Before you begin

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

### Procedure

1. In the Device Manager - Storage Navigator tree, click **User Administration**.
2. On the **User Groups** tab, click the name (not the checkbox) of a user group whose roles you want to check.
3. In the **User Administration** window, click the **Roles** tab.
   The list of roles applied to the selected user group is displayed.
4. To return to the **User Administration** window, click **User Administration**.

## Checking if a role is available to a user group

You can use Device Manager - Storage Navigator to verify the roles that are available to use with any user group.

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.

### Before you begin

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

### Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, click **User Administration**.
2. On the **User Groups** tab, click the **name** (not the checkbox) of a user group whose roles you want to check.
3. In the **User Administration** window, click the **Roles** tab. The list of roles applied to the selected user group is displayed.
4. To return to the **User Administration** window, click **User Administration**.

## 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 **Task** 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 **Task** 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 **Task** 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 **Task** 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**.

## Creating resource groups and managing storage system resources

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.

### When to use 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.

Resources such as LDEVs, parity groups, iSCSI targets, external volumes, ports, and host groups can be assigned to a resource group. These resources can be combined to flexibly compose a virtual private storage system. You should plan and create resource groups before creating volumes.

## System configuration using resource groups

Configuring resource groups prevents the risk of data leakage or data destruction by another Storage Administrator in another resource group. The Storage Administrator considers and plans which resource should be managed by which user, and then the Security Administrator creates resource groups and assigns each resource to the resource groups.

A resource group is assigned one or more storage system resources. 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.

## Resource group examples

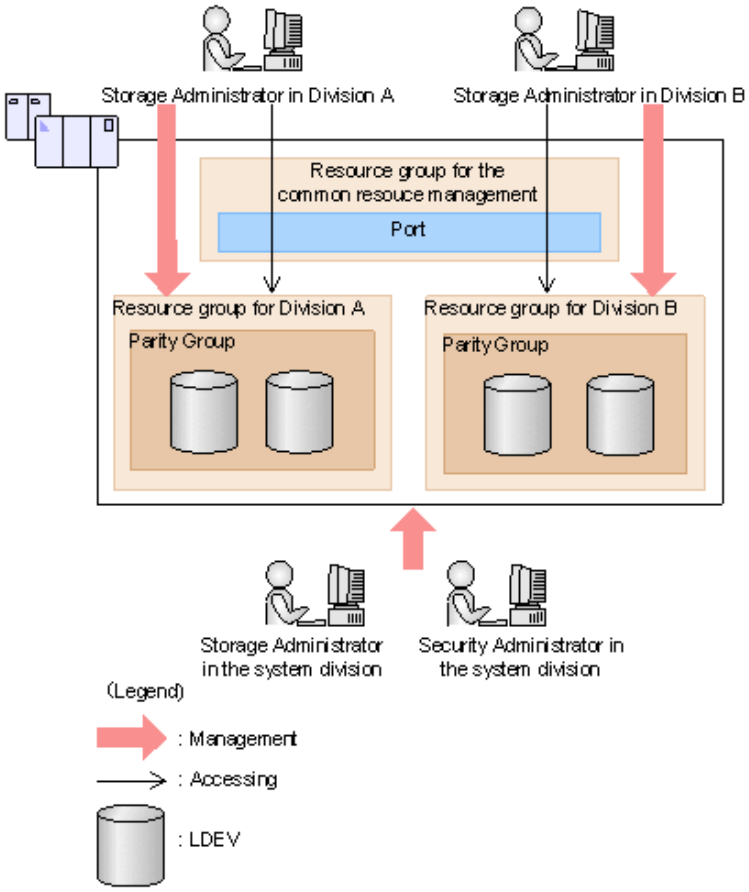
The following examples illustrate how you can configure resource groups on your storage system.

- Example of resource groups sharing a port (on page 95)
- Example of resource groups not sharing ports (on page 96)

## *Example of 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.

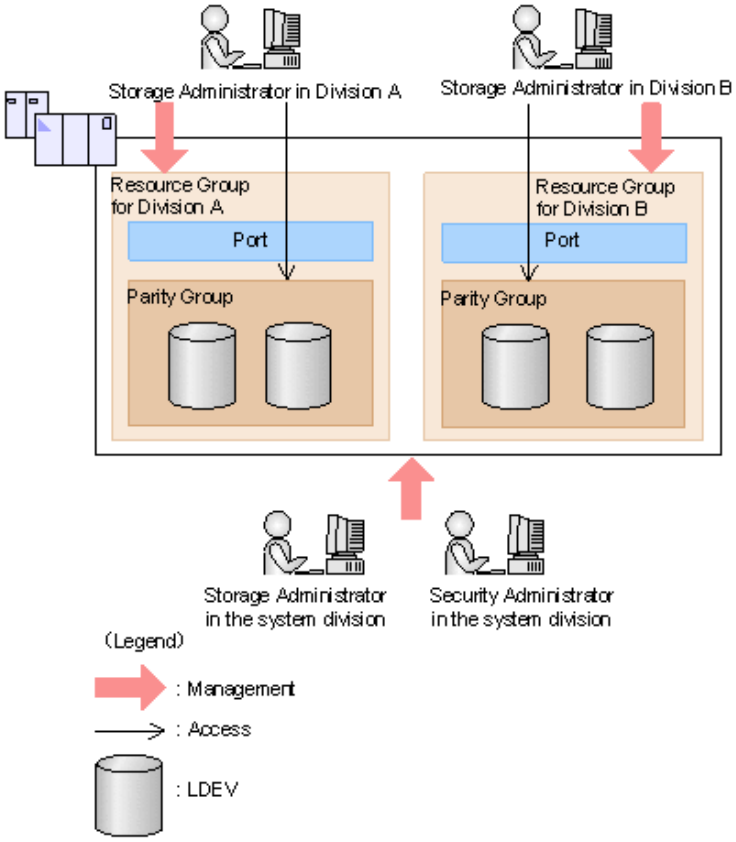
3. The Security Administrator creates the user groups.
4. The Security Administrator assigns the resource groups to the user groups.
5. The Storage Administrator in the system division sets a port.
6. The Security Administrator assigns resources to the resource groups.
7. The Security Administrator assigns 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.

### *Example of 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.

## Meta_resource

The meta_resource is a resource group comprised of additional resources (other than external volumes) and the resources that exist on the storage system before the Resource Partition Manager is installed. By default, 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

While processing a task on a resource, all of the resource groups assigned to the logged-on user are locked for exclusive access.

A secondary window (such as the **Basic Information Display**) or an operation from the service processor (SVP) locks all of the resource groups in the storage system.

When a resource is locked, a status indicator appears on the Device Manager - Storage Navigator status bar. Click the Resource Locked button to view information about the locked resource.


## User groups

User groups and associated built-in roles are defined in Device Manager - Storage Navigator. A user belongs to one or more user groups. Privileges allowed to a particular user are determined by the user group or groups to which the user belongs.

The Security Administrator assigns resource groups to user groups. A user group might already be configured, or a new user group might be required for certain resources.

## 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.

## Operations in a resource group for NAS modules

In the storage system in which the NAS module is installed, a resource group for NAS is created with the name NAS_Platform_System_RSG. Resources in NAS_Platform_System_RSG, such as LDEV format or delete, cannot be operated. Therefore, move resources in NAS_Platform_System_RSG to a different resource group before operating. For about operations for NAS_Platform_System_RSG, contact customer support.

## Resource group rules, restrictions, and guidelines

### Rules

- The maximum number of resource groups that can be created on a storage system is 1023. However, if the NAS module is installed in the storage system, the maximum number of resource groups that can be created on the storage system is 1022.
- A Storage Administrator with the Security Administrator (View & Modify) role can create resource groups and assign resources to resource groups.
- Resources removed from a resource group are returned to meta_resource.
- Only a Security Administrator (View & Modify) can manage the resources in assigned resource groups.

### Restrictions

- No new resources can be added to meta_resource and NAS_Platform_System_RSG.
- Resources cannot be deleted from meta_resource and NAS_Platform_System_RSG.
- LDEVs with the same pool IDs or journal IDs cannot be added to multiple resource groups.

  In the case of adding LDEVs that are used as pool volumes or journal volumes, add all the LDEVs that have the same pool IDs or journal IDs by using a function such as sort.

### Guidelines

- 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.

## Managing resource groups

Managing resource groups includes creating, editing, and deleting resource groups.

### *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.

Note the following restrictions for creating a resource group:

- The maximum number of resource groups that can be created on a storage system is 1023. If the NAS module is installed in the storage system, the maximum number of resource groups that can be created on the storage system is 1022.
- 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`, `NAS_Platform_System_RSG`

#### 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. Click **Create Resource Groups**.
3. 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.
4. 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**.
5. When you are finished configuring new resource groups in the **Create Resource Groups** window, click **Next**.
6. Enter a task name or accept the default, and then click **Submit**.

   If you select **View task status**, the **Tasks & Alerts** tab opens.

### *Editing resource groups*

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.

- Duplicate occurrences of the same name are not allowed.
- Resource group names can include alphanumeric characters, spaces, and the following symbols: ! # $ % & ' ( ) + - . = @ [ ] ^ _ ` { } ~
- Resource group names are case-sensitive.
- 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`, `NAS_Platform_System_RSG`
- 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 the 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.

The following tables specify the resource access requirements for Device Manager - Storage Navigator operations. For details about user groups and resource groups, see the *System Administrator Guide*.

### *Access requirements for Dynamic Provisioning and Dynamic Tiering*

The following table specifies the resource access requirements for Dynamic Provisioning and Dynamic Tiering operations.

| Operation name | Condition |
|---|---|
| Create LDEVs | If DP-VOLs are created, the following must be assigned to the Storage Administrator group that is permitted to manage them.<br>▪ LDEV ID<br>▪ Pool-VOL of the pool |
| Delete LDEVs | If DP-VOLs are deleted, the following must be assigned to the Storage Administrator group that is permitted to manage them.<br>▪ LDEV ID<br>▪ Pool-VOL of the pool |

| Operation name | Condition |
|---|---|
| Create pools<br>Expand pools | Volumes to be specified as pool-VOLs must be assigned to the Storage Administrator group permitted to manage them.<br>All the volumes that are specified when creating a pool must belong to the same resource group. |
| Edit pools<br>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<br>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*

The following 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.<br>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 LUN Manager*

The following table specifies 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.<br>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.<br>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.<br>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 initiator 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.<br>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.<br>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. |

| Operation name | Condition |
|---|---|
| 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.<br>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.<br>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. |
| 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.<br>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. |

| Operation name | Condition |
|---|---|
| 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*

The following 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*

The following 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

The following table specifies the resource access requirements for Thin Image operations.

| Operation name | Condition |
|---|---|
| Create LDEVs | If LDEVs for Thin Image are created, the following must be assigned to the Storage Administrator group that is permitted to manage them.<br>▪ LDEV ID<br>▪ Pool VOL of the pool |
| Delete LDEVs | If LDEVs for Thin Image are deleted, the following must be assigned to the Storage Administrator group that is permitted to manage them.<br>▪ LDEV ID<br>▪ Pool VOL of the pool |
| Create pools<br>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.<br>All the volumes that are specified when creating pools must belong to the same resource group. |
| Edit Pools<br>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

The following table specifies the resource access requirements for TrueCopy operations.

| Operation name | Condition |
|---|---|
| Edit Ports | Specified ports must be assigned to the user. |

| Operation name | Condition |
|---|---|
| Add Remote Connection | Specified initiator 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.<br>Initiator 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.<br>If primary volumes are specified, the initiator 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 initiator ports must be assigned to the user. |
| Remove Remote Paths | Specified initiator ports must be assigned to the user. |
| Edit Remote Connection Options | Initiator ports of remote paths that are connected to a specified remote storage must be assigned to the user. |
| Remove Remote Connections | Initiator 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 global-active device*

The following 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 initiator ports must be assigned to the user. |
| Edit Remote Connection Options | Operation can be performed with no conditions. |

| Operation name | Condition |
|---|---|
| Create Pairs | Primary volumes must be assigned to the user.<br>Initiator 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.<br>If primary volumes are specified, the initiator 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 initiator ports must be assigned to the user. |
| Remove Remote Paths | Specified initiator ports must be assigned to the user. |
| Edit Remote Connection Options | Initiator ports of remote paths that are connected to a specified remote storage must be assigned to the user. |
| Remove Remote Connections | Initiator 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 to be set as quorum disks must be assigned to the user. |

### *Access requirements for Universal Replicator*

The following 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 initiator ports must be assigned to the user. |
| Add Remote Paths | Specified initiator ports must be assigned to the user. |

| Operation name | Condition |
|---|---|
| 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. |
| Create Pairs | Journal volumes for pair volumes and primary volumes must be assigned to the user.<br>Initiator 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.<br>Initiator 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.<br>Journal volumes must be assigned to the user. |

| Operation name | Condition |
|---|---|
| Edit Mirror Options | All data volumes configuring the specified journal must be assigned to the user.<br>Journal volumes must be assigned to the user. |
| Remove Journals | Journal volumes must be assigned to the user. |
| Edit Remote Connection Options | Initiator ports of remote paths that are connected to a specified remote storage must be assigned to the user. |
| Remove Remote Paths | Specified initiator 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.<br>Specified remote command devices must be assigned to the user. |
| Release Remote Command Devices | Journal volumes must be assigned to the user.<br>Specified remote command devices must be assigned to the user. |

### *Access requirements for Universal Volume Manager*

The following 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 external port belongs.<br>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 that external volumes must be assigned to the Storage Administrator group permitted to manage them. |

| Operation name | Condition |
|---|---|
| Reconnect external storage systems | All the external volumes belonging to the specified external storage system and all the LDEVs allocated to that external volumes must be assigned to the Storage Administrator group permitted to manage them. |
| Disconnect external volumes | The specified external volume and all the LDEVs allocated to the external volumes must be assigned to the Storage Administrator group permitted to manage them. |
| Reconnect external volumes | The specified external volume and all the LDEVs allocated to the external volumes must be assigned to the Storage Administrator group permitted to manage them. |
| Edit external volumes | The specified external volume must be assigned to the Storage Administrator group permitted to manage them. |
| 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.<br>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.<br>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. |

| Operation name | Condition |
|---|---|
| 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.<br>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.<br>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*

The following 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.<br>When you create an internal or external volumes parity groups where the LDEV belongs and ID of the new LDEV 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. |

| Operation name | Condition |
|---|---|
| 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.<br>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.<br>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.<br>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*

The following 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.<br>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 Shredder*

The following 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.<br>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*

The following 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) | |

| Operation name | Conditions |
|---|---|
| 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 | |

## 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 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=passwordauth.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 an authentication server. Specify `ldap`. | Required | None |
| auth.server.name | The name of an authentication server.<br>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.<br>The names can use all ASCII code characters except for the following: \ / : , ; * ? " < > \| $ % & ' ~<br>In this manual, the value specified here is called <server_ name> hereafter. | Required | None |
| auth.group.mapping | Information about whether to work together with an authorization server:<br>▪ true: Works together<br>▪ false: Does not work together | Optional | False |

| Attribute | Description | Required / Optional | Default value |
|---|---|---|---|
| auth.ldap.<server_name>.protocol | LDAP protocol to use.<br>▪ ldaps: Uses LDAP over SSL/TLS.<br>▪ starttls: Uses StartTLS.<br>When you specify "true" to auth.ldap.<server_name>.dns_lookup, specify ldaps. | Rquired | None |
| auth.ldap.<server_name>.host | A 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.<br>If this value is specified, auth.ldap.<server_name>.dns_lookup will be ignored | Optional[1] | None |
| auth.ldap.<server_name>.port | A port number of the LDAP server.<br>Must be between 1 and 65,535.[2] | Optional | 389 |
| auth.ldap.<server_name>.timeout | The number of seconds before the connection to the LDAP server times out. It 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).<br>▪ Hierarchical model: An attribute name where the value that can identify a user is stored<br>▪ Flat model: An attribute name for a user entry's RDN<br>sAMAccountName is used for Active Directory. | Required | None |

| Attribute | Description | Required / Optional | Default value |
|---|---|---|---|
| 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 |
| auth.ldap.<server_name>.basedn | BaseDN for searching for users to authenticate.[3]<br>▪ Hierarchical model: DN of hierarchy that includes all the targeted users for searching<br>▪ 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.<br>Must be between 0 and 3. Zero means no retry.[2] | Optional | 3 |
| auth.ldap.<server_name>.domain.name | A domain name that the LDAP server manages. | Required | None |

| Attribute | Description | Required / Optional | Default value |
|---|---|---|---|
| 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.<br>▪ true: Searches with the information registered in the SRV records in the DNS server<br>▪ false: Searches with the host name and port number<br>When "host" and "port" are specified, the LDAP server is not searched with the information registered in the SRV records by specifying "true". | Optional | False |

**Notes:**

1. The 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 will be used.
3. To use symbols such as + ; , < = and >, enter a backslash (\) before each symbol. When using multiple symbols, each symbol must have a backslash before it. For example, to enter abc++ in the searchdn field, use \+ instead of + as shown here: abc\+\+

   To enter \ , /, or ", enter a backslash and then enter the ASCII code in hex for the following symbols:

   - Enter \5c for \
   - Enter \2f for /
   - Enter \22 for "

   For example, to enter abc\ in the searchdn field, enter abc\5c.

## 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=xxx.xxx.xxx.xxx
auth.radius.PrimaryServer.port=1812
auth.radius.PrimaryServer.timeout=3
auth.radius.PrimaryServer.secret=secretword
auth.radius.PrimaryServer.retry.times=3
auth.radius.PrimaryServer.attr.NAS-Identifier=xxxxxxxx
auth.group.auth.radius.PrimaryServer.domain.name=radius.example.com
auth.group.auth.radius.PrimaryServer.domain.name.protocol=ldap
auth.group.auth.radius.PrimaryServer.domain.name.host=xxx.xxx.xxx.xxx
auth.group.auth.radius.PrimaryServer.domain.name.port=386
auth.group.auth.radius.PrimaryServer.domain.name.searchdn=CN=sample1,CN=Use
rs,DC=domain,DC=local
auth.group.auth.radius.PrimaryServer.domain.name.searchpw=password
auth.ldap.PrimaryServer.basedn=CN=Users,DC=domain,DC=local
```

The attributes are defined in the following tables.

**Table 5 RADIUS definition (for authentication server)**

| Attribute | Description | Required / Optional | Default value |
|---|---|---|---|
| auth.server.type | Type of an authentication server. Specify `radius`. | Required | None |

| Attribute | Description | Required / Optional | Default value |
|---|---|---|---|
| auth.server.name | The name of an authentication server.<br>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.<br>The names can use all ASCII code characters except for the following:<br>\ / : , ; * ? " < > \| $ % & ' ~<br>In this manual, the value specified here is called *server-name* hereafter. | Required | None |
| auth.group.mapping | Information about whether to work together with an authorization server<br>▪ true: Works together<br>▪ false: Does not work together | Optional | False |
| auth.radius.*server-name*.protocol | RADIUS protocol to use.<br>▪ PAP: Password authentication protocol that transmits plaintext user ID and password<br>▪ CHAP: Challenge-handshake authentication protocol that transmits encrypted password | Required | None |
| auth.radius.*server-name*.host | A host name, an IPv4 address or an IPv6 address of the RADIUS server. An IPv6 address must be enclosed in square brackets. | Required | None |
| auth.radius.*server-name*.port | A port number of the RADIUS server.<br>Must be between 1 and 65,535.[1] | Optional | 1,812 |
| auth.radius.*server-name*.timeout | The number of seconds before the connection to the RADIUS server times out.<br>Must be between 1 and 30.[2] | Optional | 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.<br>Must be between 0 and 3. 0 means no retry.[1] | Optional | 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[2] | None |
| auth.radius.*server-name*.attr.NAS-IPv4-Address | IPv4 address of the SVP. Specify the value of the NAS-IP-Address attribute. This value is transmitted to the RADIUS server when the authentication is requested. | Optional[2] | 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[2] | None |

**Notes:**

1. If the specified value is not applicable, the default value will be used.
2. When NAS modules are installed, set `NAS-Identifier`, `NAS-IP-Address`, or `NAS-IPv6-Address`.

**Table 6 RADIUS definition (for authorization server)**

| Attribute | Description | Required / Optional | Default value |
|---|---|---|---|
| auth.radius.*server-name*.domain.name | A domain name that the LDAP server manages. In this manual, the value specified here is called *domain-name* hereafter. | Required | None |

| Attribute | Description | Required / Optional | Default value |
|---|---|---|---|
| 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.<br>▪ true: Searches with the information registered in the SRV records in the DNS server<br>▪ false: Searches with the host name and port number.<br>When "host" and "port" are specified, the LDAP server is not searched with the information registered in the SRV records by specifying "true". | Optional | false |
| auth.radius.*domain-name*.protocol | LDAP protocol to use.<br>▪ ldaps: Uses LDAP over SSL/TLS.<br>▪ starttls: Uses StartTLS.<br>When you choose ldap, specify "true" to "auth.radius.*domain-name*.dns_lookup" | Required | None |
| auth.radius.*domain-name*.host | A host name, an IPv4 address or an IPv6 address of the LDAP server. An IPv6 address must be enclosed in square brackets ([ ]). | Optional[1] | None |
| auth.radius.*domain-name*.port | A port number of the LDAP server.<br>Must be between 1 and 65535.[2] | Optional | 389 |
| auth.radius.*domain-name*.searchdn | DN of the user for searching. | Required | None |
| auth.radius.*domain-name*.searchpw | User password for searching. Specify the same password that is registered in the LDAP server. | Required | None |
| auth.radius.*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.[3] | Optional | abbr |

| Attribute | Description | Required / Optional | Default value |
|---|---|---|---|
| auth.radius.*domain-name*.timeout | The number of seconds before the connection to the LDAP server times out. Must be between 1 and 302. | Optional | 10 |
| auth.radius.*domain-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.radius.*domain-name*.retry.times | Retry times when the connection to the LDAP server fails. Must be between 0 and 3. 0 means no retry. [2] | Optional | 3 |

**Notes:**

1. The 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 will be used.
3. To use symbols such as + ; , < = and >, enter a backslash (\) before each symbol. When using multiple symbols, each symbol must have a backslash before it. For example, to enter abc++ in the searchdn field, use \+ instead of + as shown here: abc\+\+

   To enter \ , /, or ", enter a backslash and then the ASCII code in hex for these symbols.

   - Enter \5c for \.
   - Enter \2f for /.
   - Enter \22 for "

   For example, to enter abc\ in the searchdn field, enter abc\5c.

## 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 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.clockshow=300
auth.kerberos.timeout=10
auth.group.example.com.searchdn=CN=sample1,CN=Users,DC=domain,DC=localauth.
group.example.com.searchpw=passwordauth.ldap.PrimaryServer.basedn=CN=Users,
DC=domain,DC=local
```

The Kerberos attributes are defined in the following table.

**Table 7 Kerberos definition (for authentication server)**

| Attribute | Description | Required / Optional | Default value |
|---|---|---|---|
| auth.server.type | Type of an authentication server. Specify `kerberos`. | Required | None |
| auth.group.mapping | Information about whether to work together with an authorization server<br>▪ true: Works together<br>▪ false: Does not work together | Optional | false |
| auth.kerberos.default_realm | Default realm name | Required | None |

| Attribute | Description | Required / Optional | Default value |
|---|---|---|---|
| auth.kerberos.dns_lookup.kdc | This is a switch that determines which information registered in the SRV records in the DNS server to use when searching the Kerberos server.<br>▪ true: Searches with the information registered in the SRV records in the DNS server<br>▪ false: Searches with the host name and port number<br>When "realm name" and "<value specified to the realm name>.kdc" are specified, the Kerberos server is not searched with the information registered in the SRV records by specifying "true". | Optional | false |
| auth.kerberos.clock skew | The acceptable range of the difference in time between the SVP and the Kerberos server where the SVP is operating.<br>Must be between 0 and 300 seconds.[1] | Optional | 300 |
| auth.kerberos.time out | The 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.[1] | Optonal | 10 |
| auth.kerberos.real m_name | Realm identifier name<br>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. The value specified here is called <realm_name> hereafter. | Optional[2] | None |

| Attribute | Description | Required / Optional | Default value |
|---|---|---|---|
| auth.kerberos.<realm _name>.realm | The realm name set to the Kerberos server. | Optional[2] | None |
| auth.kerberos.<realm_name>.kdc | The host name, the IPv4 address, and the port number of the Kerberos server. Specify these in the format of "<Host name or IP address>[:Port number]". | Optional[2] | None |

**Notes:**

1. The 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 will be used.
3. To use symbols such as + ; , < = and >, enter a backslash (\) before each symbol. When using multiple symbols, each symbol must have a backslash before it. For example, to enter abc++ in the searchdn field, use \+ instead of + as shown here: abc\+\+

   To enter \ , /, or ", enter a backslash and then the ASCII code in hex for these symbols.

   - Enter \5c for \.
   - Enter \2f for /.
   - Enter \22 for ".

   For example, to enter abc\ in the searchdn field, enter abc\5c.

**Table 8 Kerberos definition (for authorization server)**

| Attribute | Description | Required / Optional | Default value |
|---|---|---|---|
| auth.group.<realm_na me>.protocol | LDAP protocol to use.<br>▪ ldaps: Uses LDAP over SSL/TLS.<br>▪ starttls: Uses StartTLS. | Required | None |
| auth.group.<realm_name>.port | A port number of the LDAP server.<br>Must be between 1 and 65535. [1] | Optoinal | 389 |

| Attribute | Description | Required / Optional | Default value |
|---|---|---|---|
| auth.group.<realm_name>.searchdn | DN of the user for searching.[2] | Required | 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.[2] | Optional | 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.[1] | Optional | 10 |
| auth.group.<realm_name>.retry.interval | Retry interval in seconds when the connection to the LDAP server fails. Must be between 1 and 5.[1] | Optional | 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.[1] | Optional | 3 |

| Attribute | Description | Required / Optional | Default value |
|---|---|---|---|

**Notes:**

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

   To enter \ , /, or ", enter a backslash and then the ASCII code in hex for these symbols.

   - Enter \5c for \
   - Enter \2f for /
   - Enter \22 for "

   For example, to enter abc\ in the searchdn field, enter abc\5c.

# User Administration for NAS Manager

This section describes various user roles, permissions and groups available to manage your storage system. You use NAS Manager to create and manage SMU user accounts on your storage system.

## Administrator types and responsibilities

This section describes the types of NAS storage system administrators and defines their expected roles in managing the system and the associated storage subsystems.

- **Global Administrators** can manage everything in the system: file systems, file services, or file system related features and functions, storage devices and their components. Also, the Global Administrator creates and manages SMU user profiles (Server Administrators, Storage Administrators, Server+Storage Administrators, and other Global Administrators). Global Administrators also control what servers and storage devices each administrator can access.
- **Storage Administrators** manage storage devices, as specified in the administrator profile created by the Global Administrator.

  Storage Administrators can manage only storage devices and their components (racks, physical disks, SDs, and storage pools). Storage Administrators cannot manage file systems, file services, or file system related features and functions, and they cannot manage users.
- **Server Administrators** manage servers and clusters, as specified in the administrator profile created by the Global Administrator. Server Administrators cannot manage storage devices.

  Server Administrators can manage file systems and file services such as CIFS Shares, NFS Exports, and they can manage file system related features and functions such as snapshots, quotas, and migration policies and schedules.

- **Server+Storage Administrators** manage servers, clusters, and storage devices, as specified in the administrator profile created by the Global Administrator.

  Server+Storage administrators can manage everything Server Administrators and Storage Administrators can manage: file systems, file services, or file system related features and functions, and they can also manage storage devices and their components.

All administrators can connect to the NAS storage system through NAS Manager, the browser-based management utility provided by the system management unit (SMU). Additionally, Global Administrators on an external or virtual SMU can connect to the SMU command line interface (CLI). SMU CLI access is not available on an embedded SMU or a NAS module SMU.

**Read-only users:** The above roles (when defined for local users or Active Directory groups) can be modified by making them read-only. A read-only user has permission to view most pages of the NAS Manager; however, they are not generally allowed to perform any actions on the NAS Manager that would trigger a system or configuration change.

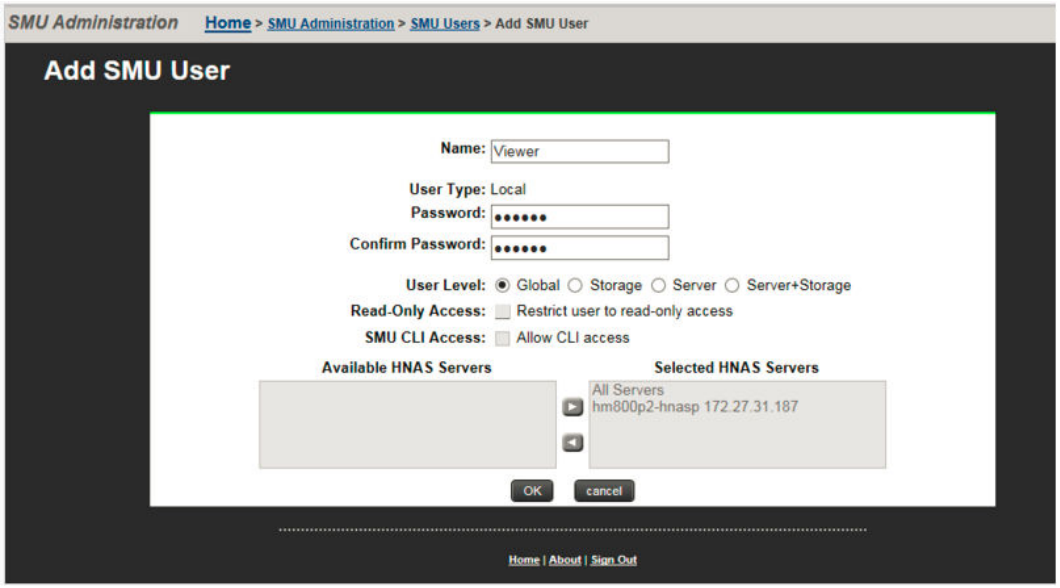
**Note:** Server Administrators, Storage Administrators, and Server+Storage Administrators cannot access all of the NAS Manager pages that a Global Administrator can access.

## Adding an SMU user (an administrator)

Use NAS Manager to add SMU user accounts for HNAS servers. For systems with NAS modules, use the maintenance utility or an external NAS Manager to create and manage user accounts.

### Procedure

1. Navigate to **Home** > **SMU Administration** > **SMU Users** to display the **SMU Users** page.
2. Click **add** to display the **Add SMU User** page:



| Field/Item | Description |
|---|---|
| Name | The name of the new user account. This name will be requested when logging in to the SMU. The rules for user names are:<br>▪ For Global administrators only, if the user will access the SMU through the CLI, the user name:<br>• Must start with a letter or an underscore, and may consist of up to 31 alphanumeric characters and the underscore (_) and the hyphen (–).<br>• Cannot match certain special purpose names: root, manager, postgres, nobody, or nfsnobody.<br>• Cannot match certain special purpose user ID numbers: for example, those with uid less than 502.<br>▪ For all types of administrators, if the user will access the SMU only through NAS Manager, the user name may consist of alphanumeric characters and/or the underscore (_), the hyphen (–), the equal sign (=), parentheses "(" or ")", brackets ( [ or ] ), the pound sign (#) and the exclamation point (!).<br>▪ **Supervisor** is a reserved system user name. It is not available as a new user name.<br>**Note:** If you are using RADIUS realms, and the global administrator will access the SMU using both NAS Manager and the CLI, use the underscore (_) to combine the user name and the realm: for example, `johnsmith_realm2`. If the global administrator will access the SMU using only NAS Manager, you can use the at sign (@) to combine the user name and the realm: for example, `johnsmith@realm3`. |
| User Type | The user type is either **local** or **RADIUS**.<br>▪ Local users are those whose passwords are locally defined and authenticated in the SMU.<br>▪ RADIUS users are those whose passwords are defined and authenticated in an external RADIUS servers. The RADIUS administrator must add a user name and password to all RADIUS servers. |
| Password | Enter the password that will be used when this user account logs in. The password cannot exceed 256 characters.<br>This field only applies when the User Type is selected to Local. It does not apply when the RADIUS User Type is selected. |

| Field/Item | Description |
|---|---|
| Confirm Password | Confirm the password entered in the previous field by entering it in again. Only applies when the Local User type is selected. |
| User Level | Specify the level for the new administrator that you are creating. You can select any one of the following:<br>▪ **Global Administrators** can manage everything in the system: file systems, file services, or file system related features and functions, storage devices and their components. Also, the Global Administrator creates and manages SMU user profiles (Server Administrators, Storage Administrators, Server+Storage Administrators, and other Global Administrators). Global Administrators also control what servers and storage devices each administrator can access.<br>▪ **Storage Administrators** manage storage devices, as specified in the administrator profile created by the Global Administrator.<br>Storage Administrators can manage only storage devices and their components (racks, physical disks, SDs, and storage pools). Storage Administrators cannot manage file systems, file services, or file system related features and functions, and they cannot manage users.<br>▪ **Server Administrators** manage servers and clusters, as specified in the administrator profile created by the Global Administrator. Server Administrators cannot manage storage devices.<br>Server Administrators can manage file systems and file services such as CIFS Shares, NFS Exports, and they can manage file system related features and functions such as snapshots, quotas, and migration policies and schedules.<br>▪ **Server+Storage Administrators** manage servers, clusters, and storage devices, as specified in the administrator profile created by the Global Administrator.<br>Server+Storage administrators can manage everything Server Administrators and Storage Administrators can manage: file systems, file services, or file system related features and functions, and they can also manage storage devices and their components.<br>**Note:** Server Administrators, Storage Administrators, and Server+Storage Administrators cannot access all of the NAS Manager pages that a Global Administrator can access. |

| Field/Item | Description |
|---|---|
| Read-Only User | Defines the user as read-only. A read-only user may be given Global, Server, Storage or Server+Storage access. Based on their defined role, an individual user may or may not perform specific tasks, such as viewing, creating, or modifying files and data. A read-only user has permission to view most pages of the NAS Manager; however, they are not generally allowed to perform any actions that would trigger a system or configuration change.<br><br>**Note:** Read-only users can not access the CLI, and a user with CLI access may not be read-only. If either of these options is checked, the other one is disabled. |
| SMU CLI Access (for Global Administrators only) | If the administrator is allowed to log in and access the SMU CLI of an external SMU, select the **SMU CLI Access** check box. |
| Available Managed Servers | For Server administrators, Storage administrators, and Server +Storage administrators, lists the servers managed by the SMU to which the administrator has not yet been given management privileges. Not available for Global administrators, because Global administrators are allowed to manage all storage and all servers. |
| Selected Managed Servers | For Server administrators, lists the servers that the administrator can manage. Note that a Server administrator cannot manage the storage attached to these servers. Not available for Global administrators, because Global administrators are allowed to manage all storage and all servers.<br><br>For Storage administrators, lists servers that have attached storage that the administrator can manage. Note that a Storage administrator cannot manage these servers, only the storage attached to these servers.<br><br>For Server+Storage administrators, lists servers that the administrator can manage. The Server+Storage administrator can also manage the storage attached to these servers. |

3. Enter the user name for the new administrator in the **Name** field.
4. Specify if the administrator login is authenticated locally (by the SMU) or by a RADIUS server by selecting the appropriate **User Type**.

**Note:** If you are authenticating this user through a RADIUS server, the **Password** and **Confirm Password** fields are not available, and you should skip the next step. You must enter the user passwords into the RADIUS server using the tools available for that server.

5. If the **User Type** is local, specify the initial login password for the new administrator by filling in the **Password** and the **Confirm Password** fields.
6. Specify the user level for the new administrator that you are creating.

   You can select one of the following:

   - **Global**
   - **Storage**
   - **Server**
   - **Server+Storage**
7. For Global Administrators only, if the administrator is allowed to log in and access the SMU command line interface (CLI) of an external SMU, select the **SMU CLI Access** check box.
8. Using the **Available Servers** and the **Selected Servers** lists, specify the servers the administrator can access or the servers with the storage the administrator can manage.
   - To grant management privileges for a server or the storage attached to a server, move the server from the **Available Servers** list to the **Selected Servers** list.
   - To revoke management privileges for a server or the storage attached to a server, move the server from the **Selected Servers** list to the **Available Servers** list.
   - To move the server between the **Available Servers** and the **Selected Servers** lists, select the server, and use the arrow buttons between the lists.
9. Review the profile, and verify that it is correct.
   - If the profile is correct, click **OK** to save and enable the user profile, and then return to return to the **SMU Users** page.
   - To return to the **SMU Users** page without saving the profile, click **back**.

## Changing user passwords

Any logged in user can change their own password. A global administrator can also change the password of any user, whether the user is currently logged in or not.

**Note:** If the user is authenticated through a RADIUS server, you cannot change the password using NAS Manager or the SMU CLI. You must change the password using the tools and utilities of the RADIUS server.

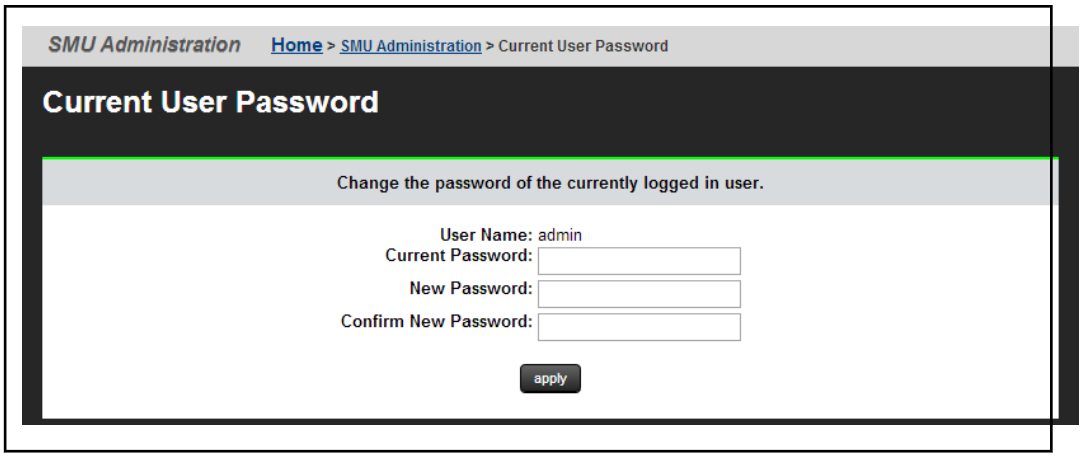
### Changing your own password

You can use NAS Manager to change your own password. If your account is authenticated through a RADIUS server, however, your password must be changed using the tools and utilities of the RADIUS server.

- For HNAS servers, use NAS Manager or the SMU CLI to change your password.
- For systems with NAS modules, use an external NAS Manager or the maintenance utility to change your password.

### Procedure

1. Navigate to **Home** > **SMU Administration** > **Current User Password** to display the **Current User Password** page.




The following table describes the fields on this page:

| Field/Item | Description |
|---|---|
| User Name | Displays your user login name (cannot be changed). |
| Current Password | Displays a series of dots representing the currently specified password (the actual password cannot be displayed). |
| New Password | The new password. The password cannot exceed 256 characters. |
| Confirm New Password | The new password again. Must be exactly the same as what you entered in the **New Password** field. |
| **apply** | Saves the new password. |

2. Enter your current password in the **Current Password** field.

   If you have forgotten you password, contact a global administrator and ask them to give you a new password. (Passwords are stored in an encrypted form, and are not retrievable or visible by anyone. If a user forgets their password, they must be given a new password, which they can then change.)
3. Enter your new password in the **New Password** field.
4. Enter the new password again in the **Confirm New Password** field.
5. When finished, click **apply** to save the new password.

## Changing another user's password

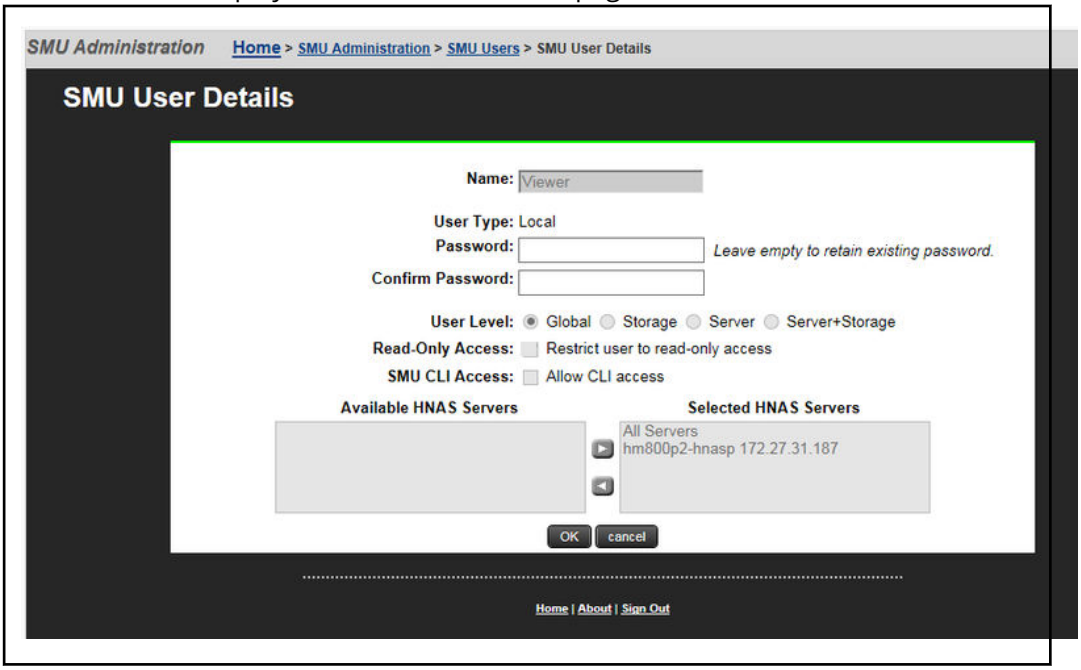
A global administrator can change the password of any user. If the user is authenticated through a RADIUS server, however, the password must be changed using the tools and utilities of the RADIUS server.

- For HNAS servers, use NAS Manager or the SMU CLI to change the user password.

- For systems with NAS modules, use an external NAS Manager or the maintenance utility to change the user password.

