

# Hitachi Virtual Storage Platform G1x00 and F1500

SVOS 8.3

---

## System Administrator Guide

This document provides information and instructions to help you set up Hitachi Device Manager - Storage Navigator for your storage system, and manage user accounts and permissions. It explains the GUI features and provides basic navigation information.

© 2010, 2018 Hitachi, Ltd. All rights reserved.

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

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

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

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

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

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

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

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

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

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

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

---

# Contents

<b>Preface.....</b>	<b>0</b>
<b>Preface.....</b>	<b>14</b>
Intended audience.....	14
Product version.....	14
Release notes.....	14
Changes in this revision.....	15
Referenced documents.....	15
Document conventions.....	15
Conventions for storage capacity values.....	16
Accessing product documentation.....	17
Getting help.....	17
Comments.....	18
<b>Chapter 1: Configuring the storage system software.....</b>	<b>19</b>
Setup workflow.....	19
Requirements for management clients.....	20
General requirements.....	20
Requirements for Windows-based computers.....	20
Requirements for UNIX/Linux-based computers.....	22
Network settings overview.....	23
Configuring IPv6 communication in Windows 7.....	23
Configuring IPv6 communication in Solaris 10.....	24
Setting up a management client.....	24
Configuring a Windows Server.....	24
Configuring the web browser.....	25
Adding your SVP to the trusted sites zone for Windows Server computers.....	25
Setting Device Manager - Storage Navigator environmental parameters.....	26
Device Manager - Storage Navigator environmental parameters.....	27
Setting up Java.....	28
Changing Java security settings.....	31
Device Manager - Storage Navigator secondary windows.....	31
Requirements for using HDvM - SN secondary windows.....	32
Installing and configuring JRE.....	33
Enabling the Device Manager - Storage Navigator secondary window.....	33

Lowering the IE security level on Windows Server 2012 or later.....	34
Device Manager - Storage Navigator restrictions.....	34
General restrictions.....	34
Web browser restrictions while using Device Manager - Storage Navigator.....	35
Unsupported actions in Windows version of HDvM - SN.....	36
Unsupported actions in UNIX version of HDvM - SN.....	36
Applying changes made in Device Manager - Storage Navigator.....	37
Updating data after a Volume Migration or Quick Restore operation.....	37
Updating data after operations performed with another application.....	38
Capacities displayed on the Device Manager - Storage Navigator screen..	38
Caution on LUN ID notation.....	38

## **Chapter 2: Using Device Manager - Storage Navigator..... 39**

Logging in to Device Manager - Storage Navigator.....	39
Initial superuser login.....	39
User login.....	40
Changing the initial password.....	41
Navigating the Device Manager - Storage Navigator user interface.....	41
Menu bar.....	42
Using the Device Manager - Storage Navigator main window.....	43
Main window controls.....	44
Main window and Modify mode.....	47
Using Device Manager - Storage Navigator secondary windows.....	47
Secondary windows and wizards.....	47
Secondary window menus and buttons.....	48
Opening Device Manager - Storage Navigator secondary windows.....	50
HDvM - SN secondary windows and Modify mode.....	51
Resetting timeout period for Modify mode.....	51
Resetting the secondary window.....	52
Cautions when using secondary windows.....	52
Troubleshooting secondary windows.....	54
Balloon dialog box.....	65
Session timeout.....	65
Updating your user view.....	65
Reverting to the default view.....	66
Creating a login message.....	67

## **Chapter 3: Configuring the storage system..... 68**

Setting storage system information.....	68
Setting up security.....	68
Setting up TCP/IP for a firewall.....	69

Managing authentication and authorization servers.....	70
Authentication server requirements.....	70
Authorization server requirements.....	72
Connecting authentication and authorization servers.....	72
Setting up SSL encryption.....	73
SSL terminology.....	74
Setting up SSL communications.....	74
Notes on updating the signed certificate to the SVP.....	75
Creating a keypair.....	75
Converting the SSL certificates to PKCS#12 format.....	77
Obtaining a signed certificate.....	78
Releasing an SSL certificate passphrase.....	79
Uploading a signed certificate.....	80
Returning the certificate to default.....	81
Problems with a website security certificate.....	82
Disabling TLSv1.0 and TLSv1.1 communications.....	83
Enabling TLSv1.0 and TLSv1.1 communications.....	83
Blocking HTTP communication to the storage system.....	83
Releasing HTTP communication blocking.....	85
Configuring certificates for HCS.....	85
Registering certificates for HCS.....	86
Notes on registering certificates for HCS.....	87
Deleting certificates for HCS.....	87
Changing advanced system settings.....	88
Backing up HDvM - SN configuration files.....	90
Restoring HDvM - SN configuration files.....	92
Using the SMI-S function with a Device Manager - Storage Navigator user account.....	93
Using the SMI-S function.....	93
Uploading a signed certificate to the SMI-S provider.....	93
Returning an SMI-S provider certificate to default.....	95
Uploading an SMI-S provider configuration file.....	96
Returning an SMI-S provider configuration file to default.....	98
Sending SMI-S artificial indication.....	99
Registering the primary SVP host name.....	100
<b>Chapter 4: User administration using Device Manager - Storage Navigator.....</b>	<b>102</b>
User administration overview.....	102
Manage roles and permissions.....	102
Roles and user groups.....	103
Resource group and user groups.....	104

User group registration example.....	104
Precautions when working with user groups.....	105
Naming a user group in Device Manager - Storage Navigator.....	105
Roles and permissions.....	105
Built-in user groups.....	108
Verifying the roles available to a user group.....	110
Verifying the roles available to a user group.....	110
Creating a new user group.....	111
Changing a user group name.....	112
Changing user group permissions.....	112
Changing assigned resource groups.....	113
Deleting a user group.....	113
User accounts.....	114
Creating user accounts.....	114
Character restrictions for user names and passwords.....	115
Changing user passwords.....	117
Changing user permissions.....	118
Enabling and disabling user accounts.....	118
Deleting user accounts.....	119
Managing resource groups.....	119
About resource groups .....	120
Examples.....	121
Resource groups sharing a port.....	121
Resource groups not sharing ports.....	122
Resource group assignments.....	124
Resource group rules, restrictions, and guidelines.....	124
Creating resource groups.....	124
Adding resources to a resource group.....	125
Deleting resource groups.....	126
Account lock policy.....	127
Unlock a user account.....	127
<b>Chapter 5: Managing license keys.....</b>	<b>128</b>
License keys overview.....	128
License key types.....	128
Using the permanent key.....	129
Using the term key.....	130
Using the temporary key.....	130
Using the emergency key.....	130
Estimating licensed capacity.....	131
Software and licensed capacity.....	131
Calculating licensed capacity for a normal volume.....	136

Calculating licensed capacity for an external volume.....	137
Calculating pool capacity.....	137
Accelerated compression-enabled parity group capacity.....	137
Installing and uninstalling software.....	137
Installing license keys using Device Manager - Storage Navigator.....	137
When the status is Installed (Disabled).....	138
Enabling a license.....	138
Disabling a license.....	139
Removing a software application.....	139
Updating license status.....	140
Examples of license information.....	140
Cautions on license capacities in license-related windows.....	141
Cautions on licenses.....	142
Resolving errors when removing Data Retention Utility.....	142
License key expiration.....	142

## **Chapter 6: Viewing and managing the storage system.....144**

Viewing storage system information.....	144
Viewing basic information.....	144
Viewing specific information.....	145
Viewing other system information.....	145
Viewing port conditions.....	146
Status icons for certain resources.....	146
Using the storage system in high temperature mode.....	147
Enabling high temperature mode.....	149
Managing tasks.....	149
Tasks window.....	150
Managing your tasks.....	150
Referencing the detailed task status.....	150
Stalled tasks.....	153
Setting the status refresh interval of the Tasks window.....	153

## **Chapter 7: Using reports to view storage system information.....154**

Creating configuration reports.....	154
Viewing configuration reports.....	154
Viewing configuration reports in the Reports window.....	155
Deleting configuration reports.....	155
Examples of Device Manager - Storage Navigator storage configuration reports.....	156
Report examples: table view.....	156
CHAP Users report.....	156
Disk Adapters report.....	157

Host Groups / iSCSI Targets report.....	158
Hosts report.....	160
Logical Devices report.....	160
LUNs report.....	163
MP Blades report.....	164
MP Blade Details report.....	164
Parity Groups report.....	165
Ports report.....	168
Power Consumption report.....	170
Spare Drives report.....	172
SSD Endurance report.....	173
Storage System Summary report.....	174
Report examples: graphical view.....	177
Cache Memories report.....	177
Channel Adapters report.....	178
Physical View report.....	178
Report examples: CSV files.....	179
AllConf.csv.....	179
CacheInfo.csv.....	179
ChapUserInfo.csv.....	180
ChaStatus.csv.....	180
DcrlInfo.csv.....	181
DeviceEquipInfo.csv.....	181
DkaInfo.csv.....	182
DkaStatus.csv.....	182
DkclInfo.csv.....	183
DkuTempInfo.csv.....	184
DkuTempAveInfo.csv.....	186
DkuTempMaxInfo.csv.....	187
DkuTempMinInfo.csv.....	188
ELunInfo.csv.....	189
EnvMonInfo.csv.....	191
FcSpNameInfo.csv.....	193
FcSpPortInfo.csv.....	193
HduInfo.csv.....	194
IscsiHostInfo.csv.....	194
IscsiPortInfo.csv.....	195
IscsiTargetInfo.csv.....	197
JnlInfo.csv.....	198
LdevCapalInfo.csv.....	199
LdevCountInfo.csv.....	199



LdevInfo.csv.....	200
LdevStatus.csv.....	203
LogPathStatus.csv.....	204
LPartition.csv.....	204
LunInfo.csv.....	205
LunPortInfo.csv.....	207
MfDMIInfo.csv.....	208
MicroVersion.csv.....	209
MlcEnduranceInfo.csv.....	210
ModePerLpr.csv.....	210
MpPathStatus.csv.....	211
MpPcbStatus.csv.....	212
PcbRevInfo.csv.....	213
PdevCapalInfo.csv.....	213
PdevInfo.csv.....	214
PdevStatus.csv.....	215
PhyPathStatus.csv.....	216
PkInfo.csv.....	217
PplInfo.csv.....	219
SMfundat.csv.....	220
SsdDriveInfo.csv.....	221
SsidInfo.csv.....	222
SysoptInfo.csv.....	222
WwnInfo.csv.....	223

**Chapter 8: Troubleshooting..... 225**

Getting help.....	225
General troubleshooting.....	225
Monitoring SIMs alerts in Device Manager - Storage Navigator.....	226
Login errors.....	227
No-response errors.....	229
Incorrect display errors.....	233
UNIX operation errors.....	236
Other errors.....	237
Clearing the cache in Internet Explorer.....	238
Clearing the cache in Firefox.....	238
Enabling JavaScript for Windows.....	239
Firefox web browser problems on UNIX.....	239
Downloading dump files using the Dump tool.....	240
Troubleshooting the SMI-S function.....	242
SMI-S artificial indication errors.....	242

## Appendix A: Device Manager - Storage Navigator user management GUI reference..... 243

User Groups window.....	243
Selected User Group Window.....	244
Create User Group wizard.....	248
Create User Group window.....	248
Create User Group confirmation window.....	250
Create User wizard.....	252
Create User window.....	252
Create User confirmation window.....	254
Change Password Wizard.....	255
Change Password window.....	255
Change Password confirmation window.....	256
Edit User wizard.....	256
Edit User window.....	256
Edit User confirmation window.....	258
Add User wizard.....	259
Add Users window.....	259
Add Users confirmation window.....	262
Remove Users window.....	263
Delete Users window.....	264
Release Lockout window .....	265
Edit User Group wizard.....	266
Edit User Group window.....	266
Edit User Group confirmation window.....	267
Delete User Groups window.....	268
Edit Resource Group Assignment wizard.....	268
Edit Resource Group Assignment window.....	268
Edit Resource Group Assignment confirmation window.....	273
Edit Role Assignment wizard.....	275
Edit Role Assignment window.....	275
Edit Role Assignment confirmation window.....	278
Setup Server wizard.....	279
Select Authentication Server window.....	279
Select Authentication Server confirmation window.....	280
LDAP Properties window.....	280
RADIUS Properties window.....	282
Kerberos Properties window.....	285
Setup Server for LDAP.....	288
LDAP Setup Server window.....	288
LDAP Setup Server confirmation window.....	292

Setup Server for RADIUS.....	294
RADIUS Setup Server window.....	294
RADIUS Setup Server confirmation window.....	301
Setup Server for Kerberos.....	303
Kerberos Setup Server window.....	303
Kerberos Setup Server confirmation window.....	309

## **Appendix B: Device Manager - Storage Navigator licenses GUI reference.....312**

License Keys window.....	312
Install Licenses wizard.....	315
Install Licenses window.....	315
Install Licenses confirmation window.....	318
Enable Licenses window.....	319
Disable Licenses window.....	321
Remove Licenses window.....	323
Update License Status window.....	325

## **Appendix C: Configuring storage systems GUI reference.....328**

Login Message window.....	328
Edit Storage System wizard.....	329
Edit Storage System window.....	329
Edit Storage System confirmation window.....	330
Edit Alert Settings wizard.....	330
Edit Alert Settings window.....	331
Add Sending Trap Setting window (SNMP v1 or v2c).....	341
Add Sending Trap Setting window (SNMP v3).....	342
Change Sending Trap Setting window (SNMP v1 or v2c).....	344
Change Sending Trap Setting window (SNMP v3).....	346
Add Request Authentication Setting window (SNMP v1 or v2c).....	347
Add Request Authentication Setting window (SNMP v3).....	349
Change Request Authentication Setting window (SNMP v1 or v2c).....	351
Change Request Authentication Setting window (SNMP v3).....	353
Add Address window.....	355
Change Settings window.....	356
Edit Alert Settings confirmation window.....	358
Column Settings window.....	362
Edit Advanced System Settings wizard.....	363
Edit Advanced System Settings window.....	364
Edit Advanced System Settings confirmation window.....	366
Edit High Temperature Mode wizard.....	367
Edit High Temperature Mode window.....	367

Edit High Temperature Mode confirmation window.....	368
<b>Appendix D: Device Manager - Storage Navigator system GUI reference.....</b>	<b>370</b>
Storage Systems window.....	370
Port Condition window.....	376
Tasks window.....	378
Task Properties window.....	380
Suspend Tasks window.....	381
Resume Tasks window.....	382
Delete Tasks window.....	383
Disable Auto Delete window.....	384
Enable Auto Delete window.....	384
Edit Information Display Settings window.....	385
Reports window.....	387
Create Configuration Report window.....	387
Delete Reports window.....	388
<b>Appendix E: Tool Panel GUI Reference.....</b>	<b>398</b>
Control Panel.....	398
Environment Parameter window.....	398
Download File window.....	399
Restore File window.....	399
Download Dump Files window.....	400
Update Certificate Files window.....	401
Update Certificate Files for the SMI-S window.....	402
Upload Configuration Files for SMI-S window.....	403
SMI-S Artificial Indication window.....	404
Set or Delete Certificate File for HCS window.....	405
<b>Appendix F: SMI-S provider configuration file.....</b>	<b>407</b>
Array-setting-01.properties file.....	407
File description format.....	407
File organization format.....	407
Parameters defined in user configuration files.....	407
VVolForSnapshot parameter.....	408
PoolIDForSnapshot parameter.....	409
ResourceGroup parameter.....	410
<b>Appendix G: System option modes (SOMs).....</b>	<b>411</b>
System option modes.....	411

**Index..... 494**

---

## Preface

This document provides information and instructions to help you set up Hitachi Device Manager - Storage Navigator for your storage system, and manage user accounts and permissions. It explains the GUI features and provides basic navigation information.

Additional information about performing specific tasks in Hitachi Device Manager - Storage Navigator is contained in the software user guides.

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

## Intended audience

This document is intended for system administrators, Hitachi Vantara representatives, and authorized service providers who are involved in installing, configuring, and operating Hitachi Virtual Storage Platform G1000, Virtual Storage Platform G1500, and Hitachi Virtual Storage Platform F1500 storage systems.

Readers of this document should be familiar with the following:

- Data processing and RAID storage systems and their basic functions.
- The Hitachi Virtual Storage Platform G1000, Virtual Storage Platform G1500, and Hitachi Virtual Storage Platform F1500 storage systems *Product Overview*.
- The operating system and web browser software on the SVP hosting the Device Manager - Storage Navigator software.

## Product version

This document applies to the following product versions:

- VSP G1x00, VSP F1500: Microcode 80-06-6x or later
- SVOS RF: 8.3 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

- Changed description of LAN cables.
- Updated information on capacity saving.
- Updated the descriptions of the following system option modes (SOMs): 448, 449, 664, 1115.

## Referenced documents

- *Hitachi Device Manager - Storage Navigator Messages*, MK-948017





## Document conventions

This document uses the following typographic conventions:

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

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

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

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

## Conventions for storage capacity values

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

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10 <sup>3</sup> ) bytes
1 megabyte (MB)	1,000 KB or 1,000 <sup>2</sup> bytes
1 gigabyte (GB)	1,000 MB or 1,000 <sup>3</sup> bytes
1 terabyte (TB)	1,000 GB or 1,000 <sup>4</sup> bytes



Physical capacity unit	Value
1 petabyte (PB)	1,000 TB or 1,000 <sup>5</sup> bytes
1 exabyte (EB)	1,000 PB or 1,000 <sup>6</sup> bytes

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

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KB Open-systems: <ul style="list-style-type: none"> <li>▪ OPEN-V: 960 KB</li> <li>▪ Others: 720 KB</li> </ul>
1 KB	1,024 (2 <sup>10</sup> ) bytes
1 MB	1,024 KB or 1,024 <sup>2</sup> bytes
1 GB	1,024 MB or 1,024 <sup>3</sup> bytes
1 TB	1,024 GB or 1,024 <sup>4</sup> bytes
1 PB	1,024 TB or 1,024 <sup>5</sup> bytes
1 EB	1,024 PB or 1,024 <sup>6</sup> bytes

## Accessing product documentation

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

## Getting help

[Hitachi Vantara Support Connect](https://support.hitachivantara.com/en_us/contact-us.html) is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect for contact information: [https://support.hitachivantara.com/en\\_us/contact-us.html](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](https://community.hitachivantara.com), register, and complete your profile.

## Comments

Please send us your comments on this document to [doc.comments@hitachivantara.com](mailto: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: Configuring the storage system software

Device Manager - Storage Navigator (HDvM - SN) is the application used to configure the storage system.

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

Device Manager - Storage Navigator is factory-installed and runs on the service processor (SVP) connected to the storage system.

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

## Setup workflow

Before you start managing your storage system, confirm the requirements and perform set up procedures. The following workflow describes the set up tasks for Device Manager - Storage Navigator:

1. Set up the management clients. See [Setting up a management client \(on page 24\)](#).
2. An Hitachi Vantara representative attaches the SVP in your storage system to the LAN. Device Manager - Storage Navigator is already set up on the SVP and is therefore ready for access by management clients.
3. Set up network connections. If needed, see [Network settings overview \(on page 23\)](#).
4. Set up additional communications security for remote operations with Secure Sockets Layer (SSL) if required. See [Setting up SSL encryption \(on page 73\)](#) for details.
5. Set up user accounts. See [User accounts \(on page 114\)](#).
6. Configure the management environment. See [Device Manager - Storage Navigator environmental parameters \(on page 27\)](#).
7. Install license keys for any software applications that are installed on the system. See [Managing license keys \(on page 128\)](#).

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

## 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 storage system concurrently.
- Use category 5e or 6a LAN cable for LAN connections when the transfer speed is 1 Gbps. Maximum cable length is 328 feet (100 meters). For assistance, contact customer support.

### Requirements for Windows-based computers

The storage system must meet hardware and software requirements to run Windows as the operating system.

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.

#### Hardware requirements

Item	Requirement
Processor (CPU)	Pentium 4 640 3.2 GHz or better (Recommended: Core2Duo E6540 2.33 GHz or better)
Memory (RAM)	2 GB or more Recommended: 3 GB

Item	Requirement
Available storage space	500 MB or more
Monitor	True Color 32-bit or better Resolution: 1280 x 1024 or better
Keyboard and mouse	You cannot use the mouse wheel feature.
Ethernet LAN card for TCP/IP network	100BASE-TX 1000BASE-T

### Software requirements

Operating system	Browser	Java Runtime Environment (JRE)	Adobe Flash Player
Windows Server 2008 (SP2) 32 bit or 64 bit	Internet Explorer 9.0	JRE 7.0 Update 17	11.7
	Internet Explorer 9.0	JRE 7.0 Update 17	11.7
Windows 2008 R2 (SP1) 64 bit	Internet Explorer 11.0	JRE 7.0 Update 51	12.0
Windows Server 2012 64 bit	Internet Explorer 10.0	JRE 7.0 Update 17	11.7
Windows Server 2012 R2 64 bit	Internet Explorer 11.0	JRE 7.0 Update 51	12.0
Windows Server 2016 64 bit	Internet Explorer 11.0	JRE 8.0 Update 111	24.0
Windows Server Vista (SP2) 32 bit or 64 bit	Internet Explorer 9.0	JRE 7.0 Update 17	11.7
	Internet Explorer 9.0	JRE 7.0 Update 17	11.7
Windows 7 (SP1) 32 bit or 64 bit	Internet Explorer 11.0	JRE 7.0 Update 51	12.0
	Internet Explorer 11.0	JRE 7.0 Update 51	12.0
Windows 8.1 32 bit or 64 bit	Google Chrome 48.0 or later	JRE 8.0 Update 71	20.0
	Internet Explorer 11.0	JRE 7.0 Update 51	12.0

Operating system	Browser	Java Runtime Environment (JRE)	Adobe Flash Player
	Google Chrome 48.0 or later	JRE 8.0 Update 71	20.0
<p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ If the SVP supports Internet Protocol Version 6 (IPv6), you can specify IPv6 addresses.</li> <li>▪ Use Adobe Flash Player with the same architecture (32 bit or 64 bit) as the browser.</li> <li>▪ Only the latest version of Internet Explorer active on each OS is supported, according to Microsoft support policy.</li> <li>▪ The Device Manager - Storage Navigator computer must be restarted after enabling Adobe Flash Player.</li> </ul>			



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

## Requirements for UNIX/Linux-based computers

The storage system must meet hardware and software requirements to run UNIX or Linux as the operating system.



**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.

### Hardware requirements

Item	Requirement
Processor (CPU)	Pentium 4 640 3.2 GHz or better (Recommended: Core2Duo E6540 2.33 GHz or better)
Memory (RAM)	2 GB or more Recommended: 3 GB
Available storage space	500 MB or more
Monitor	Resolution: 1280 x 1024 or better
Keyboard and mouse	You cannot use the mouse wheel feature.

Item	Requirement
Ethernet LAN card for TCP/IP network	100BASE-TX 1000BASE-T

### Software requirements

Operating system	Architecture	Browser	Java Runtime Environment (JRE)	Adobe Flash Player
Solaris 10	32 bit	Firefox 3.6.26	JRE 7.0 Update 17	11.2
Red Hat Enterprise Linux 6.2	64 bit	Firefox 3.6.24	JRE 7.0 Update 17	11.2

**Notes:**

- Use Flash Player with the same architecture (32 bit or 64 bit) as the browser.



**Note:**

The IPv6 HTTPS connection from Firefox is not supported.

## Network settings overview

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.

For information about how to configure IP communication from an SVP, see the hardware guide for your storage system model. 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.

### Configuring IPv6 communication in Windows 7

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

**Procedure**

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

**Configuring IPv6 communication in Solaris 10**

If the SVP uses IPv6, you must configure Solaris 10 management clients to use IPv6 for communication.

**Procedure**

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

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

**Setting up a management client**

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

The Device Manager - Storage Navigator administrator is responsible for:

- 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.

**Configuring a Windows Server**

If you are using a Windows Server and Internet Explorer, set the options described below before logging in to an SVP. For more information on configuring these settings, see the Internet Explorer help documentation.



## Procedure

1. Navigate to **Tools > Internet Options > Advanced**, and then click the **Do not save encrypted pages to disk** check box to enable it.
2. Navigate to **Tools > Internet Options > Security** and register the URL of the SVP.

## Configuring the web browser

To configure the client web browser, note the following:

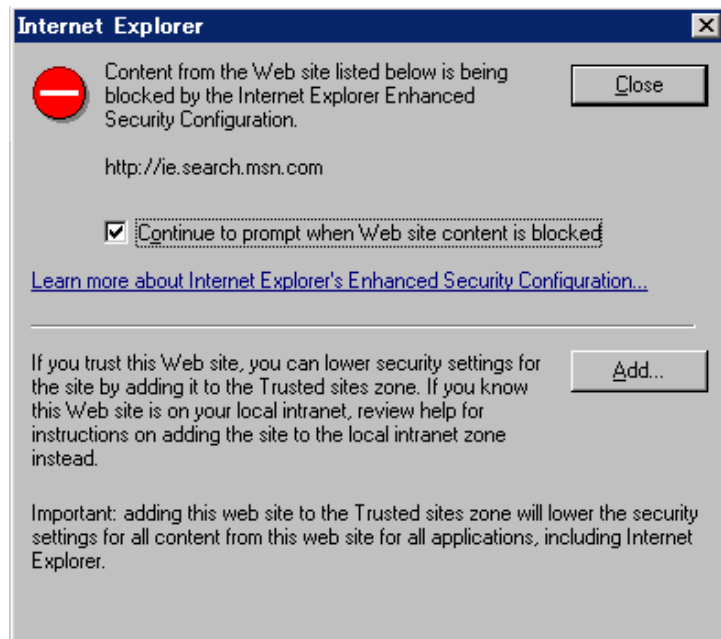
- The browser must allow first-party, third-party, and session cookies.
- Pop-up blocker and plug-ins must be disabled.
- The management client must be connected to the network via LAN.
- The version of Adobe Flash Player specified in the management client requirements must be installed.
- For Firefox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

Consult your browser's documentation for instructions.

## 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.

## Setting Device Manager - Storage Navigator environmental parameters

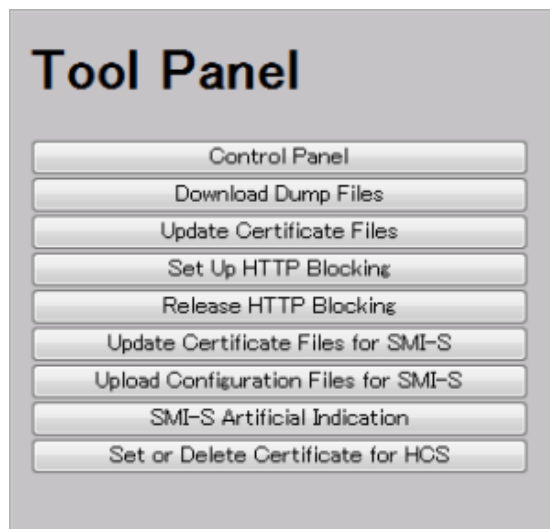
### Before you begin

- You must have the Storage Administrator (Initial Configuration) role to perform this task. See [Roles and permissions \(on page 105\)](#).
- Read the information describing the [Device Manager - Storage Navigator environmental parameters \(on page 27\)](#).


### Procedure

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

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



2. Click **Control Panel** to open the Control Panel.
3. Enter the user ID and password and click **Login**.
4. Click the **Set Env.** tab to open the **Environment Parameter** window.
5. Specify the Device Manager - Storage Navigator parameters as required.
6. Click **Submit**.

7. Click **Exit** () to close the Control Panel.
8. Log out of the Device Manager - Storage Navigator SVP and then log in again to make the new parameters take effect.
9. Back up the Device Manager - Storage Navigator configuration file by downloading the file from the SVP.

## Device Manager - Storage Navigator environmental parameters

Using the tool panel, you can set the following Device Manager - Storage Navigator environmental parameters:

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

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

Device Manager - Storage Navigator environment parameters are described in the following table.

Item	Description
RMI time-out period	<p>If the user cannot access the SVP for a certain period of time because of a network error, the RMI time-out logs the user out of the SVP.</p> <ul style="list-style-type: none"> <li>▪ The value of the RMI time-out period must be greater than the value set for the smallest polling period, either for checking exclusive lock or for checking obstacles (see below for those parameters). For example, specify a value of the RMI time-out period to satisfy the following condition:  <math display="block">\text{RMI time-out period} &gt; \min [A, B]</math>           where            A = Polling period for checking exclusive lock            B = Polling period for checking obstacles, and <math>\min [A, B]</math> indicates the minimum value selected from A and B.</li> <li>▪ The default is 1 minute. You can specify 1 minute, 5 - 60 minutes in 5-minute increments, 70 to 120 minutes in 10-minute increments, or one day (24 hours).</li> <li>▪ This parameter cannot be disabled.</li> </ul>

Item	Description
RMI time-out period for Modify	<p>If a user is in Modify mode but does not make any changes that access the RMI server for a specified period of time, Modify mode is released, and the View mode appears.</p> <ul style="list-style-type: none"> <li>▪ The default time period is 30 minutes. You can specify between 10 and 60 minutes in 10-minute increments, or between 120 and 360 minutes in 60-minute increments.</li> <li>▪ Specify NO to disable this parameter.</li> </ul>
Polling period for checking exclusive lock	<p>Using Device Manager - Storage Navigator's secondary window, specify the polling period for monitoring who is changing information while in Modify mode when other users are viewing the storage system information in View mode. The Locked and Unlocked icons are automatically updated either when a user who is in Modify mode either logs out from Device Manager - Storage Navigator or changes to View mode.</p> <ul style="list-style-type: none"> <li>▪ The shorter the time period you specify, the more frequently the Lock/Unlock status is updated, but this does increase network traffic.</li> <li>▪ The default time period is 35 seconds. You can specify 5 to 60 seconds in 5-second increments, or 70 to 120 in 10-second increments.</li> <li>▪ Specify NO to disable this parameter.</li> </ul>
Polling period for checking obstacles	<p>Specify a time interval to monitor the Disk Controller and Disk Array Unit status, which is indicated by the <b>Alerts</b> window or the Device Manager - Storage Navigator secondary window.</p> <ul style="list-style-type: none"> <li>▪ The default time period is 110 seconds. You can specify 5 to 60 seconds in 5-second increments, and 70 to 120 seconds in 10-second increments for the parameter.</li> <li>▪ Specify NO to disable this parameter.</li> <li>▪ We recommend that you select NO when Hide alert information is set in the <b>Edit Advanced System Settings</b> window.</li> </ul>

## Setting up Java

Set up Java to perform the following activities:

- Enable tracing and logging so that you can collect log files when an application error occurs on a Device Manager - Storage Navigator computer
- Change the cache settings so that to prevent the old microcode from remaining in cache when a microcode is updated, the old microcode will not remain in the cache
- Configure a proxy server

## Proxy server settings

You can set Device Manager - Storage Navigator to either use or not use a proxy server to access the SVP. To do this, change the HTTP setting on the web browser on the management client to either use a proxy server, or set the SVP as an exception so that it does not use a proxy server. Whichever setting you use, make the same setting for Java.

### Procedure

1. Start the Java Control Panel.

- In Windows, from Windows Control Panel, double-click the **Java icon**.
- In Unix, run one of the following executable files:

```
SDK-directory/jre/bin/ControlPanel
```

```
SDK-directory/jre/ControlPanel
```

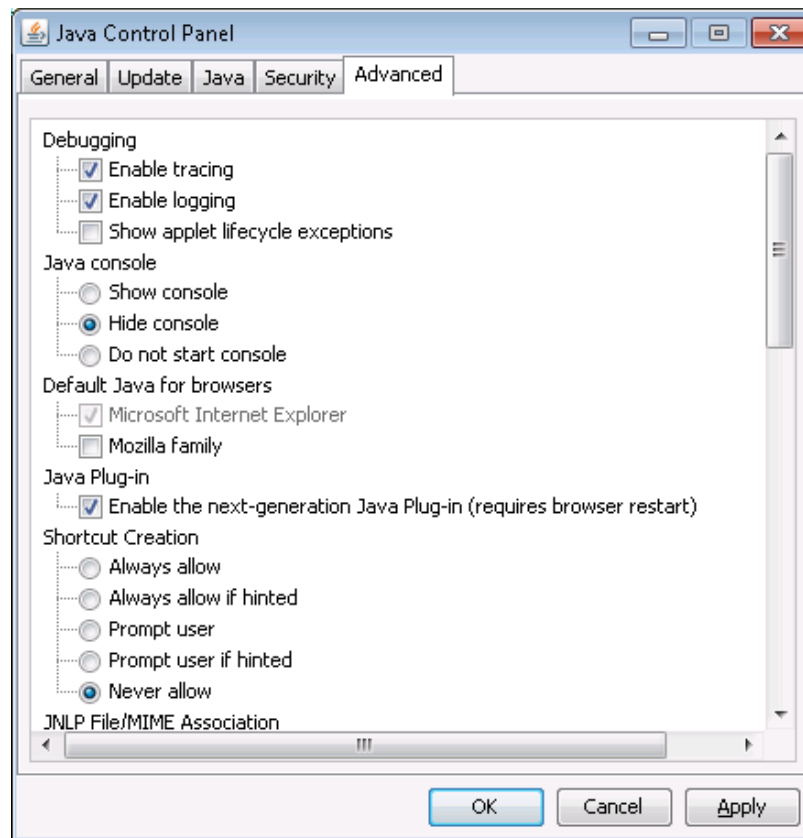
```
JDK-directory/jre/ControlPanel
```

- Alternatively, use a web browser to display one of the following Control Panel pages:

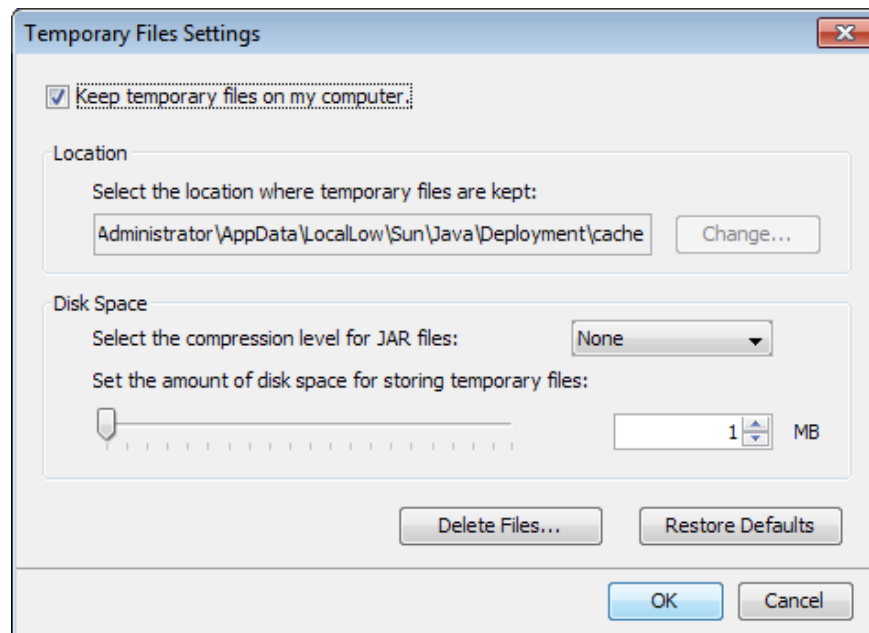
```
SDK-directory/jre/ControlPanel.html
```

```
JDK-directory/ControlPanel.html
```

2. In the Java Control Panel, click the **Advanced** tab.
3. Under Debugging, click **Enable tracing** and **Enable logging**.



4. In the Java Control Panel, click the **General** tab.
5. In the Temporary Internet Files, click **Settings**. The **Temporary Files Settings** dialog box displays.



6. In the **Temporary Files Settings** dialog box:
  - a. For JRE 7.0, click the **Keep temporary files on my computer** checkbox to enable it.

- b. In the **Disk Space** area, enter 1 MB.
  - c. Click **OK** to close the dialog box.
7. Configure the proxy settings as required.
  - a. In the **Java Control Panel**, select the **General** tab.
  - b. Click **Network Settings** to display the **Network Settings** dialog box.
8. In the Java Control Panel, click **OK** to close it.

## Changing Java security settings

If you are having trouble opening the Device Manager - Storage Navigator secondary window, make sure your Java security settings are set correctly.

If you use a management client in which Java 7 Update 55 or later is installed, or the one in which Java 8 Update 5 or later is installed, the execution of an application might be blocked when you try to open the Device Manager - Storage Navigator secondary window. In this case, you need to change Java security settings according to the procedure below.

### Procedure

1. Check the version and update information of Java installed in your management client. Click **Start > Control Panel > Java**.
2. On the **General** tab, click **About**.
3. Check the version and update information of Java, and then close the **About Java** dialog box. If your PC uses either Java 7 update 55 or later, or Java 8 Update 5 or later, you need to change Java security settings referring to Step 4 and after.
4. Select the **Security** tab.
5. Click **Edit Site List**.
6. In the **Exception Site List** dialog box, specify either of the following URLs, and then click **Add**.
  - *http://IP-address-of-SVP*
  - *https://IP-address-of-SVP*
7. Click **OK**.
8. Select the **Advanced** tab.
9. Select **Do not check (not recommended)** of **Perform signed code certificate revocation checks on**, and then click **OK**.
10. Close the **Control Panel** dialog box.

## 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
- Cache Residency Manager
- Compatible PAV
- Compatible XRC
- Data Retention Utility
- Server Priority Manager
- Volume Retention Manager

To use the Device Manager - Storage Navigator secondary window, you must enable it in advance. 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 restrictions

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.

`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.

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

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

### **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**.

## Lowering the IE security level on Windows Server 2012 or later

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

### Before you begin

You must add the URL of the SVP to the "trusted sites zone".

### Procedure

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

## Device Manager - Storage Navigator restrictions

Certain actions might cause errors within Device Manager - Storage Navigator or within the browser when using Device Manager - Storage Navigator.

To avoid errors when using Device Manager - Storage Navigator, observe the following restrictions.

### General restrictions

To avoid errors while using Device Manager - Storage Navigator:


- Do not change the local storage area value in Adobe Flash Player.
- Do not change the management client clock setting while you are logged in to the SVP.
- Do not change screen display settings such as resolution or refresh rate.
- Do not use Microsoft Remote Desktop.
- Do not use screen savers that change the screen resolution.
- Do not set the management client to standby or hibernate. Do not allow the management client battery to discharge far enough so that the management client automatically enters standby or hibernate. If you do, you must restart Device Manager - Storage Navigator.
- If applicable, disable the auto-login function of any web-based software or web site being used on the management client.



**Note:** The functions keys, as well as the **Home**, **End**, and **Delete** keys are disabled for Device Manager - Storage Navigator operations.

## Web browser restrictions while using Device Manager - Storage Navigator

When logged in to Device Manager - Storage Navigator, do not use web browser menus, shortcuts, or other browser options as described here.

- If you use Back, Next, or web browser shortcut keys such as **F5** and **Esc**, you will be logged out of Device Manager - Storage Navigator. Any settings you made during the session will be lost.
- Do not use the  button, the Close option in the File menu, or the **Alt+F4** shortcut to close the web browser. To close Device Manager - Storage Navigator, click Logout or File > Close in the Device Manager - Storage Navigator menu.
- Do not change the web browser settings such as Tools > Folder options in Internet Explorer. If you do so and see unexpected results, close the web browser and log in to Device Manager - Storage Navigator again.
- Do not disable Adobe Flash Player because Adobe Flash Player is necessary for Device Manager - Storage Navigator and works as an add-on to a web browser. If you use Internet Explorer, do not change the settings in Tools > Manage Add-ons.
- Do not use the following web browser functions: character encoding, text size, the zoom function, the **Ctrl+F** (search), **Ctrl+A** (select all).
- Use only the **Tab** key to move the focus to the Adobe Flash Player window. If you use **Shift+Tab** to move the focus in reverse, the focus may not move from the web browser to the Adobe Flash Player.
- If you click a link that is blank or one for which a hyphen is displayed, nothing happens.
- In Internet Explorer, the window closes automatically when you click Logout at the upper right corner of the Device Manager - Storage Navigator main window.

In Google Chrome, the window does not close when you logout.

When you display an HTML format report saved in your local file system in a Web browser to which Adobe Flash Player version 23 or later is applied, add the folder containing the HTML format report to Trusted Location Settings.

If a path to the folder where the report is stored is a Windows UNC path, perform either of the following beforehand:

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

### Procedure:

In Internet Explorer and Firefox:

1. Open Adobe Flash Player Settings Manager.
2. On the Advanced tab, click Trusted Location Settings under Developer Tools. The Trusted Location Settings dialog box opens.

3. Click Add. The Add Site dialog box opens.
4. Click Add Folder. Select the folder that contains the HTML format report, and then click OK.
5. In the Add Site dialog box, click Confirm.
6. In the Trusted Location Settings dialog box, click Close.
7. Close Adobe Flash Player Settings Manager.

In Google Chrome:

1. Open Adobe Flash Player Settings Manager.
2. On the Global Security Settings panel, select Add locations from the drop-down list box.
3. Enter a path to the folder containing the HTML format report in the Trust this location text box. Do not use Browse for files or Browse for folder because they do not work correctly.
4. Click Confirm.
5. Close Adobe Flash Player Settings Manager.

## Unsupported actions in Windows version of HDvM - SN

The following actions are not supported in any version of Device Manager - Storage Navigator:

- The right mouse button does not open a popup menu in the Device Manager - Storage Navigator main window. If you right click, the Adobe Flash Player pop-up menu opens instead.
- The copy (**Ctrl+C**) and paste (**Ctrl+V**) shortcuts do not copy and paste text to a text box in Device Manager - Storage Navigator.
- No drag-and-drop operation is available in Device Manager - Storage Navigator.
- The mouse wheel may not function in the Device Manager - Storage Navigator secondary window.
- The web browser zoom function does not work correctly in the Device Manager - Storage Navigator window. When you hold down on the **Ctrl** key and use the mouse wheel, part of the Device Manager - Storage Navigator window might not be displayed.



## Unsupported actions in UNIX version of HDvM - SN

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

- You cannot change the Device Manager - Storage Navigator window size.
- You cannot drag-and-drop objects in the Volume Migration or LUN Manager windows.

- If you click the Device Manager - Storage Navigator secondary window when you are using Volume Migration, the Volume Migration window may be fully or partially hidden behind the Device Manager - Storage Navigator window. However you cannot use the front Device Manager - Storage Navigator window.

Close the Volume Migration window before using the Device Manager - Storage Navigator secondary window. If the Volume Migration window is hidden behind the Device Manager - Storage Navigator window, click the Volume Migration window to bring it to the foreground, and then close it.

- The Close  button on the Volume Migration window remains active even if you click Apply while the Volume Migration process is running. If you click Close  after clicking Apply, the Volume Migration window closes but the Volume Migration process continues.
- The word "Loading..." only appears in the Volume Migration window message dialog box for the first operation. This message does not re-appear after the first operation.

## Applying changes made in Device Manager - Storage Navigator

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

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

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

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

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

## Updating data after a Volume Migration or Quick Restore operation

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

## Updating data after operations performed with another application

Be aware that it may take time to update the information in Device Manager - Storage Navigator after you have performed an operation on the storage system using another application, such as CCI.

### Capacities displayed on the Device Manager - Storage Navigator screen

Unless otherwise specified in this manual, capacity values are rounded down to the second decimal place for TB, GB, or MB or to the nearest integer for Cyl when displayed on the Device Manager - Storage Navigator screen. Therefore, displayed values may be lower than the actual values.

The value converted from 1Cyl to KB depends on the volume's emulation type. The following table lists cylinder capacities by emulation type.

Emulation Type		1 Cylinder Capacity (KB)
Open Systems	OPEN-V	960
	Other	720
Mainframe	-	870

### Caution on LUN ID notation

The format of LUN IDs in the Device Manager - Storage Navigator main and secondary windows depends on the storage system. The following table describes those differences.

Storage system	Format in the main window	Format in secondary windows
VSP G1000, VSP G1500, and VSP F1500	Decimal or hexadecimal Default: Decimal	Decimal only
USP V/VM	Hexadecimal only	Decimal only
Virtual Storage Platform	Hexadecimal only	Decimal only

If LUN IDs are displayed in hexadecimal format, you can enter LUN IDs for USP V/VM or VSP as is.

However, if LUN IDs are displayed in decimal format, you must convert them to decimal format before entering them in the Device Manager - Storage Navigator main window.

To switch the LUN ID notation of the Device Manager - Storage Navigator main window between decimal and hexadecimal, use the **Edit Information Display Settings** window. For details, see [Edit Information Display Settings window \(on page 385\)](#).

---

## Chapter 2: Using Device Manager - Storage Navigator

Follow instructions to log on to Device Manager - Storage Navigator properly. You then can use Device Manager - Storage Navigator, windows, and wizards to get started.

For information about viewing storage system information, see [Viewing and managing the storage system \(on page 144\)](#).

### 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 superuser, 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 I, which describe the screens in the GUI.

## User login

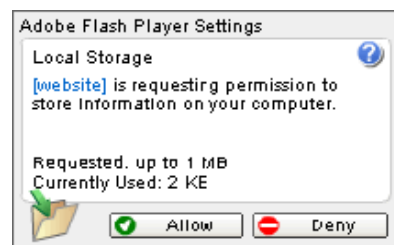
By logging in, you can manage users and licenses, create a login message, or edit advanced system settings.

### Procedure

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

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

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 \(on page 25\)](#).
3. Type the user ID and password.
4. Click **Login**.
5. If the **Security Information** dialog box appears, click **Yes**.
6. If a local storage area pop-up dialog box of Adobe Flash Player Setting appears, click **Allow** to open the 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 I, 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 the initial password

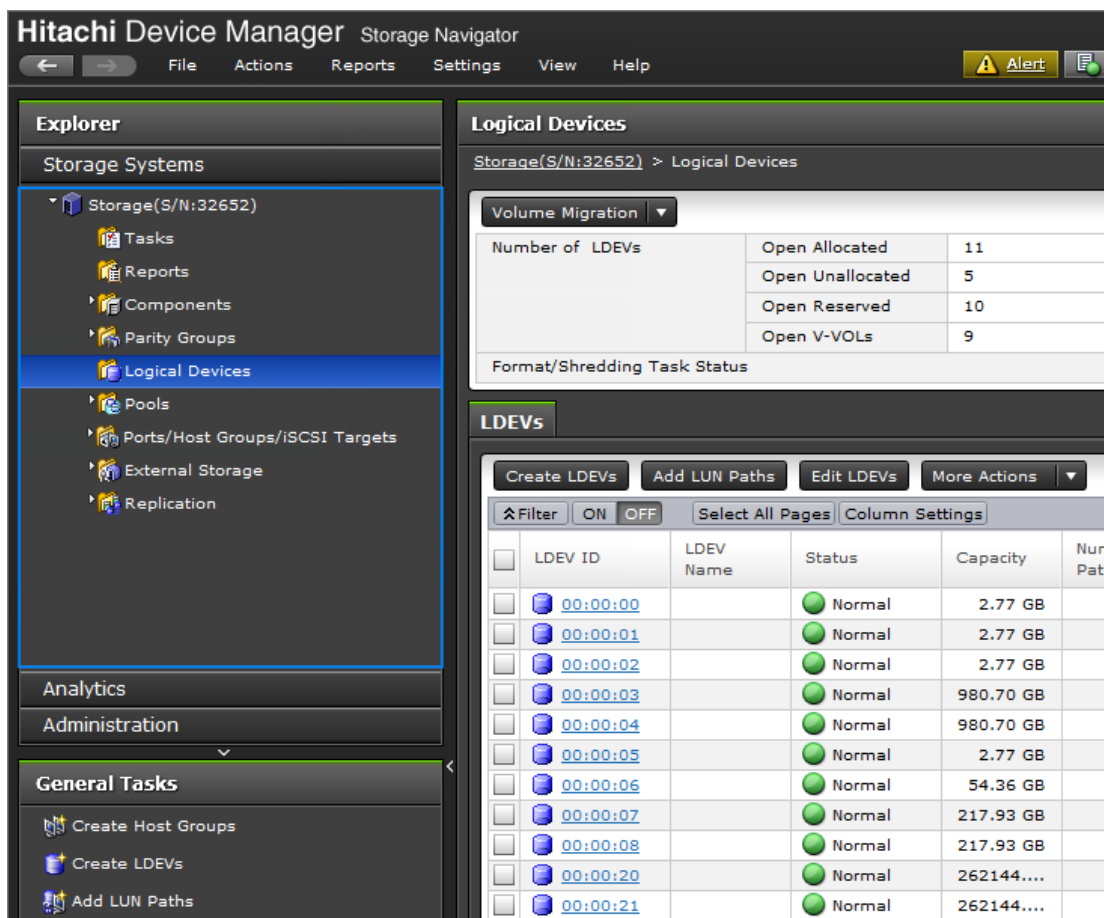
After the administrator gives you a user ID and password, you should change the password after you log in.

### 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.

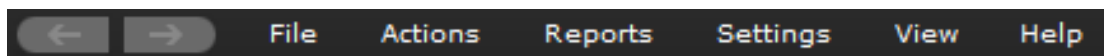
## Navigating the Device Manager - Storage Navigator user interface



The following figure shows an example of the GUI main window. In this example, Logical Devices has been selected.



## Menu bar

The following illustration shows the menu bar in the Device Manager - Storage Navigator main window. The table below the illustration describes the menu items and their functions.



Item	Description
	Click to return to the previous window.
	Click to advance to the next window.

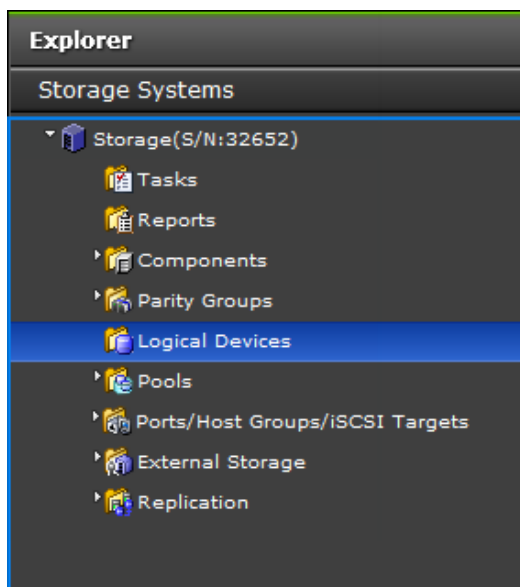
Item	Description
File	<ul style="list-style-type: none"> <li>▪ Refresh All: Acquires all the information about the storage system and updates both the SVP and Device Manager - Storage Navigator. You must have the Storage Administrator (initial configuration) permissions to use this function. See <a href="#">Roles and permissions (on page 105)</a>.</li> <li>▪ Logout: Logs the current user out of Device Manager - Storage Navigator.</li> </ul>
Actions	Provides actions to the storage system such as creating LDEVs or performing replication copy.
Reports	<ul style="list-style-type: none"> <li>▪ Task Management: Manages the tasks that will be applied to the storage system.</li> <li>▪ Configuration Report: Creates and downloads storage system configuration reports.</li> <li>▪ Performance Monitor: Monitors performance of the storage system.</li> <li>▪ Shredding Report: Downloads the shredding report.</li> </ul>
Settings	<ul style="list-style-type: none"> <li>▪ User Management: Manages Device Manager - Storage Navigator user accounts, including changing passwords.</li> <li>▪ Resource management: Performs resource group related operations</li> <li>▪ Security: Performs audit log or encryption operations</li> <li>▪ Environmental Settings: Configures the license, the refresh interval of the window or an external server. Resets view settings that can be customized, such as width or order of table column. See the table in <a href="#">Column Settings window (on page 362)</a> for items that are reset using Reset View Settings.</li> </ul>
View	Changes the font size in the window.
Help	Displays the online help

## Using the Device Manager - Storage Navigator main window

You can perform operations by using the main window and wizards.

### Procedure

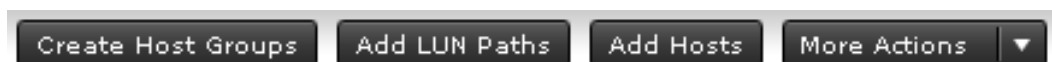
1. Click a function in the resource tree in the Explorer.



2. If necessary, choose a tab and use a filter to reduce the number of items in the table.



3. Select an item in the table and click a button to open a wizard.



4. Set options in the wizard and click **Finish** to confirm the setting.
5. Enter a task name and click **Apply** to apply the setting to the storage system. The setting is queued as a task and performed in order.



**Tip:** To open the task window after closing the wizard, select **Go to tasks window for status** and click **Apply** in the wizard.

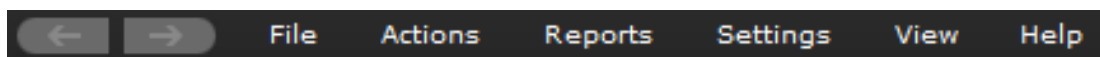


6. Open the task window to verify the result of the operation. A task can be suspended or canceled if the processing of the task is not started.

## Main window controls

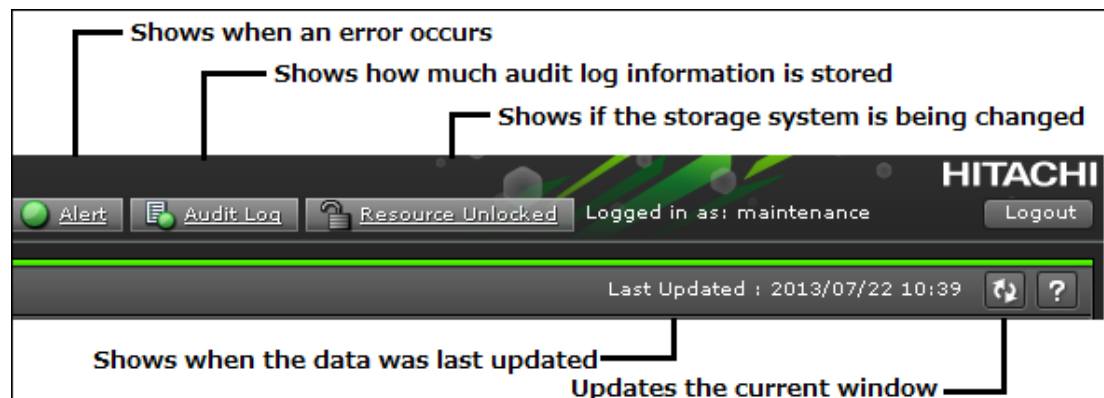
The following figure shows the buttons that appear in the upper left part of the main window.

### Buttons



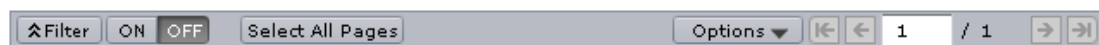
The Back button displays the previous window; the Next button displays the next window. Device Manager - Storage Navigator tracks up to 10 operations and the windows that display depend on the selection from the navigation tree.

The following figure shows the buttons that appear in the upper right part of the main window.



## Table Controls

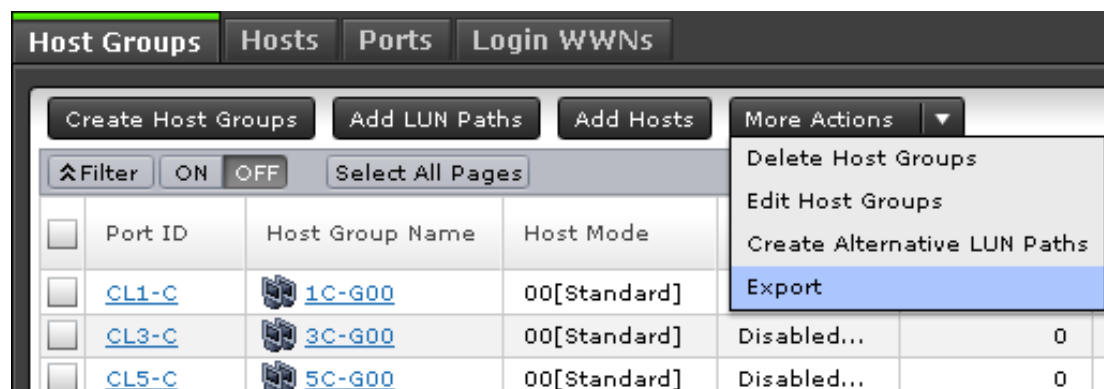
The following figures shows the controls used to view and filter the results in a main window table:



To scroll through pages of the table, use the left and right arrows or type a page number into the number field. To select all rows in the table, click Select All Pages. To display a table column, click Column Settings. If filter is ON, the filtered rows are selected. To sort the table, click the header of the column that you want to use to sort.

When you sort a capacity column, the column will be sorted by bytes regardless of the capacity unit used in the items in the column. Therefore columns in units of cylinders (cyl) may not necessarily be sorted in ascending or descending order of the number of cylinders. Even if the number of cylinders is the same, the capacity may not be the same according to the emulation type.

To save the displayed information to a TSV file, click Export under More Actions. This action is demonstrated in the following figure.



When you change the default file name, confirm that the file name contains the .tsv extension to save the file.

## Filtering

To filter the table, select or input the desired filtering conditions and click Apply.



### Note:

- Users can set up to 16 conditions.
- When the input condition is wrong, click Apply to clear the condition.
- Select the attribute whose date and time values must be entered, and then enter the values.
- The values of date and time are "YYYY/MM/DD" and "hh:mm:ss", respectively.
- After you enter the date in the first box, "00:00:00" is displayed in the second box as a default time value. Edit this value as needed and click Apply.

Attribute: Value:

1 LDEV Name is Open -

2 Status is Normal -

3 Select Item Select Item - +

Match All conditions above. Reset Clear Apply

Filter ON OFF Select All Pages

## Tooltip

When text displays in the main window, ellipses (...) may be displayed to show that the text is truncated. If you place the mouse cursor over an ellipsis (...), the full text displays in a tooltip (a small "hover box").

Port ID	Internal WWN	Speed	Security	Type	Address (Loop ID)	Fabric
CL1-C	50060E80073...	Auto(1Gbps)	Disabled	Fibre	B2 (32)	OFF
CL3-C	50060E8007303902	Auto(1Gbps)	Disabled	Fibre	B1 (33)	OFF
CL5-C	50060E80073...	Auto(1Gbps)	Disabled	Fibre	AE (34)	OFF
CL7-C	50060E80073...	Auto(1Gbps)	Disabled	Fibre	AD (35)	OFF
CL1-D	50060E80073...	Auto(1Gbps)	Disabled	Fibre	AC (36)	OFF
CL3-D	50060E80073...	Auto(1Gbps)	Disabled	Fibre	AB (37)	OFF

## Main window and Modify mode

There is no Modify mode for the Device Manager - Storage Navigator main window. Main window and wizard operations are queued as tasks and performed in order. However, when using a Device Manager - Storage Navigator secondary window, you must be in Modify mode before changing any settings. Secondary window operations are not queued or displayed in the task window.