### Procedure

1. Navigate to **Home** > **SMU Administration** > **SMU Users** to display the **SMU Users** page.
2. Click **details** to display the **SMU User Details** page.




| Item/Field | Description |
|---|---|
| Name | Administrator's user name. Cannot be changed. |
| User Type | Describes if the user is authenticated by the SMU itself (local users), or if the user is authenticated by a RADIUS server. |
| Password and Confirm Password | For users authenticated by the SMU only (local users). These fields do not apply for users authenticated by a RADIUS server.<br>The password for the user. Characters are hidden, and the exact same password must be entered in both fields. The password cannot exceed 256 characters. |

| Item/Field | Description |
|---|---|
| User Level | Displays the user level or type of administrative role.<br>▪ **Global Administrators** can manage everything in the system: file systems, file services, or file system related features and functions, storage devices and their components. Also, the Global Administrator creates and manages SMU user profiles (Server Administrators, Storage Administrators, Server +Storage Administrators, and other Global Administrators). Global Administrators also control what servers and storage devices each administrator can access.<br>▪ **Storage Administrators** manage storage devices, as specified in the administrator profile created by the Global Administrator.<br>Storage Administrators can manage only storage devices and their components (racks, physical disks, SDs, and storage pools). Storage Administrators cannot manage file systems, file services, or file system related features and functions, and they cannot manage users.<br>▪ **Server Administrators** manage servers and clusters, as specified in the administrator profile created by the Global Administrator. Server Administrators cannot manage storage devices.<br>Server Administrators can manage file systems and file services such as CIFS Shares, NFS Exports, and they can manage file system related features and functions such as snapshots, quotas, and migration policies and schedules.<br>▪ **Server+Storage Administrators** manage servers, clusters, and storage devices, as specified in the administrator profile created by the Global Administrator.<br>Server+Storage administrators can manage everything Server Administrators and Storage Administrators can manage: file systems, file services, or file system related features and functions, and they can also manage storage devices and their components.<br>▪ If the User Type is Local, you can modify the password.<br>▪ If the User Type is RADIUS, you cannot modify the password, because the password is managed on |

| Item/Field | Description |
|---|---|
| | RADIUS servers. RADIUS users cannot be defined as read-only.<br>▪ If the User Level is Global, you can select or clear the **Allow CLI Access** check box.<br>▪ If the User Level is Storage, Server, or Server+Storage, you can add or remove servers from the user's scope of management.<br>Global users implicitly have access to manage all servers and storage. Non-global users cannot be given CLI access.<br>You cannot change the User Type or User Level of a user. If such a change is needed, delete the old user and create a new user. |
| Read-Only Access | Indicates if a user is defined as read-only, or not. When displaying the details of an existing user, the read-only attribute is shown but cannot be modified. To change the read-only attribute, it is necessary to delete the user and then re-add them. |
| SMU CLI Access | For global administrators only, when the check box is selected, the administrator can access the SMU using the CLI as well as NAS Manager. |
| Available HNAS Servers | Not available for global administrators, because global administrators are allowed to manage all storage and all servers.<br>For server administrators, storage administrators, and server+storage administrators, lists the HNAS servers managed by the SMU to which the administrator has not yet been give management privileges.<br>The "All Servers" entry is used to allow privileges to all servers managed by the SMU. |

| Item/Field | Description |
|---|---|
| Selected HNAS Servers | Not available for global administrators, because global administrators are allowed to manage all storage and all servers.<br>For server administrators, lists the HNAS servers that the administrator can manage. Note that a Server administrator cannot manage the storage attached to these servers.<br>For storage administrators, lists HNAS servers that have attached storage that the administrator can manage. Note that a storage administrator cannot manage these servers, only the storage attached to these servers.<br>For server+storage administrators, lists HNAS servers that the administrator can manage. The server+storage administrator can also manage the storage attached to these servers. |
| **OK** | Saves the currently defined user profile and returns to the **SMU Users** page. |
| **Cancel** | Returns to the **SMU Users** page without saving the profile. |

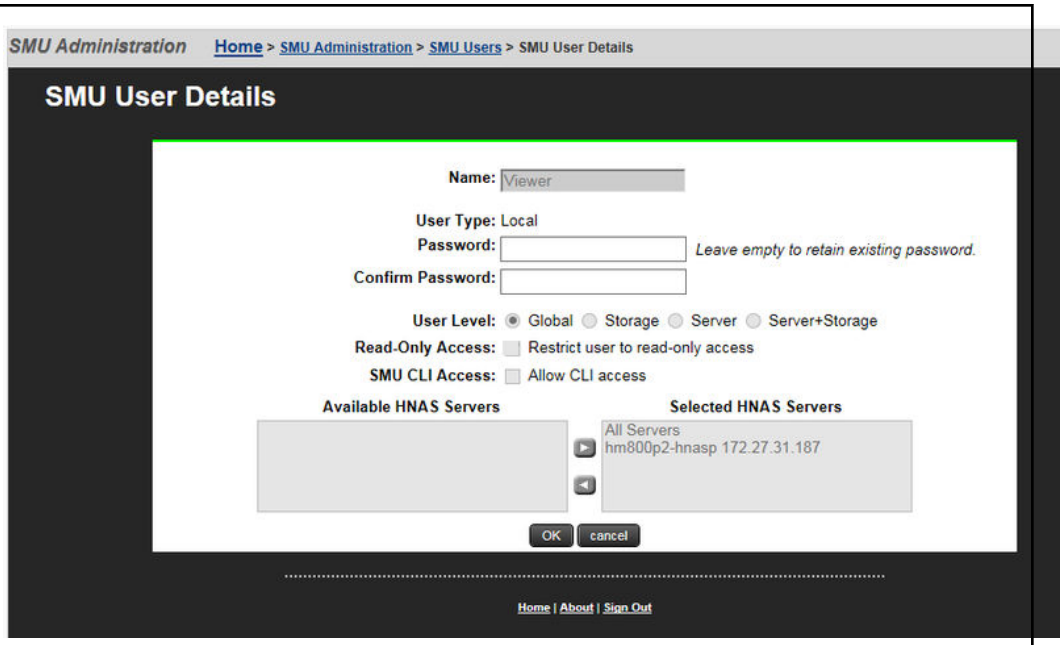
3. Enter the new password in the **Password** field.
4. Enter the new password again in the **Confirm Password** field.
5. When finished, click **OK** to save the new password.

## Changing an SMU user profile

Use NAS Manager to manage SMU user accounts for HNAS servers. For systems with NAS modules, use the maintenance utility or an external NAS Manager to manage user accounts.

### Procedure

1. Navigate to **Home** > **SMU Administration** > **SMU Users** to open the **SMU Users** page.
2. Click **details** to display the **SMU User Details** page for the user whose profile you want to modify.




| Item/Field | Description |
|---|---|
| Name | Administrator's user name. Cannot be changed. |
| User Type | Describes if the user is authenticated by the SMU itself (local users), or if the user is authenticated by a RADIUS server. |
| Password and Confirm Password | For users authenticated by the SMU only (local users). These fields do not apply for users authenticated by a RADIUS server.<br>The password for the user. Characters are hidden, and the exact same password must be entered in both fields. The password cannot exceed 256 characters. |

| Item/Field | Description |
|---|---|
| User Level | Displays the user level or type of administrative role.<br>▪ **Global Administrators** can manage everything in the system: file systems, file services, or file system related features and functions, storage devices and their components. Also, the Global Administrator creates and manages SMU user profiles (Server Administrators, Storage Administrators, Server +Storage Administrators, and other Global Administrators). Global Administrators also control what servers and storage devices each administrator can access.<br>▪ **Storage Administrators** manage storage devices, as specified in the administrator profile created by the Global Administrator.<br>Storage Administrators can manage only storage devices and their components (racks, physical disks, SDs, and storage pools). Storage Administrators cannot manage file systems, file services, or file system related features and functions, and they cannot manage users.<br>▪ **Server Administrators** manage servers and clusters, as specified in the administrator profile created by the Global Administrator. Server Administrators cannot manage storage devices.<br>Server Administrators can manage file systems and file services such as CIFS Shares, NFS Exports, and they can manage file system related features and functions such as snapshots, quotas, and migration policies and schedules.<br>▪ **Server+Storage Administrators** manage servers, clusters, and storage devices, as specified in the administrator profile created by the Global Administrator.<br>Server+Storage administrators can manage everything Server Administrators and Storage Administrators can manage: file systems, file services, or file system related features and functions, and they can also manage storage devices and their components.<br>▪ If the User Type is Local, you can modify the password.<br>▪ If the User Type is RADIUS, you cannot modify the password, because the password is managed on |

| Item/Field | Description |
|---|---|
| | RADIUS servers. RADIUS users cannot be defined as read-only.<br>▪ If the User Level is Global, you can select or clear the **Allow CLI Access** check box.<br>▪ If the User Level is Storage, Server, or Server+Storage, you can add or remove servers from the user's scope of management.<br>Global users implicitly have access to manage all servers and storage. Non-global users cannot be given CLI access.<br>You cannot change the User Type or User Level of a user. If such a change is needed, delete the old user and create a new user. |
| Read-Only Access | Indicates if a user is defined as read-only, or not. When displaying the details of an existing user, the read-only attribute is shown but cannot be modified. To change the read-only attribute, it is necessary to delete the user and then re-add them. |
| SMU CLI Access | For global administrators only, when the check box is selected, the administrator can access the SMU using the CLI as well as NAS Manager. |
| Available HNAS Servers | Not available for global administrators, because global administrators are allowed to manage all storage and all servers.<br>For server administrators, storage administrators, and server+storage administrators, lists the HNAS servers managed by the SMU to which the administrator has not yet been give management privileges.<br>The "All Servers" entry is used to allow privileges to all servers managed by the SMU. |

| Item/Field | Description |
|---|---|
| Selected HNAS Servers | Not available for global administrators, because global administrators are allowed to manage all storage and all servers.<br>For server administrators, lists the HNAS servers that the administrator can manage. Note that a Server administrator cannot manage the storage attached to these servers.<br>For storage administrators, lists HNAS servers that have attached storage that the administrator can manage. Note that a storage administrator cannot manage these servers, only the storage attached to these servers.<br>For server+storage administrators, lists HNAS servers that the administrator can manage. The server+storage administrator can also manage the storage attached to these servers. |
| **OK** | Saves the currently defined user profile and returns to the **SMU Users** page. |
| **Cancel** | Returns to the **SMU Users** page without saving the profile. |

3. Edit the SMU user password.

   **Note:** For users authenticated by the SMU only (local users), not available for users authenticated by a RADIUS server.

   To edit the user's password, type the new password in the **Password** and **Confirm Password** fields.

4. For global administrators only, allow or disallow SMU CLI access.

   When the check box is selected, the administrator can access the SMU by using the CLI as well as NAS Manager.

5. Specify server and/or storage management rights.
   - To grant management privileges for a server or the storage attached to a server, move the server from the **Available Servers** list to the **Selected Servers** list.
   - To revoke management privileges for a server or the storage attached to a server, move the server from the **Selected Servers** list to the **Available Servers** list.
   - To move the server between the **Available Servers** and the **Selected Servers** lists, select the server, and use the arrow buttons between the lists.

6. Click **OK** to save the profile and return to the **SMU Users** page.

# Chapter 5: Setting up security

This chapter describes how to set up security on your storage system.

## Setting up TCP/IP for 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.

For details about setting up the SVP, see the *Hardware Installation and Reference Guide* for your storage system.

## Working with certificates

A digital certificate can be thought of as an electronic passport that allows the SVP and storage system to exchange information securely over the Internet using the public key infrastructure (PKI).

You can use a Secure Sockets Layer (SSL) certificate, HCS certificate, or both to create a secure, encrypted connection between the SVP and the storage system.

### Managing HCS certificates

This topic explains how to set or delete certificates for Hitachi Command Suite (HCS) that are used to check the server's reliability when SSL communication for HCS external authentication is performed.

#### Registering HCS certificates

To check the server reliability during SSL communication for HCS external authentication, upload an HCS public key certificate to the web server to register the certificate.

**Note:** Ensure that you register or delete the correct certificate. Otherwise, HCS external authentication will not return.

**Before you begin**

- You must be logged into the SVP.
- The private key file on the HCS 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. In the folder where the certificate update tool is located, execute the following command:
   ```
   C:\MAPP\wk\Supervisor\MappIniSet>MappHcsCrtEntry.bat absolute-path-of-signed-public-key-certificate-file
   ```
   **Note:** A space is required between MappHcsCrtEntry.bat and the signed public key certification file path.
4. A completion message box displays. Press any key to acknowledge the message and close the message box.
5. Close the command prompt window.

## Deleting HCS certificates

You can delete the certificates you registered in the procedure of the "Registering certificates for HCS" section. After you delete a certificate, server reliability for that certificate is not checked by SSL communication for HCS external authentication.

### Before you begin

- You must be logged into the SVP.
- The private HCS server key must be updated.
- 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. In the folder where the certificate update tool is located, execute the following command:
   ```
   C:\MAPP\wk\Supervisor\MappIniSet>MappHcsCrtDelete.bat
   ```
4. A completion message box opens. Press any key to acknowledge the message and close the message box.
5. Close the command prompt window.

# Managing SSL certificates

To improve the security of remote operations between the SVP and the storage system, you can set up a Secure Sockets Layer (SSL) encrypted connection between them.

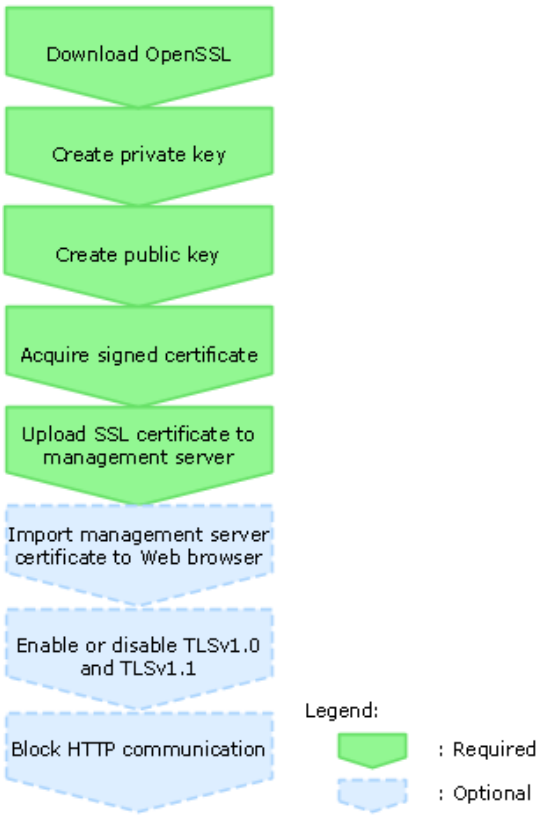
SSL certificates (also known as digital certificates) are used to establish a secure encrypted connection between an SVP and a storage system. The SSL connection protects the Hitachi Device Manager - Storage Navigator User ID and password that is exchanged during each visit (or session).

SSL certificates consist of small data files that digitally bind a cryptographic key to an SVP's log on credentials. When installed on the SVP, SSL activates the padlock and the HTTPS protocol, allowing secure connections between the SVP and the storage system.

## Flow of SSL communication settings

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. Download one from the OpenSSL website (http://www.openssl.org/).




## Creating a keypair

To enable SSL, you must create a keypair consisting of a public and a private key. The instructions use Windows 7 as an example.

### *Creating a private key*

A private key is required to create an SSL keypair. The following procedure for Windows 7 creates a private key file called `server.key` in the `c:\key` folder.

#### Before you begin

Download `openssl.exe` from the OpenSSL website.

### Procedure

1. If the read-only attribute is set, release it from the `c:\openssl` folder.
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:

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

## *Creating a public key*

A public key has the file extension `.csr`. It is required to create an SSL keypair. The following procedure is for the Windows 7 operating system.

### Before you begin

Download `openssl.exe` from the OpenSSL website.

### Procedure

1. Open a command prompt with administrator permissions.
2. Move the current directory to the folder to which the key file is output (such as `c:\key`). Execute the following command:

   ```
   c:\key > c:\openssl req -sha256 -new -key server.key -config c:
   \openssl\bin\openssl.cfg -out server.csr
   ```
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 web server (SVP). 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 of the SVP.
   - 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 149).
- 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 149).

**Note:**

When you send a request to a certificate authority, specify the SVP 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:

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

**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.

## Verifying and releasing an SSL certificate passphrase

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

### Before you begin

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

### Procedure

1. Open a command prompt window with administrator permissions.
2. Move the current directory to the folder (for example, `C:\key`) where the key file is stored, and run the following command:

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

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

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

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

**Example (when passphrase is set)**

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

```
Enter pass phrase for server.key: "Enter passphrase"
```

```
Writing RSA key
```

**Example (when passphrase is not set)**

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

```
Writing RSA key
```

## Converting SSL certificates to PKCS#12 format

Follow these instructions when converting SSL certificates to PKCS#12 format.

If you are uploading a created private key and the SSL certificate, you need to convert it to PKCS#12 format. If you are not uploading 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.

### Procedure

1. Open a command prompt with administrator permissions.
2. Enter the following command: `C:key>c:\openssl\bin\openssl pkcs12 -export -in client.crt –inkey client.key -out client.p12`
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.

## 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 SVP.

### Before you begin

- You must have the Storage Administrator (Initial Configuration) role to perform this task.
- You must be logged into the SVP.
- 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 Device Manager - Storage Navigator sessions on the SVP.
2. Open a command prompt window with administrator permissions.

3. In the folder where the .bat file is located, execute the following command:
   `C:\MAPP\wk\Supervisor\MappIniSet>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. A completion message box displays. Press any key to acknowledge the message and close the message box.
5. Close the command prompt window.

## Notes on updating a signed certificate for the service processor

The following notes provide additional information about updating a signed certificate.

- While the service processor 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 two minutes.
- If the service processor certificate is updated while Hitachi Command Suite is being set up, the setup operation will fail.
- Updating the SSL certificate might change the system drastically and may lead to service processor failure. Therefore take sufficient care to consider the content of the certificate and private key to be set.
- After the certificate update is complete, depending on the environment, the service processor can take 30 to 60 minutes to restart.

## Returning the certificate to default

You can return the certificate that was updated by the procedure in Updating a signed certificate (on page 151) 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 SVP.
- A private key (.key file) has been created. Make sure that the file name is `server.key`. See Creating a private key (on page 147).
- 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 (on page 148).
- 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 149).

- The passphrase for the private key (server.key file) must be released.

### Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Open a command prompt window with administrator permissions.
3. In the folder where the .bat file is located, execute the following command:
   ```
   C:\MAPP\wk\Supervisor\MappIniSet>MappApacheCrtInit.bat
   ```
4. A completion message box displays. Press any key to acknowledge the message and close the message box.
5. Close the command prompt window.

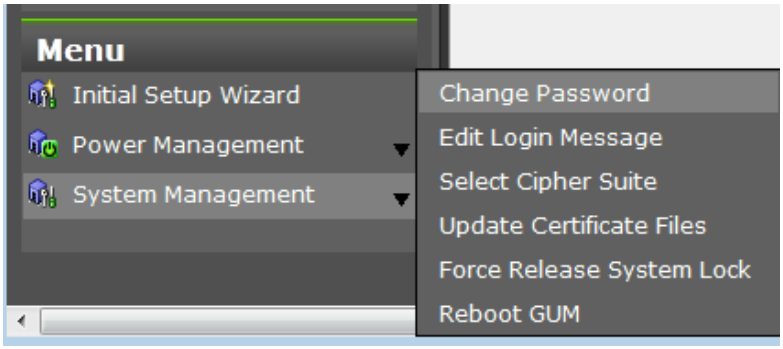
## Selecting a cipher suite

### 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**.

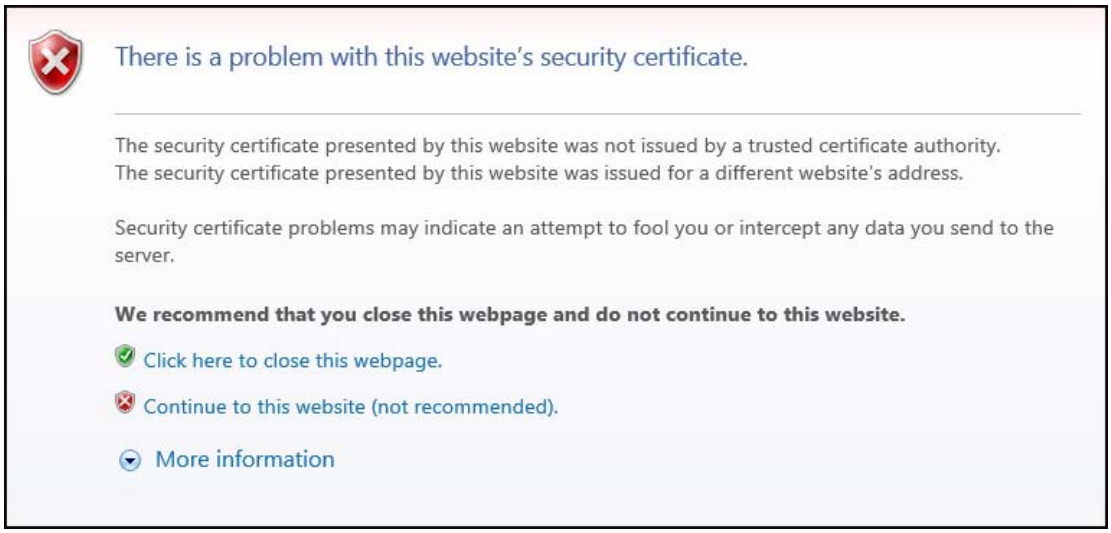



2. Click **Select Cipher Suite**.
3. Select the type of communication to use between the SVP and the storage system. The selections change the encryption level. Higher encryption provides better security but the communication speed is slower.
   - TLS_RSA_WITH_AES_128_CBC_SHA (Prioritize Transmission 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.
4. Click **Apply** to save the setting and close the dialog box.

## Problems with website security certificates

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

If the security certificate is not issued by a trusted certificate authority, the browser displays a warning message when it connects to an SSL-enabled Device Manager - Storage Navigator.




## Updating the certificate files

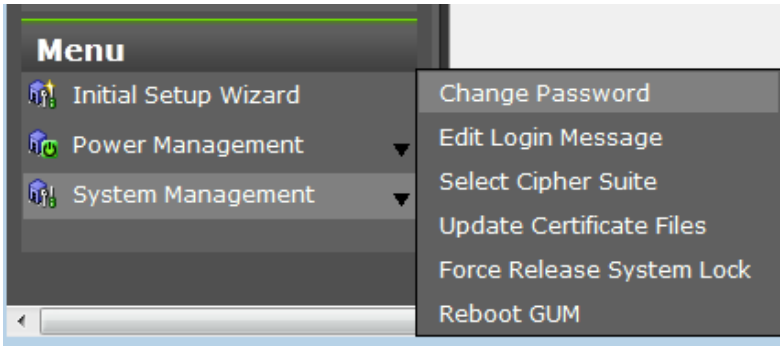
The **Update Certificate Files** window is used to update the certificates that are used for communication between the SVP and the storage system.

### Before you begin

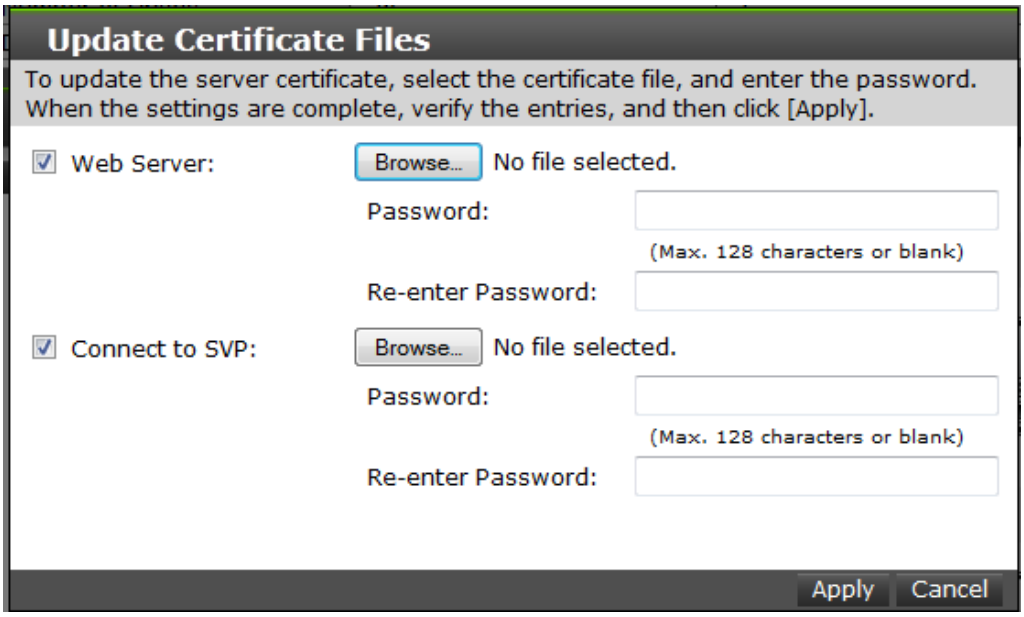
- You must have the Storage Administrator (View & Modify) role to complete this procedure.

### Procedure

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




2. Click **Update Certificate Files**.
3. Select a Web Server certificate file to update. Click 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. In the Web Server **Password:** field, enter the certificate password.
6. Enter the password again in the Web Server **Re-enter Password:** field.
7. Select a Connect to SVP certificate file to update. Click the **Connect to SVP** checkbox, then click **Browse**.
8. Browse to the certificate file and click **Open**. The **File Upload** window closes and returns you to the **Update Certificate Files** dialog box.
9. In the Connect to SVP **Password:** field, enter the certificate password.
10. Enter the password again in the Connect to SVP **Re-enter Password:** field.
11. Click **Apply** to update the certificates.

## 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.

### Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Open a command prompt window with administrator permissions.
3. In the folder where the HTTP setting tool is located, execute the following command:

   ```
   C:\MAPP\wk\Supervisor\MappIniSet>MappHttpRelease.bat
   ```
4. A completion message box displays. Press any key to acknowledge the message and close the message box.

5. Close the command prompt window.

## Disabling TLSv1.0 and TLSv1.1 communications

To enhance security, you can disable TLSv1.0 and TLSv1.1 communications and use only TLSv1.2.

This setting is optional.

### Before you begin

You must be logged into the SVP.

### Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Open a command prompt window with administrator permissions.
3. In the folder where the tool is located, execute the following command: `C:\MAPP\wk\Supervisor\MappIniSet> tlsoff.bat`.
   A completion message box appears.
4. Press any key to acknowledge the message and close the message box.
5. Close the command prompt window.
6. Restart the SVP.

## Enabling TLSv1.0 and TLSv1.1 communications

You can enable the disabled TLSv1.0 and TLSv1.1 communications.

This setting is optional.

### Before you begin

You must be logged into the SVP.

### Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Open a command prompt window with administrator permissions.
3. In the folder where the tool is located, execute the following command: `C:\MAPP\wk\Supervisor\MappIniSet> tlson.bat`.
   A completion message box appears.
4. Press any key to acknowledge the message and close the message box.
5. Close the command prompt window.
6. Restart the SVP.

## Blocking HTTP communication to the SVP

If the web server supports SSL (HTTPS), you can use the HTTP setting tool to block or allow access 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.

### Procedure

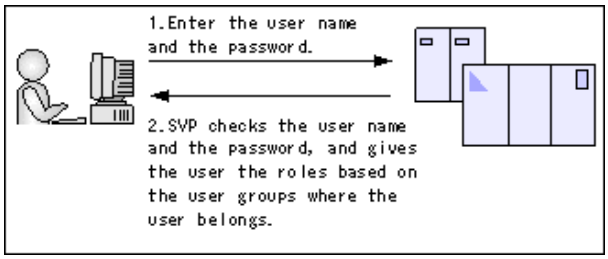
1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Open a command prompt window with administrator permissions.
3. In the folder where the HTTP setting tool is located, execute the following command:

   ```
   C:\MAPP\wk\Supervisor\MappIniSet>MappHttpBlock.bat
   ```
4. A completion message box displays. Press any key to acknowledge the message and close the message box.
5. Close the command prompt window.

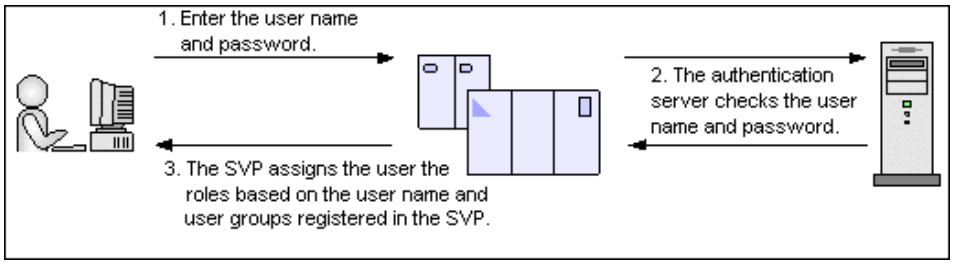
# Setting up authentication and authorization

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

The following figure shows the login workflow without an authentication server:

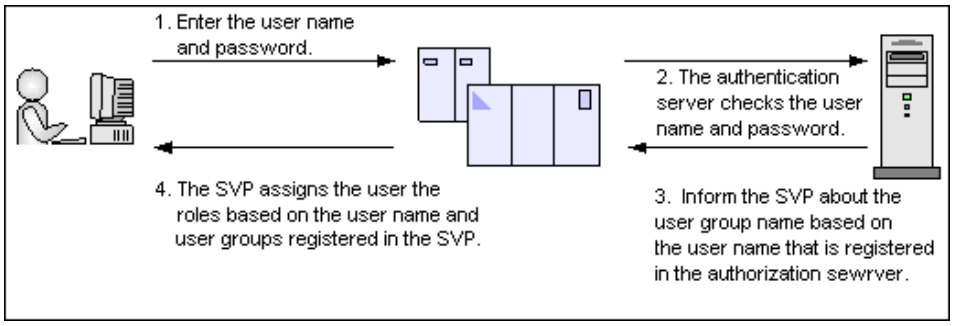



The following figure shows the login workflow with an authentication server:




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

The following figure shows the login workflow when an authentication server and an authorization server are used in combination:




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

## Authentication server protocols

Authentication servers support the following protocols:

- LDAPv3 simple bind authentication
- RFC 2865-compliant RADIUS with PAP and CHAP authentication
- Kerberos v5

The following certificate file formats are available for LDAP server settings:

- X509 DER format
- X509 PEM format

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

## Authorization server requirements

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

**Prerequisite OS**

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

- Windows Server 2012 R2

**Prerequisite software**

- Active Directory

**Authentication protocol for user for searching**

- LDAP v3 simple bind

**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.

## 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. In the folder where the .bat file is located, execute the following command specifying the configuration file path and the certificate file path:

   ```
   C:\MAPP\wk\Supervisor\MappIniSet>MappSetExAuthConf "C:\auth
   \auth.properties" "C:\auth\auth.cer"
   ```

5. 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.

   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.

## Naming a user group in Device Manager - Storage Navigator

When you create a user group in Device Manager - Storage Navigator, you name the group with the user's `memberOf` attribute value which is found in the Active Directory. Device Manager - Storage Navigator supports Active Directory nested groups.

After entering the user group name, verify that the user group name that you entered is registered in the authorization server.

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

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

# SMU user authentication

When an SMU user administrator attempts to log in, the user ID/password combination is sent to the SMU for authentication. For the SMU, authentication means testing the user ID and password pair, to see if the supplied password matches the stored password for the supplied user ID. Depending on the SMU configuration and the supplied user ID, the SMU may authenticate the user itself (locally), it may authenticate the user through a

RADIUS server, or it may authenticate the user through Active Directory. After authorization, the SMU allows the user to perform actions allowed by the user's profile.

*Active Directory* users are assigned full access rights to the SMU functionality.

For *local and RADIUS* users the user profile details are specified when the user account is created.

The user profile:

- Indicates if the user is to be authenticated locally,or through a RADIUS server.
- Specifies the user's access (privilege) level, meaning it specifies if the user is a:
  - Global administrator.
  - Storage administrator.
  - Server administrator.
  - Server+Storage administrator.
- Specifies the servers the user is allowed to access.
- Specifies if the user has CLI access (for RADIUS and Local Users).

## Active Directory user authentication

Active Directory is an LDAP-compliant hierarchical database of objects. It is very popular in enterprise environments and is becoming a de facto standard for user authentication.

After Active Directory connection settings and groups have been configured for the SMU, it will allow logins from enabled users who supply their Active Directory name and password. This is typically the same name and password that the user would use to log into Windows and other enterprise applications. Unlike SMU local and RADIUS user names, Active Directory user names are case-insensitive. Active Directory passwords are case-sensitive and cannot be changed from the SMU; they are maintained in the Active Directory server.

There are a number of benefits for SMU users. The administrator does not need to maintain a separate set of user details, because the SMU can just make use of the Active Directory enterprise user database. Users can login using their usual name and password instead of having to remember a separate set of credentials for the SMU. And instead of configuring access for individual users, the SMU administrator just has to specify the Active Directory *groups* whose members have login rights.

It is possible to assign more restrictive user levels and managed severs to Active Directory users according to their group membership. So it is possible to define a group of users who have only *server* level access, for example, or access to a restricted set of managed HNAS servers.

Although the SMU supports RADIUS and Active Directory for external authentication, they are mutually exclusive; it is not possible to have them both configured for external authentication at the same time.

When a login attempt is made, the SMU first tries to authenticate the credentials as a local user. If that fails, and Active Directory is configured, they are authenticated as an Active Directory user.

Active Directory authentication requests are sent to servers in the configured sequential order. If a successful connection cannot be made to the first server, it attempts to contact the second server and so on. When a connection is made and an authentication

response received (either positive or negative) it is treated as definitive. It does not then contact further servers because all servers are assumed to have identical content.

## Using Transport Layer Security (TLS) with Active Directory authentication

TLS is a cryptographic protocol which provides security between applications over a network.

For Active Directory authentication, the SMU supports up to TLS 1.2. It negotiates with the domain controller to use the highest version of TLS which is common to both.

For TLS, the SMU requires domain controllers to respond on port 389.

## Configuring Active Directory servers

Global Administrators can provide information to configure, modify, and list Active Directory servers for authentication on the **Active Directory Servers** page.

### Before you begin

In order to enable Active Directory, the SMU administrator needs to know the following information:

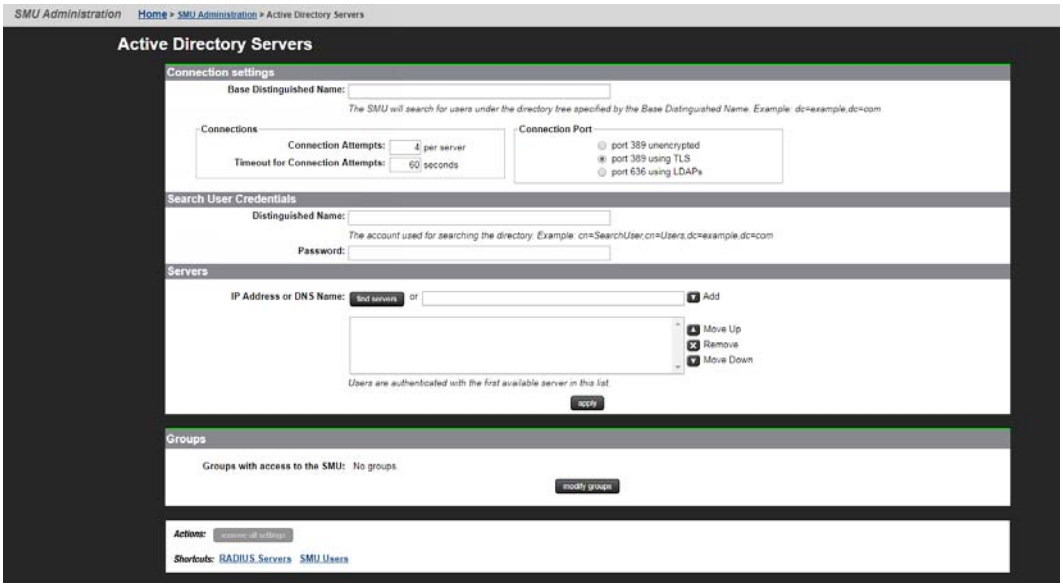
- The name of the domain from which the Active Directory users and groups will access the SMU.
- The LDAP distinguished name and password of an Active Directory user that has read access to users and groups on the Active Directory servers. This is referred to as the Search User. The user can search for users or groups under the supplied base distinguished name.
- The addresses of one or more Active Directory servers that maintain the users and groups for the domain. The content of all configured servers must be identical. If DNS servers have been configured for the SMU, then the SMU should be able to automatically discover these server addresses via the **find servers** button on the setup page. SRV records must be setup in order for **find servers** to find the Active Directory servers.
- The Active Directory group or groups whose members are to be given the right to log into the SMU.
- If RADIUS was previously in use and it is to be replaced by Active Directory, then the RADIUS configuration must first be removed before Active Directory can be configured. This is done from the **Home>SMU Administrator>RADIUS Servers** page by clicking the **remove all settings** button. No RADIUS user will be able to log into the SMU after this is done.

**Note:** On the NAS system, local users and Active Directory groups can be created with read-only access. A read-only user has permission to view most pages of the NAS Manager; however, they are not generally allowed to perform any actions on the NAS Manager that would create a system or configuration change.

## Procedure

1. Navigate to **Home** > **SMU Administrator** to display the **Active Directory Servers** page.
2. Enter the **Base Distinguished Name**.

   This name must be entered in LDAP distinguished name (DN) format which consists of a sequence of "attribute=value" pairs separated by comma or semi-colon. The Base Distinguished Name should contain the domain component (dc) attributes for the organization's domain. So for the domain *example.com* it would be "*dc=example, dc=com*". The name may also contain organization unit (ou) attributes.




The following table describes the fields on this page:

| Field/Item | Description |
|---|---|
| **Connection settings** | |
| Base Distinguished Name | The LDAP root location for users and groups. The name should only contain the domain components. |
| **Connections** | |
| Connection Attempts | The maximum number of times that the SMU attempts to connect to each Active Directory server when a connection fails. |
| Timeout for Connection Attempts | The maximum time in seconds that the SMU waits when connecting to an Active Directory server before failing with a time out. |

| Field/Item | Description |
|---|---|
| **Connection port** | The port and encryption method to use when connecting to an Active Directory server.<br>Options are:<br>▪ port 389 unencrypted<br>▪ port 389 encrypted using TLS (SSL/TLS connections)<br>▪ port 636 encrypted using LDAPs (SSL) |
| **Search User Credentials** | |
| Distinguished Name | The LDAP distinguished name for a user that has search capabilities. |
| Password | The password for the search user. |
| **Servers** | |
| IP Address or DNS Name | The address of one or more Active Directory servers for the domain. Each server should hold identical content. The maximum number of servers is 20. |
| **find servers** | Queries DNS to show the list of available Active Directory servers for the domain. The NAS Manager lists the Active Directory servers in order of their response time (quickest first). If you add them in the same order, the SMU attempts to authenticate users against the fastest responding servers first. |
| **Add** | Add an Active Directory server after you have entered its fully qualified domain name or IP address. |
| **Move Up**<br>**Move Down** | If there is more than one server, use these buttons to prioritize the list. |
| **Remove** | Remove a server from the list. |
| **apply** | Submit the page and save the connection settings and server list to the SMU database. |
| **Groups** | |
| Groups with access to the SMU | Shows groups with access to the SMU. Active Directory users who belong to these groups can access the SMU. |
| **Modify groups** | Click to go to the **Active Directory Groups** page, where you can add groups. |
| **Actions** | |

| Field/Item | Description |
|---|---|
| **remove all settings** | Removes all Active Directory server settings, including server list, connection settings, search user credentials and groups. After this action, Active Directory users can no longer log into the SMU. |

3. Configure the following settings for the connections as required:
   - **Connection Attempts** - The maximum number of times that the SMU attempts to connect to each Active Directory server when a connection fails. The default value is four attempts.
   - **Timeout for Connection Attempts** - The maximum time in seconds that the SMU waits when connecting to an Active Directory server before failing with a timeout. The default value is 60 seconds.
   - **Connection Port** - The port and encryption method to use when connecting to an Active Directory server. The options are: 'port 389 unencrypted', 'port 389 encrypted using TLS (SSL/TLS connections)' and 'port 636 encrypted using LDAPs (SSL)'. The default value is 'port 389 encrypted using TLS (SSL/TLS connections)'.
4. Enter the **Distinguished Name**.

   This is the Distinguished Name of the Search User, an existing user that has permission to access Active Directory. An Search User DN would typically contain common name (cn) and possibly organization unit (ou) attributes as well as the domain components. The domain components should match those used in the Base Distinguished Name. An example Search User DN is "*cn= ldapguest, cn=users, dc=example, dc=com".*
5. Enter the **Password** of the Search User (an existing user that may access the directory).
6. There are two ways to add Active Directory servers.
   - Enter the fully qualified domain name or IP address of the server, and click **Add**.
   - Click **find servers**. The NAS Manager lists the Active Directory servers in order of their response time (quickest first). If you add them in the same order, the SMU attempts to authenticate users against the fastest responding servers first.

     **Note:** The DNS server or servers must be configured for the SMU (under Name Services) for **find servers** to work.

     - Select one or more servers and click **add** to add them to the list. No more than 20 Active Directory servers can be configured at a time.
     - When you are finished, click **close** to return to the **Active Directory Servers** window.


7. If there is more than one server, the list can be prioritized using **Move Up** or **Move Down** .
8. Click **Apply** to submit this page and save the connection settings and server list to the SMU database.
   The SMU will perform a connection test to check that it can access the configured servers with the supplied details and display a warning if the SMU cannot, giving the user the opportunity to modify the settings or to save them as they are.

   Any information, warnings and errors related to Active Directory configuration or authentication are logged to `/var/opt/smu/log/mgr/mgr.log` and `/var/opt/smu/log/mgr/security.log`

## Configuring Active Directory groups

Before Active Directory users can log into the SMU, you must configure one or more Active Directory groups. After a group has been added and saved, members of that group can log into the SMU using their Active Directory name and password. Active Directory users belonging to the subgroups of the configured group also have SMU access.

### Before you begin

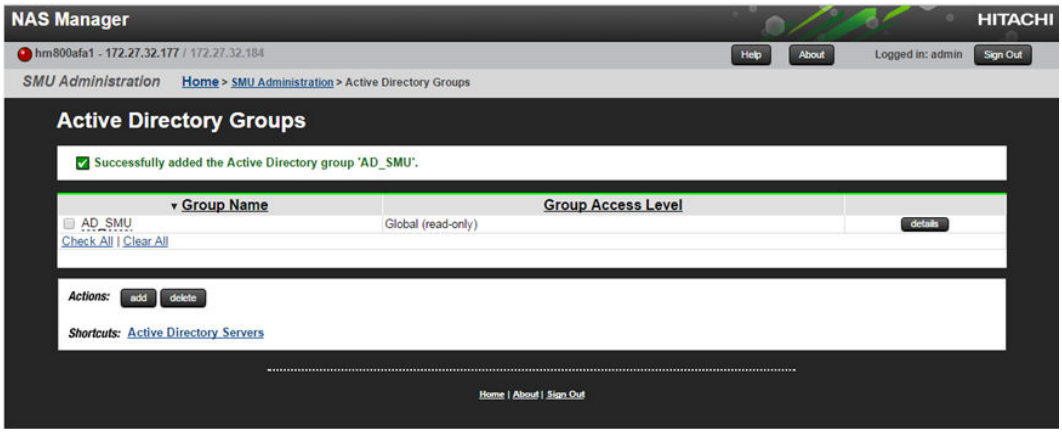
Note that the administrator is only able to configure groups after Active Directory servers have been added on the **Active Directory Servers** page.

### Procedure

1. Navigate to the **Home** > **SMU Administrator** > **Active Directory Groups** to display the **Active Directory Groups** page.

   This page shows all Active Directory groups that have been added. Note that Active Directory groups can be associated with a group access level. For example, it is possible to define a group of users who only have server level of access. Any groups that were added in a previous version of the SMU that has been upgraded will be displayed in this list with a User Level of Global Administrator.

   If an Active Directory user is member of more than one configured groups in the SMU, then their access level will be derived by combining the access level for all configured Active Directory groups. For example, if a user is a member of one group defined with storage level, but is also a member of a group with server level, then that user will have server+storage access to the SMU.

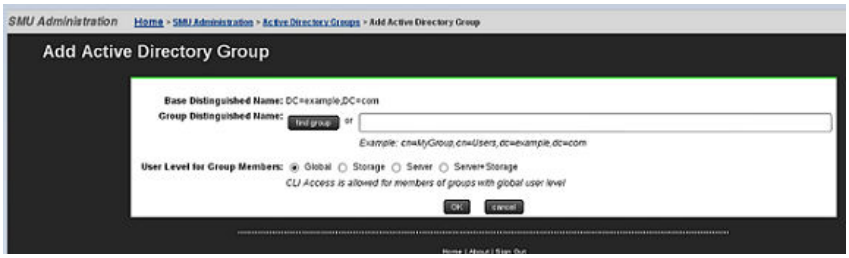



The following table describes the fields on this page:

| Field/Item | Description |
|---|---|
| **Group Name** | Group name is the user-friendly name of an Active Directory group existing on the Active Directory server.<br>The full distinguished name for a group can be viewed by hovering the mouse over the group name. The sort order of the table can be changed by clicking over a column heading. |
| **Group Access Level** | Shows the group access level. This defines the access level given to Active Directory users who are members of the group when they log onto the SMU. On an external or virtual SMU, if the Group Access Level is **Global**, then group members are given SMU CLI access. SMU CLI access is not available on an embedded SMU or a NAS module SMU.<br>This column also displays those Active Directory groups assigned the read-only attribute. A read-only group has permission to view most pages of the NAS Manager, but they are not allowed to perform any actions that would trigger a system or configuration change.<br>**Note:** Read-only users can not access the CLI, and a user with CLI access may not be read-only. If either of these options is checked, the other one is disabled. |
| **details** | Click the **details** button in the right-hand column to view details of the associated group. |
| **Check All** | Checks all boxes under **Group Name**. |
| **Clear All** | Clears all checked boxes under **Group Name**. |

| Field/Item | Description |
|---|---|
| **add** | Click to add a group. Takes you to the **Add Active Directory Group** page. |
| **delete** | Existing groups can be deleted by checking the box in left-hand column and clicking the **delete** button. The user is asked for confirmation before deleting. If all groups are being deleted, the user is warned that no Active Directory users will be authenticated. |
| **Active Directory Servers** | Takes you to the **Active Directory Servers** page. |

2. Click **add** and use the **Add Active Directory Group** page to add groups.

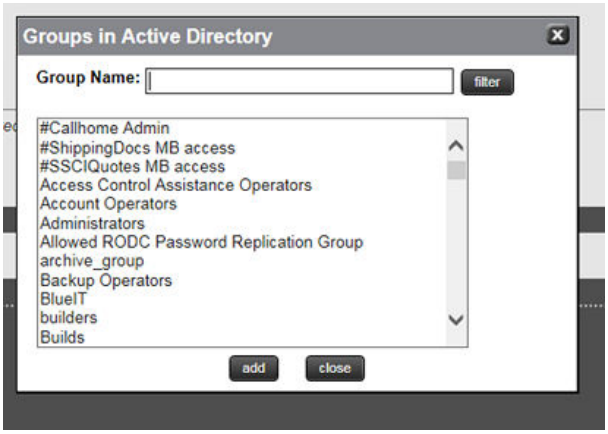



The following table describes the fields on this page:

| Field/Item | Description |
|---|---|
| Base Distinguished Name | The LDAP root location for users and groups. The name is recommended to contain just the domain components. |
| Group Distinguished Name | The LDAP root location for users and groups. The name is recommended to contain just the domain components. Groups can be added manually by entering their distinguished name and then pressing the **OK** button. A maximum of 100 groups can be added. Alternatively, groups can be added by using the **find group** button. |
| **find group** | Queries the Active Directory to show the list of available groups. The list can be filtered by entering a partial group name. A maximum of 1000 group names is displayed. |
| User Level for Group Members | The user levels that can be assigned to group members are the same as those that can be assigned to local or RADIUS users and have the same meanings. The default is **Global**, but the level can be modified by selecting one of the other radio buttons. |

| Field/Item | Description |
|---|---|
| Read-Only Access | Defines the group users as read-only. Members of the group may log into the SMU, but with read-only access. Read-only users may be given Global, Server, Storage or Server+Storage access. Based on the defined roles in the group, read-only users may not perform specific tasks, such as creating, or modifying a files and data. Users in a read-only group have permission to view most pages of the NAS Manager; however, they are not allowed to perform any actions that would trigger a system or configuration change. The Active Directory Group Details page will not allow the read-only attribute to be modified. The group would need to be deleted and re-added to change this attribute.<br><br>**Note:** Users in a group with the read-only attribute can not access the CLI, and a user with CLI access may not be read-only. For complete details on read-only access, please see the section, *Read-only users*, in the *NAS Storage System User Administration Guide*. |
| **OK** | Click to save the group details. The SMU checks that the group exists in Active Directory. If the group does not exist (or if the SMU failed to access any AD server) the user is asked for confirmation that they still wish to save it. After saving the group, the updated group list page is displayed. |
| **cancel** | Cancels input. |

3. There are two ways to add groups:
   - Enter the full Distinguished Name for the group (for example "*CN=Mygroup, CN=users, DC=example, DC=com*") and click the **add** button.
   - Click the **find group** button.
     - Groups that exist under this Base DN are displayed in a dialog window. The list can be filtered by entering a partial group name. A maximum of 1000 group names is displayed. Select a group from the list. Only one group can be added at a time.
     - Click **add** to add the group's distinguished name to this page.
     - Click **close** to return to the **Active Directory Groups** page without selecting a group from the list.