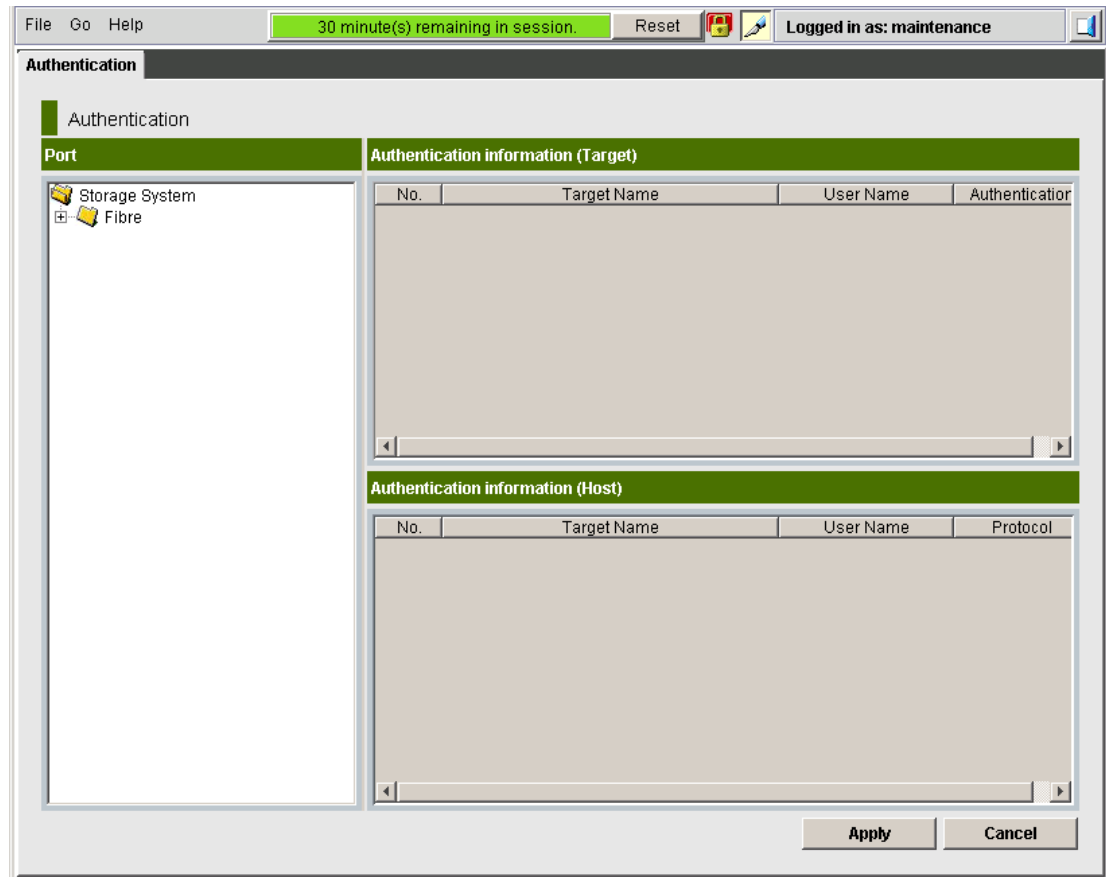
## Using Device Manager - Storage Navigator secondary windows

Some Hitachi Device Manager - Storage Navigator operations are performed through secondary window within the Java Runtime Environment (JRE).

This section describes requirements, operation methods, notes, and troubleshooting required to use Hitachi Device Manager - Storage Navigator secondary windows.

## Secondary windows and wizards

When you select an operation to perform, a secondary window or wizard is displayed.



**Figure 1 Example of a secondary window**

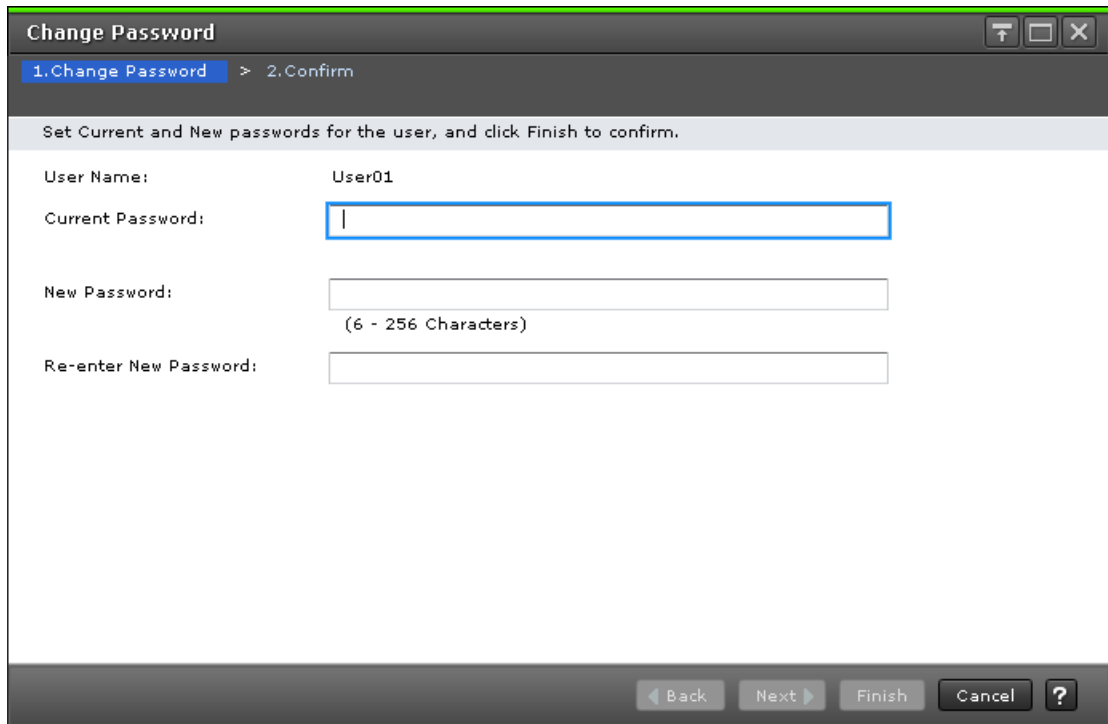
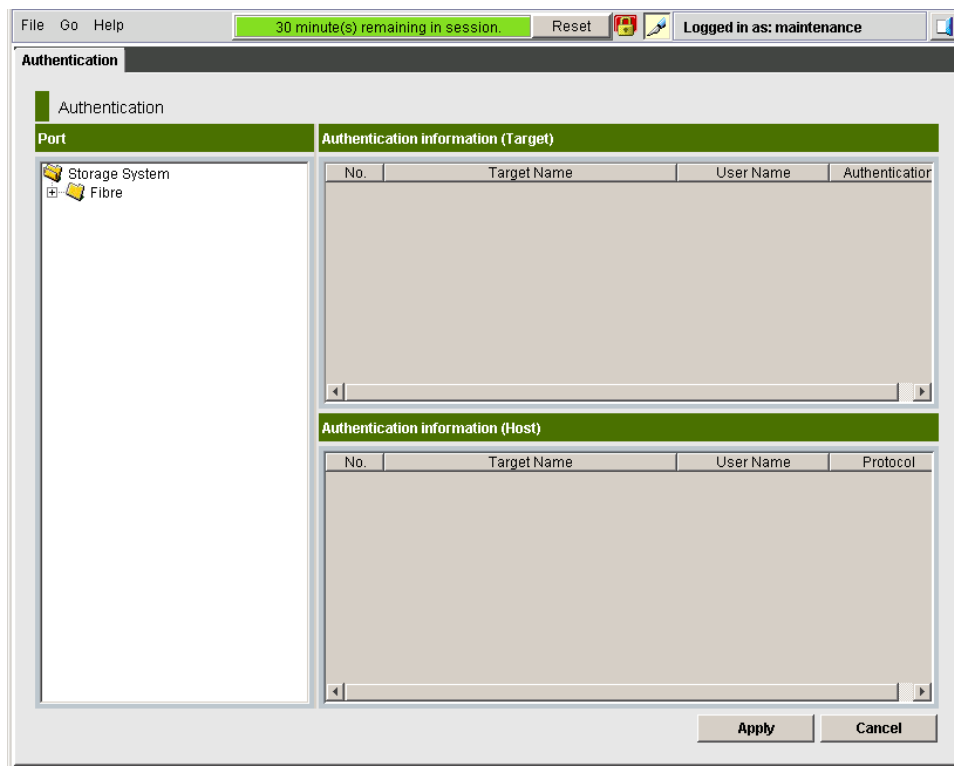


Figure 2 Example of a wizard





## Secondary window menus and buttons




The following figure shows the Device Manager - Storage Navigator secondary window.



The following table describes the menus and buttons accessible in the window.



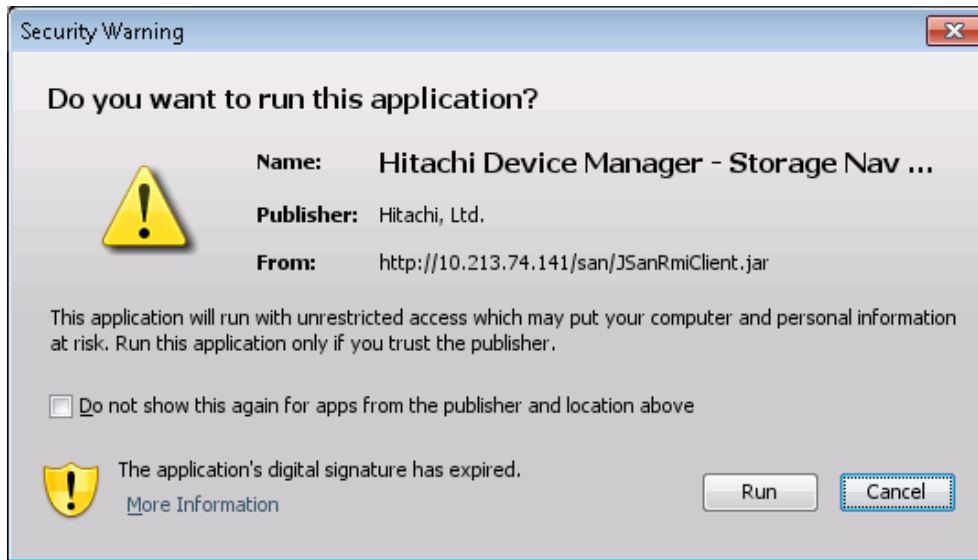
Item	Description
Title bar	<p>Provides information about the connected storage system.</p> <ul style="list-style-type: none"> <li>▪ IP indicates the IP address of the SVP.</li> <li>▪ S/N indicates the serial number.</li> <li>▪ D/N indicates the device name specified in the Edit storage system window.</li> </ul>
File > Refresh All	<p>Updates the information on the SVP. All information displayed on the Device Manager - Storage Navigator secondary window is reacquired from the storage system. We recommend that you use this command only when error recovery is required.</p> <ul style="list-style-type: none"> <li>▪ Takes time until the processing has been completed.</li> <li>▪ While updating, other users are not allowed to perform any operation on the Device Manager - Storage Navigator windows. Maintenance of the storage system or the SVP operation by the service personnel is not allowed, either.</li> <li>▪ Available only for the user with Storage Administrator (Initial Configuration) role.</li> <li>▪ Available only when the user is in Modify mode.</li> <li>▪ The information may not display correctly if SVP maintenance is in progress.</li> <li>▪ Try this command if the configuration information displayed on the Device Manager - Storage Navigator differs from the actual configuration information that can be recognized from the host.</li> </ul>
File > Refresh	<p>Displays the latest information on Device Manager - Storage Navigator.</p> <p>The information might not display correctly when the exclusive lock is effective or SVP maintenance is in progress.</p>
File > Close	Closes the Device Manager - Storage Navigator secondary window
Go menu	Indicates software names
Help menu	About: Opens the <b>About</b> dialog box to show the version of the storage system.
 Unlocked  Locked	<p>Indicates the current operational mode of Device Manager - Storage Navigator.</p> <p>If all logged in users are currently working in the view mode, the blue unlocked-shaped icon () appears. If any user is working in the Modify mode, the red locked-shaped icon () appears.</p>

Item	Description
	Note: The operational status might not be displayed correctly when the exclusive lock is effective or SVP maintenance is in progress.
 View  Modify	<p>Allows users to switch the operation mode between Modify and View. The button always shows the current user operation mode. To change the modes, click the button.</p> <p>You cannot switch to the Modify mode while any other user is operating in the Modify mode. Make sure to confirm the exclusive lock icon before switching to the Modify mode.</p>
Reset	Reset the remaining time for the Modify mode. Appears only when you are in Modify mode.
Logged in as	Shows the user ID of the currently logged-in user.
 Logout	Closes the Device Manager - Storage Navigator secondary window.
Apply	<p>Implements all the changes or settings displayed in blue bold italics. This button is available only in Modify mode.</p> <p>You can create and store up to 20,000 settings or operations before actually applying them to the storage system. To avoid a possible error, do not apply more than 20,000 settings at a time.</p>
Cancel	Cancels the changes or settings made on the window. This button is available only in Modify mode.

## Opening Device Manager - Storage Navigator secondary windows

Some Device Manager - Storage Navigator operations are performed through secondary windows that use a Java application. For this reason, whether you are using JRE 5.0 or 6.0, a message might appear and ask if you want to run a Java Application. You might see slightly different dialog boxes depending on your environment and configuration. For JRE 5.0, the **Warning - Security** dialog box (shown below) displays when the digital signature has expired.

To use Device Manager - Storage Navigator, if you select Always trust content from this publisher in the **Warning - Security** dialog box before clicking Run, Device Manager - Storage Navigator is always allowed to access the local files. When you click Run, you will not see this dialog box again.



**Note:** The Device Manager - Storage Navigator digital signature has an expiration date and it might be expired depending on the Device Manager - Storage Navigator version that you use. Even though the digital signature is expired, you can continue using Device Manager - Storage Navigator.


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

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

To start up the window, you need to change Java security settings. For details, see [Changing Java security settings \(on page 31\)](#).

## HDvM - SN secondary windows and Modify mode

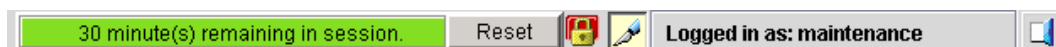
A secondary window opens when you click a command from the Device Manager - Storage Navigator menu. To make settings in a secondary window, you must change to

Modify mode by clicking . Modify mode prohibits other users or programs from changing the storage system setting. As soon as you close the secondary window, Modify mode is released.

Modify mode has a timeout period. If you do not access SVP before the end of the timeout period, Modify mode is released. On some windows, the settings made but not yet applied to the storage system will be canceled.

## Resetting timeout period for Modify mode

The secondary window displays the progress bar (shown in the following figure) indicating the remaining time in the timeout period. To extend this period and remain in Modify mode, click Reset.



The Modify mode default timeout period is 30 minutes, but can be changed by modifying RMI time-out period for Modify.

If Modify mode is released due to a timeout, the current window will still be visible, but an error message is returned when you click Apply, or when you try to update the

window through File > Refresh All  or Refresh .

## Resetting the secondary window

The Device Manager - Storage Navigator secondary window is reset when you do any of the following:

- Click Apply or Cancel
- Click Refresh or Refresh All on the File menu
- Switch tabs

## Cautions when using secondary windows

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 actually IPv4 communication is used.

- The mouse wheel may not function in the Device Manager - Storage Navigator secondary window.
- If you accept other processing while you are changing the configuration of the storage system on the secondary window, an error occurs.
- If an error occurs when you try to log in or when you click Apply, wait awhile and log in again.
- If an error occurs when you switches operation modes (View/Modify) or tabs, wait awhile and click File > Refresh.

## Java updates

Some Device Manager - Storage Navigator operations are performed using Java applications. You may be prompted to update the Java application when navigating to these operations, as shown in the following figure.



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

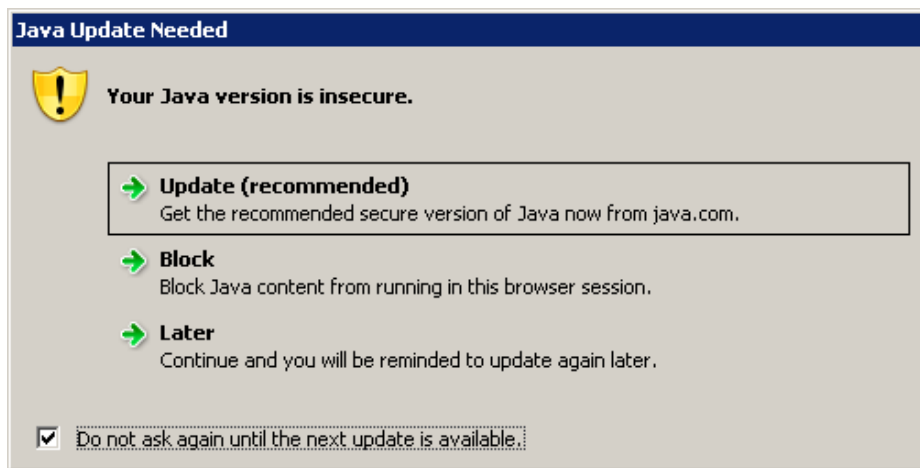
- Java 7 Update 55 or later
- Java 8 Update 5 or later

To start up the window, you need to change Java security settings. For details, see [Changing Java security settings \(on page 31\)](#).



**Note:**

The **Java Update Needed** dialog box appears when a newer version of Java is available. Depending on your environment, the appearance of this dialog box might differ.



Note the following:

- To download and install the recommended Java version, click Update (recommended). If the secondary window does not display after the update is complete, see [Enabling the Device Manager - Storage Navigator secondary window \(on page 33\)](#).
- To prevent Java content from displaying in the current browser session, click Block. If the secondary window does not display after the update is complete, see [Enabling the Device Manager - Storage Navigator secondary window \(on page 33\)](#).
- To use the currently installed Java version, click Later. The Device Manager - Storage Navigator secondary window for the application you are using opens.  
After you click Later, if the error 20020-108000 appears, open the Device Manager - Storage Navigator main window, and then open the secondary window again.
- To prevent this dialog box from appearing again, check Do not ask again until the next update is available.

## Troubleshooting secondary windows

This topic describes cautions peculiar to the Device Manager - Storage Navigator secondary window. For troubleshooting issues common to the main and secondary windows, see Chapter 8 Troubleshooting.

### Java application errors

Error condition	Probable cause / recommended action
<p>When you click the Device Manager - Storage Navigator menu, the system does not respond. One minute later, application error (20020-108000) occurs.</p>	<p>The pop-up blocker function of your web browser might restrict Device Manager - Storage Navigator. If the problem still continues after you perform the operation multiple times, perform one or both of the following actions:</p> <ul style="list-style-type: none"> <li>▪ Disable the pop-up blocker function of your web browser.</li> <li>▪ Disable the pop-up blocker function of any browser plug-in/add-on.</li> </ul> <p>If neither of the above can be performed in Internet Explorer, you can open the window by clicking the Device Manager - Storage Navigator menu while holding down the <b>Ctrl</b> key.</p> <p>Another possible cause is that a Java application was not allowed to start. If a message appears and asks if you want to run an application, click Run.</p> <p>If none of the above actions solve the problem, reinstall the JRE.</p>
<p>When you click the Device Manager - Storage Navigator menu, a message appears asking you to download the file SjsvISNStartServlet.do or SjsvIAppStartServlet.do. One minute later, the application error (20020-108000) occurs.</p>	<p>The possible causes are that the JRE is not installed in the management client, the JRE installation failed, or the JRE add-on is disabled on the web browser. Cancel the message, and install the JRE. If the JRE is already installed, reinstall it.</p>
<p>When you click the Device Manager - Storage Navigator menu, a message appears asking you to save a Jnlp file.</p>	<p>Perform the following to save the encrypted page:</p> <ol style="list-style-type: none"> <li>1. In Internet Explorer, click Tools &gt; Internet options, and then select the Advanced tab.</li> <li>2. In the Security section, uncheck Do not save encrypted pages to disk.</li> </ol>

Error condition	Probable cause / recommended action
<ul style="list-style-type: none"> <li>▪ The application errors (20020-108000 and 10-6027) occur when you click the Device Manager - Storage Navigator menu.</li> <li>▪ The application error (10-6027) occurs and Device Manager - Storage Navigator terminates when you click the Device Manager - Storage Navigator menu.</li> </ul>	<p><b>3.</b> Click OK.</p> <p>If the problem continues after you perform the operation multiple times, see the probable causes listed below.</p> <p>For Windows: Exit all applications using Java, and then terminate the javaw.exe and javaws.exe applications through Task Manager.</p> <ul style="list-style-type: none"> <li>▪ Java on the Device Manager - Storage Navigator web client might have failed to start due to timeout. Close all other applications and perform the Device Manager - Storage Navigator operation again.</li> <li>▪ The version of Device Manager - Storage Navigator installed on the management client might not match the SVP version. Close all the windows of your web browser and then clear the Java and web browser cache.</li> <li>▪ The management client might have entered standby or hibernate mode. Restart the management client.</li> <li>▪ If a proxy server is used for network connections, the proxy cache may be storing the older version of the program. If the problem continues after you clear the Java and web browser caches, contact your network administrator.</li> <li>▪ The network connection between the SVP and the management client might be blocked by a firewall or some kind of device.</li> </ul> <p>Check the firewall settings and contact your network administrator.</p> <p>If none of the above actions solve the problem, save the dump file, the Java trace file and the log file on the management client, and report to customer support. Then restart Device Manager - Storage Navigator.</p>

Error condition	Probable cause / recommended action
<p>When you click the Device Manager - Storage Navigator menu, the system does not respond.</p>	<p>If the problem continues after you perform the operation multiple times, close all the Device Manager - Storage Navigator windows and clear the Java and web browser caches.</p>
<p>The application error (1-7050) occurs when you click the Device Manager - Storage Navigator menu.</p>	<p>The version of Device Manager - Storage Navigator installed on the management client might not match the SVP version. Close all the windows of your web browser and then clear the Java and web browser caches. In addition, if a proxy server is used for network connections, the proxy server cache may be storing the older version of the program. If the problem continues after you clear cache of both Java and web browser, contact your network administrator.</p>
<p>Java console is grayed out and does not start when you try to open the Device Manager - Storage Navigator secondary window (Java application).</p>	<p>Restart the management client, or terminate the Device Manager - Storage Navigator process with one of the following methods:</p> <ul style="list-style-type: none"> <li>▪ For Windows: Exit all applications using Java, and then terminate the javaw.exe and javaws.exe applications through Task Manager.</li> <li>▪ For UNIX: Exit all applications using Java, and then terminate javaw and javaws with the kill command.</li> </ul>
<p>A message box remains displayed when opening the Device Manager - Storage Navigator secondary window (Java application). The Device Manager - Storage Navigator secondary window does not appear for a long time.</p>	<p>Restart the management client, or terminate the Device Manager - Storage Navigator process with one of the following methods:</p> <ul style="list-style-type: none"> <li>▪ For Windows: Exit all applications using Java, and then terminate the javaw.exe and javaws.exe applications through the Task Manager.</li> <li>▪ For UNIX: Exit all applications using Java, and then terminate javaw and javaws with the kill command.</li> </ul>



Error condition	Probable cause / recommended action
<p>A message remains displayed when the Device Manager - Storage Navigator secondary window opens and the system does not respond.</p>	<p>The SVP may be set as an exception on the proxy setting of the web browser.</p> <p>Make the settings the same on the <b>Network Configuration</b> dialog box, which is located in the Java Control Panel's <b>General</b> dialog box.</p>
<p>If you open the Java console dialog box by selecting the Java icon on the system tray while opening the Device Manager - Storage Navigator secondary window (Java application), the browser and Java console may stop responding.</p>	<p>Do not open the Java console dialog box while opening the Device Manager - Storage Navigator secondary window. If the browser and Java console stop responding, restart the management client.</p>
<p>When you click the Device Manager - Storage Navigator menu. The application error (20020-108000) occurs.</p>	<p>If the problem continues after you repeat the operation several times, you might have cancelled the display of the secondary window. Restart the management client, or terminate the Device Manager - Storage Navigator process with one of the following methods: For example:</p> <ul style="list-style-type: none"> <li>▪ You might have clicked Exit on the <b>Security Warning</b> window.</li> <li>▪ You might have clicked Cancel on the <b>Warning - Security</b> window.</li> </ul> <p>Close all the Device Manager - Storage Navigator windows and clear the Java and web browser caches.</p> <p>If the problem continues after you clear both Java and web browser caches, save the Device Manager - Storage Navigator dump file and the Java trace file, and send them to customer support.</p>

Error condition	Probable cause / recommended action
<p>The following message displays in Device Manager - Storage Navigator.</p> <ul style="list-style-type: none"> <li>▪ Java has discovered application components that could indicate a security concern.</li> <li>▪ Block potentially unsafe components from being run. (recommended)</li> <li>▪ The application contains both signed and unsigned code. Contact the application vendor to ensure that it has not been tampered with.</li> </ul>	<p>Select Yes to continue using Device Manager - Storage Navigator. If the problem continues, the cause may be one of the following:</p> <ul style="list-style-type: none"> <li>▪ The version of Device Manager - Storage Navigator installed on the management client might not match the SVP version. Close all the windows of your web browser and then clear the cache of both Java and the web browser</li> <li>▪ If a proxy server is used for network connections, the proxy server cache may be storing an older version of the program. Clear the cache of both Java and the web browser. If the problem remains, contact your network administrator.</li> </ul>
<p>In Internet Explorer, the following pop-up window appears when you open the Device Manager - Storage Navigator secondary window.</p> <p>"Internet Explorer has stopped working. A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available."</p>	<p>Third-party browser extensions of Internet Explorer might be enabled.</p> <p>Disable third-party browser extensions as follows:</p> <ol style="list-style-type: none"> <li>1. In the Windows menu bar, click Tools &gt; Internet Options, and then click the Advanced tab.</li> <li>2. In the Advanced tab, clear the Enable third-party browser extensions (requires restart) check box.</li> <li>3. Restart Internet Explorer.</li> </ol>
<p>In Internet Explorer, an application error (10-6027) occurs when you open the Device Manager - Storage Navigator secondary window.</p>	<p>The SmartScreen Filter function might be enabled when you use Internet Explorer 8.0 or later. Turn off SmartScreen Filter as follows:</p> <ol style="list-style-type: none"> <li>1. In the Windows menu bar, click Safety &gt; SmartScreen Filter &gt; Turn Off SmartScreen Filter.</li> <li>2. Restart Internet Explorer.</li> </ol>
<p>In Internet Explorer or Google Chrome, either of the following pop-up windows appears when you open the Device Manager - Storage Navigator secondary window.</p>	

Error condition	Probable cause / recommended action
<p>"Application Blocked by Java Security" or "Application Blocked by Security Settings"</p>	<p>Note: The following Java versions do not allow the Device Manager - Storage Navigator secondary window to display.</p> <ul style="list-style-type: none"> <li>▪ Java 7 Update 55 or later</li> <li>▪ Java 8 Update 5 or later</li> </ul> <p>To start up the window, you need to change Java security settings. For details, see <a href="#">Changing Java security settings (on page 31)</a>.</p> <p>Also, note that the certificate signed to the SVP program might be expired.</p> <p>You can perform the application by adding the SVP URL to the exception site list by using the following procedure:</p> <ol style="list-style-type: none"> <li>1. Open the Java Control Panel.</li> <li>2. Click Edit Site List on the Security tab. Exception Site List displays.</li> <li>3. Click Add.</li> <li>4. Enter URL. Begin with <code>http://</code> or <code>https://</code>  (example: <code>http://IP-address-of-SVP</code> or <code>https://IP-address-of-SVP</code>).</li> <li>5. Click OK. If Security Warning - HTTP Location displays, click Continue.</li> <li>6. Click OK on the Java Control Panel and close the window.</li> <li>7. Restart your web browser.</li> </ol>



**No response errors**

Error condition	Probable cause / recommended action
<p>Device Manager - Storage Navigator hangs and does not respond.</p>	<p>From the Device Manager - Storage Navigator secondary window, press <b>Ctrl+Alt+Shift+D</b> all at once to exit Device Manager - Storage Navigator.</p>

Error condition	Probable cause / recommended action
<p>Device Manager - Storage Navigator may hang in the following cases:</p> <ul style="list-style-type: none"> <li>▪ When you move a window displayed in front of the Device Manager - Storage Navigator secondary window, the area behind the window remains gray and does not go back to normal for a long period of time.</li> <li>▪ The entire Device Manager - Storage Navigator secondary window goes gray and does not go back to normal for a long period of time.</li> </ul>	<p>If you cannot exit Device Manager - Storage Navigator, reboot the management client or restart Device Manager - Storage Navigator after finishing Device Manager - Storage Navigator forcibly by the following way.</p> <ul style="list-style-type: none"> <li>▪ For Windows: Exit all applications using Java, and then terminate the javaw.exe and javaws.exe applications through Task Manager.</li> <li>▪ For UNIX: Exit all applications using Java, and then terminate javaw and javaws with the kill command.</li> </ul>
<p>When you click Refresh All or Refresh in the Device Manager - Storage Navigator secondary window, it displays the message "Loading" for a long time".</p>	<p>The probable causes are:</p> <ul style="list-style-type: none"> <li>▪ Another application such as Command Control Interface may be changing configuration. The window will be updated shortly after the configuration change ends.</li> <li>▪ Volume Migration operations, Quick Restore operations or Thin Image operations may be in progress. The window will be updated shortly after the operations end.</li> </ul>
<p>Error 110-67005 occurred during a Device Manager - Storage Navigator operation on the secondary window.</p>	<p>The probable causes are:</p> <ul style="list-style-type: none"> <li>▪ Another application such as Command Control Interface may be changing configuration.</li> <li>▪ Volume Migration operations, Quick Restore operations, or Thin Image operations may be in progress.</li> <li>▪ The configuration data may not be matched if a communication error occurs between the storage system and the SVP. Wait a few minutes and then click File &gt; Refresh All to reread the configuration information. Then launch Device Manager - Storage Navigator again.</li> </ul>

Error condition	Probable cause / recommended action
<p>While you are using a Device Manager - Storage Navigator secondary Window, it closes unexpectedly and error 20020-108000 occurs.</p>	<p>Start the Device Manager - Storage Navigator secondary window from the Device Manager - Storage Navigator main window again. If this error occurs repeatedly, close all the Device Manager - Storage Navigator windows, and then clear the Java and web browser caches.</p>
<p>The web browser closes abnormally</p>	<p>This problem can occur if a Mozilla process keeps running after Mozilla stops responding. Delete the "java_vm" and "mozilla" processes and continue with Device Manager - Storage Navigator operations.</p>
<p>One of the following sets of errors occurred when using Device Manager - Storage Navigator:</p> <ul style="list-style-type: none"> <li>▪ 20121-107024 and 10-6027</li> <li>▪ 20020-108000 and 10-6027</li> <li>▪ 10-6027</li> </ul>	<p>The probable causes are:</p> <ul style="list-style-type: none"> <li>▪ The SVP may have been restarted. Close Device Manager - Storage Navigator, wait 10 minutes, and then restart it.</li> <li>▪ The version of Device Manager - Storage Navigator installed on the management client might not match the SVP version. Close all the browser windows and then clear the browser cache.</li> <li>▪ The management client might be in standby or hibernate mode. Restart Device Manager - Storage Navigator.</li> <li>▪ If a proxy server is used for network connections, the proxy server cache may be storing the older version of the program. If the problem continues after you clear the browser cache, contact your network administrator.</li> <li>▪ Restart the web browser</li> </ul> <p>If none of the above actions solve the problem, save the Device Manager - Storage Navigator dump file and send it to customer support.</p>

### Incorrect display errors

Error condition	Probable cause / recommended action
Only the Exit button and the Refresh and Refresh All commands are effective when accessing the SVP from Device Manager - Storage Navigator.	The SVP might not be ready to perform some write processes from the other system. Wait a few minutes and then click File > Refresh. If the SVP is not restored, click Refresh All.
Only the Exit button and the Refresh All command are effective when accessing the SVP from the Device Manager - Storage Navigator.	An error may have occurred in the SVP. Click File > Refresh All. If the SVP is not restored, log in to Device Manager - Storage Navigator again.
The commands in the Go menu are unavailable.	<p>The required software options might not be installed or an error might occur on the window that appears after you click the command.</p> <p>Make sure that all the required software options are installed. If they are installed, do one of the following:</p> <ul style="list-style-type: none"> <li>▪ Click File &gt; Refresh.</li> <li>▪ Click File &gt; Refresh All.</li> <li>▪ Log in to Device Manager - Storage Navigator again.</li> </ul>
When you switch windows from one window to the Device Manager - Storage Navigator window, the Device Manager - Storage Navigator window is not displayed.	Close all windows, and then log in to Device Manager - Storage Navigator again.
The items in a list are not synchronized with a scroll bar.	Click the scroll buttons  or  above and below the scroll bar.
The focus disappears from the edit box.	Close all dialog boxes, and then log in to Device Manager - Storage Navigator again.
The web browser does not display correctly, because some GUI items such as labels and icons cannot be loaded properly.	Log out of Device Manager - Storage Navigator, and then log in again. If this error occurs before you log in to the Device Manager - Storage Navigator, close all dialog boxes and then log in to Device Manager - Storage Navigator.
The characters are unreadable because they are overlapped or garbled.	Log out of Device Manager - Storage Navigator, and then log in again.

Error condition	Probable cause / recommended action
<p>The characters are garbled in a window where a tree is displayed.</p>	<p>Click File &gt; Refresh.</p>
<p>Even though you have clicked Apply to change storage system settings, the new settings are not displayed in Device Manager - Storage Navigator.</p>	<p>Click File &gt; Refresh.</p>
<p>The dialog box that says Loading... stays open for a long period of time.</p>	<p>A Device Manager - Storage Navigator message dialog box other than the dialog box that says Loading... might be displayed behind this window. Press <b>Alt+Tab</b> to switch the dialog box.</p> <p>If the dialog box that says Loading... remains displayed for several hours after you apply the settings to the storage system, contact customer support.</p>
<p>The following information does not display in Device Manager - Storage Navigator windows:</p> <ul style="list-style-type: none"> <li>▪ Information on the storage system, such as ports or HDDs</li> <li>▪ Information configured with another management client</li> </ul>	<p>Click File &gt; Refresh. If the problem continues, close all Device Manager - Storage Navigator windows, and then clear the Web browser caches.</p>
<p>The Device Manager - Storage Navigator secondary window does not display.</p>	<ul style="list-style-type: none"> <li>▪ In the Java Control Panel, click the Temporary Internet Files section. In the Disk Space area, enter 1 MB, and then click Delete Files.</li> <li>▪ Click Security &gt; Java Control Panel. Ensure that Enable Java content in the browser is checked.</li> <li>▪ Clear the browser cache.</li> <li>▪ Ensure that Java Plug-in is enabled.</li> </ul> <p>If none of the above actions solve the problem, the web browser might not recognize Plug-in correctly. Initialize and redo the web browser settings.</p>

## Other errors

Error condition	Probable cause / recommended action
If you click in a Device Manager - Storage Navigator secondary window while a dialog box is open, the dialog box disappears behind the Device Manager - Storage Navigator secondary window.	Click the dialog box again.
An error occurs because a digital signature or security certificate has expired.	You can continue using Device Manager - Storage Navigator even though the digital signature for the Device Manager - Storage Navigator Java application is expired.
You specify IPv6 communication addresses when you start Device Manager - Storage Navigator, but IPv6 is not being used. Instead, IPv6 is being used and IPv4 addresses are output to audit logs for operations on the Device Manager - Storage Navigator secondary window.	IPv4 has higher priority when both IPv4 communication and IPv6 communication can be used. As a result, IPv4 may be used when you specify IPv6 communication addresses. Also, IPv4 addresses may appear in audit logs.  For details on configuring only IPv6 communication, see <a href="#">Network settings overview (on page 23)</a> .

## Clearing Java caches

When an error occurs on Device Manager - Storage Navigator, clear the Java and web browser caches to solve the problem. To clear the Java cache, click Delete the temporary files in the **General** dialog box of the Java Control Panel.

## Saving Java log and trace files

Before you contact your service representative, save the detail dump files collected using the Dump tool, and the Java log and trace file on your Device Manager - Storage Navigator computer, and then restart the web browser.

Examples of the Windows trace and log file locations are shown below.

- C:\Users\logon user ID\AppData\LocalLow\Sun\Java\Deployment\log\\*.trace
- C:\Users\logon user ID\AppData\LocalLow\Sun\Java\Deployment\log\\*.log

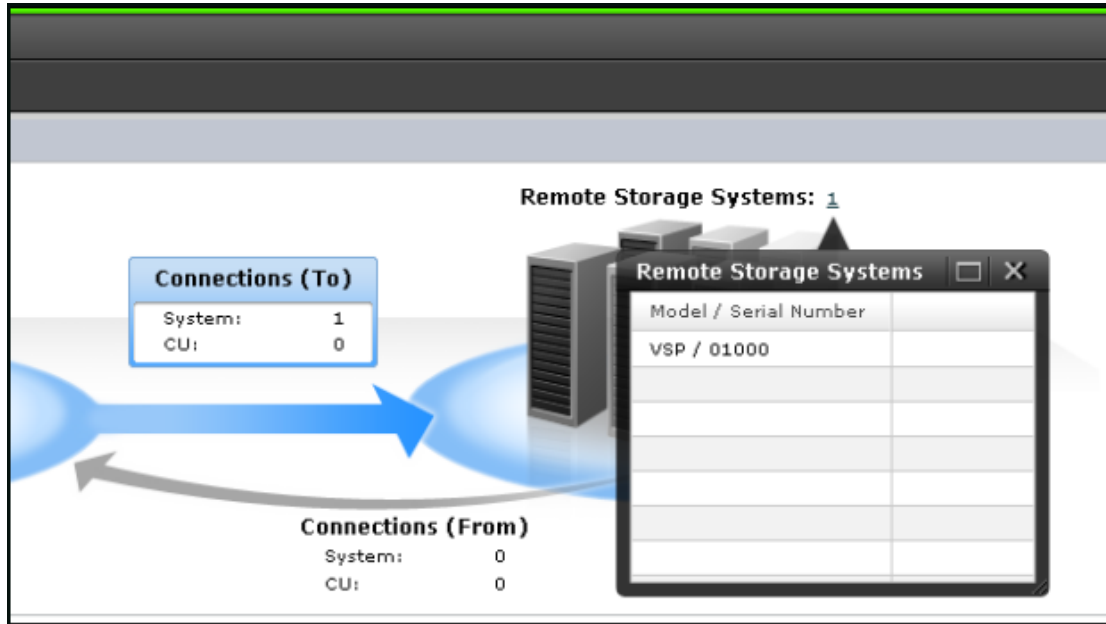
Examples of the UNIX trace and log file locations follow:

- *user home directory*\.java\deployment\log\\*.trace
- *user home directory*\.java\deployment\log\\*.log



## Balloon dialog box

When you click an underlined link on the Device Manager - Storage Navigator screen, additional information may appear as a pop-up, which is called a balloon dialog box. The following illustration shows an example of a balloon dialog box.



## Session timeout

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

## Updating your user view

If you remain in the same Device Manager - Storage Navigator view while other users change the configuration of the system, the changes that others make do not appear in your view. You can tell how long it has been since your screen was updated by checking the clock on the title bar to the left of the update button. The clock displays server time, not the time on your local workstation. When you place the cursor over the clock, the system displays the number of minutes that have passed since the screen was updated.

To see changes that others might have made, click Update in the title bar in the top right corner of the screen.

## Reverting to the default view

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

You can also return your settings to default.

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

The parts and items that are recorded as user settings are shown in the following table:

Window part		Item	State after reset
Magnification		-	Normal (100%)
Summary		Open/Closed	Open
Table	General	Selecting row	NA
		Page	First page
		Scroll position	Top left
		Setting column	Default state <sup>1</sup>
	Column	Sort	NA
		Width	Default state <sup>1</sup>
		Order	Default state <sup>1</sup>
	Option	Row/Page	1000
		Capacity unit	GB or Cyl
	Filter	ON/OFF	OFF
		Settings	NA
		Open/Closed	Closed
Wizard	Option part	Open/Closed	Default state <sup>1</sup>
LUN ID notation	-	-	Decimal integer
1. The default state varies from window to window.			

## Creating a login message

You can create text to be displayed on the Device Manager - Storage Navigator login page.


### Prerequisites

- You must have Security Administrator (View & Modify) role to perform this task.
- You must enable the Device Manager - Storage Navigator secondary window. See [Enabling the Device Manager - Storage Navigator secondary window \(on page 33\)](#).

### Procedure

1. Click **Settings > Security > Login Message**.

The Device Manager - Storage Navigator secondary window opens.

2. Click  to change to **Modify** mode.

3. Enter the message in the window.

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

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


---


## Chapter 3: Configuring the storage system

When configuring the storage system, you must set storage system information, set up the network connection, and register the SVP if using one.

### Setting storage system information

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

 **Caution:** Make sure to document the configured values, because they are required to use SNMP agents.

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

#### Before you begin

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

#### Procedure

1. In the Device Manager - Storage Navigator **Storage Systems** tree, select the storage system.
2. From **Settings**, click **Environmental Settings** > **Edit Storage System**.
3. Enter the items that you want to set.  
You can enter up to 180 alphanumeric characters (ASCII codes) excluding several symbols (\, / ; : \* ? " < > | & % ^). Do not use a space at the beginning or the end.
4. Click **Finish**.
5. In the **Confirm** window, check the settings and enter a task name in **Task Name**.
6. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Task** window opens to show the status of the task.

### Setting up security

Device Manager - Storage Navigator supports a variety of security features for authenticating users and configuring secure system operation.

Configure the storage system with the security settings appropriate for your environment.

## Setting up TCP/IP for a firewall

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

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

The following table describes the firewall configuration.

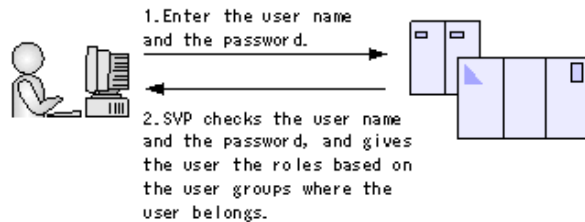
Protocol	Port number	Direction of communication
HTTP	80	From the Device Manager - Storage Navigator web client to the SVP
HTTPS	443	
HTTPS (raidinf)	5443	
RMI	1099	
RMI	51099	
RMI	51100	
SMI-S	427	
SMI-S	5989	
SNMP <sup>1</sup>	161	
SNMP Trap <sup>1</sup>	162	
Command Control Interface	31xxx <sup>2</sup>	From a host to the SVP
Command Control Interface	34xxx <sup>2</sup>	From the SVP to a host
Configuration Manager REST API	23454	From the SVP to the Configuration Manager REST API
<b>Notes:</b>		
<ol style="list-style-type: none"> <li>1. Required if you use a Device Manager - Storage Navigator web client as an SNMP manager.</li> <li>2. x indicates a number. For details about port numbers that are used for communication between a host and an SVP using CCI, see the <i>Command Control Interface User and Reference Guide</i>.</li> </ol>		

## Managing authentication and authorization servers

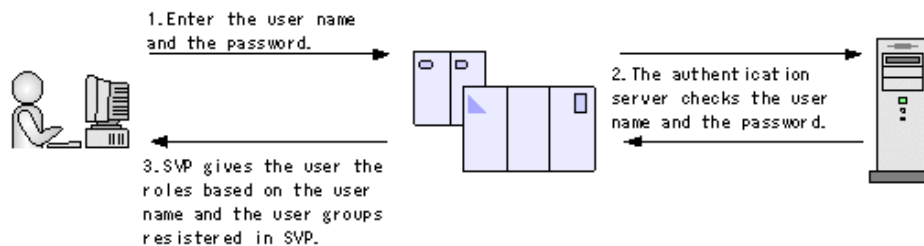
An authentication server enables users to log in to Device Manager - Storage Navigator with the same password as the password that they use for other applications.

The authentication server must be configured for each user.

The following figure shows login workflow without an authentication server:

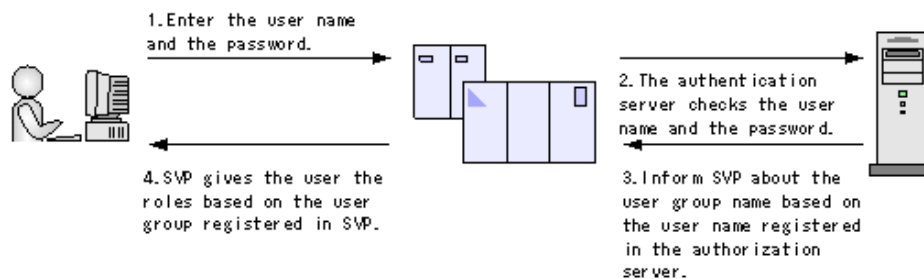


The following figure shows login workflow with an authentication server:



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 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 a service record (SRV) on 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 requirements

Authentication servers support the LDAP, RADIUS, and Kerberos protocols.

The following lists explain requirements for each protocol:

**LDAP****Authentication format**

LDAPv3 simple bind authentication

**Certificate file format**

- X509 DER format
- X509 PEM format

**RADIUS****Authentication format**

RFC 2865-compliant RADIUS

- PAP authentication
- CHAP authentication

**Kerberos****Authentication format**

Kerberos v5

**Encryption type****Windows**

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

**Solaris or Linux**

- DES-CBC-MD5

**Note:**

Two authentication servers (one primary and one secondary) can be connected to a storage system. In this case, the server configurations must be the same, except for the IP address and the port.

If you search for a server using information registered in the SRV records in the DNS server, confirm that the following conditions are satisfied. For RADIUS servers, you cannot use the SRV records.

**LDAP server conditions:**

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

**Kerberos server conditions:**

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

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

**Authorization server requirements**

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

**Prerequisite OS**

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

**Prerequisite software**

- Active Directory

**Authentication protocol for user for searching**

- LDAP v3 simple bind

**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 authentication and authorization servers**

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



### Before you begin

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

### Procedure

1. Click **Settings > Environmental Settings > View External Authentication Server Properties**.
2. Click **Setup Server** to open the **Setup Server** window
3. Select the type of the authentication server.
4. Specify options to connect to the authentication server. If you use more than one authentication server or an authorization server, specify an option for each server.
5. To test the connection, in the Server Configuration Test field, click **Check**.
6. Click **Finish**.
7. Enter a task name and then click **Apply**.
8. After you finish setting up the authentication and authorization servers and confirm that you can use the servers, save a copy of the configuration files for connecting the authentication server.

## Setting up SSL encryption

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



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



**Note:** To add the Secure attribute to cookies using Device Manager - Storage Navigator, you must block HTTP communication. For details, see [Blocking HTTP communication to the storage system \(on page 83\)](#).



**Note:** Device Manager - Storage Navigator supports HTTP Strict Transport Security (HSTS) with a max range of 31536000 seconds. To enable HSTS, you must use the security certificate issued by a trusted root certificate authority for your Device Manager - Storage Navigator domain. HSTS is valid for one year (31536000 seconds), and it is renewed automatically every time the HSTS header is sent to the browser. The security certificate to use is determined by the browser. For details, contact your browser vendor.

## SSL terminology

Note the following SSL terms:

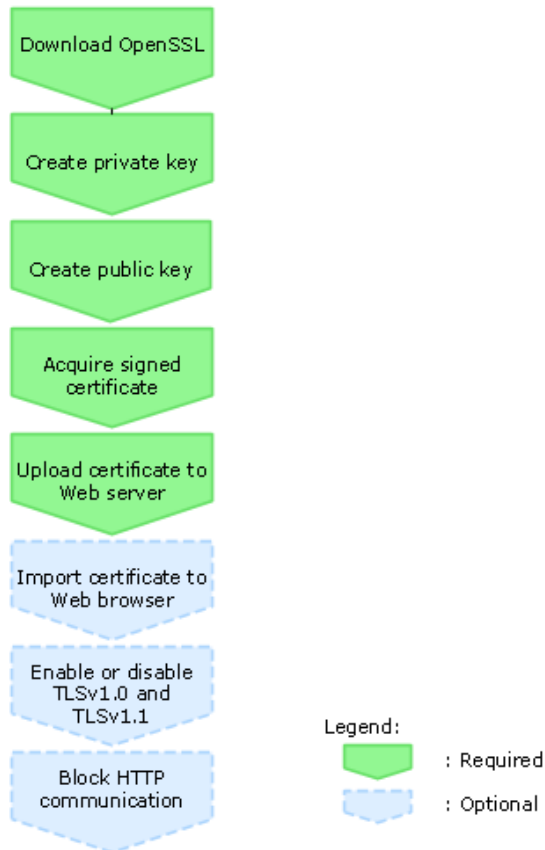
- **Secure Sockets Layer:** SSL is a protocol first developed by Netscape to securely transmit data over the Internet. Two SSL-enabled peers use their private and public keys to establish a secure communication session, with each peer encrypting transmitted data with a randomly generated and agreed-upon symmetric key.
- **Keypair:** A keypair is two mathematically-related cryptographic keys consisting of a private key and its associated public key.
- **Server Certificate:** A Server Certificate (also called a Digital Certificate) forms an association between an identity (in this case the SVP server) and a specific keypair. A Server Certificate is used to identify the SVP server to a client so that the server and client can communicate using SSL. Server Certificates come in two basic types:
  - **Self-signed:** You generate your own self-signed certificate and the subject of the certificate is the same as the issuer of the certificate. If the Device Manager - Storage Navigator computers and the SVP are on an internal LAN behind a firewall, you may find that this option provides sufficient security.
  - **Signed and Trusted:** For a Signed and Trusted Server Certificate, a Certificate Signing Request (CSR) is sent to and certified by a trusted Certificate Authority (CA) such as VeriSign (<http://www.verisign.com/>). Use of this certificate results in higher reliability in exchange for more cost and requirements.

If you enable SSL, you must make sure that the key pair and associated server certificate do not expire. If either the key pair or the server certificate expires, users will be unable to connect to the SVP.

## Setting up SSL communications

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

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



## Notes on updating the signed certificate to the SVP

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

- While the SVP server certificate is being updated, tasks that are being executed or scheduled for execution on Device Manager - Storage Navigator are not executed.
- Certificates for RMI communication are updated asynchronously (within approximately two minutes).
- If an SVP certificate is updated during Hitachi Command Suite setup operation, the Hitachi Command Suite setup operation will result in an error.
- Update of the SSL certificate gives a great influence to the system and may lead to SVP failure. Therefore take sufficient care about the content of the certificate and private key to be set.
- After the certificate update is complete, depending on the environment, the SVP web server can take 30 to 60 minutes to restart. When it takes that long, an internal server error occurs, and the update completion dialog box does not display. However, the certificate update is complete.

## Creating a keypair

To enable SSL, you must create a keypair consisting of a public and a private key on the management client. The instructions use Windows 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 2048
```

## 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 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.

- 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 []:

```

## Converting the SSL certificates to PKCS#12 format

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

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

### Before you begin

- You must store a private key and SSL certificate in the same folder.
- In the following procedure:
  - The private key file name is “client.key”.
  - The SSL certificate file name is “client.crt”.
  - The SSL certificate in PKCS#12 format is output to c:\key.

### 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.

## 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 \(on page 78\)](#).
- 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 \(on page 78\)](#).



### 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.

## 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
```

## Uploading 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.

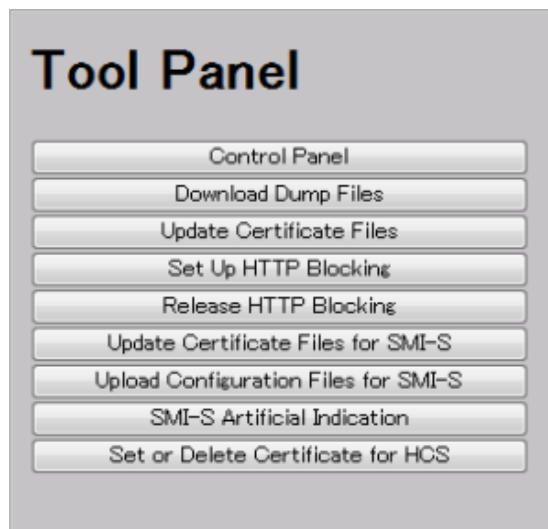
### Before you begin

- 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`. See [Creating a private key \(on page 76\)](#).
- 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 \(on page 76\)](#).
- 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 \(on page 78\)](#).
- The passphrase for the private key (server.key file) is released.

### Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. On the management client, open a web browser and enter the following URL to open the **Tool Panel** dialog box.

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



3. In the **Tool Panel** dialog box, click **Update Certificate Files**.  
If SSL communication has been established, the **Security Alert** dialog box opens before the login dialog box opens. In the **Security Alert** dialog box, click **OK**. The **Security Alert** dialog box closes and the **Login** dialog box opens.



4. In the **Login** dialog box, enter the administrator user ID and password, and click **login**. The **Upload** dialog box opens.
5. In the **Upload** dialog box, enter the public key certificate file name in the Certificate file box and the private Key file name (server.key file) in the Key file box. You can enter the file names directly or by clicking **Browse**.
6. In the **Upload** dialog box, click **Upload**. A confirmation dialog box opens.
7. Click **OK** to begin the certificate update. When the update is complete, the SVP web server restarts.

Depending on the environment, the SVP web server can take 30 to 60 minutes to restart. When it takes that long, an internal server error occurs, and the update completion dialog box does not display. However, the certificate update is complete.

It can take 30 to 60 minutes for the web server to restart. After the SVP restarts, the **Completion** dialog box does not appear. Instead, an "internal server error" message is displayed. However, the setting is actually completed.

8. In the error message box, click **OK**. If the **Security Alert** dialog box for the certificate opens, click **View Certificate** to display the certificate. Confirm that the certificate is correct, and click **Yes**.



**Note:** If an error occurs during the certificate update, an error message displays. Resolve the problem described in the error message and then repeat this procedure, starting with Step 4 (login) above.

## Returning the certificate to default

You can return the certificate that was updated by the procedure in [Uploading a signed certificate \(on page 80\)](#) to default.

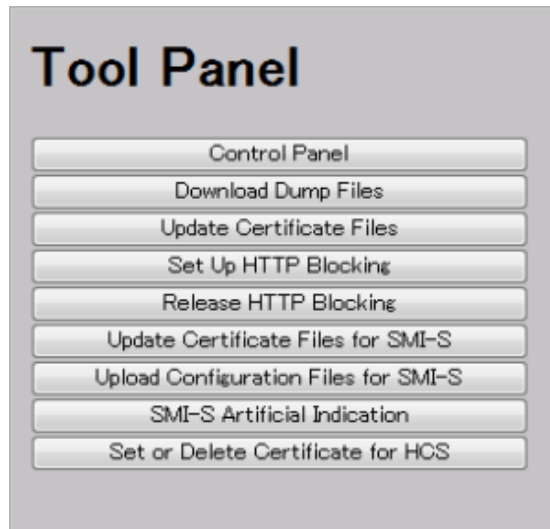
### Before you begin

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

### Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. On the Device Manager - Storage Navigator computer, open a web browser and enter the following URL to open the **Tool Panel** dialog box.

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



3. In the **Tool Panel** dialog box, click **Update Certificate Files**. The **Update Certificate Files** dialog box opens.  
If SSL communication has been established, the **Security Alert** dialog box opens before the login dialog box. In the **Security Alert** dialog box, click **OK**.
4. In the **Login** dialog box, enter the administrator user ID and password, and click **login**. The **Upload** dialog box opens.
5. In the **Upload** dialog box, click **Return to Default**. A confirmation dialog box opens.
6. Click **Yes** to confirm and close the dialog box.  
When the certificate update is complete, the SVP Web server restarts to show the update. When the restart is complete, the **Update Completion** dialog box opens.
7. In the **Update Completion** dialog box, click **OK**. The dialog box closes and the display returns to the **Login** dialog box.



**Note:** If an error occurs during the certificate update, an error message appears. Resolve the problem described in the error message and then repeat this procedure, starting with Step 4 (login) above.

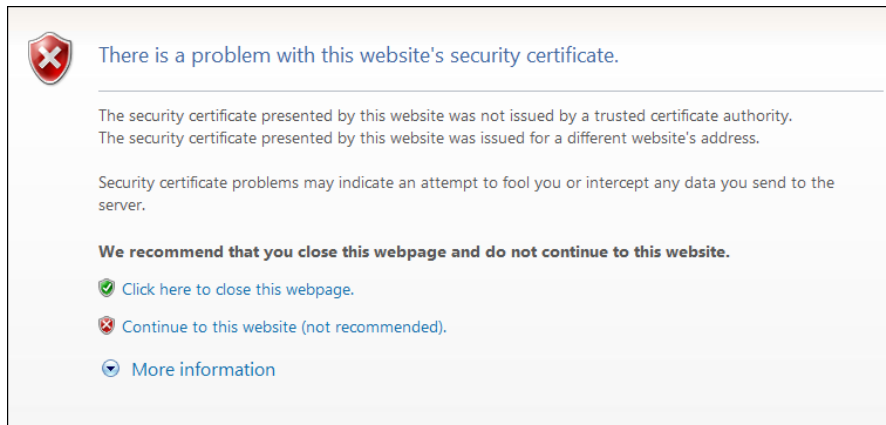


**Note:** If the **Security Alert** dialog box for the certificate opens at other times, click **View Certificate** to confirm that the certificate is correct and then click **Yes**.

## Problems with a website security certificate

Some operations in the Device Manager - Storage Navigator menu are executed with a Java application. Therefore, an SSL-related security warning may appear when the secondary window opens. 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.



## Disabling TLSv1.0 and TLSv1.1 communications

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

If you want to disable TLSv1.0 and TLSv1.1 communications, contact the customer support.



**Note:** If you disable TLSv1.0 and TLSv1.1 communications, pages might not be displayed correctly depending on the TLS setting. Change the TLS setting of the browser.

## Enabling TLSv1.0 and TLSv1.1 communications

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

If you want to enable TLSv1.0 and TLSv1.1 communications, contact the customer support.

## Blocking HTTP communication to the storage system

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

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

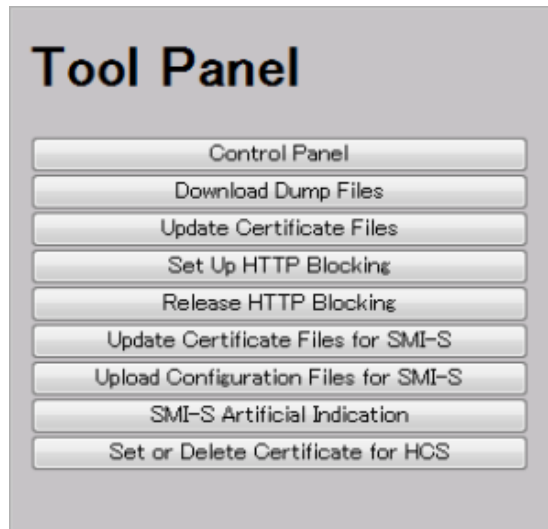
## Before you begin

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

## Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. On the Device Manager - Storage Navigator computer, open a web browser and enter the following URL to open the **Tool Panel** dialog box.

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



3. In the **Tool Panel** dialog box, click **Set up HTTP Blocking**. A login dialog box opens.
4. In the **Login** dialog box, enter the storage administrator user ID and password, then click **Login**. The **Set up HTTP Blocking** dialog box opens.
5. In the dialog box, click **OK**. A confirmation dialog box opens.
6. In the confirmation dialog box, click **OK** to implement HTTP blocking.

When the configuration change is complete, the SVP web server restarts. When the restart is complete, the **HTTP Communications Blocked** dialog box opens.

Depending on the environment, it can take 30 to 60 minutes for the web server to restart. If it does, after the SVP restarts, the **Completion** dialog box does not appear. Instead, an "internal server error" message appears. However, the setting is actually completed.

7. Click **OK** to continue the operation and return to the **Login** dialog box, or click **Cancel** to cancel the operation and return to the **Login** dialog box.

## Releasing HTTP communication blocking

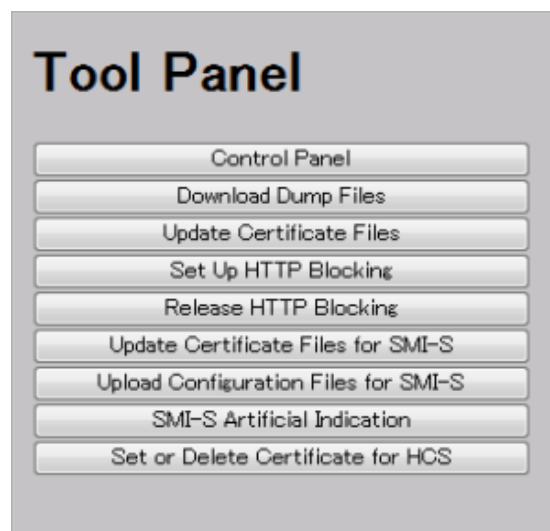
### Before you begin

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

### Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. On the Device Manager - Storage Navigator computer, open a web browser. Enter the following URL to open the **Tool Panel** dialog box.

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



3. In the **Tool Panel** dialog box, click **Release HTTP Blocking**.
4. Enter the User ID and Password for the root storage administrator, then click **Login**. The **Release HTTP Blocking** dialog box opens.
5. Click **OK**. A configuration dialog box opens.
6. Click **OK** to release HTTP blocking. When the configuration change is complete, the SVP web server reboots. Once the reboot is complete, the **Release HTTP Blocking Complete** dialog box opens.  
Depending on the environment, it can take 30 to 60 minutes for the web server to restart. After the SVP restarts, the **Completion** dialog box does not appear. Instead, an "internal server error" message is displayed. However, the setting is actually completed.
7. Click **OK** to continue the operation and return to the **Login** dialog box, or click **Cancel** to cancel the operation and return to the **Login** dialog box.

## Configuring certificates for HCS

To configure certificates for HCS, you must use the Device Manager - Storage Navigator **Tool Panel**.

Hitachi Command Suite (HCS) uses certificates to verify the server's reliability when SSL communication for HCS external authentication is performed. You can register and delete certificates by using the command prompt.

## Registering certificates for HCS

To check the server reliability at the time of SSL communication for HCS external authentication, upload an HCS public key certificate to the web server to register the certificate. Complete the steps in the following procedure to upload and register a certificate using the certificate update tool.

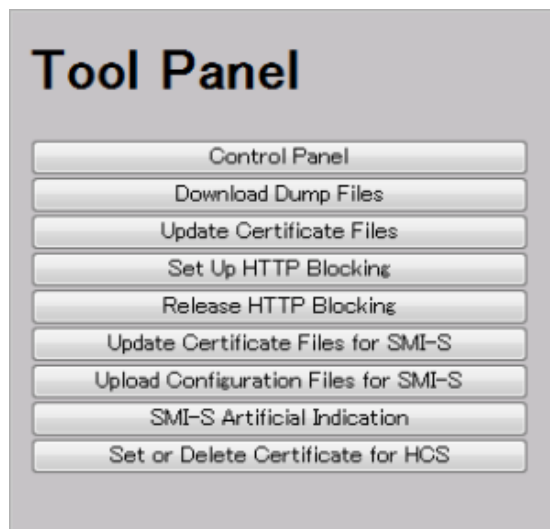
### Before you begin

- You must have the Security Administrator (View & Modify) role to perform this task.
- If the certificate to be registered has an extension other than ".crt", change it to ".crt".
- The certificate to be registered must be in X509 PEM or X509 DER format.

### Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. On the Device Manager - Storage Navigator computer, open a web browser and enter the following URL to open the **Tool Panel** dialog box.

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



3. In the **Tool Panel** dialog box, click **Set or Delete Certificate File for HCS**. The **Login** dialog box opens.  
If SSL communication has been established, the **Security Alert** dialog box opens before the **Login** dialog box. In the **Security Alert** dialog box, click **OK**.
4. When the **Login** dialog box opens, enter the administrator user ID and password, and click **Login**. The **Login** dialog box opens.

5. In the dialog box, enter the certificate file for HCS (.crt file) in the Certificate file (.crt file) box. You can enter the file name directly or by clicking **Browse** and searching for the file name.
6. Click **Register**. The execution confirmation dialog for **Set or Delete Certificate File for HCS** opens.
7. Click **OK** to register the certificate. Registration of the certificate starts.  
When the certificate is registered, the registration completion dialog box for **Set or Delete Certificate File for HCS** opens.
8. In the registration completion dialog box for **Set or Delete Certificate File for HCS**, click **OK**. The display returns to the login dialog box.



**Note:** If an error occurs during registration of the HCS certificate, an error message displays. Resolve the problem and then run the procedure again, starting with logging in to Set or Delete HCS Certificate.



**Note:** If the **Security Alert** dialog box for the certificate opens at other times, click **View Certificate** to confirm that the certificate is correct and then click **Yes**.

## Notes on registering certificates for HCS

Read the following notes about registering certificates for HCS:

- Ensure that the certificate to be registered is the right one. If you register a wrong certificate, HCS external authentication is not performed.
- Only with registration or deletion of the correct certificate, HCS external authentication operates normally

## Deleting certificates for HCS

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

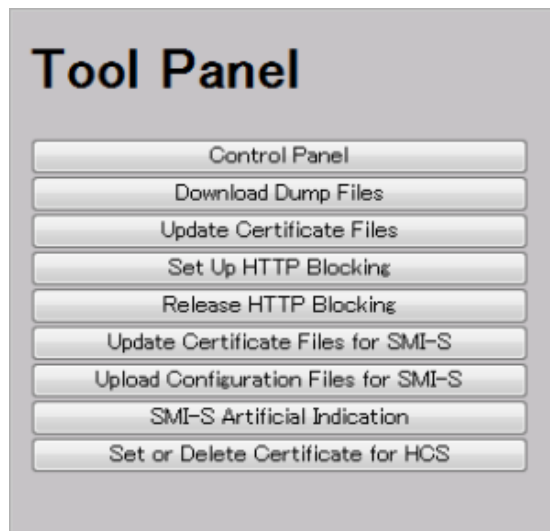
### Before you begin

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

### Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. On the Device Manager - Storage Navigator computer, open a web browser and enter the following URL to open the **Tool Panel** dialog box.

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



3. In the **Tool Panel** dialog box, click **Set or Delete Certificate File for HCS**. The login dialog box opens.  
If SSL communication has been established, the **Security Alert** dialog box opens before the login dialog box. In the **Security Alert** dialog box, click **OK**.
4. In the login dialog box, enter the administrator user ID and password, and click **Login**. The **Set or Delete Certificate File for HCS** dialog box opens.
5. In the dialog box, click **Delete**. A confirmation dialog box opens.
6. Click **OK** to delete the certificate. Deletion of the certificate starts.
7. When the certificate has been deleted, a completion dialog box opens.
8. In the completion dialog box click **OK**. The display returns to the login dialog box.



**Note:** If an error occurs during deletion of the certificate for HCS, an error message displays. Resolve the problem and then run the procedure again, starting with logging in, to Set or Delete Certificate for HCS.



**Note:** If the **Security Alert** dialog box for the certificate opens at other times, click **View Certificate** to confirm that the certificate is correct and then click **Yes**.

## Changing advanced system settings

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

Log off and log in again after you have enabled or disabled an advanced system setting.



### Before you begin

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

### Procedure

1. Click **Settings > Environmental Settings > Edit Advanced System Settings**.
2. Select the advanced system settings and click **Enable**.

Option	Description
<b>Hide alert information</b>	If you enable this advanced system setting, the <b>Alert</b> window in the Device Manager - Storage Navigator main window does not open.
<b>Refresh forcibly after Apply</b>	If you enable this advanced system setting, after settings changes are applied to the storage system, the configuration information for the storage system is always updated to the latest information.
<b>Disable data polling</b>	If you enable this advanced system setting, polling stops.
<b>Disable retry of data updating</b>	If you enable this advanced system setting, retry does not occur even if data cannot be acquired.
<b>Enable Device Manager - Storage Navigator 2 All Function</b>	If you enable this advanced system setting, the restrictions on login from Device Manager - Storage Navigator's login window are cleared, including the restrictions on the users who can log in and on the functions available after login. When enabling or disabling the advanced system setting, log in again.
<b>External Authentication Compatibility option</b>	If you enable this option, the authentication method is switched from VSP G1x00 and VSP F1500 to VSP.
<b>Enable reboot of background service</b>	If you enable this option, when either of the followings exceeds its threshold value, the background service process for managing configuration information is restarted. Enable this option only when requested. <ul style="list-style-type: none"> <li>▪ The amount of memory used in the background service process.</li> <li>▪ Time elapsed after the background service process is started.</li> </ul>
<b>Notify an alert when tier relocation is suspended by system</b>	If you enable this option, when tier relocation is suspended by the system, an alert is issued to users. For details about an alert (SIM) to be issued, see the Troubleshooting chapter of the <i>Provisioning Guide for Open Systems</i> or <i>Provisioning Guide for Mainframe Systems</i> .

Option	Description
<b>Disable login of the same user</b>	Set this option only when requested.
<b>Disable cache of the PP Info</b>	Set this option only when requested.
<b>Use a unique SNMP engine ID</b>	If you enable this option, a unique SNMP engine ID is set. If you disable it, the fixed value is set. When changing the settings for this option, first set <b>SNMP Agent</b> to <b>Disable</b> , then after the completion of the settings, set it back to <b>Enable</b> .

3. Click **Finish**. The **Confirm** window opens.
4. In the **Confirm** window, check the settings and enter a task name in **Task Name**.
5. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Task** window opens to display the status of the task.

## Backing up HDvM - SN configuration files

You can make backup copies of the various Device Manager - Storage Navigator configuration files by downloading them to a folder that you specify. You can then use the backup copies to restore one or more configuration files if it becomes necessary. See [Restoring HDvM - SN configuration files \(on page 92\)](#).

### Before you begin

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

Configuration file	Description	Required role to back up a file	Required role to restore a file
User Account Information	User account information registered to the Device Manager - Storage Navigator.	Security Administrator (View Only)	Security Administrator (View & Modify)
Environment Parameter List	The parameters settings in the Set Env. window.	Storage Administrator (Initial Configuration)	Storage Administrator (Initial Configuration)
Log Transfer Information	Settings made in the <b>Edit Audit Log Settings</b> window and the <b>Edit Alert Settings</b> wizard	Audit log Administrator (View Only)	Audit log Administrator (View & Modify)
SIMSyslog Transfer Information	Settings made in the <b>Edit Alert Settings</b> wizard	Storage Administrator (Initial Configuration)	Storage Administrator (Initial Configuration)

Configuration file	Description	Required role to back up a file	Required role to restore a file
External Authentication	Connection to the authentication server.	Security Administrator (View & Modify)	Security Administrator (View & Modify)
Key Management Server	Connection to the Key Management Server <sup>1</sup>	Security Administrator (View & Modify)	Security Administrator (View & Modify)
Password Policy	Password policy for backing up encryption keys on the Device Manager - Storage Navigator computer	Security Administrator (View & Modify)	Security Administrator (View & Modify)

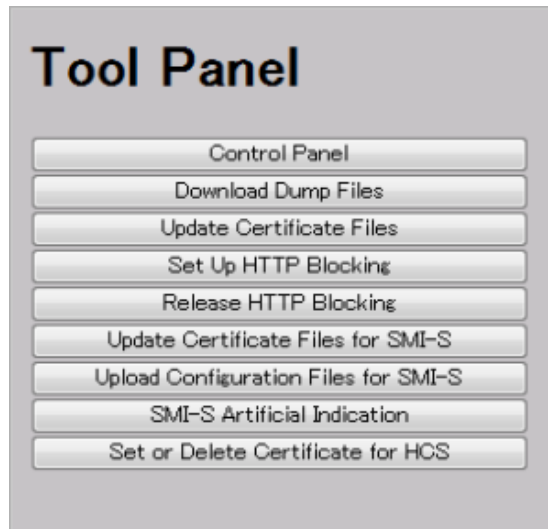
**Notes:**

1. The client certificate in use when the key management (KMIP) server is connected cannot be backed up or restored by Device Manager - Storage Navigator. Consult the administrator of the key management server to determine the best way to use the server to manage and back up the certificate.

### Procedure

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

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



2. Click **Control Panel** to open the Control Panel.
3. Enter the user ID and password and click **Login**.
4. Click the **Download** tab to open the **Download** file window.

5. Click the files to be downloaded. You can download only the files for which you have permission.
6. Click **Submit**. The **Download File** dialog box shows the list of the files to be downloaded.
7. Click **Download**. The **File Download** dialog box opens.
8. Click **Save**. The **Save As** dialog box opens.
9. Specify the name of a folder to save the compressed file, and then click **Save** to start downloading.
10. Decompress the downloaded \*.tgz file as required. To decompress the \*.tgz file, use a tool supporting tar and gzip.

## Restoring HDvM - SN configuration files

You can restore the backup copies of one or more configuration files if it becomes necessary.

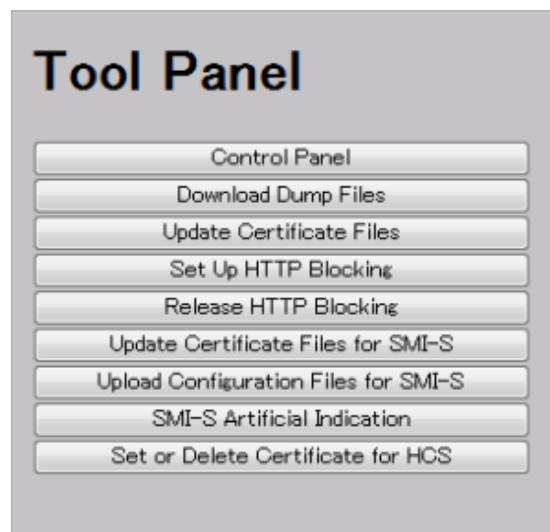
### Before you begin

- See Prerequisites in [Backing up HDvM - SN configuration files \(on page 90\)](#).

### Procedure

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

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



2. Click **Control Panel** to open the Control Panel.
3. Enter the user ID and password and click **Login**.
4. Click the **Restore** tab to open the **Restore** file window.
5. Click the files and click **Browse** to specify the directory of the file. You can restore only the files for which you have permission.

6. Click **Next**.
7. Click the configuration files to restore.
8. Click **Submit**.
9. If the **Password check** dialog box opens, enter **User ID**, **Password**, and **Re-enter Password** of the storage administrator on the backup user list, and click **Submit** on the **Password check** dialog box.  
The **Restore File** dialog box opens.
10. Confirm the restoring process has been completed successfully.
11. Click **Close** to close the dialog box.

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

Hitachi Virtual Storage Platform G1x00 and Hitachi Virtual Storage Platform F1500 storage systems support the SMI-S function developed by SNIA. Storage administrators can use the SMI-S function by using SMI-S compliant management software.

### Using the SMI-S function

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

#### Procedure

1. Create a Device Manager - Storage Navigator user account in the management software. The user account must belong to one of the following built-in user groups:
  - Storage Administrator (View & Modify) User Group: Users have full permissions to access the SMI-S function from the management software.
  - Storage Administrator (View Only) User Group: Users have read- only permissions to access the SMI-S function from the management software.
2. In the management software program, enter the following storage system information:
  - **IP Address** of the storage system
  - **Protocol**: specify **HTTPS**
  - **Port**: **5989**
  - **Namespace**:**root/hitachi/smis** or **interop**

### Uploading a signed certificate to the SMI-S provider

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

## Before you begin

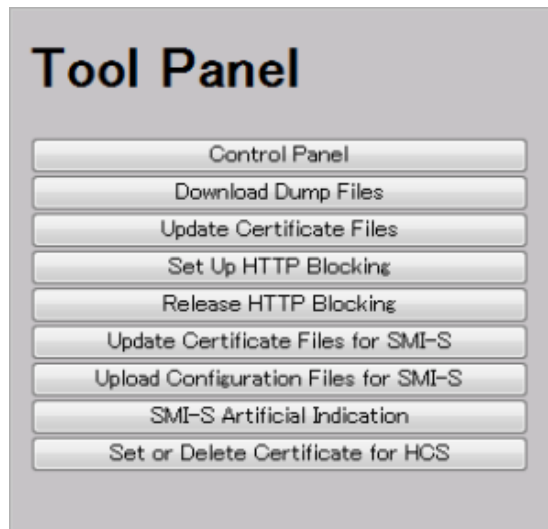
Ensure that the following items have been completed:

- You must have the Storage Administrator (View & Modify) role to perform this task.
- A private key (.key file) has been created. Change the file name to server.key unless the file is already named that. See [Creating a private key \(on page 76\)](#).
- The passphrase for the private key (server.key file) is released.
- A signed public key certificate (.crt file) has been acquired. Change the file name to server.crt unless the file is already named that. See [Creating a public key \(on page 76\)](#).
- The private key (.key file) is in PEM format. (You cannot use the DER format.)
- The signed public key certificate (.crt file) is in X509 PEM format. (You cannot use the X509 DER format.) See [Obtaining a self-signed certificate \(on page 78\)](#).

## Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. On the Device Manager - Storage Navigator computer, open a web browser and enter the following URL to open the **Tool Panel** dialog box.

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



3. In the **Tool Panel** dialog box, click **Update Certificate Files for SMI-S**. The login dialog box for **Update Certificate Files for SMI-S** opens.  
If SSL communication has been established, the **Security Alert** dialog box opens before the login dialog box. In the **Security Alert** dialog box, click **OK**.
4. In the login dialog box for Update Certificate Files for SMI-S, enter the administrator's user ID and password, and click **Login**. The upload dialog box for Update Certificate Files for SMI-S opens.
5. In the upload dialog box for Update Certificate Files for SMI-S, enter both the public key certificate file name in the Certificate file (server.crt file) box and the Private Key file (server.key file) box. You can enter the file names directly or by clicking **Browse**.

6. Click **Upload**. The execution confirmation dialog box for Update Certificate Files for SMI-S opens.
7. Click **OK** to update the certificate. Update of the certificate starts.  
Upon completion of the certificate update, the SMI-S provider restarts to reflect the update.  
  
Upon completion of the restart of the SMI-S provider, the update completion dialog box for Update Certificate Files for SMI-S opens
8. In the update completion dialog box for Update Certificate Files for SMI-S, click **OK**. The display returns to the login dialog box.



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



**Note:** If the **Security Alert** dialog box for the certificate opens at other times, click **View Certificate** to confirm that the certificate is correct and then click **Yes**.

## Returning an SMI-S provider certificate to default

You can return a certificate updated in [Uploading a signed certificate to the SMI-S provider \(on page 93\)](#) to default.

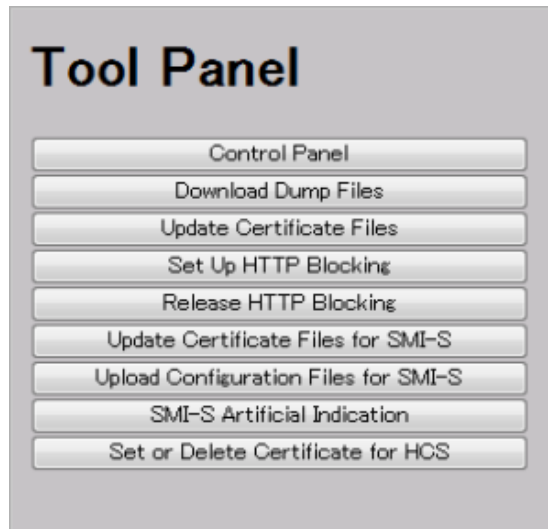
### Before you begin

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


### Procedure


1. Close all Device Manager - Storage Navigator sessions on the SMI-S provider.
2. On the Device Manager - Storage Navigator computer, open a web browser and enter the following URL to open the **Tool Panel** dialog box.

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



3. In the **Tool Panel** dialog box, click **Upload Configuration Files for SMI-S**. The **Upload Configuration Files Login** dialog box opens.  
If SSL communication has been established, the **Security Alert** dialog box opens before the login dialog box. In the **Security Alert** dialog box, click **OK**.
4. In the **Login** dialog box, enter the administrator's user ID and password, and click **Login**. The upload dialog box for Update Certificate Files for SMI-S opens.
5. In the upload dialog box for Update Certificate Files for SMI-S, click **Return to the default configuration**. The execution confirmation dialog box for Update Certificate Files for SMI-S opens.
6. Click **OK** to update the certificate. Update of the certificate starts.  
Upon completion of the certificate update, the SMI-S provider restarts to reflect the update. Upon completion of the restart of the SMI-S provider, the update completion dialog box for Update Certificate Files for SMI-S opens.
7. In the update completion dialog box for Update Certificate Files for SMI-S, click **OK**. The display returns to the login dialog box.

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

 **Note:** If the **Security Alert** dialog box for the certificate opens at other times, click **View Certificate** to confirm that the certificate is correct and then click **Yes**.

## Uploading an SMI-S provider configuration file

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



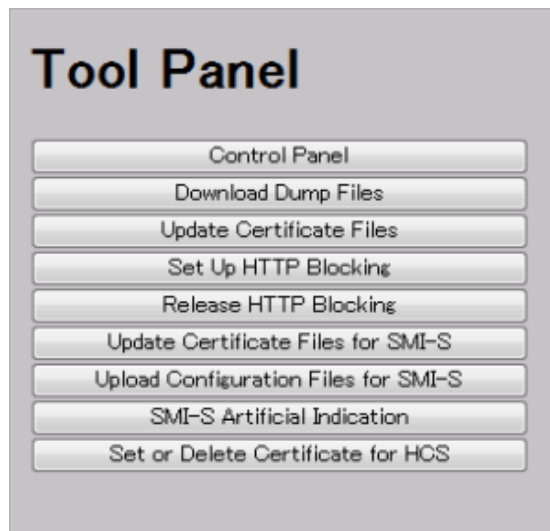
### Before you begin

- Ensure that the SMI-S provider configuration file has already been created. If the configuration is not already named array-setting-01.properties, rename it to that name.
- You must have the Storage Administrator (View & Modify) role to perform this task.


### Procedure


1. Close all Device Manager - Storage Navigator sessions on the SMI-S provider.
2. On the Device Manager - Storage Navigator computer, open a web browser and enter the following URL to open the **Tool Panel** dialog box.

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



3. In the **Tool Panel** dialog box, click **Upload Configuration Files for SMI-S**. The **Login** dialog box opens.  
If SSL communication has been established, the **Security Alert** dialog box opens before the **Login** dialog box. In the **Security Alert** dialog box, click **OK** to confirm and open the **Login** dialog box.
4. In the **Login** dialog box, enter the administrator user ID and password, and click **Login**. The **Upload** dialog box opens.
5. In the **Upload** dialog box, enter the SMI-S provider configuration file (array-setting-01.properties).  
Enter a file name in Configuration file or click **Browse** and then select a file in the displayed dialog box.
6. Click **Upload**. The execution confirmation dialog box opens.
7. Click **OK** to update the configuration file. Update of the configuration file starts.  
Upon completion of the configuration file update, the SMI-S provider restarts to reflect the update. Upon completion of the restart of the SMI-S provider, the update completion dialog box for Upload Configuration Files for SMI-S opens.
8. In the **Upload Configuration Files for SMI-S** dialog box, click **OK**. The display returns to the login dialog box.

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

 **Note:** If the **Security Alert** dialog box for the certificate opens at other times, click **View Certificate** to confirm that the certificate is correct and then click **Yes**.

## Returning an SMI-S provider configuration file to default

You can return a configuration file updated in [Uploading an SMI-S provider configuration file \(on page 96\)](#).

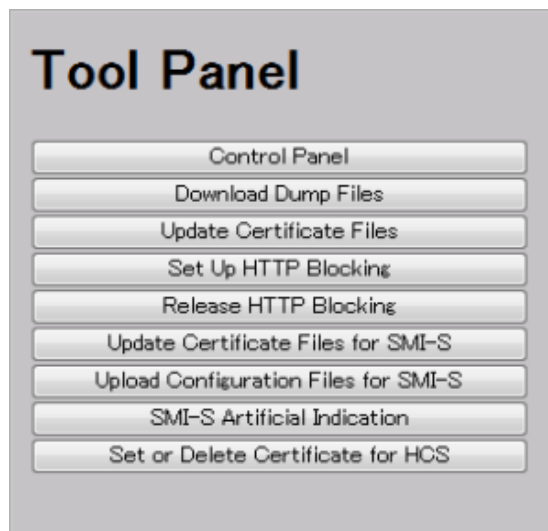
### Before you begin

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

### Procedure

1. Close all Device Manager - Storage Navigator sessions on the SMI-S provider.
2. On the Device Manager - Storage Navigator computer, open a web browser and enter the following URL to open the **Tool Panel** dialog box.

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



3. In the **Tool Panel** dialog box, click **Upload Configuration Files for SMI-S**. The **Login** dialog box opens.  
If SSL communication has been established, the **Security Alert** dialog box opens before the **Login** dialog box. In the **Security Alert** dialog box, click **OK** to confirm and open the **Login** dialog box.
4. In the **Login** dialog box, enter the administrator user ID and password, and click **Login**. The **Upload** dialog box opens.

5. In the **Upload** dialog box, click **Return to the default configuration**. A confirmation dialog box opens.
6. In the confirmation dialog box, click **OK** to update the configuration file. The update process starts.  
When the file has been updated, the SMI-S provider restarts to include the update. When the SMI-S provider restarts, the update completion dialog box opens.
7. In the update completion dialog box, click **OK** to confirm and return to the **Login** dialog box.



**Note:** If an error occurs during update of the SMI-S provider configuration file, an error message appears. Resolve the problem described in the error message and then run the procedure again, starting with Step 4.



**Note:** If the **Security Alert** dialog box for the certificate opens at other times, click **View Certificate** to confirm that the certificate is correct and then click **Yes**.

## Sending SMI-S artificial indication

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

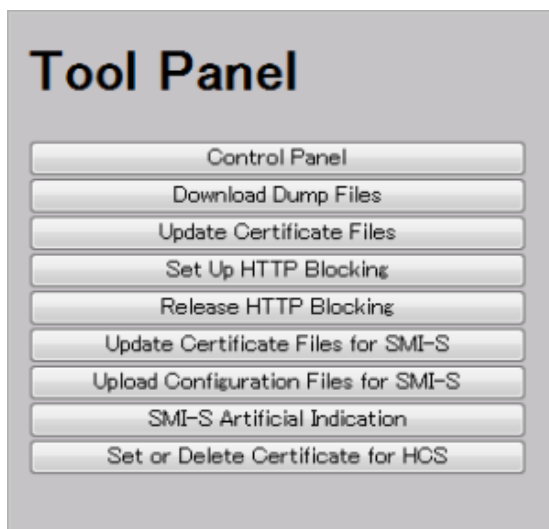
### Before you begin

- SMI-S Provider software application must be installed.
- The network environment is configured so that the computer on which the listener application operates is connected to the SVP.
- The listeners are subscribed to the SMI-S provider.
- You must have the Storage Administrator (View & Modify) role to perform this task.

### Procedure

1. Close all Device Manager - Storage Navigator sessions connected to the related SMI-S provider.
2. On the Device Manager - Storage Navigator computer, open a web browser and enter the following URL to open the **Tool Panel** dialog box.

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



3. In the **Tool Panel** dialog box, click **SMI-S Artificial Indication**. The **SMI-S Artificial Indication** dialog box opens.
4. In the **SMI-S Artificial Indication** dialog box, enter the user ID and password, and click **Test**. The testing begins.
5. When the test communication is completed, **SMI-S Artificial Indication Result** window opens. In the **SMI-S Artificial Indication Result** window, click **OK**.

The dialog box closes and the display returns to the **SMI-S Artificial Indication** dialog box.



**Note:** If the SMI-S artificial indication fails, an error message and a code display. Resolve the problem described in the error message.

## 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`

---

## Chapter 4: User administration using Device Manager - Storage Navigator

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

### User administration overview

Device Manager - Storage Navigator provides a rich set of user administration, roles and permissions, and access control features. Administrators can manage users by groups and set up access control by defining who can access what storage resources .

### Manage roles and permissions

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 modify storage system settings 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 \(on page 113\)](#).
- Regardless of assigned roles, users in a user group to which no resource groups are assigned cannot modify storage system settings.
- 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 <sup>1</sup>
User A	user group 10	Storage Administrator <sup>2</sup>	Resource group 10
User B	user group 20	Storage Administrator <sup>2</sup>	Resource group 20
<b>Notes:</b>			
<ol style="list-style-type: none"> <li>1. For the user group that is assigned the Security Administrator role, All Resource Groups Assigned is automatically set to Yes.</li> <li>2. There are a few types of storage administrators. For more information, see <a href="#">Roles and permissions (on page 105)</a>.</li> </ol>			

## Roles and user groups

Roles are defined for each user group. The tasks that users can do on the system depend on the roles assigned to the user groups to which they belong. Users can belong to from one to eight groups. To change the privileges that are assigned to users, use either of the following methods:

- Add users to groups with the permissions they need or delete users from groups with permissions they don't need.
- Change the roles assigned to the group to which the users belong.

## Resource group and user groups

The resource groups determine the resources that users can manage. They are associated with user groups rather than users. There are two ways to change the resources that are allowed to users:

- Moving users to another user group.
- Change the resource groups assigned to the user group where the user belongs.

For details about resource groups, see the *Provisioning Guide for Open Systems*.

## User group registration example

- 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 <sup>1</sup>
User A	user group 10	Storage Administrator <sup>2</sup>	Resource group 10
User B	user group 20	Storage Administrator <sup>2</sup>	Resource group 20
<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. For the user group that is assigned the Security Administrator role, All Resource Groups Assigned is automatically set to Yes.</li> <li>2. There are a few types of storage administrators. For more information, see <a href="#">Roles and permissions (on page 105)</a>.</li> </ol>			



## Precautions when working with user groups

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 \(on page 113\)](#).

## 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.

## Roles and permissions

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.



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

Role	Permissions
Security Administrator (View Only)	<ul style="list-style-type: none"> <li>▪ Viewing information about user accounts and encryption settings</li> <li>▪ Viewing information about the encryption key in the key management server</li> </ul>
Security Administrator (View & Modify)	<ul style="list-style-type: none"> <li>▪ Configuring user accounts</li> <li>▪ Creating encryption keys and configuring encryption settings</li> <li>▪ Viewing and switching where encryption keys are generated</li> <li>▪ Backing up and restoring encryption keys</li> <li>▪ Deleting encryption keys backed up in the key management server</li> <li>▪ Viewing and changing the password policy for backing up encryption keys on the management client</li> <li>▪ Connection to the external server</li> <li>▪ Backing up and restoring connection configuration to the external server</li> <li>▪ Configuring the certificate used for the SSL communication</li> <li>▪ Configuring the fibre channel authentication (FC-SP)</li> <li>▪ Configuring resource groups</li> <li>▪ Editing virtual management settings</li> <li>▪ Setting reserved attributes for global-active device</li> </ul>
Audit Log Administrator (View Only)	<ul style="list-style-type: none"> <li>▪ Viewing audit log information and downloading audit logs</li> </ul>
Audit Log Administrator (View & Modify)	<ul style="list-style-type: none"> <li>▪ Configuring audit log settings and downloading audit logs</li> </ul>
Storage Administrator (View Only)	<ul style="list-style-type: none"> <li>▪ Viewing storage system information</li> </ul>
Storage Administrator (Initial Configuration)	<ul style="list-style-type: none"> <li>▪ Configuring settings for storage systems</li> <li>▪ Configuring settings for SNMP</li> <li>▪ Configuring settings for e-mail notification</li> <li>▪ Configuring settings for license keys</li> </ul>

Role	Permissions
	<ul style="list-style-type: none"> <li>▪ Viewing, deleting, and downloading storage configuration reports</li> <li>▪ Acquiring all the information about the storage system and updating Device Manager - Storage Navigator window by clicking Refresh All</li> </ul>
Storage Administrator (System Resource Management)	<ul style="list-style-type: none"> <li>▪ Configuring settings for CLPR</li> <li>▪ Configuring settings for MP Blade</li> <li>▪ Deleting tasks and releasing exclusive locks of resources</li> <li>▪ Completing SIMs</li> <li>▪ Configuring attributes for ports</li> <li>▪ Configuring LUN security</li> <li>▪ Configuring Server Priority Manager</li> <li>▪ Configuring tiering policies</li> </ul>
Storage Administrator (Provisioning)	<ul style="list-style-type: none"> <li>▪ Configuring caches</li> <li>▪ Configuring LDEVs, pools, and virtual volumes</li> <li>▪ Formatting and shredding LDEVs</li> <li>▪ Configuring external volumes</li> <li>▪ Configuring alias volumes for Compatible PAV</li> <li>▪ Configuring Dynamic Provisioning</li> <li>▪ Configuring host groups, paths, and WWN</li> <li>▪ Configuring Volume Migration except splitting Volume Migration pairs when using CCI</li> <li>▪ Configuring access attributes for LDEVs</li> <li>▪ Configuring LUN security</li> <li>▪ Creating and deleting quorum disk used with global-active device</li> <li>▪ Creating and deleting global-active device pairs</li> </ul>
Storage Administrator (Performance Management)	<ul style="list-style-type: none"> <li>▪ Configuring monitoring</li> <li>▪ Starting and stopping monitoring</li> </ul>
Storage Administrator (Local Copy)	<ul style="list-style-type: none"> <li>▪ Performing pair operations for local copy</li> <li>▪ Configuring environmental settings for local copy</li> <li>▪ Splitting Volume Migration V2 pairs when using CCI</li> </ul>
Storage Administrator (Remote Copy)	<ul style="list-style-type: none"> <li>▪ Remote copy operations in general</li> <li>▪ Operating global-active device pairs (except for creation and deletion)</li> </ul>

Role	Permissions
Support Personnel (View & Modify)	Configuring the SVP <ul style="list-style-type: none"> <li>▪ Normally, this role is for service representatives.</li> <li>▪ Downloading dump files using the Dump tool</li> </ul>



**Note:** Normally, the Support Personnel role is reserved for service representatives, but if the role is assigned to a user account, dump files can be downloaded using the Dump tool.

## Built-in user groups

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

The following table shows all the built-in groups, and their built-in roles and resource groups.

Built-in group	Role	Resource group
Administrator	<ul style="list-style-type: none"> <li>▪ Security Administrator (View &amp; Modify)</li> <li>▪ Audit Log Administrator (View &amp; Modify)</li> <li>▪ Storage administrator (Initial Configuration)</li> <li>▪ Storage Administrator (System Resource Management)</li> <li>▪ Storage Administrator (Provisioning)</li> <li>▪ Storage Administrator (Performance Management)</li> <li>▪ Storage Administrator (Local Copy)</li> <li>▪ Storage Administrator (Remote Copy)</li> </ul>	All Resource Groups Assigned
System	<ul style="list-style-type: none"> <li>▪ Security Administrator (View &amp; Modify)</li> <li>▪ Audit Log Administrator (View &amp; Modify)</li> </ul>	All Resource Groups Assigned

Built-in group	Role	Resource group
	<ul style="list-style-type: none"> <li>▪ Storage Administrator (Initial Configuration)</li> <li>▪ Storage Administrator (System Resource Management)</li> <li>▪ Storage Administrator (Provisioning)</li> <li>▪ Storage Administrator (Performance Management)</li> <li>▪ Storage Administrator (Local Copy)</li> <li>▪ Storage Administrator (Remote Copy)</li> </ul>	
Security Administrator (View Only)	<ul style="list-style-type: none"> <li>▪ Security Administrator (View Only)</li> <li>▪ Audit Log Administrator (View Only)</li> <li>▪ Storage Administrator (View Only)</li> </ul>	All Resource Groups Assigned
Security Administrator (View & Modify)	<ul style="list-style-type: none"> <li>▪ Security Administrator (View &amp; Modify)</li> <li>▪ Audit Log Administrator (View &amp; Modify)</li> <li>▪ Storage Administrator (View Only)</li> </ul>	All Resource Groups Assigned
Audit Log Administrator (View Only)	<ul style="list-style-type: none"> <li>▪ Audit Log Administrator (View Only)</li> <li>▪ Storage Administrator (View Only)</li> </ul>	All Resource Groups Assigned
Audit Log Administrator (View & Modify)	<ul style="list-style-type: none"> <li>▪ Audit Log Administrator (View &amp; Modify)</li> <li>▪ Storage Administrator (View Only)</li> </ul>	All Resource Groups Assigned
Storage Administrator (View Only)	<ul style="list-style-type: none"> <li>▪ Storage Administrator (View Only)</li> </ul>	meta_resource
Storage Administrator (View & Modify)	<ul style="list-style-type: none"> <li>▪ Storage Administrator (Initial Configuration)</li> <li>▪ Storage Administrator (System Resource Management)</li> <li>▪ Storage Administrator (Provisioning)</li> <li>▪ Storage Administrator (Performance Management)</li> </ul>	meta_resource

Built-in group	Role	Resource group
	<ul style="list-style-type: none"> <li>▪ Storage Administrator (Local Copy)</li> <li>▪ Storage Administrator (Remote Copy)</li> </ul>	
Support Personnel	<ul style="list-style-type: none"> <li>▪ Storage Administrator (Initial Configuration)</li> <li>▪ Storage Administrator (System Resource Management)</li> <li>▪ Storage Administrator (Provisioning)</li> <li>▪ Storage Administrator (Performance Management)</li> <li>▪ Storage Administrator (Local Copy)</li> <li>▪ Storage Administrator (Remote Copy)</li> <li>▪ Support Personnel</li> </ul>	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**.

## 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.

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 256 user groups, including the 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**.

## User accounts

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

For more information about roles, permissions, and user groups, see [Roles and permissions \(on page 105\)](#).

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 512 user accounts, including the built-in user accounts.

### 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.
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.
7. To use an authentication server, select **External**. To authenticate users with only Device Manager - Storage Navigator, select **Local**.
8. If you select **Local**, enter the password for this user account in two places. 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

The user account you created for Device Manager - Storage Navigator can also be used for SVP, CCI, and the raidinf command. Note that the Support Personnel (View & Modify) role is required to log in to SVP.

The number of characters and characters you can use for the user name and password are determined by the software you will log in. You can log in to one or more of Device Manager - Storage Navigator, SVP, CCI, and the raidinf command. If you log in to multiple programs, specify the user name and the password that satisfy the user name and password requirements (listed below) for the applicable software applications.

Note the following restrictions for user names and passwords.

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

Item	Length in characters	Characters that can be used
User name	1-256	<ul style="list-style-type: none"> <li>▪ Alphanumeric (ASCII code) characters</li> <li>▪ The following symbols: # \$ % &amp; ' * + - . / = ? @ ^ _ ` {   } ~</li> </ul> <p>You cannot use the # symbol when you enter a user name in a screen from the <b>Tool Panel</b> dialog box.</p>
Password	6-256	<ul style="list-style-type: none"> <li>▪ Alphanumeric (ASCII code) characters</li> <li>▪ All symbols</li> </ul> <p>You cannot use the quotation mark (") or backslash (\) symbols when you enter a password in a screen from the <b>Tool Panel</b> dialog box.</p>



**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	<ul style="list-style-type: none"> <li>▪ Alphanumeric (ASCII code) characters</li> <li>▪ The following symbols: ! # \$ % &amp; ' - . @ ^ _ ` { } ~</li> </ul>
Password	6- 127	<ul style="list-style-type: none"> <li>▪ Alphanumeric (ASCII code) characters</li> <li>▪ All symbols</li> </ul>

**User name and password for logging in to CCI or the raidinf command**

Item	Length in characters	Characters that can be used
User name	1-63	<ul style="list-style-type: none"> <li>▪ Alphanumeric (ASCII code) characters</li> <li>▪ The following symbols<sup>1</sup>: - . @ _</li> </ul>

Item	Length in characters	Characters that can be used
Password	6- 63	<ul style="list-style-type: none"> <li>▪ Alphanumeric (ASCII code) characters</li> <li>▪ The following symbols<sup>1, 2</sup>: - , . : @ _</li> </ul>
<p><b>Note:</b></p> <ol style="list-style-type: none"> <li>1. If the host on which CCI is installed is running on UNIX, a slash (/) can be specified.</li> <li>2. If the host on which CCI is installed is running on Windows, a back slash (\) can be specified.</li> </ol>		

## 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.

### 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 group can contain a maximum of 512 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 and disabling user accounts

To allow or prevent a user from logging in to Device Manager - Storage Navigator, follow the steps below.

**Before you begin**

- Log into an account that is different from the user whose account that you want to disable.
- You must have the Security Administrator (View & Modify) role to perform this task.

**Procedure**

1. In the Device Manager - Storage Navigator **Administration** tree, click **User Groups**.
2. On the **User Group** tab, select the user group.
3. On the **Users** tab, select a user.
4. Click **Edit User**.
5. Click the **Account Status** check box, then 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.

**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.

**Managing resource groups**

You can divide a provisioned storage system into resource groups that allow you to manage the storage system as multiple virtual private storage systems. Configuring resource groups involves creating resource groups, moving storage system resources into the resource groups, and assigning resource groups to user groups.

## About resource groups

A storage system can connect to multiple hosts and be shared by multiple divisions in a company or by multiple companies. Many storage administrators from different organizations can access the storage system. Managing the entire storage system can become complex and difficult. Potential problems are that private data might be accessed by other users, or a volume in one organization might be accidentally destroyed by a storage administrator in another organization.

To avoid such problems, use Hitachi Resource Partition Manager software to set up resource groups that allow you to manage one storage system as multiple virtual private storage systems. The storage administrator in each resource group can access only their assigned resources. Resource groups prevent the risk of data leakage or data destruction by another storage administrator in another resource group.

The following resources can be assigned to resource groups.

- LDEV IDs
- Parity groups
- External volumes
- Ports
- Host group IDs
- iSCSI target IDs



### Note:

Before you create LDEVs, you can reserve the desired number of LDEV IDs and assign them to a resource group for future use. You can also reserve and assign host group IDs and iSCSI target IDs in advance because the number of host groups or iSCSI targets per port is limited.

### meta\_resource

The meta\_resource group is the resource group consisting of the resources that exist on the storage system (other than external volumes) before Resource Partition Manager is installed. By default, all existing resources initially belong to the meta\_resource group to ensure compatibility with older software when a system is upgraded to include Resource Partition Manager.

### Resource lock

When a task is being processed on a resource, all of the resource groups assigned to the logged-on user are locked for exclusive access. When a resource is locked, a status indicator appears on the Device Manager - Storage Navigator status bar. To view information about the locked resource, click Resource Locked.



**Note:** Opening a Device Manager - Storage Navigator secondary window (such as **Basic Information Display**) or performing an operation from the service processor (SVP) locks all of the resource groups in the storage system.



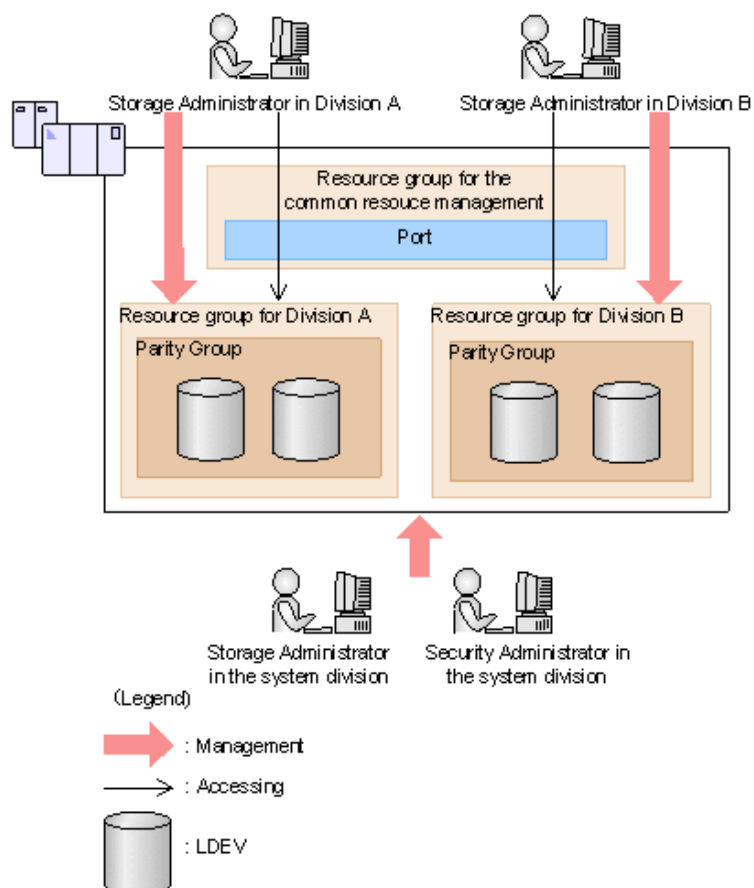
## Examples

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

### Resource groups sharing a port

If you have a limited number of ports, you can still operate a storage system effectively by sharing ports using resource groups.

The following example shows the system configuration of an in-house division providing virtual private storage system for two divisions. Divisions A and B each use their own assigned parity group, but share a port between the two divisions. The shared port is managed by the system division.



The Security Administrator in the system division creates resource groups for each division in the storage system and assigns them to the respective divisions. The Storage Administrator in Division A can manage the resource groups for Division A but cannot access the resource groups for Division B. In the same manner, the Storage Administrator in Division B can manage the resource groups for Division B but cannot access the resource groups for Division A.

The Security Administrator creates a resource group for managing the common resources, and the Storage Administrator in the system division manages the port that is shared between Divisions A and B. The Storage Administrators in Divisions A and B cannot manage the shared port belonging to the resource group for common resources management.

#### **Configuration workflow for resource groups sharing a port**

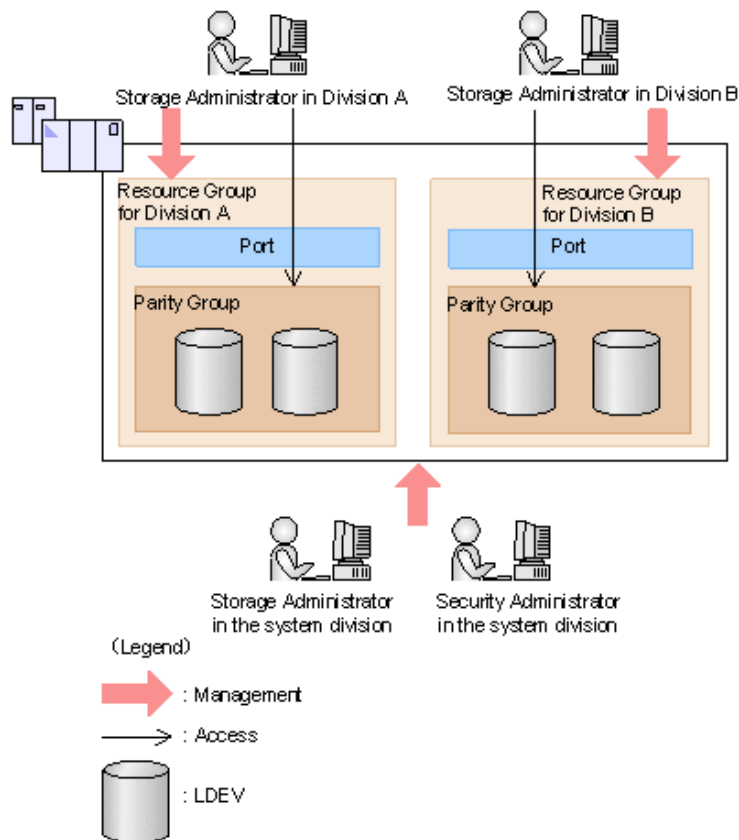
1. The system division forms a plan about the resource group creation and assignment of the resources.
2. The Security Administrator creates the resource groups.
3. The Security Administrator creates the user groups.
4. The Security Administrator assigns the resource groups to the user groups.
5. The Storage Administrator in the system division sets a port.
6. The Security Administrator assigns resources to the resource groups.
7. The Security Administrator assigns the Storage Administrators to the appropriate user groups.

After the above procedures, the Storage Administrators in Divisions A and B can manage the resource groups assigned to their own division.

#### **Resource groups not sharing ports**

If you assign ports to each resource group without sharing, performance can be maintained on a different port even if the bulk of I/O is issued from one side port.

The following shows a system configuration example of an in-house system division providing the virtual private storage system for two divisions. Divisions A and B each use individual assigned ports and parity groups. In this example, they do not share a port.



The Security Administrator in the system division creates resource groups for each division in the storage system and assigns them to the respective divisions. The Storage Administrator in Division A can manage the resource groups for Division A but cannot access the resource groups for Division B. In the same manner, the Storage Administrator in Division B can manage the resource groups for Division B but cannot access the resource groups for Division A.

### Configuration workflow for resource groups not sharing a port

1. The system division forms a plan about creating resource groups and the assigning resources to the groups.
2. The Security Administrator creates the resource groups.
3. The Security Administrator creates the user groups.
4. The Security Administrator assigns the resource groups to user groups.
5. The Storage Administrator in the system division sets ports.
6. The Security Administrator assigns resources to the resource groups.
7. The Security Administrator assigns each Storage Administrator to each user group.

After the above procedures, the Storage Administrators in Divisions A and B can access the resource groups allocated to their own division.

## Resource group assignments

All resource groups are normally assigned to the Security Administrator and the Audit Log Administrator.

Each resource group has a designated Storage Administrator who can access only their assigned resources and cannot access other resources.

All resource groups to which all resources in the storage system belong can be assigned to a user group. Configure this in Device Manager - Storage Navigator by setting All Resource Groups Assigned to Yes.

A user who has All Resource Groups Assigned set to Yes can access all resources in the storage system. For example, if a user is a Security Administrator (with View & Modify privileges) and a Storage Administrator (with View and Modify privileges) and All Resource Groups Assigned is Yes on that user account, the user can edit the storage for all the resources.

If allowing this access becomes a problem with security on the storage system, then register the following two user accounts and use these different accounts for different purposes.

- A user account for a Security Administrator where All Resource Groups Assigned is set to Yes.
- A user account for a Storage Administrator who does not have all resource groups assigned and has only some of the resource groups assigned.

## Resource group rules, restrictions, and guidelines

### Rules

- The maximum number of resource groups that can be created on a storage system is 1023.

If you are providing a virtual private storage system to different companies, you should not share parity groups, external volumes, or pools if you want to limit the capacity that can be used by each user. When parity groups, external volumes, or pools are shared between multiple users, and if one user uses too much capacity of the shared resource, the other users might not be able to create an LDEV.

## Creating resource groups

When you create a resource group, you enter a name and assign the desired resources (parity groups, LDEVs, ports, host groups, and iSCSI targets) to the new group. You can create more than one resource group at a time.

### Before you begin

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

## Procedure

1. In the **Explorer** pane, expand the **Storage Systems** tree, click the **Administration** tab, and then select **Resource Groups**.
2. 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.

Naming guidelines:

- A resource group name can use alphanumeric characters, spaces, and the following symbols: ! # \$ % & ' ( ) + - . = @ [ ] ^ \_ ` { } ~
  - The characters in a resource group name are case-sensitive.
  - Duplicate occurrences of the same name are not allowed.
  - You cannot use the following names: `meta_resource`
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**.



**Note:** The maximum number of resource groups that can be created on a storage system is 1023.

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.

## Adding resources to a resource group

You can add resources to, remove resources from, and rename existing resource groups.

Note the following restrictions for editing resource groups:

- Only resources allocated to `meta_resource` can be added to resource groups.
- Resources removed from a resource group are returned to `meta_resource`.
- No resource can be added to or removed from `meta_resource`.
- The name of the `meta_resource` group cannot be changed or used for any resource group other than the `meta_resource` group.
- The system does not allow duplicate names.

- LDEVs with the same pool ID or journal ID cannot be added to multiple resource groups or partially removed from a resource group. For example, if two LDEVs belong to the same pool, you must allocate both to the same resource group. You cannot allocate them separately.

You cannot partially remove LDEVs with the same pool ID or journal ID from a resource group. If LDEV1 and LDEV2 belong to the same pool, you cannot remove LDEV1 and leave only LDEV2 in the resource group.

Use the sort function to sort the LDEVs by pool ID or journal ID. Then select the IDs and add or remove them all at once.

- Host groups that belong to the initiator port cannot be added to a resource group.
- To add or delete DP pool volumes, you must first add or delete DP pools.

### Before you begin

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

### Procedure

1. In the **Explorer** pane, click the **Administration** tab, and then select **Resource Groups**.
2. Select the desired resource group (check the box next to the name of the resource group) to display the resource information for the resource group.
  - To change the name of the selected resource group, click **Edit Resource Group**, and enter the new name.
  - To add resources to the selected resource group, select the **Parity Groups, LDEVs, Ports, or Host Groups / iSCSI Targets** tab, click **Add Resources**, and follow the instructions on the **Add Resources** window.
  - To remove resources from the selected resource group, select the **Parity Groups, LDEVs, Ports, or Host Groups / iSCSI Targets** tab, select the resources to be removed, and then click **Remove Resources**.
3. Enter a task name or accept the default, and then click **Submit**.  
If you select **View task status**, the **Tasks & Alerts** tab opens.

## Deleting resource groups

You can delete a resource group only when the resource group does not contain any resources and is not assigned to any user groups.

The following resource groups cannot be deleted:

- `meta_resource`
- A resource group that is assigned to a user group
- A resource group that has resources assigned to it
- Resource groups included in different resource groups cannot be removed at the same time.

### Before you begin

The Security Administrator (View & Modify) role is required to perform this task.

### Procedure

1. In the **Explorer** pane, expand the **Storage Systems** tree, click the **Administration** tab, select **Resource Groups**.
2. Click the check box of a **Resource Group Name**.
3. Click **Delete Resource Groups**.
4. Enter a task name or accept the default, and then click **Submit**.  
If you select **View task status**, the **Tasks & Alerts** tab opens.

## Account lock policy

A user account is automatically locked after three unsuccessful logins to Device Manager - Storage Navigator or Command Control Interface. The account is locked for 60 seconds.

## Unlock a user account

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**.

---

## Chapter 5: Managing license keys

Accessing software functionality for your storage system requires a license key.

### License keys overview

When you install a license key, it is also enabled. The functionality for the software that you installed is available in Device Manager - Storage Navigator.

The license key can be disabled. This allows you to conserve time on a term key, for example. If you have a 365-day term key for a software product, the license server starts the count the day you install the key. However, you may not use the license immediately, in which case you can disable the key. Disabling stops the count. You re-enable the key when you become ready to use it.

This topic provides information in the order it is required:

- [License key types \(on page 128\)](#). Lists the key types; explains whether keys are permanent or temporary; shows the term limit, if any; and provides the estimated license capacity, if required.
- [Using the term key \(on page 130\)](#). Explains that you can conserve the term key when you are not using it.
- [Using the temporary key \(on page 130\)](#). Explains that you can conserve the temporary key when you are not using it.
- [Estimating licensed capacity \(on page 131\)](#). Provides information and instructions for calculating license capacity according to your system and organization requirements.
- [Installing and uninstalling software \(on page 137\)](#). Provides instructions for installing, disabling, enabling, and removing keys.
- [License key expiration \(on page 142\)](#) provide information for dealing with these situations.

### 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 7ff7xx) 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 <sup>1</sup>	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
<b>Notes:</b>			
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.

## 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:

**Table 1 Licensed capacity types**

Type	Description
Used capacity	<p>The licensed capacity is calculated by using one of the following capacities:</p> <ul style="list-style-type: none"> <li>▪ Normal volumes (volumes)</li> <li>▪ External volumes mapped to the storage system</li> <li>▪ Pools</li> </ul> <p>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.</p>
Mounted capacity/ usable capacity	<p>The licensed capacity is estimated by using the capacity of all the volumes in the storage system.</p> <p>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.</p>
Unlimited capacity	You can use the software regardless of the volume capacity.

The following table lists the software and the licensed capacity.

Option name	Licensed capacity	Notes
HDvM/Device Manager - Storage Navigator	Mounted capacity	
SNMP Agent	Mounted capacity	
JAVA API	Mounted capacity	
SMI-S Provider	Mounted capacity	
LUN Manager	Mounted capacity	Used only for open-system devices (including LUN security).
Virtual LVI	Mounted capacity	
Open Volume Management	Mounted capacity	Used only for open-systems devices
Volume Shredder	Mounted capacity	
Cache Residency Manager	Mounted capacity	
Cache Residency Manager for Mainframe	Mounted capacity	
Performance Monitor	Mounted capacity	
Server Priority Manager	Mounted capacity	To use Server Priority Manager, first install Performance Monitor.
Volume Migration	Mounted capacity	To use Volume Migration, first install Performance Monitor.  For information about Volume Migration, contact the customer support.
Volume Migration V2	Mounted capacity	For information about Volume Migration V2, contact the customer support.
TrueCopy	Used capacity for normal volumes <sup>1</sup>	Default state <sup>1</sup>

Option name	Licensed capacity	Notes
TrueCopy for Mainframe	Used capacity for normal volumes <sup>1</sup>	
Universal Replicator	Used capacity for normal volumes <sup>1</sup>	To use Universal Replicator, first install TrueCopy.
Universal Replicator for Mainframe	Used capacity for normal volumes <sup>1</sup>	To use Universal Replicator for Mainframe, first install TrueCopy for Mainframe.
Disaster Recovery Extended	Unlimited	To use Disaster Recovery Extended, first install Universal Replicator or Universal Replicator for Mainframe. See the prerequisites for these in the two rows directly above this one.
ShadowImage	Used capacity for normal volumes <sup>1</sup>	
ShadowImage for Mainframe	Used capacity for normal volumes <sup>1</sup>	
Compatible FlashCopy <sup>®</sup> V2	Used capacity for normal volumes <sup>1</sup>	
Hitachi Compatible FlashCopy <sup>®</sup>	Used capacity for normal volumes <sup>1</sup>	
Thin Image	Used capacity for normal volumes <sup>1</sup> + total pool capacity	To use Thin Image, first install Dynamic Provisioning.
Dynamic Provisioning	Used capacity (Total pool capacity)	
Dynamic Provisioning for Mainframe	Used capacity (Total pool capacity)	To use Dynamic Provisioning for Mainframe, first install Dynamic Provisioning.

Option name	Licensed capacity	Notes
Dynamic Tiering	Used capacity (Total pool capacity)	To use Dynamic Tiering, first install Dynamic Provisioning.
Dynamic Tiering for Mainframe	Used capacity (Total pool capacity)	To use Dynamic Tiering for Mainframe, first install Dynamic Provisioning for Mainframe and Dynamic Tiering.
Active flash	Used capacity (Total pool capacity)	To use active flash, first install Dynamic Tiering.
Active flash for mainframe	Used capacity (Total pool capacity)	To use active flash for mainframe, first install active flash and Dynamic Tiering for Mainframe.
Compatible PAV	Used capacity for normal volumes	
Compatible Hyper PAV	Unlimited	To use Compatible Hyper PAV, first install Compatible PAV.
Compatible XRC	Used capacity for normal volumes	For controller emulation type I-2107 only.
FICON® Data Migration	Used capacity for external volumes	
High Performance Connectivity for FICON®	Unlimited	
Data Retention Utility	Mounted capacity	
Volume Retention Manager	Mounted volumes	