4. Select a User Level to be assigned to members of the group.

   CLI access is given to members of all groups defined with the **Global** level.

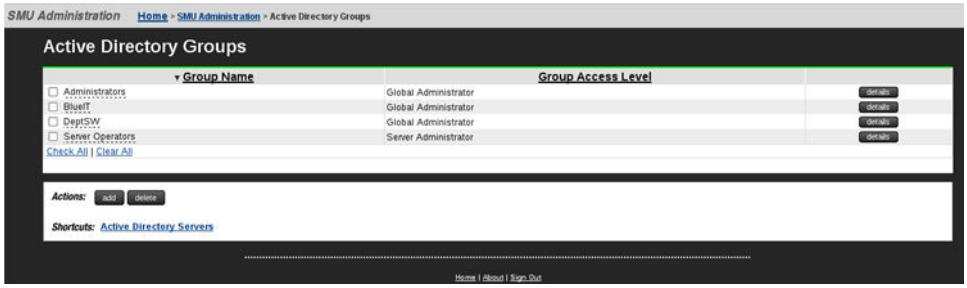
   Active directory users are given the same access level to all managed HNAS servers.

5. Click **OK** to save the group.

   The SMU will perform a test to check the group exists in Active Directory and displays warning if it is not, giving the user the opportunity to modify the group.

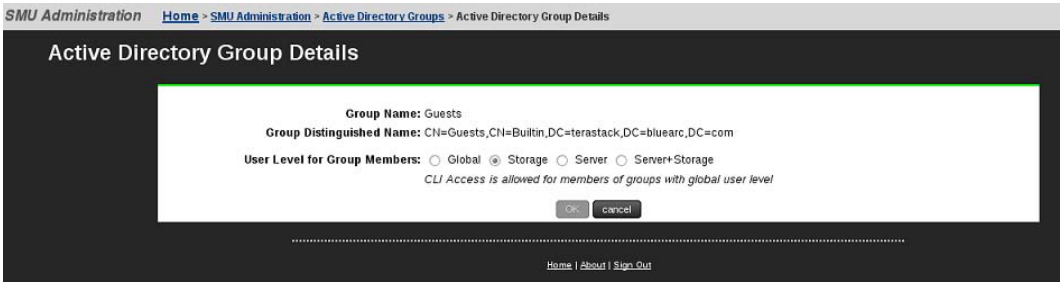
   Any information, warnings and errors related to Active Directory configuration or authentication are logged to `/var/opt/smu/log/mgr/mgr.log` and `/var/opt/smu/log/mgr/security.log`

   On returning to **Active Directory Groups** page, the current list of configured groups is displayed.




6. Click the **details** button in the right-hand column to view details of a previously defined group.

   When displaying the group details, the SMU checks that the group exists in Active Directory and displays a warning if it does not exist or if it could not access an Active Directory server. The user level cannot be modified once the group has been added. In order to modify the user level, the group would have to be deleted, then added again. Click the **cancel** button to return to the **Active Directory Groups** page.



The following table describes the fields on this page:

| Field/Item | Description |
|---|---|
| Group Name | Name of group that details are provided for. |
| Group Distinguished Name | The LDAP root location for users and groups. The name is recommended to contain just the domain components. |
| User Level for Group Members | The user levels that can be assigned to group members are the same as those that can be assigned to local or RADIUS users and have the same meanings. The default is **Global** , but the level can be modified by selecting one of the other radio buttons. |
| **OK** | No details can be modified for a group, so the **OK** button is disabled. |
| **cancel** | Returns to the **Active Directory Groups** page. |

## User authentication through RADIUS servers (HNAS server only)

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting management for computers to connect and use a network service.

RADIUS is a client/server protocol that runs in the application layer, using UDP as transport. The SMU acts as a RADIUS client component that communicates with the RADIUS server to validate logins. The RADIUS server is usually a background process running on a Unix or Microsoft Windows server.

RADIUS serves three functions:

- Authenticates users or devices before granting them access to a network.
- Authorizes those users or devices for certain network services.
- Accounts for usage of those services.

The RADIUS server compatibility is as follows:

- For IPv4 only, works with FreeRADIUS 2.1 or Windows 2003 Internet Authentication Service (IAS).
- For IPv6, requires FreeRADIUS 2.2 or Windows 2008 Network Policy Server (NPS).

Configuring user authentication through a RADIUS server requires the following:

- The RADIUS server must be set up and operational.
- The SMU must be able to communicate with the RADIUS server using the network.
- You must know the RADIUS server's:
  - IP address or DNS name.
  - Authentication port.
  - Shared secret for the SMU.

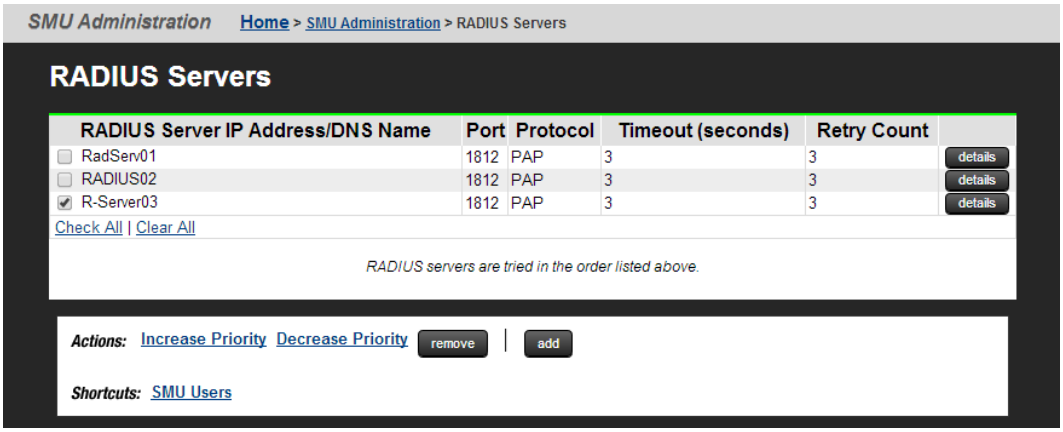
You can specify and prioritize multiple RADIUS servers for authentication.

**Note:** The SMU contacts RADIUS servers in order of priority; the SMU will always try to contact higher priority servers before lower priority servers, and you cannot map SMU users to authenticate through a specific RADIUS server. If you specify an incorrect secret or there are network problems that prevent the SMU from communicating with the highest priority RADIUS server, the SMU will try to contact the secondary RADIUS server, then the third RADIUS server, then the next server, until the SMU has tried to contact all the RADIUS servers in the list.

## Displaying list of RADIUS servers

### Procedure

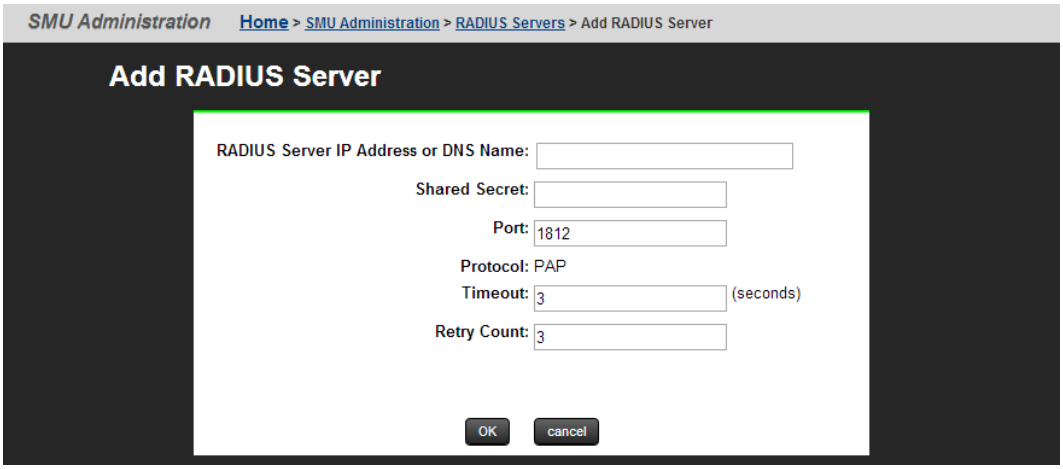
1. Navigate to **Home** > **SMU Administration** > **RADIUS Servers**.




## Adding a RADIUS server

### Procedure

1. Navigate to **Home** > **SMU Administration** > **RADIUS Servers** to display the **RADIUS Servers** page.
2. Click **add** to display the **Add RADIUS Server** page.



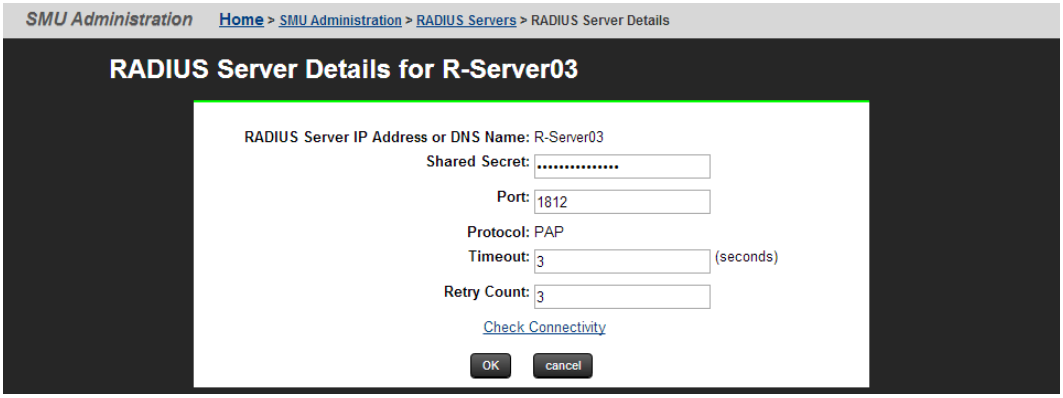
| Field/Item | Description |
|---|---|
| RADIUS server IP address or DNS name | To connect with the RADIUS server, specify an IPv4 or IPv6 address, or a host name (host name is not recommended). An IP address is preferred, both because it eliminates the dependency on the network DNS sever(s), and to improve login performance.<br><br>The **SMU Network Configuration** page (navigate to **Home** > **SMU Administration** > **SMU Network Configuration**) shows the active IP addresses. It is recommended that IPv4 on eth0 and the current IPv6 addresses be added to the "allowed client" list on each RADIUS server. For more information on setting up the SMU Network Configuration for IPv6, see the *Network Administration Guide*. |
| Shared Secret | Specify the shared secret.<br><br>Some RADIUS Servers limit the length of the shared secret and require that it be comprised only of characters that can be typed on a keyboard which uses only 94 out of 256 possible ASCII characters.<br><br>If the shared secret must be a sequence of keyboard characters, choose shared secrets that are at least 22 characters long and consisting of a random sequence of upper and lower case letters, numbers, and punctuation.<br><br>▪ To ensure a random shared secret, use a computer program to generate a random sequence at least 22 characters long. Windows 2008 Server allows you to generate a shared secret when adding the RADIUS client.<br>▪ The SMU will support a shared secret from 1 up to 128 characters.<br>▪ Use a different shared secret for each RADIUS server-RADIUS client pair. |
| Port | Specify the RADIUS server authentication port. The default RADIUS server authentication port is 1812, but you should check with the RADIUS server administrator to make sure that 1812 is the correct port. |
| Protocol | The protocol for the RADIUS server. |
| Timeout | Specify the timeout, which is the number of seconds the SMU waits before retrying (retying is re-transmitting the authentication request to the same RADIUS server). The default is 3 seconds. If the timeout is reached and there is no response from the first RADIUS server in the list, the SMU attempts another retry. |

| Field/Item | Description |
|---|---|
| Retry Count | Specify the retry count. The default is 3. When the retry limit is reached, the SMU sends the request to the next RADIUS server in the list. When the retry limit for the second server is reached, the SMU attempts to reach the next server in the list, until there are no more servers to try. If there are no more servers to try, the user cannot be authenticated, and the login fails. |
| **OK** | When you are done making changes, click **OK** to test connectivity and save the configuration for this RADIUS server and return to the **RADIUS Servers** page. |
| **cancel** | Exits without saving the configuration. |

## Displaying details of RADIUS server

### Procedure

1. Navigate to **Home** > **SMU Administration** > **RADIUS Server** to display the **RADIUS Server** page.
2. Select a RADIUS server, and click **details** to display the **RADIUS Server Details** page.




| Field/Item | Description |
|---|---|
| RADIUS server IP address or DNS name | The RADIUS server IP address or DNS name. |
| Shared Secret | The shared secret, displayed with asterisks. |
| Port | The RADIUS server authentication port. |
| Protocol | Protocol associated with the RADIUS server. |

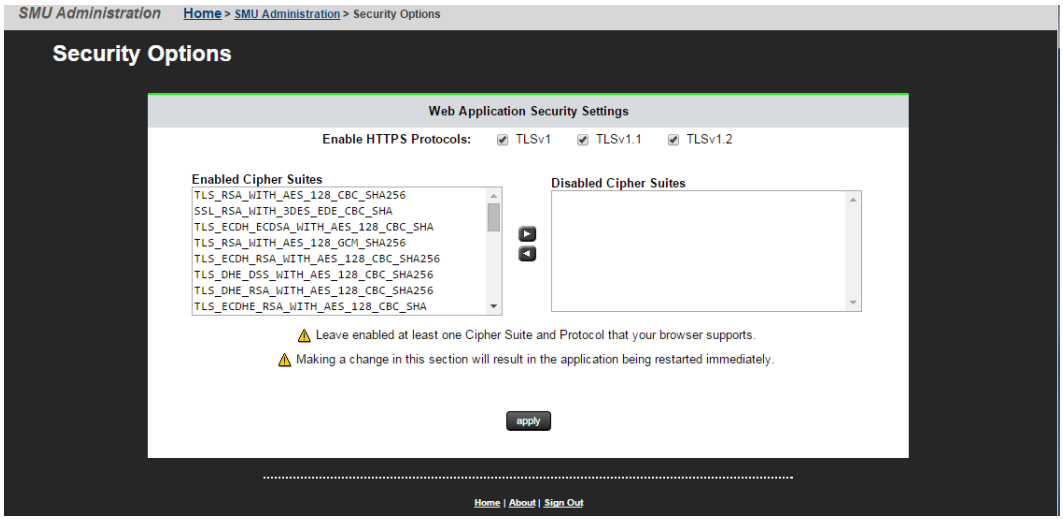
| Field/Item | Description |
|---|---|
| Timeout | The number of seconds the SMU waits before retrying (retrying is re-transmitting the authentication request to the same RADIUS server). If the timeout is reached and there is no response from the first RADIUS server in the list, the SMU attempts another retry. |
| Retry Count | When the retry limit is reached, the SMU sends the request to the next RADIUS server in the list. When the retry limit for the second server is reached, the SMU attempts to reach the next server in the list, until there are no more servers to try. If the timeout is reached, and there are no more servers to try, the user cannot be authenticated, and the login fails. |
| Check connectivity | Click to check the connectivity status of the RADIUS server. |

## Configuring SMU security (NAS module only)

This screen allows you to change web application security settings.

The SMU can be configured to control the hosts that can access the SMU and auxiliary devices managed by the SMU.

**Note:** If you have a standby SMU, it may take up to 5 minutes after a configuration change to be synchronized with the active SMU




### Procedure

1. Navigate to **Home** > **SMU Administration** > **Security Options**.

| Field/Item | Description |
|---|---|
| **Web Application Security Settings** | This section allows you to change web application security settings.<br>**Note:** Making any change in this section results in the application being restarted immediately. |
| Enable HTTPS Protocols | By default, all HTTPS protocols are enabled, and the boxes next to the protocols are checked. Uncheck the check box next to a protocol to change its state to disabled. Leave at least one protocol enabled that your browser supports. |
| Enabled Cipher Suites | By default, all cipher suites are enabled and are shown in the Enabled Cipher Suites list box. |
| Disabled Cipher Suites | To disable cipher suites, use the arrow to move selected cipher suites to the Disabled Cipher Suites list box. Leave at least one cipher suite enabled that your browser supports. |
| **apply** | Click **apply** to save your changes. |

2. Optionally, to disable cipher suites, use the arrow to move enabled cipher suites from the **Enabled Cipher Suites** list at the left to the **Disabled Cipher Suites** list at the right. It is necessary to have at least one cipher suite remain enabled.

   **Note:** Take care before disabling cipher suites, because not all cipher suites are supported by all browsers.

3. Optionally, to disable protocols, at **Enable HTTPS Protocols**, uncheck the check box next to a protocol to change its state to disabled. It is necessary to have at least one protocol remain enabled.

   **Note:** Take care before disabling HTTPS protocols, because not all HTTPS protocols are supported by all browsers.

4. Click **apply** to save the currently defined security options.

# Chapter 6: Alert notifications

Use alert notifications to monitor the storage system for changes in configuration or status.

## Viewing alert notifications

You can view alert email messages, alert Syslog messages, and alert SNMP trap messages in the Device Manager - Storage Navigator Alerts tab and the **Alert Detail** window.

### Before you begin

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

- 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 the SNMP Manager in Device Manager - Storage Navigator. See the *Hitachi SNMP Agent User Guide* for information about using SNMP traps.

## Configuring alert notifications

### Procedure

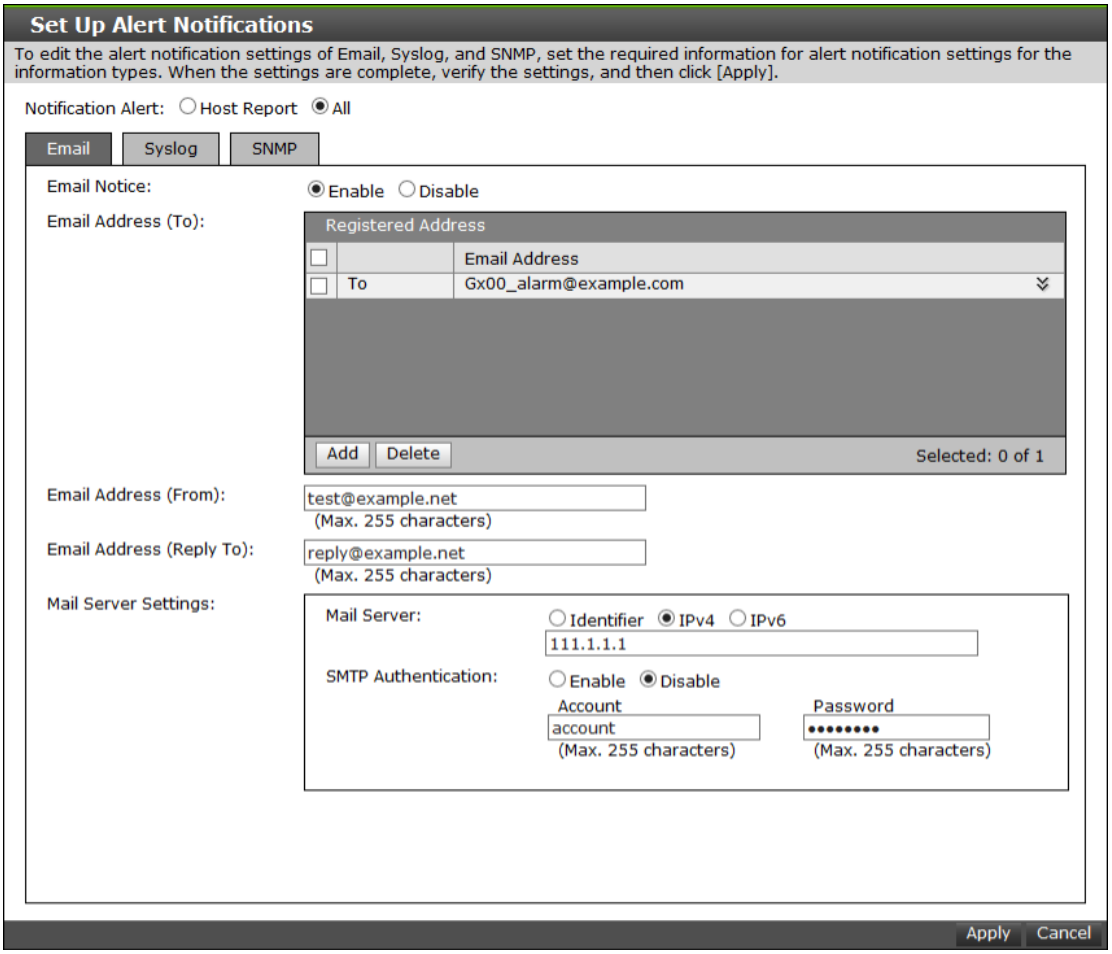
1. In the maintenance utility, click the **SNMP** tab to display it.
2. In **SNMP Agent**, click **Enable** to use the agent or **Disable** not to use it.
3. Select the **Email** tab. The **Email** window displays the current settings for the Mail Server, SMTP Authentication, an Email Address.
4. To send a test email message, click **Send Test Email**. A completion notice displays.
5. Click OK to acknowledge the notice and close the message.
6. Click the **Syslog** tab. The **Syslog** window displays the current settings for the Primary Server, IP address, and port number, and for the secondary server IP address and port number.
7. To send a test message to the Syslog server, click **Send Test message to the Syslog Server**. A completion notice displays.
8. Click **OK** to acknowledge the notice and close the message.

9. Click the **SNMP** tab. The **SNMP** window displays the current settings for the Storage System Name, Contact, Location, SNMP Trap and SNMP Manager.
10. To send a test SNMP trap, click **Send Test SNMP Trap**. A completion notice displays.
11. Click **OK** to acknowledge the notice and close the message.

## General settings

### Procedure

1. In the maintenance utility **Administration** pane, select **Alert Notifications**.
2. In the **Alert Notifications** window, click **Set Up**. The **Set Up Alert Notifications** window displays the **Email** tab by default.



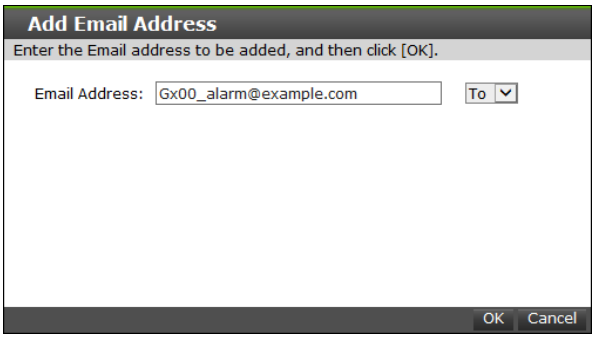

3. Select the type of report to send.
   - **Host Report**: Sends alerts only to the hosts for which a SIM report setting is made.
   - **All**: Sends alerts to all hosts.

   The alert notification destination is common to Syslog, SNMP, and email.

## Email settings

### Procedure

1. To send email notices, click **Enable**, next to **Email Notice**. Click **Disable** to not send email notices.
2. Click **Add** to add an email address to the list of registered addresses.

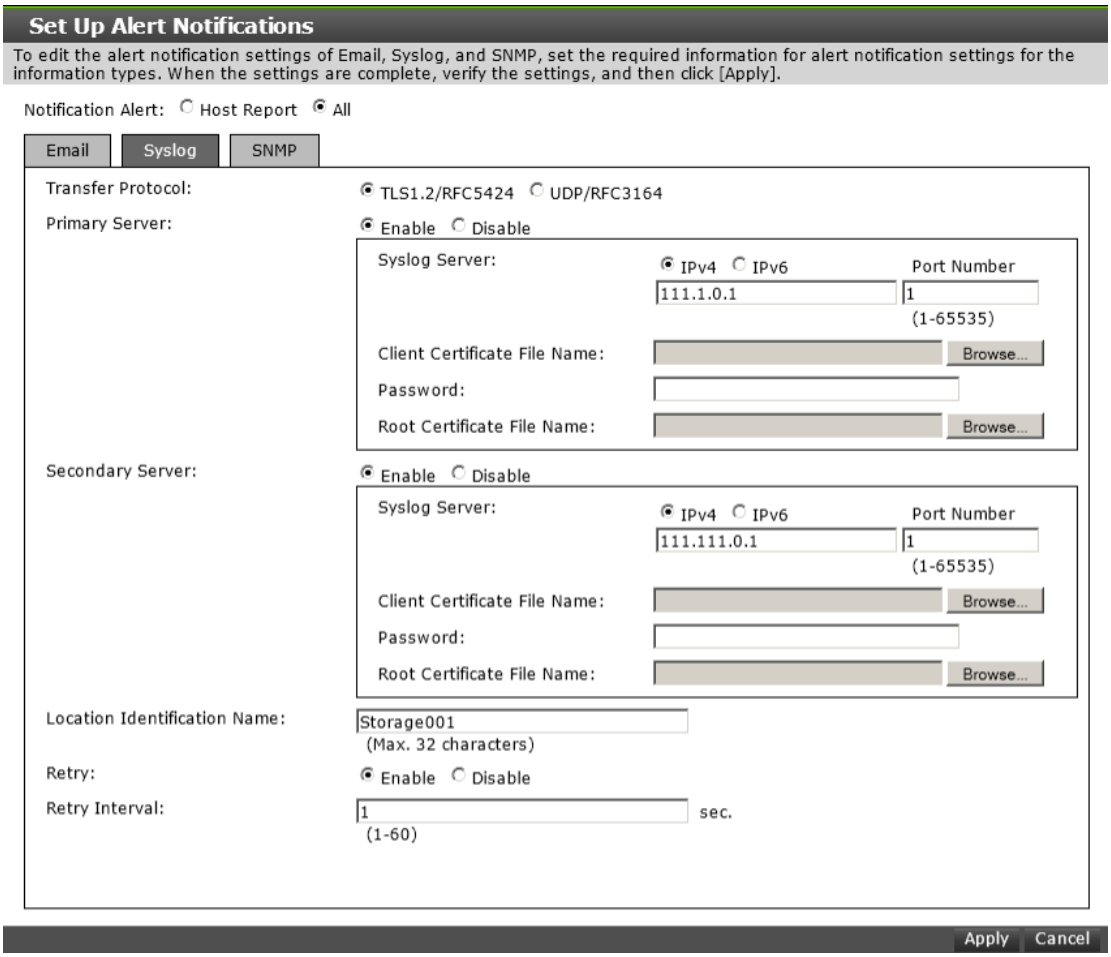



3. Enter the email address and then use the pull-down menu to select the type of address: **To**, **Cc**, or **Bcc.**
4. Click **OK** to save the email address and close the dialog box.
5. Enter an email address in **Email Address (From)**.
6. Enter an email address in **Email Address (Reply To:)**.
7. In **Mail Server Settings**, select the mail server type: **Identifier**, **IPv4**, or **IPv6.**
8. To use SMTP authentication, click **Enable**.
9. In **Account**, enter an SMTP account name.
10. In **Password**, enter the SMTP account password.
11. Click **Apply** to save the changes and close the **Set Up Alert Notifications** window.

## Syslog settings

### Procedure

1. Click the **Syslog** tab.



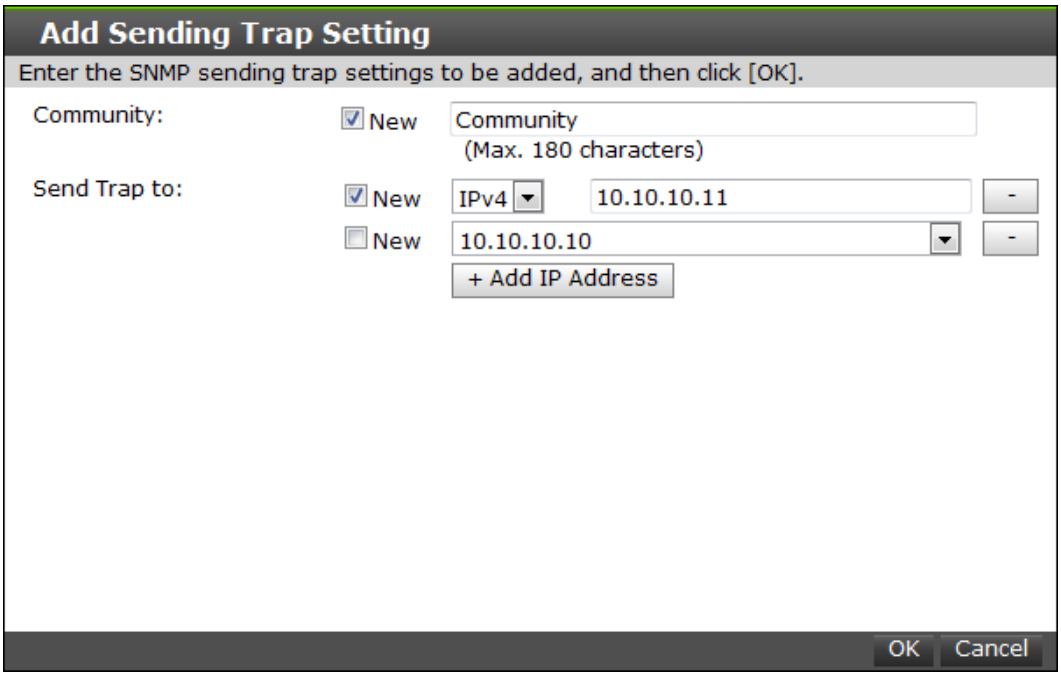

2. Select the type of transfer protocol to use.
3. In **Primary Server**:
   a. Click **Enable** to use the server or **Disable** not to use it.
   b. Select the type of IP address to use for the server: **IPv4** or **IPv6**.
   c. In **Client Certificate File Name**, click **Browse** to select a client 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.

## SNMP settings

### 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.

# Sending test messages

The lower section of the **Alert Notifications** window contains three tabs: Email, Syslog, and SNMP. Select the desired tab to send a test message of the type specified in the tab name.

## 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 displays.
3. Click **OK** to acknowledge the notice and close the message.