Universal Volume Manager	Used capacity for external volumes	
Virtual Partition Manager	Unlimited	You may use up to four CLPRs without the Virtual Partition Manager license key. With a license key, you can define up to 32 CLPRs.
Resource Partition Manager	Unlimited	

Option name	Licensed capacity	Notes
Nondisruptive migration	Used capacity for external volumes.	
Encryption License Key	Unlimited	
FMD Encryption License Key	Unlimited	
Global-active device	Used capacity for normal volumes <sup>1</sup>	
High temperature mode	Unlimited	
FIPS140-2 Level2	Unlimited	To use, first install Encryption License Key.
VSP F1500 All Flash Array	Unlimited	A license key which is required for VSP F1500.
Dedupe and compression	Unlimited	A license which is required to use the capacity saving function. To use the capacity saving function, you need to install Dynamic Provisioning.
VSP G1500 and F1500 VSD	Unlimited	A license which is required to upgrade from VSP G1000 to VSP G1500. To upgrade to VSP G1500, change the MP blade type from MPB1 to MPB2 before installing this license.
<p><b>Notes:</b></p> <p>1. If you use V-VOLs of Dynamic Provisioning, Dynamic Provisioning for Mainframe, Dynamic Tiering, or Dynamic Tiering for Mainframe as P-VOLs or S-VOLs of the following software applications, the license capacity is calculated using the page capacity allocated to the V-VOLs (that is, used pool capacity).</p> <ul style="list-style-type: none"> <li>▪ ShadowImage</li> <li>▪ Thin Image</li> <li>▪ TrueCopy</li> <li>▪ Universal Replicator</li> <li>▪ ShadowImage for Mainframe</li> <li>▪ TrueCopy for Mainframe</li> <li>▪ Universal Replicator for Mainframe</li> </ul>		

Option name	Licensed capacity	Notes
<ul style="list-style-type: none"> <li>▪ Compatible FlashCopy®</li> <li>▪ Global-active device</li> </ul>		

## 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. For OPEN-V volumes, the licensed capacity of a volume is the same as the capacity specified when creating the volume.

**Table 2 Formulas for calculating capacity of a normal volume**

Volume emulation type	Formula for calculating capacity of a normal volume
3390-x <sup>1</sup>	870 KB × <i>number-of-user-cylinders</i>
OPEN-x <sup>1</sup>	Same as the capacity specified when creating the volume
<b>Notes:</b>	
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 3 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	$870 \text{ KB} \times 3,339 \times 2,048 = 5,949,296,640 \text{ KB}$ $5,949,296,640 \text{ KB} / 1,024 = 5,809,860 \text{ MB}$ $5,809,860 \text{ MB} / 1,024 \doteq 5,673.70 \text{ GB}$ $5,673.70 \text{ GB} / 1,024 \doteq 5.55 \text{ TB}$
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:

$$\text{External Volume Capacity (KB)} = \text{Volume Capacity (number of blocks)} \times \frac{512 \text{ (bytes)}}{1,024}$$

## 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 for Open Systems* and the *Provisioning Guide for Mainframe Systems*.

## 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

## Installing and uninstalling software

This section provides instructions for installing and uninstalling software.

### Installing license keys using Device Manager - Storage Navigator

Use license keys to install software.

#### Before you begin

- You must have the Storage Administrator (Initial Configuration) role to perform this task.
- You must install a license key for each software application before you use it.

## Procedure

1. From the **Administration** tree, click **License Keys**.
2. In the **License Keys** window, click **Install Licenses**.
3. 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 several symbols (" \ ; : \* ? < > | / ,). The file extension is "plk".
4. Click **Add**.
5. In the **Selected License Keys** table, set the status of license keys for each software application.
  - **Enable Licenses:** Installs license keys in enabled status. You can select more than one software application to install licenses for.
  - **Disable Licenses:** Installs license keys in disabled status. You can select more than one software application to install licenses for.
  - **Clear All:** Delete all license keys from the Selected License Keys table.
6. Click **Finish**. The **Confirm** window opens.
7. In the **Confirm** window, check the settings. In the **Task Name** field, enter a task name.
8. Click **Apply**. The task is registered. If the **Go to tasks window for status** check box is checked, the **Task** window opens.

If a software installation fails, the **Error Message** window opens. To display the cause of error, from the **Error Message** window, select the software and click **Detail**.

## When the status is Installed (Disabled)

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.

## 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 **Administration** tree, click **License Keys**.

2. In the **License Keys** window, select one or more licenses to enable, and then click **Enable Licenses**.
3. Check the settings, and then 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 **Administration** tree, click **License Keys**.
2. In the **License Keys** window, select one or more licenses to disable, and then click **Disable Licenses**.
3. Check the settings, and then click **Apply**.

## Removing a software application

Remove software from the storage system by uninstalling license keys.

### Before you begin

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

### Procedure

1. From the **Administration** tree, click **License Keys**.
2. In the **License Keys** window, select one or more licenses to uninstall.



#### Note:

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

3. Click **Remove** to display the **Remove Licenses** window.
4. Check the settings, and then click **Apply**.



#### Note:

To reinstall a license key after uninstalling it, contact customer support to reissue the license key file.

## Updating license status

In the following cases, the status of software might remain at Not Enough License or Grace Period. In that case, update the license status.

- When the licensed capacity exceeds the mounted capacity after you reduce the number of LDEVs
- When the licensed capacity exceeds the used capacity after you delete pairs or pool volumes

### Before you begin

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

### Procedure

1. From the **Administration** tree, click **License Keys**.
2. In the **License Keys** window, click **Update License Status**.
3. Check the settings, and then click **Apply**

## Examples of license information

The following table provides examples of license information displayed in the **License Key** window.

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

## 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<sup>®</sup>, 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.

## Cautions on licenses

Observe the following precautions when working with licenses:

 **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 for Open Systems*.

 **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.

## Resolving errors when removing Data Retention Utility

If a Data Retention Utility error occurs during removal, you must resolve it before continuing removal.

For details about the **Data Retention** window, see the *Provisioning Guide for Open Systems*.

### 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 (secondary volumes).
3. Change the settings so that the logical volumes are usable as S-VOLs.
4. Uninstall Data Retention Utility.

## 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 6: Viewing and managing the storage system

Use Device Manager - Storage Navigator to view storage system information, manage system configuration reports, and manage queued operations.

This section describes how to navigate to your storage system information, create and download system configuration reports, and manage Device Manager - Storage Navigator tasks.

### Viewing storage system information

Use Device Manager - Storage Navigator to view high-level information, create reports, and manage tasks.

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

### Viewing basic information

The main window shows basic information about the storage system.

The screenshot displays the Hitachi Device Manager Storage Navigator interface. The main window shows the following information:

**Storage(S/N:176)**

Edit Storage System			
Storage System Name	Storage	Microcode Version	Main
Storage System Type	VSP G1000		SVP
Serial Number	176		RMI Server
IP Address	158.214.121.118	Total Cache Size	
Contact			
Location			

**Allocation Summary**

Internal/External :	Total	Open/Mainframe:	Total	Capacity Unit:	Appropriate	Number of
<b>Physical Summary</b>						
				Physical Capacity		Number of
				Allocated	1.27 TB	[7%]
				Reserved	2.13 GB	[1%]
				Used DP Pool	121.73 GB	[1%]
				Unused DP Pool	4.13 GB	[1%]
				Other	0.00 MB	[0%]
				Available Space	14.26 TB	[90%]
				Unallocated	15.66 TB	
				Free Space		
				Physical Total		
<b>Virtual Summary</b>						
				Virtual Capacity		Number of
				DP Allocated	0.00 MB	
				DP Unallocated	64.00 GB	
				Other	0.00 MB	
				Virtual Total	64.00 GB	

Total DP Subscription Rate: 51% Total Number of LD



## Viewing specific information

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

The screenshot shows the Hitachi Device Manager Storage Navigator interface. The left pane (Explorer) shows a tree view with 'Ports/Host Groups' selected. The main pane displays the 'Ports/Host Groups' view for 'Storage(S/N:30174)'. It includes a summary table for 'Number of Ports' and a detailed table of host groups.

Number of Ports	Target	16
RCU Target	0	
Total	16	

Port ID	Host Group Name	Host Mode	Port Security	Number of Hosts	Number of LUNs	Res Nar
<input type="checkbox"/> CL1-C	1C-G00	00[Standard]	Disabled...	0	0	me
<input type="checkbox"/> CL3-C	3C-G00	00[Standard]	Disabled...	0	0	me
<input type="checkbox"/> CL5-C	5C-G00	00[Standard]	Disabled...	0	0	me
<input type="checkbox"/> CL7-C	7C-G00	00[Standard]	Disabled...	0	0	me
<input type="checkbox"/> CL1-D	1D-G00	00[Standard]	Disabled...	0	0	me
<input type="checkbox"/> CL3-D	3D-G00	00[Standard]	Disabled...	0	0	me
<input type="checkbox"/> CL5-D	5D-G00	00[Standard]	Disabled...	0	0	me
<input type="checkbox"/> CL7-D	7D-G00	00[Standard]	Disabled...	0	0	me
<input type="checkbox"/> CL2-C	2C-G00	00[Standard]	Disabled...	0	0	me
<input type="checkbox"/> CL4-C	4C-G00	00[Standard]	Disabled...	0	0	me
<input type="checkbox"/> CL6-C	6C-G00	00[Standard]	Disabled...	0	0	me
<input type="checkbox"/> CL8-C	8C-G00	00[Standard]	Disabled...	0	0	me
<input type="checkbox"/> CL2-D	2D-G00	00[Standard]	Disabled...	0	0	me
<input type="checkbox"/> CL4-D	4D-G00	00[Standard]	Disabled...	0	0	me
<input type="checkbox"/> CL6-D	6D-G00	00[Standard]	Disabled...	0	0	me
<input type="checkbox"/> CL8-D	8D-G00	00[Standard]	Disabled...	0	0	me

## Viewing other system information

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

### Procedure

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

## Viewing port conditions

You can view port conditions by clicking Actions > Component > View Port conditions.

The screenshot shows a 'Port Condition' window for DKC0. It features a 'Refresh' button and a summary table of port counts:

Number of Ports	Condition	Count
	Available (Connected)	14
	Available (Not Connected)	13
	Not Available	13
	Not Installed	

Below the summary is a graphical representation of port status for various adapters (1PB, 1PC, 1PE, 2PE, 2PC, 2PB). Each port is shown with a status icon (green for available, grey for not available) and a label (e.g., 9C, 1A, 1E, etc.).

At the bottom is a detailed table:



Channel Adapter	Adapter Type	Port ID	Attribute	Condition	Speed
CHA-1PC	8FC16 (Fibre)	CL1-A	External	Not Available	Auto(-)
CHA-1PC	8FC16 (Fibre)	CL3-A	Initiator	Available (Not Connected)	Auto(-)
CHA-1PC	8FC16 (Fibre)	CL1-B	Target	Available (Not Connected)	Auto(-)
CHA-1PC	8FC16 (Fibre)	CL3-B	Target	Available (Connected)	Auto(-)
CHA-1PE	16FC8 (Fibre)	CL1-E	Target	Available (Connected)	Auto(-)
CHA-1PE	16FC8 (Fibre)	CL3-E	Initiator	Not Available	Auto(-)
CHA-1PE	16FC8 (Fibre)	CL5-E	Target	Available (Not Connected)	Auto(-)
CHA-1PE	16FC8 (Fibre)	CL7-E	Target	Available (Connected)	Auto(-)
CHA-1PE	16FC8 (Fibre)	CL1-F	Target	Not Available	Auto(-)
CHA-1PE	16FC8 (Fibre)	CL3-F	External	Available (Not Connected)	Auto(-)
CHA-1PE	16FC8 (Fibre)	CL5-F	Target	Available (Connected)	Auto(-)

The table includes a 'Filter' toggle (ON/OFF), an 'Export' button, and a 'Total: 40' indicator. A 'Close' button is at the bottom right.

## Status icons for certain resources

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

Status	Description
	The resource can be used normally.

Status	Description
	<p>The resource has the following status:</p> <ul style="list-style-type: none"> <li>▪ The resource can be used, but has a limit on I/O performance and so on.</li> <li>▪ The status of the resource is changing.</li> <li>▪ The status of the resource is being confirmed.</li> <li>▪ The resource has subresources of different status.</li> </ul> <p>For example, parity groups are in this status if the statuses of logical volumes in the parity groups are not the same.</p> <p>In this case, the subresources might be blocked. Confirm the status of subresources.</p>
	<p>The resource has the following status:</p> <ul style="list-style-type: none"> <li>▪ The resource cannot be used because it is blocked due to a failure or maintenance operations.</li> <li>▪ The status of the resource is unknown.</li> </ul> <p>Restore the resource to the normal status.</p>

## Using the storage system in high temperature mode

High temperature mode is a licensed feature that allows the storage system to be run at either standard temperature (60.8°F to 89.6°F / 16°C to 32°C) or at higher temperatures (60.8°F to 104°F / 16°C to 40°C) in a data center, saving energy and cooling costs.

### Normal and high temperature alerts

When high temperature mode is disabled, a SIM displays when the temperature in the storage system exceeds 89.6°F / 32°C.

When high temperature mode is enabled, a SIM displays when the temperature in the storage system exceeds 104°F / 40°C.



**Caution:** Important information about using high temperature mode. See the *Hardware Guide for Hitachi Virtual Storage Platform G1000, G1500, and F1500* for additional information.

- Notify Technical Support. Before enabling high temperature mode, call the customer support. They may have updates or additional information besides the following notes.
- Operating with FMDs. Do not enable high temperature mode if the system contains FMDs. FMDs can be used only in the standard temperature environment.
- Operating Altitude. The lifetime of a storage system that is operated in standard temperature mode is six years. The lifetime of a storage system that is operated in high temperature mode is five years.
- Cache Flash Memory battery life. When high temperature mode is enabled, the cache flash memory battery life will be reduced to two-thirds of the battery life that remains at the time when high temperature mode is enabled.

Example 1: A new cache flash memory battery has three years of usable life when operated in a standard temperature environment. If you enable high temperature mode when the battery is new, the battery life will be reduced to two years.

Example 2: The storage system is used for two years at normal temperature mode. The cache battery has one year of usable life remaining at that time. If you enable high temperature mode, the life of the battery will be reduced to eight months.

- Cache Flash Memory battery date. When high temperature mode is enabled, the battery replacement notice displays one year earlier than when high temperature mode is disabled.

After high temperature mode is enabled, the date of the battery replacement notice cannot be changed back to normal, even if high temperature mode is disabled. When high temperature mode is enabled, a confirmation message is displayed.

- System noise. When the storage system is used in a high temperature environment near 104°F / 40°C, the fans operate at high speed, increasing noise. See Appendix A, Specifications, in the *Hardware Guide for Hitachi Virtual Storage Platform G1000, G1500, and F1500* for information about system noise levels.

## Enabling high temperature mode

### Before you begin

- You must have the Storage Administrator (Initial Configuration) role to perform this task.
- The license for this feature must be installed before using it.
- For details about the **Components** window, see the *Provisioning Guide for Open Systems* and the *Provisioning Guide for Mainframe Systems*.

### Procedure

1. In the **Storage Systems** tree, select the **Components** tab.
2. In the **Components** tab, click **Edit High Temperature Mode**. The **Edit High Temperature Mode** window opens.
3. Click **Enable (16-40 degrees C)**.
4. Click **Finish**.
5. In the **Confirm** window, verify the settings and enter a task name.
6. Click **Apply**. The task is registered. If the **Go to tasks window for status** check box is checked, the **Task** window opens.

## Managing tasks

You can use Device Manager - Storage Navigator to handle multiple tasks without interruption.

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

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



**Note:** You cannot use a secondary window to make any settings while a task in the main window has a status of In Progress, Waiting, or Suspended.

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

- Create LDEVs
- Format LDEVs

- Shred LDEVs
- Shrink Pool
- Edit Encryption

## Tasks window

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

## Managing your tasks

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

### Before you begin

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

### Procedure

1. In the tree, click **Storage Systems > Tasks**. The list of tasks appears.
2. In the list, click the task or tasks that you want to modify.
3. In the bottom right corner of the window, click the corresponding button for the task you want to perform:
  - Click **Delete Tasks** to delete or cancel a task.
  - Click **Suspend Tasks** to suspend a queued task.
  - Click **Resume Tasks** to resume a suspended task.
  - Click **More Actions > Enable Auto Delete** to delete tasks from the Task list when they have completed and the task list is full. This allows you to check for completed tasks and to clear the list when the limit (384) is reached.
  - Click **More Actions > Disable Auto Delete** to keep tasks in the task list after the tasks are completed.
4. Verify the displayed settings and click **Apply**.


## Referencing the detailed task status

To view the Task Status, click Status for each task in the **Tasks** window.




**Task Status**

Task Name: 130924-CreateLDEVs

 **Task Failed**

An error occurred during the task (Create LDEVs) processing. Due to the error, some settings cannot be applied because the internal processing has been interrupted. Verify all configuration settings of the task, including ones applied normally, and then retry the operation.

 Check the error details with the error code from the following list.

(20222-109021)

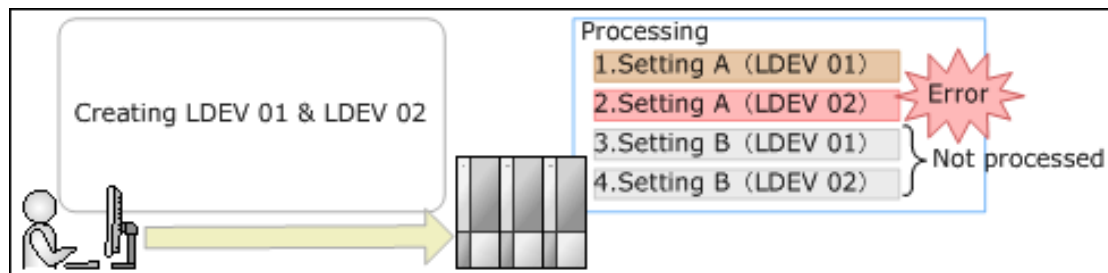
Selected LDEVs					
Error Code	LDEV ID	LDEV Name	Pool Name(ID)	Drive Type/RPM	RAID
<a href="#">03205-058474</a>	00:03:34		HDT0(0)	SSD/-	6(140)
<a href="#">03205-006537</a>	00:03:35		HDT0(0)	SSD/-	6(140)
<a href="#">03205-006537</a>	00:03:36		HDT0(0)	SSD/-	6(140)
<a href="#">03205-006537</a>	00:03:37		HDT0(0)	SSD/-	6(140)
<a href="#">03205-006537</a>	00:03:38		HDT0(0)	SSD/-	6(140)
<a href="#">03205-006537</a>	00:03:39		HDT0(0)	SSD/-	6(140)

Total: 1740

Close

For example, the following figure shows a single task in which "an LDEV 01 and an LDEV 02" are created. Though shown as a single task, this task is internally divided into two parts: a setting for LDEV 01 (setting A) and a setting for LDEV 02 (setting B). If an error occurs in the setting A task, the setting B task will not be processed. The operation result for the setting A task is displayed in the Status of the Tasks window. The setting B task will also not be processed for LDEV 01.

After the task operation is complete, check both the LDEV 02 which has failed in the setting A task and the setting A task for LDEV 01 which has completed. Then run the necessary task again.





## Stalled tasks

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

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

## Setting the status refresh interval of the Tasks window

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

### Procedure

1. Click **Settings > Environmental Settings > Edit Information Display Settings**.
2. Specify the interval for Task Screen Refresh Interval. If **No Update** is specified, the Tasks window will not be automatically updated. In this case, to update the window, you must use **Refresh** or **File > Refresh All**.
3. Click **Apply**.

---

## Chapter 7: Using reports to view storage system information

Device Manager - Storage Navigator can generate reports that contain information about your storage system's physical configurations and logical settings. Reports can cover specific areas of the storage system, such as reporting on configuration, ports, channel adapters, and disk adapters. You can save reports as comma-separated-value (CSV) files or as HTML files. Tables in the HTML version of the configuration reports are sortable.

Before making changes to a storage system, generate reports of your storage system's physical configurations and logical settings. Generate a similar report after the changes, and then compare the reports to verify that new settings were made as intended.

### 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.

#### 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.

### 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.

## 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**.


## Examples of Device Manager - Storage Navigator storage configuration reports

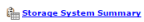
















The Device Manager - Storage Navigator can show configuration reports for your storage systems in table, graph, and CSV formats.

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

### Report examples: table view

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

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

Configuration Reports										
Report Types	Ports									
 Storage System Summary	This report is about ports. A record is created for each port.									
 Physical View										
 Cache Memories										
 Channel Adapters										
 Ports										
 Host Groups / iSCSI Targets										
 Hosts										
 LUNs										
 Logical Devices										
 Parity Groups										
 MP Blades										
 MP Blade Details										
 Disk Adapters										
 SSD Endurance										
 Spare Drives										
 Power Consumption										
 CHAP Users										
CHA	Type	Port Location	Port Attribute	TCP Port Number	Port Internal WWN	Fabric	Connection Type	IPv4 : IP Address	IPv4 : SubnetMask	
CHA-1PC	16FCB(Fibre )	1A	Target		- 50060E8007003200	OFF	FC-AL	-	-	
CHA-1PC	16FCB(Fibre )	3A	Initiator		- 50060E8007003220	OFF	FC-AL	-	-	
CHA-1PC	16FCB(Fibre )	5A	Target		- 50060E8007003240	OFF	FC-AL	-	-	
CHA-1PC	16FCB(Fibre )	7A	Initiator		- 50060E8007003260	OFF	FC-AL	-	-	
CHA-1PC	16FCB(Fibre )	1B	RCU Target		- 50060E8007003201	OFF	FC-AL	-	-	
CHA-1PC	16FCB(Fibre )	3B	Target		- 50060E8007003221	OFF	FC-AL	-	-	
CHA-1PC	16FCB(Fibre )	5B	Initiator		- 50060E8007003241	OFF	FC-AL	-	-	
CHA-1PC	16FCB(Fibre )	7B	Target		- 50060E8007003261	OFF	FC-AL	-	-	
CHA-1PE	16MB (Mfibre)	1E	HTP		- 50060E8007003204	-	-	-	-	
CHA-1PE	16MB (Mfibre)	3E	HTP		- 50060E8007003224	-	-	-	-	
CHA-1PE	16MB (Mfibre)	5E	HTP		- 50060E8007003244	-	-	-	-	
CHA-1PE	16MB (Mfibre)	7E	HTP		- 50060E8007003264	-	-	-	-	
CHA-1PE	16MB (Mfibre)	1F	HTP		- 50060E8007003205	-	-	-	-	
CHA-1PE	16MB (Mfibre)	3F	HTP		- 50060E8007003225	-	-	-	-	
CHA-1PE	16MB (Mfibre)	5F	HTP		- 50060E8007003245	-	-	-	-	
CHA-1PE	16MB (Mfibre)	7F	HTP		- 50060E8007003265	-	-	-	-	
CHA-1PB	81S10 (iSCSI)	9C	Target	3260				192.168.0.90	255.255.255.0	
CHA-1PB	81S10 (iSCSI)	9C	Target	3260				192.168.0.91	255.255.255.0	
CHA-1PB	81S10 (iSCSI)	9D	Target	3260				192.168.0.94	255.255.255.0	
CHA-1PB	81S10 (iSCSI)	9D	Target	3260				192.168.0.95	255.255.255.0	
CHA-2PC	16FCB(Fibre )	2A	Target		- 50060E8007003210	OFF	FC-AL	-	-	
CHA-2PC	16FCB(Fibre )	4A	External		- 50060E8007003230	OFF	FC-AL	-	-	
CHA-2PC	16FCB(Fibre )	6A	External		- 50060E8007003250	OFF	FC-AL	-	-	
CHA-2PC	16FCB(Fibre )	8A	RCU Target		- 50060E8007003270	ON	FC-AL	-	-	
CHA-2PC	16FCB(Fibre )	2B	Target		- 50060E8007003211	OFF	FC-AL	-	-	
CHA-2PC	16FCB(Fibre )	4B	Target		- 50060E8007003231	ON	Point to Point	-	-	
CHA-2PC	16FCB(Fibre )	6B	RCU Target		- 50060E8007003251	OFF	FC-AL	-	-	
CHA-2PC	16FCB(Fibre )	8B	External		- 50060E8007003271	OFF	FC-AL	-	-	
CHA-2PE	16MB (Mfibre)	2E	HTP		- 50060E8007003214	-	-	-	-	
CHA-2PE	16MB (Mfibre)	4E	HTP		- 50060E8007003234	-	-	-	-	
CHA-2PE	16MB (Mfibre)	6E	HTP		- 50060E8007003254	-	-	-	-	
CHA-2PE	16MB (Mfibre)	8E	HTP		- 50060E8007003274	-	-	-	-	
CHA-2PE	16MB (Mfibre)	2F	HTP		- 50060E8007003215	-	-	-	-	
CHA-2PE	16MB (Mfibre)	4F	HTP		- 50060E8007003235	-	-	-	-	

- 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 Adapters report

The following illustration shows an example of a Disk Adapters report. The table following the illustration describes the items in the report.

Disk Adapters						
This report is about disk adapters. A record is created for each disk adapter.						
DKA	Module	Number of PGs	Number of LDEVs(Total)	Number of LDEVs(Unallocated)	Total LDEV Capacity(MB)	Unallocated LDEV Capacity(MB)
DKA-1PA	0	4	320	320	3276899.20	3276899.20
DKA-1PB	0	4	320	320	3276899.20	3276899.20
DKA-2PA	0	4	320	320	3276899.20	3276899.20
DKA-2PB	0	4	320	320	3276899.20	3276899.20

Item	Description
DKA	Location of the disk adapter (also called a back-end director). <ul style="list-style-type: none"> <li>"External" is displayed when the storage system has an external storage system.</li> <li>"External (FICON DM)" is displayed when the storage system has volumes for FICON DM.</li> </ul>
Module	Module number. A hyphen (-) displays if "DKA" is "External" or "External (FICON DM)".

Item	Description
Number of PGs	The number of the parity groups that the disk adapter controls. <ul style="list-style-type: none"> <li>If "DKA" is "External", this item indicates the number of parity groups mapped to external volumes.</li> <li>If "DKA" is "External (FICON DM)", this item indicates the number of parity groups mapped to volumes for FICON DM.</li> </ul>
Number of LDEVs (Total)	The number of the logical volumes belonging to the parity groups that the disk adapter 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 adapter.
Total LDEV Capacity (MB)	Total capacity of the logical volumes belonging to the parity groups that the disk adapter 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 adapter.

## 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 DKAs	The number of disk adapters 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 <ul style="list-style-type: none"> <li>▪ CHAP</li> <li>▪ None</li> <li>▪ Comply with Host Setting</li> </ul>
Authentication : Mutual CHAP	Enable or disable the iSCSI target mutual CHAP <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> </ul>
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.

<b>Hosts</b>					
This report is about hosts. A record is created for each host. When a host is registered to more than one port, more than one record shows information about the same host.					
Port Location	Type	Port Internal WWN	Port Security	Host Group Name / iSCSI Target Alias	iSCSI Target Name
1B	ISCSI(OPT)		Disabled	1B-G00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
2B	ISCSI(OPT)		Disabled	2B-G00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
3B	ISCSI(OPT)		Disabled	3B-G00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
4B	ISCSI(OPT)		Disabled	4B-G00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
Total:4					

Item	Description
Port Location	Name of the port
Type	Port type
Port Internal WWN	Port WWN
Port Security	Port security setting
Host Group Name / iSCSI Target Alias	Name of the host group / alias of the iSCSI target
iSCSI Target Name	Name of the iSCSI target
Host Mode	Host mode of the host group
Host Mode Option	Host group host mode option. When more than one host mode option is specified, they are separated by semicolons (;)
Host Name	Name of the host that can access the LU path through the port
HBA WWN / iSCSI Name	Host WWN / 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.

<b>Logical Devices</b>								
This report is about logical volumes. A record is created for each logical volume.								
LDEV ID	LDEV Name	Capacity(MB)	Emulation Type	Resource Group Name	Resource Group ID	PG	RAID Level	Drive Type/RPM
00:00:00		10240.31	OPEN-V	RSG_001	1	1-1	RAID5(3D+1P)	SAS/15k
00:00:01		10240.31	OPEN-V	RSG_001	1	1-1	RAID5(3D+1P)	SAS/15k
00:00:02		10240.31	OPEN-V	RSG_001	1	1-1	RAID5(3D+1P)	SAS/15k
00:00:03		10240.31	OPEN-V	RSG_001	1	1-1	RAID5(3D+1P)	SAS/15k
00:00:04		10240.31	OPEN-V	RSG_001	1	1-1	RAID5(3D+1P)	SAS/15k
00:00:05		10240.31	OPEN-V	RSG_001	1	1-1	RAID5(3D+1P)	SAS/15k



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	<p>The parity group number.</p> <ul style="list-style-type: none"> <li>▪ If the number starts with "E" (for example, E1-1), the parity group contains external volumes.</li> <li>▪ If the number starts with "M" (for example, M1-1), the parity group contains FICON DM volumes.</li> </ul> <p>A hyphen displays for Dynamic Provisioning or Thin Image V-VOLs.</p>
RAID Level	RAID level of the parity group where the logical volume belongs <sup>1</sup>
Drive Type/RPM	<p>Drive type and round-per-minute (RPM) of the drive of the parity group where the logical volume belongs.</p> <p>A hyphen (-) is displayed as RPM when the drive is SSD.<sup>1</sup></p>
Drive Type-Code	Type code of the drive of the parity group where the logical volume belongs <sup>1</sup>
Drive Capacity	Capacity of the drive of the parity group where the logical volume belongs. <sup>1</sup>
PG Members	List of the drive locations of the parity group where the logical volume belongs <sup>1</sup>
Allocated	<p>Information about whether the host can access the logical volume.</p> <p>For mainframe volumes and multi-platform volumes, "Y" is displayed unless the volumes are in the reserved status.</p>
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	<ul style="list-style-type: none"> <li>▪ For V-VOLs of Dynamic Provisioning, the name of the pool related to the logical volume is displayed<sup>1</sup></li> <li>▪ If the logical volume attribute is Pool, the name of the pool where the logical volume belongs is displayed</li> <li>▪ When neither of the above are displayed, the pool name is blank</li> </ul>
Pool ID	The ID of the pool indicated by "Pool Name" A hyphen (-) displays for volumes other than pool-VOLs or V-VOLs
Current MPB	The number of the microprocessor that currently controls the logical volume
Setting MPB	The number of the MP blade 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	<p>Indicates whether the parity group to which the LDEV belongs is encrypted.</p> <ul style="list-style-type: none"> <li>▪ For internal volumes: Enabled (encrypted) or Disabled (not encrypted)</li> <li>▪ For external volumes: blank</li> </ul>
T10 PI	<p>Indicates the T10 PI attribute set for the LDEV.</p> <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> <li>▪ Blank if the emulation type is not OPEN-V</li> </ul>
ALUA Mode	<p>Indicates whether the ALUA mode is enabled:</p> <ul style="list-style-type: none"> <li>▪ Enabled: ALUA mode is enabled.</li> <li>▪ Disabled: ALUA mode is disabled.</li> </ul>
<p><b>Notes:</b></p> <p>1. A hyphen (-) displays if the LDEV is an external volume or a FICON DM volume.</p>	

## 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.

<b>LUNs</b>			
This report is about LU path definitions. A record is created for each LU path.			
Port Location	HBA WWN / iSCSI Name	Port Security	Host Group Name / iSCSI Target Name
1A	50060E8012000100	Disabled	1A-G00
3A	50060E8012000120	Disabled	3A-G00
Total: 2			

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: <ul style="list-style-type: none"> <li>▪ Active/Optimized: Prioritized</li> <li>▪ Active/Non-Optimized: Lower priority</li> </ul>

## MP Blades report

The following illustration shows an example of an MP blades report. The table following the illustration describes the items in the report.

<b>MP Blades</b>						
This report is about MP blades. A record is created for each MP blade.						
MP Blade ID	MP Blade Name	Module	Auto Assignment	Number of Resources(LDEV)	Number of Resources(Journal)	
MPB0	MPB-1MA	0	Enabled	0		0
MPB1	MPB-1MB	0	Enabled	0		0
MPB4	MPB-2MA	0	Enabled	0		0
MPB5	MPB-2MB	0	Enabled	0		0
Total:4						

Item	Description
MP Blade ID	MP blade ID
MP Blade Name	MP blade name
Module	Module number
Auto Assignment	Auto assignment attribute for the MP blade
Number of Resources (LDEV)	The number of logical volumes that the MP blade controls
Number of Resources (Journal)	The number of journals that the MP blade controls
Number of Resources (External Volume)	The number of external volumes that the MP blade controls, including FICON DM volumes
Number of Resources (Total)	The total number of resources that the MP blade controls The sum of "Number of Resources (LDEV)", "Number of Resources (Journal)", and "Number of Resources (External Volume)"
MP Blade Type	Package type of the MP blade

## MP Blade Details report

The following illustration shows an example of an MP blade details report. The table following the illustration describes the items in the report.

**MP Blade Details**

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

MP Blade ID	MP Blade Name	Auto Assignment	Resource ID	Resource Name	Type	MP Blade Type
MPB0	MPB-1MA	Enabled	00:00:09		LDEV	MPB1
MPB0	MPB-1MA	Enabled	00:00:0D		LDEV	MPB1
MPB0	MPB-1MA	Enabled	00:00:0F		LDEV	MPB1
MPB0	MPB-1MA	Enabled	00:00:11		LDEV	MPB1
MPB0	MPB-1MA	Enabled	00:00:1B		LDEV	MPB1
MPB1	MPB-1MB	Enabled	00:00:00		LDEV	MPB2
MPB1	MPB-1MB	Enabled	00:00:01		LDEV	MPB2
MPB1	MPB-1MB	Enabled	00:00:04		LDEV	MPB2
MPB1	MPB-1MB	Enabled	00:00:08		LDEV	MPB2
MPB1	MPB-1MB	Enabled	00:00:0B		LDEV	MPB2
MPB1	MPB-1MB	Enabled	00:00:0C		LDEV	MPB2
MPB2	MPB-1PE	Enabled	00:00:03		LDEV	MPB1
MPB2	MPB-1PE	Enabled	00:00:10		LDEV	MPB1
MPB2	MPB-1PE	Enabled	00:00:14		LDEV	MPB1

Total:32

Item	Description
MP Blade ID	MP blade ID
MP Blade Name	MP blade name
Auto Assignment	Auto assignment attribute for the MP blade
Resource ID	ID of this resource that the MP blade controls
Resource Name	The name of the resource that the MP blade 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 blade controls
MP Blade Type	Package type of the MP blade

## 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.

**Parity Groups**

This report is about parity groups. A record is created for each parity group.

PG	Module	DKA	RAID Level	Resource Group Name	Resource Group ID	Emulation Type	Number of LDEVs(Total)
1-1	0	DKA-1PA;DKA-2PB	RAID5(3D+1P)	meta_resource	0	OPEN-V	3
3-1	1	DKA-1PG;DKA-2PG	RAID1(2D+2D)	meta_resource	0	OPEN-V	1
3-2	1	DKA-1PG;DKA-2PG	RAID1(2D+2D)	meta_resource	0	OPEN-V	1
3-3	1	DKA-1PG;DKA-2PG	RAID1(2D+2D)	meta_resource	0	OPEN-V	1
4-1	1	DKA-1PG;DKA-2PG	RAID1(2D+2D)	meta_resource	0	OPEN-V	1
4-2	1	DKA-1PG;DKA-2PG	RAID1(2D+2D)	meta_resource	0	OPEN-V	1
4-3	1	DKA-1PG;DKA-2PG	RAID1(2D+2D)	meta_resource	0	OPEN-V	1

Total:7

Item	Description
PG	Parity group number <ul style="list-style-type: none"> <li>▪ If the number starts with "E" (for example, E1-1), the parity group contains external volumes (Hitachi Universal Volume Manager User Guide).</li> <li>▪ If the number starts with "M" (for example, M1-1), the parity group contains volumes for FICON DM.</li> </ul>
Module	Module number <sup>1</sup>
DKA	Name of the disk adapter that controls the parity group <sup>1</sup>
RAID Level	RAID level of the parity group <sup>1</sup>
Resource Group Name	Name of the resource group in which the parity group belongs
Resource Group ID	ID for the resource group in which the parity group belongs
Emulation Type	Emulation type of the parity group
Number of LDEVs (Total)	The number of the logical volumes in the parity group
Number of LDEVs (Unallocated)	The number of the logical volumes in the parity group that the host cannot access
Total LDEV Capacity (MB)	Capacity of the logical volumes in the parity group
Unallocated LDEV Capacity (MB)	Capacity of the logical volumes in the parity group that the host cannot access
Drive Type-Code	The type code of the drive in the parity group. <ul style="list-style-type: none"> <li>▪ The type code of the first drive in the parity group.</li> <li>▪ If the parity group contains external volumes, the drive type code displays the vendor, the model, and the serial number of the storage system.</li> <li>▪ A hyphen (-) displays if the parity group contains volumes for FICON DM.</li> </ul>
Drive Type/RPM	Drive type and revolutions-per-minute (RPM) of the drive in the parity group <sup>1</sup> A hyphen (-) is displayed instead of the RPM when the drive is an SSD.
Drive Capacity	Capacity of the drive in the parity group <sup>1</sup>
RAID Concatenation #0	The number indicating a parity group #0 connected to this parity group <sup>1,2</sup>

Item	Description
RAID Concatenation #1	The number indicating a parity group #1 connected to this parity group <sup>1,2</sup>
RAID Concatenation #2	The number indicating a parity group #1,2 connected to this parity group <sup>1,2</sup>
Encryption	<p>Indicates whether the parity group is encrypted.</p> <ul style="list-style-type: none"> <li>▪ For internal volumes: Enabled (encrypted) or Disabled (not encrypted)</li> <li>▪ For external volumes: A hyphen (-) is displayed</li> </ul>
Accelerated Compression	<p>Accelerated compression of the parity group</p> <ul style="list-style-type: none"> <li>▪ If accelerated compression is supported, Enabled or Disabled is displayed.</li> <li>▪ If accelerated compression is not supported, a hyphen (-) is displayed.</li> </ul>
Automatically manage compressed space of FMD parity group	<p>Indicates whether to manage the compressed area of the FMD parity group automatically.</p> <ul style="list-style-type: none"> <li>▪ When accelerated compression is supported, Enabled (the area is managed automatically) or Disabled (the area is not managed automatically) is displayed.</li> <li>▪ If accelerated compression is not supported, a hyphen (-) is displayed.</li> </ul>
<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. A hyphen is displayed if the parity group contains external volumes or FICON DM volumes.</li> <li>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.</li> </ol>	

## 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.							
CHA	Type	Port Location	Port Attribute	TCP Port Number	Internal WWN / Internal iSCSI Name	Fabric	Connection Type
CHA-1PC	8IS10 (iSCSI)	1A	Target	3260		-	-
CHA-1PC	8IS10 (iSCSI)	3A	Target	3260		-	-
CHA-1PC	8IS10 (iSCSI)	1B	Target	3260		-	-
CHA-1PC	8IS10 (iSCSI)	3B	Target	3260		-	-
CHA-1PD	16FC8(Fibre )	1C	External		50060E800701A002	OFF	FC-AL
CHA-1PD	16FC8(Fibre )	3C	RCU Target		50060E800701A022	OFF	FC-AL
CHA-1PD	16FC8(Fibre )	5C	RCU Target		50060E800701A042	OFF	FC-AL
CHA-1PD	16FC8(Fibre )	7C	Initiator		50060E800701A062	OFF	FC-AL
CHA-1PD	16FC8(Fibre )	1D	Target		50060E800701A003	OFF	FC-AL
CHA-1PD	16FC8(Fibre )	3D	Initiator		50060E800701A023	ON	Point to Point
CHA-1PD	16FC8(Fibre )	5D	Target		50060E800701A043	ON	Point to Point
CHA-1PD	16FC8(Fibre )	7D	RCU Target		50060E800701A063	OFF	FC-AL
CHA-1PE	16M8 (Mfibre)	1E	HTP		50060E800701A004	-	-
CHA-1PE	16M8 (Mfibre)	3E	HTP		50060E800701A024	-	-
CHA-1PE	16M8 (Mfibre)	5E	HTP		50060E800701A044	-	-
CHA-1PE	16M8 (Mfibre)	7E	HTP		50060E800701A064	-	-
CHA-1PE	16M8 (Mfibre)	1F	HTP		50060E800701A005	-	-
CHA-1PE	16M8 (Mfibre)	3F	HTP		50060E800701A025	-	-
CHA-1PE	16M8 (Mfibre)	5F	HTP		50060E800701A045	-	-
CHA-1PE	16M8 (Mfibre)	7F	HTP		50060E800701A065	-	-
CHA-1PF	8FC16(Fibre )	1G	Initiator		50060E800701A006	OFF	Point to Point
CHA-1PF	8FC16(Fibre )	3G	RCU Target		50060E800701A026	OFF	Point to Point
CHA-1PF	8FC16(Fibre )	1H	Target		50060E800701A007	OFF	FC-AL
CHA-1PF	8FC16(Fibre )	3H	RCU Target		50060E800701A027	OFF	FC-AL
CHA-2PD	16FC8(Fibre )	2D	Target		50060E800701A013	OFF	FC-AL
CHA-2PD	16FC8(Fibre )	4D	Initiator		50060E800701A033	OFF	FC-AL

Item	Description
CHA	Name of the channel adapter (also called a front-end director)
Type	Package type of the channel adapter
Port Location	Name of the port on the channel adapter
Port Attribute	Attribute of the 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 <sup>1</sup>
Connection Type	One of the Fibre topology settings <sup>1</sup> <ul style="list-style-type: none"> <li>▪ Point to Point</li> <li>▪ FC-AL</li> </ul>



Item	Description
IPv4 : IP Address	IPv4 address of the port Output example: 192.168.0.100
IPv4 : Subnet Mask	IPv4 subnet mask of the port Output example: 255.255.255.0
IPv4 : Default Gateway	IPv4 default gateway of the port Output example: 255.255.255.0
IPv6 : Mode	IPv6 settings of the port <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> </ul>
IPv6 : Link Local Address	IPv6 link local address of the port (16-digit hexadecimal)
IPv6 : Global Address	IPv6 global address of the port. Output example: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (hexadecimal)
IPv6 : Global Address 2	IPv6 global address 2 of the port. Output example: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (hexadecimal)
IPv6 : Assigned Default Gateway	Assigned IPv6 default gateway
Selective ACK	Selective ACK mode <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> </ul>
Ethernet MTU Size (Byte)	MTU settings (binary) <ul style="list-style-type: none"> <li>▪ 1,500</li> </ul>
Keep Alive Timer	iSCSI keep alive timer (0 to 64,800) (sec)
VLAN : Tagging Mode	Tagging mode of VLAN <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> </ul>
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 <ul style="list-style-type: none"> <li>▪ ON</li> <li>▪ OFF</li> </ul>

Item	Description
iSNS Server : IP Address	IP address of the iSNS server (30 to 65,535)
iSNS Server : TCP Port Number	Number of the TCP port used in iSNS (binary)
Address (Loop ID)	Fibre port address and Loop ID of the port <sup>1</sup>
Port Security	Security of the port <sup>1</sup> <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> </ul>
Speed	Data transfer speed of the port <sup>1</sup>
T10 PI Mode	Indicates whether the T10 PI mode can be applied to the port. <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> <li>▪ Blank if the port type is a Fibre port other than 16FC2(CHB). For iSCSI ports, a hyphen (-) is displayed.</li> </ul>
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 <sup>1</sup>
Number of LUNs	The number of the LU paths defined to the port <sup>1</sup>
Number of LDEVs	The number of the logical volumes that can be accessed through the port <sup>1</sup>
Number of PGs	The number of the parity groups having the logical volumes that can be accessed through the port <sup>1</sup>
Number of DKAs	The number of the disk adapters controlling the parity group that contains the logical volumes that can be accessed through the port <sup>1</sup>
<b>Notes:</b>	
1. For ports in a mainframe system, a hyphen is displayed.	

## 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.

<b>Power Consumption</b>				
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
TEMP:DKC1-Cluster1 Average (degrees C)	Average temperature of DKC1:CL1
TEMP:DKC1-Cluster1 Maximum (degrees C)	Maximum temperature of DKC1:CL1
TEMP:DKC1-Cluster1 Minimum (degrees C)	Minimum temperature of DKC1:CL1
TEMP:DKC1-Cluster2 Average (degrees C)	Average temperature of DKC1:CL2

Item	Description
TEMP:DKC1-Cluster2 Maximum (degrees C)	Maximum temperature of DKC1:CL2
TEMP:DKC1-Cluster2 Minimum (degrees C)	Minimum temperature of DKC1:CL2

**Table 4 Power Consumption report for DKU00**

Item	Description
Date and Time	Date and time when temperature was recorded
TEMP:DKU00-DKUPS000-1 Average (Temperature in degrees C) , TEMP:DKU00-DKUPS000-1 Maximum (Temperature in degrees C) , TEMP:DKU00-DKUPS000-1 Minimum (Temperature in degrees C) , ... ,TEMP:DKU00-DKUPS007-2 Average (Temperature in degrees C) , TEMP:DKU00-DKUPS007-2 Maximum (Temperature in degrees C) , TEMP:DKU00-DKUPS007-2 Minimum (Temperature in degrees C)	Average temperature, maximum temperature, and minimum temperature of the DKU for the two-hour period. Outputs in the following format: TEMP:DKUXY-DKUPSXYZ-CL Average, Maximum, or Minimum (Temperature in degrees Celsius) <ul style="list-style-type: none"> <li>• X: Module number (0, 1)</li> <li>• Y: DKU number (0 to 5)</li> <li>• Z: HDU number (0 to 7)</li> <li>• CL: Cluster number (1, 2)</li> </ul>

## 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 illustration shows an example of part of a report of a summary of the storage system. The actual report includes several more rows of information. The table following the illustration describes the items in the report.

<b>Storage System Summary</b>	
This report shows a summary of the storage system.	
<b>Storage System Type</b>	
VSP G1000	
<b>Serial Number</b>	
50	
<b>IP Address</b>	
126.10.50.15	
<b>Microcode Versions</b>	
Main	8003300805
HTP	800220
FHTP	800303
FCHF	800403
FOEF	800121
ISCF	800101
DKAF	800932
SVP	80033000
SSVP	80030000
FCDG	800003
FCDG	800301
CUDG4	800201
ROM BOOT	800003
RAM BOOT	800004
CMBK	800300
BTCL	800121
Expander	81000E
Expander(FMU)	C10011
Config	80033060
CFM	SD128-A/A21 : 00030000
HDD	DKS5E-J600SS : 7F03
	DKS2D-H3R0SS : 7FA1
HDD(SVP)	DKR5D-J : 00GCGC
	DKR5E-J : 00G7G7
	DKS5E-J : 007F09
	DKR5C-K : 00G9G9
	DKS5C-K : 007F53
	DKS2E-H : 007FA6
	DKS2F-H : 007FA6
	SLR5C-M : 00A7A7
	NFHAA-P : 00K130
	NFHAB-P : 00K130
	SLB5A-M : 00T1MC
	NFH1A-P : 00K130
	NFH1B-P : 00K130
	NFH1C-P : 00K130
	NFHAE-Q : 00A0T2
Printout Tool	80-03-30/00
<b>Number of CUs</b>	
255	
<b>Shared Memory Size(GB)</b>	
40	

Item	Description
Storage System Type	Type of the storage system.
Serial Number	Serial number of the storage system.
IP Address	IP address of the SVP.
Microcode Versions	Version of the following programs. <ul style="list-style-type: none"> <li>▪ Main</li> <li>▪ HTP</li> <li>▪ FHTP</li> <li>▪ FCHF</li> <li>▪ FOEF</li> <li>▪ ISCF</li> </ul>


Item	Description
	<ul style="list-style-type: none"> <li>▪ DKAF</li> <li>▪ SVP</li> <li>▪ SSVF</li> <li>▪ FCDG</li> <li>▪ FFCDG</li> <li>▪ CUDG4</li> <li>▪ ROM BOOT</li> <li>▪ RAM BOOT</li> <li>▪ CMBK</li> <li>▪ BTCL</li> <li>▪ Expander</li> <li>▪ Expander(FMU)</li> <li>▪ Config</li> <li>▪ CFM</li> <li>▪ HDD</li> <li>▪ HDD (SVP)</li> <li>▪ Printout Tool</li> </ul>
Number of CUs	The number of control units in the storage system
Shared Memory Size (GB)	Shared memory capacity Includes the cache management information (directory)
Cache Size (GB)	Cache capacity
Number of DKAs	The number of disk adapters 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
OPEN Volume Capacity (GB) <sup>1</sup>	List of the capacity of the open volumes
M/F Volume Capacity (GB) <sup>1</sup>	The list of the capacity of the mainframe volumes and multi-platform volumes



Item	Description
Number of LDEVs <sup>1</sup>	<p>List of the numbers of the volumes in the following status.</p> <ul style="list-style-type: none"> <li>▪ allocated</li> <li>▪ unallocated</li> <li>▪ reserved</li> <li>▪ free</li> </ul> <p>The list for open-systems and the list for mainframe-systems are separate.</p>
<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. You cannot sort this list.</li> </ol>	

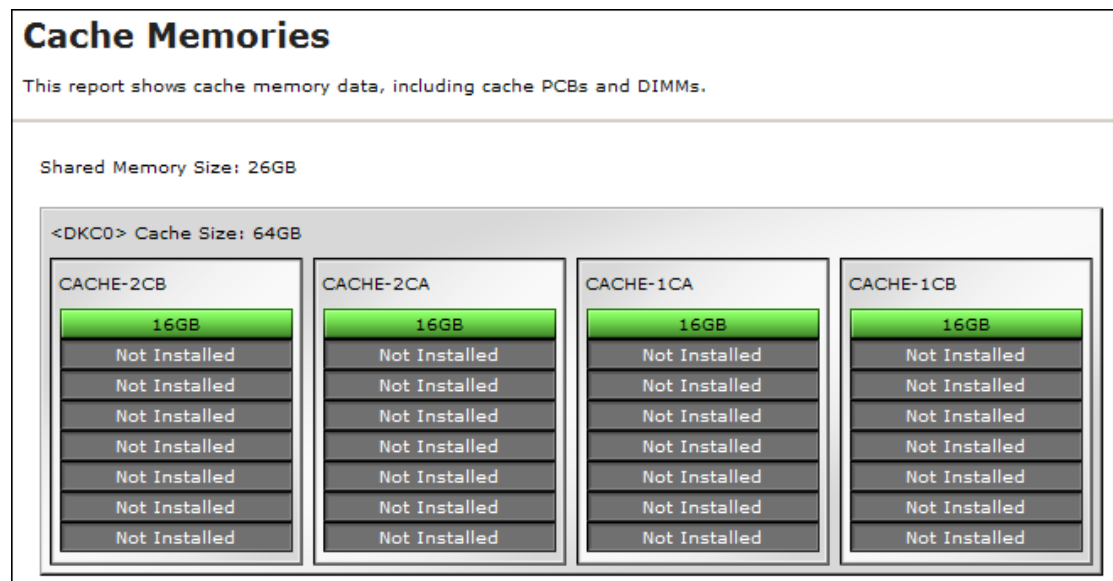
## Report examples: graphical view

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

The reports described in this topic display as graphics.  icons are displayed before the names of reports in graphical view. If the icons or graphics are not displayed properly, update the window.

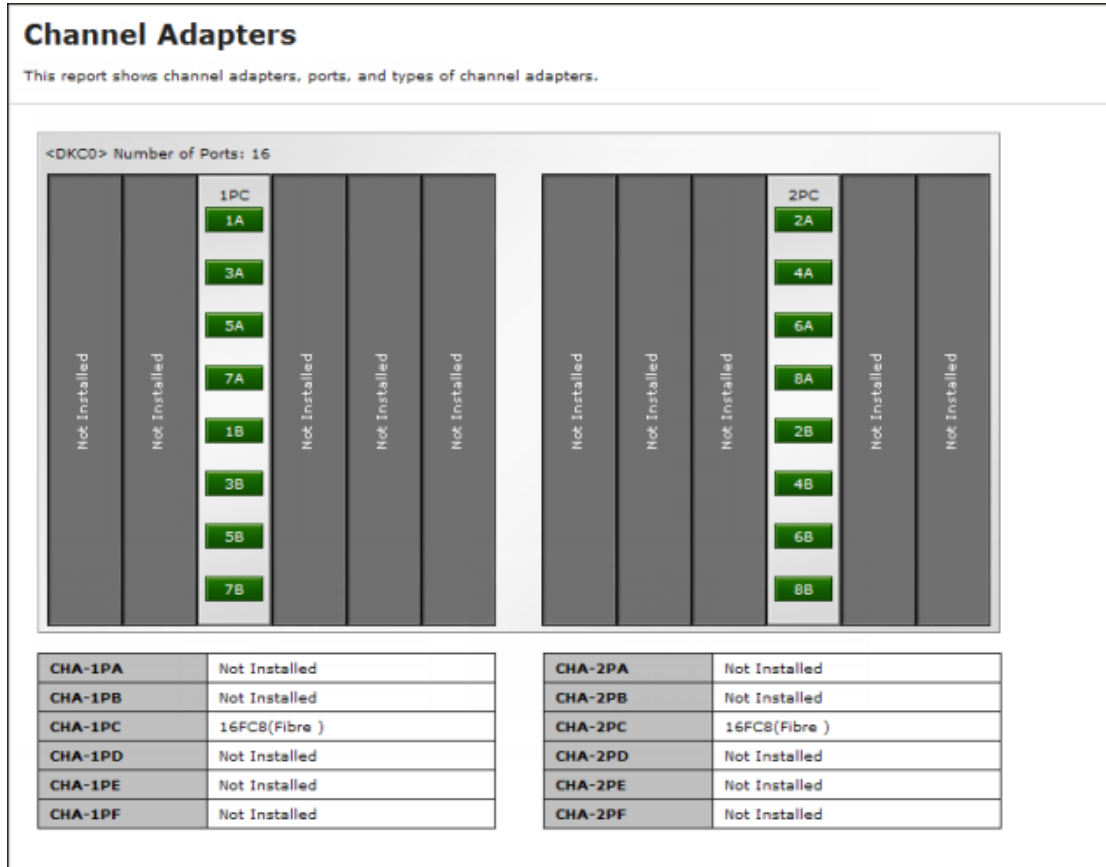
### Cache Memories report

This report shows cache memory data, including shared memory capacity, PCB cache, and DIMM cache.



## Channel Adapters report

This report shows the channel adapters (also called front-end directors) and the ports, and also indicates the type of channel adapter for each port. The keys (green = installed, gray= not installed) show which channel adapters are installed and which are not installed.



## Physical View report

This report shows disk controllers and disk units, and includes cache PCBs, MP blades, channel adapters (also called front-end directors), disk adapters (also called back-end directors), data drives, and spare drives.

The report also shows the storage system type, serial number, and microcode version. You can also check the legend for disk units, such as SAS, SSD, Spare, or Not Installed.

## Physical View

This report shows disk controllers and disk units, and includes cache PCBs, MP blades, channel adapters, disk adapters, data drives, and spare drives.

Storage System Type: VSP G1000, Serial Number: 2624, Microcode Version = 8000000000

[DKC-0](#)  
[DKC-1](#)  
[DKU-00](#)  
[DKU-01](#)  
[DKU-02](#)  
[DKU-03](#)  
[DKU-04](#)  
[DKU-05](#)  
[DKU-10](#)  
[DKU-11](#)  
[DKU-12](#)  
[DKU-13](#)  
[DKU-14](#)  
[DKU-15](#)

< Front View >

DKC-0							
MPB-2MB	MPB-2MA	CACHE-2CB	CACHE-2CA	CACHE-1CA	CACHE-1CB	MPB-1MA	MPB-1MB

< Back View >

DKC-0							
DKA-1PA	DKA-1PB	CHA-1PC	CHA-1PD	MPB-1PE	MPB-1PF	MPB-2PF	MPB-2PE
CHA-2PD	CHA-2PC	DKA-2PB	DKA-2PA				

DKC-1							
MPB-2MD	MPB-2MC	CACHE-2CD	CACHE-2CC	CACHE-1CC	CACHE-1CD	MPB-1MC	MPB-1MD

DKC-1							
DKA-1PG	DKA-1PH	CHA-1PJ	CHA-1PK	MPB-1PL	MPB-1PM	MPB-2PM	MPB-2PL
CHA-2PK	CHA-2PJ	DKA-2PH	DKA-2PG				

< Disk Unit >

DKU-00															
600	600	600	600	600	600	-	-	-	-	-	-	-	-	-	-
600	600	600	600	600	600	-	-	-	-	-	-	-	-	-	-
600	600	600	600	600	600	-	-	-	-	-	-	-	-	-	-
600	600	600	600	600	600	-	-	-	-	-	-	-	-	-	-
600	600	600	600	600	600	-	-	-	-	-	-	-	-	-	-

## Report examples: CSV files

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

This topic describes reports that are saved in CSV format.

### AllConf.csv

This is the concatenated file of all the csv files.

### CacheInfo.csv

This CSV file contains information about cache packages. A record is created for each cache package.

**Table 5 CacheInfo.csv file (Title: <<Cache>>)**

Item	Content
Module#	Module number
Cache Location	Name of cache package
CM DIMM Size (GB)	Capacity of one CM DIM in cache package (in GB)
Cache Size (GB)	Total cache capacity of this package (in GB)
SM Size (GB)	Shared memory capacity (in GB). Includes the cache management information (directory). Output only when Cache Location is CACHE-1CA or CACHE-2CA. Blank displays in other cases.
Cache Residency Size (MB)	Capacity allocated to the cache package for Cache Residency Manager (in MB). Output only when Cache Location is CACHE-1CA or CACHE-2CA. Blank displays in other cases.
CFM Size (GB)	Backup package CFM capacity (in GB)

### ChapUserInfo.csv

This CSV file contains information about the iSCSI CHAP authenticated user registered to the port in the channel adapter. A record is created for each target related to the CHAP authenticated user.

Item	Content
Port	Port name
User Name	Name of the CHAP authenticated user <sup>1</sup>
iSCSI Target ID <sup>2</sup>	The iSCSI number of the target (00 to fe, hexadecimal)
Notes:	
<ol style="list-style-type: none"> <li>1. If the character string contains a comma, the comma is converted to a tab.</li> <li>2. For the target information, see the record information with the same iSCSI target ID in lscsiTargetInfo.csv.</li> </ol>	

### ChaStatus.csv

This CSV file contains information about the status of each channel adapter (CHA). A record is created for each CHA.

**Table 6 ChaStatus.csv file (Title: <<Cha Status>>)**

Item	Content
Module#	Module number
CHA Location	CHA name
PCB Status	Status of this CHA <sup>1</sup>
Port#00, #01, ..., #07	Status of ports on this CHA <sup>2</sup>
DRR#00, #01	Status of DRR on this CHA <sup>2</sup>
DMA#00, #01, ..., #03	Status of DMA on this CHA <sup>2</sup>
MFDMA#00	Status of MFDMA#00 on this CHA <sup>1</sup>
*1 Normal, 0: Abnormal	

### DcrInfo.csv

This CSV file contains information about Cache Residency Manager. A record is created for each logical volume for which Cache Residency Manager is set.

**Table 7 DcrInfo.csv file (Title: <<DCR Information>>)**

Item	Content
HDEV#	ID of the logical volume for which Cache Residency Manager is set. "No Install BIND/PRI0 Extent" displays if Cache Residency Manager is not set.
Type	Cache Residency Manager type. <ul style="list-style-type: none"> <li>▪ BIND</li> <li>▪ PRI0</li> </ul>
From	Start slot for Cache Residency Manager.
To	End slot for Cache Residency Manager
PreStaging Request	Information about whether data is the target of prestaging or not. <ul style="list-style-type: none"> <li>▪ On</li> <li>▪ Off</li> </ul>

### 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, DKU, and SVP. A record is created for each device.

Item	Content
Module#	Module number
Device Location	Device location name. For example: <ul style="list-style-type: none"> <li>▪ For DKCPS: DKCPS-00</li> <li>▪ For DKUPS: DKUPS000-1</li> <li>▪ For Battery: BATTERY-1BA</li> <li>▪ For SVP: SVP-BASIC</li> </ul>
Equip Status	Equipment status of the device: <ul style="list-style-type: none"> <li>▪ Equipped</li> <li>▪ Not Equipped</li> </ul>
Status	Status of the device: <ul style="list-style-type: none"> <li>▪ Normal</li> <li>▪ Abnormal</li> <li>▪ Blank if "Equip Status" is Not Equipped</li> </ul>

### DkaInfo.csv

This CSV file contains information about disk adapters (DKAs). A record is created for each DKA.

**Table 8 DkaInfo.csv file (Title: <<DKA Information>>)**

Item	Content
Module #	Module number
DKA Location	DKA name
Package Type	DKA type Example: <ul style="list-style-type: none"> <li>▪ DKA (4Port)</li> </ul>

### DkaStatus.csv

This CSV file contains information about the status of disk adapters (DKAs). A record is created for each DKA.

**Table 9 DkaStatus.csv file (Title: <<DKA Status>>)**

Item	Content
Module #	Module number
DKA Location	DKA name
PCB Status	Status of this DKA <sup>1</sup>
BECON#00, #01	Status of BECON on this DKA <sup>2</sup>
BEPOR#0000, #0001, ..., #0103.	Status of BEPORT on this DKA. <sup>2</sup> Items are output in the format of "BEPOR#XXYY". XX: BE controller number (2-digit hexadecimal (00 to 01)) YY: BE port number (2-digit hexadecimal (00 to 03))
DRR#00, #01.	Status of DRR on this DKA <sup>2</sup>
DMA#00, #01, ..., #03	Status of DMA on this DKA <sup>2</sup>
<b>Notes:</b>	
<ol style="list-style-type: none"> <li>1: Normal, 0: Abnormal</li> <li>1: Normal, 0: Abnormal, Blank: Not installed</li> </ol>	

**DkcInfo.csv**

This CSV file contains information about DKC. A record is created for each module.  
When Module #1 is not installed, the record for Module #1 is not created.

**Table 10 DkcInfo.csv file (Title: <<DKC Information>>)**

Item	Content
Storage System Type	Storage system type. Output example: VSP G1000
Serial Number #	Serial product number (in the decimal format, from 1 to 99999)
IP Address	IP address <sup>1</sup> Output example: xxx.xxx.xxx.xxx (xxx is in decimal format)
Subnet Mask	Subnet mask <sup>1</sup> Output example: xxx.xxx.xxx.xxx (xxx is in decimal format)
Number of CUs	Number of CUs (number in the decimal format) <sup>1</sup>
Number of DKAs	Number of DKAs (number in the decimal format) <sup>2</sup>

Item	Content
Configuration Type	Configuration type <sup>1</sup> Output example: PCM
Module #	Module number
<b>Notes:</b>	
<ol style="list-style-type: none"> <li>1. The same value is output for Module #0 and #1.</li> <li>2. Different values are output for Module #0 and #1.</li> </ol>	

## DkuTempInfo.csv

This CSV file contains information about DKU temperature for every two hours. A record is DKU temperature information obtained from the environment monitor. A record output to the first line shows the latest temperature information. Because DKU temperature information is measured by DKUPS, items are displayed in this unit\*.

DkuTempInfo.csv shows the average temperature, maximum temperature, and minimum temperature as DKU temperature data. The total number of items is 577.

The DKU 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 DKU temperature data for DkuTempInfo.csv.

No reports are output if the breakers of the storage system are turned off. In addition, if the system is in maintenance mode or the SVP is rebooted, the data which 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 11 DkuTempInfo.csv file (Title: <<DKU temperature Information>>)**

Item	Description
Date	Year, month, and date when temperature data was acquired in the format: <i>YYYY/MM/DD hh:mm:ss</i>
DKU00 DKUPS0001 Temperature average	Average temperature (°C) for the two-hour period of DKU00 DKUPS0001
DKU00 DKUPS0001 Temperature maximum value	Maximum temperature (°C) for the two-hour period of DKU00 DKUPS0001
DKU00 DKUPS0001 Temperature minimum value	Minimum temperature (°C) for the two-hour period of DKU00 DKUPS0001



Item	Description
DKU15 DKUPS1572 Temperature average	Average temperature (°C) for the two-hour period of DKU15 DKUPS1572
DKU15 DKUPS1572 Temperature maximum value	Maximum temperature (°C) for the two-hour period of DKU15 DKUPS1572
DKU15 DKUPS1572 Temperature minimum value	Minimum temperature (°C) for the two-hour period of DKU15 DKUPS1572

**Note:** An item name is displayed as DKUxx DKUPSxy. The names are listed in ascending order of the DKU number.

The following tables list DKUxy, DKUPSxyz: xy values

DKU #	0	1	2	3	4	5
x	0	1	0	1	0	1
y	0	0	1	1	2	2
DKUxy	DKU00	DKU10	DKU01	DKU11	DKU02	DKU12
DKUPSxyz c	DKU00zc	DKU10zc	DKU01zc	DKU11zc	DKU02zc	DKU12zc

DKU #	6	7	8	9	10	11
x	0	1	0	1	0	1
y	3	3	4	4	5	5
DKUxx	DKU03	DKU13	DKU04	DKU14	DKU05	DKU15
DKUxy	DKU03zc	DKU13zc	DKU04zc	DKU14zc	DKU05zc	DKU15zc

The following tables list DKUPSxyz: zc values (where DKC# is 0 and xy is 00)

DKU #	0					
z	0	0	1	1	2	2
c	1	2	1	2	1	2

DKU #	0					
DKUPSxyz c	DKUPS00 01	DKUPS000 2	DKUPS001 1	DKUPS001 2	DKUPS00 21	DKUPS00 22

DKU #	0					
z	3	3	4	4	5	5
c	1	2	1	2	1	2
DKUPSxyz c	DKUPS00 31	DKUPS003 2	DKUPS004 1	DKUPS004 2	DKUPS005 1	DKUPS00 52

DKU #	0			
z	6	6	7	7
c	1	2	1	2
DKUPSxyzc	DKUPS0061	DKUPS0062	DKUPS0071	DKUPS0072

### DkuTempAveInfo.csv

This CSV file contains information about DKU temperature for every two hours. A record is DKU temperature information obtained from the environment monitor. A record output to the first line shows the latest temperature information. Because DKU temperature information is measured by DKUPS, items are displayed in this unit\*.

DkuTempAveInfo.csv shows the average temperature as DKU temperature data. The total number of items is 193.

The DKU 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 DKU temperature data for DkuTempInfo.csv.

No reports are output if the breakers of the storage system are turned off. In addition, if the system is in maintenance mode or the SVP is rebooted, the data which 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 12 DkuTempAveInfo.csv file (Title: <<DKU temperature average value Information>>)**

Item	Description
Date	Year, month, and date when temperature data was acquired in the format: <i>YYYY/MM/DD hh:mm:ss</i>
DKU00 DKUPS0001 Temperature average	Average temperature (°C) for the two-hour period of DKU00 DKUPS0001
DKU15 DKUPS1572 Temperature average	Average temperature (°C) for the two-hour period of DKU15 DKUPS1572

**\*Note:** An item name is displayed as DKUxx DKUPSxxy. The names are listed in ascending order of the DKU number.

### DkuTempMaxInfo.csv

This CSV file contains information about DKU temperature for every two hours. A record is DKU temperature information obtained from the environment monitor. A record output to the first line shows the latest temperature information. Because DKU temperature information is measured by DKUPS, items are displayed in this unit\*.

DkuTempMaxInfo.csv shows the maximum temperature as DKU temperature data. The total number of items is 193.

The DKU 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 DKU temperature data for DkuTempInfo.csv.

No reports are output if the breakers of the storage system are turned off. In addition, if the system is in maintenance mode or the SVP is rebooted, the data which 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 13 DkuTempMaxInfo.csv file (Title: <<DKU temperature maximum value Information>>)**

Item	Description
Date	Year, month, and date when temperature data was acquired in the format: <i>YYYY/MM/DD hh:mm:ss</i>
DKU00 DKUPS0001 Temperature maximum value	Maximum temperature (°C) for the two-hour period of DKU00 DKUPS0001

Item	Description
DKU15 DKUPS1572 Temperature maximum value	Maximum temperature (°C) for the two-hour period of DKU15 DKUPS1572

**\*Note:** An item name is displayed as DKUxx DKUPSsxy. The names are listed in ascending order of the DKU number.

## DkuTempMinInfo.csv

This CSV file contains information about DKU temperature for every two hours. A record is DKU temperature information obtained from the environment monitor. A record output to the first line shows the latest temperature information. Because DKU temperature information is measured by DKUPS, items are displayed in this unit\*.

DkuTempMinInfo.csv shows the minimum temperature as DKU temperature data. The total number of items is 193.

The DKU 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 DKU temperature data for DkuTempInfo.csv.

No reports are output if the breakers of the storage system are turned off. In addition, if the system is in maintenance mode or the SVP is rebooted, the data which 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 14 DkuTempMinInfo.csv file (Title: <<DKU temperature minimum value Information>>)**

Item	Description
Date	Year, month, and date when temperature data was acquired in the format: <i>YYYY/MM/DD hh:mm:ss</i>
DKU00 DKUPS0001 Temperature minimum value	Minimum temperature (°C) for the two-hour period of DKU00 DKUPS0001
DKU15 DKUPS1572 Temperature minimum value	Minimum temperature (°C) for the two-hour period of DKU15 DKUPS1572

**\*Note:** An item name is displayed as DKUxx DKUPSsxy. The names are listed in ascending order of the DKU number.

## 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*.

Item	Content
VDEV#	Virtual device number to which the external volume is mapped
Characteristic1	Identification number of the external volume <sup>1</sup>
Characteristic2	Extended information for identifying the external volume
Device	Product name reported to the host by the external volume <sup>1</sup>
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 <ul style="list-style-type: none"> <li>▪ Enabled: Asynchronously</li> <li>▪ Disabled: Synchronously</li> </ul>
ECC Group	Number of parity group to which the external volume is mapped. If the number starts with "E" (for example, E1-1), the parity group contains external volumes.
Current MP Blade	Number and name of a current MP blade controlling the parity group to which the external volume is mapped
Setting MP Blade	Number and name of an MP blade configured to control the external volume indicated by ECC Group
Vendor	Vendor name of the external storage system
Product Name	Product name of the external storage system
Serial Number#	Serial product number of the external storage system
Path Mode	Mode which indicates how the paths between local and external storage systems operate <ul style="list-style-type: none"> <li>▪ Multi</li> <li>▪ Single</li> <li>▪ ALUA</li> </ul>
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

Item	Content
	If "Package Type" is iSCSI, a blank space is displayed.
LUN	LU number set for the external volume.
Priority	Priority of the paths between the storage systems to be used for connection with the external volume. "1" indicates the path of the highest priority.
Status	Status of the path between storage systems. <ul style="list-style-type: none"> <li>▪ Normal</li> <li>▪ Blocked</li> </ul>
IO TOV	I/O timeout value for the external volume
QDepth	The number of Read/Write commands that can be issued to the external volume at a time
Resource Group ID (ECC Group)	Resource group ID for the parity group that is mapping external volumes (in hexadecimal format)
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 <ul style="list-style-type: none"> <li>▪ Normal Round-robin</li> <li>▪ Extended Round-robin</li> <li>▪ Disabled</li> </ul> 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: <ul style="list-style-type: none"> <li>▪ Multi</li> <li>▪ Single</li> </ul>
ALUA Settable	Indicates whether ALUA mode can be set as path mode on the external storage system <ul style="list-style-type: none"> <li>▪ Yes: ALUA mode can be set</li> <li>▪ No: ALUA mode cannot be set</li> </ul>
ALUA Permitted	Indicates whether ALUA is used as path mode on the local storage system: <ul style="list-style-type: none"> <li>▪ Enabled: ALUA mode is used</li> <li>▪ Disabled: ALUA mode is not used</li> </ul>

Item	Content
Target Port Asymmetric Access State	Status of the port on the external storage system when the path mode is ALUA: <ul style="list-style-type: none"> <li>Active/Optimized</li> <li>Active/Non-Optimized</li> </ul>
Package Type	Type of CHA to which a port of the local storage system connecting to the external storage system belongs <ul style="list-style-type: none"> <li>Fibre: 16FC8(Fibre ), 8FC16(Fibre ), 16FC16(Fibre )</li> <li>FCoE: 16FE10(FCoE)</li> <li>iSCSI: 8IS10(iSCSI)</li> </ul>