### Example of a test email message

```
Subject: VSP Gx00 Report
DATE : 24/10/2014
```

```
TIME : 10:09:30
Machine : Hitachi Virtual Storage Platform Gx00 (Serial# 64019)
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. |

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

## 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 displays.
3. Click **OK** to acknowledge the notice and close the message.

## 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.

# Using the Windows event log

Some failure information is output to the Windows event log.

# Monitoring failure information in 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 `83<model-name><serial-number>`, where <*model-name*> is one of the following:

     VSP G200: 2000

     VSP G400 or VSP F400, VSP G600 or VSP F600: 4000

     VSP G800 or VSP F800: 6000

     For example, for a VSP G600 that has the serial number 400102, the value is `834000400102`.

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.

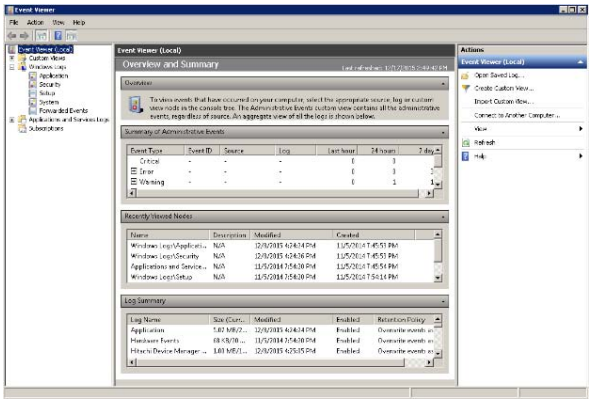
4. Close the command prompt.

## Viewing the Windows event log

You can view the Windows event log which is output to the SVP.

### Procedure

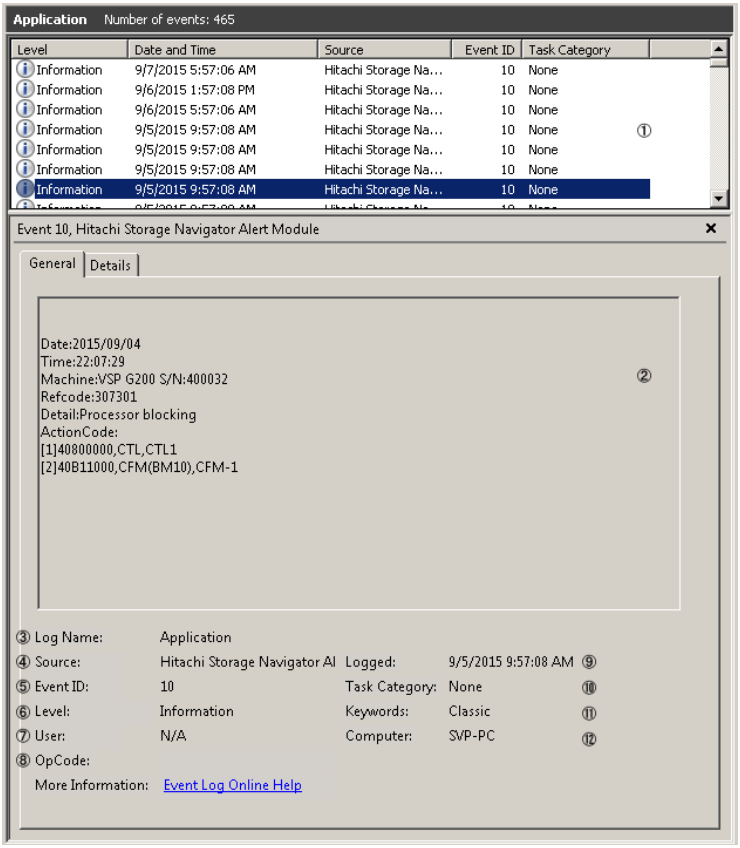
1. From the Windows start menu, click **Control Panel** > **System and Security** > **Administrative Tools** > **Event Viewer**.
2. Click **Windows Logs** > **Application** in the left pane.



## Output example of the failure information

The storage system delivers a report after you send failure information to the event log.

The storage system failure information will look 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<br>Date: Date of the event occurrence<br>Time: Time of the event occurrence<br>Machine: Model name and serial number of the storage system<br>Refcode: Reference code*<br>Detail: Detailed failure information*<br>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<br>This is always displayed as "Application" |

| # | Item | Description |
|---|---|---|
| 4 | Source | Displays the name of the application which issued the event<br>This is always displayed as "Hitachi Storage Navigator Alert Module" |
| 5 | Event ID | Displays the event ID<br>This is always displayed as "10" |
| 6 | Level | Displays the event alert level<br>▪ Error: Acute or Serious<br>▪ Warning: Moderate<br>▪ 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 SNMP failure trap reference code section in the *Hitachi SNMP Agent User Guide*. | | |

# Chapter 7: Managing license keys

This storage system includes base and optional software features for Hitachi Virtual Storage Platform G200, G400, G600, G800 or Hitachi Virtual Storage Platform F400, F600, F800 storage systems that must be enabled by installing license keys. This chapter describes the types of available licenses, license capacity calculation, and instructions for installing, enabling, disabling, and uninstalling license keys.

## Overview

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 it without uninstalling it. When you need the software, enable the license again.

If you do not install the software before you install the license key software, the software will install correctly but will be disabled. To enable a license key, install the prerequisite software, and then enable the key.

## License key types

To use software, you must install the license key provided when you purchase that software.

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 when 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.

The following table describes the four types of license keys.

| Type | Description | Effective term[1] | 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 |

| Type | Description | Effective term[1] | Estimating licensed capacity |
|---|---|---|---|

**Notes:**

1. When you log in to Device Manager - Storage Navigator, a warning message appears if 45 days or less remain before the expiration.

## Using the permanent key

You can purchase the permanent key to use a 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.

## 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

Three licensed capacity types are available. The one you choose depends on the software application. The following tables describe the licensed capacity types:

**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 to calculate pool capacity, see the *Provisioning Guide*.

**Table 9 Licensed capacity types**

| Type | Description |
|---|---|
| Used capacity | The licensed capacity is calculated by using one of the following capacities:<br>▪ Normal volumes (volumes)<br>▪ External volumes mapped to the storage system<br>▪ Pools<br>If the pool contains pool volumes that belong in accelerated compression-enabled parity groups, you must purchase physical capacity of the pool for the license capacity. |
| Mounted capacity/ usable capacity | The licensed capacity is estimated by using the capacity of all the volumes in the storage system.<br>When you estimate for the capacity of the accelerated compression-enabled parity groups, the physical capacity of the parity group is the maximum of the estimated capacity, even if you created an internal volume which exceeds the physical capacity of the accelerated compression-enabled parity group. See the Provisioning Guide for an explanation of accelerated compression. |
| Unlimited capacity | You can use the software regardless of the volume capacity. |

**Table 10 Software bundle licensed capacity for VSP G200, G400, G600, G800**

| Software bundle | VSP G200 | VSP G400, G600 | VSP G800 |
|---|---|---|---|
| Hitachi Storage Virtualization Operating System (SVOS) | Unlimited | Mounted capacity | Mounted capacity |
| Hitachi Remote Replication | Unlimited | Mounted capacity | Used capacity[1,2] |

| Software bundle | VSP G200 | VSP G400, G600 | VSP G800 |
|---|---|---|---|
| Hitachi Local Replication | Unlimited | Mounted capacity | Used capacity[1] |
| Hitachi Data Mobility | Unlimited | Mounted capacity | Used capacity[1] |
| Hitachi Encryption Key | Unlimited | Unlimited | Unlimited |
| Hitachi Disaster Recovery Extended | Unlimited | Unlimited | Unlimited |
| Nondisruptive migration | Unlimited | Unlimited | Unlimited |
| Global-active device | Unlimited | Mounted capacity | Used capacity[1] |

**Note:**

1. The method for calculating the licensed capacity varies depending on the software contained in each software bundle.
2. The used capacity for Remote Replication is the sum of TrueCopy and Universal Replicator.

**Table 11 Software bundle licensed capacity for VSP F400, F600, F800**

| Software bundle | VSP F400, F600, F800 |
|---|---|
| Hitachi Storage Virtualization Operating System (SVOS) | Unlimited |
| Hitachi Remote Replication | Unlimited |
| Hitachi Encryption Key | Unlimited |
| Hitachi Disaster Recovery Extended | Unlimited |

## Calculating licensed capacity for a normal volume

A normal volume is a volume that is not blocked or protected. The volume can be written to. The calculation of the normal volume capacity depends on the volume emulation type. Use the formula in the following table to estimate capacity for purchase. When you calculate the volume capacity, round the value up to the second decimal place.

**Table 12 Formulas for calculating capacity of a normal volume**

| Volume emulation type | Formula for calculating capacity of a normal volume |
|---|---|
| 3390-*x*[1] | 870 KB × *number-of-user-cylinders* |
| OPEN-*x*[1] | Same as the capacity specified when creating the volume |
| **Notes:**<br>**1.** *x* indicates a number or a letter. For example, OPEN-*x* refers to emulation types such as OPEN-3 and OPEN-V. | |

An example is shown in the following table.

**Table 13 Example of calculating license capacity**

| Item | Value |
|---|---|
| Volume emulation type | 3390-3 |
| Number of user cylinders | 3,339 |
| Number of volumes | 2,048 |
| Total capacity of all the volumes | 870 KB × 3,339 × 2,048 = 5,949,296,640 KB<br>5,949,296,640 KB / 1,024 = 5,809,860 MB<br>5,809,860 MB / 1,024 ≒ 5,673.70 GB<br>5,673.70 GB / 1,024 ≒ 5.55 TB |
| Estimated required capacity | At least 6 TB |

## Calculating licensed capacity for an external volume

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

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

## Calculating pool capacity

The license capacity of Dynamic Provisioning is calculated using the total capacity of the Dynamic Provisioning pool. If you use Dynamic Provisioning V-VOLs as P-VOLs or S-VOLs of ShadowImage, TrueCopy, Universal Replicator, 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*.

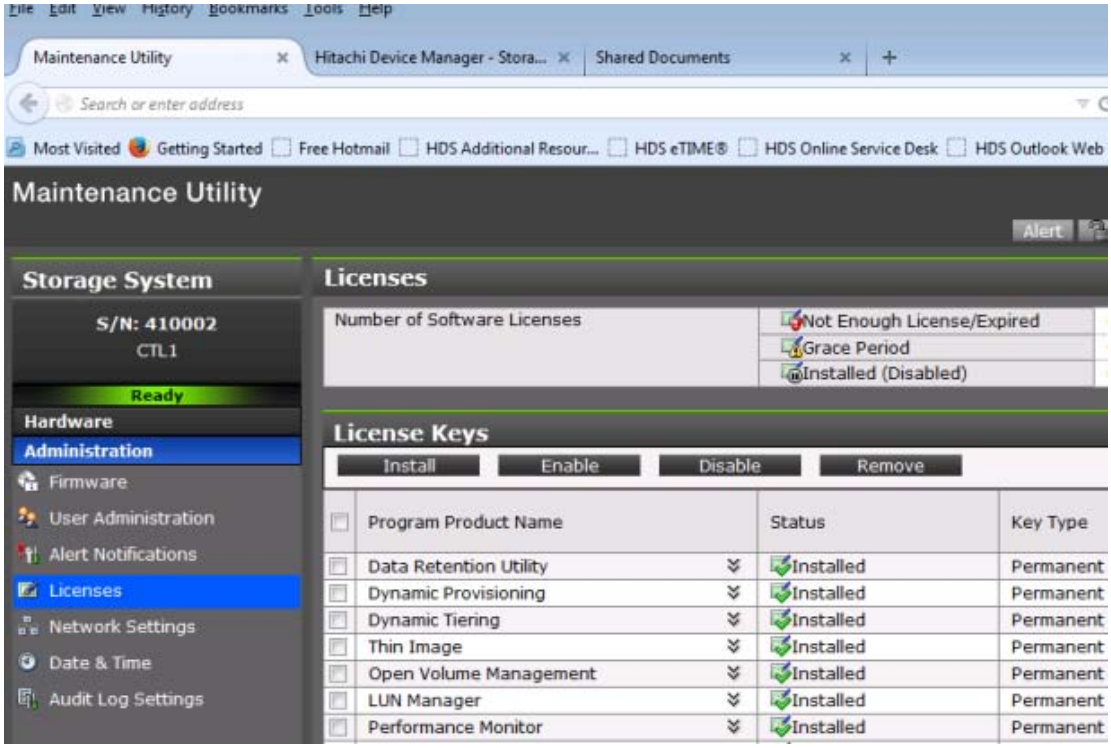
## Accelerated compression-enabled parity group capacity

For the actual capacity of accelerated compression-enabled parity groups, the total capacity of LDEVs created in the parity group and the physical capacity are compared. The one with the least capacity is added as the actual capacity. See the following table for an example.

| Total LDEV capacity in the parity group | Physical capacity | Actual capacity which is added |
|---|---|---|
| 12 TB | 20 TB | 12 TB |
| 24 TB | 20 TB | 20 TB |

# Managing licenses

Use the Licenses window in the maintenance utility to install and uninstall block license keys.




Use NAS Manager to install and enable both block and file license keys on VSP Gx00 models with NAS modules. Using NAS Manager, you can install both block and file licenses but only remove file licenses. To remove block licenses, you must use the maintenance utility.

**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 block and file licenses using NAS Manager

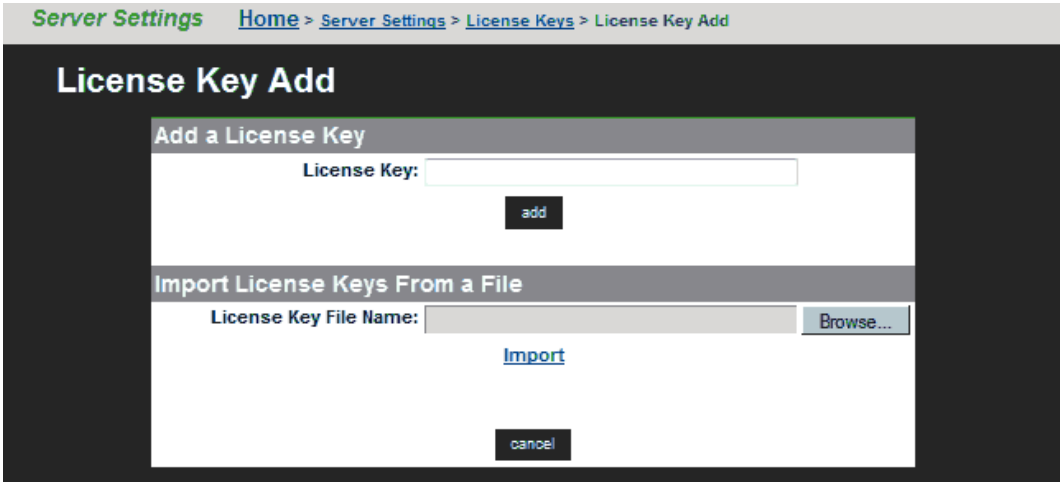
Use NAS Manager to install and enable both block and file license keys on VSP Gx00 models with NAS modules. Using NAS Manager, you can install both block and file licenses but only remove file licenses. To remove block licenses, you must use the maintenance utility.

### Adding a license key

Adding a license key can enable services or increase the capabilities of your system. To add a license key:

#### Procedure

1. Navigate to **Home** > **Server Settings** > **License Keys**.
2. Click **add**.




The following table describes the fields on this page:

| Field/Item | Description |
|---|---|
| **Add a File License Key** | |
| File License Key | Enables the user to manually enter the license key. |
| **Import File License Keys From a File** | |

| Field/Item | Description |
|---|---|
| File License Key File Name | Enables the user to import a license key from a file. |
| **Import Block License Keys From a File** (NAS module only) | |
| Block License Key File Name | Enables the user to import a software application license key from a file. |
| **cancel** | Closes the page without saving configuration changes. |

**Note:** After adding a license key, if a reboot is required in order to start a service/protocol or enable a feature, you are instructed to reboot or restart the system.

For a file license, you can either enter the key manually or import it from a file. For a block license, you can only import the key from a file:

- To enter the key manually, type it in the field, then click **add**.
- To import the key, click **Choose File / Browse**, navigate to the file, select the key file, then click **Import**.

After all the keys have been entered or imported, they will be displayed on the **License Keys** page. Follow the instructions to reboot the system (if necessary).

## Installing block licenses using maintenance utility

### Before you begin

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

**Note:** If you do not install the prerequisite software before you install the license key software, the software will install correctly but will be disabled. To enable a license key, install the prerequisite software, and then enable the key.

### Procedure

1. In the maintenance utility **Administration** tree, select **Licenses.**
2. Select whether to enter a key code or specify a license key file.
   - **Key Code**: Enter a key code to install the software. In **Key Code**, enter the license key code for the software.
   - **File**: Specify a license key file to install the software. Click **Browse** and specify the license key file. You can use a file name of up to 200 alphanumeric characters excluding these symbols: (“ \ : ; , * ? < > | / ). Include the .plk file extension.
3. Click **Apply.**

## 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 a software license that is in disabled status.

### 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 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 uninstall the software.

**Note:** To reinstall a license key after uninstalling it, contact Hitachi Data Systems customer support to reissue the license key file.

## 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.

| 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 |

| License key status (example) | Status | Key type | Licensed capacity | Term (Days) |
|---|---|---|---|---|
| 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 |
| 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.

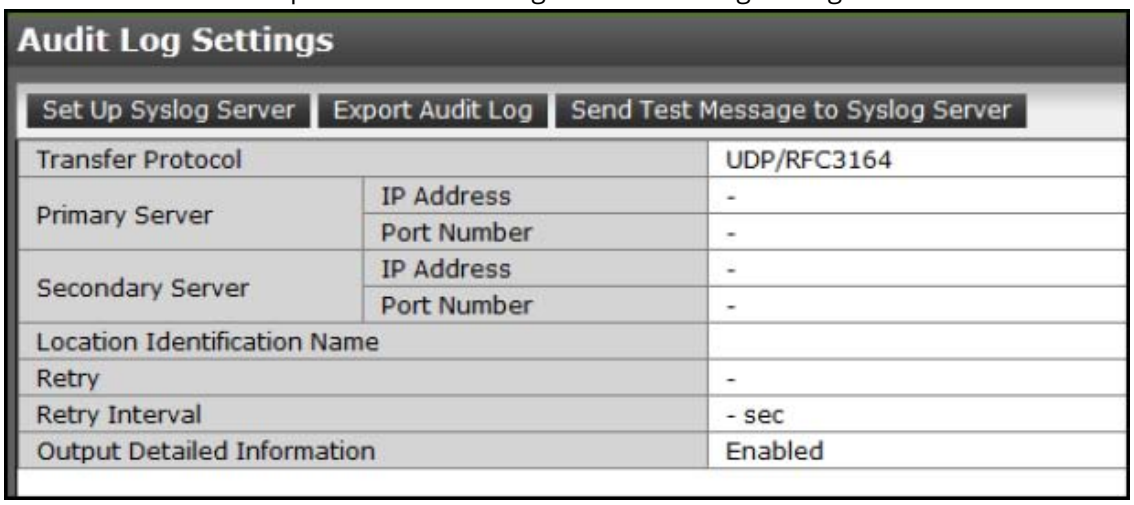
After your license key expires, no new configuration settings can be made, and no monitoring functions can be used with Performance Monitor. Configuration settings made before the expiration of the license key remain in effect. You can cancel configuration changes for some software.

# Chapter 8: Configuring audit logs

This chapter describes how to change the audit log settings in the maintenance utility.

## Audit log settings

This section shows the procedures to configure the audit log settings.




The **Audit Log Settings** window shows the current audit log settings. Select one of more of the three tabs to change the settings.

### Setting up a syslog server

#### Before you begin

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

#### Procedure

1. In the maintenance utility **Administration** tree, select **Audit Log Settings**.
2. Click **Set Up Syslog Server**.
3. Select the desired **Transfer Protocol**.
4. Enable or disable the **Primary Server**.
5. Enable or disable the **Secondary Server**.
6. Enable or disable the **Output Detailed Information**.
7. Click **Apply** to save the settings or **Cancel** to close the window without saving the settings.

## Exporting an audit log

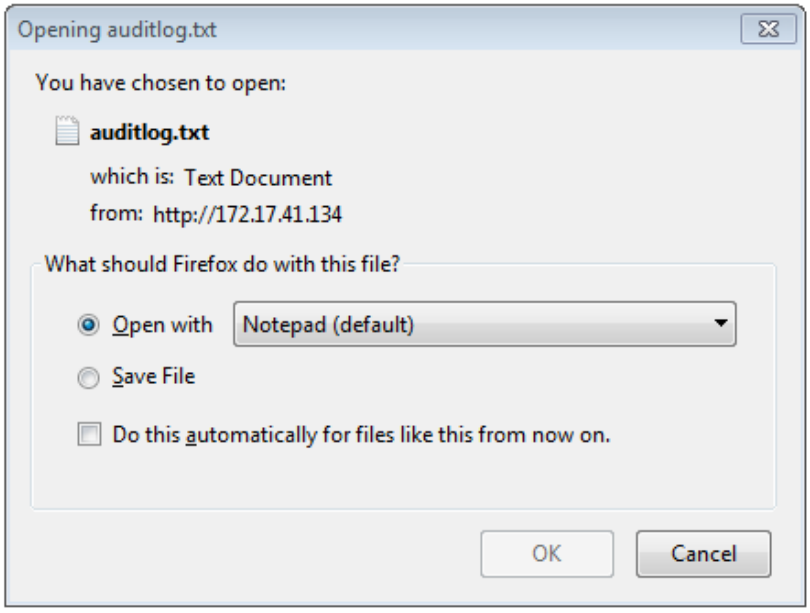
Use the following procedure to send a display an audit log file on the screen or to save it to a file on the SVP or your laptop.

### Before you begin

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

### Procedure

1. In the maintenance utility **Administration** tree, select **Audit Log Settings**.
2. Click **Export Audit Log**.




3. To open the file without saving, click **Open with** and then use the pull-down menu to select the software application to use to open the file.
4. Click **OK**. The auditlog.txt file is displayed.
5. To save the file, click **Save File**.
6. To use one of the two settings in steps 3 through 5 when you export an another auditlog.txt file, click **Do this automatically for files like this from now on**.
7. Click **OK**.
8. Browse to the directory where you want to save the file. Use the default file name auditlog.txt or change the file name as desired.

   Click **Save**. The file is saved and the dialog box closes.
9. Browse to the directory where you want the file. Use the default file name auditlog.txt or change the file name as desired.
10. Click **Save**. The file auditlog.txt file is saved.

## Send test message to syslog server

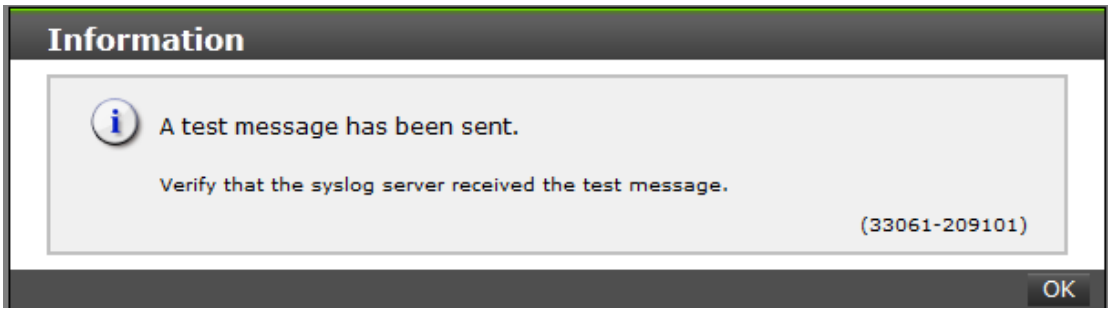
Use the following procedure to send a test audit log message to the syslog server.

### 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.

# Chapter 9: Managing 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.

## About 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.

## Viewing configuration reports

You can view configuration reports in three ways: in table view, in graphical view, and as comma-separated value (CSV)-formatted files.

### Before you begin

- Adobe Flash Player must be installed.
- Users can view the reports that they created.
- Users that have the Storage Administrator (Initial Configuration) role can view all reports.

**Note:** The window used to specify the location where the folder will be saved might not appear when downloading the report in Google Chrome. In this case, follow Chrome Menu > Settings > Show advanced settings and uncheck the Protect you and your device from dangerous sites checkbox under Privacy.

### Procedure

1. Expand the **Storage Systems** tree, and then click **Reports**.
2. Specify the report to download.
3. Click **Download Reports**.
4. Specify a folder in which to save a `.tgz` file.
5. Extract the downloaded `.tgz` file.
6. Display the report.
   For HTML reports:

   Open the file *extracted-folder*`\html\index.html`.

   For CSV reports:

   Open a 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.

### 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 up to 20 configuration reports for each storage system. If you already created 20 reports, delete unnecessary reports first, and then create a new report.

**Note:** If you use the configuration setting (**`raidcom`**) command of CCI to create parity groups and LDEVs, click File > Refresh All to update the configuration information before creating a configuration report.

### Before you begin

You must have Storage View permission to perform this task.

### Procedure

1. Open the **Create Configuration Report** window. From **General Tasks**, click **Create Configuration Report**.
2. Specify a task name and click **Apply**. This task name is used as the report name in the **Reports** window. This process takes approximately 10 minutes to complete.
3. Click **Refresh** to update the **Reports** window. The created report appears in the list.

## 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.

### Before you begin

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

### Procedure

1. Expand the **Storage Systems** tree, and then click **Reports**.
2. Select the report to delete.
3. Click **Delete Reports**.
4. Click **Apply**.

## Collecting dump files using the Dump tool

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 HDS 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.

There are two types of dump files:

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

### Before you begin

- You must be logged into the SVP.
- Device Manager - Storage Navigator must be running.
- The configuration information must be refreshed by selecting File > Refresh All in Device Manager - Storage Navigator.
- 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.

**Note:**

If the error is in regards to Device Manager - Storage Navigator starting up, collect information about the SVP using the Dump tool, without Device Manager - Storage Navigator running.

### Procedure

1. Close all Device Manager - Storage Navigator 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` or `Dump_Normal.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`.
   - When the tool is being executed, is displayed in the command prompt. When the execution is completed, is displayed.