IP Address	IP address for an iSCSI target of an external storage system <ul style="list-style-type: none"> <li>IPv6: (XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX) XX: 00 to FF (hexadecimal)</li> <li>IPv4: (XXX.XXX.XXX.XXX) XXX: 0 to 255 (decimal)</li> </ul>
TCP Port Number	TCP port number (1 through 65535) for the iSCSI target of an external storage system
iSCSI Target Name	iSCSI target name of an external storage system
<b>Notes:</b>	
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.

Item	Description
Date	Year, month, and date when record data was acquired for the two-hour period in the format:

Item	Description
	YYYY/MM/DD HH:MM:SS
Electric power average	Average value of electric power (W)
Electric power maximum value	Maximum value of electric power (W)
Electric power minimum value	Minimum value of electric power (W) In the following cases, a lower value might be temporarily displayed: <ul style="list-style-type: none"> <li>▪ When the storage system is starting up</li> <li>▪ Right after replacing storage system parts</li> <li>▪ During or after microcode update</li> </ul>
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)
DKC1 CL1 Temperature average	DKC1: Average temperature of CL1 (°C)
DKC1 CL1 Temperature maximum value	DKC1: Maximum temperature of CL1 (°C)
DKC1 CL1 Temperature minimum value	DKC1: Minimum temperature of CL1 (°C)
DKC1 CL2 Temperature average	DKC1: Average temperature of CL2 (°C)
DKC1 CL2 Temperature maximum value	DKC1: Maximum temperature of CL2 (°C)
DKC1 CL2 Temperature minimum value	DKC1: 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 for Open Systems*.

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)
Authentication of Group	Information about whether to perform authentication or not <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> </ul>
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 for Open Systems*.

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)

Item	Content
Mode	Mode of authentication between ports and FC switches <ul style="list-style-type: none"> <li>▪ Bidirectional</li> <li>▪ Unidirectional</li> </ul>
Authentication of Fabric Switch	Information about whether to perform authentication of the FC switch identified by "Switch Port Username" <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> </ul>

### HduInfo.csv

This CSV file contains information about hard disk units (HDUs). A record is created for each HDU.

**Table 15 HduInfo.csv file (Title: <<HDU Information>>)**

Item	Content
Module#	Module number
HDU Location	HDU location name Output example: HDU000
HDU Status	Information about whether this HDU is installed or not <ul style="list-style-type: none"> <li>▪ Installed</li> <li>▪ Not Installed</li> </ul>
Slot Size	Slot size (inches) <ul style="list-style-type: none"> <li>▪ 2.5</li> <li>▪ 3.5</li> <li>▪ Blank when DKU is FBX (FMD, FMD DC2, or FMD-HDE)</li> </ul>
DKU Type	DKU type of HDU <ul style="list-style-type: none"> <li>▪ SBX (DKU for 2.5-inch drive)</li> <li>▪ UBX (DKU for 3.5-inch drive)</li> <li>▪ FBX (DKU for FMD, FMD DC2, or FMD-HDE)</li> </ul>

### IscsiHostInfo.csv

This CSV file contains information about iSCSI Initiator (Host) set to the channel adapter port. A record is created for each iSCSI Host (Initiator) target.

Item	Content
Port	Port name
iSCSI Name	iSCSI host name
Host Name	Nickname for iSCSI host name
iSCSI Target ID <sup>1</sup>	iSCSI target number (hexadecimal format, 00 to fe)
<b>Notes:</b>	
<ol style="list-style-type: none"> <li>1. For the target information, see the record information with the same iSCSI target ID in IscsiTargetInfo.csv.</li> </ol>	

### IscsiPortInfo.csv

This CSV file contains information about iSCSI information set to the channel adapter port. A record is created for each iSCSI host (initiator) target.

Item	Content
Port	Port name
IPv4   IP Address	IPv4 address Output example: xxx.xxx.xxx.xxx (decimal)
IPv4   Subnet Mask	IPv4 subnet mask (decimal) Output example: xxx.xxx.xxx.xxx (decimal)
IPv4   Default Gateway	Port IPv4 default gateway Output example: xxx.xxx.xxx.xxx (decimal)
IPv6   Mode	Port IPv6 settings <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> </ul>
IPv6   Link Local Address	Port IPv6 link local address <ul style="list-style-type: none"> <li>▪ Output example: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (hexadecimal)</li> <li>▪ Output example: Auto</li> </ul> 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 <ul style="list-style-type: none"> <li>▪ Output example: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (hexadecimal)</li> <li>▪ Output example: Auto</li> </ul>

Item	Content
	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 <ul style="list-style-type: none"> <li>▪ Output example: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (hexadecimal)</li> </ul> Blank if "IPv6   Mode" is Disabled.
Channel Speed	Data transfer speed of the port (10 Gbps)
Security Switch	Port security switch settings <ul style="list-style-type: none"> <li>▪ On</li> <li>▪ Off</li> </ul>
TCP Port Number	The number of the port for using socket (1 to 65535)
Ethernet MTU Size (Byte)   MTU	MTU settings <ul style="list-style-type: none"> <li>▪ 1500</li> <li>▪ 4500</li> <li>▪ 9000</li> </ul>
Keep Alive Timer (sec.)	Keep alive timer value of iSCSI (30 to 64800) (sec)
Selective ACK	Selective ACK mode <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> </ul>
Delayed ACK	Delayed ACK mode <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> </ul>
Maximum Window Size (KB)	Window scale option settings <ul style="list-style-type: none"> <li>▪ 64KB</li> <li>▪ 128KB</li> <li>▪ 256KB</li> <li>▪ 512KB</li> <li>▪ 1024KB</li> </ul>
iSNS Server   Mode	iSNS mode settings <ul style="list-style-type: none"> <li>▪ On</li> <li>▪ Off</li> </ul>

Item	Content
iSNS Server   IP Address	IP address of the iSNS server <ul style="list-style-type: none"> <li>IPv4: xxx.xxx.xxx.xxx (decimal)</li> <li>IPv6: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (hexadecimal)</li> <li>Blank if "iSNS Server   Mode" is Off.</li> </ul>
iSNS Server   TCP Port Number	Port number of TCP used for iSNS (1 to 65535). Blank if "iSNS Server   Mode" is Off.
VLAN   Tagging Mode	VLAN tagging mode set to the port <ul style="list-style-type: none"> <li>On</li> <li>Off</li> </ul>
VLAN   ID	VLAN number set to the port (1 to 4094) 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 <ul style="list-style-type: none"> <li>Output example: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (hexadecimal)</li> <li>Output example: Auto</li> </ul> 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 adapter port. A record is created for each iSCSI target.

Item	Content
Port	Port name
iSCSI Target Alias	iSCSI target alias
iSCSI Target ID	Number of the iSCSI target (00 to fe, hexadecimal)

Item	Content
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) Separated with a semicolon (;) if multiple host mode options are set.
Security Switch	Security switch status set to the iSCSI target port <ul style="list-style-type: none"> <li>▪ On</li> <li>▪ Off</li> </ul>
Authentication   Method	Authentication method settings of the iSCSI target <ul style="list-style-type: none"> <li>▪ CHAP</li> <li>▪ None</li> <li>▪ Comply with Host Setting</li> </ul>
Authentication   Mutual CHAP	Mutual CHAP authentication function settings of the iSCSI target <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> </ul>
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 16 JnlInfo.csv file (Title: <<JNL Information>>)**

Item	Content
JNL#	Journal number (in the hexadecimal format)
Current MP Blade	Number and name of MP blade currently controlling the journal
Setting MP Blade	Number and name of MP blade configured to control the journal

**LdevCapalInfo.csv**

This CSV file contains information about LDEV capacities. A record is created for each of the classifications shown in "Volume Kind".

Item	Content
Volume Kind	The following classifications are output: <ul style="list-style-type: none"> <li>▪ Internal OPEN Volumes</li> <li>▪ Internal Mainframe Volumes</li> <li>▪ External OPEN Volumes</li> <li>▪ External Mainframe Volumes</li> <li>▪ Total OPEN Volumes</li> <li>▪ Total Mainframe Volumes</li> </ul>
Allocated LDEV Capacity (GB)	Allocated LDEV capacity
Unallocated LDEV Capacity (GB)	Unallocated LDEV capacity
Reserved Capacity (GB)	Reserved LDEV capacity
Total Volume Capacity (GB)	Total capacity of "Allocated LDEV Capacity", "Unallocated LDEV Capacity" and "Reserved Capacity"
Free Space (GB)	Free Space
Total Capacity (GB)	Total Capacity The sum of "Total Volume Capacity" and "Free Space"

**LdevCountInfo.csv**

This CSV file contains information about the number of logical devices (LDEVs). A record is created for each of the classifications shown in "Volume Kind".

Item	Content
Volume Kind	The following classifications are output: <ul style="list-style-type: none"> <li>▪ Internal Volumes</li> <li>▪ External Volumes</li> <li>▪ Total Volumes</li> </ul>
Allocated OPEN LDEVs	The number of allocated open-system volumes (LDEVs).

Item	Content
Unallocated OPEN LDEVs	The number of unallocated open-system volumes (LDEVs).
Reserved OPEN LDEVs	The number of reserved open-system volumes (LDEVs).
Allocated Mainframe LDEVs	The number of allocated mainframe and multi-platform volumes (LDEVs).
Reserved Mainframe LDEVs	The number of reserved mainframe and multi-platform volumes (LDEVs).
V-VOL	The number of virtual volumes. Output only when "Volume Kind" is Total Volumes.
Total(All LDEVs)	Total number of LDEVs.
ECC Groups	Total number of parity groups.

### LdevInfo.csv

This CSV file contains information about logical devices (LDEVs). A record is created for each LDEV.

For details of LDEVs, see the *Provisioning Guide for Open Systems*.

**Table 17 Ldevinfo.csv file (Title: <<LDEV Status>>)**

Item	Content
ECC Group	Number of parity group where the LDEV belongs. <ul style="list-style-type: none"> <li>▪ If the number starts with "E" (for example, E1-1), the parity group contains external volumes.</li> <li>▪ If the number starts with "M" (for example, M1-1), the parity group contains FICON DM volumes.</li> <li>▪ If "LDEV Type" is Dynamic Provisioning, Thin Image, or ALU (Administrative Logical Unit), a hyphen (-) is output.</li> </ul>
LDEV#	LDEV number
LDEV Name	LDEV name <sup>1</sup>
LDEV Emulation	LDEV emulation type
LDEV Type	LDEV type: <ul style="list-style-type: none"> <li>▪ Basic</li> <li>▪ Dynamic Provisioning</li> <li>▪ External</li> </ul>



Item	Content
	<ul style="list-style-type: none"> <li>▪ Thin Image (Thin Image virtual volume)</li> <li>▪ ALU</li> </ul>
LDEV Attribute	LDEV Attribute: <ul style="list-style-type: none"> <li>▪ CMDDEV (Command device)</li> <li>▪ CMDDEV* (Remote command device)</li> <li>▪ Journal (Journal volume)</li> <li>▪ Pool (Pool volume)</li> <li>▪ Reserve (Reserved volume)</li> <li>▪ Quorum disk (Quorum Disk used with global-active device)</li> <li>▪ TSE (Volume for Hitachi Compatible FlashCopy<sup>®</sup>)</li> <li>▪ ALU</li> <li>▪ SLU (Subsidiary Logical Unit)</li> <li>▪ Deduplication system data volume</li> <li>▪ Regular (Others)</li> </ul>
Volume Size(Cyl)	LDEV capacity (in cylinders)
Volume Size(MB)	LDEV capacity (in MB)
Volume Size(Blocks)	LDEV capacity (in blocks)
CVS	Information about whether the LDEV is a custom-sized volume or not: <ul style="list-style-type: none"> <li>▪ On: Custom-sized volume</li> <li>▪ Off: Others</li> </ul>
Pool ID	Pool number. This is blank except for the following cases: <ul style="list-style-type: none"> <li>▪ If "LDEV Type" is Dynamic Provisioning</li> <li>▪ If LDEV Attribute is Pool</li> </ul>
RAID Concatenation#0	Number of parity group to be concatenated to parity group (#0) identified by ECC Group. Blank if the parity group is not concatenated to another parity group.
RAID Concatenation#1	Number of parity group to be concatenated to parity group (#1) identified by ECC Group. Blank if the parity group is not concatenated to another parity group.
RAID Concatenation#2	Number of parity group to be concatenated to parity group (#2) identified by ECC Group. Blank if the parity group is not concatenated to another parity group.

Item	Content
ORACLE CHECK SUM	Information about whether this LDEV is Oracle check sum target or not. <ul style="list-style-type: none"> <li>▪ For open-system or multi-platform volumes: On or Off</li> <li>▪ For other volumes: blank</li> </ul>
Current MP Blade	Number and name of MP blade currently controlling the LDEV.
Setting MP Blade	Number and name of MP blade configured to control LDEV.
Allocated	Information about whether this LDEV is allocated to a host or not. <ul style="list-style-type: none"> <li>▪ When mainframe or multi-platform volumes, "Y" is output for all except Reserved.</li> <li>▪ When open-system volumes, "Y" is output for volumes accessible to host.</li> </ul>
Pool Name	The pool's name <sup>1</sup> Name of the pool indicated by Pool ID
CmdDevSecurity	Indicates whether Security is specified as the attribute for the command device.
CmdDevUserAuth	Indicates whether User Authentication is specified as the attribute for the command device.
CmdDevDevGrpDef	Indicates whether Device Group Definition is specified as the attribute for the command device.
Resource Group ID (LDEV)	LDEV resource group ID (number in the decimal format)
Resource Group Name (LDEV)	LDEV resource group name
Encryption	Indicates whether the parity group identified by ECC Group is encrypted. <ul style="list-style-type: none"> <li>▪ For internal volumes: Enabled (encrypted) or Disabled (not encrypted)</li> <li>▪ For external volumes: blank</li> </ul>
ALUA Mode	Indicates whether the ALUA mode is enabled: <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> <li>▪ For mainframe volumes: blank</li> </ul>

Item	Content
T10 PI	Indicates the T10 PI attribute set for the LDEV. <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> <li>▪ Blank if "LDEV Emulation" is not OPEN-V.</li> </ul>
Accelerated Compression	Indicates whether accelerated compression is enabled For internal volumes: <ul style="list-style-type: none"> <li>▪ Enabled: accelerated compression is enabled.</li> <li>▪ Disabled: accelerated compression is disabled.</li> </ul> If the parity group with LDEV does not support accelerated compression, a blank space is displayed. For external volumes, a blank is displayed.
Notes:	
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.

Item	Content
VDEV#	Virtual device number in which the LDEV is defined
VDEV Status	VDEV status of "VDEV#" <ul style="list-style-type: none"> <li>▪ 1: Normal</li> <li>▪ 0: Abnormal</li> </ul>
HDEV#	LDEV number
HDEV Status	LDEV status <ul style="list-style-type: none"> <li>▪ 1: Normal</li> <li>▪ 0: Abnormal</li> </ul>
LDEV Emulation	LDEV emulation type

Item	Content
ECC Group	<p>Number of the parity group where the LDEV belongs.</p> <ul style="list-style-type: none"> <li>▪ If the number starts with "E" (for example, E1-1), the parity group contains external volumes.</li> <li>▪ If the type of the LDEV is a Dynamic Provisioning, Thin Image, or ALU virtual volume, a hyphen is output.</li> </ul> <p>Refer to "LdevInfo.csv" for information about the LDEV type.</p>

## LogPathStatus.csv

This CSV file contains information about mainframe logical paths.

**Table 18 LogPathStatus.csv file (Title: <<Main Frame Logical Path Status>>)**

Item	Content
Module#	Module number
LPN#	Logical path number (in the hexadecimal format)
CHA Location	CHA name
Port	Port name
Link	Link address of the connected host (6-digit number in the hexadecimal format)
LGCL	Logical address of the connected host (number in the hexadecimal format)
LDKC#	Number of connected LDKC (in the hexadecimal format)
CU#	Number of connected CU (in the hexadecimal format)

## 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 *Virtual Partition Manager*.

**Table 19 LPartition.csv file (Title: <<Logical Partitioning>>)**

Item	Content
CLPR#	CLPR ID (in the decimal format)
CLPR Name	CLPR name

Item	Content
Cache Size(MB)	Cache size allocated to this CLPR ID (in MB)
Cache Residency Size(MB)	Cache Residency Manager cache size allocated to this CLPR ID (in MB)
ECC Group	Number of parity group allocated to this CLPR ID.
LDEV#(V-VOL)	LDEV number allocated to this CLPR ID 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 LU path definition. For details about LU path definitions, see the *Provisioning Guide for Open Systems*. For information about iSCSI targets, see *IscsiTargetInfo.csv*.

Item	Description
Port	Port name
Host Group	Host group name If "Package Type" is iSCSI, the iSCSI target alias is output.
Host Mode	Host mode specified for this host group (hexadecimal)
Host Mode Option	Host mode option set for this host group (number in the decimal format) 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: <ul style="list-style-type: none"> <li>▪ On: Command Device</li> <li>▪ On*: Remote Command Device</li> <li>▪ Off: Others</li> </ul>
Command Security	Information about whether the command device is secured: <ul style="list-style-type: none"> <li>▪ On</li> <li>▪ Off</li> </ul>

Item	Description
CVS	Information about whether the LDEV is a custom-sized volume: <ul style="list-style-type: none"> <li>▪ On: Customized volume</li> <li>▪ Off: Other volumes</li> </ul>
CHA Location	Name of the CHA on which this port is installed
Package Type	CHA type for CHA Location: <ul style="list-style-type: none"> <li>▪ Fibre:               <ul style="list-style-type: none"> <li>• 16FC8 (Fibre )</li> <li>• 8FC16 (Fibre )</li> <li>• 16FC16 (Fibre)</li> </ul> </li> <li>▪ FCoE:               <ul style="list-style-type: none"> <li>• 16FE10 (FCoE )</li> </ul> </li> <li>▪ iSCSI:               <ul style="list-style-type: none"> <li>• 8IS10 (iSCSI)</li> </ul> </li> </ul>
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. <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> <li>▪ Blank if "Package Type" is "8FC16(Fibre )" or "16FC16(Fibre)"</li> </ul>
T10 PI	Information about the T10 PI attribute which is set for the LDEV number of the LU path definition. <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> <li>▪ Blank if LDEV# is blank</li> </ul>
Asymmetric Access State	Asymmetric access status (output only for an open system CHA that is Fibre or FCoE) Indicates the asymmetric access status: <ul style="list-style-type: none"> <li>▪ Active/Optimized: Prioritized</li> <li>▪ Active/Non-Optimized: Lower priority</li> </ul> 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 for Open Systems*. For information about iSCSI ports, see *IscsiPortInfo.csv*.

Item	Content
Port	Port name.
Security Switch	The setting status of the security switch: <ul style="list-style-type: none"> <li>▪ On</li> <li>▪ Off</li> </ul>
Port Address	Port address (2-digit hexadecimal number) 00 to ff Blank if "Package Type" is iSCSI
Loop ID	Port address (0 - 125, decimal) Blank if "Package Type" is iSCSI
Fabric	One of the Fibre topology settings indicating the setting status of the Fabric switch: <ul style="list-style-type: none"> <li>▪ On</li> <li>▪ Off</li> <li>▪ Blank if "Package Type" is iSCSI</li> </ul>
Connection	One of the Fibre topology settings: <ul style="list-style-type: none"> <li>▪ Point to Point</li> <li>▪ FC-AL</li> <li>▪ Blank if "Package Type" is iSCSI</li> </ul>
Channel Speed	Channel Speed of this port <ul style="list-style-type: none"> <li>▪ 2 Gbps</li> <li>▪ 4 Gbps</li> <li>▪ 8 Gbps</li> <li>▪ 10 Gbps</li> <li>▪ 16 Gbps</li> <li>▪ 32 Gbps</li> <li>▪ Auto</li> </ul>
WWN	WWN of this port (hexadecimal number) Blank if "Package Type" is iSCSI

Item	Content
CHA Location	CHA on which the port is installed.
Package Type	CHA type for CHA Location <ul style="list-style-type: none"> <li>▪ Fibre: <ul style="list-style-type: none"> <li>• 16FC8 (Fibre )</li> <li>• 8FC16 (Fibre )</li> <li>• 16FC16 (Fibre)</li> </ul> </li> <li>▪ FCoE: <ul style="list-style-type: none"> <li>• 16FE10 (FCoE )</li> </ul> </li> <li>▪ iSCSI: <ul style="list-style-type: none"> <li>• 8IS10 (iSCSI)</li> </ul> </li> </ul>
T10 PI Mode	Indicates whether the T10 PI mode can be applied to the port. <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> <li>▪ Blank if "Package Type" is "8FC16(Fibre )" or "16FC16(Fibre)"</li> </ul>

### MfDMInfo.csv

This CSV file contains information about migration volumes for mainframe. A record is created for each migration volume.

**Table 20 MfDMInfo.csv file (Title: <<M/F DM Information>>)**

Item	Content
Migration Volume Group	Number of the migration volume The number starts with "M" (for example, M1-1)
Current MP Blade	Number and name of the MP Blade that is controlling the migration volume
Setting MP Blade	Number and name of the MP Blade specified to control the migration volume
Resource Group ID (ECC Group)	Resource group ID of migration volume (number in the decimal format)
Resource Group Name (ECC Group)	Resource group name of migration volume



**MicroVersion.csv**

This CSV file contains information about microcode versions.

**Table 21 MicroVersion.csv file (Title: <<Micro Version>>)**

Item	Content
DKCMAIN	The version of the microcode for the RAID storage system (10 digits)
HTP	HTP microcode version (6 digits)
DKAF	DKAF microcode version (6 digits)
SVP	The version of the microcode installed on the service processor (8 digits)
SSVP	SSVP microcode version (6 digits)
FCDG	FCDG microcode version (6 digits)
CUDG4	CUDG4 microcode version (6 digits)
ROM BOOT	ROM BOOT microcode version (6 digits)
RAM BOOT	RAM BOOT microcode version (6 digits)
CMBK	CMBK microcode version (6 digits)
Config	Config microcode version (8 digits)
HDD	HDD microcode version (4 digits) HDD version in the format of "(HDD device type - code):(version)." If an HDD drive is not installed, only a colon (:) is displayed.
HDD (SVP)	HDD(SVP) microcode version (4 digits)
Expander	Expander microcode version (6 digits)
CFM	CFM microcode version (8 digits)
Printout Tool	Printout tool version
Expander(FMU)	FMU Expander version (6 digits)
FCHF	FCHF version (6 digits)
BTCL	BTCL version (6 digits)
FOEF	FOEF version (6 digits)
FHTP	FHTP version (6 digits)
FFCDG	FFCDG version (6 digits)
ISCF	ISCF version (6 digits)

## MlcEnduranceInfo.csv

This CSV file contains information about endurance information of SSD or FMD. A record is created for each SSD or FMD endurance information.

If you change the SVP time 1 month or more, the history acquisition months will not be in order.

Item	Content
ECC Group	Number of parity group of which this SSD or FMD is a component
CR#	C# and R# (2-digit hexadecimal numbers), which identify the PDEV Output in the format of "XX/YY" XX: C# YY: R#
Device Type-Code	Drive type code of this drive Output example: SLR5B-M200SS
Used Endurance Indicator (%)	Current SSD life (0 to 100)
History1 (date)	Date on which SSD life was acquired (1 month ago) 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) 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.

Item	Content
System Option Mode#	System option mode # (decimal number)

Item	Content
LPR#0, LPR#1, ..., LPR#31	System option mode for LPR#0 to LPR#31 <ul style="list-style-type: none"> <li>▪ If the system option mode is on: On</li> <li>▪ If the system option mode is not on: Blank</li> </ul>

## MpPathStatus.csv

This CSV file contains information about the status of logical paths. A record is created for each MP blade or LR.

**Table 22 MpPathStatus.csv file (Title: <<MP Path Status>>)**

Item	Content
Module#	Module number.
MPB#/LR#	MP blade number or LR number <ul style="list-style-type: none"> <li>▪ For MP blade number MPB#00 to MPB#0f</li> <li>▪ For LR number LR#00 to LR#1f</li> </ul>
MPB#00-00, ..., MPB#00-0f, MPB#01-00, ..., MPB#01-0f, MPB#02-00, ..., MPB#02-0f, MPB#03-00, ..., MPB#03-0f	MP blade path status for MP blade number in the format of "MPB#XX-YY". <sup>1</sup> XX: MSW number in one module (2-digit number in the hexadecimal format) YY: MP blade number (2-digit number in the hexadecimal format)
LR#00-00, ..., LR#00-1f, LR#01-00, ..., LR#01-1f, LR#02-00, ..., LR#02-1f, LR#03-00, ..., LR#03-1f	LR path status for MP blade number in the format of "LR#XX-YY". <sup>1</sup> XX: MSW number in one module (2-digit number in the hexadecimal format) YY: LR number (2-digit number in the hexadecimal format)
CACHE#00-00, CACHE#00-07,	Cache package path status for MP blade number in the format of "CACHE#XX-YY". <sup>1</sup> XX: E path number (2-digit number in the hexadecimal format)

Item	Content
CACHE#01-00, CACHE#01-07	YY: Cache package number (2-digit number in the hexadecimal format)
CACHE#00-00, CACHE#00-07, CACHE#01-00, CACHE#01-07	Cache package path status for LR number in the format of "CACHE#XX-YY". <sup>1</sup>  XX: P path number (2-digit number in the hexadecimal format) YY: Cache package number (2-digit number in the hexadecimal format)
<b>Notes:</b>	
1. 1=Normal, 0=Abnormal	

### MpPcbStatus.csv

This CSV file contains information about the status of MP Blades. A record is created for each MP blade.

**Table 23 MpPcbStatus.csv file (Title: <<MP PCB Status>>)**

Item	Content
Module#	Module number
MP PCB Location	MP blade name
MP PCB ID	MP blade ID
Auto Assignment	Information about whether this MP blade is set to be automatically assigned to each resource or not <ul style="list-style-type: none"> <li>▪ Enabled Set to be automatically assigned</li> <li>▪ Disabled Not set to be automatically assigned</li> </ul>
PCB Status	MP blade status <sup>1</sup>
MP#00, #01, #02..., #07	MP status on MP blades #0 to #07 <sup>1</sup>
MP PCB Type	MP blade type  Output example: MPB1 or MPB2
<b>Notes:</b>	
1. 1=Normal, 0=Abnormal	

## PcbRevInfo.csv

This CSV file contains information about revisions of packages such as channel adapters (CHAs) and others. A record is created for each package.

**Table 24 PcbRevInfo.csv file (Title: <<PCB Revision Information>>)**

Item	Content
Module#	Module number
Cluster#	Cluster number
Location	Package name Output example: <ul style="list-style-type: none"> <li>▪ For CHA: CHA-1PC</li> <li>▪ For port: 1A</li> </ul>
Name	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

## PdevCapalInfo.csv

This CSV file contains information about physical device (PDEV) capacities. A record is created for each of the classifications shown in "PDEV Kind".

Item	Content
PDEV Kind	The following four classifications are output: <ul style="list-style-type: none"> <li>▪ OPEN System (TB)</li> <li>▪ Mainframe System (TB)</li> <li>▪ Total Capacity (TB)</li> <li>▪ Number of PDEVs</li> </ul>
SAS Drive	SAS drive capacity (TB)
Spare Drive	Spare drive capacity (TB)
SSD Drive	SSD capacity (TB)

## PdevInfo.csv

This CSV file contains information about physical devices (PDEVs). A record is created for each PDEV.

Item	Content
ECC Group	Number of parity group of which this PDEV is a component. <ul style="list-style-type: none"> <li>▪ Spare Drive: For spare drives</li> </ul>
Emulation Type	Emulation type for the parity group indicated by "ECC Group" <ul style="list-style-type: none"> <li>▪ Blank: "ECC Group" is Spare Drive.</li> </ul>
CR#	C# and R# (2-digit hexadecimal numbers), which identify the PDEV Output in the format XX/YY, where: <ul style="list-style-type: none"> <li>▪ XX: C#</li> <li>▪ YY: R#</li> </ul>
PDEV Location	PDEV location name
Module #	Module number
Device Type	Drive type <ul style="list-style-type: none"> <li>▪ SAS</li> <li>▪ SSD</li> </ul>
RPM	Revolutions per minute Blank displays as RPM when the drive is SSD.
Device Type-Code	Device type code of this drive Output example: DKR5D-J600SS
Device Size	Drive size (inches) <ul style="list-style-type: none"> <li>▪ 2.5</li> <li>▪ 3.5</li> <li>▪ Blank when DKU is FBX (FMC or FMD)</li> </ul>
Device Capacity	Drive capacity (GB or TB)
Drive Version	Drive firmware version (4-digit hexadecimal number)
DKA1	Name of the DKA (1) controlling the PDEV
DKA2	Name of the DKA (2) controlling the PDEV
Serial Number #	Serial number of this drive
RAID Level	RAID level of the parity group indicated by "ECC Group"

Item	Content
	Blank if the "ECC Group" is Spare Drive
RAID Concatenation #0	Number of parity group to be concatenated to parity group (#0) identified by "ECC Group" <sup>1</sup>
RAID Concatenation #1	Number of parity group to be concatenated to parity group (#1) identified by "ECC Group" <sup>1</sup>
RAID Concatenation #2	Number of parity group to be concatenated to parity group (#2) identified by "ECC Group" <sup>1</sup>
Resource Group ID (ECC Group)	Resource group ID of parity group (decimal number)
Resource Group Name (ECC Group)	Resource group name of parity group
Encryption	Encryption status of the parity group to which the PDEV belongs <ul style="list-style-type: none"> <li>▪ Enabled: Encryption enabled</li> <li>▪ Disabled: Encryption disabled</li> </ul>
Accelerated Compression	Accelerated compression setting. <ul style="list-style-type: none"> <li>▪ Enabled: accelerated compression is enabled.</li> <li>▪ Disabled: accelerated compression is disabled.</li> </ul> <p>If the parity group with PDEV does not support accelerated compression, or if the ECC Group is Spare Drive, a blank space is displayed.</p>
Automatically manage compressed space of FMD parity group	Indicates whether to manage the compressed area of the FMD parity group automatically. <sup>2</sup> <ul style="list-style-type: none"> <li>▪ Enabled: The area is managed automatically.</li> <li>▪ Disabled: The area is not managed automatically.</li> </ul>
<b>Notes:</b>	
<ol style="list-style-type: none"> <li>1. Blank if the parity group is not concatenated to another parity group or is Spare Drive.</li> <li>2. Blank if the parity group to which PDEV belongs does not support accelerated compression.</li> </ol>	

## PdevStatus.csv

This CSV file contains information about the status of physical devices (PDEVs). A record is created for each PDEV.

Item	Content
CR#	C# and R# (2-digit hexadecimal numbers), which identify the PDEV Output in the format XX/YY, where: <ul style="list-style-type: none"> <li>▪ XX: C#</li> <li>▪ YY: R#</li> </ul>
Pdev Status	PDEV status <sup>1</sup>
Port0 Status	Status of Port 0 on this PDEV <sup>1</sup>
Port1 Status	Status of Port 1 on this PDEV <sup>1</sup>
Pdev Location	Location name of this PDEV
<b>Notes:</b>	
1. 1=Normal, 0=Abnormal	

### PhyPathStatus.csv

This CSV file contains information about mainframe physical paths.

**Table 25 PhyPathStatus.csv file (Title: <<Main Frame Physical Path Status>>)**

Item	Content
Module#	Module number
CHA Location	CHA name
Port	Port name
Link(Self)	DKC port address (6-digit number in the hexadecimal format)
Link(Dest)	Link address of the adjacent node (6-digit number in the hexadecimal format)
Status	Information about whether the adjacent node is enabled: <ul style="list-style-type: none"> <li>▪ VALID (CUR)</li> <li>▪ INVALID</li> </ul>
Type/Model	Type of the adjacent node (6-digit number in the hexadecimal format) and model name of the adjacent node (3-digit number in the hexadecimal format)
SeqNumber	Serial product number of the adjacent node (14-digit number in the hexadecimal format)



Item	Content
Tag	Tag information of the adjacent node (4-digit number in the hexadecimal format)
WWN(N_Port_Name)	N_Port_Name of the adjacent node (16-digit number in the hexadecimal format)
WWN(Node_Name)	Node_Name of the adjacent node (16-digit number in the hexadecimal format)
Speed	Data transfer speed: <ul style="list-style-type: none"> <li>▪ 2 Gbps</li> <li>▪ 4 Gbps</li> <li>▪ 8 Gbps</li> </ul>

### PkInfo.csv

This CSV file contains information about channel adapters (CHAs). A record is created for each CHA.

**Table 26 PkInfo.csv file (Title: <<PK>>)**

Item	Content
Module#	Module number
CHA Location	CHA name
DKC Emulation	DKC emulation type
Port#	Number of the port installed on the CHA (2-digit number in the hexadecimal format)
Port	Name of port installed on the CHA
Package Type	CHA type CHA for mainframe systems: <ul style="list-style-type: none"> <li>▪ 16M8 (Mfibre)</li> <li>▪ 16M16 (Mfibre)</li> </ul>

Item	Content
	CHA for open systems: <ul style="list-style-type: none"> <li>▪ Fibre:               <ul style="list-style-type: none"> <li>• 16FC8 (Fibre )</li> <li>• 8FC16 (Fibre )</li> <li>• 16FC16 (Fibre)</li> </ul> </li> <li>▪ FCoE:               <ul style="list-style-type: none"> <li>• 16FE10 (FCoE )</li> </ul> </li> <li>▪ iSCSI:               <ul style="list-style-type: none"> <li>• 8IS10 (iSCSI)</li> </ul> </li> </ul>
SFP Kind	SFP (Small Form factor Pluggable) kind: <ul style="list-style-type: none"> <li>▪ Short Wave</li> <li>▪ Long Wave</li> </ul>
SFP Status	SFP status: <ul style="list-style-type: none"> <li>▪ Normal</li> <li>▪ Failed</li> <li>▪ Not Fix</li> </ul>
Port Type	Port type Output example: <ul style="list-style-type: none"> <li>▪ Initiator</li> <li>▪ Target</li> <li>▪ External</li> </ul>
Fabric	One of the Fibre topology settings indicating the setting status of the Fabric switch (output only for an open system CHA that is Fibre or FCoE): <ul style="list-style-type: none"> <li>▪ On</li> <li>▪ Off</li> </ul>
Connection	One of the Fibre topology settings (output only for an open system CHA that is Fibre or FCoE) <ul style="list-style-type: none"> <li>▪ Point to Point</li> <li>▪ FC-AL</li> </ul>
Port Address	Port address (2-digit number in the hexadecimal format) Output only for an open system CHA that is Fibre or FCoE

Item	Content
Resource Group ID (Port)	Resource group ID of port (number in the decimal format)
Resource Group Name (Port)	Resource group name of port
Port Internal WWN	WWN of the port (output only for an open system CHA that is Fibre or FCoE)
T10 PI Mode	Indicates whether the T10 PI mode can be applied to the port. <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> <li>▪ Blank if "Package Type" is "8FC16(Fibre )" or "16FC16(Fibre)"</li> </ul>

## 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 \(on page 128\)](#).

Item	Content
Program Product Name	Software name.
Install	Information about whether the installed license key is enabled or not <ul style="list-style-type: none"> <li>▪ Enabled: Installed and the software can be used</li> <li>▪ Disabled: Installed but the software cannot be used</li> </ul>
Key Type	Installed license key type <ul style="list-style-type: none"> <li>▪ Permanent</li> <li>▪ Temporary</li> <li>▪ Emergency</li> <li>▪ Term</li> </ul> If no license key is installed, "Not Installed" is output.
Permitted Volumes(TB)	Permitted volume capacity for this software (in TB) <sup>1</sup> If no upper limit value is set for the capacity, "Unlimited" is output.
Expiration Date	Expiration date of the software. The format is <i>mm/dd/yyyy</i> (Month/Day/Year).

Item	Content
Status	License key status of the software <ul style="list-style-type: none"> <li>▪ Installed</li> <li>▪ Not Enough License</li> <li>▪ Grace Period</li> <li>▪ Expired</li> <li>▪ Not Installed</li> <li>▪ Installed (Disabled)</li> </ul>
<b>Notes:</b> 1. The used volume capacity is not output.	

### SMfundat.csv

This CSV file contains information about SM functions. A record is created for each of the classifications shown in "SM Install Function".

Item	Content
SM Install function	The following classifications are output <sup>1</sup> : <ul style="list-style-type: none"> <li>▪ Base(16KLDEV/SI/VM/DP/TI/FC)</li> <li>▪ 64KLDEV Extension</li> <li>▪ TC/UR/GAD</li> <li>▪ HDT/Active Flash</li> <li>▪ DP/HDT/Active Flash/TI Extension1</li> <li>▪ DP/HDT/Active Flash/TI Extension2</li> <li>▪ DP/HDT/Active Flash/TI Extension3</li> </ul>
Availability	Information about whether the function of "SM Install function" is enabled <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> </ul>

Item	Content
<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>The following values are output: <ul style="list-style-type: none"> <li>Active Flash: active flash</li> <li>DP: Dynamic Provisioning</li> <li>FC: Compatible FlashCopy®</li> <li>GAD: global-active device</li> <li>HDT: Dynamic Tiering</li> <li>SI: ShadowImage</li> <li>TI: Thin Image</li> <li>TC: TrueCopy</li> <li>TPF: Transaction Processing Facility</li> <li>UR: Universal Replicator</li> <li>VM: Volume Migration</li> </ul> </li> </ol>	

### SsdDriveInfo.csv

This CSV file contains information about SSDs. A record is created for each SSD.

Item	Content
ECC Group	Number of the parity group of which this SSD is a component.
CR#	C# and R# (2-digit hexadecimal numbers), which identify the PDEV Output in the format XX/YY, where: <ul style="list-style-type: none"> <li>XX: C#</li> <li>YY: R#</li> </ul>
PDEV Location	Location name of the PDEV Output example: SLR5B-M200SS
Device Type-Code	Drive type code Output example: SLR5B-M200SS
Device Capacity	Drive capacity in GB or TB
SSD Device Type	SSD drive type <ul style="list-style-type: none"> <li>MLC</li> <li>FMD</li> </ul>

Item	Content
	<ul style="list-style-type: none"> <li>▪ FMC</li> <li>▪ FMD-HDE</li> </ul>
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) Blank if SSD is other than FMD
FMD Battery Life Indicator (%)	Used battery life (0 to 100) Blank if SSD is other than FMD

### SsidInfo.csv

This CSV file contains information about SSIDs. A record is created for each SSID.

Item	Content
DEV# Start	First LDEV number for the SSID
DEV# End	Last LDEV number for the SSID
SSID	Subsystem ID (hexadecimal)

### SysoptInfo.csv

This CSV file contains information about system options.

Item	Content
Spare Disk Recover	Speed of copying data to the spare drive. <ul style="list-style-type: none"> <li>▪ Interleave mode</li> <li>▪ Full Speed mode</li> </ul>

Item	Content
Dynamic Sparing	Information about whether to perform automatic copy to a spare drive if the occurrences of drive failures exceed the threshold. <ul style="list-style-type: none"> <li>▪ On</li> <li>▪ Off</li> </ul>
Correction Copy	Information about whether to perform correction copy to a spare drive if a drive is blocked. <ul style="list-style-type: none"> <li>▪ On</li> <li>▪ Off</li> </ul>
Disk Copy pace	Speed of copying the spare drive in the Interleave mode. <ul style="list-style-type: none"> <li>▪ Faster</li> <li>▪ Medium</li> <li>▪ Slower</li> </ul>
System Option On	System options that are set to ON. Output example: modeXXXX (0 to 2047, decimal number)
Link Failure Threshold	Threshold to notify the link failure (0 to 255, decimal)
WDCP Enable	Information about whether the WDCP option is set or not. Output only in cases where the Config type is H. <ul style="list-style-type: none"> <li>▪ On</li> <li>▪ Off</li> </ul>
DDUMP Enable	DDUMP Enable Information about whether the DDUMP option is set or not. Output only in cases where the Config type is H. <ul style="list-style-type: none"> <li>▪ On</li> <li>▪ Off</li> </ul>

## 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 for Open Systems*. For information about iSCSI hosts, see *IscsiHostInfo.csv*. For information about iSCSI targets, see *IscsiTargetInfo.csv*.

**Table 27 WwnInfo.csv file (Title: <<World Wide Name Information>>)**

Item	Content
Port	Port name

Item	Content
Host Group	Host group name If "Package Type" is iSCSI, the iSCSI target alias is output.
Host Mode	Host mode that is set for the host group (number in hexadecimal format)
Host Mode Option	Host mode option that is set for the host group (number in the hexadecimal format) Multiple options are separated by semicolons.
WWN	World Wide Name of the host bus adapter registered to the host group (number in hexadecimal format) Blank if Package Type is iSCSI.
Nickname	Nickname of the host Blank if Package Type is iSCSI.
Host Group#	Host group number (hexadecimal) If "Package Type" is iSCSI, the iSCSI target alias is output.
CHA Location	CHA on which the port is installed
Package Type	CHA type for CHA Location <ul style="list-style-type: none"> <li>▪ Fibre: <ul style="list-style-type: none"> <li>• 16FC8 (Fibre )</li> <li>• 8FC16 (Fibre )</li> <li>• 16FC16 (Fibre)</li> </ul> </li> <li>▪ FCoE: <ul style="list-style-type: none"> <li>• 16FE10 (FCoE )</li> </ul> </li> <li>▪ iSCSI: <ul style="list-style-type: none"> <li>• 8IS10 (iSCSI)</li> </ul> </li> </ul>
T10 PI Mode	Indicates whether the T10 PI mode can be applied to the port. <ul style="list-style-type: none"> <li>▪ Enabled</li> <li>▪ Disabled</li> <li>▪ Blank if "Package Type" is "8FC16(Fibre )" or "16FC16(Fibre)"</li> </ul>



---

## Chapter 8: Troubleshooting

Troubleshooting for Device Manager - Storage Navigator involves identifying the cause of the error and resolving the problem.

This section provides information for identifying and correcting problems with Device Manager - Storage Navigator for your storage system.

### Getting help

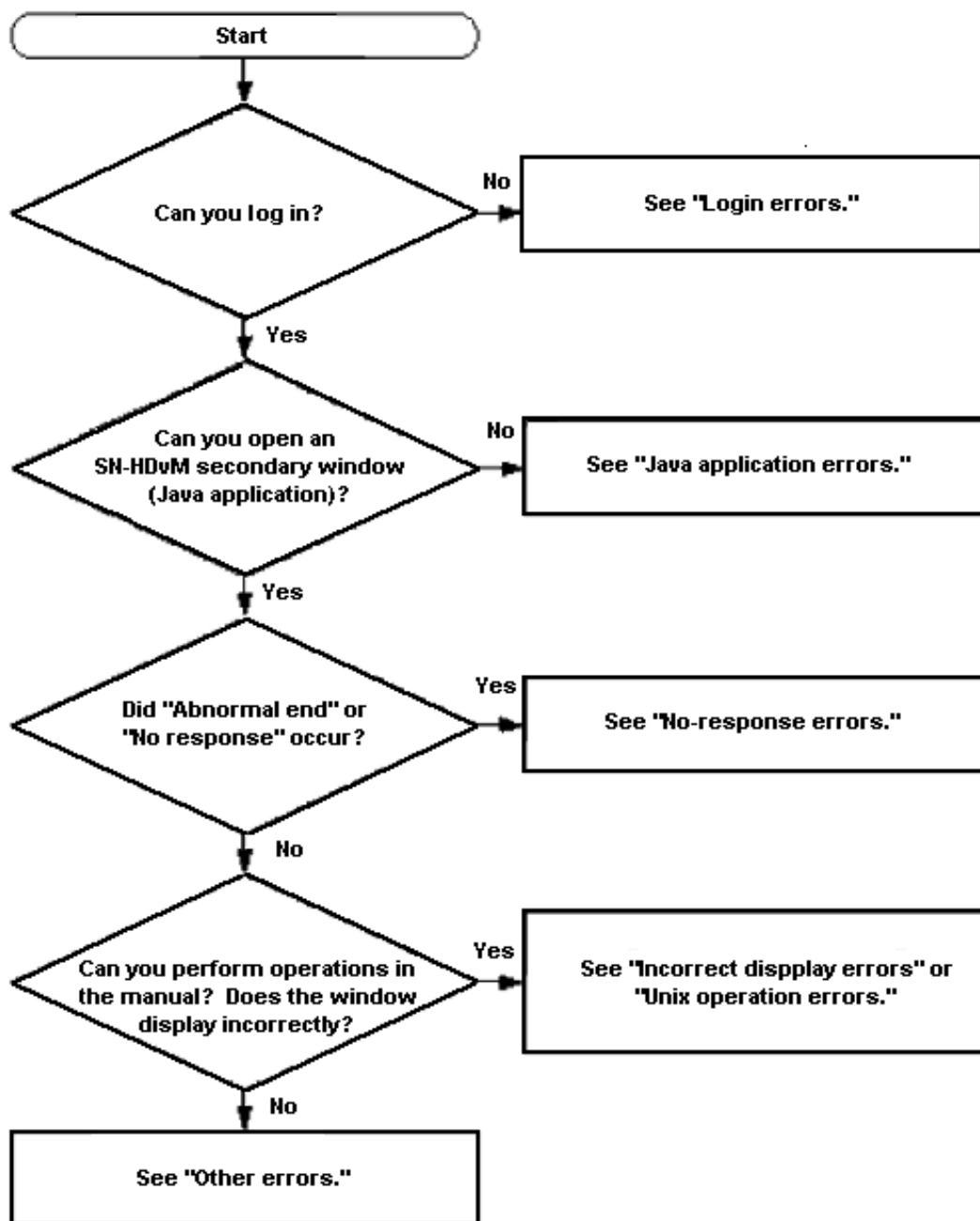
If you have difficulty with any of the procedures included in this chapter, or if a procedure does not provide the answer or results you expect, contact Hitachi Vantara support. See Getting Help in the preface of this manual.

### General troubleshooting

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

- Check the cabling and the LAN. Verify that both the management client and LAN cabling are firmly attached, and that the LAN is operating properly.
- Reboot the management client. Close any programs that are not responding. If necessary, reboot the management client and restart a Device Manager - Storage Navigator web client session.
- Check for any general error conditions. For a complete list of Device Manager - Storage Navigator error codes, see the *Hitachi Device Manager - Storage Navigator Messages*.
- Check the alert icon. Confirm the severity level of the storage system alert by clicking Alert in the Device Manager - Storage Navigator main window. If you cannot resolve an error condition, contact customer support.

The following illustration shows the workflow for troubleshooting:

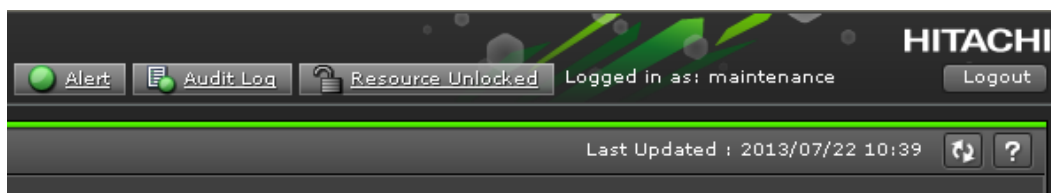


## Monitoring SIMs alerts in Device Manager - Storage Navigator

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

### Procedure

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



2. To check the details of each alert, select and right-click one row, and then click **Detail** in the pop-up menu. The detail dialog box opens.
3. If the following SIM reference codes appear (see table below), you must resolve the error.

Reference code	Program product
601xxx*	Thin Image
602xxx*	
602ffe	
620xxx*	Dynamic Provisioning
621xxx*	Dynamic Provisioning for Mainframe
622xxx*	
624000	Thin Image Dynamic Provisioning Dynamic Provisioning for Mainframe
625000	Dynamic Provisioning
626xxx*	Dynamic Provisioning for Mainframe
641xxx*	Dynamic Tiering Dynamic Tiering for Mainframe
*xxx indicates a pool number. Pool numbers are decimal and displayed on the <b>Alert Properties</b> window.	

For details on how to resolve the error, see the *Hitachi Thin Image User Guide*, the *Provisioning Guide for Open Systems*, or the *Provisioning Guide for Mainframe Systems*.

## Login errors

The following table lists login errors:


Error condition	Probable cause / Recommended action
Failed to login is displayed.	<p>Check that the user name and password are correct. If you forget your password, log in with the Security Administrator (View &amp; Modify) and set a new password.</p> <p>When you are using an external authentication server such as LDAP, check the following:</p> <ul style="list-style-type: none"> <li>▪ The authentication server has been started.</li> <li>▪ The authentication server can be accessed from the SVP via the network</li> <li>▪ The user account has been established on the authentication server</li> <li>▪ The connection information for the authentication server that has set on the SVP is correct.</li> </ul> <p>If the symptom recurs even after you correct the above settings, use the dump tool to collect Device Manager - Storage Navigator normal dump files to some recording media and then contact customer support.</p>
The page is not displayed because of an invalid syntax error.	Enter the URL of the desired SVP in the Trusted sites section of the <b>Internet Options</b> dialog box.
The Device Manager - Storage Navigator window is not displayed.	Make sure that the TLS setting of SVP and that of the browser are correct.
Device Manager - Storage Navigator does not start even with repeated attempts.	<p>Close all the web browser windows and then clear the web browser cache.</p> <p>Use the Task Manager to check for "hung" or duplicate processes.</p>
A network error occurred when you logged in to Device Manager - Storage Navigator.	Close all dialog boxes and log in to the Device Manager - Storage Navigator again. If the same error occurs, check the network environment.
The login to a storage system from the Hitachi Command Suite server fails	If you change your password for a storage system, you need to change the information registered in Hitachi Command Suite. For details, see the section describing how to change storage system settings in the Hitachi Command Suite User Guide.
The login window is not displayed.	You might be using Internet Explorer 11 with Adobe Flash Player version 10 or earlier. Update Adobe Flash Player if needed.

## No-response errors

The following table lists no-response errors:



Error condition	Probable cause / Recommended action
<p>The following error occurs when using Device Manager - Storage Navigator:</p> <ul style="list-style-type: none"> <li>▪ 20121-107024</li> </ul>	<p>The SVP web server might have been restarted. Close Device Manager - Storage Navigator, wait 10 minutes, and then restart Device Manager - Storage Navigator.</p>
<p>Error (20121-107096) occurs repeatedly while you are using Device Manager - Storage Navigator.</p>	<p>A timeout error may have occurred in Adobe Flash Player.</p> <p>Close the Device Manager - Storage Navigator window. Click X in the corner of the browser window or click the window and press <b>Alt+F4</b>.</p>
<p>The following errors occur when using Device Manager - Storage Navigator:</p> <ul style="list-style-type: none"> <li>▪ 20121-107024</li> <li>▪ 20121-107025</li> <li>▪ 20121-107096</li> <li>▪ 20121-107097</li> </ul>	<p>This error may occur if the load to the management client is high, or if you start multiple instances of Device Manager - Storage Navigator by using multiple tabs in a tab browser or multiple browsers.</p> <p>Close the other applications which cause the high load, or make sure to start only one Device Manager - Storage Navigator</p>
<p>The following application error occurs when using Device Manager - Storage Navigator:</p> <ul style="list-style-type: none"> <li>▪ 20020-108000</li> </ul>	<ul style="list-style-type: none"> <li>▪ The version of Device Manager - Storage Navigator installed on the management client might not match the SVP version. Close all the browser windows and then clear the browser cache.</li> <li>▪ The management client might have entered standby or hibernate mode. Restart Device Manager - Storage Navigator.</li> </ul>

Error condition	Probable cause / Recommended action
	<ul style="list-style-type: none"> <li>▪ If a proxy server is used for network connections, the proxy server cache may be storing the older version of the program. If the problem continues after you clear the browser cache, contact your network administrator.</li> <li>▪ Java content might be disabled in the web browser using the JRE 7.0 Update 10 or later. To enable Java content in the web browser: <ol style="list-style-type: none"> <li>1. From Windows, open the Java Control Panel.</li> <li>2. In the Java Control Panel, click the Security tab.</li> <li>3. If Enable Java content in the browser is checked, uncheck it and click Apply.</li> <li>4. The <b>User Account Control</b> dialog box opens. Click Yes. The confirmation window opens. Click OK.</li> <li>5. Restart the browser.</li> </ol> </li> </ul> <p>If none of the above actions solve the problem, save the Device Manager - Storage Navigator dump file and send it to customer support. Then restart the web browser.</p>
<p>Device Manager - Storage Navigator does not respond.</p> <p>Device Manager - Storage Navigator may hang in the following cases:</p> <ul style="list-style-type: none"> <li>▪ The Device Manager - Storage Navigator main window is grayed out and does not display the percentage of progress, and you cannot perform any operation for a long period of time.</li> <li>▪ You cannot perform any operation for a long period of time and the dialog box that says <b>Loading...</b> is not displayed.</li> <li>▪ The dialog box that says <b>Loading...</b> opens when the window switches. However, you cannot move the dialog box or perform any operation for a long period of time.</li> <li>▪ The login window does not appear and the white screen continues.</li> </ul>	<p>Close the web browser and reopen it. When using the Device Manager - Storage Navigator secondary window, exit Device Manager - Storage Navigator by pressing <b>Ctrl+Alt+Shift+D</b> all at once.</p> <p>If you close the web browser but you cannot exit Device Manager - Storage Navigator, reboot the management client or restart Device Manager - Storage Navigator after forcibly closing Device Manager - Storage Navigator as follows:</p> <ul style="list-style-type: none"> <li>▪ In Windows: <p>Exit the web browser and then use the Task Manager to terminate iexplorer.exe (if you are using Internet Explorer) or chrome.exe (if you are using Google Chrome).</p> </li> <li>▪ In UNIX: <p>Exit the web browser, and then terminate firefox-bin with the kill command.</p> </li> <li>▪ If the problem continues, ask your maintenance personnel to restart the SVP.</li> </ul>

Error condition	Probable cause / Recommended action
A network error occurred. There is no response to any operation even after 30 minutes.	Restart the management client. An operation may take over 30 minutes depending on the use condition. For example, when several Device Manager - Storage Navigator web clients are running, an operation may take a long time.
An internal error occurs, or a web browser ended abnormally.	Close all dialog boxes and log in to Device Manager - Storage Navigator again. If the same error occurs, restart the management client.
During a Device Manager - Storage Navigator operation, the web browser suddenly disappears.	Restart the management client.
An error (1-4011) occurs while you are using Device Manager - Storage Navigator.	The clock time of the management client may have been changed. Log in to Device Manager - Storage Navigator again.
The management client reboots on its own.	Restart the management client.
A Device Manager - Storage Navigator window is forcibly closed during a time-consuming process, such as LDEV formatting.	Close all windows, wait until processing finishes, and then restart Device Manager - Storage Navigator.
<p>A Device Manager - Storage Navigator window is incorrectly closed when you do one of the following:</p> <ul style="list-style-type: none"> <li>▪ Click </li> <li>▪ Use commands such as File &gt; Close on the web browser</li> <li>▪ Press the <b>Alt</b> and <b>F4</b> keys</li> </ul>	Restart Device Manager - Storage Navigator. If you cannot log in, wait for one minute and try again.
During a Device Manager - Storage Navigator operation, an add-on (Flash10e.ocx) error occurs.	Restart the management client. If this error occurs repeatedly, reinstall Adobe Flash Player on the management client.
When you log out from the Device Manager - Storage Navigator, an Internet Explorer error occurs.	<p>The probable causes are as follows:</p> <ul style="list-style-type: none"> <li>▪ Internet Explorer has not been updated. Install the latest updates</li> <li>▪ Internet Explorer may be configured incorrectly. Re-install Internet Explorer.</li> </ul>

Error condition	Probable cause / Recommended action
<p>When you click File &gt; Refresh All or Refresh in the Device Manager - Storage Navigator main window, the percentage of progress remains 99%.</p>	<p>The probable causes are as follows:</p> <ul style="list-style-type: none"> <li>▪ Another application such as Command Control Interface may be changing configuration. The window will be updated shortly after the configuration change ends.</li> <li>▪ Volume Migration operations, Quick Restore operations or Thin Image operations may be in progress. The window will be updated shortly after the operations end.</li> </ul>
<p>One of the following errors occurred during a Device Manager - Storage Navigator operation in the main window</p> <ul style="list-style-type: none"> <li>▪ 20123-107027</li> <li>▪ 20123-108004</li> <li>▪ 00002-058578</li> <li>▪ 00003-002003</li> <li>▪ xxxxx-065740</li> <li>▪ xxxxx-068800</li> </ul> <p>where xxxxx indicates any code.</p>	<ul style="list-style-type: none"> <li>▪ Another application such as Command Control Interface may be changing configuration.</li> <li>▪ Volume Migration operations, Quick Restore operations, or Thin Image operations may be in progress.</li> <li>▪ The configuration data may not be matched if a communication error occurs between the storage system and SVP.</li> </ul> <p>Wait a few minutes and then click File &gt; Refresh All to reload the configuration information. Then run Device Manager - Storage Navigator again.</p> <p>When using Encryption License Key or FMD Encryption License Key:</p> <ul style="list-style-type: none"> <li>▪ If a failure (00002-058578) occurs when you set the Encryption Environment for the first time from the <b>Edit Encryption Environmental Settings</b> window, do the following: <ol style="list-style-type: none"> <li>1. Wait a few minutes and then click File &gt; Refresh All to reload the configuration information.</li> <li>2. Initialize the Encryption Environment Settings.</li> <li>3. Set the Encryption Environment again.</li> </ol> </li> <li>▪ If a failure (00002-058578) occurs when you set the Encryption Environment again from the <b>Edit Encryption Environmental Settings</b> window, do the following: <ol style="list-style-type: none"> <li>1. Wait a few minutes and then click File &gt; Refresh All to reload the configuration information.</li> <li>2. Set the Encryption Environment again.</li> </ol> </li> </ul>




Error condition	Probable cause / Recommended action
<p>The Device Manager - Storage Navigator window turns white and the icon shown below displays in the center of the web browser when you use Device Manager - Storage Navigator.</p> <p>If you are using Internet Explorer: </p> <p>If you are using Google Chrome: </p>	<p>Restart the management client.</p>
<p>Operations cannot be performed due to a problem with the Device Manager - Storage Navigator main window. For example, tables are not displayed correctly or some buttons are not displayed. Logging out and back in does not solve the problem.</p>	<p>The Device Manager - Storage Navigator window setting information may have been saved with an incorrect value. Click Settings &gt; Environmental Settings &gt; Reset View to Settings in the Device Manager - Storage Navigator main window to clear the window setting information. Then click any button in the Device Manager - Storage Navigator window and check that it operates correctly. You do not need to log out and back in.</p>
<p>Device Manager - Storage Navigator closes automatically when operating the IPv6 address setting from Device Manager - Storage Navigator.</p>	<p>When the symptom occurs, the resource group status remains locked.</p> <p>Open the <b>Resource Lock Properties</b> window and release the locked resource group caused by the symptom. Suspend other operations when releasing the resource group, as other resource groups are also released the lock. See <a href="#">Resource Lock Properties window (on page 393)</a>.</p>

## Incorrect display errors

The following table lists incorrect display errors:

Error condition	Probable cause / Recommended action
A question mark or icon displays in a table or other area of the window.	<ul style="list-style-type: none"> <li>▪ When the question mark appears in the <b>View Tier Properties</b> window, see the topic describing this window in the <i>Provisioning Guide for Open Systems</i>. If the problem still persists, contact customer support.</li> <li>▪ When the question mark appears in the <b>Add External Volumes</b> window, see the topic describing this window in the <i>Hitachi Universal Volume Manager User Guide</i>. If the problem still persists, contact customer support.</li> <li>▪ If the question mark or icon appears in another window, update the window. Contact customer support if the question mark remains after you update the window.</li> </ul>
The product name, vendor name, and function name displayed in Device Manager - Storage Navigator are incorrect.	Contact customer support.
A part of the Device Manager - Storage Navigator window is not displayed.	You may be using the zoom in and zoom out function of the web browser. Do not use this function of the web browser when using Device Manager - Storage Navigator.
The display on Device Manager - Storage Navigator's main window is not updated to the latest information. "Last Updated" on Device Manager - Storage Navigator's main window is not updated.	Volume Migration operations, Quick Restore operations, or Thin Image operations may be in progress. The window will be updated shortly after the operations end.
<p>The following message is displayed when connected to Device Manager - Storage Navigator on Internet Explorer or Google Chrome.</p> <p>This content requires Adobe Flash Player.</p> <ul style="list-style-type: none"> <li>▪ Get and install Adobe Flash Player from the Adobe web site.</li> <li>▪ Enable Adobe Flash Player.</li> <li>▪ Adjust the browser security settings.</li> </ul>	<p>This message displays when Adobe Flash Player is not installed. Do the following:</p> <ul style="list-style-type: none"> <li>▪ Install Adobe Flash Player</li> <li>▪ Disable ActiveX Filtering</li> </ul>

Error condition	Probable cause / Recommended action
	<p>If you are using Internet Explorer 9 or later, click  Tools &gt; Safety and uncheck ActiveX Filtering.</p> <ul style="list-style-type: none"> <li>▪ When a message appears indicating that the specific site was blocked, perform the procedure described in <a href="#">Adding your SVP to the trusted sites zone for Windows Server computers (on page 25)</a>.</li> <li>▪ Do not change the local storage area value in Adobe Flash Player.</li> <li>▪ Do not disable Adobe Flash Player because Adobe Flash Player is necessary for Device Manager - Storage Navigator and works as an add-on to a web browser. If you use Internet Explorer, do not change the settings in Tools &gt; Manage add-ons.</li> </ul>
<p>When many items are set, some items might not be displayed even if you scroll through the table.</p>	<p>Depending on the size of a window, some items in a table might not be displayed. Do the following:</p> <ul style="list-style-type: none"> <li>▪ Increase the resolution so that more areas of the table can be shown.</li> <li>▪ Use the zoom in or zoom out function of your browser to adjust the viewing area.</li> </ul> <p><b>Note:</b> Text might become too small.</p> <p>If you still cannot solve the problem, contact customer support.</p>

Error condition	Probable cause / Recommended action
The Tools panel of Google Chrome is not displayed correctly in Japanese.	<p>Click the Chrome menu &gt; Settings &gt; Show advanced settings &gt; Languages &gt; Language and input settings.</p> <ol style="list-style-type: none"> <li>1. If you do not have Japanese in the list, click Add to add Japanese.</li> <li>2. From the list, select Japanese, and then click Display Google Chrome in this language &gt; Done.</li> <li>3. To apply the changes, close all Google Chrome windows.</li> <li>4. Click the Chrome menu &gt; Settings &gt; Show advanced settings &gt; Languages &gt; Language and input setting.</li> <li>5. In the languages list, select another language. Click the x symbol which is displayed when you select another language to delete the selected language. Delete all languages except Japanese.</li> <li>6. Click Done to close the window.</li> </ol>
The message "Unable to launch the application" appears on the secondary window, then operation ends abnormally.	<p>Perform the following:</p> <p>To disable TLSv1.0 and TLSv1.1 communications, using JRE 8 or later is recommended. If you use JRE 8, Solaris is not supported.</p> <p>Confirm Use TLS 1.2 for Java is enabled.</p>

## UNIX operation errors

The following table lists UNIX operation errors:

Error condition	Probable cause / Recommended action
<p>The web browser is incorrectly displayed because GUI items, such as labels and icons, cannot be loaded properly.</p> <p>Part of a button is outside the window.</p>	<p>If you use Device Manager - Storage Navigator on the Japanese version of Firefox, log out of Device Manager - Storage Navigator, and then log in to Device Manager - Storage Navigator again. Enter the following commands using the X Server Emulator.</p> <ul style="list-style-type: none"> <li>▪ B Shell:</li> </ul> <pre>LANG=C</pre>

Error condition	Probable cause / Recommended action
	<pre>export LANG</pre> <ul style="list-style-type: none"> <li>C Shell:</li> </ul> <pre>setenv LANG C</pre>
The web browser closes abnormally.	This problem can occur if a Mozilla process keeps running after Mozilla stops responding. Delete the "java_vm" and "mozilla" processes and continue with Device Manager - Storage Navigator operations.

## Other errors

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

Error condition	Probable cause / Recommended action
<ul style="list-style-type: none"> <li>Error about insufficient capacity when creating an LDEV with sufficient capacity.</li> <li>Operation error about an LDEV that does not exist when creating a pair for an LDEV that does exist.</li> </ul>	<p>Configuration information displayed in Device Manager - Storage Navigator and controller configuration information might not match.</p> <p>Click File &gt; Refresh All in the Device Manager - Storage Navigator main window to reload configuration information.</p> <p>If the problem persists, contact customer support.</p>
The microcode on the SVP is upgraded or downgraded.	Close all Device Manager - Storage Navigator windows, and then clear the browser cache. Even when you are not sure that the microcode on the SVP is upgraded or downgraded, clear the browser cache.
Device Manager - Storage Navigator processing is temporarily delayed.	Internal processing (such as, configuration change, P.P. check, or operational information acquisition) might be running on the SVP.
Device Manager - Storage Navigator processing is delayed.	<p>The local storage value for Adobe Flash Player might decrease. Follow these steps:</p> <ol style="list-style-type: none"> <li>Right-click on the Device Manager - Storage Navigator main window and click Settings to open the <b>Adobe Flash Player Settings</b> window.</li> <li>In the local storage settings, move the slider until Unlimited appears and then click Close.</li> </ol>

Error condition	Probable cause / Recommended action
	<ol style="list-style-type: none"> <li>3. Close Device Manager - Storage Navigator.</li> <li>4. Restart Device Manager - Storage Navigator.</li> <li>5. If the local storage confirmation dialog box appears, click Allow.</li> </ol>
Installing of signed SSL certificate fails.	The passphrase for the SSL certificate might be set. Release the passphrase. If needed, see <a href="#">Releasing an SSL certificate passphrase (on page 79)</a> .
You cannot resolve an error condition.	<p>Do the following, and then contact the customer support.</p> <ol style="list-style-type: none"> <li>1. Copy the Device Manager - Storage Navigator detailed dump files onto recording media using the Dump tool.</li> <li>2. Obtain the Java log and trace files.</li> </ol>

## Clearing the cache in Internet Explorer

If an error occurs in Device Manager - Storage Navigator, try clearing the web browser cache to solve the problem.



**Note:** These instructions are for IE8 on Windows 7. If you are using a different version, the labels in windows might be different.

### Procedure

1. Click **Tools > Internet Options**.
2. On the **General** tab, under **Browsing history**, click **Delete**.

This will delete the temporary internet files, history, cookies, saved passwords, and web form information.

## Clearing the cache in Firefox

If an error occurs in Device Manager - Storage Navigator, try clearing the web browser cache to solve the problem.



**Note:** These instructions are for Firefox version 35 on Windows 7. If you are using a different version, the labels in windows might be different.

### Procedure

1. Click **Tools > Options**.

2. In the **Options** window, click **Advanced**.
3. On the **Network** tab, under **Cached Web Content**, click **Clear Now**.

## Enabling JavaScript for Windows

When using Internet Explorer for the secondary window, you might need to enable JavaScript.

If you use Windows 8.1, Windows Server 2012, or Windows Server 2012 R2, enable JavaScript.

### Procedure

1. Launch Internet Explorer.
2. From Internet Explorer's menu bar, click **Tools > Internet Options > Security**. The **Internet Options** window opens.
3. Click the **Security** tab. The **Security** window opens.
4. Click **Custom Level**. The **Security Settings** window opens.
5. Set **Active scripting** to **Enable**.
6. Click **OK**.
7. When the **Warning** dialog box appears, click **YES**.
8. Click **OK** to close the **Internet Options** window.
9. Restart Internet Explorer.

## Firefox web browser problems on UNIX

Note the following when using Firefox web browser on UNIX:

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

In a B Shell, enter the following command:

```
LANG=C
export LANG
```

In a C Shell, enter the following command:

```
setenv LANG C
```

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

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

In Firefox, when you click Logout at the upper right corner of the Device Manager - Storage Navigator main window, the Device Manager - Storage Navigator login window appears after you logout. With Internet Explorer, the window closes after the logout.

## Downloading dump files using the Dump tool

Use the Dump tool to download dump files onto a Device Manager - Storage Navigator computer. 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 Hitachi Vantara support personnel.
- check system configuration. First click File > Refresh All to update the configuration information, and then use the Dump tool to download dump files.

### Before you begin

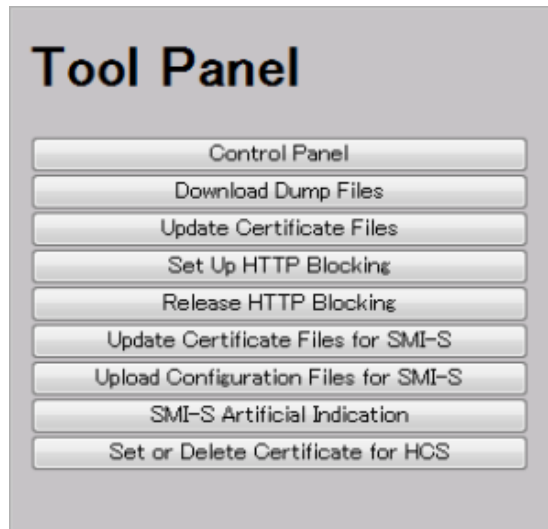
- All other users (including the SVP user) must stop using the Dump tool.
- Stop all maintenance operations.
- You must have Support Personnel role to log in.

### Procedure

1. Start a web browser and specify the following URL to open the Tool Panel:

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





2. Click **Download Dump Files**. The **Login** dialog box opens.
3. Enter the user ID and password and click **Login**. The **Download Dump Files** dialog box opens.
4. Select a file that you want to download.
  - **Existing Dump Files** indicates the last dump file that you downloaded. Select this when you want to re-download a previously downloaded dump file. If you have not downloaded any dump files from the Tool Panel, this item does not display even if you have acquired a dump file via SVP.
  - **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.
  - **Detail Dump (for DKC Performance)** contains the I/O-performance-related information. This includes performance monitor collection information, in addition to information applicable to Detail Dump. Choose **Detail Dump (for DKC Performance)** to check for I/O performance problems.
 

Note that while processing takes place, DKC I/O performance may be affected. During processing, you cannot use Device Manager - Storage Navigator to change the system configuration or perform SVP maintenance operations.
5. Click **Next**. A message appears confirming the execution of compression of the dump files.
6. Click **OK**. File compression processing starts. When the file is compressed, the **Download Dump Files** dialog box opens for the download.
7. Click **Download**. The **File Download** dialog box opens.
8. On the **File Download** dialog box, click **Save this file to disk**, and then click **OK**. The **Save As** dialog box opens.

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

## Troubleshooting the SMI-S function

If you cannot access the SMI-S function, check the network environment and access destination. If access cannot be made even though there is no problem with the network environment and access destination, contact customer support.

The SMI-S certificate might have expired when you receive a storage system. If so, you must upload a new signed certificate to the SMI-S provider. Follow the procedure on [Uploading a signed certificate to the SMI-S provider \(on page 93\)](#).

## SMI-S artificial indication errors

The following table lists SMI-S artificial indication errors:

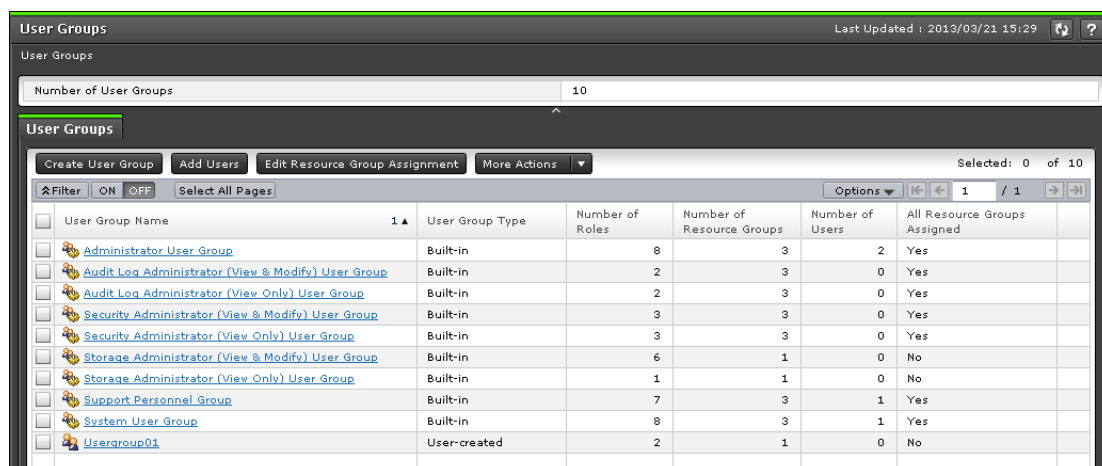
Error condition	Probable cause / Recommended action
The user ID or the password is not valid. (00190 77302)	User ID or password is invalid. Enter the correct user ID or password, and then retry the operation.
An error occurred during the listener information acquisition. (00190 77303)	An error occurred during the listener information acquisition. Collect Device Manager - Storage Navigator normal dump file to the media using the dump tool.
No listeners are subscribed to the provider. (00190 77304)	The listeners are not subscribed to the SMI-S provider. Have the listeners subscribe to the provider, and retry.
The artificial indication cannot be sent to some listeners. (00190 77305)	The artificial indication cannot be sent to some listeners. Use the dump tool to collect and save Device Manager - Storage Navigator normal dump files. Then contact the customer support.
A time-out error occurred. (00190 77306)	Send the artificial indication again. If this problem persists, use the dump tool to collect Device Manager - Storage Navigator normal dump files to some recording media and then contact the customer support.
An internal error occurred. (00190 77307)	Use the dump tool to collect Device Manager - Storage Navigator normal dump files to some recording media and then contact the customer support.

# Appendix A: Device Manager - Storage Navigator user management GUI reference

This section describes the Device Manager - Storage Navigator windows and wizards that you use to manage user security and to set up and manage user accounts on your storage system.

## User Groups window

This window lists all user groups created in Device Manager - Storage Navigator.



User Group Name	User Group Type	Number of Roles	Number of Resource Groups	Number of Users	All Resource Groups Assigned
Administrator User Group	Built-in	8	3	2	Yes
Audit Log Administrator (View & Modify) User Group	Built-in	2	3	0	Yes
Audit Log Administrator (View Only) User Group	Built-in	2	3	0	Yes
Security Administrator (View & Modify) User Group	Built-in	3	3	0	Yes
Security Administrator (View Only) User Group	Built-in	3	3	0	Yes
Storage Administrator (View & Modify) User Group	Built-in	6	1	0	No
Storage Administrator (View Only) User Group	Built-in	1	1	0	No
Support Personnel Group	Built-in	7	3	1	Yes
System User Group	Built-in	8	3	1	Yes
Usergroup01	User-created	2	1	0	No

### Summary

The following table describes the fields in the summary section in the **User Groups** window.

Item	Description
Number of User Groups	Number of user groups created in Device Manager - Storage Navigator.

### User Groups tab

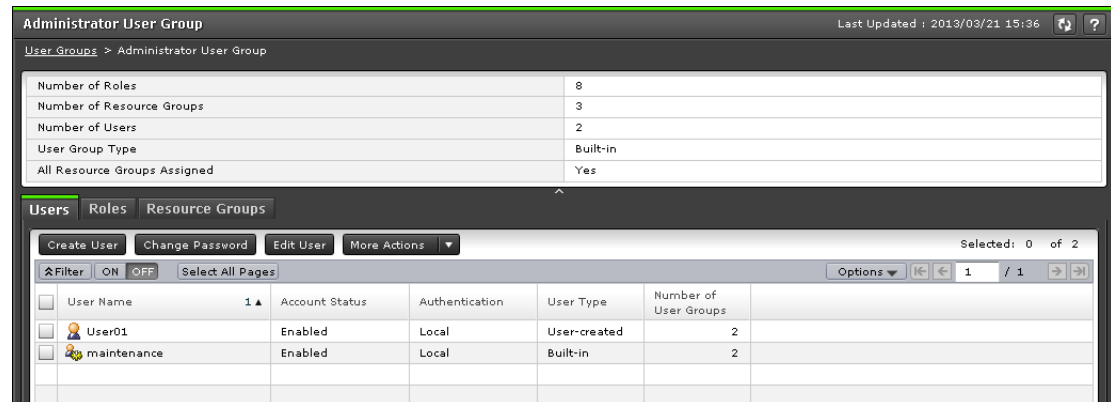
The following table describes the fields in the User Groups tab in the **User Groups** window.

Item	Description
User Group Name	Displays user group name.
User Group Type	Displays the user group type. Built-in: Indicates a built-in user group. User-created: Indicates a user group that users created.
Number of Roles	Displays the number of the roles that are assigned to the user group.
Number of Resource Groups	Displays the number of the resource groups that are assigned to the user group.
Number of Users	Displays the number of users who belong to the user group.
All Resource Groups Assigned	Displays whether all the resource groups are assigned. Yes: All the resource groups are assigned to the user group. No: All the resource groups are not assigned to the user group.
Create User Group	Creates a new user group.
Add Users	Adds the created users to the selected user group.
Edit Resource Group Assignment	Assigns the created resource groups to the selected user groups.
Edit Role Assignment*	Assigns the created roles to the selected user groups.
Delete User Groups*	Deletes the selected user groups.
Edit User Group*	Edits the user group name.
Export*	Displays a window for outputting table information.
* Appears when you click More Actions.	

## Selected User Group Window

The **User Group** window lists the names of all of the built-in user groups and any user groups that were created in Device Manager - Storage Navigator. To open a window for a specific user group, in the User Groups tab, click the user group name.

The features of the window that opens when a user group is selected are the same, no matter which user group is selected. The following example uses the **Administrator User Group** window to show the features in the window.



The window for each selected user group contains a Summary section and three tabs.

### Summary section

The following table describes the fields and settings in the Summary section of the selected user group window.

Item	Description
Number of Roles	Displays the number of roles that are assigned to the selected user group.
Number of Resource Groups	Displays the number of resource groups that are assigned to the selected user group.
Number of Users	Displays the number of users who belong to the selected user group.
User Group Type	Displays the user group type. Built-in: Indicates a built-in user group. User-created: Indicates a user group that a user created.
All Resource Groups Assigned	Displays whether all the resource groups are assigned. Yes: All the resource groups are assigned to the user group. No: All the resource groups are not assigned to the user group.

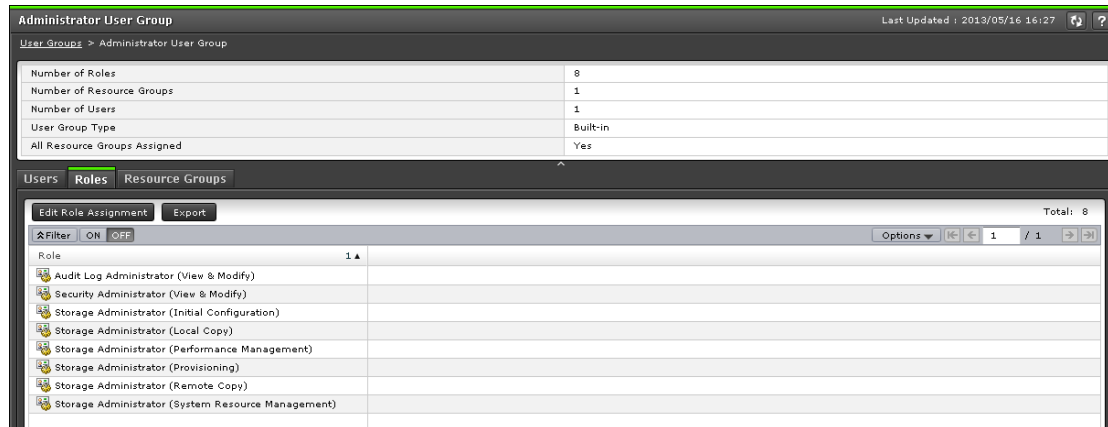
### Users tab

The following table describes the fields and settings in the Users tab of the selected user group window. It lists the users who belong to the selected user group.

Item	Description
User Name	Name of user who belongs to the user group.
Account Status	Account status. The following statuses are available: Enabled: The user can use the account. Disabled: The user cannot use the account or log in to Device Manager - Storage Navigator.
Lockout <sup>1</sup>	Indicates whether the status is locked. <ul style="list-style-type: none"> <li>▪ Yes: The user account is locked, so login to Device Manager - Storage Navigator is not possible.</li> <li>▪ No: The user can use the account.</li> </ul>
Authentication	Authentication method. The following methods are available: Local: Does not use authentication server. Uses a dedicated password for Device Manager - Storage Navigator. External: Uses authentication server.
User Type	User type. The following types are available: Built-in or User-created
Number of User Groups	Displays the number of the user groups where the user belongs.
Create User	Creates a new user account.
Change Password	Changes your own password if you click this. Changes the password of other users if you select a user and then click this.
Edit User	Changes the setting for authentication or for the account status. You can set the password of the selected user if you change Authentication from External to Local.
Add Users <sup>2</sup>	Adds the created users to the selected user group.
Remove Users <sup>2</sup>	Removes the selected user from the user group. The user account itself will not be deleted.
Delete Users <sup>2</sup>	Deletes the selected users.
Export <sup>2</sup>	Displays a window for outputting table information.
<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This content is not displayed by default. To display it, change the settings in the <b>Column Settings</b> window in the table options.</li> <li>2. Appears when you click More Actions.</li> </ol>	

## Roles tab

The following illustration shows the Roles tab of the selected user group window.

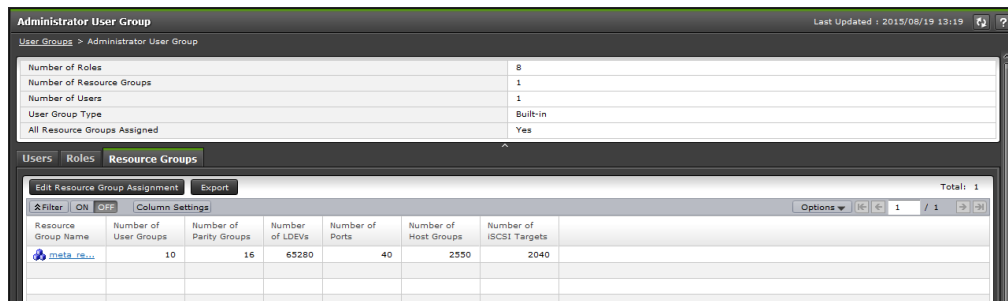


The following table describes the fields and settings in the Roles tab of the selected user group window. Role displays the roles assigned to the user group, which determines the operations the user can perform.

Role	Permitted operations
Roles	Displays the roles that are assigned to the user group.
Edit Role Assignment	Assigns the created roles to the selected user groups.
Export	Displays a window for outputting table information.

## Resource Groups tab

The following illustration shows the Resource Groups tab of the selected user group window.



The following table describes the fields and settings in the Resource Groups tab of the selected user group window. It lists the resource groups that are assigned to the selected user group.

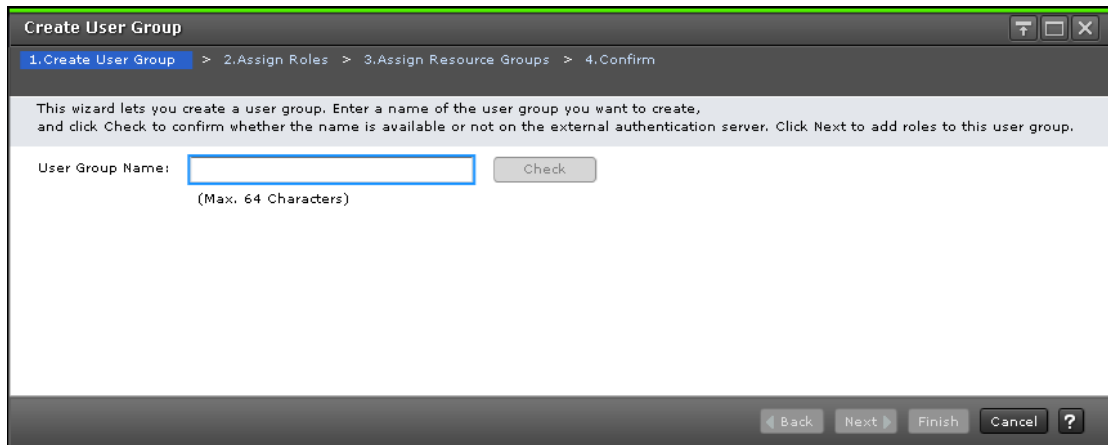
Item	Description
Resource Group Name	Displays the name and ID of the resource group assigned to the user group.
Number of User Groups	Displays the number of user groups that are assigned to the resource group.
Number of Parity Groups	Displays the number of the parity groups that are assigned to the resource group.
Number of LDEVs	Displays the number of the LDEVs that are assigned to the resource group.
Number of Ports	Displays the number of the ports that are assigned to the resource group.
Number of Host Groups	Displays the number of the host groups that are assigned to the resource group.
Number of iSCSI Targets	Displays the number of the iSCSI targets that are assigned to the resource group.
Virtual Storage Machine*	Displays the model type and serial number of the virtual storage machine set for the resource group.
Edit Resource Group Assignment	Assigns the created resource groups to the user groups.
Export	Displays a window for outputting table information.
* This content is not displayed by default. To display it, change the settings in the <b>Column Settings</b> window in the table options.	

## Create User Group wizard

### Create User Group window

Use this window to create a new user group.





Item	Description
User Group Name	Enter the name of the user group to be created. You can specify ASCII code characters, spaces, and the following symbols: ! # \$ % & ' ( ) + - . = @ [ ] ^ _ ` { } ~
Check	Check whether the entered user group name is registered to the authorization server when you use an authorization server.

## Create User Group confirmation window

1.Create User Group > 2.Assign Roles > 3.Assign Resource Groups > 4.Confirm

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

Task Name:  (Max. 32 Characters)

Create User Group				
User Group Name	Number of Roles	Number of Resource Groups	Number of Users	All Resource Groups Assigned
Usergroup	2	0	0	Yes

Assigned Roles	
Role	
Audit Log Administrator (View Only)	
Storage Administrator (View Only)	
Total: 2	

Assigned Resource Groups						
Resource Group Name (ID)	Number of User Groups	Number of Parity Groups	Number of LDEVs	Number of Ports	Number of Host Groups	
No Data						
Total: 0						

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

### Create User Group

The following table describes the fields in the Create User Group section of the Create User Group Window.

Item	Description
User Group Name	Displays the name of user groups that are created.
Number of Roles	Displays the number of roles that are assigned to the user group created.
Number of Resource Groups	Displays the number of resource groups that are assigned to the user group created.

Item	Description
Number of Users	Displays the number of users that belong to the user group created.
All Resource Groups Assigned	Displays whether all resource groups are assigned. Yes: All resource groups are assigned to the user group. No: All resource groups are not assigned to the user group.

### Assigned Roles

The following table describes the fields in the Assigned Roles section of the Create User Group Window.

Item	Description
Role	Displays the roles that are assigned to the user group created.

### Assigned Resource Groups

The following table describes the fields in the Assigned Resource Group section of the Create User Group Window.

Item	Description
Resource Group Name (ID)	Displays the name and ID of the resource group assigned to the user group created.
Number of User Groups	Displays the number of user groups that are assigned to the resource group.
Number of Parity Groups	Displays the number of parity groups that are assigned to the resource group.
Number of LDEVs	Displays the number of LDEVs that are assigned to the resource group.
Number of Ports	Displays the number of ports that are assigned to the resource group.
Number of Host Groups	Displays the number of host groups that are assigned to the resource group.
Number of iSCSI Targets	Displays the number of the iSCSI targets that are assigned to the resource group.
Detail	Displays details of the selected resource group.

### Selected Users

The following table describes the fields in the Selected Users section of the Create User Group Window. This table displays only when users are added to the user group. This table displays only when users are added to the user group.

Item	Description
User Name	Displays the name of the users that belong to the user group to be created.
Account Status	Displays the account status. The following status are available: Enabled: The user can use the account. Disabled: The user cannot use the account or log in to Device Manager - Storage Navigator.
Authentication	Displays the authentication method. The following methods are available: Local: Does not use authentication server. Uses a dedicated password for Device Manager - Storage Navigator. External: Uses authentication server.
Number of User Groups	Displays the number of user groups where the user belongs.

## Create User wizard

### Create User window

Use this window to create a new user account.

The following table describes the fields and settings in the **Create User** window.

Item	Description
User Name	Enter the user name to be created. The allowable characters and length of user names depend on the application that the user uses.
Account Status	Account statuses. The following statuses are available: Enable: The user can use the account. Disable: The user cannot use the account or log in to Device Manager - Storage Navigator.
Authentication	Authentication method. The following methods are available: Local: Does not use authentication server. Uses a dedicated password for Device Manager - Storage Navigator. External: Uses authentication server.
Password	Password that the user enters for login. The allowable characters and length of passwords depend on the application that the user uses.
Re-enter Password	Password as above.

## Create User confirmation window

1. Create User > 2. Confirm

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

Task Name:  (Max. 32 Characters)

Selected User	
Item	Value
User Name	User02
Account Status	Enabled
Authentication	Local
Password	*****
User Group Name	Administrator User Group

Go to tasks window for status Back Next Apply Cancel ?

### Selected Users

The following table describes the fields and settings used to create a new user account.

Item	Description
User Name	User name to be created.
Account Status	Account statuses. The following statuses are available: Enabled: The user can use the account. Disabled: The user cannot use the account or log in to Device Manager - Storage Navigator.
Authentication	Authentication methods. The following methods are available: Local: Does not use authentication server. Uses a dedicated password for Device Manager - Storage Navigator. External: Uses authentication server.
Password	Password that the user enters for login.
User Group Name	User group name where the user is added.

# Change Password Wizard

## Change Password window

Use this window to change the password for yourself or another user.

The following table describes the fields and settings used to change a password.

Item	Description
User Name	Selected user name.
Current Password	Current password of your user account. Required only when you change your own password.
New Password	New password that the selected user enters for login. The allowable characters and length of passwords depend on the application that the user uses.
Re-enter New Password	Same password as above.

## Change Password confirmation window

Change Password

1. Change Password > 2. Confirm

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

Task Name:  (Max. 32 Characters)

Selected User	
Item	Value
User Name	User01
Current Password	*****
New Password	*****

Go to tasks window for status Back Next Apply Cancel ?

The following table describes the fields and settings used to change user passwords.

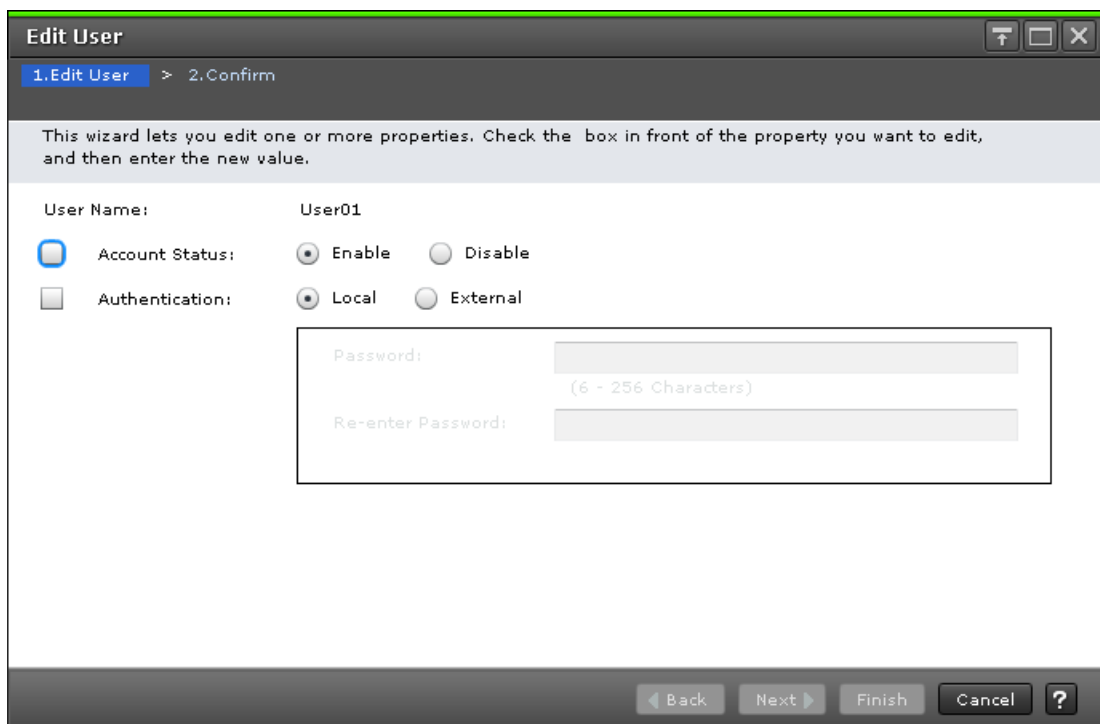
Item	Description
User Name	Selected user name.
Current Password	Current password. A hyphen (-) indicates no current password is specified.
New Password	New password.

## Edit User wizard

### Edit User window

Use this window to change the setting for authentication or for the account status.





The following table describes the fields and settings used to edit user account information.

Item	Description
User Name	Selected user name.
Account Status	Account statuses. The following statuses are available: Enabled: The user can use the account. Disabled: The user cannot use the account or log in to Device Manager - Storage Navigator.
Authentication	Authentication method. The following methods are available: Local: Does not use authentication server. Uses a dedicated password for Device Manager - Storage Navigator. External: Uses authentication server.
Password	Password that the user enters for login. You can specify ASCII code characters and the following symbols: ! # \$ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` {   } ~
Re-enter Password	Password that the user enters for login.

## Edit User confirmation window

1. Edit User > 2. Confirm

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

Task Name:  (Max. 32 Characters)

Selected User	
Item	Value
User Name	User01
Account Status	Disabled
Authentication	Local
Password	*****

Go to tasks window for status     ?

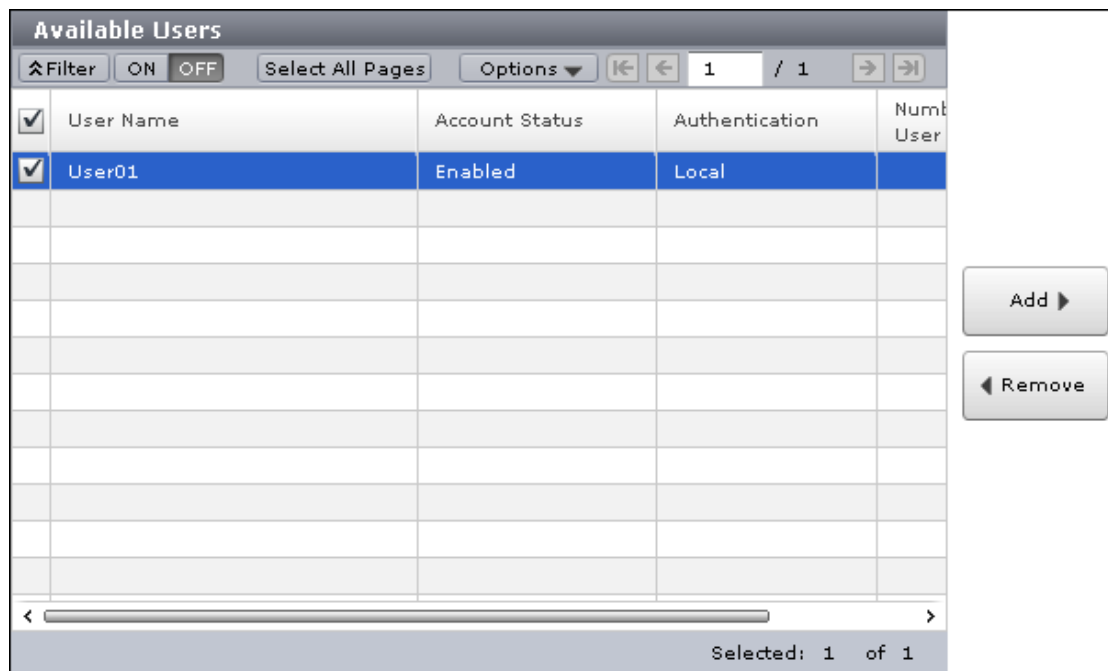
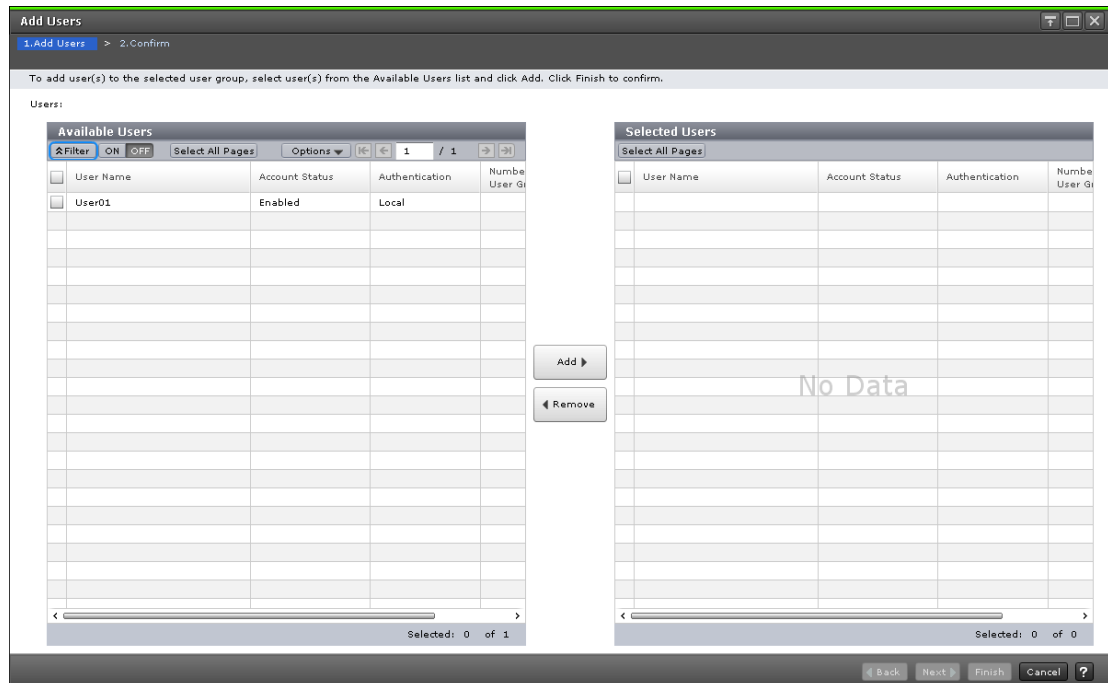
The following table describes the fields and settings in the **Edit Users** window.

Item	Description
User Name	Selected user name.
Account Status	Account status. The following statuses are available: Enabled: The user can use the account. Disabled: The user cannot use the account or log in to Device Manager - Storage Navigator.
Authentication	Authentication method. The following methods are available: Local: Does not use authentication server. Uses a dedicated password for Device Manager - Storage Navigator. External: Uses authentication server.
Password	Password that the user enters for login.

## Add User wizard

### Add Users window

Use this window to add the created user accounts to the selected user group.



**Available Users**

The following table lists all the candidate users who do not belong to the selected user group.

Item	Description
User Name	Selected user name.
Account Status	Account status. The following statuses are available: Enabled: The user can use the account. Disabled: The user cannot use the account or log in to Device Manager - Storage Navigator.
Authentication	Authentication method. The following methods are available: Local: Does not use authentication server. Uses a dedicated password for Device Manager - Storage Navigator. External: Uses authentication server.
Number of User Groups	Displays the number of user groups where the user belongs.

**Add button**

Adds the selected users in the Available Users list to the Selected Users list.

**Remove button**

Removes the selected users from the Selected Users list and relocates the selected users to the Available User list.



## Add Users confirmation window

1.Add Users > 2. Confirm

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

Task Name:  (Max. 32 Characters)

Selected User Group	
User Group Name	
Storage Administrator (View Only) User Group	

Selected Users			
User Name	Account Status	Authentication	Number of User Groups
User01	Enabled	Local	2
			Total: 1

Go to tasks window for status

Back Next Apply Cancel ?

## Selected User Group

Item	Description
User Group Name	Displays the user group name where the user is added.

## Selected Users table

Item	Description
User Name	Selected user name.
Account Status	Account status. The following statuses are available: Enabled: The user can use the account. Disabled: The user cannot use the account or log in to Device Manager - Storage Navigator.
Authentication	Authentication method. The following methods are available:

Item	Description
	Local: Does not use authentication server. Uses a dedicated password for Device Manager - Storage Navigator. External: Uses authentication server.
Number of User Groups	Displays the number of user groups where the user belongs.

## Remove Users window

The **Remove Users** window is used to remove users from a particular group. However, the removed users will still remain in the system. To delete users entirely from the system, see [Deleting user accounts \(on page 119\)](#).

The screenshot shows the 'Remove Users' window with the following elements:

- Window title: Remove Users
- Step indicator: 1. Confirm
- Warning message: The authorization of User Group can not be used for this user. Are you sure to continue?
- Task Name field: 130321-RemoveUsers (Max. 32 Characters)
- Selected User Group table:
 

User Group Name	Administrator User Group
- Selected Users table:
 

User Name	Account Status	Authentication	Number of User Groups
User01	Enabled	Local	2
			Total: 1
- Bottom controls:
  - Go to tasks window for status
  - Back
  - Next
  - Apply
  - Cancel
  - Help (?)

### Selected User Group table

Item	Description
User Group Name	Displays the name of the user group where the user is removed.

**Selected Users table**

Item	Description
User Name	Selected user name.
Account Status	Account status. The following statuses are available: Enabled: The user can use the account. Disabled: The user cannot use the account or log in to Device Manager - Storage Navigator.
Authentication	Authentication method. The following methods are available: Local: Does not use authentication server. Uses a dedicated password for Device Manager - Storage Navigator. External: Uses authentication server.
Number of User Groups	Displays the number of user groups where the user belongs.

**Delete Users window**

The **Delete Users** window is used to delete users entirely from the system. If you want to remove users from a particular group without deleting them in the system, see [Changing user permissions \(on page 118\)](#).

The screenshot shows the 'Delete Users' window with the following elements:

- Window title: Delete Users
- Step indicator: 1. Confirm
- Warning message: Selected Users will be deleted. Are you sure to continue?
- Task Name field: 130321-DeleteUsers (Max. 32 Characters)
- Selected Users table:

User Name	Account Status	Authentication	Number of User Groups
User01	Enabled	Local	2
			Total: 1

At the bottom of the window, there are several controls:

- Go to tasks window for status
- Back button
- Next button
- Apply button
- Cancel button
- Help button (?)



Item	Description
User Name	Selected user name.
Account Status	Account status. the following statuses are available: Enabled: The user can use the account. Disabled: The user cannot use the account or log in to Device Manager - Storage Navigator.
Authentication	Authentication method. The following methods are available: Local: Does not use authentication server. Uses a dedicated password for Device Manager - Storage Navigator. External: Uses authentication server.
Number of User Groups	Displays the number of user groups to which the user belongs.

## Release Lockout window

**Release Lockout**

1. Confirm

⚠ The lockout status of the selected user will be released. Are you sure to continue?

Task Name:  (Max. 32 Characters)

Selected Users	
User Name	
maintenance	
Total: 1	

Go to tasks window for status   Back   Next   Apply   Cancel   ?

Item	Description
User Name	Name of the user whose account you want to unlock

## Edit User Group wizard

### Edit User Group window

Use this window to change the name of a user group.

The screenshot shows a window titled "Edit User Group" with a progress bar indicating the current step is "1. Edit User Group" and the next step is "2. Confirm". Below the progress bar, there is a text box labeled "User Group Name" containing the text "Usergroup01". To the right of the text box is a "Check" button. Below the text box, it says "(Max. 64 Characters)". At the bottom of the window, there are buttons for "Back", "Next", "Finish", "Cancel", and a help icon.

The following table describes the fields and settings used to edit user group information.

Item	Description
User Group Name	Enter the new name of the user group. You can use ASCII code characters, spaces, and the following symbols: ! # \$ % & ' ( ) + - . = @ [ ] ^ _ ` { } ~
Check	Check whether the entered user group name is registered to the authentication server when you use an authentication server.

## Edit User Group confirmation window

1. Edit User Group > 2. Confirm

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

Task Name:  (Max. 32 Characters)

Selected User Group					
User Group Name	Number of Roles	Number of Resource Groups	Number of Users	All Resource Groups Assigned	
Usergroup	2	1	0	No	

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

The following table describes the fields and settings used to edit user group information.

Item	Description
User Group Name	Displays the new name of the user group.
Number of Roles	Displays the number of roles that are assigned to the user group.
Number of Resource Groups	Displays the number of resource groups that are assigned to the user group.
Number of Users	Displays the number of users that belong to the user group.
All Resource Groups Assigned	Displays whether all the resource groups are assigned. Yes: All resource groups are assigned to the user group. No: All resource groups are not assigned to the user group.

## Delete User Groups window

**Delete User Groups**

1. Confirm

**!** The selected user group(s) will be deleted. Are you sure to continue?

Task Name:   
(Max. 32 Characters)

Selected User Groups				
User Group Name 1 ▲	Number of Roles	Number of Resource Groups	Number of Users	All Resource Groups Assigned
Usergroup01	2	1	0	No
				Total: 1

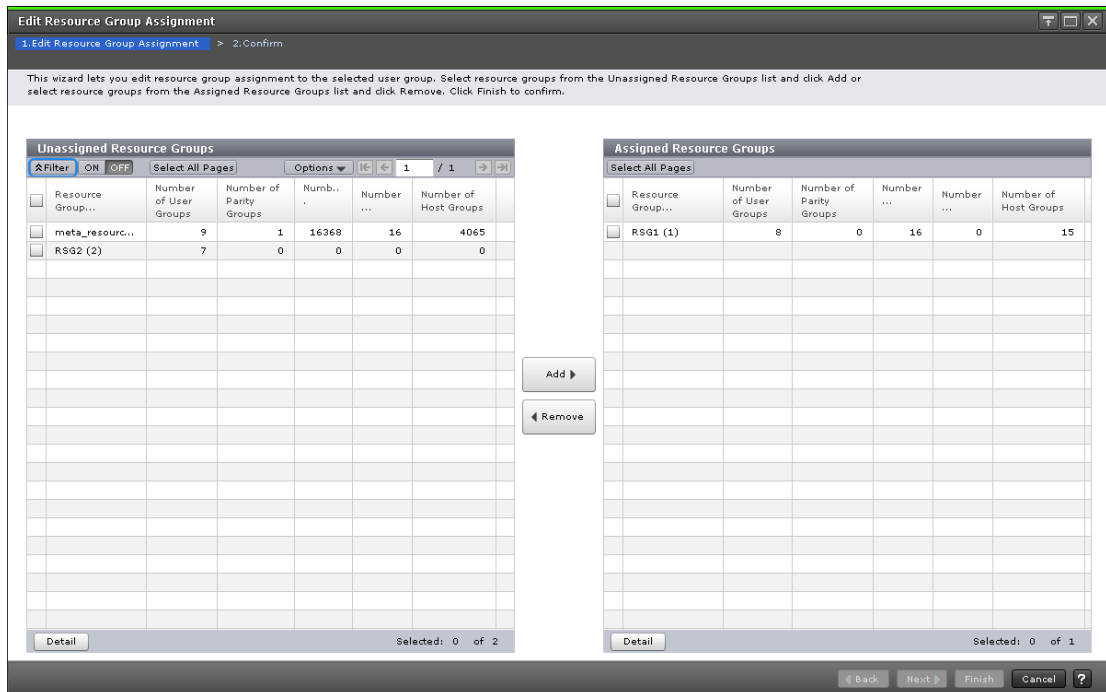
Go to tasks window for status    < Back    Next >    Apply    Cancel    ?

Item	Description
User Group Name	Displays the new name of the user group.
Number of Roles	Displays the number of roles that are assigned to the user group.
Number of Resource Groups	Displays the number of resource groups that are assigned to the user group.
Number of Users	Displays the number of users that belong to the user group.
All Resource Groups Assigned	Displays whether all resource groups are assigned. Yes: All resource groups are assigned to the user group. No: All resource groups are not assigned to the user group.

## Edit Resource Group Assignment wizard

### Edit Resource Group Assignment window

Use this window to assign created resource groups to the user group and to assign created resource groups to the user group in the Create User Group.



The following table describes the fields and settings used to assign resource groups with the **Create User Group** wizard.

Item	Description
All Resource Groups Assigned	<p>Displays whether all the resource groups are assigned to the user group.</p> <p>This item is set to Yes when the following roles are assigned in the <b>Assign Roles</b> window.</p> <ul style="list-style-type: none"> <li>▪ Security Administrator (View Only)</li> <li>▪ Security Administrator (View &amp; Modify)</li> <li>▪ Audit log Administrator (View Only)</li> <li>▪ Audit log Administrator (View &amp; Modify)</li> <li>▪ Support Personnel (Vendor Only)</li> </ul> <p>When this item is set to Yes, Unassigned Resource Groups table, Assigned Resource Groups table, Add button, and Remove button are disabled.</p>

**Unassigned Resource Groups table**

Resource Group...	Number of User Groups	Number of Parity Groups	Numb..	Number...	Number of Host Groups
meta_resourc...	9	1	16368	16	4065
RSG2 (2)	7	0	0	0	0

The following table lists the resource groups that are not assigned to the user group.

Item	Description
Resource Group Name (ID)	Displays the name and ID of the resource group that is not assigned to the user group to be created.
Number of User Groups	Displays the number of user groups that are not assigned to the resource group.
Number of Parity Groups	Displays the number of parity groups that are not assigned to the resource group.
Number of LDEVs	Displays the number of LDEVs that are not assigned to the resource group.
Number of Ports	Displays the number of ports that are not assigned to the resource group.

Item	Description
Number of Host Groups	Displays the number of host groups that are not assigned to the resource group.
Number of iSCSI Targets	Displays the number of the iSCSI targets that are assigned to the resource group.
Detail	Displays the detail of the selected resource group.

**Add button**

Adds the selected resource groups in the Unassigned Resource Groups list to the Assigned Resource Groups list.

**Remove button**

Removes the selected resource groups from the Assigned Resource Groups list and relocates the resource groups to the Unassigned Resource Groups list.





Item	Description
Number of Host Groups	Displays the number of host groups that are assigned to the resource group.
Number of iSCSI Targets	Displays the number of the iSCSI targets that are assigned to the resource group.
Detail	Displays the detail of the selected resource group.

## Edit Resource Group Assignment confirmation window

1. Edit Resource Group Assignment > 2. Confirm

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

Task Name:  (Max. 32 Characters)

**Selected User Group**

User Group Name
usergroup01

**Selected Resource Groups as Assigned**

Resource Group Name (ID)	Number of User Groups	Number of Parity Groups	Number of LDEVs	Number of Ports	Number of Host Groups
meta_resource ...	10	11	65280	112	16320
					Total: 1

**Selected Resource Groups as Unassigned**

Resource Group Name (ID)	Number of User Groups	Number of Parity Groups	Number of LDEVs	Number of Ports	Number of Host Groups
No Data					
					Total: 0

Go to tasks window for status

The following tables describe the fields and settings used to assign user group names with the **Create User Group** wizard.

Item	Description
User Group Name	Displays the new name of the user group.

### Selected Resource Groups as Assigned Table

The following table describes the fields and settings used to assign resource groups with the **Create User Group** wizard.

Item	Description
Resource Group Name (ID)	Displays the name and ID of the resource group assigned to the user group to be created.
Number of User Groups	Displays the number of user groups that are assigned to the resource group.
Number of Parity Groups	Displays the number of parity groups that are assigned to the resource group.
Number of LDEVs	Displays the number of LDEVs that are assigned to the resource group.
Number of Ports	Displays the number of ports that are assigned to the resource group.
Number of Host Groups	Displays the number of host groups that are assigned to the resource group.
Number of iSCSI Targets	Displays the number of the iSCSI targets that are assigned to the resource group.
Detail	Displays the detail of the selected resource group.

### Selected Resource Groups as Unassigned Table

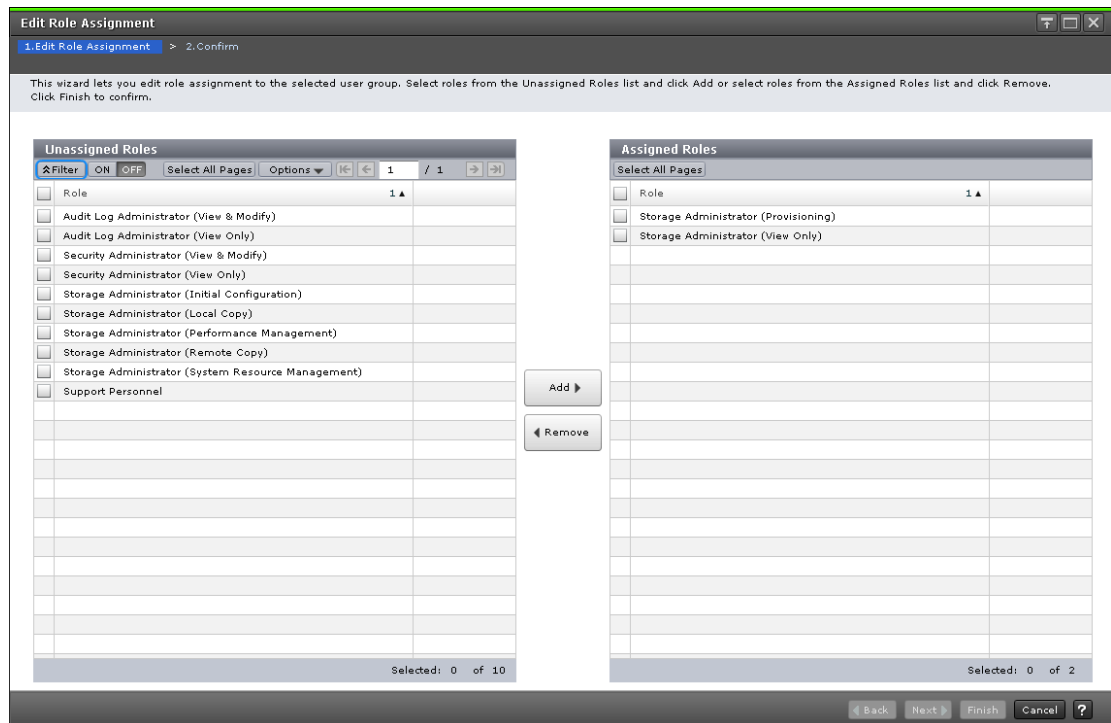
The following table lists the resource groups that are not assigned to the user group.

Item	Description
Resource Group Name (ID)	Displays the name and ID of the resource group not assigned to the user group to be created.
Number of User Groups	Displays the number of user groups that are not assigned to the resource group.
Number of Parity Groups	Displays the number of parity groups that are not assigned to the resource group.

Item	Description
Number of LDEVs	Displays the number of LDEVs that are not assigned to the resource group.
Number of Ports	Displays the number of ports that are not assigned to the resource group.
Number of Host Groups	Displays the number of host groups that are not assigned to the resource group.
Number of iSCSI Targets	Displays the number of the iSCSI targets that are assigned to the resource group.
Detail	Displays the detail of the selected resource group.

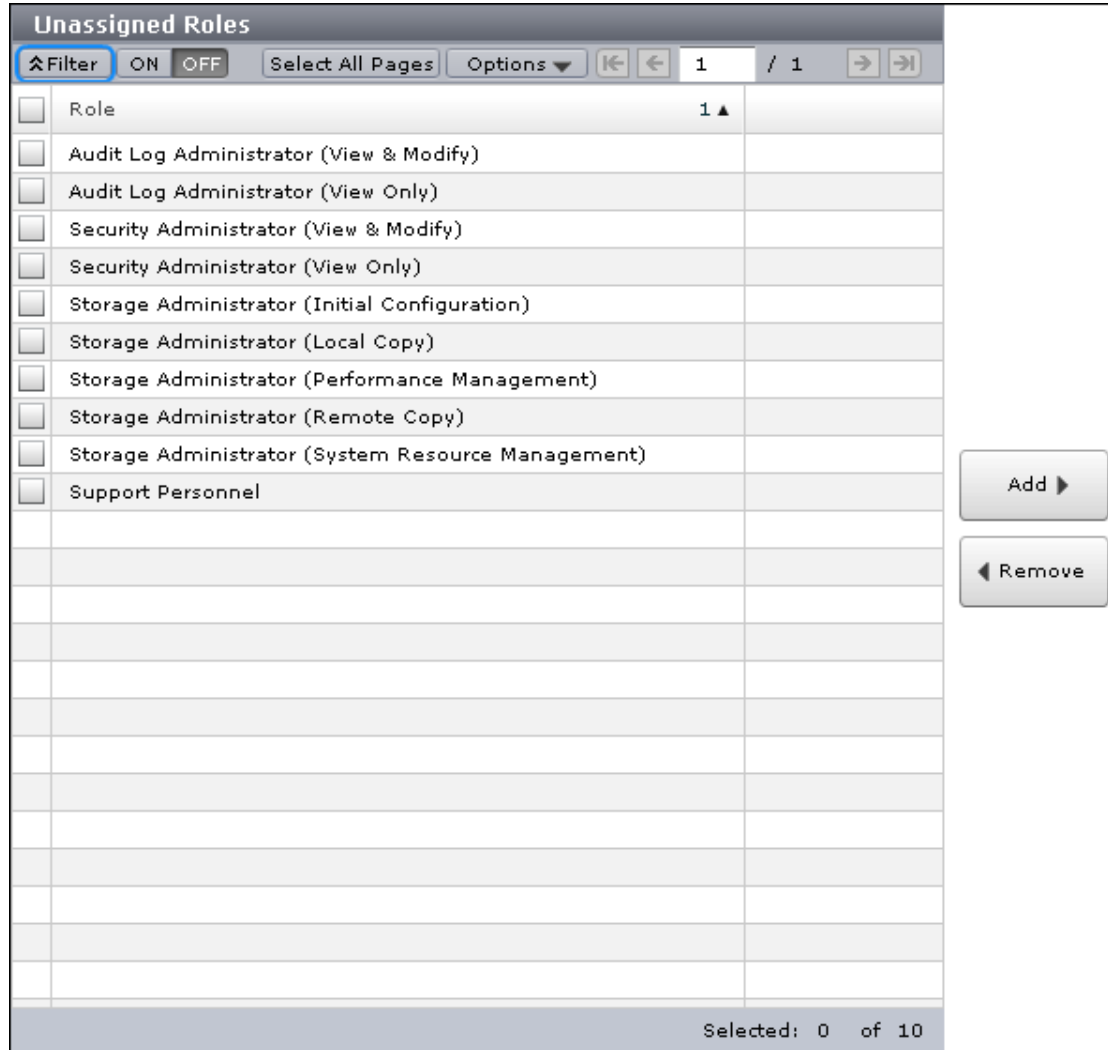
## Edit Role Assignment wizard

### Edit Role Assignment window



Use this window to add roles to the user group and to assign roles to the user group in the Create User Group.

## Unassigned Roles



Lists roles that are not assigned to the user group.

Item	Description
Role	Displays roles.

### Add button

Adds the selected roles in the Unassigned Roles list to the Assigned Roles list.

### Remove button

Removes the selected roles from the Assigned Roles list and relocates the selected roles to the Unassigned Roles list.

### Assigned Roles

The following window shows the roles that can be assigned to the selected user group.



## Edit Role Assignment confirmation window

### Selected User Group

Item	Description
User Group Name	Displays the new name of the user group.
All Resource Groups Assigned	Displays whether all the resource groups are assigned. Yes: All the resource groups are assigned to the user group. No: All the resource groups are not assigned to the user group.

### Selected Assigned Roles

Item	Description
Role	Displays the roles that are assigned to the user group.

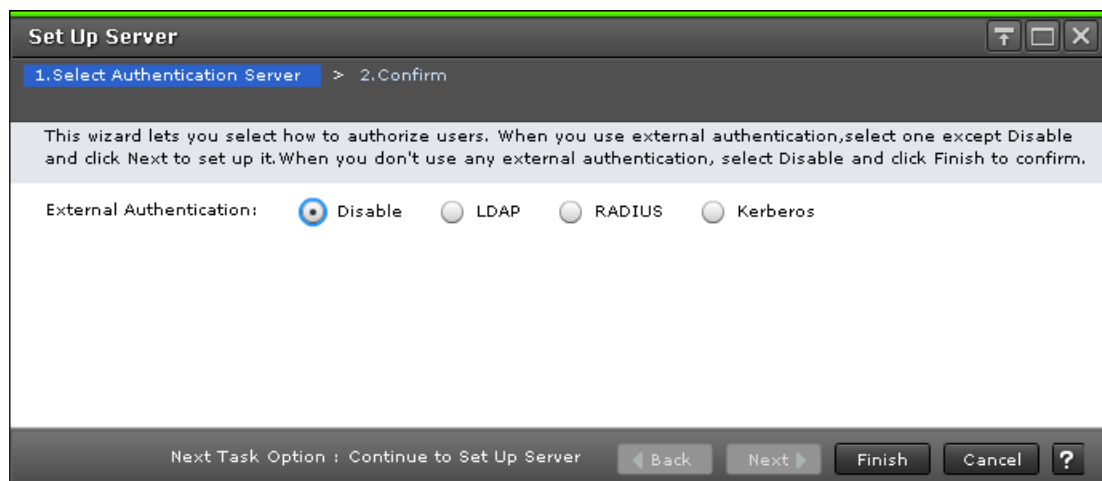
## Selected Unassigned Roles

Item	Description
Role	Displays the roles that are not assigned to the user group.

## Setup Server wizard

### Select Authentication Server window

To open this window, select Server Setup from the LDAP, RADIUS, or Kerberos properties window.



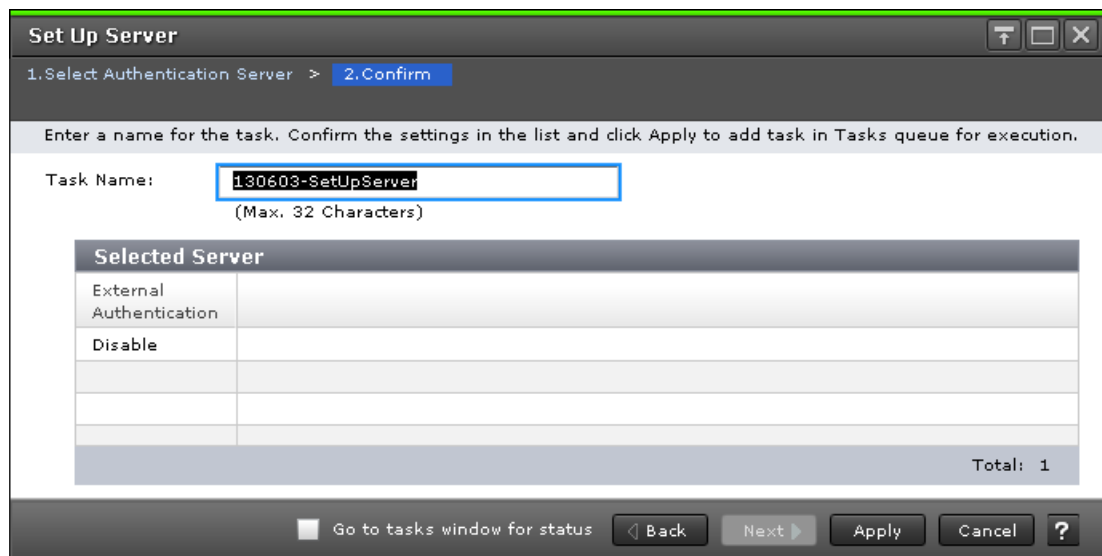
The following tables describe the fields and settings used to set up external authentication in the **Select Authentication Server** window.

Item	Description
External Authentication	<p>Select the type of authentication server.</p> <ul style="list-style-type: none"> <li>▪ Disable: Does not use any authentication server. Users are authenticated with user information registered in the SVP.</li> <li>▪ LDAP: Users are authenticated with user information registered in the LDAP server.</li> <li>▪ RADIUS: Users are authenticated with user information registered in the RADIUS server.</li> <li>▪ Kerberos: Users are authenticated with user information registered in the Kerberos server.</li> </ul> <p>When you select Disable, click Finish to open the confirmation window.</p>

Item	Description
	When you select LDAP, RADIUS, or Kerberos, click Next to open the <b>Setup Server</b> window.

## Select Authentication Server confirmation window

To open this window, select Disable in the **Select Authentication Server** window.



The following table describes the fields and settings in the Disable authentication server setup window.

Item	Description
External Authentication	<p>Displays the type of the authentication server.</p> <ul style="list-style-type: none"> <li>Disable: Does not use any authentication server. Users are authenticated with user information registered in the SVP.</li> <li>LDAP: Users are authenticated with user information registered in the LDAP server.</li> <li>RADIUS: Users are authenticated with user information registered in the RADIUS server.</li> <li>Kerberos: Users are authenticated with user information registered in the Kerberos server.</li> </ul>

## LDAP Properties window

To open this window, select Disable or LDAP in the **External Authentication** window.



The screenshot shows a window titled "LDAP Properties" with a table of configuration settings. The settings are as follows:

LDAP Properties	
DNS Lookup	Disable
Authentication Protocol	STARTTLS
External User Group Mapping	Enable
Primary Host Name	xx.xxx.xx.xxx
Primary Port Number	389
Domain Name	example.com
User Name Attribute	sAMAccountName
Base DN	sample
Search User's DN	sample
Password	*****
Timeout	10 Second(s)
Retry Interval	1 Second(s)
Number of Retries	3
Secondary Host Name	-
Secondary Port Number	-

At the bottom right of the table area is a button labeled "Set Up Server". At the bottom right of the window is a "Close" button and a help icon.

Item	Description
DNS Lookup	<p>Displays whether to search for the LDAP server using the information registered in the SRV records in the DNS server.</p> <ul style="list-style-type: none"> <li>▪ Enable: Performs the search using information registered in the SRV records in the DNS server.</li> <li>▪ Disable: Performs the search using the host name and the port number.</li> </ul>
Authentication Protocol	Displays the LDAP protocol to use.

Item	Description
External User Group Mapping	Displays whether to connect an authentication server to an authorization server. <ul style="list-style-type: none"> <li>▪ Enable: Connects an authentication server to an authorization server.</li> <li>▪ Disable: Does not connect an authentication server to an authorization server.</li> </ul>
Primary Host Name	Displays the host name of the LDAP server.
Primary Port Number	Displays the port number of the LDAP server.
Domain Name	Displays the domain name that the LDAP server manages.
User Name Attribute	Displays the attribute name to identify a user, such as a user ID.
Base DN	Displays the Base DN for searching for users to authenticate.
Search User's DN	Displays the DN of the user for searching.
Password	Displays asterisks (*) to mask the password of the user for searching.
Timeout	Displays the number of seconds before connection to the LDAP server times out.