```
"Executing..."
```

```
"zSv_AutoDump.exe is completed."
```

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.
6. Close the Windows command prompt.

# Appendix A: Examples of storage configuration reports

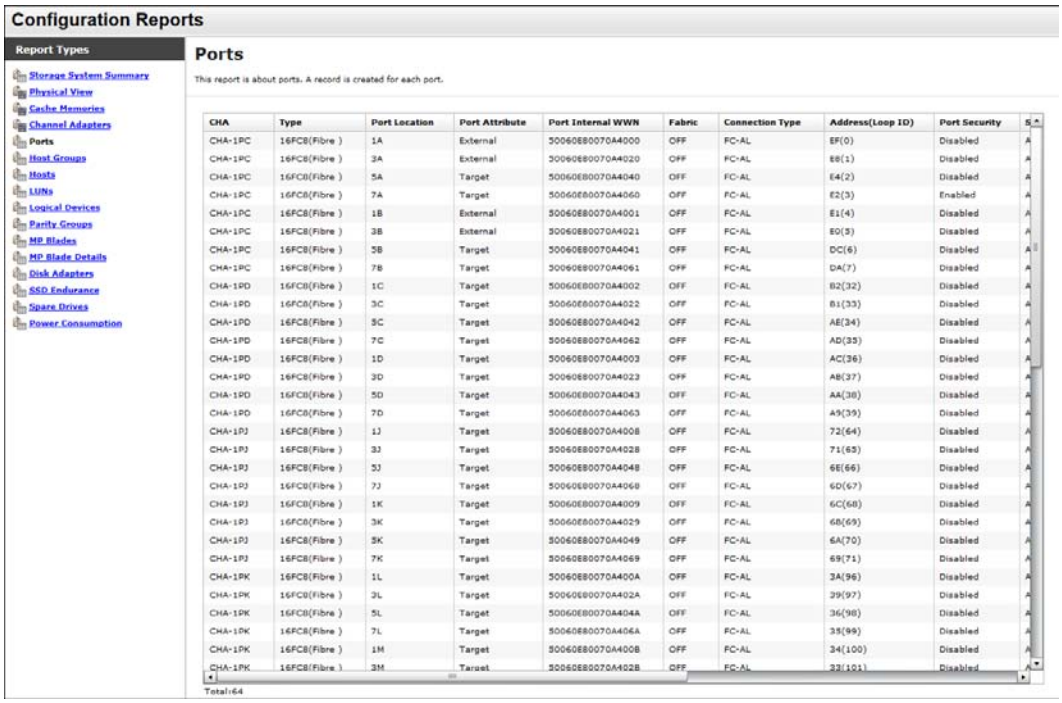
The Device Manager - Storage Navigator can show configuration reports table, graph, and CSV formats.

The following examples show various storage configuration reports in table, graph, and CSV formats.

## Reports in table view

Some Device Manager - Storage Navigator reports appear in table format.

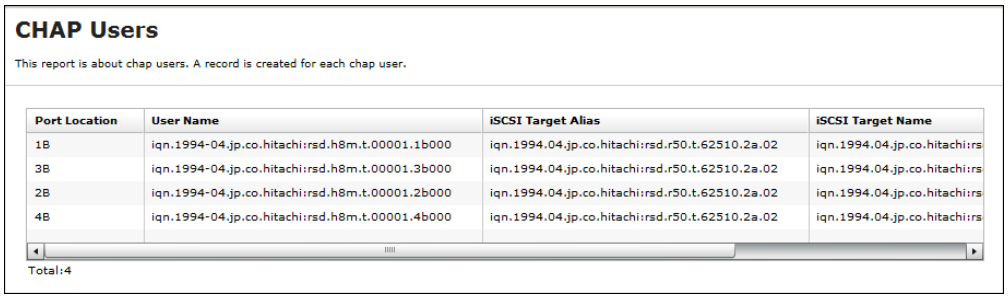
The following figure provides examples of reports in table format. The icons are displayed before the names of the reports in table view. If the icons are not displayed correctly, update the window.




- To sort data in table reports, click any column header.
- While a table is reading a large amount of data, the table columns cannot be manipulated, sorted, or resized. However, you can view previously displayed items, select rows, and scroll.

## 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.


CHAP Users

This report is about chap users. A record is created for each chap user.

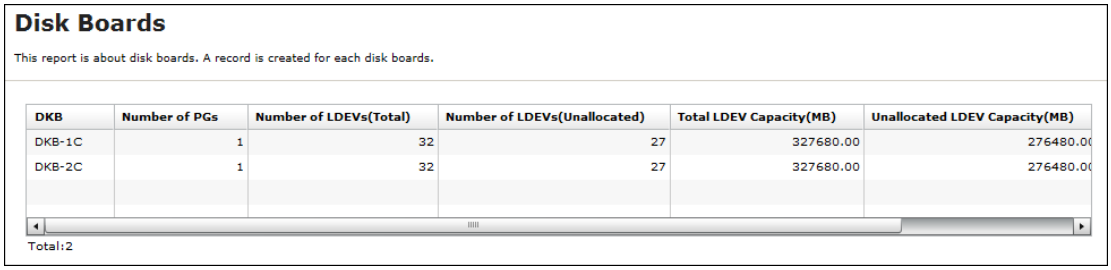
| Port Location | User Name | iSCSI Target Alias | iSCSI Target Name |
|---|---|---|---|
| 1B | iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000 | iqn.1994.04.jp.co.hitachi:rsd.r50.t.62510.2a.02 | iqn.1994.04.jp.co.hitachi:rs |
| 3B | iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.3b000 | iqn.1994.04.jp.co.hitachi:rsd.r50.t.62510.2a.02 | iqn.1994.04.jp.co.hitachi:rs |
| 2B | iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.2b000 | iqn.1994.04.jp.co.hitachi:rsd.r50.t.62510.2a.02 | iqn.1994.04.jp.co.hitachi:rs |
| 4B | iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.4b000 | iqn.1994.04.jp.co.hitachi:rsd.r50.t.62510.2a.02 | iqn.1994.04.jp.co.hitachi:rs |

Total:4

| 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.


Disk Boards

This report is about disk boards. A record is created for each disk boards.

| DKB | Number of PGs | Number of LDEVs(Total) | Number of LDEVs(Unallocated) | Total LDEV Capacity(MB) | Unallocated LDEV Capacity(MB) |
|---|---|---|---|---|---|
| DKB-1C | 1 | 32 | 27 | 327680.00 | 276480.0( |
| DKB-2C | 1 | 32 | 27 | 327680.00 | 276480.0( |

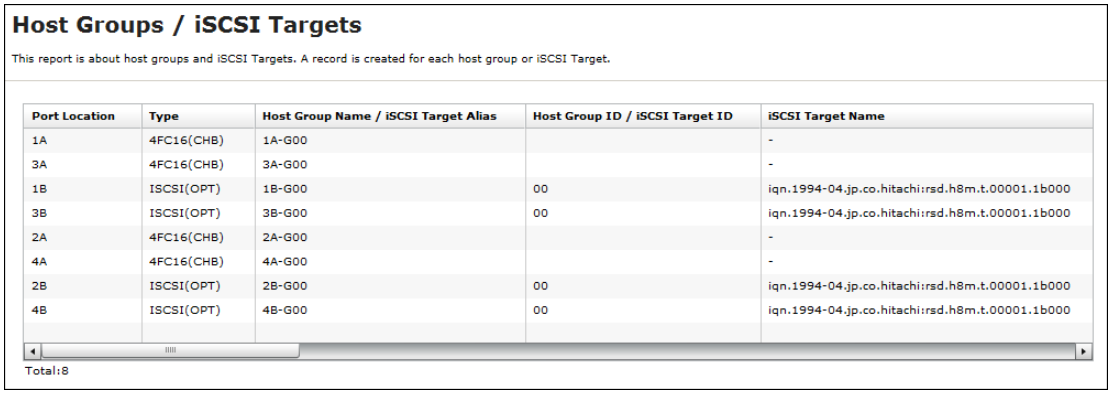
Total:2

| Item | Description |
|---|---|
| DKB | Location of the disk board.<br>▪ "External" is displayed when the storage system has an external storage system.<br>▪ "External (FICON DM)" is displayed when the storage system has volumes for FICON DM. |

| Item | Description |
|---|---|
| Number of PGs | The number of the parity groups that the disk board controls.<br>▪ If "DKB" is "External", this item indicates the number of parity groups mapped to external volumes.<br>▪ If "DKB" is "External (FICON DM)", this item indicates the number of parity groups mapped to volumes for FICON DM. |
| 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 |

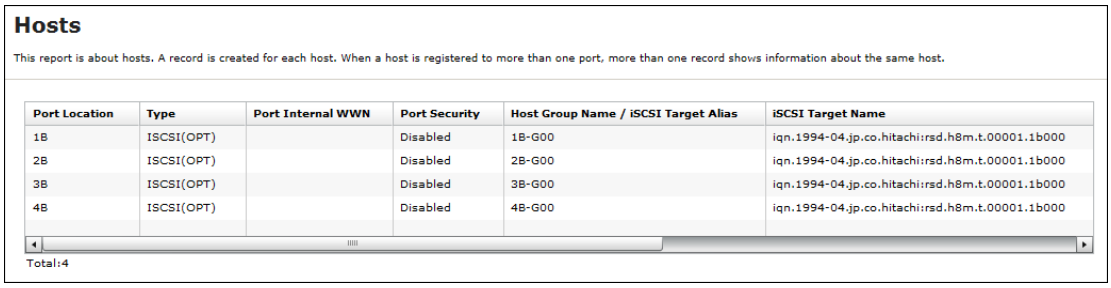
Total:8

| 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 |

| Item | Description |
|---|---|
| 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 |
| 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<br>▪ CHAP<br>▪ None<br>▪ Comply with Host Setting |
| Authentication : Mutual CHAP | Enable or disable the iSCSI target mutual CHAP<br>▪ Enabled<br>▪ 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

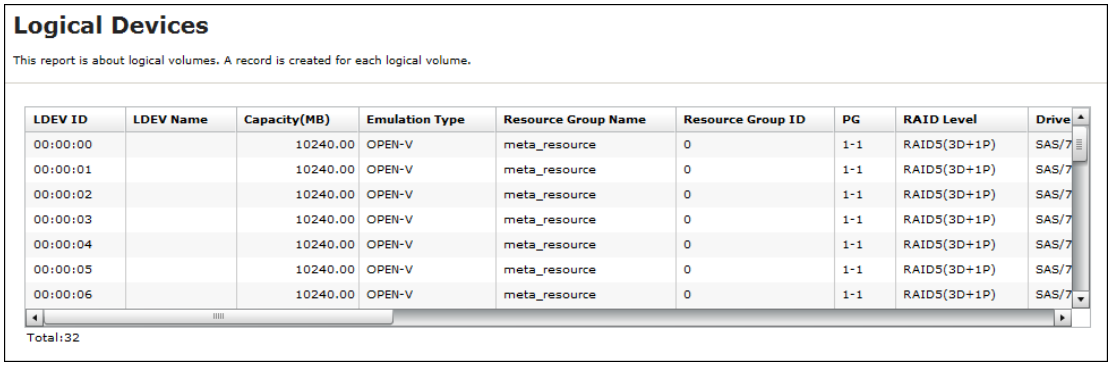
The following figure shows an example of a hosts report. The table following the figure describes the items in the report. When a host is registered to more than one port, more than one record shows information about the same host.




| 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 / host iSCSI name. The name is in 16-digit hex format. |

## Logical Devices report

The following figure shows an example of a logical volumes report. The table following the figure describes the items in the report.

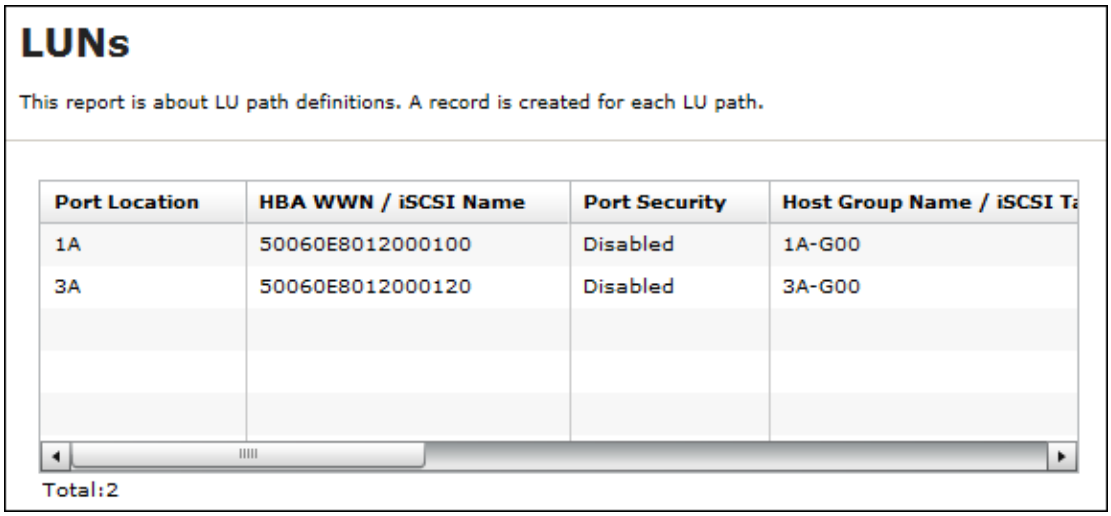


| Item | Description |
|---|---|
| LDEV ID | The logical volume number |
| LDEV Name | The logical volume name |
| Capacity (MB) | Capacity of the logical volume |
| Emulation Type | Emulation type of the logical volume |
| Resource Group Name | Resource group name where LDEV belongs |
| Resource Group ID | Resource group ID where LDEV belongs |
| PG | The parity group number.<br>▪ If the number starts with "E" (for example, E1-1), the parity group contains external volumes.<br>▪ If the number starts with "M" (for example, M1-1), the parity group contains FICON DM volumes.<br>A hyphen displays for Dynamic Provisioning or Thin Image V-VOLs. |
| RAID Level | RAID level of the parity group where the logical volume belongs[1] |
| Drive Type/RPM | Drive type and round-per-minute (RPM) of the drive of the parity group where the logical volume belongs.<br>A hyphen (-) is displayed as RPM when the drive is SSD.[1] |
| Drive Type-Code | Type code of the drive of the parity group where the logical volume belongs[1] |
| Drive Capacity | Capacity of the drive of the parity group where the logical volume belongs.[1] |
| PG Members | List of the drive locations of the parity group where the logical volume belongs[1] |
| Allocated | Information about whether the host can access the logical volume.<br>For mainframe volumes and multi-platform volumes, "Y" is displayed unless the volumes are in the reserved status. |
| SSID | SSID of the logical volume |
| CVS | Information about whether the logical volume is a customized volume |
| OCS | Oracle checksum |
| Attribute | The attribute of the logical volume |
| Provisioning Type | Provisioning type of the logical volume |

| Item | Description |
|---|---|
| Pool Name | ▪ For V-VOLs of Dynamic Provisioning, the name of the pool related to the logical volume is displayed[1]<br>▪ If the logical volume attribute is Pool, the name of the pool where the logical volume belongs is displayed<br>▪ When neither of the above are displayed, the pool name is blank |
| Pool ID | The ID of the pool indicated by "Pool Name" A hyphen (-) displays for volumes other than pool-VOLs or V-VOLs |
| Current MPU | The number of the MP unit that currently controls the logical volume |
| Setting MPU | The number of the MP unit that you specified to control the logical volume |
| Command Device: Security | Indicates whether Security is specified as the attribute for the command device. A hyphen (-) displays when "Attribute" is not "CMDDEV". |
| Command Device: User Authentication | Indicates whether User Authentication is specified as the attribute for the command device. A hyphen (-) displays 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 (-) displays when "Attribute" is not "CMDDEV". |
| Encryption | Indicates whether the parity group to which the LDEV belongs is encrypted.<br>▪ For internal volumes: Enabled (encrypted) or Disabled (not encrypted)<br>▪ For external volumes: blank |
| T10 PI | Indicates the T10 PI attribute set for the LDEV.<br>▪ Enabled<br>▪ Disabled<br>▪ Blank if the emulation type is not OPEN-V |
| ALUA Mode | Indicates whether the ALUA mode is enabled:<br>▪ Enabled: ALUA mode is enabled.<br>▪ Disabled: ALUA mode is disabled. |
| **Notes:**<br>**1.** A hyphen (-) displays if the LDEV is an external volume. | |

## LUNs report

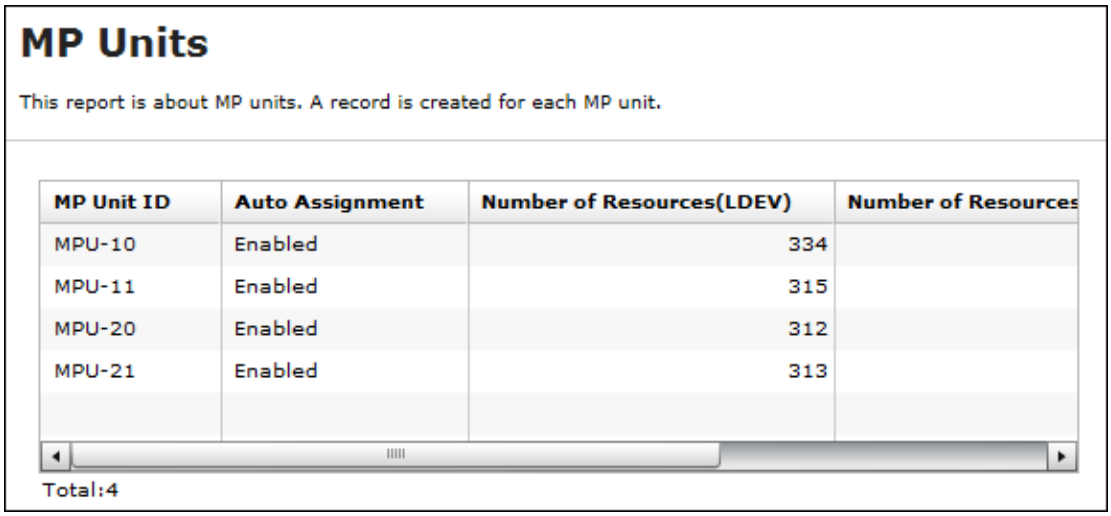
The following figure shows an example of an LU path definitions report. A record is created for each LU path. The table following the figure describes the items in the report.




| Item | Description |
|---|---|
| Port Location | Name of the port |
| HBA WWN / iSCSI Name | Port WWN or name of the iSCSI (16 digits in hexadecimal) |
| 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:<br>▪ Active/Optimized: Prioritized<br>▪ 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.

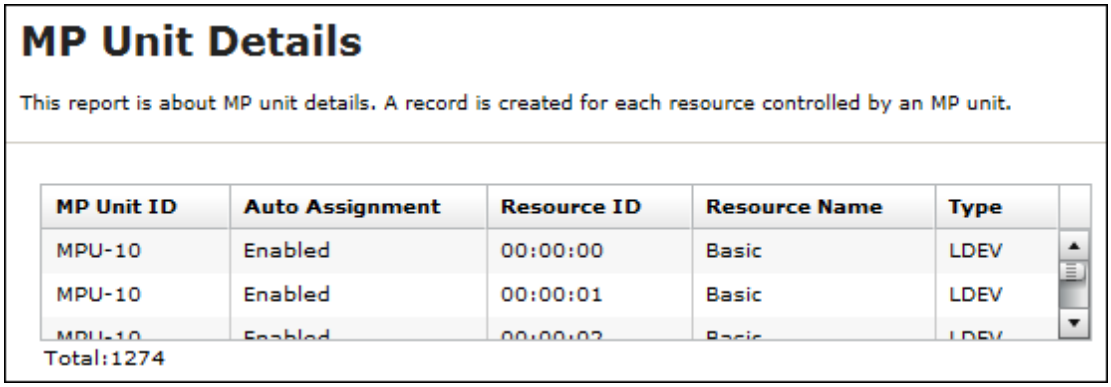
| MP Unit ID | Auto Assignment | Number of Resources(LDEV) | Number of Resources |
|---|---|---|---|
| MPU-10 | Enabled | 334 | |
| MPU-11 | Enabled | 315 | |
| MPU-20 | Enabled | 312 | |
| MPU-21 | Enabled | 313 | |

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.



MP Unit Details

This report is about MP unit details. A record is created for each resource controlled by an MP unit.

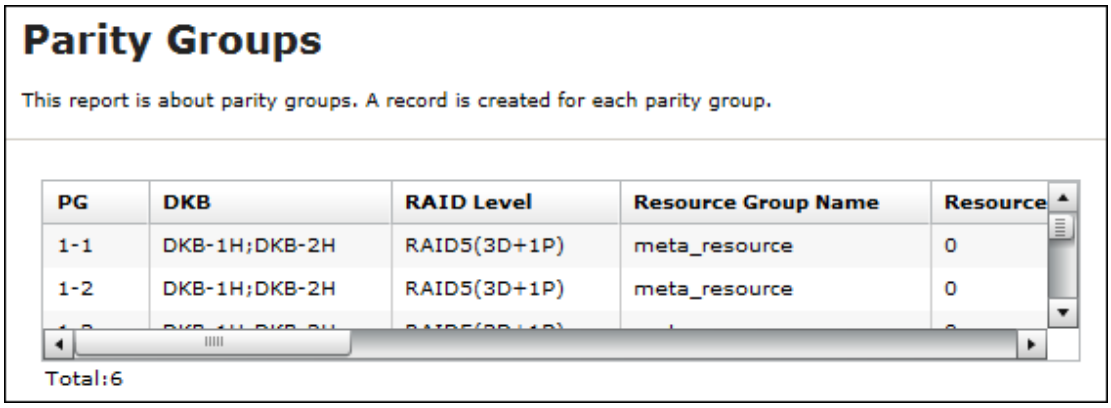
| MP Unit ID | Auto Assignment | Resource ID | Resource Name | Type |
|---|---|---|---|---|
| MPU-10 | Enabled | 00:00:00 | Basic | LDEV |
| MPU-10 | Enabled | 00:00:01 | Basic | LDEV |
| MPU-10 | Enabled | 00:00:02 | Basic | LDEV |

Total:1274

| 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

The following figure shows an example of a parity groups report. The table following the figure describes the items in the report.




| Item | Description |
|---|---|
| PG | Parity group number<br>▪ If the number starts with "E" (for example, E1-1), the parity group contains external volumes (Hitachi Universal Volume Manager User Guide).<br>▪ 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 |

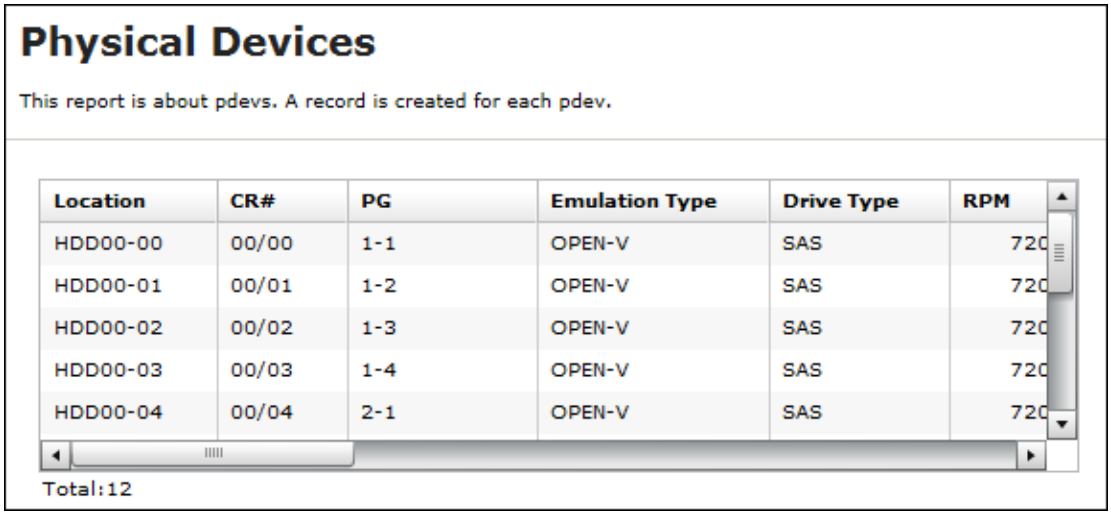
| Item | Description |
|---|---|
| Number of LDEVs (Total) | The number of the logical volumes in the parity group |
| Number of LDEVs (Unallocated) | The number of the logical volumes in the parity group that the host cannot access |
| Total LDEV Capacity (MB) | Capacity of the logical volumes in the parity group |
| Unallocated LDEV Capacity (MB) | Capacity of the logical volumes in the parity group that the host cannot access |
| Drive Type-Code | The type code of the drive in the parity group.<br>▪ The type code of the first drive in the parity group.<br>▪ If the parity group contains external volumes, the drive type code displays the vendor, the model, and the serial number of the storage system.<br>▪ Separated by semicolons (;) if multiple drive types are set. |
| Drive Type/RPM | Drive type and revolutions-per-minute (RPM) of the drive in the parity group[1]<br>A hyphen (-) is displayed instead of the RPM when the drive is an SSD. |
| Drive Capacity | Capacity of the drive in the parity group[1] |
| RAID Concatenation #0 | The number indicating a parity group #0 connected to this parity group[1,2] |
| 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.<br>▪ For internal volumes: Enabled (encrypted) or Disabled (not encrypted)<br>▪ For external volumes: A hyphen (-) is displayed |
| Accelerated Compression | Accelerated compression of the parity group<br>▪ If accelerated compression is supported, Enabled or Disabled is displayed.<br>▪ If accelerated compression is not supported, a hyphen (-) is displayed. |

**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. The table following the figure describes the items in the report.

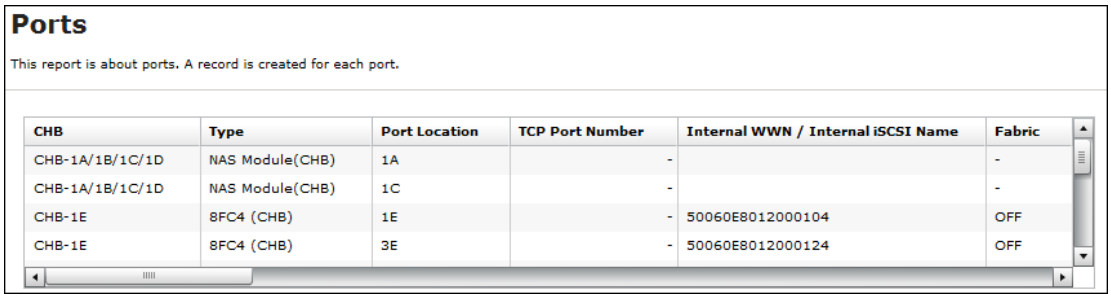



| Item | Description |
|---|---|
| Location | Name of physical devices |
| CR# | C# and R# to define physical devices<br>Output as "XX/YY" |
| PG | Parity group of physical devices |
| Emulation Type | Parity group of physical devices |
| Drive type | Drive type of physical devices<br>▪ SAS<br>▪ SSD |
| RPM | Revolutions-per-minute (RPM) in the parity group<br>▪ 8000<br>▪ 15000<br>A hyphen (-) is displayed instead of the RPM when the drive type is an SSD. |
| Drive Type-Code | Type code of the drive in the parity group.<br>Output example: SLR5B- M200SS;SFB5A-M200SS; (if multiple drive types are set) |
| Drive Size | Drive size (inches)<br>▪ 2.5<br>▪ 3.5 |

| Item | Description |
|---|---|
| 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 |
| Serial Number# | Serial product number of the physical devices<br>▪ yy: year (last 2 digits)<br>▪ mm: month (2 digits)<br>▪ xxxxxxxx: product number of the physical devices |
| RAID Level | RAID level of the physical devices<br>▪ RAID1(2D+2D)<br>▪ RAID5(7D+1P)<br>▪ RAID6(6D+2P)<br>▪ RAID6(14D+2P) |
| RAID Concatenation#0 | Number indicating a parity group #0 connected to this parity group<br>Output example: 2-1, 3-1, 4-1 |
| RAID Concatenation#1 | Number indicating a parity group #1 connected to this parity group<br>Output example: 2-1, 3-1, 4-1 |
| RAID Concatenation#2 | Number indicating a parity group #2 connected to this parity group<br>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) |
| Encryption | Enable or disable status of the parity group to which the physical devices belong<br>▪ Enabled: Encryption is enabled.<br>▪ Disabled: Encryption is disabled. |

## Ports report

The following figure shows an example of part of a ports report. The actual report includes several more columns of information. The table following the figure describes the items in the report.



**Ports**

This report is about ports. A record is created for each port.

| CHB | Type | Port Location | TCP Port Number | Internal WWN / Internal iSCSI Name | Fabric |
|---|---|---|---|---|---|
| CHB-1A/1B/1C/1D | NAS Module(CHB) | 1A | - | | - |
| CHB-1A/1B/1C/1D | NAS Module(CHB) | 1C | - | | - |
| CHB-1E | 8FC4 (CHB) | 1E | - | 50060E8012000104 | OFF |
| CHB-1E | 8FC4 (CHB) | 3E | - | 50060E8012000124 | OFF |

| 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 | WWN / iSCSI name of the port |
| Fabric | One of the Fibre topology settings indicating the setting status of the Fabric switch |
| Connection Type | One of the Fibre topology settings<br>▪ Point to Point<br>▪ FC-AL |
| IPv4 : IP Address | IPv4 address of the port<br>Output example: 192.168.0.100 |
| IPv4 : Subnet Mask | IPv4 subnet mask of the port<br>Output example: 255.255.255.0 |
| IPv4 : Default Gateway | IPv4 default gateway of the port<br>Output example: 255.255.255.0 |
| IPv6 : Mode | IPv6 settings of the port<br>▪ Enabled<br>▪ Disabled |
| IPv6 : Link Local Address | IPv6 link local address of the port (16-digit hexadecimal) |
| IPv6 : Global Address | IPv6 global address of the port.<br>Output example: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal) |

| Item | Description |
|---|---|
| IPv6 : Global Address 2 | IPv6 global address 2 of the port.<br>Output example: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal) |
| IPv6 : Assigned Default Gateway | Assigned IPv6 default gateway |
| Selective ACK | Selective ACK mode<br>▪ Enabled<br>▪ Disabled |
| Ethernet MTU Size (Byte) | MTU settings (binary)<br>▪ 1,500 |
| Keep Alive Timer | iSCSI keep alive timer (0 to 64,800) (sec) |
| VLAN : Tagging Mode | Tagging mode of VLAN<br>▪ Enabled<br>▪ 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<br>▪ ON<br>▪ OFF |
| 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 |
| Port Security | Security of the port<br>▪ Enabled<br>▪ Disabled |
| Speed | Data transfer speed of the port |

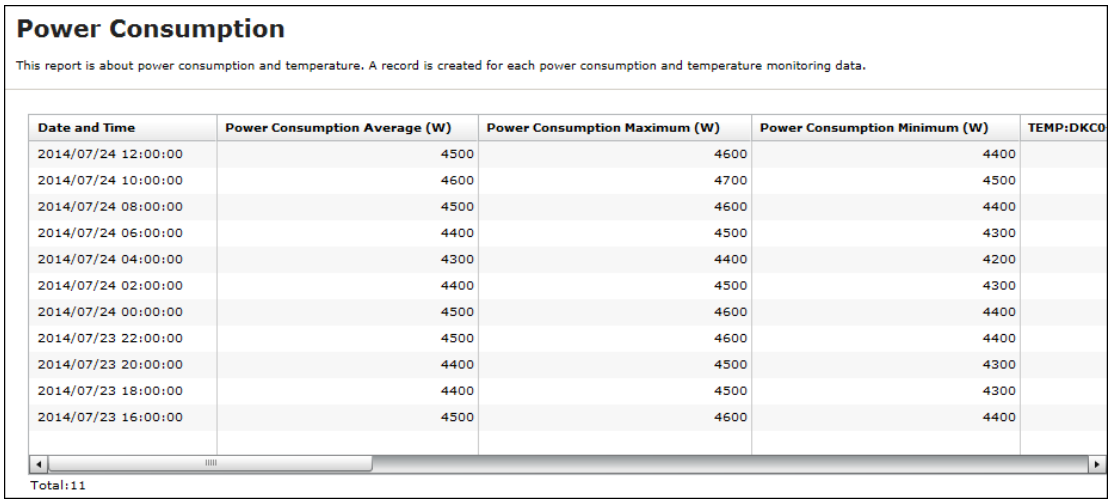
| Item | Description |
|---|---|
| SFP Data Transfer Rate | Maximum transfer rate of SFP which the mounted package supports.<br>▪ 8G<br>▪ 10G<br>▪ 16G<br>▪ 32G<br>▪ A hyphen (-) is displayed if Type is 10iSCSI2c (CHB) or NAS module (CHB). |
| T10 PI Mode | Indicates whether the T10 PI mode can be applied to the port.<br>▪ Enabled<br>▪ Disabled<br>▪ Blank if the port type is a Fibre port other than 16FC2(CHB). For iSCSI ports, a hyphen (-) is displayed. |
| Resource Group Name | Name of the resource group to which the port belongs |
| Resource Group ID | ID for the resource group to which the port belongs (0 to 1023) |
| Number of Hosts | The number of the hosts registered to the port |
| Number of LUNs | The number of the LU paths defined to the port |
| Number of LDEVs | The number of the logical volumes that can be accessed through the port |
| Number of PGs | The number of the parity groups having the logical volumes that can be accessed through the port |
| Number of DKBs | The number of the disk boards controlling the parity group that contains the logical volumes that can be accessed through the port |

## 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.

No records are created during a system power failure or if the breakers are turned off. If the system is in maintenance mode or the SVP is rebooted, up to two hours of records could be lost.

If a failure occurs in the storage system, the correct information might not be output.



**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 power consumption and temperature were recorded for the two-hour period |
| 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 (degrees C) | Average temperature of DKC0:CL1 |
| TEMP:DKC0-Cluster1 Maximum (degrees C) | Maximum temperature of DKC0:CL1 |
| TEMP:DKC0-Cluster1 Minimum (degrees C) | Minimum temperature of DKC0:CL1 |
| TEMP:DKC0-Cluster2 Average (degrees C) | Average temperature of DKC0:CL2 |
| TEMP:DKC0-Cluster2 Maximum (degrees C) | Maximum temperature of DKC0:CL2 |
| TEMP:DKC0-Cluster2 Minimum (degrees C) | Minimum temperature of DKC0:CL2 |

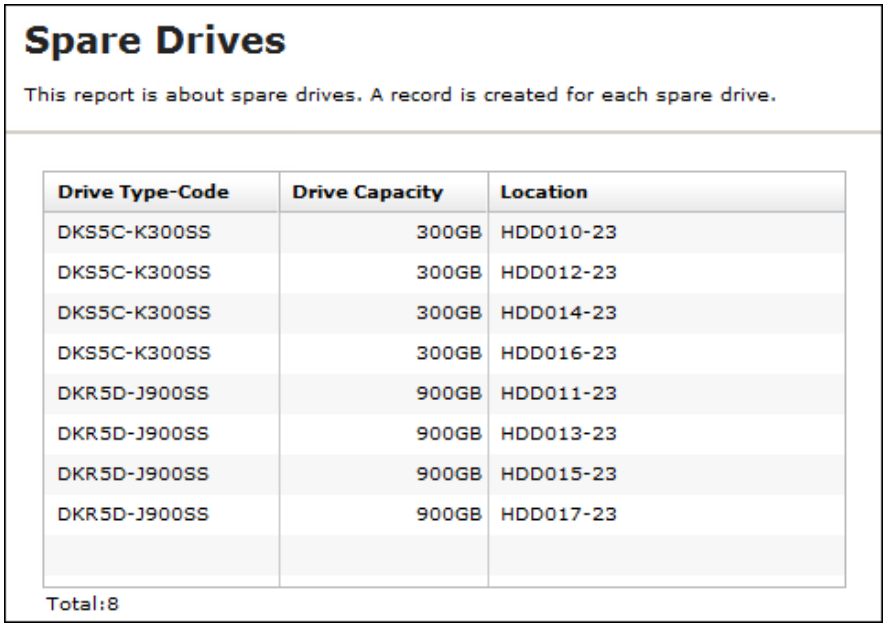
**Table 14 Power Consumption report**

| Item | Description |
|---|---|
| Date and Time | Date and time when temperature was recorded |

| | |
|---|---|
| TEMP:DB00-DBPS00-1 Average (Temperature in degrees C)<br>TEMP:DB00-DBPS00-1 Maximum (Temperature in degrees C),<br>TEMP:DB00-DBPS00-1 Minimum (Temperature in degrees C),<br>TEMP:DB00-DBPS00-2 Average (Temperature in degrees C),<br>TEMP:DB00-DBPS00-2 Maximum (Temperature in degrees C),<br>TEMP:DB00-DBPS00-2 Minimum (Temperature in degrees C) | Average temperature, maximum temperature, and minimum temperature of the DB for the two-hour period. Outputs in the following format:<br>TEMP:DB *XX* -DBPS *XX* -*CL* Average, Maximum, or Minimum (Temperature in degrees Celsius)<br>▪ *XX*: DB number<br>00 to 07 (VSP G200)<br>00 to 23 (VSP G400, G600, VSP F400, F600)<br>00 to 47 (VSP G800 or VSP F800)<br>▪ CL: Cluster number (1 or 2) |

## 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.

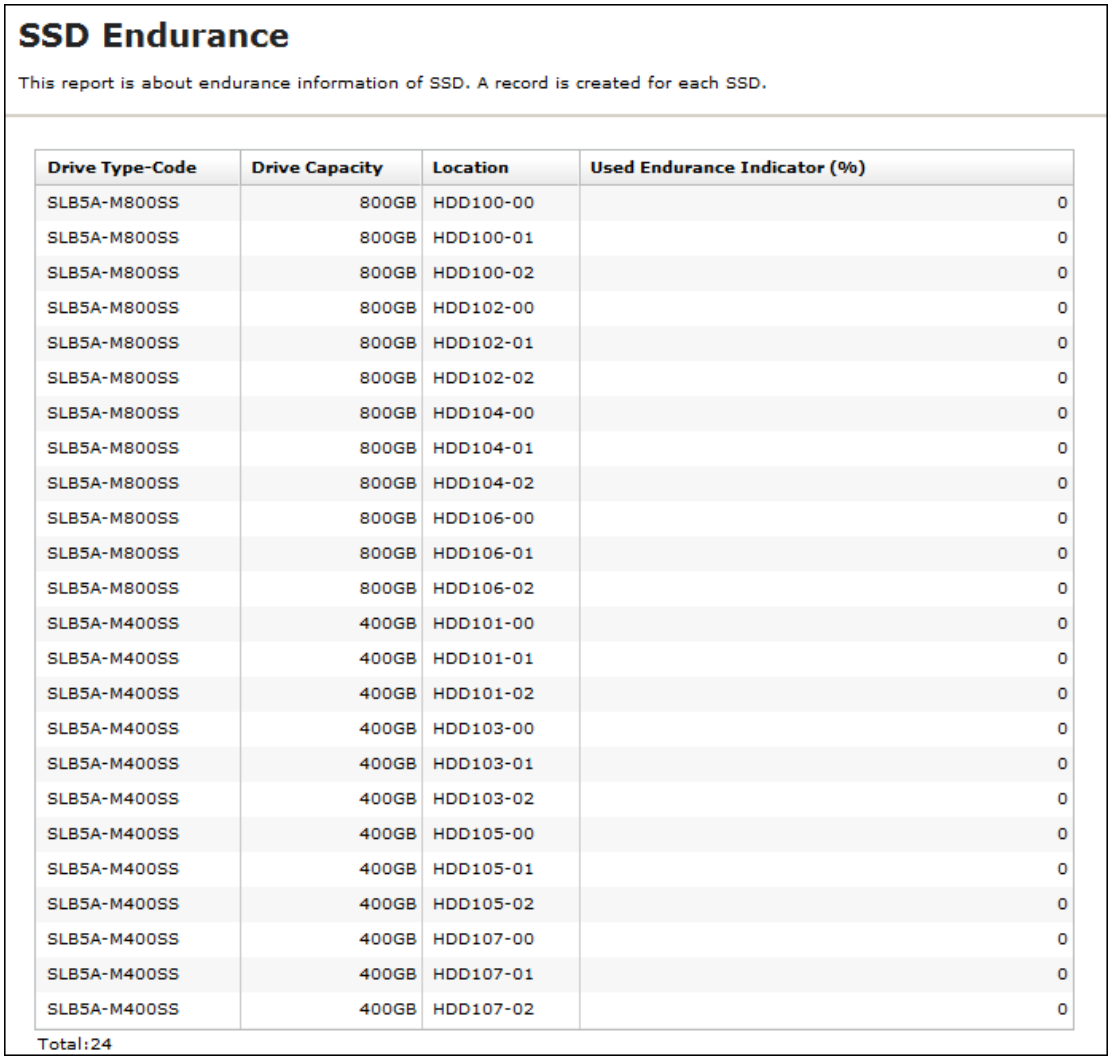
| Drive Type-Code | Drive Capacity | Location |
|---|---|---|
| DKS5C-K300SS | 300GB | HDD010-23 |
| DKS5C-K300SS | 300GB | HDD012-23 |
| DKS5C-K300SS | 300GB | HDD014-23 |
| DKS5C-K300SS | 300GB | HDD016-23 |
| DKR5D-J900SS | 900GB | HDD011-23 |
| DKR5D-J900SS | 900GB | HDD013-23 |
| DKR5D-J900SS | 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.

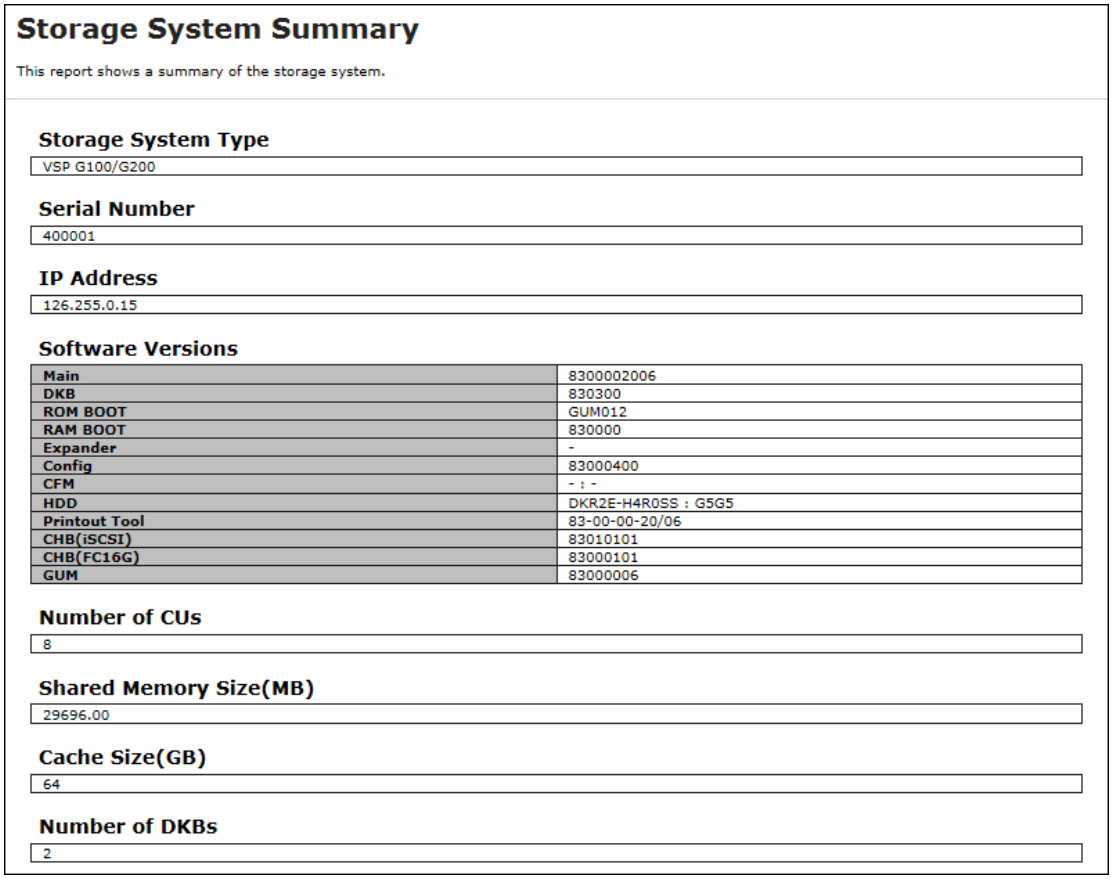
| Drive Type-Code | Drive Capacity | Location | Used Endurance Indicator (%) |
|---|---|---|---|
| SLB5A-M800SS | 800GB | HDD100-00 | 0 |
| SLB5A-M800SS | 800GB | HDD100-01 | 0 |
| SLB5A-M800SS | 800GB | HDD100-02 | 0 |
| SLB5A-M800SS | 800GB | HDD102-00 | 0 |
| SLB5A-M800SS | 800GB | HDD102-01 | 0 |
| 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 SSD |
| Drive Capacity | Capacity of the SSD |
| Location | Location of the SSD |
| Used Endurance Indicator (%) | Used endurance of the SSD |

## Storage System Summary report

The following figure shows an example of part of a Storage System Summary report. The actual report includes several more rows of information. The table following the figure describes the items in the report.



**Storage System Summary**

This report shows a summary of the storage system.

**Storage System Type**

VSP G100/G200

**Serial Number**

400001

**IP Address**

126.255.0.15

**Software Versions**

| | |
|---|---|
| Main | 8300002006 |
| DKB | 830300 |
| ROM BOOT | GUM012 |
| RAM BOOT | 830000 |
| Expander | - |
| Config | 83000400 |
| CFM | - : - |
| HDD | DKR2E-H4R0SS : G5G5 |
| Printout Tool | 83-00-00-20/06 |
| CHB(iSCSI) | 83010101 |
| CHB(FC16G) | 83000101 |
| GUM | 83000006 |

**Number of CUs**

8

**Shared Memory Size(MB)**

29696.00

**Cache Size(GB)**

64

**Number of DKBs**

2

**Figure 1 Storage System Summary report (VSP G200)**

### System Options

| |
|---|
| mode164 |
| mode449 |
| mode467 |
| mode872 |
| mode917 |

### Drive Capacity(TB)

| |
|---|
| 0.00 |

### Spare Drive Capacity(TB)

| |
|---|
| 0.00 |

### Free Drive Capacity(TB)

| |
|---|
| 35.25 |

### Volume Capacity(GB)

| | Allocated | Unallocated | Reserved | Free | Total |
|---|---|---|---|---|---|
| Internal Volumes | 0 | 0 | 0 | 0 | 0 |
| External Volumes | 0 | 0 | 0 | 0 | 0 |
| Total Volumes | 0 | 0 | 0 | 0 | 0 |

### Number of LDEVs

| | Allocated | Unallocated | Reserved | V-VOL | Total |
|---|---|---|---|---|---|
| Internal Volumes | 0 | 0 | 0 | - | 0 |
| External Volumes | 0 | 0 | 0 | - | 0 |
| Total Volumes | 0 | 0 | 0 | 0 | 0 |

**Figure 2 Storage System Summary report (VSP G200)**

## Storage System Summary

This report shows a summary of the storage system.

### Storage System Type

| |
|---|
| VSP G400/G600 |

### Serial Number

| |
|---|
| 400001 |

### IP Address

| |
|---|
| 126.255.0.15 |

### Software Versions

| | |
|---|---|
| **Main** | 8304524000 |
| **DKB** | 831014 |
| **ROM BOOT** | 830003 |
| **RAM BOOT** | 830101 |
| **Expander** | 835877 |
| | testexp |
| **Config** | 83044200 |
| **CFM** | - : - |
| **HDD** | DKS5C-K300SS : 4F56 |
| **Printout Tool** | 83-00-00-60/00 |
| **CHB(iSCSI)** | 830452 |
| **CHB(FC16G)** | 830104 |
| **GUM** | GUM_verInfo |

### Number of CUs

| |
|---|
| 16 |

### Shared Memory Size(MB)

| |
|---|
| 0.00 |

### Cache Size(GB)

| |
|---|
| 321 |

### Number of DKBs

| |
|---|
| 2 |

**Figure 3 Storage System Summary report (VSP G400, VSP G600)**

### System Options

| |
|---|
| mode164 |
| mode449 |
| mode467 |
| mode872 |
| mode917 |

### Drive Capacity(TB)

| |
|---|
| 0.00 |

### Spare Drive Capacity(TB)

| |
|---|
| 0.00 |

### Free Drive Capacity(TB)

| |
|---|
| 4.62 |

### Volume Capacity(GB)

| | Allocated | Unallocated | Reserved | Free | Total |
|---|---|---|---|---|---|
| Internal Volumes | 0 | 0 | 0 | 0 | 0 |
| External Volumes | 0 | 0 | 0 | 0 | 0 |
| Total Volumes | 0 | 0 | 0 | 0 | 0 |

### Number of LDEVs

| | Allocated | Unallocated | Reserved | V-VOL | Total |
|---|---|---|---|---|---|
| Internal Volumes | 0 | 0 | 0 | - | 0 |
| External Volumes | 0 | 0 | 0 | - | 0 |
| Total Volumes | 0 | 0 | 0 | 0 | 0 |

**Figure 4 Storage System Summary report (VSP G400, VSP G600)**

## Storage System Summary

This report shows a summary of the storage system.

### Storage System Type

| |
|---|
| VSP G800 |

### Serial Number

| |
|---|
| 400001 |

### IP Address

| |
|---|
| 126.255.0.15 |

### Software Versions

| | |
|---|---|
| **Main** | 8300006001 |
| **DKB** | 830100 |
| **ROM BOOT** | |
| **RAM BOOT** | 830000 |
| **Expander** | - |
| **Config** | 83000100 |
| **CFM** | - : - |
| **HDD** | DKR5D-J900SS : GCGC |
| **Printout Tool** | 83-00-00-60/00 |
| **CHB(iSCSI)** | 000200 |
| **CHB(FC16G)** | 800105 |
| **GUM** | |

### Number of CUs

| |
|---|
| 16 |

### Shared Memory Size(MB)

| |
|---|
| 34560.00 |

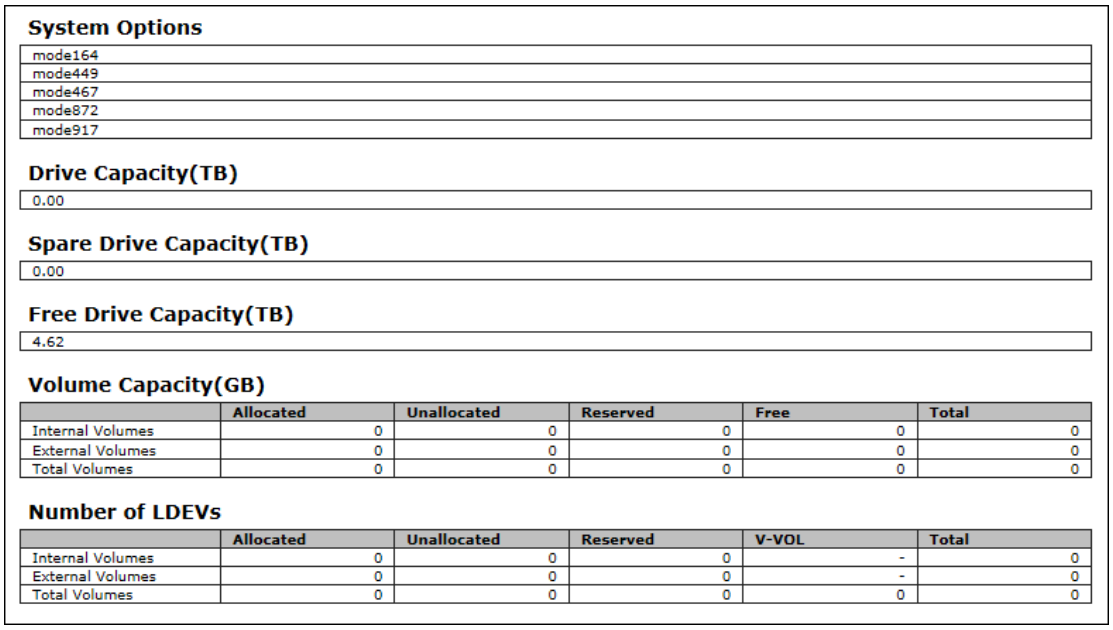
### Cache Size(GB)

| |
|---|
| 128 |

### Number of DKBs

| |
|---|
| 2 |

**Figure 5 Storage System Summary report (VSP G800)**



**System Options**

| |
|---|
| mode164 |
| mode449 |
| mode467 |
| mode872 |
| mode917 |

**Drive Capacity(TB)**

| |
|---|
| 0.00 |

**Spare Drive Capacity(TB)**

| |
|---|
| 0.00 |

**Free Drive Capacity(TB)**

| |
|---|
| 4.62 |

**Volume Capacity(GB)**

| | Allocated | Unallocated | Reserved | Free | Total |
|---|---|---|---|---|---|
| Internal Volumes | 0 | 0 | 0 | 0 | 0 |
| External Volumes | 0 | 0 | 0 | 0 | 0 |
| Total Volumes | 0 | 0 | 0 | 0 | 0 |

**Number of LDEVs**

| | Allocated | Unallocated | Reserved | V-VOL | Total |
|---|---|---|---|---|---|
| Internal Volumes | 0 | 0 | 0 | - | 0 |
| External Volumes | 0 | 0 | 0 | - | 0 |
| Total Volumes | 0 | 0 | 0 | 0 | 0 |

**Figure 6 Storage System Summary report (VSP G800)**

| 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 |

| Item | Description |
|---|---|
| Software Versions | Version of the following programs.<br>▪ Main<br>▪ DKB<br>▪ ROM BOOT<br>▪ RAM BOOT<br>▪ Expander<br>▪ Config<br>▪ CFM<br>▪ HDD<br>▪ Printout Tool<br>▪ CHB (iSCSI)<br>▪ CHB (FC16G)<br>▪ CHB (FC32G)<br>▪ GUM<br>▪ Unified Hypervisor<br>▪ NASFWINST<br>▪ NASFW |
| Number of CUs | The number of control units in the storage system |
| Shared Memory Size (GB) | Capacity of shared memory<br>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) [1] | List of the capacity of the open volumes |

| Item | Description |
|---|---|
| Number of LDEVs[1] | List of the numbers of the volumes in the following status.<br>▪ Allocated<br>▪ Unallocated<br>▪ Reserved<br>▪ V-VOL |
| **Notes:**<br>**1.** You cannot sort the list. | |

# Reports in 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.

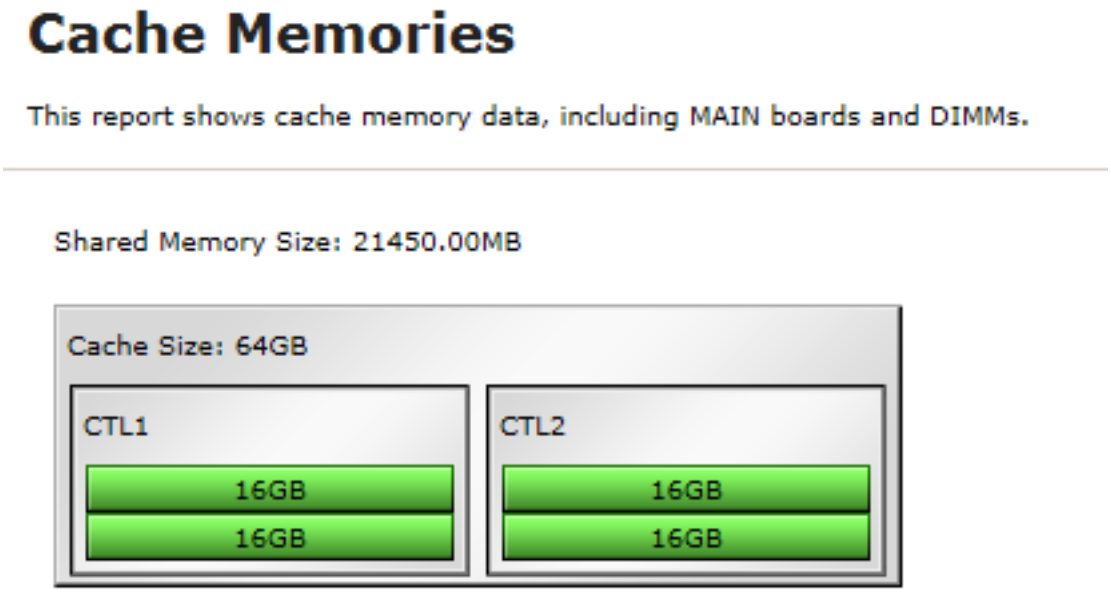



**Figure 7 Cache Memories report (VSP G200)**

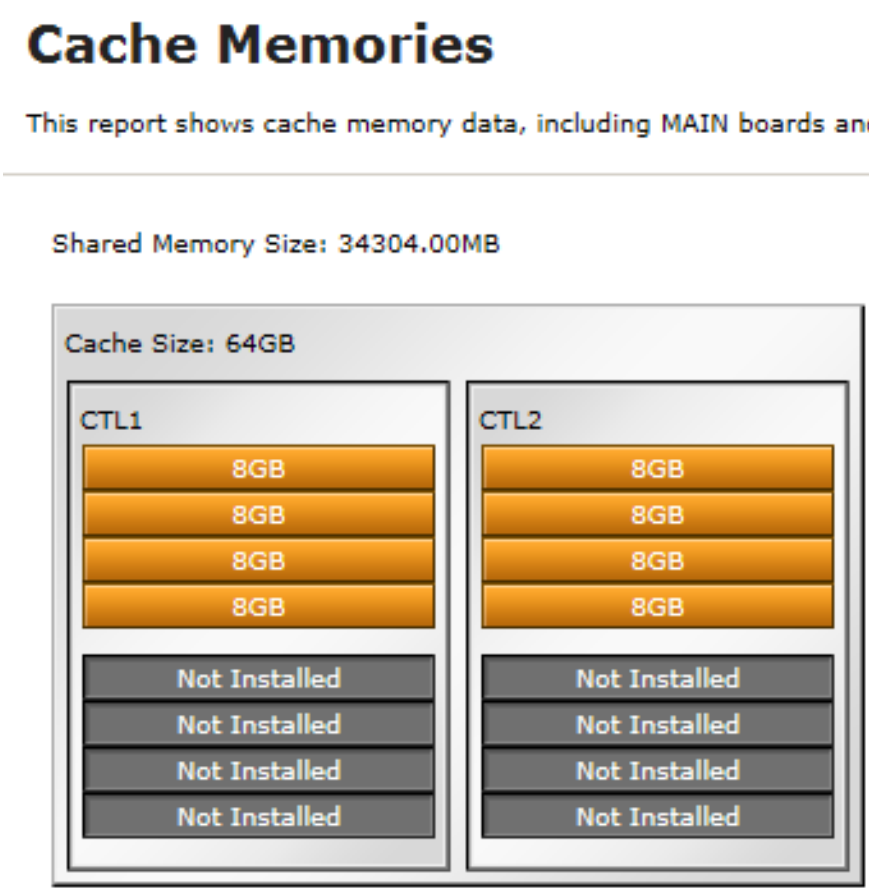



**Figure 8 Cache Memories report (VSP G400, G600, VSP F400, F600)**

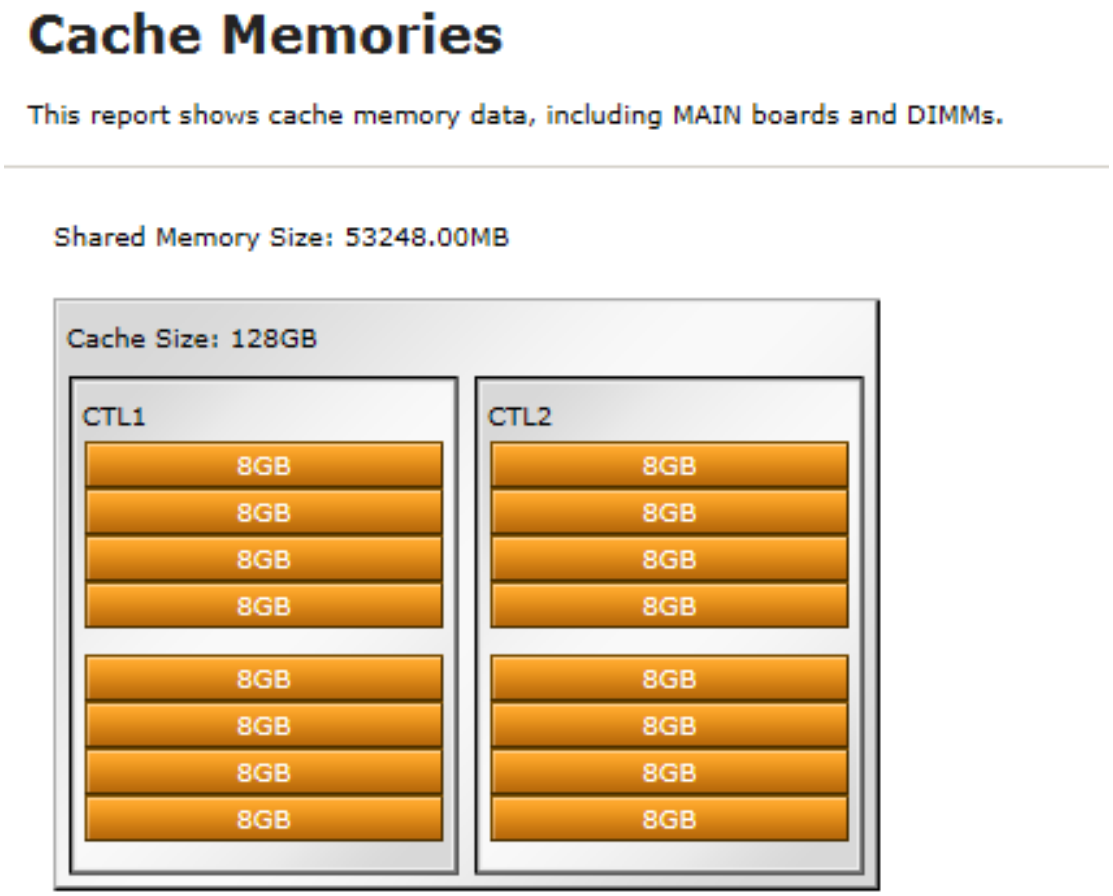



**Figure 9 Cache Memories report (VSP G800, VSP F800)**

Total capacity of the cache memory and shared memory is displayed separately for each module.

## 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.

If a NAS module is mounted on a channel board, the status of the module is displayed.

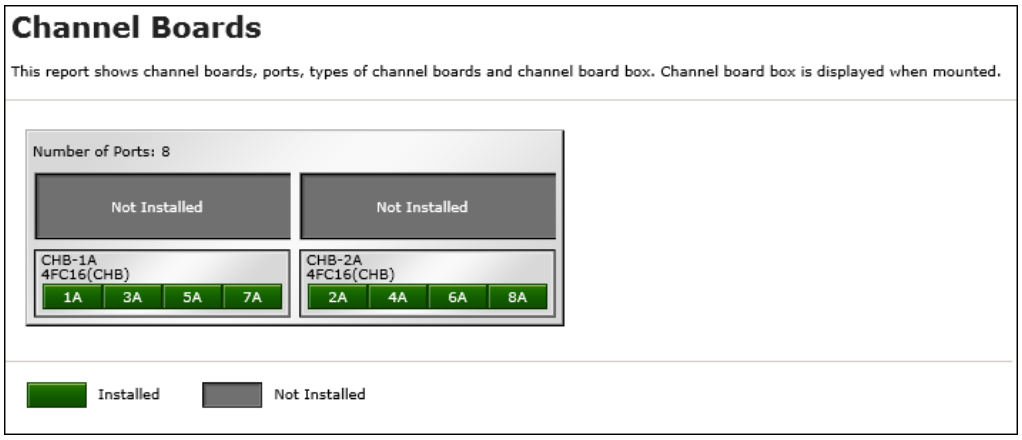



**Figure 10 Channel Boards (VSP G200)**

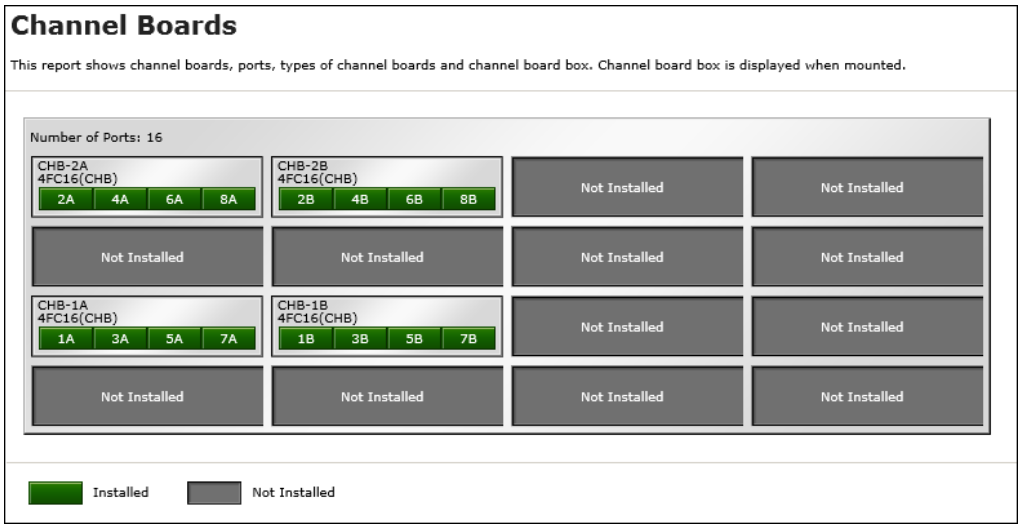



**Figure 11 Channel Boards report (VSP G400, G600, VSP F400, F600)**

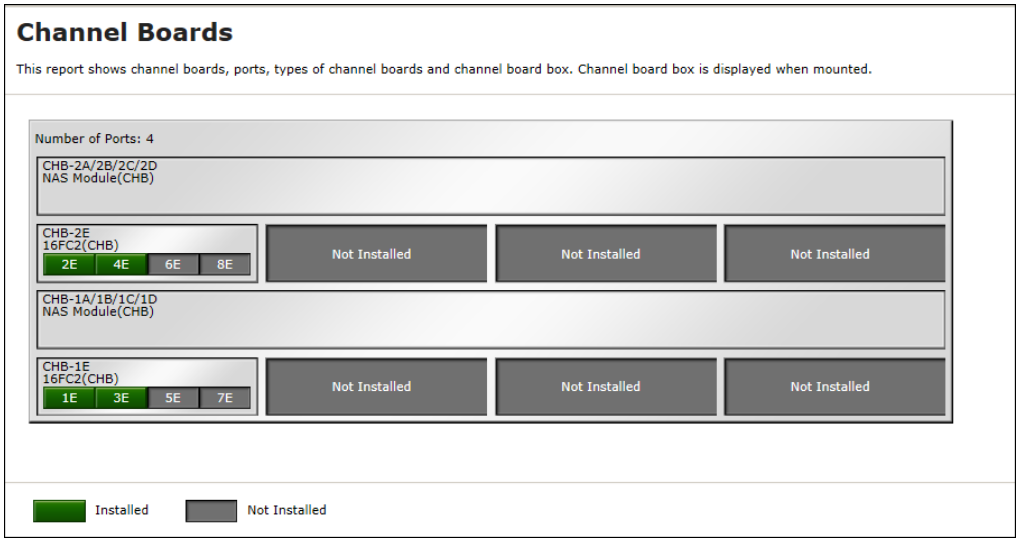



**Figure 12 Channel Boards Report (when a NAS module is mounted)**

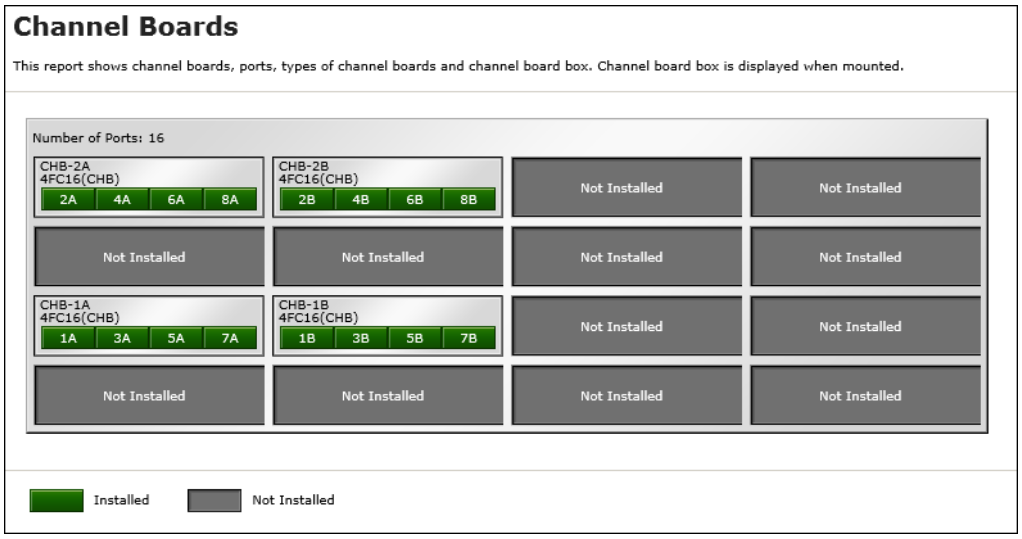



**Figure 13 Channel Boards report (VSP G800, VSP F800)**

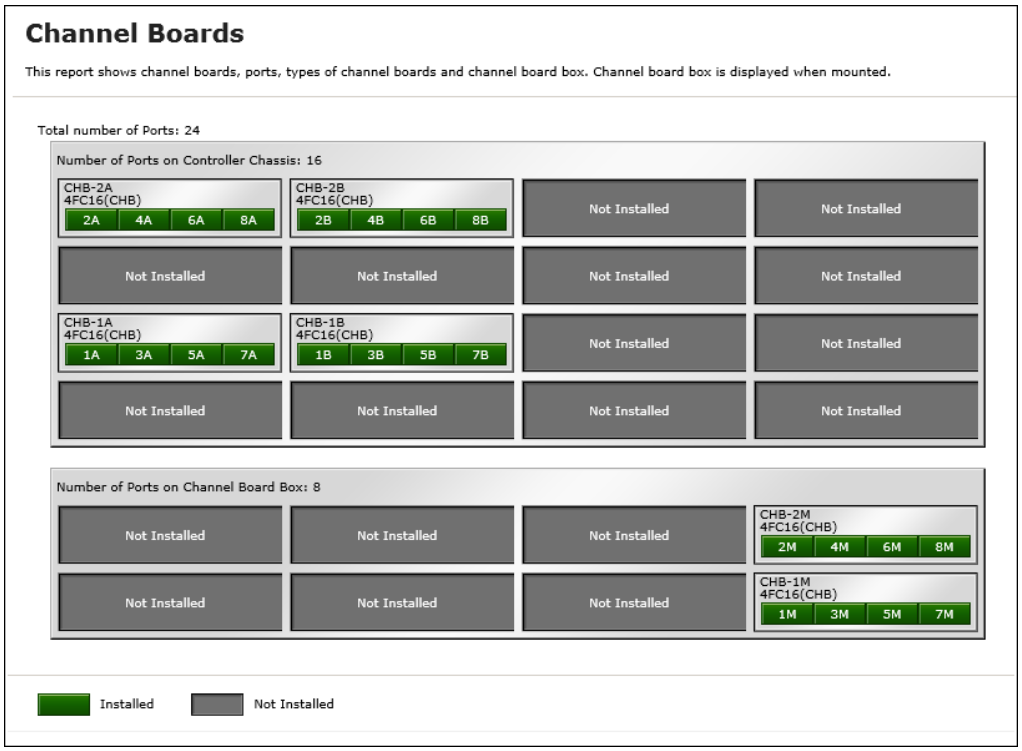



**Figure 14 Channel Boards report (when a channel board box is connected)**

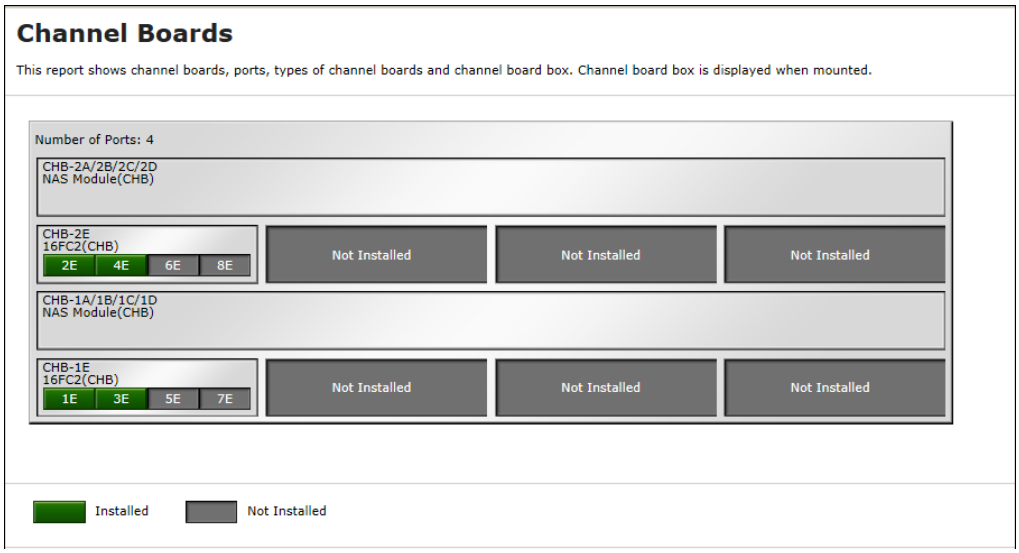



**Figure 15 Channel Boards report (when a NAS module is mounted)**

## 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.

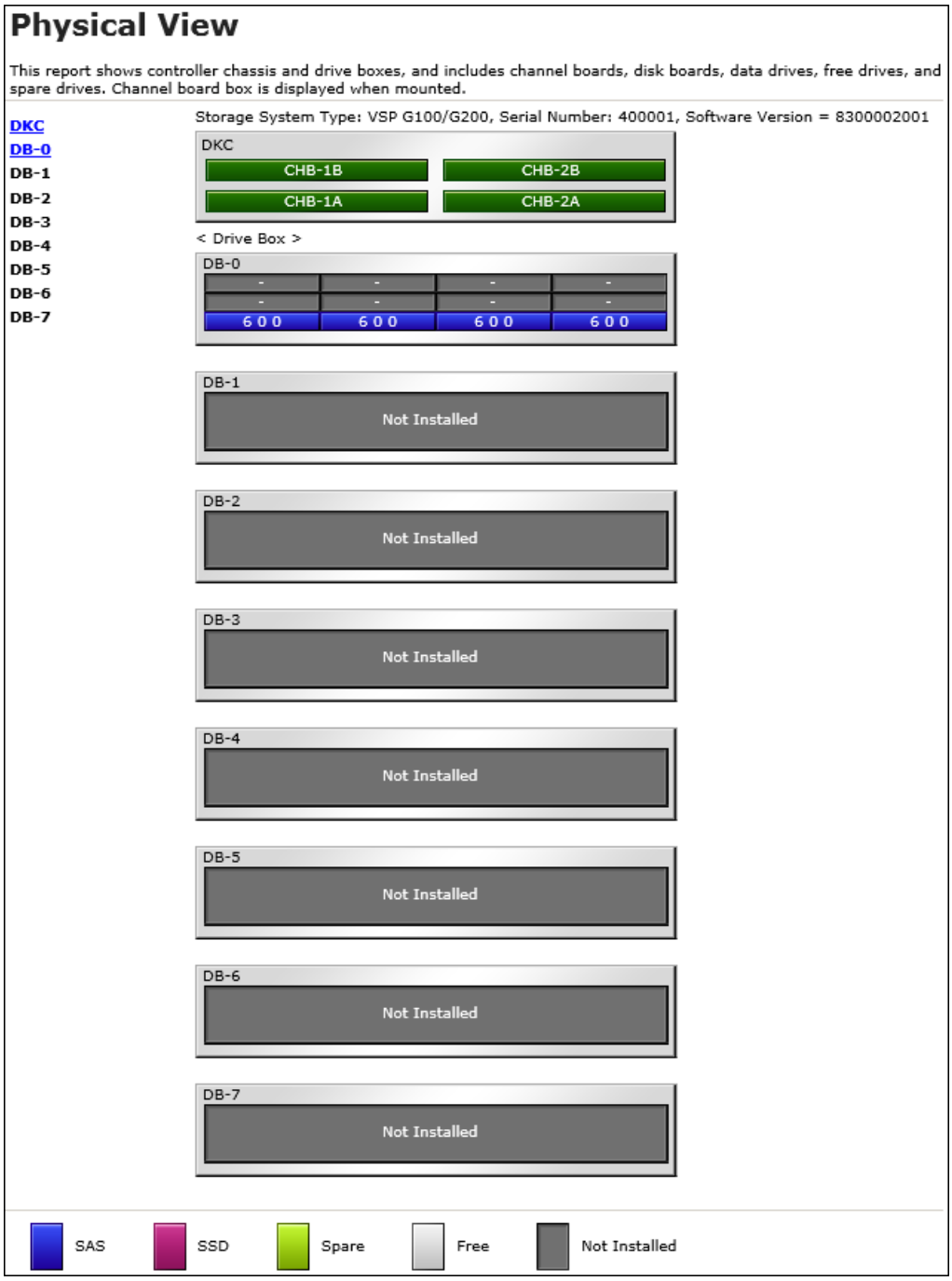



**Figure 16 Physical View report (VSP G200)**

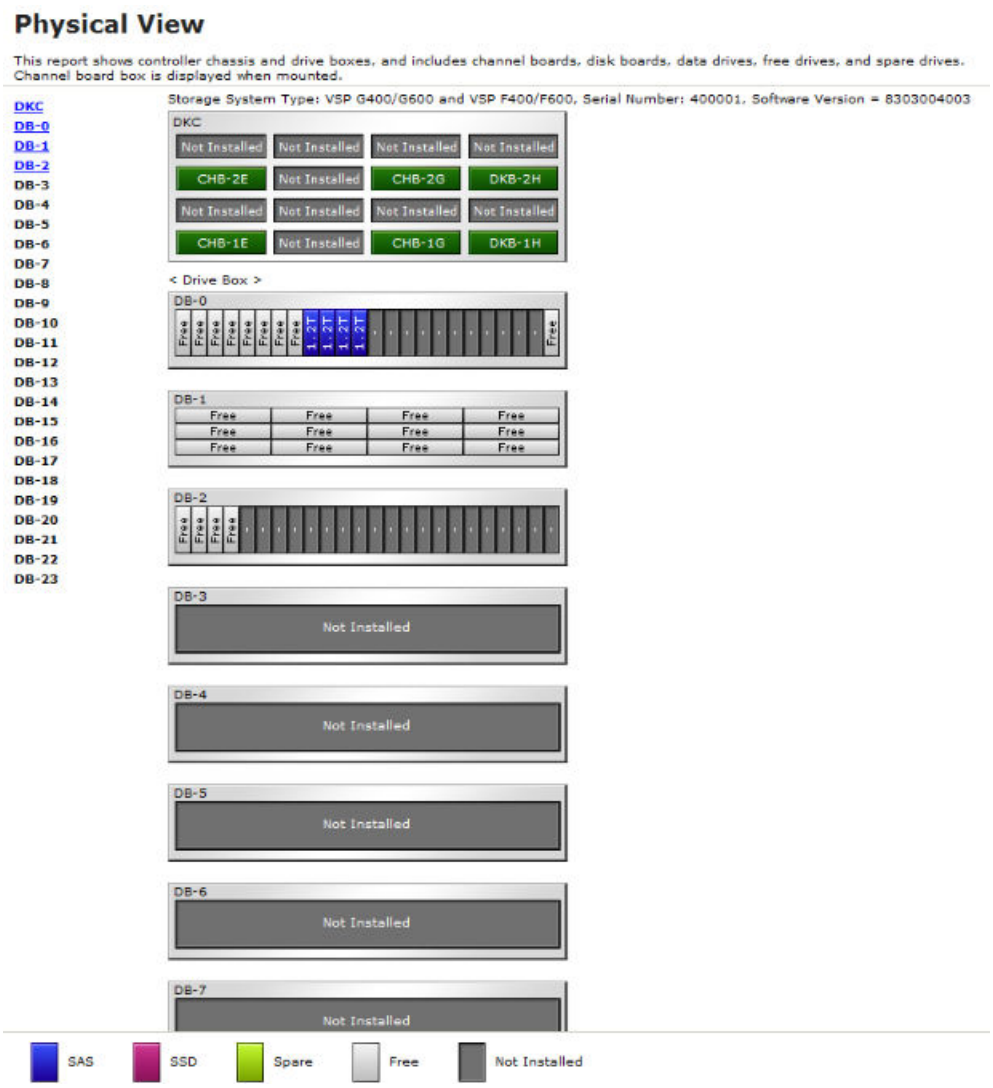



**Figure 17 Physical View report (VSP G400, G600, VSP F400, F600)**

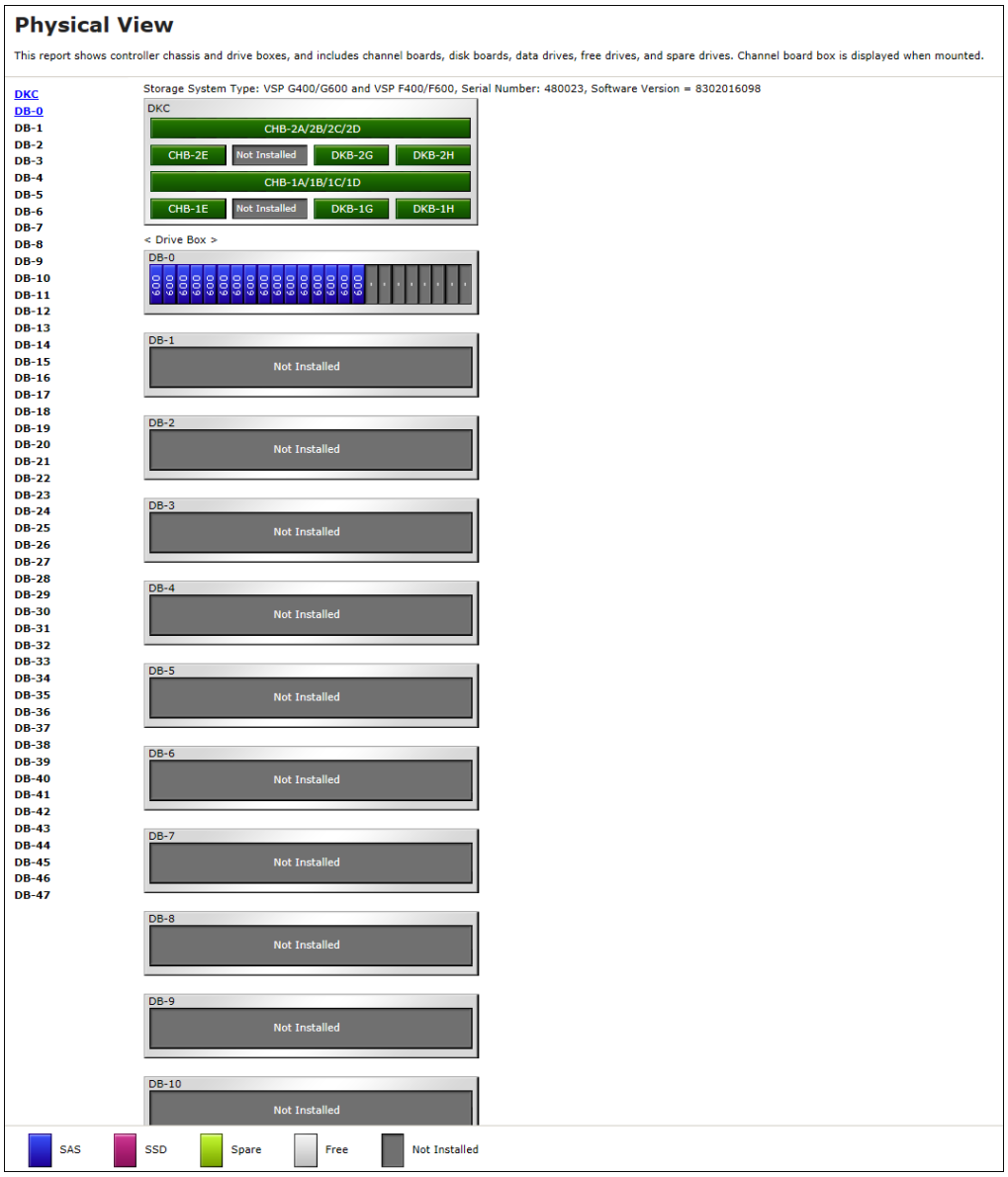



**Figure 18 Physical View report (when a NAS module is mounted)**

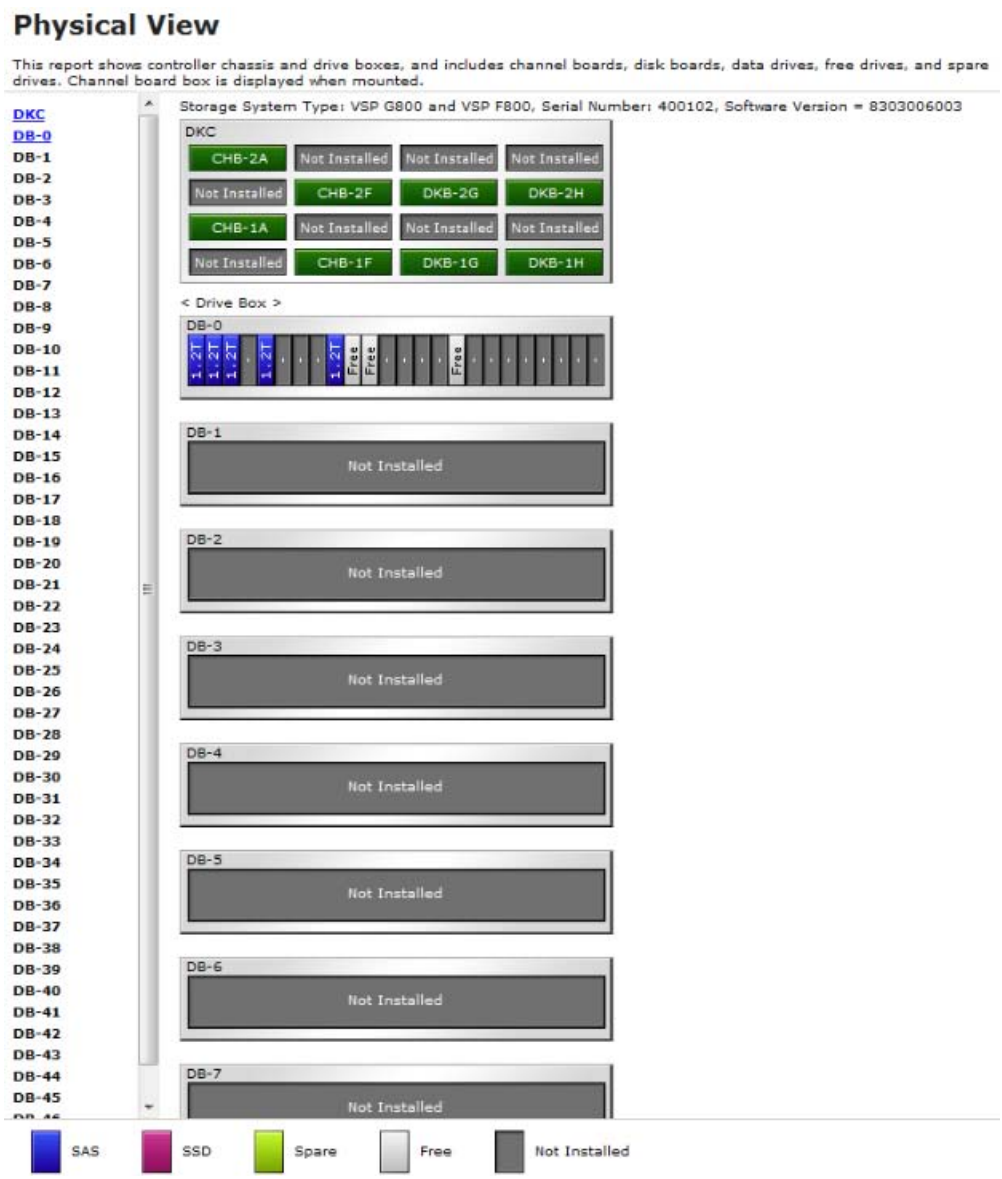



**Figure 19 Physical View report (VSP G800, VSP F800)**

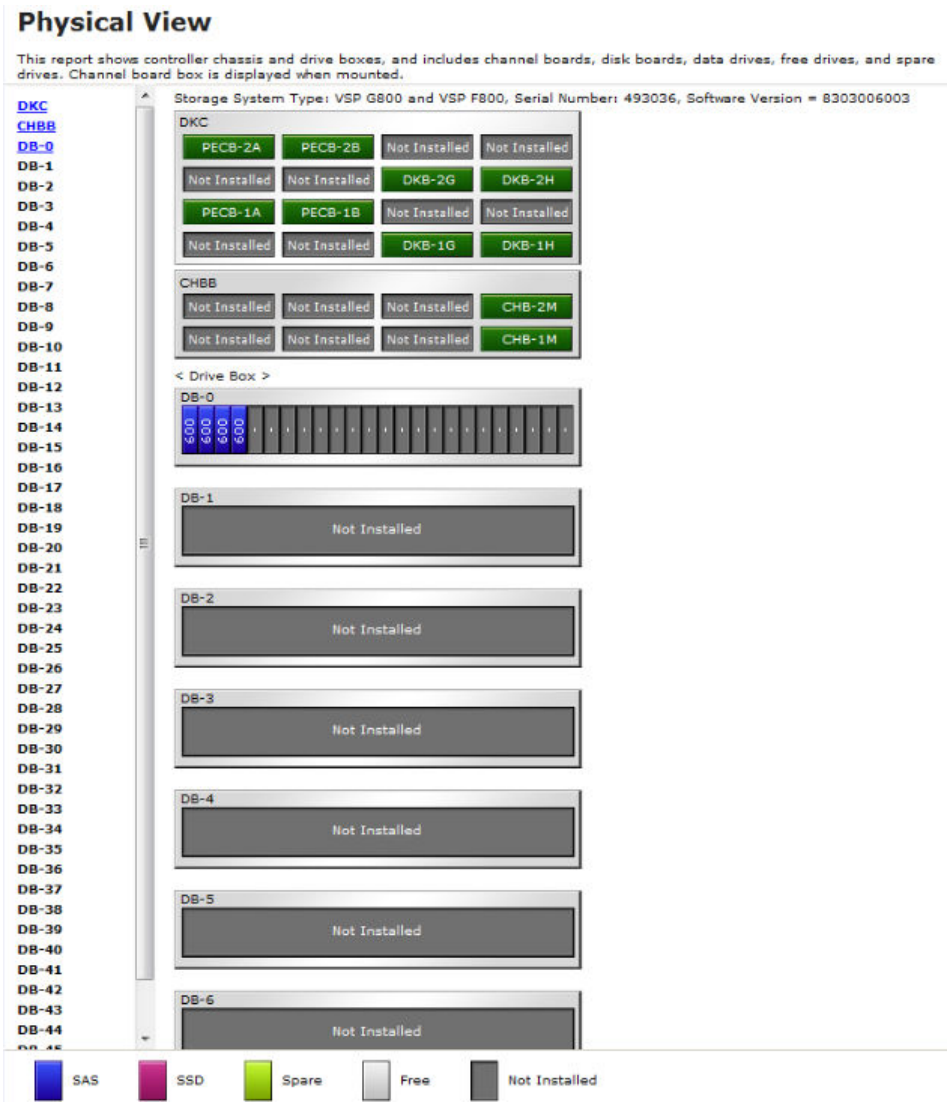



**Figure 20 Physical View report (when a channel board box is connected)**

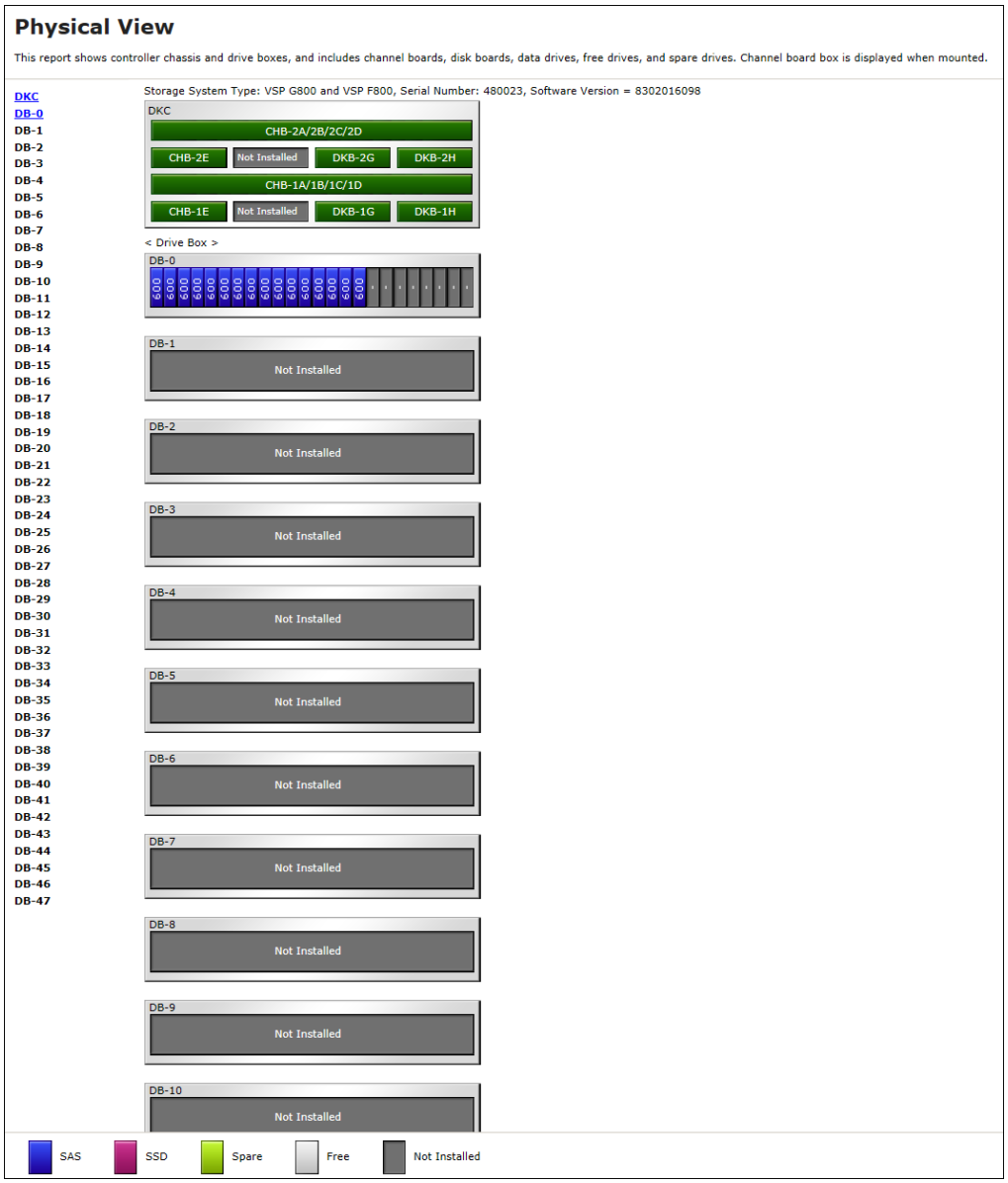



**Figure 21 Physical View report (when a NAS module is mounted)**

# 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.

**Table 15 CacheInfo.csv file (Title: <<Cache>>)**

| Item | Content |
|---|---|
| Location | Name of the cache controller board on which the memory is installed |
| CMG#0 Size (GB)<br>CMG#1 Size (GB) | Cache memory capacity in the controller board per CMG (16/32/64/128/ blank). The number of CMG differs by model and the displayed items are different.<br>▪ VSP G200: Only CMG#0 Size displays<br>▪ VSP G400, G600, G800 or VSP F400, F600, F800: CMG#0 Size and CMG#1 Size display<br>Depending on the installed number of the cache memory (DIMM), one of the CMG capacities might be blank for VSP G400, G600, G800 or VSP F400, F600, F800. |
| Cache Size (GB) | Total cache memory capacity on the controller board (0 to 256) |
| SM Size (MB) | The capacity that cannot be used as data cache memory in the total cache memory capacity inside of the controller board.<br>The capacity per cluster is displayed.<br>Includes the shared memory capacity, cache directory capacity, and the fixed capacity.<br>Fixed capacity is the cache memory capacity that is used for controlling the storage system with the controller board.<br>▪ VSP G200: (0 to 18944)<br>▪ VSP G400, G600 or VSP F400, F600: (0 to 37888)<br>▪ VSP G800 or VSP F800: (0 to 47744) |
| CFM#0 Type<br>CFM#1 Type | Type of CFM in the cluster (BM 10/BM 20/BM 30/blank). The number of CFM differs by model and the number of the displayed items are different.<br>▪ VSP G200: CFM#0 type only<br>▪ VSP G400, G600, G800 or VSP F400, F600, F800: CFM #0 Type or CFM#1 Type<br>Depending on the installed CFM number, one of the CFM types might be displayed as blank.<br>Information about the NAS module is not displayed in this CSV file. |

| Item | Content |
|---|---|
| Unified Hypervisor Cache Size (GB) | The cache memory capacity (blank/16/32/64) (Unit: GB) assigned for Unified Hypervisor usage within the total cache memory capacity in controller board.<br>▪ Blank if Unified Mode of DkcInfo.csv is Off.<br>This item is not displayed for VSP G200. |

## 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. Information about the NAS module is not displayed in this CSV file.

**Table 16 ChapUserInfo.csv file Title: <<CHAP User Information>>)**

| 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) |
| Notes:<br>**1.** If the character string contains a comma, the comma is converted to a tab.<br>**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.

**Table 17 ChaStatus.csv file (Title: <<CHB Status>>)**

| Item | Content |
|---|---|
| CHB Location | CHB name (CHB-1A/1B/1C/1D or CHB-2A/2B/2C/2D if Package Type is NAS module) |
| PCB Status | Status of this CHB[1] (Blank if CHB location is CHB-1A/1B/1C/1D or CHB-2A/2B/2C/2D in NAS module) |
| Port#00, #01, ..., #03 | Status of ports on this CHB (Blank if CHB location is CHB-1A/1B/1C/1D or CHB-2A/2B/2C/2D in NAS module) |

| Item | Content |
|---|---|
| **Notes:**<br>**1.** 1 Normal, 0: Abnormal | |

## DeviceEquipInfo.csv

This CSV file contains information about equipment and devices that are part of the storage system, including power supplies and batteries for DKC, DB, and CHBB. A record is created for each device.

**Table 18 DeviceEquipInfo.csv file (Title: <<Device Equipment Information>>)**

| Item | Content |
|---|---|
| Device Location | Device location name. For example:<br>▪ For DKCPS: DKCPS-00<br>▪ For DKUPS: DKUPS000-1<br>▪ For Battery: BATTERY-1BA<br>▪ For SVP: SVP-BASIC |
| Equip Status | Equipment status of the device:<br>▪ Equipped<br>▪ Not Equipped |
| Status | Status of the device:<br>▪ Normal<br>▪ Abnormal<br>▪ Blank if "Equip Status" is Not Equipped |

## DkaInfo.csv

This CSV file contains information about disk boards (DKBs). A record is created for each DKB.

**Table 19 DkaInfo.csv file (Title: <<DKB Information>>)**

| Item | Content |
|---|---|
| DKB Location | DKB name |

| Item | Content |
|---|---|
| Package Type | DKB type<br>Output example:<br>▪ Unecryption DKB (2Port)<br>▪ Encryption EDKB (2Port) |

## DkaStatus.csv

This CSV file contains information about the status of disk boards (DKBs). A record is created for each DKB.

**Table 20 DkaStatus.csv file (Title: <<DKB Status>>)**

| Item | Content |
|---|---|
| DKB Location | DKB name |
| PCB Status | Status of this DKB[1] |
| BECON#00 | Status of BECON[1] |
| BEPORT#0000 to #0001 | Status of BEPORT on this DKB[1]<br>Items are output in the format BEPORT#*XXYY*, where:<br>▪ *XX*: BE controller number (2-digit hexadecimal)<br>▪ *YY*: BE port number (2-digit hexadecimal) |
| Notes:<br>**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.

**Table 21 DkcInfo.csv file (Title: <<DKC Information>>)**

| Item | Content |
|---|---|
| Storage System Type | Storage system type.<br>Output example:<br>▪ G200[1]<br>▪ VSP G400, G600 and VSP F400, F600[2]<br>▪ VSP G800 and VSP F800[3] |

| Item | Content |
|---|---|
| Serial Number # | Serial product number (decimal, from 400001 to 499999) |
| IP Address | IP address<br>Output example: xxx.xxx.xxx.xxx (decimal, 0 to 255) |
| Subnet Mask | Subnet mask<br>Output example: xxx.xxx.xxx.xxx (decimal, 0 to 255) |
| Number of CUs | Number of CUs (decimal, 0 to 64) |
| Number of DKBs | Number of DKBs (decimal, 0 to 8)<br>Zero (0) is sometimes displayed if an HDD is not installed. |
| Configuration Type | Configuration type<br>Output example: PCM |
| Model | Storage system model: S, M, or H |
| Unified Mode | Unified Mode of the storage system.<br>▪ On: Operating with Unified Mode<br>▪ Off: Not operating with Unified Mode<br>This item is not displayed for VSP G200. |

Notes:

- To determine if the model type is VSP G200, see PpInfo.csv (on page 282) .
  - VSP G200: Install is Enabled for Model upgrade license
- To determine whether the model type is VSP G400, VSP F400, VSP G600, or VSP F600, see PpInfo.csv (on page 282) .
  - VSP G400: Install is Disabled for both Model upgrade license and All Flash Array
  - VSP F400: Install is Disabled for Model upgrade license and Install is Enabled for All Flash Array
  - VSP G600: Install is Enabled for Model upgrade license and Install is Disabled for All Flash Array
  - VSP F600: Install is Enabled for both Model upgrade license and All Flash Array
- To determine whether the model type is VSP G800 or VSP F800, see PpInfo.csv (on page 282) .
  - VSP G800: Install is Disabled for All Flash Array
  - VSP F800: Install is Enabled for All Flash Array

## 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 total number of items depends on the model (VSP G200: 17, VSP G400/VSP G600/VSP F400/VSP F600: 49, VSP G800/VSP F800: 97).

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.

**Table 22 DkuTempAveInfo.csv file (Title: <<DB temperature average Information>>)**

| Item | Description |
|---|---|
| Date | Year, month, and date when temperature data was acquired in the format:<br>*YYYY/MM/DD hh:mm:ss* |
| DB00 DBPS001<br>Temperature average | Average temperature (°C) for the two-hour period of DB00 DBPS001 |
| DB47 DBPS472<br>Temperature average | Average temperature (°C) for the two-hour period of DB47 DBPS472<br>For VSP G200, item shows up to DB07 DBPS072.<br>For VSP G400, VSP G600, VSP F400, VSP F600, item shows up to DB23 DBPS232. |

**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 248) 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 total number of items depends on the model (VSP G200: 49, VSP G400/ VSP G600/VSP F400/VSP F600: 145, VSP G800, VSP F800: 289).

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.

**Table 23 DkuTempInfo.csv file (Title: <<DB temperature Information>>)**

| Item | Description |
|---|---|
| Date | Year, month, and date when temperature data was acquired in the format:<br>*YYYY*/*MM*/*DD hh*:*mm*:*ss* |
| DB00 DBPS001<br>Temperature average | Average temperature (°C) for the two-hour period of DB00 DBPS001 |
| DB00 DBPS001<br>Temperature maximum value | Maximum temperature (°C) for the two-hour period of DB00 DBPS001 |
| DB00 DBPS001<br>Temperature minimum value | Minimum temperature (°C) for the two-hour period of DB00 DBPS001 |
| DB47 DBPS472<br>Temperature average | Average temperature (°C) for the two-hour period of DB47 DBPS472<br>For VSP G200, item shows up to DB07 DBPS072.<br>For VSP G400, VSP G600, VSP F400, VSP F600, item shows up to DB23 DBPS232. |
| DB47 DBPS472<br>Temperature maximum value | Maximum temperature (°C) for the two-hour period of DB47 DBPS472<br>For VSP G200, item shows up to DB07 DBPS072.<br>For VSP G400, VSP G600, VSP F400, VSP F600, item shows up to DB23 DBPS232. |
| DB47 DBPS472<br>Temperature minimum value | Minimum temperature (°C) for the two-hour period of DB47 DBPS472<br>For VSP G200, item shows up to DB07 DBPS072.<br>For VSP G400, VSP G600, VSP F400, VSP F600, item shows up to DB23 DBPS232. |

***Note:** An item name is displayed as DB*xx* DBPS*xxy*. The names are listed in ascending order of the DB number.

The following tables list DB*xx* and DBPS*xxy*: *xx* values, where *xx* is a value from 00 to 07 (VSP G200), 00 to 23 (VSP G400, G600, VSP F400, VSP F600), or 00 to 47 (VSP G800, VSP F800).

| DB # | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| *xx* | 00 | 01 | 02 | 03 | 04 | 04 |
| DB*xx* | DB00 | DB01 | DB02 | DB03 | DB04 | DB05 |
| DB*xxy* | DBPS00y | DBPS01y | DBPS02y | DBPS03y | DBPS04y | DBPS05y |

| DB # | 42 | 43 | 44 | 45 | 46 | 47 |
|---|---|---|---|---|---|---|
| *xx* | 42 | 43 | 44 | 45 | 46 | 47 |
| DB*xx* | DB42 | DB43 | DB44 | DB45 | DB46 | DB47 |
| DB*xxy* | DBPS42y | DBPS43y | DBPS44y | DBPS45y | 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 total number of items depends on the following model:

- VSP G200: 17
- VSP G400/VSP G600/VSP F400/VSP F600: 49
- VSP G800/VSP F800: 97

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.

**Table 24 DkuTempMaxInfo.csv file (Title: <<DB temperature maximum value Information>>)**

| Item | Description |
|---|---|
| Date | Year, month, and date when temperature data was acquired in the format:<br>*YYYY*/*MM*/*DD hh*:*mm*:*ss* |
| DB00 DBPS001<br>Temperature maximum value | Maximum temperature (°C) for the two-hour period of DB00 DBPS001 |
| DB47 DBPS472<br>Temperature maximum value | Maximum temperature (°C) for the two-hour period of DB47 DBPS472<br>For VSP G200, item shows up to DB07 DBPS072.<br>For VSP G400, VSP G600, VSP F400, VSP F600, item shows up to DB23 DBPS232. |

**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 248) for locations and values for DB*xx* and DBPS*xxy.*

## 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 total number of items depends on the following model:

- VSP G200: 17
- VSP G400/VSP G600/VSP F400/VSP F600: 49
- VSP G800/VSP F800: 97

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.

**Table 26 DkuTempMinInfo.csv file (Title: <<DB temperature minimum value Information>>)**

| Item | Description |
|---|---|
| Date | Year, month, and date when temperature data was acquired in the format:<br>*YYYY*/*MM*/*DD hh*:*mm*:*ss* |
| DB00 DBPS001<br>Temperature minimum value | Minimum temperature (°C) for the two-hour period of DB00 DBPS001 |
| DB47 DBPS472<br>Temperature minimum value | Minimum temperature (°C) for the two-hour period of DB47 DBPS472<br>For VSP G200, item shows up to DB07 DBPS072.<br>For VSP G400, VSP G600, VSP F400, VSP F600, item shows up to DB23 DBPS232. |

## ELunInfo.csv

This CSV file contains information about external volumes. Information about one external volume is output to multiple records according to the number of prioritized paths between the local and the external storage systems.

For details of external volumes, see *Hitachi Universal Volume Manager User Guide*. Information about the NAS module is not displayed in this CSV file.

**Table 27 ELunInfo.csv file (Title: <<External LUN Information>>)**

| Item | Content |
|---|---|
| VDEV# | Virtual device number to which the external volume is mapped |
| Characteristic1 | Identification number of the external volume[1] |
| Characteristic2 | Extended information for identifying the external volume |
| Device | Product name reported to the host by the external volume[1] |
| 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<br>▪ Enabled: Asynchronously<br>▪ Disabled: Synchronously |

| Item | Content |
|---|---|
| ECC Group | Number of parity group to which the external volume is mapped.<br>If the number starts with "E" (for example, E1-1), the parity group contains external volumes.<br>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<br>▪ MPU-10<br>▪ MPU-11<br>▪ MPU-20<br>▪ MPU-21 |
| Setting MPU | Number and name of an MP unit configured to control the external volume indicated by ECC Group<br>▪ MPU-10<br>▪ MPU-11<br>▪ MPU-20<br>▪ MPU-21 |
| Vendor | Vendor name of the external storage system |
| Product Name | Product name of the external storage system |
| Serial Number# | Serial product number of the external storage system |
| Path Mode | Mode which indicates how the paths between local and external storage systems operate<br>▪ Multi<br>▪ Single<br>▪ 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<br>Blank if "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.<br>"1" indicates the path of the highest priority. |

| Item | Content |
|---|---|
| Status | Status of the path between storage systems.<br>▪ Normal<br>▪ Blocked |
| IO TOV | I/O timeout value for the external volume<br>Range of values: 5 to 240 |
| QDepth | The number of Read/Write commands that can be issued to the external volume at a time<br>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)<br>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<br>▪ Normal Round-robin<br>▪ Extended Round-robin<br>▪ Disabled<br>A hyphen is displayed if Single is specified in Path Mode |
| Path Mode on Profile | Path mode on profile information of the external storage system:<br>▪ Multi<br>▪ Single |
| ALUA Settable | Indicates whether ALUA mode can be set as path mode on the external storage system<br>▪ Yes: ALUA mode can be set<br>▪ No: ALUA mode cannot be set |
| ALUA Permitted | Indicates whether ALUA is used as path mode on the local storage system:<br>▪ Enabled: ALUA mode is used<br>▪ 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:<br>▪ Active/Optimized<br>▪ Active/Non-Optimized |

| Item | Content |
|---|---|
| Package Type | Type of CHB to which a port of the local storage system connecting to the external storage system belongs<br>▪ Fibre: 8FC4 (CHB), 16FC2 (CHB), 32FC4R (CHB)<br>▪ iSCSI: 10iSCSI2o (CHB), 10iSCSI2c (CHB) |
| IP Address | IP address for an iSCSI target of an external storage system<br>▪ IPv6:<br>*XXXX*:*XXXX*:*XXXX*:*XXXX*:*XXXX*:*XXXX*:*XXXX*:*XXXX* (hexadecimal)<br>▪ IPv4:<br>*XXX*.*XXX*.*XXX*.*XXX* (decimal)<br>▪ Blank if "Package Type" is iSCSI. |
| TCP Port Number | TCP port number (1 through 65535) for the iSCSI target of an external storage system<br>Blank if "Package Type" is Fibre. |
| iSCSI Target Name | iSCSI target name of an external storage system<br>Blank if "Package Type" is Fibre. |
| **Notes:**<br>**1.** If the character string contains a comma, the comma is converted to a tab. | |

## 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 two hours.

No records are created during a system power failure or if the breakers are turned off. If the system is in maintenance mode or the SVP is rebooted, up to two hours of records could be lost.

If a failure occurs in the storage system, the correct information might not be output.

**Table 28 EnvMonInfo.csv file (Title: <<Electric power and temperature Information>>)**

| Item | Description |
|---|---|
| Date | Year, month, and date when record data was acquired for the two-hour period in the format:<br>*YYYY*/*MM*/*DD HH*:*MM*:*SS* |
| Electric power average | Average value of electric power (W) |

| Item | Description |
|---|---|
| Electric power maximum value | Maximum value of electric power (W) |
| Electric power minimum value | Minimum value of electric power (W)<br>In the following cases, a lower value might be temporarily displayed:<br>▪ When the storage system is starting up<br>▪ Right after replacing storage system parts<br>▪ During or after microcode update |
| DKC0 CL1 Temperature average | DKC0: Average temperature of CL1 (°C) |
| DKC0 CL1 Temperature maximum value | DKC0: Maximum temperature of CL1 (°C) |
| DKC0 CL1 Temperature minimum value | DKC0: Minimum temperature of CL1 (°C) |
| DKC0 CL2 Temperature average | DKC0: Average temperature of CL2 (°C) |
| DKC0 CL2 Temperature maximum value | DKC0: Maximum temperature of CL2 (°C) |
| DKC0 CL2 Temperature minimum value | DKC0: Minimum temperature of CL2 (°C) |

## FcSpNameInfo.csv

This CSV file contains information about Fibre Channel Security Protocols (FCSPs). A record is created for each initiator (host).

For details of port setting, see the *Provisioning Guide*. Information about the NAS module is not displayed in this CSV file.

**Table 29 FcSpNameInfo.csv file (Title: <<FC-SP Name Information>>)**

| Item | Content |
|---|---|
| Port | Port name |
| Host Group | Host group name |
| Target Username | WWN information about the storage system required for authentication (16-digit hexadecimal number) |

| Item | Content |
|---|---|
| Authentication of Group | Information about whether to perform authentication or not<br>▪ Enabled<br>▪ Disabled |
| Initiator Username | WWN information about the host required for authentication (16-digit hexadecimal number) |
| Protocol | Protocol used for authentication ("CHAP" or blank) |

## FcSpPortInfo.csv

This CSV file contains information about ports related to Fibre Channel Security Protocols (FCSPs). A record is created for each port.

For details of port setting, see the *Provisioning Guide*. Information about the NAS module is not displayed in this CSV file.

**Table 30 FcSpPortInfo.csv file (Title: <<FC-SP Port Information>>)**

| Item | Content |
|---|---|
| Port | Port name |
| Time out(Sec) | Time interval (in seconds) before retrying authentication in case of failure in authentication |
| Refusal Intvl.(Min) | Time interval (in minutes) before starting next authentication in case of failure in authentication for the number of times displayed by "Refusal Freq(Counts)" |
| Refusal Freq.(Counts) | Number of times of authentication allowable for connection to a port |
| Switch Port Username | WWN information about the Fabric switch required for authentication (16-digit hexadecimal number) |
| Mode | Mode of authentication between ports and FC switches<br>▪ Bidirectional<br>▪ Unidirectional |
| Authentication of Fabric Switch | Information about whether to perform authentication of the FC switch identified by "Switch Port Username"<br>▪ Enabled<br>▪ Disabled |

## HduInfo.csv

This CSV file contains information about hard drive boxes (DB). A record is created for each drive box.

**Table 31 DBInfo.csv file (Title: <<DB Information>>)**

| Item | Description |
|---|---|
| DB Location | DB location name |
| DB Status | Information about whether this DB is installed<br>▪ Installed<br>▪ Not installed |
| Slot Size | Slot size (inches)<br>▪ 2.5<br>▪ 3.5<br>▪ Blank for DBF (FMC and FMD). |
| DB Type | DB type<br>▪ DBS (DB for 2.5-inch drives)<br>▪ DBL (DB for 3.5-inch drives)<br>▪ DB60 (dense drive box for 3.5-inch drives)<br>▪ DBF (DB for FMC and FMD, 2PORT) |

## 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. Information about the NAS module is not displayed in this CSV file.

**Table 32 IscsiHostInfo.csv file (Title: <<iSCSI Host Information>>)**

| 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. Information about the NAS module is not displayed in this CSV file.

**Table 33 IscsiPortInfo.csv file (Title: <<iSCSI Port Information>>)**

| Item | Content |
|---|---|
| Port | Port name |
| IPv4 \| IP Address | IPv4 address<br>Output example: *xxx.xxx.xxx.xxx* (decimal) |
| IPv4 \| Subnet Mask | IPv4 subnet mask (decimal)<br>Output example: *xxx.xxx.xxx.xxx* (decimal) |
| IPv4 \| Default Gateway | Port IPv4 default gateway<br>Output example: *xxx.xxx.xxx.xxx* (decimal) |
| IPv6 \| Mode | Port IPv6 settings<br>▪ Enabled<br>▪ Disabled |
| IPv6 \| Link Local Address | Port IPv6 link local address<br>▪ Output example: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal)<br>▪ Output example: Auto<br>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<br>▪ Output example: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal)<br>▪ Output example: Auto<br>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<br>▪ Output example: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal)<br>Blank if "IPv6 \| Mode" is Disabled. |
| Channel Speed | Data transfer speed of the port (10 Gbps) |
| Security Switch | Port security switch settings<br>▪ On<br>▪ Off |

| Item | Content |
|---|---|
| TCP Port Number | The number of the port for using socket (1 to 65535) |
| Ethernet MTU Size (Byte) \| MTU | MTU settings<br>▪ 1500<br>▪ 4500<br>▪ 9000 |
| Keep Alive Timer (sec.) | Keep alive timer value of iSCSI (30 to 64800) (sec) |
| Selective ACK | Selective ACK mode<br>▪ Enabled<br>▪ Disabled |
| Delayed ACK | Delayed ACK mode<br>▪ Enabled<br>▪ Disabled |
| Maximum Window Size (KB) | Window scale option settings<br>▪ 64KB<br>▪ 128KB<br>▪ 256KB<br>▪ 512KB<br>▪ 1024KB |
| iSNS Server \| Mode | iSNS mode settings<br>▪ On<br>▪ Off |
| iSNS Server \| IP Address | IP address of the iSNS server<br>▪ IPv4: *xxx.xxx.xxx.xxx* (decimal)<br>▪ IPv6: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal)<br>▪ Blank if "iSNS Server \| Mode" is Off. |
| iSNS Server \| TCP Port Number | Port number of TCP used for iSNS (1 to 65535).<br>Blank if "iSNS Server \| Mode" is Off. |
| VLAN \| Tagging Mode | VLAN tagging mode set to the port<br>▪ On<br>▪ Off |

| Item | Content |
|---|---|
| VLAN \| ID | VLAN number set to the port (1 to 4094)<br>Blank if "VLAN \| Tagging Mode" is set to Off. |
| 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<br>▪ Output example: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal)<br>▪ Output example: Auto<br>Auto is displayed if the global address 2 is automatically set. Blank if "IPv6 \| Mode" is 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. Information about the NAS module is not displayed in this CSV file.

**Table 34 IscsiTargetInfo.csv file (Title: <<iSCSI Target Information>>)**

| 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 (0 to 127, decimal)<br>Separated with a semicolon (;) if multiple host mode options are set. |
| Security Switch | Security switch status set to the iSCSI target port<br>▪ On<br>▪ Off |

| Item | Content |
|---|---|
| Authentication \| Method | Authentication method settings of the iSCSI target<br>▪ CHAP<br>▪ None<br>▪ Comply with Host Setting |
| Authentication \| Mutual CHAP | Mutual CHAP authentication function settings of the iSCSI target<br>▪ Enabled<br>▪ 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.

**Table 35 JnlInfo.cvs file (Title: <<JNL Information>>)**

| Item | Content |
|---|---|
| JNL# | Journal number (in hexadecimal) |
| Current MPU | Number and name of MP unit currently controlling the journal<br>(MPU-10, MPU-11, MPU-20, MPU-21) |
| Setting MPU | Number and name of MP unit configured to control the journal<br>(MPU-10, MPU-11, MPU-20, MPU-21) |

## LdevCapaInfo.csv

This CSV file contains information about LDEV capacities. A record is created for each of the classifications shown in "Volume Kind".

**Table 36 LdevCapaInfo.csv file (Title: <<LDEV Capacity Information>>)**

| Item | Content |
|---|---|
| Volume Kind | The following classifications are output:<br>▪ Internal OPEN Volumes<br>▪ External OPEN Volumes<br>▪ 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<br>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".

**Table 37 LdevCountInfo.csv file (Title: <<LDEV Count Information>>)**

| Item | Content |
|---|---|
| Volume Kind | The following classifications are output:<br>▪ Internal Volumes<br>▪ External Volumes<br>▪ Total Volumes |
| Allocated OPEN LDEVs | The number of allocated open-system volumes (LDEVs). |
| Unallocated OPEN LDEVs | The number of unallocated open-system volumes (LDEVs). |
| Reserved OPEN LDEVs | The number of reserved open-system volumes (LDEVs). |
| V-VOL | The number of virtual volumes.<br>Output only when "Volume Kind" is Total Volumes. |
| Total(All LDEVs) | Total number of LDEVs. |

| Item | Content |
|---|---|
| ECC Groups | Total number of parity groups. |

## LdevInfo.csv

This CSV file contains information about logical devices (LDEVs). A record is created for each LDEV.

For details of LDEVs, see the *Provisioning Guide*.

**Table 38 Ldevinfo.csv file (Title: <<LDEV Status>>)**

| Item | Content |
|---|---|
| ECC Group | Number of parity group where the LDEV belongs.<br>Output example: *X-Y* (decimals)<br>▪ If the number starts with "E" (for example, E1-1), the parity group contains external volumes.<br>▪ If "LDEV Type" is Dynamic Provisioning or Thin Image, a hyphen is output. |
| LDEV# | LDEV number<br>(00:00:00 to 00:3f:ff) |
| LDEV Name | LDEV name[1] |
| LDEV Emulation | LDEV emulation type |
| LDEV Type | LDEV type:<br>▪ Basic<br>▪ Dynamic Provisioning<br>▪ External<br>▪ Thin Image<br>▪ ALU |

| Item | Content |
|---|---|
| LDEV Attribute | LDEV Attribute:<br>▪ CMDDEV (Command device)<br>▪ CMDDEV[1] (Remote command device)<br>▪ Journal (Journal volume)<br>▪ Pool (Pool volume)<br>▪ Quorum disk (used with global-active device)<br>▪ ALU<br>▪ SLU<br>▪ Deduplication system data volume<br>▪ Regular (Others) |
| Volume Size(Cyl) | LDEV capacity (in cylinders) |
| Volume Size(MB) | LDEV capacity (in MB) |
| Volume Size(Blocks) | LDEV capacity (in blocks) |
| CVS | Information about whether the LDEV is a custom-sized volume:<br>▪ On: Custom-sized volume<br>▪ Off: Others |
| Pool ID | Pool number. This is blank except for the following cases:<br>▪ If "LDEV Type" is Dynamic Provisioning<br>▪ 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. |
| ORACLE CHECK SUM | Information about whether this LDEV is an Oracle check sum target.<br>▪ On<br>▪ Off |
| Current MPU | Number of the MP unit currently controlling the LDEV.<br>(MPU-10, MPU-11, MPU-20, MPU-21) |

| Item | Content |
|---|---|
| Setting MPU | Number of the MP unit configured to control LDEV.<br>(MPU-10, MPU-11, MPU-20, MPU-21) |
| Allocated | Information about whether this LDEV is allocated to a host.<br>▪ "Y" is output for volumes accessible to the host. |
| Pool Name | The pool's name[1]<br>▪ If the provisioning type is Dynamic Provisioning, the name of the pool related to the logical volume is displayed.<br>▪ If the attribute is Pool, the name of the pool where the logical volume belongs is displayed.<br>▪ When neither of the above are displayed, the pool name is blank. |
| CmdDevSecurity | Indicates whether Security is specified as the attribute for the command device.<br>▪ Enabled: Command device security setting is set.<br>▪ Disabled: Command device security setting is not set.<br>▪ Blank: "LDEV Attribute" is not CMDDEV. |
| CmdDevUserAuth | Indicates whether User Authentication is specified as the attribute for the command device.<br>▪ Enabled: User authentication setting is set.<br>▪ Disabled: User authentication setting is not set.<br>▪ Blank: "LDEV Attribute" is not CMDDEV. |
| CmdDevDevGrpDef | Indicates whether Device Group Definition is specified as the attribute for the command device.<br>▪ Enabled: Device group definition setting is set.<br>▪ Disabled: Device group definition setting is not set.<br>▪ 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.<br>▪ For internal volumes: Enabled (encrypted) or Disabled (not encrypted)<br>▪ For external volumes: blank |

| Item | Content |
|---|---|
| T10 PI | Indicates the T10 PI attribute set for the LDEV.<br>▪ Enabled<br>▪ Disabled<br>▪ Blank if "LDEV Emulation" is not OPEN-V. |
| ALUA Mode | Indicates whether the ALUA mode is enabled.<br>▪ Enabled: ALUA mode is enabled.<br>▪ Disabled: ALUA mode is disabled. |
| Accelerated Compression | Indicates whether accelerated compression is enabled.<br>For internal volumes:<br>▪ Enabled: accelerated compression is enabled.<br>▪ Disabled: accelerated compression is disabled.<br>If the parity group with LDEV does not support accelerated compression, a blank space is displayed. Also, for external volumes, a blank is displayed. |
| **Notes:**<br>**1.** If the character string contains a comma, the comma is converted to a tab. | |

## LdevStatus.csv

This CSV file contains information about the status of logical devices (LDEVs). A record is created for each LDEV.

**Table 39 LdevStatus.csv file (Title: <<LDEV Status>>)**

| Item | Content |
|---|---|
| VDEV# | Virtual device number in which the LDEV is defined |
| VDEV Status | VDEV status of "VDEV#"<br>▪ 1: Normal<br>▪ 0: Abnormal |
| HDEV# | LDEV number |
| HDEV Status | LDEV status<br>▪ 1: Normal<br>▪ 0: Abnormal |
| LDEV Emulation | LDEV emulation type |

| Item | Content |
|---|---|
| ECC Group | Number of the parity group where the LDEV belongs.<br>▪ If the number starts with "E" (for example, E1-1), the parity group contains external volumes.<br>▪ If the type of the LDEV is a Dynamic Provisioning or Thin Image virtual volume, a hyphen is output.<br>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 of the cache logical partitioning function, see the *Performance Guide*.

**Table 40 LPartition.csv file (Title: <<Logical Partitioning>>)**

| 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.<br>▪ If the number starts with "E" (for example, E1-1), the parity group contains external volumes.<br>▪ If the type of the LDEV is a Dynamic Provisioning or Thin Image virtual volume, a hyphen is output.<br>Refer to "LdevInfo.csv" for information about the LDEV type. |
| LDEV#(V-VOL) | LDEV number allocated to this CLPR.<br>▪ VSP G200: (00:00:00 to 00:07:ff)<br>▪ VSP G400, G600 or VSP F400, F600: (00:00:00 to 00:0f:ff)<br>▪ VSP G800 or VSP F800: (00:00:00 to 00:3f:ff)<br>The type of this LDEV is Dynamic Provisioning, Thin Image, or ALU. |

## LunInfo.csv

This CSV file contains information about LU path definitions. A record is created for each host group. For more information about LU path definitions, see the *Provisioning Guide*.

**Table 41 LunInfo.csv file (Title: <<LUN Information>>)**

| Item | Description |
|---|---|
| Port | Port name |
| Host Group | Host group name<br>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 (0 to 127, hexadecimal)<br>If more than one option is specified, the options are separated by semicolons (;). |
| LUN# | LUN number for this LU path definition (hexadecimal) |
| LDEV# | LDEV number for this LU path definition |
| Command Device | Information about whether the LDEV is a command device:<br>▪ On: Command Device<br>▪ On*: Remote Command Device<br>▪ Off: Others |
| Command Security | Information about whether the command device is secured:<br>▪ On<br>▪ Off |
| CVS | Information about whether the LDEV is a custom-sized volume:<br>▪ On: Customized volume<br>▪ Off: Other volumes |
| CHB Location | Name of the CHB on which this port is installed<br>CHB-1A/1B/1C/1D or CHB-2A/2B/2C/2D if Package Type is NAS module. |
| Package Type | CHB type for CHB Location:<br>▪ Fibre:<br>• `8FC4 (CHB)`<br>• `16FC2 (CHB)`<br>• `32FC4R (CHB)`<br>▪ iSCSI:<br>• `10iSCSI2o (CHB)`<br>• `10iSCSI2c (CHB)`<br>▪ NAS module:<br>• `NAS module (CHB)` |

| Item | Description |
|---|---|
| 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.<br>▪ Enabled<br>▪ Disabled<br>▪ Blank if "Package Type" is not 16FC2 (CHB) or 32FC4R (CHB). |
| T10 PI | Information about the T10 PI attribute which is set for the LDEV number of the LU path definition.<br>▪ Enabled<br>▪ Disabled<br>▪ Blank if LDEV# is blank |
| Asymmetric Access State | Asymmetric access status (output only for an open system CHA that is Fibre or FCoE)<br>Indicates the asymmetric access status:<br>▪ Active/Optimized: Prioritized<br>▪ Active/Non-Optimized: Lower priority<br>Blank if "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*.

**Table 42 LunPortInfo.csv file (Title: <<LUN Port Information>>)**

| Item | Content |
|---|---|
| Port | Port name. |
| Security Switch | The setting status of the security switch:<br>▪ On<br>▪ Off<br>▪ Blank if "Package Type" is NAS module |

| Item | Content |
|---|---|
| Port Address | Port address (2-digit hexadecimal number)<br>Blank if "Package Type" is iSCSI or NAS module |
| Loop ID | Port address (0 - 125, decimal)<br>Blank if "Package Type" is iSCSI or NAS module |
| Fabric | One of the Fibre topology settings indicating the setting status of the Fabric switch:<br>▪ On<br>▪ Off<br>▪ Blank if "Package Type" is iSCSI or NAS module |
| Connection | One of the Fibre topology settings:<br>▪ Point to Point<br>▪ FC-AL<br>▪ Blank if "Package Type" is iSCSI or NAS module |
| Channel Speed | Channel Speed of this port<br>▪ 1 Gbps<br>▪ 2 Gbps<br>▪ 4 Gbps<br>▪ 8 Gbps<br>▪ 10 Gbps<br>▪ 16 Gbps<br>▪ 32 Gbps<br>▪ Auto<br>▪ Blank if "Package Type" is NAS module |
| WWN | WWN of this port (hexadecimal number)<br>Blank if "Package Type" is iSCSI or NAS module |
| CHB Location | CHB on which the port is installed. CHB-1A/1B/1C/1D or CHB-2A/2B/2C/2D if "Package Type" is NAS module. |

| Item | Content |
|---|---|
| Package Type | CHB type for CHB Location<br>▪ Fibre:<br>• 8FC4 (CHB)<br>• 16FC2 (CHB)<br>• 32FC4R (CHB)<br>▪ iSCSI:<br>• 10iSCSI2o (CHB)<br>• 10iSCSI2c (CHB)<br>▪ NAS module:<br>• NAS Module (CHB) |
| T10 PI Mode | Indicates whether the T10 PI mode can be applied to the port.<br>▪ Enabled<br>▪ Disabled<br>▪ Blank if "Package Type" is not 16FC2 (CHB) or 32FC4R (CHB) |

## MicroVersion.csv

This CSV file contains information about software versions.

**Table 43 MicroVersion.csv file (Title: <<Software Version>>)**

| 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)<br>HDD version in the format "(*HDD-device-type - code*):(*version*)".<br>If an HDD drive is not installed, only a colon is displayed. |
| Expander | Expander firmware version (6 digits) |
| CFM | CFM firmware version (8 digits) |
| DKB | DKB firmware version (6 digits) |
| Printout Tool | Printout tool version (xx-yy-zz-mm/aa) |

| Item | Content |
|---|---|
| CHB (FC16G) | 16G FC protocol chip firmware version (8 digits) |
| CHB (FC32G) | 32G FC protocol chip firmware version (8 digits) |
| CHB (iSCSI) | CHB(iSCSI) protocol chip firmware version (8 digits) |
| GUM | GUM firmware version (8 digits) |
| Unified Hypervisor | Unified Hypervisor version (8 digits)<br>▪ The version is displayed in each CL1, CL2.<br>▪ This item is not displayed in VSP G200. |
| NASFWINST | NASFWINST version (9 digits)<br>▪ The version is displayed in each CL1, CL2.<br>▪ This item is not displayed in VSP G200. |
| NASFW | NASFW version (9 digits)<br>▪ The version is displayed in each CL1, CL2.<br>▪ This item is not displayed in VSP G200. |

## MlcEnduranceInfo.csv

This CSV file contains information about endurance information of MLC. A record is created for each MLC endurance information.

If you change the SVP time 1 month or more, the history acquisition months will not be in order.

**Table 44 MlcEnduranceInfo.csv file (Title: <<MLC Endurance Information>>)**

| Item | Content |
|---|---|
| ECC Group | Number of parity group of which this MLC (including FMD and FMC) is a component<br>▪ If it is a spare drive, Spare Drive is displayed.<br>▪ If it is a free drive, Free Drive is displayed. |
| CR# | C# and R# (2-digit hexadecimal numbers), which identify the PDEV<br>Output in the format of "*XX*/*YY*"<br>*XX*: C#<br>*YY*: R# |
| Device Type-Code | Drive type code of this drive<br>Output example: SLR5A-M800SS |

| Item | Content |
|---|---|
| Used Endurance Indicator (%) | Current SSD life (0 to 100) |
| History1 (date) | Date on which SSD life was acquired (1 month ago)<br>Output example: *yyyy*/*mm*/*dd* |
| History1 (%) | SSD life (0 to 100)(1 month ago) |
| History2 (date) | Date on which SSD life was acquired (2 months ago)<br>Output example: *yyyy*/*mm*/*dd* |
| History2 (%) | SSD life (0 to 100) (2 months ago) |
| History3 (%) ... History 119 (%) | SSD life (0 to 100) (3 months ago ...119 months ago) |
| History120 (date) | Date on which SSD life was acquired (120 months ago) |
| History120 (%) | 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.

**Table 45 ModePerLpr.csv file (Title: <<System Option Mode Per LPR>>)**

| 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<br>▪ If the system option mode is on:<br>On<br>▪ If the system option mode is not on:<br>Blank |

## MpPathStatus.csv

This CSV file contains information about the status of logical paths. A record is created for each MP blade or LR.

**Table 46 MpPathStatus.csv file (Title: <<MP Path Status>>)**

| Item | Content |
|---|---|
| MPU#/CTL# | MP unit number or CTL number (2-digit hexadecimal number)<br>▪ For MP unit number<br>MPU#00 to MPU#03<br>The MPU#01 or MPU#03 line is blank if Unified Mode of DkcInfo.csv is On.<br>▪ For CTL number<br>CTL#00 to CTL#01 |
| CMG#00-00 to 01<br>CMG#01-00 to 01 | Path status[1] for the MP unit number with the cache module<br>(CMG#*XX-YY*) *XX*: I path, *YY*: CMG#<br>For VSP G200, CMG#00-00 to 01 only |
| MPU#00-00 to 03<br>MPU#01-00 to 03 | Path status[1] and the MP unit for the MP unit number<br>(MPU#*XX-YY*) *XX*: I path, *YY*: MPU#<br>The display in MPU#00-01, MPU#00-03, MPU#01-01, or MPU#01-03 is blank if Unified Mode of DkcInfo.csv is On.<br>For VSP G200, MPU#00-00 to 03 only |
| CMG#00-00 to 01<br>CMG#01-00 to 01 | Path status[1] with the cache module for the CTL number<br>(CMG#*XX-YY*) *XX*: I path, *YY*: CMG#<br>For VSP G200, CMG#00-00 to 01 only |
| MPU#00-00 to 03<br>MPU#01-00 to 03 | Path status[1] with the MP unit number for the CTL number<br>(MPU#*XX-YY*) *XX*: I path, *YY*: MPU#<br>For VSP G200, MPU#00-00 to 03 only<br>The display in MPU#00-01, MPU#00-03, MPU#01-01, or MPU#01-03 is blank if Unified Mode of DkcInfo.csv is On. |

**Note:**

**1.** 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.

**Table 47 MpPcbStatus.csv file (Title: <<MP PCB Status>>)**

| Item | Content |
|---|---|
| MPU ID | MP unit ID (MPU-10, MPU-11, MPU-20, MPU-21)<br>MPU-10 and MPU-20 are displayed if Unified Mode of DkcInfo.csv is On. |
| Auto Assignment | Information about whether this MP unit is set to be automatically assigned to each resource.<br>▪ Enabled: Set to be automatically assigned<br>▪ Disabled: Not set to be automatically assigned |
| PCB Status | MP unit status[1] |
| MP#00, #01,..., #07 | MP status[1]<br>The number of output items differs for each model, because the number of installed MPs is different.<br>▪ VSP G200: MP#00,01<br>▪ VSP G400, G600 or VSP F400, F600: MP#00, 01,..., 03<br>▪ VSP G800 or VSP F800: MP#00, 01,..., 07 |
| **Note:**<br>**1.** 1=Normal, 0=Abnormal | |

## 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.

**Table 48 PcbRevInfo.csv file (Title: <<PCB Revision Information>>)**

| Item | Content |
|---|---|
| Cluster# | Cluster number<br>▪ 1<br>▪ 2 |
| Location | Name of the part |
| 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 |

## 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".

**Table 49 PdevCapaInfo.csv file (Title: <<PDEV Capacity Information>>)**

| Item | Content |
|---|---|
| PDEV Kind | The following four classifications are output:<br>▪ OPEN System (TB)<br>▪ Total Capacity (TB)<br>▪ Number of PDEVs |
| SAS Drive | SAS 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.

**Table 50 PdevInfo.csv file (Title: <<PDEV>>)**

| Item | Content |
|---|---|
| ECC Group | Number of parity group of which this PDEV is a component.<br>▪ Spare Drive: For spare drives<br>▪ Free Drive: For free drives |
| Emulation Type | Emulation type for the parity group indicated by "ECC Group"<br>▪ Blank: "ECC Group" is Spare Drive.<br>▪ Free Drive: "ECC Group" is Free Drive. |
| CR# | C# and R# (2-digit hexadecimal numbers), which identify the PDEV<br>Output in the format *XX*/*YY*, where:<br>▪ *XX*: C#<br>▪ *YY*: R# |
| PDEV Location | PDEV location name |

| Item | Content |
|---|---|
| Device Type | Drive type<br>▪ SAS<br>▪ SSD |
| RPM | Revolutions per minute<br>Blank displays as RPM when the drive is SSD. |
| Device Type-Code | Device type code of this drive<br>Output example: DKR5D-J600SS |
| Device Size | Drive size (inches)<br>▪ 2.5<br>▪ 3.5<br>▪ Blank for DBF (FMC or FMD) |
| Device Capacity | Drive capacity (GB or TB) |
| Drive Version | Drive firmware version (4-digit hexadecimal number) |
| DKB1 | Name of the DKB1 controlling the PDEV |
| DKB2 | Name of the DKB2 controlling the PDEV |
| Serial Number # | Serial number of this drive (*yymm xxxxxx*), where:<br>▪ *yy* Year (last 2 digits)<br>▪ *mm* Month (2 digits)<br>▪ *xxxxxx*: Serial number of this drive |
| RAID Level | RAID level of the parity group indicated by "ECC Group"<br>Blank if the "ECC Group" is Spare Drive or Free Drive |
| RAID Concatenation #0 | Number of parity group to be concatenated to parity group (#0) identified by "ECC Group"[1] |
| RAID Concatenation #1 | Number of parity group to be concatenated to parity group (#1) identified by "ECC Group"[1] |
| RAID Concatenation #2 | Number of parity group to be concatenated to parity group (#2) identified by "ECC Group"[1] |
| Resource Group ID (ECC Group) | Resource group ID of parity group (0 to 1023, decimal number) |
| Resource Group Name (ECC Group) | Resource group name of parity group |

| Item | Content |
|---|---|
| Encryption | Encryption status of the parity group to which the PDEV belongs<br>▪ Enabled: Encryption enabled<br>▪ Disabled: Encryption disabled |
| Accelerated Compression | Accelerated compression setting.<br>▪ Enabled: accelerated compression is enabled.<br>▪ Disabled: accelerated compression is disabled.<br>If the parity group with PDEV does not support accelerated compression, or if the ECC Group is Spare Drive, a blank space is displayed. |
| **Notes:**<br>**1.** Blank if the parity group is not concatenated to another parity group or is Spare Drive. | |

## PdevStatus.csv

This CSV file contains information about the status of physical devices (PDEVs). A record is created for each PDEV.

**Table 51 PdevStatus.csv file (Title: <<PDEV Status>>)**

| Item | Content |
|---|---|
| CR# | C# and R# (2-digit hexadecimal numbers), which identify the PDEV<br>Output in the format *XX*/*YY*, where:<br>▪ *XX*: C#<br>▪ *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:**<br>**1.** 1=Normal, 0=Abnormal | |

## PECBInfo.csv

This CSV file contains information about the PECB (PCIe channel board) and connecting destination for VSP G800 or VSP F800.

For all other VSP Gx00 models or VSP Fx00 models, hyphens are displayed for all contents.

**Table 52 PECBInfo.csv file (Title: <<PECB Information>>)**

| Item | Content |
|---|---|
| Location | PECB location name |
| Status | Whether the PECB is installed<br>▪ Installed<br>▪ Not Installed |
| Type | Destination module type of the PECB<br>▪ CHBB |
| Expansion mode | Expansion mode set in the destination module of the PECB<br>▪ 1:2 |

## PkInfo.csv

This CSV file contains information about channel boards (CHBs). A record is created for each CHB.

**Table 53 PkInfo.csv file (Title: <<PK>>)**

| Item | Content |
|---|---|
| CHB Location | CHB name<br>CHB-1A/1B/1C/1D or CHB-2A/2B/2C/2D if "Package Type" is NAS module. |
| Port# | Number of the port installed on the CHB (2-digit hexadecimal number) |
| Port | Name of port installed on the CHB |
| Package Type | CHB type indicated on the CHB Location<br>▪ Fibre: 8FC4 (CHB), 16FC2 (CHB), 32FC4R (CHB)<br>▪ iSCSI: 10iSCSI2o (CHB), 10iSCSI2c (CHB)<br>▪ NAS module: NAS module (CHB) |
| SFP Kind | SFP (Small Form factor Pluggable) Kind<br>▪ Short Wave<br>▪ Long Wave<br>▪ Blank if "Package Type" is 10iSCSI2c (CHB) or NAS module (CHB). |

| Item | Content |
|---|---|
| SFP Status | SFP Status:<br>▪ Normal<br>▪ Failed<br>▪ Not Fix<br>▪ Blank if "Package Type" is 10iSCSI2c (CHB) or NAS module (CHB). |
| Fabric | One of the Fibre topology settings indicating the setting status of the Fabric switch:<br>▪ On<br>▪ Off<br>▪ Blank if "Package Type" is iSCSI or NAS module. |
| Connection | One of the Fibre topology settings<br>▪ Point to Point<br>▪ FC-AL<br>▪ Blank if "Package Type" is iSCSI or NAS module. |
| Port Address | Port address (00 to ff, 2-digit hexadecimal number)<br>Blank if "Package Type" is iSCSI or NAS module. |
| 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<br>Blank if "Package Type" is iSCSI or NAS module. |
| T10 PI Mode | Indicates whether the T10 PI mode can be applied to the port.<br>▪ Enabled<br>▪ Disabled<br>▪ Blank if "Package Type" is not 16FC2 (CHB) or 32FC4R (CHB). |
| SFP Data Transfer Rate | Maximum transfer rate of SFP which the mounted package supports.<br>▪ 8G<br>▪ 10G<br>▪ 16G<br>▪ 32G<br>▪ Blank if the "Package Type" is 10iSCSI2c (CHB) or NAS module (CHB). |

## 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 187) .

**Table 54 PpInfo.csv file (Title: <<PP Information>>)**

| Item | Content |
|---|---|
| Program Product Name | Software name. |
| Install | Information about whether the installed license key is enabled or not<br>▪ Enabled: Installed and the software can be used<br>▪ Disabled: Installed but the software cannot be used |
| Key Type | Installed license key type<br>▪ Permanent<br>▪ Temporary<br>▪ Emergency<br>▪ Term<br>If no license key is installed, "Not Installed" is output. |
| Permitted Volumes(TB) | Permitted volume capacity for this software (in TB)<br>If no upper limit value is set for the capacity, "Unlimited" is output. |
| Expiration Date | Expiration date of the software.<br>The format is *mm*/*dd*/*yyyy* (Month/Day/Year). |
| Status | License key status of the software<br>▪ Installed<br>▪ Not Enough License<br>▪ Grace Period<br>▪ Expired<br>▪ Not Installed<br>▪ 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".

**Table 55 SMfundat.csv file (Title: <<SM Install function>>)**

| Item | Content |
|---|---|
| SM Install function | The following classifications are output for VSP G200:<br>**1.** Base<br>**2.** Extension 1<br>**3.** Extension 2<br>The following classifications are output for VSP G400, G600, G800 or VSP F400, F600, F800:<br>**1.** Base<br>**2.** Extension1<br>**3.** Extension2<br>**4.** Extension3<br>**5.** Extension4 |
| Availability | Information about whether the function of "SM Install function" is enabled<br>▪ Enabled<br>▪ Disabled |

## SsdDriveInfo.csv

This CSV file contains information about SSDs. A record is created for each SSD.

**Table 56 SsdDriveInfo.csv file (Title: <<SSD Drive Status>>)**

| Item | Content |
|---|---|
| ECC Group | Number of the parity group of which this SSD is a component.<br>▪ Spare Drive: The SSD is a spare drive.<br>▪ Free Drive: The SSD is a free drive. |
| CR# | C# and R# (2-digit hexadecimal numbers), which identify the PDEV<br>Output in the format *XX*/*YY*, where:<br>▪ *XX*: C#<br>▪ *YY*: R# |
| PDEV Location | Drive type code of the PDEV location name for this drive |
| Device Type-Code | Drive type code<br>Output example: SLR5A-M800SS |
| Device Capacity | Drive capacity in GB or TB |

| Item | Content |
|---|---|
| SSD Device Type | SSD drive type<br>▪ MLC<br>▪ FMC<br>▪ FMD |
| Used Endurance Indicator (%) | SSD life (0 to 100) |
| Used Endurance Indicator Threshold (%) | SSD 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)<br>Blank if SSD is other than FMD |
| FMD Battery Life Indicator (%) | Used battery life (0 to 100)<br>Blank if SSD is other than FMD |

## SsidInfo.csv

This CSV file contains information about SSIDs. A record is created for each SSID.

**Table 57 SsidInfo.csv file (Title: <<Subsystem ID >>)**

| Item | Content |
|---|---|
| DEV# Start | First LDEV number for the SSID |
| DEV# End | Last LDEV number for the SSID |
| SSID | Subsystem ID (hexadecimal) |

## SysoptInfo.csv

This CSV file contains information about system options.

**Table 58 Sysoptinfo.csv file (Title: <<System Option Information>>)**

| Item | Content |
|---|---|
| Spare Disk Recover | Speed of copying data to the spare drive.<br>▪ Interleave mode<br>▪ 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.<br>▪ On<br>▪ Off |
| Correction Copy | Information about whether to perform correction copy to a spare drive if a drive is blocked.<br>▪ On<br>▪ Off |
| Disk Copy pace | Speed of copying the spare drive in the Interleave mode.<br>▪ Faster<br>▪ Medium<br>▪ Slower |
| System Option On | System options that are set to ON.<br>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.

For details about the host setting, see the *Provisioning Guide*.

**Table 59 WwnInfo.csv file (Title: <<World Wide Name Information>>)**

| Item | Content |
|---|---|
| Port | Port name. |
| Host Group | Host group name<br>iSCSI target alias is output if the "Package Type" is iSCSI. |
| Host Mode | Host mode that is set for the host group (0 to 127, hexadecimal) |
| Host Mode Option | Host mode option that is set for the host group (decimal)<br>Multiple options are separated by semicolons (;) |

| Item | Content |
|---|---|
| WWN | World Wide Name of the host bus adapter registered to the host group (hexadecimal number)<br>Blank if the "Package Type" is iSCSI or NAS module. |
| Nickname | Nickname of the host<br>Blank if the "Package Type" is iSCSI or NAS module. |
| Host Group# | Host group number (00 to ff, hexadecimal)<br>iSCSI target ID will be output if the "Package Type" is iSCSI. |
| CHB Location | Name of port installed on the CHB<br>CHB-1A/1B/1C/1D or CHB-2A/2B/2C/2D if "Package Type" is NAS module. |
| Package Type | CHB type indicated on the CHB Location<br>▪ Fibre: 8FC4 (CHB), 16FC2 (CHB), 32FC4R(CHB)<br>▪ iSCSI: 10iSCSI2o (CHB), 10iSCSI2c (CHB)<br>▪ NAS module: NAS module (CHB) |
| T10 PI Mode | Indicates whether the T10 PI mode can be applied to the port.<br>▪ Enabled<br>▪ Disabled<br>▪ Blank if "Package Type" is not 16FC2 (CHB) or 32FC4R (CHB). |

# Appendix B: System option modes

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. The SOMs are set on the service processor (SVP) by your service representative. 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.

The following table lists and describes the SOMs for firmware version 83-05-01.