Retry Interval	Displays the retry interval in seconds when the connection to the LDAP server fails.
Number of Retries	Displays the retry times when the connection to the LDAP server fails.
Secondary Host Name	Displays the host name of the secondary LDAP server.
Secondary Port Number	Displays the port number of the secondary LDAP server.
Setup Server	Displays the <b>Setup Server</b> window.

## RADIUS Properties window

This window opens when you select RADIUS in External Authentication.

The screenshot shows a window titled "RADIUS Properties" with a standard Windows-style title bar (minimize, maximize, close). The window contains a list of configuration fields:

- Authentication Protocol: PAP
- Primary Host Name: sample
- Secret: \*\*\*\*\*
- NAS Address: xx.xxx.xx.xx
- Primary Port Number: 1812
- Timeout: 10 Second(s)
- Number of Retries: 3
- Secondary Host Name: -
- Secondary Port Number: -
- External User Group Mapping (expanded):
  - Authentication Protocol: -
  - DNS Lookup: -
  - Host Name: -
  - Port Number: -
  - Domain Name: -
  - Base DN: -
  - Search User's DN: -
  - Password: -
  - Timeout: -
  - Retry Interval: -
  - Number of Retries: -

At the bottom right of the main configuration area is a "Set Up Server" button. At the bottom right of the window is a "Close" button and a help icon (?).

The following table describes the fields and settings in the RADIUS properties window.

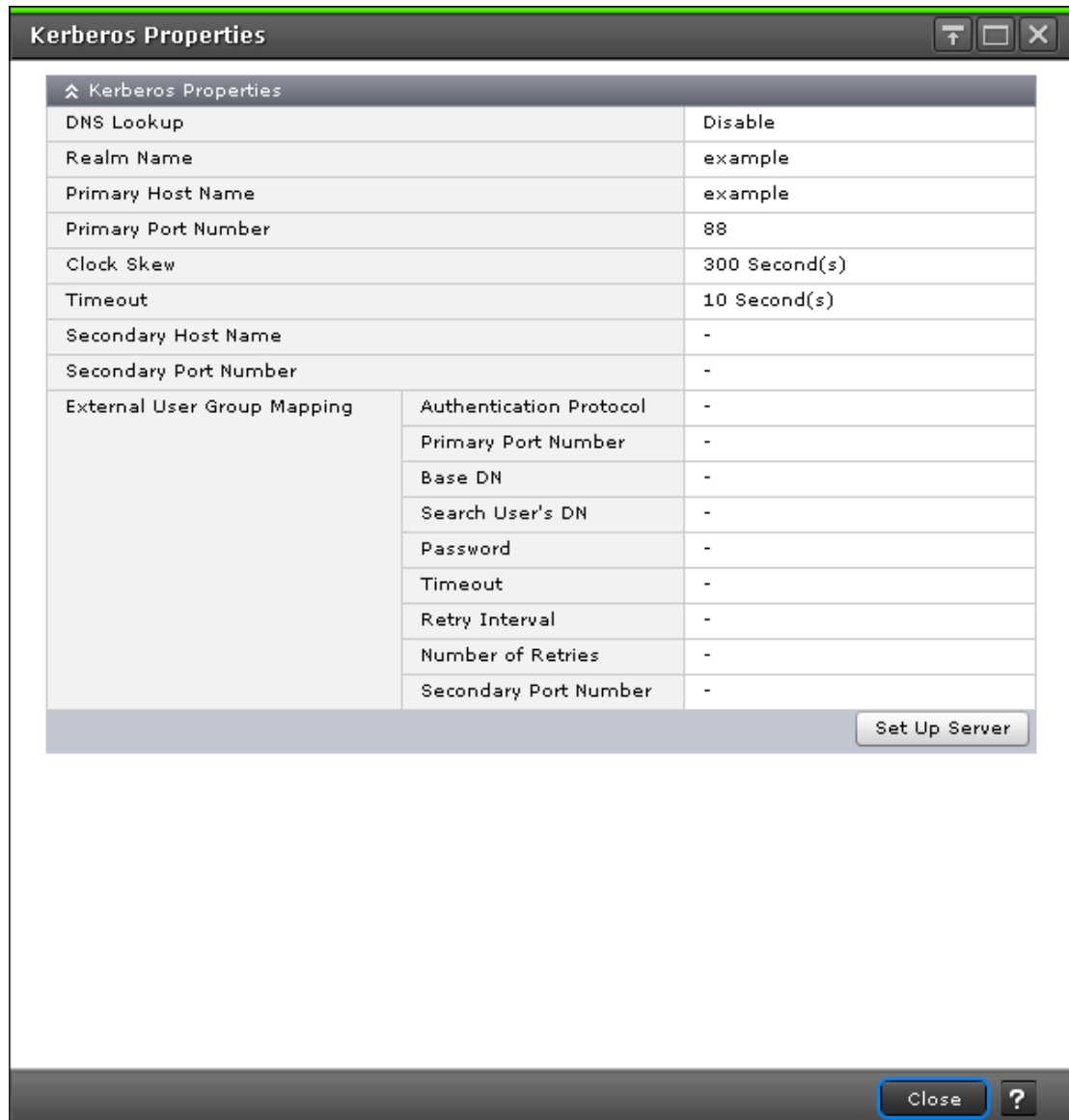
Item	Description
Authentication Protocol	Displays the RADIUS protocol to use. <ul style="list-style-type: none"> <li>▪ PAP: Password authentication protocol that transmits plaintext user ID and password.</li> <li>▪ CHAP: Challenge-handshake authentication protocol that transmits encrypted password.</li> </ul>
Primary Host Name	Displays the host name, the IPv4 address, or the IPv6 address of the RADIUS server.
Secret	Displays asterisks (*) to mask the RADIUS secret key used for the PAP or CHAP authentication.

Item	Description
NAS Address	Displays the identifier for the RADIUS server to find SVP.
Primary Port Number	Displays the port number of the RADIUS server.
Timeout	Displays the number of seconds before connection to the RADIUS server times out.
Number of Retries	Displays the retry times when the connection to the RADIUS server fails.
Secondary Host Name	Displays the host name, the IPv4 address, or the IPv6 address of the secondary RADIUS server.
Secondary Port Number	Displays the port number of the secondary RADIUS server.
External User Group Mapping - Authentication Protocol	Displays the LDAP protocol to use.
External User Group Mapping - DNS Lookup	<p>Displays whether to search for the LDAP server using the information registered in the SRV records in the DNS server.</p> <ul style="list-style-type: none"> <li>▪ Enable: Performs the search using information registered in the SRV records in the DNS server.</li> <li>▪ Disable: Performs the search using the host name and the port number.</li> </ul>
External User Group Mapping - Host Name	Displays the host name, the IPv4 address, or the IPv6 address of the LDAP server.
External User Group Mapping - Port Number	Displays the port number of the LDAP server.
External User Group Mapping - Domain Name	Displays the domain name of the LDAP server.
External User Group Mapping - Base DN	Displays the base DN to search for users to authenticate.
External User Group Mapping - Search User's DN	Displays the search user's domain name.
External User Group Mapping - Password	Displays asterisks (*) to mask the password of the user for searching.
External User Group Mapping - Timeout	Displays the number of seconds before connection to the LDAP server times out.

Item	Description
External User Group Mapping - Retry Interval	Displays the retry interval in seconds when the connection to the LDAP server fails.
External User Group Mapping - Number of Retries	Displays the retry times when the connection to the LDAP server fails.
Setup Server	Displays the <b>Setup Server</b> window.

## Kerberos Properties window

To open this window, select Kerberos in the **External Authentication** window.



The following table describes the fields and settings used to edit the Kerberos properties.

Item	Description
DNS Lookup	Displays whether to search for the Kerberos server using the information registered in the SRV records in the DNS server. <ul style="list-style-type: none"> <li>Enable: Performs the search using information registered in the SRV records in the DNS server.</li> <li>Disable: Performs the search using the host name and the port number.</li> </ul>
Realm Name	Displays the default realm name.
Primary Host Name	Displays the name of the Kerberos server.

Item	Description
Primary Port Number	Displays the port number of the Kerberos server.
Clock Skew	Displays the acceptable range of time difference between the SVP and the Kerberos server.
Timeout	Displays the number of seconds before connection to the Kerberos server times out.
Secondary Host Name	Displays the name of the secondary Kerberos server.
Secondary Port Number	Displays the port number of the secondary Kerberos server.
External User Group Mapping - Authentication Protocol	Displays the LDAP protocol to use.
External User Group Mapping - Primary Port Number	Displays the port number of the LDAP server.
External User Group Mapping - Base DN	Displays the base domain name to search for users to authenticate.
External User Group Mapping - Search User's DN	Displays the search user's domain name.
External User Group Mapping - Password	Displays asterisks (*) to mask the password of the user for searching.
External User Group Mapping - Timeout	Displays the number of seconds before connection to the LDAP server times out.
External User Group Mapping - Retry Interval	Displays the retry interval in seconds when the connection to the LDAP server fails.
External User Group Mapping - Number of Retries	Displays the retry times when the connection to the LDAP server fails.
External User Group Mapping - Secondary Port Number	Displays the port number of the secondary LDAP server.
Setup Server	Displays the <b>Setup Server</b> window.

# Setup Server for LDAP

## LDAP Setup Server window

To open this window, select LDAP in the **Select Authentication Server** window.

The following table describes the fields and settings used to edit the server information.

Item	Description
Certificate File Name	Specify a certificate file. Click Browse to find the file.



Item	Description
DNS Lookup	<p>Specify whether to search for the LDAP server using the information registered in the SRV records in the DNS server.</p> <ul style="list-style-type: none"> <li>▪ Enable: Performs the search using information registered in the SRV records in the DNS server.</li> <li>▪ Disable: Performs the search using the host name and the port number.</li> </ul>
Authentication Protocol	<p>Specify an LDAP protocol to use. Available protocols are as follows.</p> <ul style="list-style-type: none"> <li>▪ LDAP over SSL/TLS</li> <li>▪ STARTTLS</li> </ul> <p>If you select Enable in DNS Lookup, you cannot select LDAP over SSL/TLS.</p>
External User Group Mapping	<p>Specify whether to connect an authentication server to an authorization server.</p> <ul style="list-style-type: none"> <li>▪ Enable: Connects an authentication server to an authorization server.</li> <li>▪ Disable: Does not connect an authentication server to an authorization server.</li> </ul>
External User Group Mapping - Host Name	<p>Specify a host name of the LDAP server.</p> <p>ASCII code characters, hyphens (-), and periods (.) can be specified.</p> <p>If you select Enable in DNS Lookup, this item is disabled.</p>
External User Group Mapping - Port Number	<p>Specify a port number of the LDAP server.</p> <p>If you select Enable in DNS Lookup, this item is disabled.</p>
External User Group Mapping - Domain Name	<p>Specify a domain name that the LDAP server manages.</p> <p>You can specify ASCII code characters, hyphens (-), and periods (.).</p>
External User Group Mapping - User Name Attribute	<p>Specify an attribute name to identify a user, such as a user ID.</p> <p>You can specify ASCII code characters and the following symbols:</p>

Item	Description
	<p>! # \$ % &amp; ' ( ) * + , - . / : ; &lt; = &gt; ? @ [ \ ] ^ _ ` {   } ~</p> <ul style="list-style-type: none"> <li>▪ Hierarchical model Specify an attribute name where the value that can identify a user is stored.</li> <li>▪ Flat model Specify an attribute name for a user entry's RDN.</li> </ul>
External User Group Mapping - Timeout	Specify the number of seconds before connection to the LDAP server times out.
External User Group Mapping - Retry Interval	Specify a retry interval in seconds when the connection to the LDAP server fails.
External User Group Mapping - Number of Retries	Specify retry times when the connection to the LDAP server fails.
External User Group Mapping - Base DN	Displays the base DN to search for users to authenticate.
External User Group Mapping - Search User's DN	Displays the search user's domain name.
External User Group Mapping - Password	<p>Search for a user by specifying his password. Search for a user by specifying his password. Specify the same password that is registered in the LDAP server.</p> <p>You can specify ASCII code characters and the following symbols:</p> <p>! # \$ % &amp; ' ( ) * + - . = @ \ ^ _  </p> <p>If you specify <code>sAMAccountName</code> in External User Group Mapping - User Name Attribute, or if you select Enable in External User Group Mapping, this item must be specified.</p>
External User Group Mapping - Re-enter Password	<p>Re-enter the password of the user group you are searching for to confirm your entry.</p> <p>You can specify ASCII code characters and the following symbols:</p> <p>! # \$ % &amp; ' ( ) * + - . = @ \ ^ _  </p> <p>If you enter any password in External User Group Mapping - Password, you must specify this item.</p>

Item	Description
Secondary Server	Specify whether to use a secondary LDAP server. <ul style="list-style-type: none"> <li>▪ Enable: Uses a secondary LDAP server.</li> <li>▪ Disable: Does not use a secondary LDAP server.</li> </ul> If you select Enable in DNS Lookup, this item is disabled.
Secondary Server - Host Name	Specify a host name of the secondary LDAP server. You can specify ASCII code characters, hyphens (-), and periods (.). If you select Disable in Secondary Server, this item is disabled.
Secondary Server -Port Number	Specify a port number of the secondary LDAP server. If you select Disable in Secondary Server, this item is disabled.
Test User Name	Specify a user name for a server connection test. You can specify ASCII code characters and the following symbols: ! # \$ % & ' * + - . / = ? @ ^ _ ` {   } ~
Password	Specify a password of the user name for a server connection test. You can specify ASCII code characters and the following symbols: ! # \$ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` {   } ~
Server Configuration Test	Click Check to conduct a server connection test for the authentication server and the authorization server based on the specified settings.
Server Configuration Test - Result	Displays a result of the server connection test for the authentication server and the authorization server.



Item	Description
	<ul style="list-style-type: none"> <li>▪ RADIUS: Users are authenticated with user information registered in the RADIUS server.</li> <li>▪ Kerberos: Users are authenticated with user information registered in the Kerberos server.</li> </ul>

### Setup Server

Item	Description
Certificate File Name	Displays the certificate file.
DNS Lookup	<p>Displays whether to search for the LDAP server using the information registered in the SRV records in the DNS server.</p> <ul style="list-style-type: none"> <li>▪ Enable: Performs the search using information registered in the SRV records in the DNS server.</li> <li>▪ Disable: Performs the search using the host name and the port number.</li> </ul>
Authentication Protocol	Displays the LDAP protocol.
External User Group Mapping	<p>Displays whether to connect an authentication server to an authorization server.</p> <ul style="list-style-type: none"> <li>▪ Enable: Connects an authentication server to an authorization server.</li> <li>▪ Disable: Does not connect an authentication server to an authorization server.</li> </ul>
Primary Host Name	Displays the host name of the LDAP server.
Primary Port Number	Displays the port number of the LDAP server.
Domain Name	Displays the domain name that the LDAP server manages.
User Name Attribute	Displays the attribute name to identify a user.
Base DN	Displays the base DN for searching for users to authenticate.
Search User's DN	Displays the DN of a user for searching.
Password	Displays asterisks (*) to mask the password of the user for searching.

Item	Description
Timeout	Displays the number of seconds before connection to the LDAP server times out.
Retry Interval	Displays the retry interval in seconds when the connection to the LDAP server fails.
Number of Retries	Displays the retry times when the connection to the LDAP server fails.
Secondary Host name	Displays the host name of the secondary LDAP server.
Secondary Port Number	Displays the port number of the secondary LDAP server.

## Setup Server for RADIUS

### RADIUS Setup Server window

To open this window, select RADIUS in the **Select Authentication Server** window.

The following table describes the fields and settings used to edit server RADIUS information.

Item	Description
Authentication Protocol	Specify a RADIUS protocol to use. <ul style="list-style-type: none"> <li>▪ PAP: Password authentication protocol that transmits plaintext user ID and password.</li> <li>▪ CHAP: Challenge-handshake authentication protocol that transmits encrypted password.</li> </ul>
Host Name	Specify a name of the RADIUS server.

Item	Description
	You can specify ASCII code characters, hyphens (-), and periods (.).
Secret	<p>Specify a RADIUS secret key used for the PAP authentication or the CHAP authentication.</p> <p>You can specify ASCII code characters and the following symbols: ! # \$ % &amp; ' ( ) * + - . = @ \ ^ _  </p>
Re-enter Secret	<p>Re-enter the RADIUS secret key to confirm your entry.</p> <p>You can specify ASCII code characters and the following symbols: ! # \$ % &amp; ' ( ) * + - . = @ \ ^ _  </p>
NAS Address	<p>Specify an identifier for the RADIUS server to find SVP.</p> <ul style="list-style-type: none"> <li>▪ To specify a host name, select Identifier and enter the host name. You can specify ASCII code characters and the following symbols: ! " # \$ % &amp; ' ( ) * + , - . / ; : &lt; &gt; = ? @ [ \ ] ^ _ { } ~</li> <li>▪ To specify an IPv4 address, select IPv4 and enter 4 numbers (0-255). For example: XXX.XXX.XXX.XXX (X indicates a digit) Specify only numbers. Do not specify any periods.</li> <li>▪ To specify an IPv6 address, select IPv6 and enter 8 hexadecimal numbers (0-FFFF). For example: YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY (Y indicates a hexadecimal digit) Enter 0 to omit a segment.</li> </ul>
Port Number	Specify a port number of the RADIUS server.
Timeout	Specify the number of seconds before connection to the RADIUS server times out.
Number of Retries	Specify the retry times when the connection to the RADIUS server fails.



Item	Description
Secondary Server	<p>Specify whether to use a secondary RADIUS server and a secondary LDAP server.</p> <ul style="list-style-type: none"> <li>▪ Enable: Uses secondary servers.</li> <li>▪ Disable: Does not use secondary servers.</li> </ul>
Secondary Server - Host Name	<p>Specify a name of the secondary RADIUS server.</p> <p>You can specify ASCII code characters, hyphens (-), and periods (.).</p> <p>If you select Disable in Secondary Server, this item is disabled.</p>
Secondary Server - Port Number	<p>Specify a port number of the secondary RADIUS server.</p> <p>If you select Disable in Secondary Server, this item is disabled.</p>
External User Group Mapping	<p>Specify whether to connect an authentication server to an authorization server.</p> <ul style="list-style-type: none"> <li>▪ Enable: Connects an authentication server to an authorization server.</li> <li>▪ Disable: Does not connect an authentication server to an authorization server.</li> </ul>
External User Group Mapping - Certificate File Name	<p>Specify a certificate file. Click Browse to find the file.</p> <p>If you select Disable in External User Group Mapping, this item is disabled.</p>
External User Group Mapping - DNS Lookup	<p>Specify whether to search for the LDAP server using the information registered in the SRV records in the DNS server.</p> <ul style="list-style-type: none"> <li>▪ Enable: Performs the search using information registered in the SRV records in the DNS server.</li> <li>▪ Disable: Performs the search using the host name and the port number.</li> </ul> <p>If you select Disable in External User Group Mapping, this item is disabled.</p>
External User Group Mapping - Authentication Protocol	<p>Specify an LDAP protocol to use. Available protocols are as follows.</p> <ul style="list-style-type: none"> <li>▪ LDAP over SSL/TLS</li> <li>▪ STARTTLS</li> </ul> <p>If you select Enable in DNS Lookup, you cannot select LDAP over SSL/TLS.</p> <p>If you select Disable in External User Group Mapping, this item is disabled.</p>

Item	Description
External User Group Mapping - Host Name	<p>Specify a host name of the LDAP server.</p> <p>You can specify ASCII code characters, hyphens (-), and periods (.).</p> <p>If you select Enable in DNS Lookup, or if you select Disable in External User Group Mapping, this item is disabled.</p>
External User Group Mapping - Port Number	<p>Specify a port number of the LDAP server.</p> <p>If you select Enable in DNS Lookup, or if you select Disable in External User Group Mapping, this item is disabled.</p>
External User Group Mapping - Domain Name	<p>Specify a domain name of the LDAP server.</p> <p>You can specify ASCII code characters, hyphens (-), and periods (.).</p> <p>If you select Disable in External User Group Mapping, this item is disabled.</p>
External User Group Mapping - Base DN	<p>Specify a base DN to search for users to authenticate.</p> <p>Available characters: Alphanumeric characters (ASCII characters) and all symbols.</p> <ul style="list-style-type: none"> <li>▪ Hierarchical model <p>Specify a DN of hierarchy that includes all the targeted users for searching.</p> </li> <li>▪ Flat model <p>Specify a DN of hierarchy that is one level up of the targeted user for searching.</p> </li> </ul> <p>You can enter alphanumeric characters and all symbols. Note, however, that when you enter symbols like the following, you need to use a backslash to escape for each symbol:</p> <p>+ ; , &lt; = &gt; \ / "</p> <p>In some cases, you may need to use a backslash and an ASCII character to escape.</p> <ul style="list-style-type: none"> <li>▪ \ -&gt; \5c (hexadecimal)</li> <li>▪ / -&gt; \2f (hexadecimal)</li> <li>▪ " -&gt; \22 (hexadecimal)</li> </ul>
External User Group Mapping - Search User's DN	<p>Search for a user by specifying a DN</p> <p>Available characters: Alphanumeric characters (ASCII characters) and all symbols.</p>

Item	Description
	<p>If you specify <code>sAMAccountName</code> in External User Group Mapping - User Name Attribute, or if you select Enable in External User Group Mapping, this item must be specified.</p> <p>You can enter alphanumeric characters and all symbols. Note, however, that when you enter symbols like the following, you need to use a backslash to escape for each symbol:</p> <p>+ ; , &lt; = &gt; \ / "</p> <p>In some cases, you may need to use a backslash and an ASCII character to escape.</p> <ul style="list-style-type: none"> <li>▪ \ -&gt; \5c (hexadecimal)</li> <li>▪ / -&gt; \2f (hexadecimal)</li> <li>▪ " -&gt; \22 (hexadecimal)</li> </ul>
External User Group Mapping - Password	<p>Search for a user by specifying his password. Specify the same password that is registered in the LDAP server.</p> <p>You can specify ASCII code characters and the following symbols:</p> <p>! # \$ % &amp; ' ( ) * + - . = @ \ ^ _  </p> <p>If you select Disable in External User Group Mapping, this item is disabled.</p>
External User Group Mapping - Re-enter Password	<p>Re-enter the password of the user you are searching for to confirm your entry.</p> <p>You can specify ASCII code characters and the following symbols:</p> <p>! # \$ % &amp; ' ( ) * + - . = @ \ ^ _  </p> <p>If you enter any password in External User Group Mapping - Password, you must specify this item.</p> <p>If you select Disable in External User Group Mapping, this item is disabled.</p>
External User Group Mapping - Timeout	<p>Specify the number of seconds before connection to the LDAP server times out.</p> <p>If you select Disable in External User Group Mapping, this item is disabled.</p>
External User Group Mapping - Retry Interval	<p>Specify a retry interval in seconds when the connection to the LDAP server fails.</p> <p>If you select Disable in External User Group Mapping, this item is disabled.</p>
External User Group Mapping - Number of Retries	<p>Specify retry times when the connection to the LDAP server fails.</p>

Item	Description
	If you select Disable in External User Group Mapping, this item is disabled.
Test User Name	Specify a user name for a server connection test. You can specify ASCII code characters and the following symbols: ! # \$ % & ' * + - . / = ? @ ^ _ ` {   } ~
Password	Specify a password of the user name for a server connection test. You can specify ASCII code characters and the following symbols: ! # \$ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` {   } ~
Server Configuration Test	Click Check to conduct a server connection test for the authentication server and the authorization server based on the specified settings.
Server Configuration Test - Result	Displays a result of the server connection test for the authentication server and the authorization server.

## RADIUS Setup Server confirmation window

1. Select Authentication Server > 2. Set Up Server > 3. Confirm

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

Task Name:  (Max. 32 Characters)

Selected Server	
External Authentication	
RADIUS	
Total: 1	

Set Up Server						
Authentication ...	Primary Host Name	Secret	NAS Address	Primary Port Number	Timeout (sec.)	Num Re
PAP	sample	*****	xx.xxx.xx.xx	1812	10	
Total: 1						

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

### Selected Server

The following table describes the fields and settings in the Server section of the confirmation window for (RADIUS Setup Server) window.

Item	Description
External Authentication	<p>Displays the type of the authentication server.</p> <ul style="list-style-type: none"> <li>Disable: Does not use any authentication server. Users are authenticated with user information registered in the SVP.</li> <li>LDAP: Users are authenticated with user information registered in the LDAP server.</li> <li>RADIUS: Users are authenticated with user information registered in the RADIUS server.</li> <li>Kerberos: Users are authenticated with user information registered in the Kerberos server.</li> </ul>

## Setup Server

The following table describes the fields and settings in the Setup Server section of the confirmation window for (RADIUS Setup Server) window.

Item	Description
Authentication Protocol	Displays the RADIUS protocol to use. <ul style="list-style-type: none"> <li>▪ PAP: Password authentication protocol that transmits plaintext user ID and password.</li> <li>▪ CHAP: Challenge-handshake authentication protocol that transmits encrypted password.</li> </ul>
Primary Host Name	Displays the name of the RADIUS server.
Secret	Displays asterisks (*) to mask the RADIUS secret key used for the PAP authentication or the CHAP authentication.
NAS Address	Displays the identifier for the RADIUS server to find SVP.
Primary Port Number	Displays the port number of the RADIUS server.
Timeout	Displays the number of seconds before connection to the RADIUS server times out.
Number of Retries	Displays the retry times when the connection to the RADIUS server fails.
Secondary Host Name	Displays the name of the secondary RADIUS server.
Secondary Port Number	Displays the port number of the secondary RADIUS server.
External User Group Mapping - Certificate File Name	Displays the certificate file.
External User Group Mapping - Authentication Protocol	Displays the LDAP protocol to use.
External User Group Mapping - DNS Lookup	Displays whether to search for the LDAP server using the information registered in the SRV records in the DNS server. <ul style="list-style-type: none"> <li>▪ Enable: Performs the search using information registered in the SRV records in the DNS server.</li> <li>▪ Disable: Performs the search using the host name and the port number.</li> </ul>

Item	Description
External User Group Mapping - Host Name	Displays the LDAP server host name
External User Group Mapping - Port Number	Displays the LDAP server port number
External User Group Mapping - Domain Name	Displays the LDAP server domain name.
External User Group Mapping - Base DN	Displays the base DN to search for users to authenticate.
External User Group Mapping - Search User's DN	Displays the user's DN for searching.
External User Group Mapping - Password	Displays asterisks (*) to mask the password of the user for searching.
External User Group Mapping - Timeout	Displays the number of seconds before connection to the LDAP server times out.
External User Group Mapping - Retry Interval	Displays the retry interval in seconds when the connection to the LDAP server fails.
External User Group Mapping - Number of Retries	Displays the retry times when the connection to the LDAP server fails.

## Setup Server for Kerberos

### Kerberos Setup Server window

To open this window, select Kerberos in the **Select Authentication Server** window.

The following table describes the fields and settings in the Setup Server section of Kerberos window.

Item	Description
DNS Lookup	Specify whether to search for the Kerberos server using the information registered in the SRV records in the DNS server. <ul style="list-style-type: none"> <li>Enable: Performs the search using information registered in the SRV records in the DNS server.</li> <li>Disable: Performs the search using the host name and the port number.</li> </ul>
Realm Name	Specify a default realm name.



Item	Description
	You can specify ASCII code characters and hyphens (-).
Host Name	Specify a host name of the Kerberos server. You can specify ASCII code characters, hyphens (-), and periods (.). If you select Enable in DNS Lookup, this item is disabled.
Port Number	Specify a port number of the Kerberos server. If you select Enable in DNS Lookup, this item is disabled.
Clock Skew	Specify an acceptable range of time difference between the SVP and the Kerberos server.
Timeout	Specify the number of seconds before connection to the Kerberos server times out.
Secondary Server	Specify whether to use a secondary Kerberos server. <ul style="list-style-type: none"> <li>▪ Enable: Uses the secondary server.</li> <li>▪ Disable: Does not use the secondary server.</li> </ul> If you specify Enable in DNS Lookup, this item is disabled.
Secondary Server - Host Name	Specify a name of the secondary Kerberos server. You can specify ASCII code characters, hyphens (-), and periods (.). If you select Enable in DNS Lookup, or if you select Disable in Secondary Server, this item is disabled.
Secondary Server - Port Number	Specify a port number of the secondary Kerberos server. If you select Enable in DNS Lookup, or if you select Disable in Secondary Server, this item is disabled.
External User Group Mapping	Specify whether to connect an authentication server to an authorization server. <ul style="list-style-type: none"> <li>▪ Enable: Connects an authentication server to an authorization server.</li> <li>▪ Disable: Does not connect an authentication server to an authorization server.</li> </ul>
External User Group Mapping - Certificate File Name	Specify a certificate file. Click Browse to find the file. If you select Disable in External User Group Mapping, this item is disabled.

Item	Description
External User Group Mapping - Authentication Protocol	<p>Specify an LDAP protocol to use. Available protocols are:</p> <ul style="list-style-type: none"> <li>▪ LDAP over SSL/TLS</li> <li>▪ STARTTLS</li> </ul> <p>If you select Enable in DNS Lookup, you cannot select LDAP over SSL/TLS.</p> <p>If you select Disable in External User Group Mapping, this item is disabled.</p>
External User Group Mapping - Primary Port Number	<p>Specify a port number of the LDAP server.</p> <p>If you select Enable in DNS Lookup, or if you select Disable in External User Group Mapping, this item is disabled.</p>
External User Group Mapping - Secondary Port Number	<p>Specify a port number of the secondary LDAP server.</p> <p>If you select Disable in Secondary Server, Enable in DNS Lookup, or External User Group Mapping fields, this item is disabled.</p>
External User Group Mapping - Base DN	<p>Specify a base DN to search for users to authenticate.</p> <p>Available characters: Alphanumeric characters (ASCII characters) and all symbols.</p> <ul style="list-style-type: none"> <li>▪ Hierarchical model <p>Specify a DN of hierarchy that includes all the targeted users for searching.</p> </li> <li>▪ Flat model <p>Specify a DN of hierarchy that is one level up of the targeted user for searching.</p> </li> </ul> <p>You can enter alphanumeric characters and all symbols. Note, however, that when you enter symbols like the following, you need to use a backslash to escape for each symbol:</p> <p>+ ; , &lt; = &gt; \ / "</p> <p>In some cases, you may need to use a backslash and an ASCII character to escape.</p> <ul style="list-style-type: none"> <li>▪ \ -&gt; \5c (hexadecimal)</li> <li>▪ / -&gt; \2f (hexadecimal)</li> <li>▪ " -&gt; \22 (hexadecimal)</li> </ul>
External User Group Mapping - Search User's DN	<p>Search for a user by specifying a DN</p> <p>Available characters: Alphanumeric characters (ASCII characters) and all symbols.</p>

Item	Description
	<p>If you specify <code>sAMAccountName</code> in External User Group Mapping - User Name Attribute, or if you select Enable in External User Group Mapping, this item must be specified.</p> <p>If you select Disable in External User Group Mapping, this item is disabled.</p> <p>You can enter alphanumeric characters and all symbols. Note, however, that when you enter symbols like the following, you need to use a backslash to escape for each symbol:</p> <p>+ ; , &lt; = &gt; \ / "</p> <p>In some cases, you may need to use a backslash and an ASCII character to escape.</p> <ul style="list-style-type: none"> <li>▪ \ -&gt; \5c (hexadecimal)</li> <li>▪ / -&gt; \2f (hexadecimal)</li> <li>▪ " -&gt; \22 (hexadecimal)</li> </ul>
External User Group Mapping - Password	<p>Search for a user by specifying his password. Specify the same password that is registered in the LDAP server.</p> <p>You can specify ASCII code characters and the following symbols:</p> <p>! # \$ % &amp; ' ( ) * + - . = @ \ ^ _  </p> <p>If you select Disable in External User Group Mapping, this item is disabled.</p>
External User Group Mapping - Re-enter Password	<p>Re-enter the password of the user you are searching for to confirm your entry.</p> <p>You can specify ASCII code characters and the following symbols:</p> <p>! # \$ % &amp; ' ( ) * + - . = @ \ ^ _  </p> <p>If you enter any password in External User Group Mapping - Password, you must specify this item.</p> <p>If you select Disable in External User Group Mapping, this item is disabled.</p>
External User Group Mapping - Timeout	<p>Specify the number of seconds before connection to the LDAP server times out.</p> <p>If you select Disable in External User Group Mapping, this item is disabled.</p>
External User Group Mapping - Retry Interval	<p>Specify a retry interval in seconds when the connection to the LDAP server fails.</p> <p>If you select Disable in External User Group Mapping, this item is disabled.</p>

Item	Description
External User Group Mapping - Number of Retries	Specify retry times when the connection to the LDAP server fails. If you select Disable in External User Group Mapping, this item is disabled.
Test User Name	Specify a user name for a server connection test. You can specify ASCII code characters and the following symbols: ! # \$ % & ' * + - . / = ? @ ^ _ ` {   } ~
Password	Specify a password of the user name for a server connection test. You can specify ASCII code characters and the following symbols: ! # \$ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` {   } ~
Server Configuration Test	Click Check to conduct a server connection test for the authentication server and the authorization server based on the specified settings.
Server Configuration Test - Result	Displays a result of the server connection test for the authentication server and the authorization server.

## Kerberos Setup Server confirmation window

Set Up Server

1. Select Authentication Server > 2. Set Up Server > 3. Confirm

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

Task Name:  (Max. 32 Characters)

Selected Server	
External Authentication	
Kerberos	
Total: 1	

Set Up Server						
DNS Lookup	Realm Name	Primary Host Name	Primary Port Number	Clock Skew (sec.)	Timeout (sec.)	Se Ho
Disable	example	example	88	300	10	-
Total: 1						

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

### Selected Server

The following table describes the fields and settings in the Server section of the confirmation window for Kerberos Setup Server).

Item	Description
External Authentication	<p>Displays the type of the authentication server.</p> <ul style="list-style-type: none"> <li>▪ Disable: Does not use any authentication server. Users are authenticated with user information registered in the SVP.</li> <li>▪ LDAP: Users are authenticated with user information registered in the LDAP server.</li> <li>▪ RADIUS: Users are authenticated with user information registered in the RADIUS server.</li> <li>▪ Kerberos: Users are authenticated with user information registered in the Kerberos server.</li> </ul>

## Setup Server

The following table describes the fields and settings in the Setup Server section of the confirmation window for Kerberos Setup Server.

Item	Description
DNS Lookup	Displays whether to search for the Kerberos server using the information registered in the SRV records in the DNS server. <ul style="list-style-type: none"> <li>▪ Enable: Performs the search using information registered in the SRV records in the DNS server.</li> <li>▪ Disable: Performs the search using the host name and the port number.</li> </ul>
Realm Name	Displays the default realm name.
Primary Host Name	Displays the name of the Kerberos server.
Primary Port Number	Displays the port number of the Kerberos server.
Clock Skew	Displays the acceptable range of time difference between the SVP and the Kerberos server.
Timeout	Displays the number of seconds before connection to the Kerberos server times out.
Secondary Host Name	Displays the name of the secondary Kerberos server.
Secondary Port Number	Displays the port number of the secondary Kerberos server.
External User Group Mapping - Certificate File Name	Displays the certificate file.
External User Group Mapping - Authentication Protocol	Displays the LDAP protocol to use.
External User Group Mapping - Primary Port Number	Displays the port number of the LDAP server.
External User Group Mapping - Base DN	Displays the base DN to search for users to authenticate.

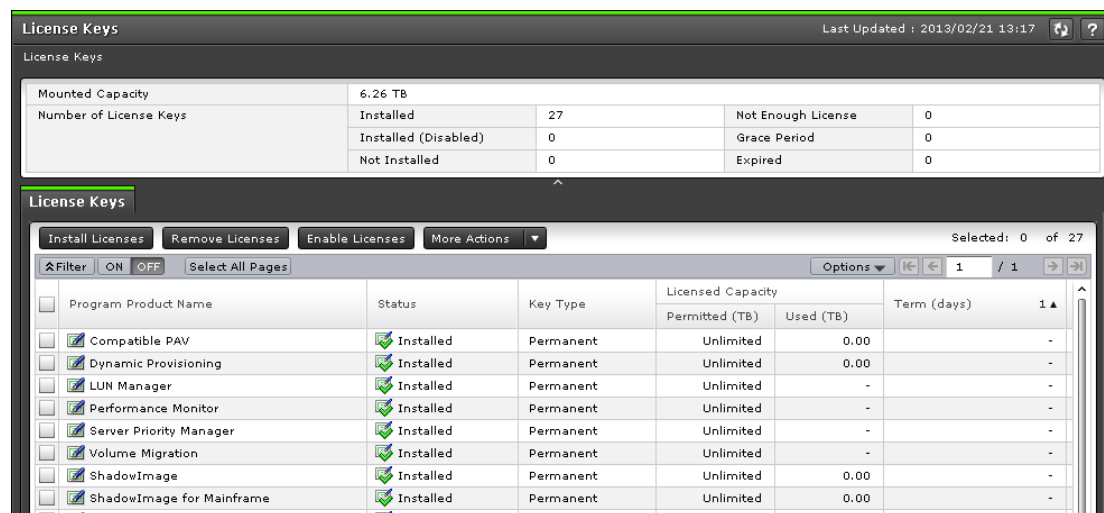
Item	Description
External User Group Mapping - Search User's DN	Displays the search user's domain name.
External User Group Mapping - Password	Displays asterisks (*) to mask the password of the user for searching.
External User Group Mapping - Timeout	Displays the number of seconds before connection to the LDAP server times out.
External User Group Mapping - Retry Interval	Displays the retry interval in seconds when the connection to the LDAP server fails.
External User Group Mapping - Number of Retries	Displays the retry times when the connection to the LDAP server fails.
External User Group Mapping - Secondary Port Number	Displays the port number of the secondary LDAP server.

# Appendix B: Device Manager - Storage Navigator licenses GUI reference

This section describes the Device Manager - Storage Navigator windows that you use to view and manage the licenses for the software applications on your storage system.

## License Keys window

Use the **License Keys** window to install and uninstall license keys.



### Summary

The following table describes the fields and settings in the Summary section of the **License Keys** window.

Item	Description
Mounted capacity	Displays the capacity of internal and external volumes created in the storage system. When you install the software whose license capacity type is Mounted Capacity, install more license capacity than the mounted capacity to keep the software in Installed status. Values are rounded up to the second decimal place.



Item	Description
Number of License Keys	Numbers of license keys are displayed for each status.

### License Keys

The following table describes the fields and settings in the License Keys section of the **License Keys** window.

Item	Description
Program Product Name	Name of the software application
Status	<p>The current status of the software</p> <ul style="list-style-type: none"> <li>▪ Installed: The software is available.</li> <li>▪ Installed (Disabled): Installation is complete, but the license is set to Disabled. This status might appear if an error occurs after you install software. Resolve the error and enable the license. This status also appears when the license key of this software is installed but the license key of the prerequisite software has expired.</li> <li>▪ Not Installed: The software is not installed.</li> <li>▪ Not Enough License: Installation is complete, but the license capacity is insufficient. Not Enough License might remain displayed when the licensed capacity exceeds the mounted capacity after you reduce the number of LDEVs, or when the licensed capacity exceeds the used capacity after you delete pairs or pool volumes. In these cases, you can update the license status by selecting Update License Status and then installing the software.</li> <li>▪ Grace Period: The licensed capacity is insufficient because LDEVs are added, or copy pairs are created, or pool volumes are added. The license expires in 30 days. Please purchase the licenses before the license key expires. Grace Period might remain displayed when the licensed capacity exceeds the mounted capacity after you reduce the number of LDEVs, or when the licensed capacity exceeds the used capacity after you delete pairs or pool volumes. In these cases, you can update the license status by selecting Update License Status and then installing the software.</li> <li>▪ Expired: The term has already expired for the temporary key. When the status is Expired, you cannot re-install the temporary key.</li> </ul>

Item	Description
Key Type	<p>The license key type:</p> <ul style="list-style-type: none"> <li>▪ permanent</li> <li>▪ term</li> <li>▪ temporary</li> <li>▪ emergency</li> </ul> <p>This field is blank if no license key is installed.</p>
Licensed Capacity	<ul style="list-style-type: none"> <li>▪ Permitted (TB): Displays the permitted volume capacity for this software in integers. If no upper limit value is set for the capacity, "Unlimited" displays. This field is blank if no license is installed.</li> <li>▪ Used (TB): Capacity of the volumes used by the software. Up to the second decimal place is displayed. The third decimal place is rounded up. If the license capacity type is other than Used, a hyphen (-) displays. If no license is installed, a blank displays.</li> </ul> <p>Licensed capacity displayed is found from calculations based on the following:</p> <p>1k byte = 1,024 bytes, 1M byte = 1,024 kilobytes, 1G byte = 1,024 megabytes, 1T byte = 1,024 gigabytes</p>
Term (days)	<p>The number of days remaining before the expiration of a temporary key, an emergency key, or a term key. After the temporary key has expired, the column shows the number of days that remain before you can reinstall the temporary key. If there is no limit on validity, a hyphen (-) displays. This field is blank if no license is installed.</p>
Install Licenses	Opens the <b>Install Licenses</b> window
Uninstall Licenses	Opens the <b>Uninstall Licenses</b> window
Enable	Opens the <b>Enable Licenses</b> window
Disable*	Opens the <b>Disable Licenses</b> window
Update License Status*	Opens the <b>Update License Status</b> window
Export*	Displays a window that shows the information in the table
* Appears when you click More Actions.	