**Note:** The SOM information might have changed since this document was published. Contact customer support for the latest SOM information.

**Table 60 System option modes for VSP Gx00 models and VSP Fx00 models**

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 15 | Common | This SOM can reduce the host response time to be within about 6 seconds.<br>The default setting for this SOM depends on the microcode level:<br>▪ Default = ON: 83-05-01 and later<br>▪ Default = OFF: 83-04-xx and earlier<br>**Notes:**<br>**1.** This SOM is used on a storage system where slow or delayed drive response may affect business operations.<br>**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.<br>**3.** Even though SOM 15 is set to ON, the function does not apply to SATA or NL-SAS drives.<br>**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.<br>**5.** When this SOM is applied, SOM 142 is disabled.<br>**6.** For additional details about this SOM (interaction with other SOMs, operational details), contact customer support (see SOM015 sheet). | ON | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 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.<br>**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.<br>**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).<br>One of the controlling option for correction/drive copy. | OFF | None |
| 80 | ShadowImage | In response to the Restore instruction from the host, if neither Quick nor Normal is specified, the following operation is performed.<br>**Mode 80 = ON:** Normal Restore / Reverse Copy is performed.<br>**Mode 80 = OFF (default):** Quick Restore is performed.<br>**Notes:**<br>**1.** This SOM is applied when the specification for Restore of SI is switched between Quick (default) and Normal.<br>**2.** The performance of Restore differs depending on the Normal or Quick specification. | OFF | - |
| 87 | ShadowImage | Determines whether NormalCopy or QuickResync, if not specified, is performed at the execution of pairresync by CCI.<br>**Mode 87 = ON:** QuickResync is performed.<br>**Mode 87 = OFF (default):** NormalCopy is performed. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 122 | ShadowImage | For Split or Resync request from the Mainframe host and Storage Navigator.<br><br>**Mode 122 = ON:** By specifying Split or Resync, Steady/Quick Split or Normal/Quick Resync is respectively executed in accordance with Normal/Quick setting.<br><br>**Mode 122 = OFF (default):** By specifying Split or Resync, Steady/Quick Split or Normal/Quick Resync is respectively executed in accordance with Normal/Quick setting.<br><br>For details about pairsplit/pairresync command behavior, contact customer support (see SOM122 sheet).<br><br>**Notes:**<br><br>**1.** Executing the pairresync command from CCI may be related to the SOM 87 setting.<br>**2.** When performing At-Time Split from CCI, set this SOM to OFF, or specify the environment variable HORCC_SPLT for Quick. Otherwise, Pairsplit may turn timeout.<br>**3.** This SOM becomes effective after specifying Split/Resync following the mode setting. The mode function does not work if it is set during the Split/Resync operation. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 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.<br><br>**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.<br><br>**Mode 142 = OFF:** The threshold value of blocking a drive port due to command time-out does not change.<br><br>*The default setting for this SOM depends on the microcode level:<br><br>▪ Default = ON: 83-03-28 and later (within 83-03-2x range), 83-04-03 and later<br>▪ Default = OFF: earlier than 83-03-28, earlier than 83-04-03 (within 83-04-0x range)<br><br>**Notes:**<br><br>**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.<br>**2.** This SOM is effective for the entire storage system. | ON | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 144 | Common | The drive whose command response time is permanently delayed is blocked. At the same time, SSB=AE4A (total response time exceeds threshold) is reported. In this case, cache can become overloaded so that the storage system performance is degraded.<br><br>**Mode 144 = ON (default*):** Check if there is a permanently delayed drive for each port, and block the corresponding port at the first time when all of the following conditions are met:<br><br>**1.** The total time for the drive to respond to 200 commands is 20 seconds or more.<br>**2.** The response time of the drive is two times or more longer than the average response time of the parity group (excluding the slow drive).<br>**3.** The drive is in one of the following statuses:<br><br>- Normal<br><br>- A source drive or a target drive (spare drive) during drive copy.<br><br>- A target drive (not spare drive) during copy back.<br><br>- A target drive (spare drive) during correction copy.<br><br>**Mode 144 = OFF:** Checking for delayed drives is not performed.<br><br>*The default setting for this SOM depends on the microcode level:<br><br>▪ Default = 83-03-28 and later (within 83-03-2x range), 83-04-03 and later<br>▪ Default = earlier than 83-03-28, earlier than 83-04-03 (within 83-04-0x range)<br><br>**Note:** If there are multiple response-delayed drives in the same parity group, only the first one is blocked. | ON | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 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.<br>**Mode 310 = OFF (default):** The monitoring timer for MP hang-up is 8 seconds.<br>**Notes:**<br>**1.** This SOM applies to a site where strict host response performance is required.<br>**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 | When the SVP detects a blocked path:<br>**Mode 448 = ON:** An error is assumed and the mirror is immediately suspended.<br>**Mode 448 = OFF (default):** If the path does not recover within a specified period of time, an error is assumed and the mirror is suspended.<br>**Note:** SOM 448 setting is available only when SOM 449 is set to OFF. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 449 | Universal Replicator | This SOM is used to enable and disable detection of communication failures between the MCU and RCU.<br><br>**Mode 449 = ON (default):** On the MCU side, checking read journal disruption from RCU is disabled, and monitoring read journal failures is disabled on the RCU side.<br><br>**Mode 449 = OFF:** Detecting communication failures between the MCU and RCU is enabled.<br><br>**Notes:**<br>**1.** This SOM applies when disabling the detection of communication failures between the MCU and RCU in UR configuration is required.<br>**2.** When this SOM is set to ON, SOM 448 does not work.<br>**3.** This SOM setting is not changed by microcode upgrade.<br>**4.** This SOM is not effective for remote paths between an Initiator port on the MCU and a Target port on the RCU.<br>**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.<br><br>**Mode 454 = OFF (default):** 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.)<br><br>*a: (Write Pending capacity of CLPR#x of concerned MPB) ÷ (Cache capacity of CLPR#x of concerned MPB), x=0 to 31<br><br>CLPR whose value above is the highest of all CLPRs<br><br>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.<br><br>Therefore, set SOM 454 to OFF in most cases.<br><br>**Mode 454 = ON:**<br><br>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.)<br><br>*b: (Write Pending capacity of the entire system of concerned MPB) ÷ (Cache capacity of the entire system of concerned MPB)<br><br>**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.<br><br>**Notes:** | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| | | **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.<br><br>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.<br><br>**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. | | |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 457 | Universal Volume Manager | This SOM has two purposes: High-Speed LDEV Format for External Volumes, and Support for Mainframe Control Block Write GUI.<br>**Mode 457 = ON:**<br>**1.** High-Speed LDEV Format for External Volumes.<br>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. However, if the external LDEV is a mainframe volume, the write processing for mainframe control information only will be performed after the write skip.<br>**2.** Support for Mainframe Control Block Write GUI.<br>Control Block Write of the external LDEVs in mainframe emulation is supported by Device Manager - Storage Navigator (GUI).<br>▪ If the LDEV is not written with data “0” before performing the function, the LDEV format might fail.<br>▪ After the format processing, make sure to set SOM 457 to OFF.<br>**Mode 457 = OFF (default):** High-speed LDEV format for external volumes and support for mainframe control block write GUI are not available. | 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:<br>**Mode 459 = ON:** When suspending an SI pair: The copy data is created in cache memory. When the write processing on the external storage completes and the data is fixed, the pair status will change to SPLIT.<br>**Mode 459 = OFF (default):** When suspending an SI pair: Once the copy data has been created in cache memory, the pair status will change to SPLIT. The external storage data is not fixed (current spec). | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 466 | Universal Replicator | It is strongly recommended that the path between the primary and secondary storage systems have a minimum data transfer speed of 100 Mbps. If the data transfer speed falls to 10 Mbps or lower, UR operations cannot be properly processed. As a result, many retries occur and UR pairs might be suspended. This SOM is provided to ensure proper system operation for data transfer speeds of at least 10 Mbps.<br><br>**Mode 466 = ON:** Data transfer speeds of 10 Mbps and higher are supported. The JNL read is performed with 4-multiplexed read size of 256 KB.<br><br>**Mode 466 = OFF (default):** For conventional operations. Data transfer speeds of 100 Mbps and higher are supported. The JNL read is performed with 32-multiplexed read size of 1 MB by default.<br><br>**Note:** The data transfer speed can be changed using the Change JNL Group options. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 467 | ShadowImage<br>Snapshot<br>Volume Migration<br>Universal Volume Manager | 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.<br>▪ SI<br>▪ Snapshot<br>▪ UVM<br>▪ Volume Migration<br>**Mode 467 = ON (default):** 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.<br>**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.<br>**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.<br>**Notes:**<br>**1.** It takes longer to finish the copy processing because it stops for prioritizing the host I/O performance.<br>**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.<br>**3.** Check the write pending rate of each CLPR per MP blade. Even though there is some free cache capacity in the entire system, if the write pending rate of an MP blade to which pairs* belong exceeds the threshold, the copy operation is stopped.<br>*Applies to pairs of SI, SIz, FCv2, FCSE, Snapshot, and Volume Migration. | ON | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 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.<br><br>The SIM-RCs reported by setting the SOM to ON are: 601xxx (Pool utilization threshold exceeded), 603000 (SM space warning).<br><br>**Mode 471 = ON:** These SIM-RCs are reported to maintenance personnel.<br><br>**Mode 471 = OFF:** These SIM-RCs are not reported to maintenance personnel.<br><br>**Note:** Set this SOM to ON when it is required to inform maintenance personnel of these SIM-RCs. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 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.<br><br>**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.<br><br>**Mode 474 = OFF (default):** 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.<br><br>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.<br><br>**Notes:**<br><br>**1.** Set this SOM for both primary and secondary storage systems.<br>**2.** When this SOM is set to ON:<br>▪ Execute all pair operations from CCI/BCM.<br>▪ Use a dedicated script.<br>▪ Initial copy operation is prioritized over update I/O. Therefore, the processing speed of the update I/O slows down.<br>**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.<br>**4.** If this SOM is not set to ON for both sides, the behavior is as follows:<br>▪ OFF in primary and secondary storage systems: Normal UR initial copy performance.<br>▪ ON in the primary storage system/OFF in the secondary storage system: TC Sync pair creation fails. | OFF | Both |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| | | ▪ OFF in the primary storage system/ON in the secondary storage system: The update data is copied to the S-VOL synchronously.<br>**5.** While this SOM is set to ON, make sure not to perform microcode downgrade to an unsupported version.<br>**6.** While this SOM is set to ON, make sure not to perform the Take Over function.<br>**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.<br>**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. | | |
| 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.<br>The UR Delta Resync configuration is required.<br>**Mode 506 = ON:**<br>▪ Without update I/O: Delta Resync is enabled.<br>▪ With update I/O: Delta Resync is enabled.<br>**Mode 506 = OFF:**<br>▪ Without update I/O: Total data copy of Delta Resync is performed.<br>▪ With update I/O: Delta Resync is enabled.<br>**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 |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 561 | ShadowImage<br>Universal Volume Manager | Allows Quick Restore for external volumes with different Cache Mode settings.<br>**Mode 561 = ON:** Quick Restore for external volumes with different Cache Mode settings is prevented.<br>**Mode 561 = OFF (default):** Quick Restore for external volumes with different Cache Mode settings is allowed. | OFF | Both |
| 589 | Universal Volume Manager | When this SOM is ON, the frequency of progress update of disconnection is changed.<br>**Mode 589 = ON:** For each external volume, progress is updated only when the progress rate is 100%.<br>**Mode 589 = OFF (default):** Progress is updated when the progress rate exceeds the previous level.<br>**Notes:**<br>**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.<br>**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<br>global-active device | Allows you to slow the initial copy and resync operations when the write-pending rate on the RCU exceeds 60%.<br>**Mode 689 = ON:** The initial copy and resync copy operations are slowed down when the Write Pending rate on RCU exceeds 60%.<br>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.<br>**Mode 689 = OFF (default):** The initial copy and resync copy operations are not slowed down when the Write Pending rate on RCU exceeds 60% (the same as before).<br>**Notes:**<br>**1.** This SOM can be set online.<br>**2.** The micro-programs on both MCU and RCU must support this SOM.<br>**3.** This SOM should be set when requested by the user.<br>**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.<br>**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.<br>**6.** Do not set this SOM if the primary or secondary system is connected to USP V/VM with microcode earlier than 60-02-xx-xx/xx. If this SOM is applied and the write-pending rate reaches 60%, pair suspend might occur.<br>**7.** As this SOM is enabled per storage system, in an environment where TC and GAD are used, this SOM is applied to both program products. When GAD is installed in a storage system that already uses TC, TC initial copy might take longer time. | OFF | Both |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 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:<br>▪ When CLPR of JNL-Volume exceeds 60%, Read JNL is prevented.<br>▪ When CLPR of Data (secondary)-Volume exceeds 60%, JNL Restore is prevented.<br>**Mode 690 = ON:** Read JNL or JNL Restore is prevented when the Write Pending rate on RCU exceeds 60%.<br>**Mode 690 = OFF (default):** Read JNL or JNL Restore is not prevented when the Write Pending rate on RCU exceeds 60% (the same as before).<br>**Notes:**<br>**1.** This SOM can be set online.<br>**2.** This SOM should be set per customer's requests.<br>**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.<br>**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.<br>**5.** When USP/NSC is used on the P-VOL side, this SOM cannot be used. If this SOM is set to ON, SSB=8E08 on the P-VOL side and SSB=C8D1 on the S-VOL side might be output frequently. | OFF | RCU |
| 696 | Open | This SOM is available to enable or disable the QoS function.<br>**Mode 696 = ON:** QoS is enabled. (In accordance with the Share value set to SM, I/Os are scheduled. The Share value setting from RMLIB is accepted)<br>**Mode 696 = OFF (default):** QoS is disabled. (The Share value set to SM is cleared. I/O scheduling is stopped. The Share value setting from host is rejected.)<br>**Note:** Set this SOM to ON when you want to enable the QoS function. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 701 | Universal Volume Manager | Issues the Read command at the logical unit discovery operation using UVM.<br>**Mode 701 = ON:** The Read command is issued at the logical unit discovery operation.<br>**Mode 701 = OFF (default):** The Read command is not issued at the logical unit discovery operation.<br>**Notes:**<br>**1.** When the external storage is USP/NSC and the Open LDEV Guard attribute (VMA) is defined on an external device, set this SOM to ON.<br>**2.** As the VMA information is USP/NSC specific, this SOM does not need to be ON when the external storage is other thanUSP/NSC.<br>**3.** When this SOM is set to ON, it takes longer time to complete the logical unit discovery. The amount of time depends on external storages.<br>**4.** With this SOM OFF, if searching for external devices with VMA ia set, the VMA information cannot be read.<br>**5.** When this SOM is set to ON while the following conditions are met, the external volume is blocked:<br>▪ An external volume to which Nondisruptive migration (NDM) attribute is set exists.<br>▪ The external volume is reserved by the host<br>**6.** Set this SOM to OFF when the following conditions are met:<br>▪ An external volume to which Nondisruptive migration (NDM) attribute is set exists. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 704 | ShadowImage<br>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.<br>**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.<br>**Mode 704 = OFF (default):** Copy processing requested is not registered into a newly created queue. Only the existing queue is used.<br>**Notes:**<br>**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.<br>**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. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 721 | Common | When a parity group is uninstalled or installed, the following operation is performed according to the setting of SOM 721.<br><br>**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.<br><br>**Mode 721 = OFF (default):** 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.<br><br>**Notes:**<br><br>**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.<br>**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 | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 725 | Universal Volume Manager | This SOM determines the action that will be taken when the status of an external volume is Not Ready.<br><br>**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.<br><br>When the status of a device is Not Ready blockade, Device Health Check is executed after 30 seconds.<br><br>**Mode 725 = OFF (default):** 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).<br><br>**Notes:**<br><br>**1.** Applying this SOM is prohibited when USP V/VM is used as an external storage system and its external volume is DP-VOL.<br>**2.** Applying this SOM is recommended when the above condition (1) is not met and SUN storage is used as an external storage.<br>**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.<br>**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.<br>**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.<br>**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. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 729 | Dynamic Provisioning<br>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.<br>**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.)<br>**Mode 729 = OFF (default):** 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.<br>For details, contact customer support (see SOM729 & 803 sheet).<br>**Notes:**<br>**1.** This SOM is applied when:<br>▪ The threshold of pool is high (for example, 95%) and the pool may be full.<br>▪ File system is used.<br>▪ Data Retention Utility is installed.<br>**2.** Since the Protect attribute is set for V-VOL, the Read operation cannot be allowed as well.<br>**3.** When Data Retention Utility is not installed, the desired effect is not achieved.<br>**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.<br>**5.** With 83-01-21-x0/00 and later, the Virtual Volume Protection (VVP) function is supported. VVP 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. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| | | **6.** With or 83-01-21-x0/00 and later, 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. | | |
| 733 | ShadowImage<br>Volume Migration | This SOM enables to suspend Volume Migration or Quick Restore operation during LDEV-related maintenance.<br>**Mode 733 = ON:** Volume Migration or Quick Restore operation during LDEV-related maintenance is not suspended.<br>**Mode 733 = OFF (default):** Volume Migration or Quick Restore operation during LDEV-related maintenance is suspended.<br>**Notes:**<br>**1.** Note that behavior when this SOM is set to ON and OFF is reversed between USP V/VM and VSP/HUS VM and later.<br>**2.** This SOM should be applied to perform Volume Migration or Quick Restore during maintenance operation.<br>**3.** Set SOM 733 to ON if you want to prioritize the Volume Migration or Quick Restore operation over maintenance activities. In this case, maintenance activities may fail when the Volume Migration or Quick Restore operation works during the maintenance activities.<br>**4.** An LDEV-related maintenance operation such as LDEV installation/removal may fail when Volume Migration or Quick Restore takes place. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 734 | Dynamic Provisioning | When exceeding the pool threshold, the SIM is reported as follows:<br><br>**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.<br><br>**Mode 734 = OFF (default):** 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. The SIM is not reported while the pool usage rate continues to exceed the warning threshold and the depletion threshold.<br><br>**Notes:**<br><br>**1.** This SOM is turned ON to prevent the write I/O operation from being unavailable due to pool full.<br>**2.** If the exceeding pool threshold SIM occurs frequently, other SIMs may not be reported.<br>**3.** Though turning on this SOM can increase the warning effect, if measures such as adding a pool fail to be done in time so that the pool becomes full, SOM 729 can be used to prevent file systems from being destroyed.<br>**4.** Turning on SOM 741 can provide the SIM report to not only the users but also the service personnel. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 741 | Dynamic Provisioning | This SOM enables to switch over whether to report the following SIM for users to the service personnel:<br>SIM-RC 625000 (DP pool usage rate continues to exceed the threshold)<br>**Mode 741 = ON:** SIM is reported to the service personnel.<br>**Mode 741 = OFF (default):** SIM is not reported to the service personnel.<br>**Notes:**<br>**1.** This SOM is set to ON to have SIM for users reported to the service personnel:<br>▪ For the system where SNMP and E-mail notification are not set.<br>▪ If Device Manager - Storage Navigator is not periodically activated.<br>**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. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 745 | Universal Volume Manager | Enables to change the area where the information is obtained as the Characteristic1 item from SYMMETRIX.<br>**Mode 745 = ON:**<br>▪ The area where the information is obtained as the Characteristic1 item from SYMMETRIX is changed.<br>▪ 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.<br>**Mode 745 = OFF (default):**<br>▪ The area where the information is obtained as the Characteristic1 item from SYMMTRIX is set to the default.<br>▪ When CheckPaths or Device Health Check (1/hour) is performed, the information of an already-mapped external volume is updated to the default.<br>**Notes:**<br>**1.** This SOM is applied when the EMC SYMMETRIX is connected using UVM.<br>**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.<br>**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. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 749 | Dynamic Provisioning<br>Dynamic Tiering<br>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.<br>**Mode 749 = ON:** The HDP Rebalance function and the HDT Tier relocation function are disabled.<br>**Mode 749 = OFF (default):** The HDP Rebalance function and the HDT Tier relocation function are enabled.<br>**Notes:**<br>**1.** This SOM is applied when no change in performance characteristic is desired.<br>**2.** When a pool is newly installed, the load may be concentrated on the installed pool volumes.<br>**3.** When 0 data discarding is executed, load may be unbalanced among pool volumes.<br>**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.<br>**Mode 757 = ON:** Output is disabled.<br>**Mode 757 = OFF (default):** Output is enabled.<br>**Notes:**<br>**1.** Mode 757 applies to the sites where outputting the In-band audit logs is not needed.<br>**2.** When this SOM is set to ON:<br>▪ There is no access to SM for the In-band audit logs, which can avoid the corresponding performance degradation.<br>▪ SM is not used for the In-band audit logs.<br>**3.** If outputting the In-band audit log is desired, set this SOM to OFF. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 784 | TrueCopy<br>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.)<br><br>This SOM is applied to TC and GAD. This SOM supports Fibre remote copy paths but not iSCSI.<br><br>**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.<br><br>**Mode 784 = OFF (default):** The operation is processed in accordance with the TC or GAD specification.<br><br>**Notes:**<br><br>**1.** This SOM is applied to the environment where Mainframe host MIH time is set to 15 seconds.<br>**2.** This SOM is applied to the environment where OPEN host time-out time is set to 15 seconds or less.<br>**3.** This SOM is applied to reduce RI/O MIH time to 5 seconds.<br>**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.<br>**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.<br>**6.** If a failure occurs on the switched path between storage systems, Mainframe host MIH or Open server time-out may occur.<br>**7.** If an MP to which the path between storage systems belongs is overloaded, switching to an | OFF | Both |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| | | alternate path delays and host MIH or time-out may occur.<br>**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.<br>**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 occur due to a path failure between storage systems.<br>**10.** Operation commands are not available for promptly switching to an alternate path.<br>**11.** This SOM works for the pair for which initial pair creation or Resync operation is executed.<br>**12.** Micro-program downgrade to an unsupported version cannot be executed unless all the TC and GAD pairs are suspended or deleted.<br>**13.** For operational specifications in each combination of MCU and RCU of TC, contact customer support (see SOM784 sheet).<br>**14.** For GAD pairs, this SOM is effective if the microcode version supports GAD.<br>**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. | | |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 803 | Dynamic Provisioning<br>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.<br>**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.<br>**Mode 803 = OFF (default):** 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.<br>For more details, contact customer support (see SOM729 & 803 sheet).<br>**Notes:**<br>**1.** This SOM is applied when:<br>▪ A file system using DP pool VOLs is used.<br>▪ Data Retention Utility is installed.<br>**2.** Because the DRU attribute is set to Protect for the V-VOL, a read I/O is also disabled.<br>**3.** If Data Retention Utility is not installed, the expected effect cannot be achieved.<br>**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.<br>**5.** With 83-01-21-x0/00 and later, the Virtual Volume Protection (VVP) function is supported. VVP 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. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 855 | ShadowImage<br>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.<br>**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.<br>**Mode 855 = OFF (default):** The copy processing is stopped when the amount of dirty data is over 60%.<br>For details, contact customer support (see SOM855 sheet).<br>**Notes:**<br>**1.** This SOM is applied when all the following conditions are met<br>▪ ShadowImage is used with SOM 467 set to ON.<br>▪ Write pending rate of an MP blade that has LDEV ownership of the copy target is high<br>▪ Usage rate of a parity group to which the copy target LDEV belongs is low.<br>▪ ShadowImage copy progress is delayed.<br>**2.** This SOM is available only when SOM 467 is set to ON.<br>**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. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 857 | Common | This SOM enables or disables to limit the cache allocation capacity per MP blade/unit to within the prescribed capacity* except for Cache Residency Manager.<br><br>**Mode 857 = ON:** The cache allocation capacity is limited to within the prescribed capacity*.<br><br>**Mode 857 = OFF (default):** The cache allocation capacity is not limited to within the prescribed capacity*.<br><br>*Prescribed capacity:<br><br>▪ VSP G800, VSP, HUS VM: 128 GB<br>▪ VSP G400, G600: 64 GB<br>▪ VSP G200: 16 GB<br><br>**Notes:**<br><br>**1.** This SOM is applied to stabilize the performance by preventing paging of PM control information from occurring. For details, refer to the section of Virtual Partition Manager in the guideline.<br>**2.** The cache hit rate may decrease.<br>**3.** The cache allocation capacity per MPB/MPU is limited to within the prescribed capacity. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 867 | Dynamic Provisioning<br>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.<br>**Mode 867 = ON (default*):** LDEV format of the DP-VOL is performed with page reclamation.<br>**Mode 867 = OFF:**LDEV format of the DP-VOL is performed with 0 data writing.<br>*The default is OFF for VSP, HUS VM, and VSP Fx00 models and VSP Gx00 models with firmware 83-03-*xx* and earlier.<br>**Notes:**<br>**1.** This SOM is applied from factory shipment.<br>**2.** Do not change the setting of this SOM during DP-VOL format.<br>**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 | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 896 | Dynamic Provisioning<br>Dynamic Tiering<br>Thin Image | This SOM enables or disables the background format function performed on an unformatted area of a DP/DT/TI pool.<br>For information regarding operating conditions, see the *Provisioning Guide* for your storage system.<br>**Mode 896 = ON:** The background format function is disabled.<br>**Mode 896 = OFF (default):** The background format function is enabled.<br>**Notes:**<br>**1.** This SOM is applied when a customer requires the background format for a DP/DT/TI pool in the environment where new page allocation (in the case that system files are created from a host for newly created multiple DP-VOLs, for example) frequently occurs and the write performance degrades because of an increase in write pending rate.<br>**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.<br>**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.<br>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.<br>**4.** If the background format function is disabled by changing this SOM setting, the format progress is initialized and the entire area becomes unformatted.<br>**5.** The background format for FMC drives is not disabled. When FMC drives are used, use SOM 1093. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 897 | Dynamic Tiering | By the combination of SOM 897 and 898 setting, the expansion width of Tier Range upper I/O value (IOPH) can be changed as follows.<br>**Mode 897 = ON:**<br>▪ SOM 898 is OFF: 110%+0IO<br>▪ SOM 898 is ON: 110%+2IO<br>**Mode 897 = OFF (default):**<br>▪ SOM 898 is OFF: 110%+5IO (default)<br>▪ SOM 898 is ON: 110%+1IO<br>By setting the SOMs to ON to lower the upper limit for each tier, the gray zone between other tiers becomes narrow and the frequency of page allocation increases.<br>**Notes:**<br>**1.** Apply this SOM when the upper tier usage is low and lower tier usage is high.<br>**2.** This SOM must be used with SOM 898.<br>**3.** Narrowing the gray zone increases the number of pages to migrate between tiers per relocation.<br>**4.** 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.<br>For more details about the interactions between SOMs 897, 898, and 901, contact customer support (see SOM897_898_901 sheet). | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 898 | Dynamic Tiering | By the combination of SOM 898 and 897 setting, the expansion width of Tier Range upper I/O value (IOPH) can be changed as follows.<br>**Mode 898 = ON:**<br>▪ SOM 897 is OFF: 110%+1IO<br>▪ SOM 897 is ON: 110%+2IO<br>**Mode 898 = OFF (default):**<br>▪ SOM 897 is OFF: 110%+5IO (default)<br>▪ SOM 897 is ON: 110%+0IO<br>By setting the SOMs to ON to lower the upper limit for each tier, the gray zone between other tiers becomes narrow and the frequency of page allocation increases.<br>**Notes:**<br>**1.** Apply this SOM when the usage of upper tier is low and that of lower tier is high.<br>**2.** This SOM must be used with SOM 897.<br>**3.** Narrowing the gray zone increases the number of pages to migrate between tiers per relocation.<br>**4.** 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.<br>For more details about the interactions between SOMs 897, 898, and 901, contact customer support (see SOM897_898_901 sheet). | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 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.<br>**Mode 899 = ON:**<br>▪ SOM 900 is ON: I/O synchronous copy starts without retrying Volume Migration.<br>▪ SOM 900 is OFF: I/O synchronous copy starts when the threshold of Volume Migration retry is exceeded. (Recommended)<br>**Mode 899 = OFF (default):**<br>▪ SOM 900 is ON: I/O synchronous copy starts when the number of retries reaches half of the threshold of Volume Migration retry.<br>▪ SOM 900 is OFF: Volume Migration is retired and I/O synchronous copy is not executed.<br>**Notes:**<br>**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.<br>**2.** During I/O synchronous copy, host I/O performance degrades. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 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.<br>**Mode 900 = ON:**<br>▪ SOM 899 is ON: I/O synchronous copy starts without retrying Volume Migration.<br>▪ SOM 899 is OFF: I/O synchronous copy starts when the number of retries reaches half of the threshold of Volume Migration retry.<br>**Mode 900 = OFF (default):**<br>▪ SOM 899 is ON: I/O synchronous copy starts when the threshold of Volume Migration retry is exceeded. (Recommended)<br>▪ SOM 899 is OFF: Volume Migration is retired and I/O synchronous copy is not executed.<br>**Notes:**<br>**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.<br>**2.** During I/O synchronous copy, host I/O performance degrades. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 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.<br><br>**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<br><br>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.<br><br>**Mode 901 = OFF (default):** 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.<br><br>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].<br><br>**Notes:**<br><br>**1.** This SOM is applied when pages with the maximum capacity need to be allocated to tier1 (drive type is SSD) with Dynamic Tiering.<br>**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.<br>**3.** The following is recommended when applying SOM 901.<br><br>actual I/O value (total number of I/Os of all tiering policies) < performance potential value of Tier1* × 0.6<br><br>* The performance potential value of Tier1 displayed on Monitor information by using Dx-ray. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| | | For more details about the interactions between SOMs 897, 898, and 901, contact customer support (see SOM897_898_901 sheet). | | |
| 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.<br>**Mode 904 = ON:** The number of pages to be migrated at tier relocation is set to up to one page per second.<br>**Mode 904 = OFF (default):**No restriction on the number of pages to be migrated at tier relocation (existing specification).<br>**Notes:**<br>**1.** This SOM is applied when the requirement for response time is severe.<br>**2.** The number of pages to be migrated per unit time at tier relocation decreases. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 908 | Universal Replicator | This SOM can change CM capacity allocated to MPBs with different workloads.<br><br>**Mode 908 = ON:** The difference in CM allocation capacity among MPBs with different workload is large.<br><br>**Mode 908 = OFF (default):** The difference in CM allocation capacity among MPBs with different workload is small (existing operation) .<br><br>**Notes:**<br><br>**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.<br><br>Example:<br><br>(a) A CLPR only for UR JNLG.<br><br>(b) A configuration where MPBs and CLPRs are separately used for Open and Mainframe systems.<br><br>**2.** Since CM capacity allocated to MPBs with low load is small, the performance is affected by a sudden increase in load.<br><br>**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.<br><br>**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. | OFF | Both |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 930 | Dynamic Provisioning<br>Dynamic Tiering<br>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.)<br>* Zero data page reclamation by WriteSame and UNMAP functions, and IO synchronous page reclamation are not disabled.<br>**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.)<br>**Mode 930 = OFF (default):** The zero data page reclamation is performed.<br>For details about interactions with SOM 755, contact customer support (see SOM930 sheet).<br>**Notes:**<br>**1.** This SOM is applied when stopping or disabling zero data page reclamation by user request is required.<br>**2.** When this SOM is set to ON, the zero data page reclamation does not work at all.<br>* Zero data page reclamation by Write Same and UNMAP, and IO synchronous page reclamation can work.<br>**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.<br>* Because the zero data page reclamation does not work at all while this SOM is set to ON.<br>**4.** This SOM is related to SOM 755. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 937 | Dynamic Provisioning<br>Dynamic Tiering | By setting this SOM to ON, HDT monitoring data is collected even if the pool is a DP pool.<br>**Mode 937 = ON:** HDT monitoring data is collected even if the pool is a DP pool.<br>Only Manual execution mode and Period mode are supported.<br>**Mode 937 = OFF (default):** HDT monitoring data is not collected if the pool is a DP pool<br>**Notes:**<br>**1.** This SOM is applied when HDT monitoring data collection is required in DP environment.<br>**2.** When HDT is already used, do not set this SOM to ON.<br>**3.** For HDT monitoring data collection, shared memory for HDT must be installed. For details, contact customer support (see SOM937 sheet).<br>**4.** If monitoring data collection is performed without shared memory for HDT installed, an error is reported and the monitoring data collection fails.<br>**5.** Before removing the shared memory for HDT, set this SOM to OFF and wait for 30 minutes.<br>**6.** Tier relocation with monitoring data collected when this SOM is set to ON is disabled.<br>**7.** When DP is converted into HDT (after purchase of software license), the collected monitoring data is discarded.<br>**8.** Before downgrading the micro-program to an unsupported version, set SOM 937 to OFF and wait for at least 30 minutes. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 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).<br>**Notes:**<br>**1.** This SOM is applied when a delay in host I/O response due to reclamation processing occurs in a customer environment.<br>**2.** Reclamation processing is delayed.<br>**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.<br>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 details, contact customer support (see SOM972_973 sheet).<br>**Notes:**<br>**1.** This SOM is applied when a delay in host I/O response due to reclamation processing occurs in a customer environment.<br>**2.** When this SOM is set to ON, reclamation processing is delayed.<br>**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.<br>For details about the interaction between this SOM and SOM 1069, contact customer support (see SOM1069 sheet). | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 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.<br><br>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.<br><br>**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.<br><br>**Mode 1015 = OFF (default):** The pair status changes directly to PAIR/Duplex when a delta resync is performed in a 3DC multi-target configuration.<br><br>**Notes:**<br><br>**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.<br>**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.<br>**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.<br>**4.** Regardless of the remote command device setting, the copy status does not change to COPY/Pending and then the delta resync is completed.<br>**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. | OFF | MCU |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| | | **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.<br>**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.<br>**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.<br>**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.<br>**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.<br>**Mode 1021 = OFF (default):** An external volume that is blocked due to Not Ready status might not be recovered automatically depending on the type of external storage system.<br>**Notes:**<br>**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.<br>**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. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 1043 | Universal Replicator | This SOM disables journal copy.<br>**Mode 1043 = ON:** When the following conditions are met at the UR secondary site, the journal copy is disabled.<br>For VSP Fx00 models and VSP Gx00 models, the following conditions (1) and (2) or (1) and (3) are met:<br>**1.** 4,096 or more journals are accumulated at the secondary site.<br>**2.** The CLPR write pending rate for journal volumes of MP blade/unit for which journal ownership at the RCU is defined is 25% or higher (including the write pending rate for other than journal volumes).<br>**3.** The initiator operating rate of the MP blade/unit for which journal ownership at the RCU is defined is 40% or higher.<br>**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.<br>**Mode 1043 = OFF (default):** The journal copy is not disabled.<br>**Notes:**<br>**1.** This SOM applies when one of the following conditions is met:<br>**a.** Multiple journals are registered in a consistency group of CCI.<br>**b.** Multiple journals are registered in an extended consistency group.<br>**c.** Journals are accumulated at the secondary site, causing the system performance to decrease.<br>**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.<br>**3.** When the host write speed is faster than the JNL copy speed, the usage rate of the master journal increases.<br>**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. | OFF | Both |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| | | 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.<br>**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.) | | |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 1067 | Universal Replicator | This SOM is used to enable microcode downgrade to a version that does not support URxUR (including delta).<br><br>**Mode 1067 = ON:** Even when a UR pair has been registered, downgrading the microcode to a version that does not support URxUR (including delta) is allowed.<br><br>**Mode 1067 = OFF (default):** If any UR pair has been registered, downgrading the microcode to a version that does not support URxUR (including delta) is not allowed.<br><br>**Notes:**<br><br>**1.** This SOM is applied to enable microcode downgrade to a version that does not support URxUR (including delta) if the configuration where any UR pair has been registered is not URxUR (including delta).<br>**2.** Setting this SOM to ON allows microcode downgrade at sites where only 1 mirror is used in URxUR multi-target configuration without delta resync and cascade configuration (L or R site in multi-target, and P or R site in cascade), but the following phenomena occur after microcode downgrade. Make sure that the target storage system does not contain pairs of URxUR configuration.<br><br>Phenomena:<br><br>**1.** When the microcode is downgraded at S site (local or remote) in multi-target configuration, the pair between P site and the target S site cannot be resynchronized.<br>**2.** When the pair between I site and R site in cascade configuration is resynchronized, the pair status cannot change from COPY to PAIR.<br>**3.** When the microcode is downgraded at R site in cascade configuration, the pair between I site and R site cannot be resynchronized. | OFF | Both |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 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).<br>**Notes:**<br>**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.<br>**2.** When this SOM is set to ON, reclamation processing is delayed.<br>**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).<br>**Mode 1070 = ON:** The status change of all pairs in a consistency group. is performed for 50 msec.<br>**Mode 1070 = OFF (default):** The status change of all pairs in a consistency group is performed for 1 msec.<br>**Notes:**<br>**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.<br>**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). | OFF | Both |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 1079 | Dynamic Provisioning<br>Dynamic Tiering | This SOM is set not to run the Proprietary ANCHOR command during microcode downgrade from a version that supports the Proprietary ANCHOR command to a version that does not support the command.<br>**Mode 1079 = ON:** The Proprietary ANCHOR command is unavailable.<br>**Mode 1079 = OFF (default):** The Proprietary ANCHOR command is available.<br>**Notes:**<br>**1.** This SOM is applied when downgrading the microcode from a version that supports the Proprietary ANCHOR command to a version that does not support the command.<br>**2.** Whether the Proprietary ANCHOR command can be run or not varies depending on the setting combination of SOM 1079 and HMO 97 as follows:<br>**a.** SOM 1079 setting ON/HMO 97 setting ON --> Proprietary ANCHOR command Unavailable<br>**b.** SOM 1079 setting ON/HMO 97 setting OFF --> Proprietary ANCHOR command Unavailable<br>**c.** SOM 1079 setting OFF/HMO 97 setting ON --> Proprietary ANCHOR command Available<br>**d.** SOM 1079 setting OFF/HMO 97 setting OFF --> Proprietary ANCHOR command Unavailable | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 1080 | Global-active device<br>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.<br><br>**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.<br><br>If a response to ABTS is delayed for 12 seconds or longer, the quorum disk may be blocked.<br><br>**Mode 1080 = OFF (default):** 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.<br><br>**Notes:**<br><br>**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.<br><br>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.<br><br>**2.** When connection performance degradation occurs, the quorum disk blockage is more likely to occur. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 1083 | Dynamic Provisioning<br>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.<br>**Mode 1083 = ON:** DP-VOL deletion is enabled.<br>**Mode 1083 = OFF (default):** DP-VOL deletion is disabled.<br>**Notes:**<br>**1.** This SOM is applied when the following conditions are met.<br>▪ A DP-VOL with data direct mapping attribute is deleted.<br>▪ 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.<br>**2.** When SOM 1083 is set to ON, the data of external volumes cannot be guaranteed.<br>**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<br>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.<br>**Mode 1086 = ON (default):** The performance improvement is enabled.<br>**Mode 1086 = OFF:** The performance improvement is disabled.<br>**Notes:**<br>**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.<br>**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.) | ON | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 1093 | Dynamic Provisioning<br>Dynamic Tiering<br>Thin Image | This SOM is used to disable background unmap during microcode downgrade from a version that supports pool reduction rate correction to a version that does not support the function.<br>**Mode 1093 = ON:** Background unmap cannot work.<br>**Mode 1093 = OFF (default):** Background unmap can work.<br>**Note:** This SOM is applied when downgrading microcode from a version that supports pool reduction rate correction to a version that does not support the function is disabled. | OFF | - |
| 1097 | Common | This SOM disables the warning LED to blink when specific SIMs are reported.<br>**Mode 1097 = ON:** When SIM=452XXX, 462XXX, 3077XY, 4100XX, or 410100 is reported, the warning LED does not blink.<br>**Mode 1097 = OFF (default):** When SIM=452XXX, 462XXX, 3077XY, 4100XX, or 410100 is reported, the warning LED blinks.<br>**Note:** This SOM disables the warning LED to blink when specific SIMs are reported. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 1106 | Dynamic Provisioning<br>Dynamic Tiering | This SOM is used to monitor the page usage rate of parity groups defined to a pool, and perform rebalance to balance the usage rate if the rate differs significantly among parity groups.<br>**Mode 1106 = ON:** The usage rate is checked once a day and the rebalance works if the rate is not even.<br>**Mode 1106 = OFF (default):** The rebalance does not work even when the usage rate is not balanced.<br>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.<br>**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.<br>Examples:<br>**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.<br>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.<br>**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.<br>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.<br>**3.** In an HDT pool, if the usage rates of PG1, PG2, and PG3 are 80% (SSD), 40% (SAS15K) and 30% (SAS15K), it is not determined as unbalanced, because:<br>▪ The average parity group usage rate of Tier1 is (80%) / 1 ＝ 80% and the difference in the | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| | | rate between the parity group and the average is 0%.<br>▪ 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.<br>**Note:** This SOM is applied when balancing the usage rate is required at a customer site where the usage rate is not even. | | |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 1115 | Deduplication and Compression | When this SOM is set to ON, data is initialized without using metadata at LDEV format for a virtual volume with Capacity Saving enabled.<br><br>**Mode 1115 = ON:** When LDEV format is performed for a virtual volume whose capacity saving setting is Compression, the data is initialized without using the metadata.<br><br>**Mode 1115 = OFF (default):** When LDEV format is performed for a virtual volume whose capacity saving setting is Compression, normal formatting is performed, but if one of the following conditions is met, the data is initialized without using metadata.<br><br>▪ There is a pinned slot.<br>▪ The capacity saving status is “Failed”.<br>▪ The virtual volume is blocked (Normal restore cannot be performed).<br><br>**Notes:**<br><br>**1.** This SOM is applied to recover a blocked pool volume in a pool to which a virtual volume whose capacity saving setting is Compression belongs.<br><br>For the information of setting timing, refer to the procedure for blocked pool volume recovery in the Maintenance Manual.<br><br>**2.** The processing time increases with increase in pool capacity.<br><br>Estimate of processing time:<br><br>Processing time (minutes) = ceiling(pool capacity (TB)/40) + 5<br><br>ceiling: The value enclosed in ceiling( ) must be rounded up to the nearest whole number.<br><br>The processing finishes early if there is less capacity of allocated pages.<br><br>**3.** Do not change this SOM setting during LDEV format for a virtual volume whose capacity saving setting is Compression. If the setting is changed, the processing cannot be performed correctly and may end abnormally depending on the timing.<br><br>**4.** This SOM is effective only for LDEV format for a virtual volume whose capacity saving setting is | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| | | Compression, so that there is no side effect in relation to user data, but the processing may take more time than that when this SOM is set to OFF depending on the pool capacity. Therefore, basically do not use this SOM for cases other than pool volume blockage recovery. | | |
| 1118 | Open | This SOM is used to disable the ENC reuse function.<br>**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.<br>**Mode 1118 = OFF (default):** When a failure occurs in the Expander chip mounted on a controller board (CTLS, CTLSE) or an ENC board, the reuse function works.<br>If the ENC is reusable, SIM=CF12XX and then CF14XX are reported, and the ENC is reused.<br>If the ENC is not reusable, SIM=CF12XX is reported, and the ENC is blocked.<br>**Note:** The ENC reuse function is enabled as default. This SOM is applied when you want to disable the ENC reuse function. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 1119 | Deduplication and Compression | This SOM is used to downgrade the microcode as follows while capacity saving is enabled:<br>▪ VSP Fx00 models, VSP Gx00 models: From 83-04-03-x0/00 or later to 83-04-01-x0/00 or 83-04-02-x0/00<br>New control information is added with 83-04-03 for the inflow control processing when capacity saving is enabled. However, it must be guaranteed that the area is not used when the microcode version is 83-04-01 or later. This SOM disables the control information added with 83-04-21 when capacity saving is enabled to enable microcode downgrade.<br>**Mode 1119 = ON:** The control information is not used when capacity saving is enabled.<br>**Mode 1119 = OFF (default):** The control information is used when capacity saving is enabled.<br>**Notes:**<br>**1.** Set this SOM to ON when the microcode downgrade described above is performed, even if capacity saving is not currently in use but has been used before.<br>**2.** After the microcode downgrade is complete, make sure to set this SOM to OFF.<br>**3.** This SOM is effective for the entire storage system.<br>**4.** The write performance might degrade when this SOM is ON. | OFF | - |

| Mode | Category | Description | Default | MCU/RCU |
|---|---|---|---|---|
| 1120 | Dynamic Provisioning<br>Thin Image | This SOM disables TI pair creation in DP pools and releases cache management devices to enable the microcode downgrade from 80-05-44 or later to earlier than 80-05-44 or from 83-04-44 or later to earlier than 83-04-44.<br>**Mode 1120 = ON:** TI pair creation with DP pool specified is disabled. Also, if any cache management devices are reserved while there is no TI pool in the storage system, all cache management devices are released.<br>**Mode 1120 = OFF (default):** No action.<br>**Notes:**<br>**1.** Set this SOM to ON when the microcode downgrade described above is performed while there is a DP pool in the storage system.<br>**2.** Set this SOM to ON only when downgrading the microcode.<br>**3.** Before setting this SOM to ON, delete all TI pairs in DP pools.<br>**4.** After the microcode downgrade is complete, make sure to set this SOM to OFF. | OFF | - |

# Glossary

## #

**2DC**

two-data-center. Refers to the local and remote sites, or data centers, in which TrueCopy (TC) and Universal Replicator (UR) combine to form a remote replication configuration.

In a 2DC configuration, data is copied from a TC primary volume at the local site to the UR master journal volume at an intermediate site, then replicated to the UR secondary volume at the remote site. Since this configuration side-steps the TC secondary volume at the intermediate site, the intermediate site is not considered a data center.

**3DC**

three-data-center. Refers to the local, intermediate, and remote sites, or data centers, in which TrueCopy and Universal Replicator combine to form a remote replication configuration.

In a 3DC configuration, data is copied from a local site to an intermediate site and then to a remote site (3DC cascade configuration), or from a local site to two separate remote sites (3DC multi-target configuration).

## A

**array**

See disk array

**audit log**

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

## B

**back-end director (BED)**

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

**BED**

See back-end director.

**bind mode**

In bind mode the Cache Residency Manager extents are used to hold read and write data for specific extent(s) on volume(s). Data written to the Cache Residency Manager bind area is not destaged to the drives. For bind mode, all targeted read and write data is transferred at host data transfer speed.

**blade**

A computer module, generally a single circuit board, used mostly in servers.

## C

**cache logical partition (CLPR)**

Consists of virtual cache memory that is set up to be allocated to different hosts in contention for cache memory.

**capacity**

The amount of data storage space available on a physical storage device, usually measured in bytes (MB, GB, TB, and so on).

**CCI**

Command Control Interface

**CHAP**

challenge handshake authentication protocol

**CLPR**

See *cache logical partition (CLPR)*.

**cluster**

Multiple-storage servers working together to respond to multiple read and write requests.

**command device**

A dedicated logical volume used only by Command Control Interface and Business Continuity Manager to interface with the storage system. Can be shared by several hosts.

**controller**

The component in a storage system that manages all storage functions. It is analogous to a computer and contains a processors, I/O devices, RAM, power supplies, cooling fans, and other sub-components as needed to support the operation of the storage system.

**copy pair**

A pair of volumes in which one volume contains original data and the other volume contains the copy of the original. Copy operations can be synchronous or asynchronous, and the volumes of the copy pair can be located in the same storage system (local copy) or in different storage systems (remote copy).

A copy pair can also be called a volume pair, or just pair. A pair created by Compatible FlashCopy® is called a relationship.

**copy-on-write (COW)**

Point-in-time snapshot copy of any data volume within a storage system. Copy-on-write snapshots only store changed data blocks, therefore the amount of storage capacity required for each copy is substantially smaller than the source volume.

**COW**

See *copy-on-write (COW)*.

**COW Snapshot**

Hitachi Copy-on-Write Snapshot

**custom volume (CV)**

A custom-size volume whose size is defined by the user using Virtual LVI/Virtual LUN.

**CV**

See custom volume.

**CVS**

custom volume size

**CXFS**

clustered version of XFS file system

# D

**data drive**

A physical data storage device that can be either a hard disk drive (HDD) or a flash drive (also called a solid-state device).

**DBV**

Hitachi Database Validator

**DC**

data center

**delta resync**

A disaster recovery solution in which TrueCopy and Universal Replicator systems are configured to provide a quick recovery using only differential data stored at an intermediate site.

**device**

A physical or logical unit with a specific function.

**device emulation**

Indicates the type of logical volume. Mainframe device emulation types provide logical volumes of fixed size, called logical volume images (LVIs), which contain EBCDIC data in CKD format. Typical mainframe device emulation types include 3390-9 and 3390-M. Open-systems device emulation types provide logical volumes of variable size, called logical units (LUs), that contain ASCII data in FBA format. The typical open-systems device emulation type is OPEN-V.

**disaster recovery**

A set of procedures to recover critical application data and processing after a disaster or other failure.

**disk array**

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

**disk controller (DKC)**

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

**DKC**
See *disk controller (DKC)*.
**DKCMAIN**
disk controller main. Refers to the software for the storage system.
**DKU**

disk unit. Refers to the cabinet (floor model) or rack-mounted hardware component that contains data drives and no controller components.

**dump**

A collection of data that is saved to a file when an error or crash occurs. The data is used by support personnel to determine the cause of the error or crash.

**Dump tool**

Downloads Device Manager - Storage Navigator configuration information onto recording media for backup and troubleshooting purposes.

# E

**emulation**

The operation of a storage system to emulate the characteristics of a different storage system. For device emulation, the mainframe host recognizes the logical devices on the storage system as 3390-x devices. For controller emulation, the mainframe host recognizes the control units (CUs) on the storage system as 2105 or 2107 controllers.

The storage system operates the same as the storage system being emulated.

**emulation group**

A set of device emulation types that can be intermixed within a RAID group and treated as a group.

**external application**

A software module that is used by a storage system but runs on a separate platform.

**external volume**

A logical volume whose data resides on drives that are physically located outside the Hitachi storage system.

# F

**FC**

Fibre Channel; FlashCopy

**FC-AL**

fibre-channel arbitrated loop

**FCP**

fibre-channel protocol

**FCSP**

fibre-channel security protocol

**FICON**

Fibre Connectivity

**flash drive**

A data drive that uses a solid-state memory device instead of a rotating hard disk.

**flash module**

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

**FMD**

See flash module

# H

**HBA**

host bus adapter

**HDD**

hard disk drive

**HDT**

Hitachi Dynamic Tiering

**HDU**

hard disk unit

**head LDEV**

See top LDEV.

**host group**

A group of hosts of the same operating system platform.

**host mode**

Operational modes that provide enhanced compatibility with supported host platforms. Used with fibre-channel ports on RAID storage systems.

**host mode option**

Additional options for fibre-channel ports on RAID storage systems. Provide enhanced functionality for host software and middleware.

**HP XP7 CVAE**

HP XP7 Command View Advanced Edition - a set of software applications included in the system firmware. Via the GUI, they are used to configure, control, and monitor the storage system.

# I

**in-system replication**

The original data volume and its copy are located in the same storage system. ShadowImage in-system replication provides duplication of logical volumes; Thin Image in-system replication provides "snapshots" of logical volumes that are stored and managed as virtual volumes (V-VOLs).

See also *remote replication*.

**initiator**

An attribute of the port that is connected to the port with RCU target attribute.

**internal volume**

A logical volume whose data resides on drives that are physically located within the storage system. See also *external volume*.

# J

**JNL**

journal

**journal volume**

A volume that records and stores a log of all events that take place in another volume. In the event of a system crash, the journal volume logs are used to restore lost data and maintain data integrity.

In Universal Replicator, differential data is held in journal volumes on until it is copied to the S-VOL.

**JRE**

Java Runtime Environment

# K

**key management server**

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

**keypair**

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

# L

**LBA**

logical block address

**LCP**

local control port; link control processor

**LD**

local directory; logical device

**LDAP**

lightweight directory access protocol

**LDEV**

logical device

**LDKC**

See *logical disk controller (LDKC)*.

**LDM**

Logical Disk Manager

**license key**

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

**local control port (LCP)**

A serial-channel (ESCON) port configured to receive I/Os from a host or remote I/Os from a TrueCopy main control unit (MCU).

**local copy**

See in-system replication.

**local storage system**

A storage system connected to the management client.

**logical device (LDEV)**

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

**logical disk controller (LDKC)**

A group of 255 control unit (CU) images in the RAID storage system that is controlled by a virtual (logical) storage system within the single physical storage system. For example, the Hitachi Universal Storage Platform V storage system supports two LDKCs, LDKC 00 and LDKC 01.

**logical partition (LPAR)**

A subset of a system's hardware resources that is virtualized as a separate system. For a storage system, logical partitioning can be applied to cache memory and/or storage capacity.

**logical unit (LU)**

A logical volume that is configured for use by open-systems hosts (for example, OPEN-V).

**logical unit (LU) path**

The path between an open-systems host and a logical unit.

**logical volume (LV)**

See *volume*.

**logical volume image (LVI)**

A logical volume that is configured for use by mainframe hosts (for example, 3390-9).

**LU**

See *logical unit (LU)*.

**LUN**

See logical unit number

**LUN volume**

A custom-size volume whose size is defined by the user using Virtual LUN. Also called a custom volume (CV).

**LV**

logical volume

**LVI**

See *logical volume image*.

# M

**MF, M/F**

mainframe

**modify mode**

The mode of operation of Device Manager - Storage Navigator that allows changes to the storage system configuration. See also view mode.

# O

**OPEN-V**

A logical unit (LU) of user-defined size that is formatted for use by open-systems hosts.

**OPEN-x**

A logical unit (LU) of fixed size (for example, OPEN-3 or OPEN-9) that is used primarily for sharing data between mainframe and open-systems hosts using Hitachi Cross-OS File Exchange.

# P

**P-VOL**

This term is used only in the earlier version of the Device Manager - Storage Navigator GUI (still in use) for the primary volume. See primary volume.

**pair**

Two logical volumes in a replication relationship in which one volume contains original data to be copied and the other volume contains the copy of the original data. The copy operations can be synchronous or asynchronous, and the pair volumes can be located in the same storage system (in-system replication) or in different storage systems (remote replication).

**parity group**

See RAID group.

**PAV**

Hitachi Compatible PAV

**PCB**

printed circuit board

**PDEV**

physical device

**PG**

parity group. See RAID group.

**physical device**

See device.

**pool**

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

**pool volume (pool-VOL)**

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

**port attribute**

Indicates the type of fibre-channel port: target, RCU target, or initiator.

**primary volume (P-VOL)**

The volume in a copy pair that contains the original data to be replicated. The data on the P-VOL is duplicated synchronously or asynchronously on the secondary volume (S-VOL).

The following Hitachi products use the term P-VOL: Thin Image, Copy-on-Write Snapshot, ShadowImage, TrueCopy, Universal Replicator, Universal Replicator for Mainframe, and High Availability Manager.

See also secondary volume.

**prio**

priority mode. Used in Cache Residency Manager.

# Q

**quick format**

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

**quick restore**

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

# R

**RAID**

redundant array of inexpensive disks

**RAID group**

A set of RAID disks that have the same capacity and are treated as one group for data storage and recovery. A RAID group contains both user data and parity information. This allows user data to be accessed in the event that one or more of the drives within the RAID group are not available. The RAID level of a RAID group determines the number of data drives and parity drives and how the data is "striped" across the drives. For RAID1, user data is duplicated within the RAID group, so there is no parity data for RAID1 RAID groups.

A RAID group can also be called an array group or a parity group.

**RAID level**

The type of RAID implementation. RAID levels include RAID0, RAID1, RAID2, RAID3, RAID4, RAID5 and RAID6.

**RCU**

See remote control unit.

**RCU target port**

A fibre-channel port that is configured to receive remote I/Os from an initiator port on another storage system.

**remote control unit (RCU)**

A storage system at a secondary or remote site that is configured to receive remote I/Os from one or more storage systems at the primary or main site.

**remote copy**

See remote replication.

**resync**

resynchronize.

**RMI**

Remote Method Invocation

# S

**S-VOL**

See secondary volume or source volume. When used for "secondary volume", "S-VOL" is only seen in the earlier version of the Device Manager - Storage Navigator GUI (still in use).

**SAS**

serial-attached SCSI

**secondary volume (S-VOL)**

The volume in a copy pair that is the copy of the original data on the primary volume (P-VOL). The following Hitachi products use the term "secondary volume": Thin Image, Copy-on-Write Snapshot, ShadowImage, TrueCopy, Universal Replicator, Universal Replicator for Mainframe, and High Availability Manager.

See also primary volume.

**service information message (SIM)**

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

**service processor**

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

**severity level**

Applies to service information messages (SIMs) and Device Manager - Storage Navigator error codes.

**SFP**

small form-factor pluggable

**shared memory**

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

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

**shredding**

See volume shredding.

**SIM**

See service information message.

**size**

Generally refers to the storage capacity of a memory module or cache. Not usually used for storage of data on disk or flash drives.

**SM**

shared memory

**SMTP**

simple mail transfer protocol

**snapshot**

A point-in-time virtual copy of a Hitachi Thin Image primary volume (P-VOL). The snapshot is maintained when the P-VOL is updated by storing pre-updated data (snapshot data) in a data pool.

**SNMP**

See *Simple Network Management Protocol*.

**SOM**

See system option mode.

**source volume (S-VOL)**

Used only in the earlier version of the Device Manager - Storage Navigator GUI (still in use). This is the volume in a mainframe copy pair containing the original data that is duplicated on the target volume (T-VOL). The following Hitachi products use the term source volume: ShadowImage for Mainframe, Dataset Replication, and Compatible FlashCopy®.

In the current version of the GUI, "target volume" and "T-VOL" are replaced with "primary volume".

See also source volume.

**space**

Generally refers to the data storage capacity of a disk drive or flash drive.

**SRM**

Storage Replication Manager

**SSD**

solid-state drive. Also called flash drive.

**SSID**

See *storage subsystem identifier*.

**SSL**

secure socket layer

**storage cluster**

See cluster.

**storage tiers**

See tiered storage.

**SVP**

See *service processor*.

**SVS**

Storage Virtualization System

**SW, sw**

short wavelength, software

**syslog**

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

**system disk**

The volume from which an open-systems host boots.

**system option mode (SOM)**

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

# T

**T-VOL**

See target volume.

**target**

An attribute of the port that is connected to the host.

**target port**

A fibre-channel port that is configured to receive and process host I/Os.

**target volume (T-VOL)**

The volume in a mainframe copy pair that is the copy of the original data on the source volume (S-VOL). The term is used only in the earlier version of the Device Manager - Storage Navigator GUI (still

in use), for the following Hitachi products: ShadowImage for Mainframe, Dataset Replication, and Compatible FlashCopy® V2.

See also *source volume*.

**TC**

Hitachi TrueCopy

**TI**

See Thin Image.

**tiered storage**

A layered structure of performance levels, or tiers, that matches data access requirements with the appropriate performance tiers. The tiers are:

Tier 1: Static content. Tier 1 is fully supported computing expected to be production quality.

Tier 2: Application logic. Tier 2 platforms are not supported by the security officer and release engineering teams. Tier 2 systems are targeted for Tier 1 support, but are still under development.

Tier 3: Database. Tier 3 platforms are architectures for which hardware is not or will not be available or that are considered legacy systems unlikely to see broad future use.

Tier 4 systems are not supported.

**total capacity**

The aggregate amount of storage space in a data storage system.

**TPF**

Transaction Processing Facility

# V

**V-VOL**

virtual volume

**VDEV**

See virtual device.

**view mode**

The mode of operation of Device Manager - Storage Navigator that allows viewing only of the storage system configuration. The two Device Manager - Storage Navigator modes are view mode and modify mode.

**virtual device (VDEV)**

A group of logical devices (LDEVs) in a RAID group. A VDEV typically consists of some fixed volumes (FVs) and some free space. The number of fixed volumes is determined by the RAID level and device emulation type.

**virtual volume (V-VOL)**

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

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

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

**VLUN**

Hitachi Virtual LUN

**VM**

volume migration; volume manager

**volume (VOL or vol)**

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

**volume shredding**

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

# Index

## E



## F



## G



## H



## I



## J



## K



## L



## M



## N



## O



## P

## R



## S

## T



## U



## V



## W

**Hitachi Vantara**

Corporate Headquarters
2845 Lafayette Street
Santa Clara, CA 95050-2639 USA
www.HitachiVantara.com | community.HitachiVantara.com

Regional Contact Information
Americas: +1 866 374 5822 or info@hitachivantara.com
Europe, Middle East, and Africa: +44 (0) 1753 618000 or info@emea@hitachivantara.com
Asia Pacific: + 852 3189 7900 or info.marketing.apac@hitachivantara.com