## Install Licenses wizard

This topic describes the **Install Licenses** wizard.

### Install Licenses window

Item	Description
License Key	<p>Select whether to enter a key code or specify a license key file.</p> <ul style="list-style-type: none"> <li>Key Code: Enter a key code to install the software. Use the license key code for the software to be installed.</li> <li>File: Specify a license key file to install software. Click Browse and specify the license key file.</li> </ul>
Add button	Adds the specified license key to the Selected License Keys table.

## Selected License Keys

Item	Description
Program Product Name	Name of the software application
Status	<p>The current status of the software</p> <ul style="list-style-type: none"> <li>▪ Installed: The software is available.</li> <li>▪ Installed (Disabled): Installation is complete, but the license is set to Disabled. This status might appear if an error occurs after you install software. Resolve the error and enable the license. This status also appears when the license key of this software is installed but the license key of the prerequisite software has expired.</li> <li>▪ Not Installed: The software is not installed.</li> <li>▪ Not Enough License: Installation is complete, but the license capacity is insufficient. Not Enough License might remain displayed when the licensed capacity exceeds the mounted capacity after you reduce the number of LDEVs, or when the licensed capacity exceeds the used capacity after you delete pairs or pool volumes. In these cases, you can update the license status by selecting Update License Status and then installing the software.</li> <li>▪ Grace Period: The licensed capacity is insufficient because LDEVs are added, or copy pairs are created, or pool volumes are added. The license expires in 30 days. Please purchase the licenses before the license key expires. Grace Period might remain displayed when the licensed capacity exceeds the mounted capacity after you reduce the number of LDEVs, or when the licensed capacity exceeds the used capacity after you delete pairs or pool volumes. In these cases, you can update the license status by selecting Update License Status and then installing the software.</li> <li>▪ Expired: The term has already expired for the temporary key. When the status is Expired, you cannot re-install the temporary key.</li> </ul>
Key Type	<p>The license key type:</p> <ul style="list-style-type: none"> <li>▪ permanent</li> <li>▪ term</li> <li>▪ temporary</li> <li>▪ emergency</li> </ul> <p>This field is blank if no license key is installed.</p>

Item	Description
Licensed Capacity	<ul style="list-style-type: none"> <li>▪ Permitted (TB): The window displays the permitted volume capacity for this software in integers. If no upper limit value is set for the capacity, "Unlimited" displays. This field is blank if no license is installed.</li> <li>▪ Used (TB): This is the capacity of the volumes used by the software. Up to the second decimal place is displayed. The third decimal place is rounded up. If the license capacity type is other than Used, a hyphen (-) displays. If no license is installed, a blank displays.</li> </ul> <p>Licensed capacity displayed is found from calculations based on the following:</p> <p>1k byte = 1,024 bytes, 1M byte = 1,024 kilobytes, 1G byte = 1,024 megabytes, 1T byte = 1,024 gigabytes</p>
Term (days)	The number of days remaining before the expiration of a temporary key, an emergency key, or a term key. After the temporary key has expired, the column shows the number of days that remain before you can reinstall the temporary key. If there is no limit on validity, a hyphen (-) displays. This field is blank if no license is installed.
Enable	Installs license keys in Enabled status. You can select more than one software product.
Disable	Installs license keys in Disabled status. You can select more than one software product.
Clear All	Deletes all license keys from the Selected License Keys table.

## Install Licenses confirmation window

1. Install Licenses > 2. Confirm

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

Task Name:   
(Max. 32 Characters)

Program Product Name	Status	Key Type	Licensed Capacity	
			Permitted (TB)	Used (TB)
Compatible PAV	Install	Permanent	Unlimited	0.00
Dynamic Provisioning	Install	Permanent	Unlimited	0.00
LUN Manager	Install	Permanent	Unlimited	-
Performance Monitor	Install	Permanent	Unlimited	-
Server Priority Manager	Install	Permanent	Unlimited	-
Volume Migration	Install	Permanent	Unlimited	-
ShadowImage	Install	Permanent	Unlimited	0.00
ShadowImage for Mainframe	Install	Permanent	Unlimited	0.00
Compatible FlashCopy(R) V2	Install	Permanent	Unlimited	0.00
TrueCopy	Install	Permanent	Unlimited	0.00
TrueCopy for Mainframe	Install	Permanent	Unlimited	0.00

Total: 27

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

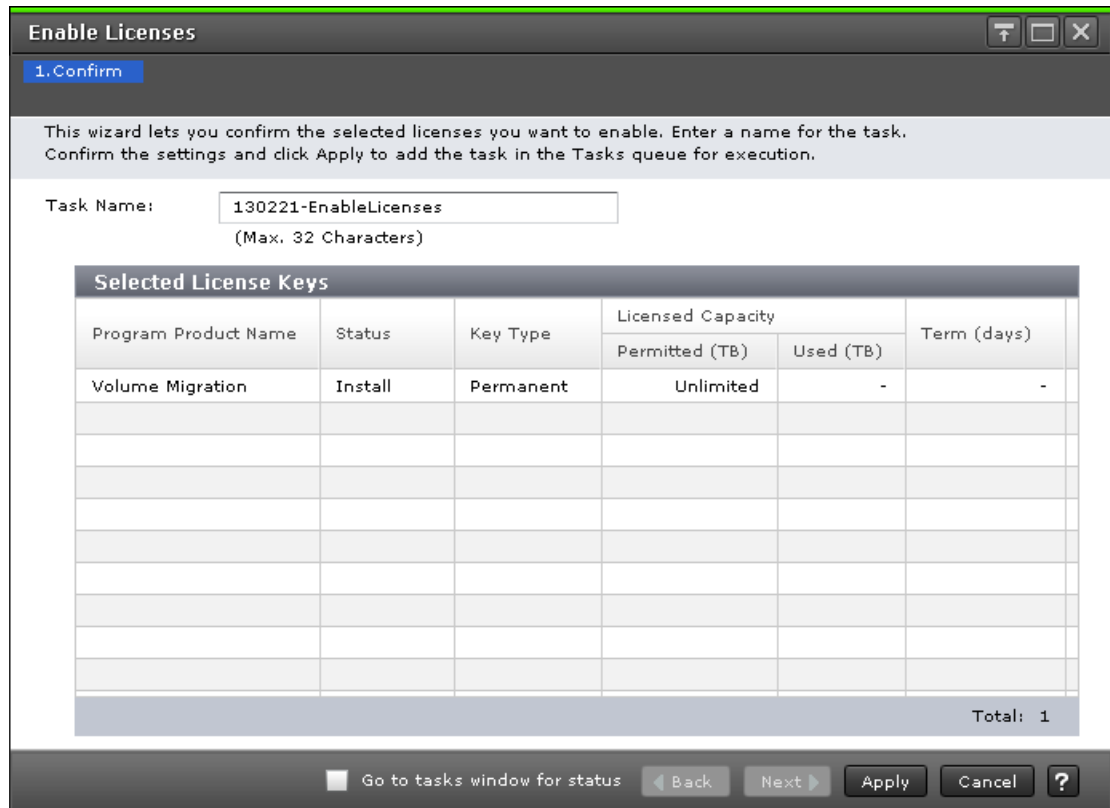
This topic describes the Install Licenses confirmation window.

Item	Description
Program Product Name	Name of the software application
Status	Displays the software's installation status. See the Status item in the Selected License Keys table in the section <a href="#">Install Licenses window (on page 315)</a> .
Key Type	The license key type: <ul style="list-style-type: none"> <li>▪ permanent</li> <li>▪ term</li> <li>▪ temporary</li> <li>▪ emergency</li> </ul> This field is blank if no license key is installed.

Item	Description
Licensed Capacity	<ul style="list-style-type: none"> <li>▪ Permitted (TB): The window displays the permitted volume capacity for this software in integers. If no upper limit value is set for the capacity, "Unlimited" displays. This field is blank if no license is installed.</li> <li>▪ Used (TB): This is the capacity of the volumes used by the software. Up to the second decimal place is displayed. The third decimal place is rounded up. If the license capacity type is other than Used, a hyphen (-) displays. If no license is installed, a blank displays.</li> </ul> <p>Licensed capacity displayed is found from calculations based on the following:</p> <p>1k byte = 1,024 bytes, 1M byte = 1,024 kilobytes, 1G byte = 1,024 megabytes, 1T byte = 1,024 gigabytes</p>
Term (days)	<p>The number of days remaining before the expiration of a temporary key, an emergency key, or a term key. After the temporary key has expired, the column shows the number of days that remain before you can reinstall the temporary key. If there is no limit on validity, a hyphen (-) displays. This field is blank if no license is installed.</p>

## Enable Licenses window

This section describes the **Enable Licenses** window.



The following table describes the fields and settings in the **Enable Licenses** window.

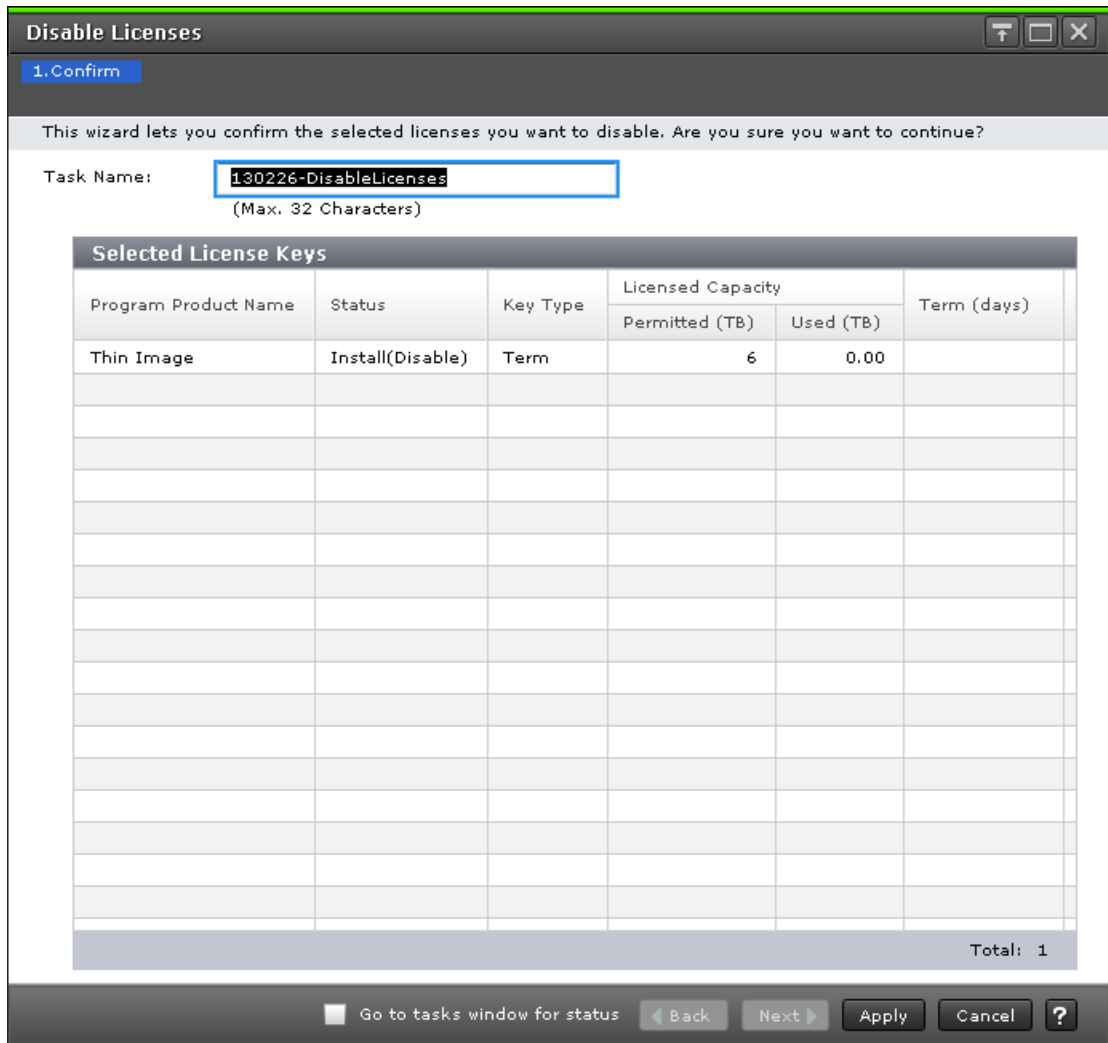
Item	Description
Program Product Name	Name of the software application
Status	Displays the software's installation status. See the Status item in the Selected License Keys table in the section <a href="#">Install Licenses window (on page 315)</a> .
Key Type	The license key type: <ul style="list-style-type: none"> <li>▪ Permanent</li> <li>▪ Term</li> <li>▪ Temporary</li> <li>▪ Emergency</li> </ul> This field is blank if no license key is installed.



Item	Description
Licensed Capacity (TB)	<ul style="list-style-type: none"> <li>▪ Permitted: The window displays the permitted volume capacity for this software in integers. If no upper limit value is set for the capacity, "Unlimited" displays. This field is blank if no license is installed.</li> <li>▪ Used: This is the capacity of the volumes used by the software. Up to the second decimal place is displayed. The third decimal place is rounded up. If the license capacity type is other than Used, a hyphen (-) displays. If no license is installed, a blank displays.</li> </ul> <p>Licensed capacity displayed is found from calculations based on the following:</p> <p>1 KB= 1,024 bytes, 1 MB = 1,024 KB, 1 GB = 1,024 MB, 1 TB= 1,024 GB</p>
Term (days)	<p>The number of days remaining before the expiration of a temporary key, an emergency key, or a term key. After the temporary key has expired, the column shows the number of days that remain before you can reinstall the temporary key. If there is no limit on validity, a hyphen (-) displays. This field is blank if no license is installed.</p>

## Disable Licenses window

This section describes the **Disable Licenses** window.



The following table describes the fields and settings in the **Disable Licenses** window.

Item	Description
Program Product Name	Name of the software application
Status	Displays the software's installation status. See the Status item in the Selected License Keys table in the section <a href="#">Install Licenses window (on page 315)</a> .
Key Type	The license key type: <ul style="list-style-type: none"> <li>▪ Permanent</li> <li>▪ Term</li> <li>▪ Temporary</li> <li>▪ Emergency</li> </ul> This field is blank if no license key is installed.

Item	Description
Licensed Capacity (TB)	<ul style="list-style-type: none"> <li>▪ Permitted: The window displays the permitted volume capacity for this software in integers. If no upper limit value is set for the capacity, "Unlimited" displays. This field is blank if no license is installed.</li> <li>▪ Used: This is the capacity of the volumes used by the software. Up to the second decimal place is displayed. The third decimal place is rounded up. If the license capacity type is other than Used, a hyphen (-) displays. If no license is installed, a blank displays.</li> </ul> <p>Licensed capacity displayed is found from calculations based on the following:</p> <p>1 KB= 1,024 bytes, 1 MB = 1,024 KB, 1 GB = 1,024 MB, 1 TB= 1,024 GB</p>
Term (days)	<p>The number of days remaining before the expiration of a temporary key, an emergency key, or a term key. After the temporary key has expired, the column shows the number of days that remain before you can reinstall the temporary key. If there is no limit on validity, a hyphen (-) displays. This field is blank if no license is installed.</p>

## Remove Licenses window

This topic describes the **Remove Licenses** window.



Item	Description
Licensed Capacity	<ul style="list-style-type: none"> <li>▪ Permitted (TB): The window displays the permitted volume capacity for this software in integers. If no upper limit value is set for the capacity, "Unlimited" displays. This field is blank if no license is installed.</li> <li>▪ Used (TB): This is the capacity of the volumes used by the software. Up to the second decimal place is displayed. The third decimal place is rounded up. If the license capacity type is other than Used, a hyphen (-) displays. If no license is installed, a blank displays.</li> </ul> <p>Licensed capacity displayed is found from calculations based on the following:</p> <p>1 KB= 1,024 bytes, 1 MB = 1,024 KB, 1 GB = 1,024 MB, 1 TB= 1,024 GB</p>
Term (days)	<p>The number of days remaining before the expiration of a temporary key, an emergency key, or a term key. After the temporary key has expired, the column shows the number of days that remain before you can reinstall the temporary key. A hyphen (-) displays if there is no limit on validity, a hyphen (-) displays. This field is blank if no license is installed.</p>

## Update License Status window

This topic describes the **Update License Status** window.



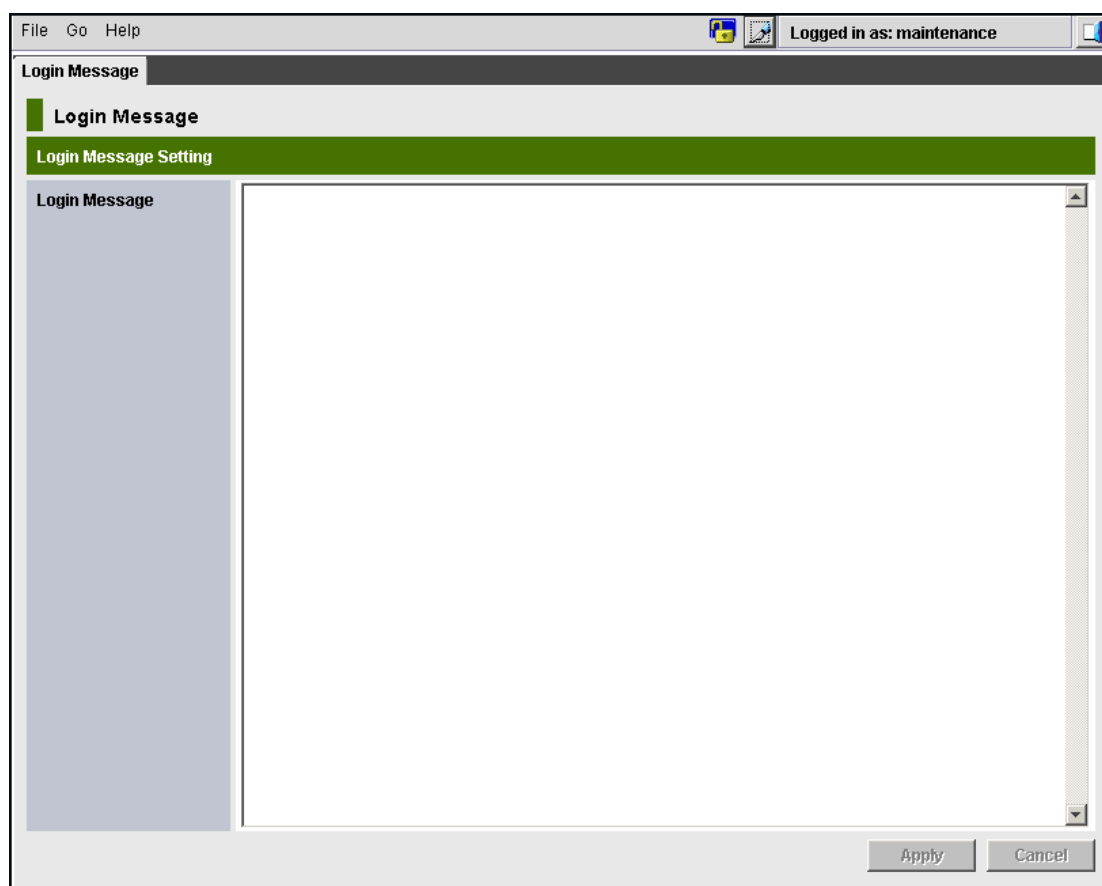
Item	Description
Licensed Capacity	<ul style="list-style-type: none"> <li>▪ Permitted (TB): The window displays the permitted volume capacity for this software in integers. If no upper limit value is set for the capacity, "Unlimited" displays. This field is blank if no license is installed.</li> <li>▪ Used (TB): This is the capacity of the volumes used by the software. Up to the second decimal place is displayed. The third decimal place is rounded up. If the license capacity type is other than Used, a hyphen (-) displays. If no license is installed, a blank displays.</li> </ul> <p>Licensed capacity displayed is found from calculations based on the following:</p> <p>1k byte = 1,024 bytes, 1M byte = 1,024 kilobytes, 1G byte = 1,024 megabytes, 1T byte = 1,024 gigabytes</p>
Term (days)	<p>The number of days remaining before the expiration of a temporary key, an emergency key, or a term key. After the temporary key has expired, the column shows the number of days that remain before you can reinstall the temporary key. If there is no limit on validity, a hyphen (-) displays. This field is blank if no license is installed.</p>

---

## Appendix C: Configuring storage systems GUI reference

This section describes the Device Manager - Storage Navigator windows and wizards that you use to configure storage systems.

### Login Message window



The following table describes the fields and settings in the **Login Message** window.

Item	Description
Login Message	Enter a login message. You can use up to 2,048 alphanumeric characters (ASCII codes) and symbols.



## Edit Storage System wizard

### Edit Storage System window

The following table describes the fields and settings in the **Edit Storage System** window.

Item	Description
Storage System Name	Device name of the storage system.
Contact	Contact information such as personnel and telephone number where you can inquire about the storage system.
Location	Location of the connected storage system.



## Edit Alert Settings window

Item	Description
Notification Alert	<p>Select the destination of the alert notification.</p> <ul style="list-style-type: none"> <li>All: Sends alerts of all SIMs.</li> <li>Host Report: Sends alerts only of SIMs that report to hosts.</li> </ul> <p>Alert destinations are common to Syslog, SNMP, and Email.</p>

### Syslog tab

The screenshot shows the 'Edit Alert Settings' window with the 'Syslog' tab selected. The 'Notification Alert' is set to 'Host Report'. Under the 'Syslog' tab, the 'Transfer Protocol' is set to 'New Syslog Protocol (TLS1.2/RFC5424)'. The 'Primary Server' is enabled with 'IPv4' selected and IP address '127.0.0.1' and port '514'. The 'Secondary Server' is disabled. The 'Location Identification Name' is 'Storage001'. The 'Timeout' is 10 seconds, 'Retry Interval' is 1 second, and 'Number of Retries' is 3. There are buttons for 'Send Test Message to Syslog Server' and 'Reset Settings' at the bottom.

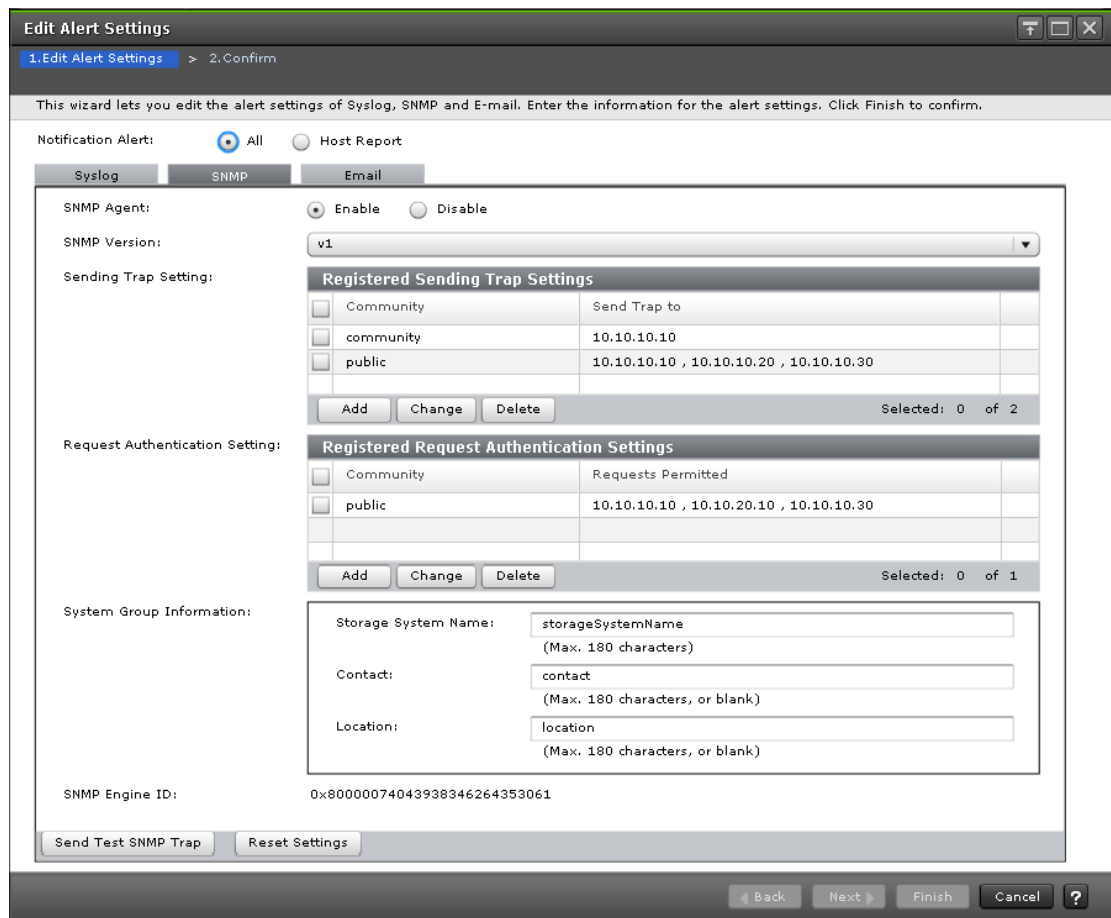
The following table describes the fields and settings in the Syslog tab.

Item	Description
Transfer Protocol	Select the protocol for Syslog transfer. <ul style="list-style-type: none"> <li>▪ New Syslog Protocol (TLS1.2/RFC5424)</li> <li>▪ Old Syslog Protocol (UDP/RFC3164)</li> </ul>
Primary Server	Select whether or not to use the Syslog Server. <ul style="list-style-type: none"> <li>▪ Enable: Reports SIM to the Syslog Server through Syslog.</li> <li>▪ Does not report SIM to the Syslog Server through Syslog.</li> </ul>
Primary Server - Server Setting	Enter the IP address of the server that you want to set as the Syslog Server. You cannot set an address with all 0s. <ul style="list-style-type: none"> <li>▪ IPv4: Enter a valid IPv4 address in the format XXX.XXX.XXX.XXX (where XXX is a number from 0 to 255)</li> <li>▪ IPv6: Enter a valid IPv6 address in the format YYY:YYY:YYY:YYY:YYY:YYY:YYY:YYY: (where YYY is a hexadecimal number from 0 to FFFF).</li> </ul> Use this field only when you select Enable in Primary Server.
Primary Server - Port Number	Enter the port number used by the Syslog Server. Use this field only when you selected Enable in Primary Server.
Primary Server - Client Certificate File Name	Specify a certificate file. Click Browse and specify the certificate file. Use this field only when you select New Syslog Protocol (TLS1.2/RFC5424) in Transfer Protocol and selected Enable in Primary Server.
Primary Server - Password	Enter a password for the client certificate. You can enter up to 128 alphanumeric characters and the following symbols: ! # \$ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` {   } ~ Use this field only when you specified Client Certificate File Name.
Primary Server - Root Certificate File Name	Specify a certificate file. Click Browse and specify the certificate file. Use this field only when you select New Syslog Protocol (TLS1.2/RFC5424) in Transfer Protocol and selected Enable in Primary Server.
Secondary Server	Select whether or not to use an alternate server for the Syslog Server. <ul style="list-style-type: none"> <li>▪ Enable: Reports SIM to the alternate server for the Syslog Server through Syslog.</li> <li>▪ Disable: Does not report SIM to the alternate server for the Syslog Server through Syslog.</li> </ul>

Item	Description
Secondary Server - Server Setting	<p>Enter the IP address of the server that you want to set as the Syslog Server. You cannot set an address with all 0s.</p> <ul style="list-style-type: none"> <li>▪ IPv4: Enter a valid IPv4 address in the format <i>XXX.XXX.XXX.XXX</i> (where <i>XXX</i> is a number from 0 to 255)</li> <li>▪ IPv6: Enter a valid IPv6 address in the format <i>YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY</i>: (where <i>YYYY</i> is a hexadecimal number from 0 to FFFF).</li> </ul> <p>Use this field only when you select Enable in Secondary Server.</p>
Secondary Server - Port Number	Specify a certificate file. Click Browse and specify the certificate file. Use this field only when you select New Syslog Protocol (TLS1.2/RFC5424) in Transfer Protocol and select Enable in Secondary Server.
Secondary Server - Client Certificate File Name	Specify a certificate file. Click Browse and specify the certificate file. Use this field only when you select New Syslog Protocol (TLS1.2/RFC5424) in Transfer Protocol and selected Enable in Secondary Server.
Secondary Server - Password	<p>Enter a password for the client certificate. You can enter up to 128 alphanumeric characters and the following symbols:</p> <p>! # \$ % &amp; ' ( ) * + , - . / : ; &lt; = &gt; ? @ [ \ ] ^ _ ` {   } ~</p> <p>Use this field only when you specify Client Certificate File Name.</p>
Secondary Server - Root Certificate File Name	Specify a certificate file. Click Browse and specify the certificate file. Use this field only when you select New Syslog Protocol (TLS1.2/RFC5424) in Transfer Protocol and selected Enable in Secondary Server.
Location Identification Name	<p>Enter a name for identification of the storage system for which SIM is transferred to the Syslog Server. You can enter up to 32 alphanumeric characters and the following symbols:</p> <p>! # \$ % &amp; ' ( ) * + , - . / : ; &lt; = &gt; ? @ [ \ ] ^ _ ` {   } ~</p> <p>Spaces are not allowed.</p>
Timeout	<p>Enter a value as the time before the timeout for connection to the Syslog Server is detected. The default is 10.</p> <p>Use this field only when you selected New Syslog Protocol (TLS1.2/RFC5424) in Transfer Protocol.</p>
Retry Interval	Enter a value between 1 and 60 (seconds) as the retry interval when communication with the Syslog Server fails. The default is 1. Use this field only when you selected New Syslog Protocol (TLS1.2/RFC5424) in Transfer Protocol.

Item	Description
Number of Retries	Enter a value between 1 and 50 as the number of retries when communication with the Syslog Server fails. The default is 3. Use this field only when you selected New Syslog Protocol (TLS1.2/RFC5424) in Transfer Protocol.
Send Test Message to Syslog Server	Reports SIM for test with Syslog.
Reset settings	Cancels the changes within the tab

**SNMP tab (when the SNMP protocol version is SNMP v1 or SNMP v2c)**

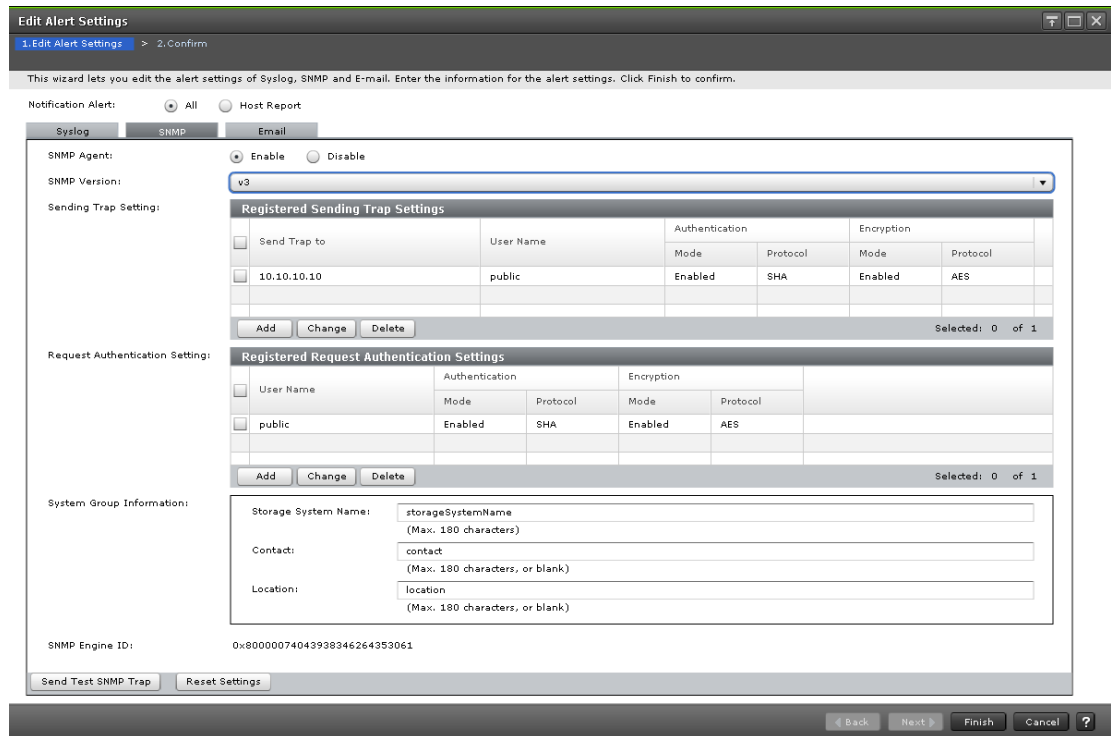


The following table describes the fields and settings in the SNMP tab when the SNMP protocol version is v1 or v2c.

Item	Description
SNMP Agent	<p>Select whether to use the SNMP agent.</p> <ul style="list-style-type: none"> <li>▪ Enable: Reports SIM through SNMP trap that permits GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST*</li> <li>▪ Disable: Does not report SIM through SNMP or permit GET REQUEST, GETNEXT REQUEST, or GETBULK REQUEST*</li> </ul>
SNMP Version	Select the SNMP protocol version.
Sending Trap Setting	<p>Displays, in the Registered Sending Trap Settings table, the user names and IP addresses for which SNMP trap information is reported.</p> <ul style="list-style-type: none"> <li>▪ Community: Displays the community for which SNMP trap information is reported.</li> <li>▪ Send Trap to: Displays the IP address to which SNMP trap information is reported</li> <li>▪ Add: Opens the <b>Add Sending Trap Setting</b> window. You can register up to 32 communities.</li> <li>▪ Change: To change a community, select it, and then click this button to open the <b>Change Sending Trap Setting</b> window.</li> <li>▪ Delete: To delete a community, select it, and then click this button.</li> </ul>
Request Authentication Setting	<p>Displays, in the Registered Request Authentication Settings table, the community names and IP addresses that permit GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST*.</p> <ul style="list-style-type: none"> <li>▪ Community: Displays the community names that permit GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST*</li> <li>▪ Requests Permitted: Displays the IP addresses that permit GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST*</li> <li>▪ Add: The Add Request Authentication Setting window opens. You can register up to 32 communities.</li> <li>▪ Change: To change a community, select it, and then click this button.</li> <li>▪ Delete: To delete a community, select it, and then click this button</li> </ul>
System Group Information - Storage System Name	<p>Enter the storage system name. You can enter up to 180 alphanumeric characters and symbols, except for the following:</p> <p>\, / ; : * ? " &lt; &gt;   &amp; % ^</p> <p><b>Note:</b> Do not include space characters at the beginning or end.</p> <p><b>Caution:</b> Make sure to document the information about the storage system because the settings will be cleared when the SVP is replaced.</p>
System Group Information - Contact	Enter the administrator's name or contact information. You can enter up to 180 alphanumeric characters and symbols, except for the following:

Item	Description
	\, / ; : * ? " < >   & % ^ <b>Note:</b> Do not include space characters at the beginning or end.
System Group Information - Location	Specify a location of the storage system. You can enter up to 180 alphanumeric characters and symbols, except for the following: \, / ; : * ? " < >   & % ^ <b>Note:</b> Do not include space characters at the beginning or end.
SNMP Engine ID	Displays the SNMP engine identifier.
Send Test SNMP Trap	Reports test trap to IP addresses that are already registered in the storage system. <b>Note:</b> Trap is reported using the content applied previously to the storage system rather than the current settings in the SNMP tab. Before reporting test trap, click Finish to apply the changes to the storage system.
Reset settings	Cancels the changes within the tab.
* Only SNMP v2c supports GETBULK REQUEST.	

### SNMP tab (when the SNMP protocol version is SNMP v3)



The following table describes the fields and settings in the SNMP tab when the SNMP protocol version is v3.

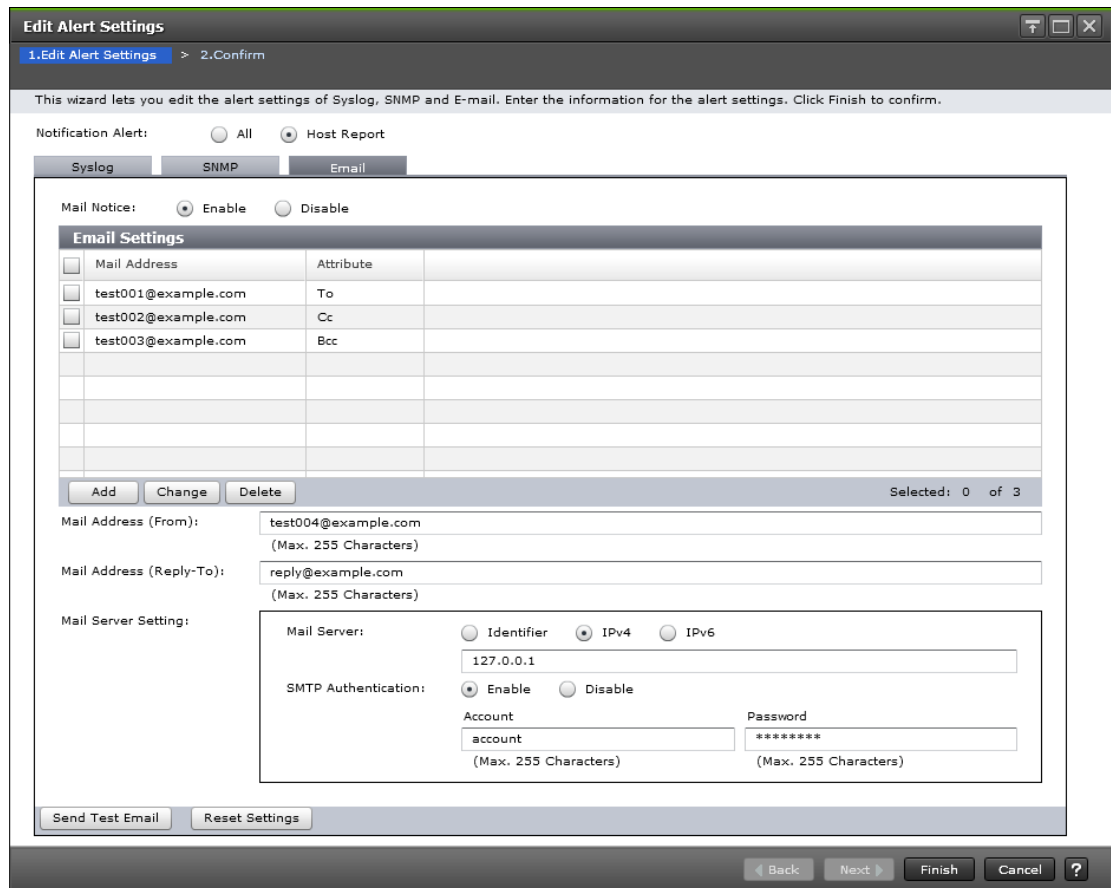


Item	Description
SNMP Agent	Select whether to use the SNMP agent. <ul style="list-style-type: none"> <li>▪ Enable: Reports SIM through SNMP trap that permits GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST</li> <li>▪ Disable: Does not report SIM through SNMP or permit GET REQUEST, GETNEXT REQUEST, or GETBULK REQUEST</li> </ul>
SNMP Version	Select the SNMP protocol version.
Sending Trap Setting	Displays, in the Registered Sending Trap Settings table, the community names and IP addresses for which SNMP trap information is reported. <ul style="list-style-type: none"> <li>▪ Send Trap to: Displays the IP address to which SNMP trap information is reported</li> <li>▪ User Name: Displays the user used for reporting SNMP trap information</li> <li>▪ Authentication - Mode: Displays whether authentication is enabled</li> <li>▪ Authentication - Protocol: If authentication is enabled, the authentication method is displayed</li> <li>▪ Encryption - Mode: Displays whether encryption is enabled</li> <li>▪ Encryption - Protocol: If encryption is enabled, the encryption method is displayed</li> <li>▪ Add: Opens the <b>Add Sending Trap Setting</b> window. You can register up to eight IP addresses.</li> <li>▪ Change: To change a destination, select it, and then click this button to open the <b>Change Sending Trap Setting</b> window.</li> <li>▪ Delete: To delete a destination, select it, and then click this button.</li> </ul>

Item	Description
Request Authentication Setting	<p>Displays the user name that permit GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST, in the Registered Request Authentication Settings table.</p> <ul style="list-style-type: none"> <li>▪ User Name: Displays the user names that permit GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST</li> <li>▪ Authentication - Mode: Displays whether authentication is enabled</li> <li>▪ Authentication - Protocol: If authentication is enabled, the authentication method is displayed</li> <li>▪ Encryption - Mode: Displays whether encryption is enabled</li> <li>▪ Encryption - Protocol: If encryption is enabled, the encryption method is displayed</li> <li>▪ Add: Opens the <b>Add Request Authentication Setting</b> window. You can register up to 8 users.</li> <li>▪ Change: To change a user, select it, and then click this button to open the <b>Change Request Authentication Setting</b> window.</li> <li>▪ Delete: To delete a user, select it, and then click this button.</li> </ul>
System Group Information - Storage System Name	<p>Enter the storage system name. You can enter up to 180 alphanumeric characters and symbols, except for the following:  \, / ; : * ? " &lt; &gt;   &amp; % ^</p> <p><b>Note:</b> Do not include space characters at the beginning or end.</p> <p><b>Caution:</b> Make sure to document the information about the storage system because the settings will be cleared when the SVP is replaced.</p>
System Group Information - Contact	<p>Enter the administrator's name or contact information. You can enter up to 180 alphanumeric characters and symbols, except for the following:  \, / ; : * ? " &lt; &gt;   &amp; % ^</p> <p><b>Note:</b> Do not include space characters at the beginning or end.</p>
System Group Information - Location	<p>Specify a location of the storage system. You can enter up to 180 alphanumeric characters and symbols, except for the following:  \, / ; : * ? " &lt; &gt;   &amp; % ^</p> <p><b>Note:</b> Do not include space characters at the beginning or end.</p>
SNMP Engine ID	Displays the SNMP engine identifier.
Send Test SNMP Trap	Reports test trap to IP addresses that are already registered in the storage system.

Item	Description
	<b>Note:</b> Trap is reported using the content applied previously to the storage system rather than the current settings in the SNMP tab. Before reporting test trap, click Finish to apply the changes to the storage system.
Reset settings	Cancels the changes within the tab.

### Email tab



Item	Description
Mail Notice	Select whether or not to report failure information through email. <ul style="list-style-type: none"> <li>Enable: Reports SIM through email.</li> <li>Disable: Does not report SIM through email.</li> </ul>
Email Settings	This field is mandatory when you selected Enable in Mail Notice. <ul style="list-style-type: none"> <li>Mail Address: The email address displays.</li> <li>Attribute: Adds email addresses. The <b>Add Address</b> window opens.</li> </ul>

Item	Description
	<ul style="list-style-type: none"> <li>▪ Add: Adds email addresses. The <b>Add Address</b> window opens</li> <li>▪ Change: Changes the selected email address and attribute. The opens.</li> </ul> <p>You can select more than one email address. When you select more than one email address, you can change only attributes.</p> <ul style="list-style-type: none"> <li>▪ Delete: Deletes the selected email address. You can select more than one email address.</li> </ul>
Mail Address (From)	<p>Enter the source address of the email for failure information report.</p> <p>You can enter up to 255 alphanumeric characters and the following symbols:</p> <p>! # \$ % &amp; ` + - * / ' ^ { } _ .</p> <p>This field is mandatory when you selected Enable in Mail Notice.</p>
Mail Address (Reply - To)	<p>Specify the return email address. If you specify this address, return email from the email recipient is transmitted to the address. If you omit this address, return email from the email recipient is transmitted to Mail Address (From).</p> <p>You can enter up to 255 alphanumeric characters and the following symbols:</p> <p>! # \$ % &amp; ` + - * / ' ^ { } _ .</p>
Mail Server Setting - Email Server	<p>Enter the Email server information. You cannot set an IP address with all 0s.</p> <ul style="list-style-type: none"> <li>▪ Identifier: To specify a host name, select Identifier. You can enter a name of up to 63 characters.</li> <li>▪ IPv4: Enter a valid IPv4 address in the format XXX.XXX.XXX.XXX (where XXX is a number from 0 to 255)</li> <li>▪ IPv6: Enter a valid IPv6 address in the format YYY:YYY:YYY:YYY:YYY:YYY:YYY:YYY: (where YYY is a hexadecimal number from 0 to FFFF). You can also use an IPv6 address in abbreviated format.</li> </ul> <p>This field is mandatory when you select Enable in Mail Notice.</p>
Mail Server Setting - SMTP Authentication	<p>Select whether or not to perform SMTP authentication.</p> <ul style="list-style-type: none"> <li>▪ Enable: Performs SMTP authentication.</li> <li>▪ Disable: Does not perform SMTP authentication.</li> </ul> <p>When you select Enable, enter values in Account and Password.</p> <p>You can enter up to 255 alphanumeric characters and the following symbols:</p> <p>! # \$ % &amp; ` + - * / ' ^ { } _ .</p>

Item	Description
	This field is mandatory when you select Enable in Mail Notice.
Send Test Email	Sends SIM for testing through email.
Reset settings	Cancels the changes within the tab

## Add Sending Trap Setting window (SNMP v1 or v2c)

Use the Add Sending Trap Setting window to set up an alert notification when using SNMP v1 or SNMP v2c.

This window appears when you click Add on the SNMP tab of the **Set Up Alert Notifications** window if the SNMP protocol version is SNMP v1 or SNMP v2c.

Item	Description
Community	Specify the community to which SNMP traps are reported.

Item	Description
	<p>You can select an existing community from the pull down menu or create a new community. You can enter up to 180 alphanumeric characters excluding the following symbols:</p> <p>\ , / ; : * ? " &lt; &gt;   &amp; % ^ ' </p> <p><b>Note:</b> Do not include space characters at the beginning or end.</p>
Send Trap to	<p>Specify the IP address to which SNMP traps are reported.</p> <p>Select an existing IP address from the pull down menu or enter a new address.</p> <ul style="list-style-type: none"> <li>▪ IPv4: Enter a valid IPv4 address in the format <i>XXX.XXX.XXX.XXX</i> (where <i>XXX</i> is a number from 0 to 255)</li> <li>▪ IPv6: Enter a valid IPv6 address in the format <i>YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY</i>: (where <i>YYYY</i> is a hexadecimal number from 0 to FFFF). You can also use an IPv6 address in abbreviated format.</li> <li>▪ Minus symbol: Removes the IP address in that row.</li> <li>▪ Add IP Address: Adds an IP address. You can add up to 32 IP addresses.</li> </ul>

## Add Sending Trap Setting window (SNMP v3)

Use the Add Sending Trap Setting window to set up an alert notification when using SNMP v3.

This window appears when you click Add on the SNMP tab of the **Set Up Alert Notifications** window if the SNMP protocol version is SNMP v3.

Item	Description
Send Trap to	Specify the IP address to which SNMP traps are reported. <ul style="list-style-type: none"> <li>IPv4: Enter a valid IPv4 address in the format <i>XXX.XXX.XXX.XXX</i> (where <i>XXX</i> is a number from 0 to 255)</li> <li>IPv6: Enter a valid IPv6 address in the format <i>YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY</i> (where <i>YYYY</i> is a hexadecimal number from 0 to FFFF). You can also use an IPv6 address in abbreviated format.</li> </ul>
User Name	Enter the user name to be used for reporting SNMP traps. You can enter up to 32 alphanumeric characters, excluding the following symbols: <code>\ , / ; : * ? " &lt; &gt;   &amp; % ^</code> <b>Note:</b> Do not include space characters at the beginning or end.
Authentication	Select whether to perform authentication. <ul style="list-style-type: none"> <li>Enable: Authentication is performed.</li> <li>Disable: Authentication is not performed.</li> </ul>

Item	Description
	Authentication and encryption information is displayed only if authentication is enabled.
Authentication - Protocol	If authentication is enabled, select the authentication method. <ul style="list-style-type: none"> <li>▪ SHA</li> <li>▪ MD5</li> </ul>
Authentication - Password	If authentication is enabled, enter a password. The password must be 8 to 180 alphanumeric characters, including the following symbols: \ , / ; : * ? " < >   & % ^ <b>Note:</b> Do not include space characters at the beginning or end.
Encryption	Select whether to perform encryption. <ul style="list-style-type: none"> <li>▪ Enable: Encryption is performed.</li> <li>▪ Disable: Encryption is not performed.</li> </ul> Encryption information is displayed only if encryption is enabled.
Encryption - Protocol	If encryption is enabled, select the encryption method. <ul style="list-style-type: none"> <li>▪ AES</li> <li>▪ DES</li> </ul>
Encryption - Key	If encryption is enabled, enter a key. The key must be 8 to 180 alphanumeric characters, including the following symbols: \ , / ; : * ? " < >   & % ^ <b>Note:</b> Do not include space characters at the beginning or end.
Encryption - Re-enter Key	Re-enter the same key.

## Change Sending Trap Setting window (SNMP v1 or v2c)

Use the Change Sending Trap Setting window to set up an alert notification when using SNMP v1 or SNMP v2c.

This window appears when you click Change on the SNMP tab of the **Set Up Alert Notifications** window if the SNMP protocol version is SNMP v1 or SNMP v2c.



Item	Description
Community	<p>Specify the community to which SNMP traps are reported.</p> <p>You can select an existing community from the pull down menu or create a new community. You can enter up to 180 alphanumeric characters excluding the following symbols:</p> <p>\, / ; : * ? " &lt; &gt;   &amp; % ^</p> <p><b>Note:</b> Do not include space characters at the beginning or end.</p>
Send Trap to	<p>Specify the IP address to which SNMP traps are reported.</p> <p>Select an existing IP address from the pull down menu or enter a new address.</p> <ul style="list-style-type: none"> <li>▪ IPv4: Enter a valid IPv4 address in the format XXX.XXX.XXX.XXX (where XXX is a number from 0 to 255)</li> <li>▪ IPv6: Enter a valid IPv6 address in the format YYY:YYY:YYY:YYY:YYY:YYY:YYY:YYY: (where YYY is a hexadecimal number from 0 to FFFF). You can also use an IPv6 address in abbreviated format.</li> <li>▪ Minus symbol: Removes the IP address in that row.</li> <li>▪ Add IP Address: Adds an IP address. You can add up to 32 IP addresses.</li> </ul>

## Change Sending Trap Setting window (SNMP v3)

Use the Change Sending Trap Setting window to set up an alert notification when using SNMP v3.

This window appears when you click Change on the SNMP tab of the **Set Up Alert Notifications** window if the SNMP protocol version is SNMP v3.

Item	Description
Send Trap to	Specify the IP address to which SNMP traps are reported. <ul style="list-style-type: none"> <li>IPv4: Enter a valid IPv4 address in the format <i>XXX.XXX.XXX.XXX</i> (where <i>XXX</i> is a number from 0 to 255)</li> <li>IPv6: Enter a valid IPv6 address in the format <i>YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY</i> (where <i>YYYY</i> is a hexadecimal number from 0 to FFFF). You can also use an IPv6 address in abbreviated format.</li> </ul>
User Name	Enter the user name to be used for reporting SNMP traps. You can enter up to 32 alphanumeric characters, excluding the following symbols: \\, /, ;, : * ? " < >   & % ^

Item	Description
	<b>Note:</b> Do not include space characters at the beginning or end.
Authentication	Select whether to perform the authentication. <ul style="list-style-type: none"> <li>▪ Enable: Authentication is performed.</li> <li>▪ Disable: Authentication is not performed.</li> </ul> Authentication and encryption information is displayed only if authentication is enabled.
Authentication - Protocol	If authentication is enabled, select the authentication method. <ul style="list-style-type: none"> <li>▪ SHA</li> <li>▪ MD5</li> </ul>
Authentication - Password	If authentication is enabled, enter a password. The password must be 8 to 180 alphanumeric characters, including the following symbols: \ , / ; : * ? " < >   & % ^ <b>Note:</b> Do not include space characters at the beginning or end.
Encryption	Select whether to perform the encryption <ul style="list-style-type: none"> <li>▪ Enable: Encryption is performed.</li> <li>▪ Disable: Encryption is not performed.</li> </ul> Encryption information is displayed only if encryption is enabled.
Encryption - Protocol	If encryption is enabled, select the encryption method. <ul style="list-style-type: none"> <li>▪ AES</li> <li>▪ DES</li> </ul>
Encryption - Key	If encryption is enabled, enter a key. The key must be at least 8 alphanumeric characters, including the following symbols: \ , / ; : * ? " < >   & % ^ <b>Note:</b> Do not include space characters at the beginning or end.
Encryption - Re-enter Key	Re-enter the same key.

## Add Request Authentication Setting window (SNMP v1 or v2c)

Use the Add Request Authentication Setting window to set up an alert notification when using SNMP v1 or SNMP v2c.

This window appears when you click Add on the SNMP tab of the Set Up Alert Notifications window if the SNMP protocol version is SNMP v1 or SNMP v2c.

Item	Description
Community	<p>Select an existing community, or create one, permitted to execute GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST*.</p> <p>You can enter up to 180 alphanumeric characters excluding the following symbols:                      \, / ; : * ? " &lt; &gt;   &amp; % ^ '                 </p> <p><b>Note:</b> Do not include space characters at the beginning or end.</p>

Item	Description
Requests permitted	<p>Specify which users have permission to execute GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST*.</p> <ul style="list-style-type: none"> <li>▪ All: Accepts GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST from all users. If All is selected, the IP address information is not displayed.</li> <li>▪ Specific IP addresses: <ul style="list-style-type: none"> <li>• Select an existing IP address from the pull down menu or enter a new address.</li> <li>• IPv4: Enter a valid IPv4 address in the format <i>XXX.XXX.XXX.XXX</i> (where <i>XXX</i> is a number from 0 to 255)</li> <li>• IPv6: Enter a valid IPv6 address in the format <i>YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY</i>: (where <i>YYYY</i> is a hexadecimal number from 0 to FFFF). You can also use an IPv6 address in abbreviated format.</li> <li>• Minus symbol: Removes the IP address in that row.</li> <li>• Add IP Address: Adds an IP address. You can add up to 32 IP addresses.</li> </ul> </li> </ul>
* Only SNMP v2c supports GETBULK REQUEST.	

## Add Request Authentication Setting window (SNMP v3)

Use the Add Request Authentication Setting window to set up an alert notification when using SNMP v3.

The Add Request Authentication Setting window appears when you click Add on the SNMP tab of the **Set Up Alert Notifications** window if the SNMP protocol version is SNMP v3.

Item	Description
User Name	<p>Enter the name of the user permitted to execute GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST.</p> <p>You can enter up to 32 alphanumeric characters, excluding the following symbols:</p> <p>\, / ; : * ? " &lt; &gt;   &amp; % ^</p> <p><b>Note:</b> Do not include space characters at the beginning or end.</p>
Authentication	<p>Select whether to perform the authentication.</p> <ul style="list-style-type: none"> <li>Enable: Authentication is performed.</li> <li>Disable: Authentication is not performed.</li> </ul> <p>Authentication information is displayed only if authentication is enabled.</p>
Authentication - Protocol	<p>If authentication is enabled, select the authentication method.</p> <ul style="list-style-type: none"> <li>SHA</li> <li>MD5</li> </ul>

Item	Description
Authentication - Password	<p>If authentication is enabled, enter a password. The password must be 8 to 180 alphanumeric characters excluding the following symbols:            \, / ; : * ? " &lt; &gt;   &amp; % ^</p> <p><b>Note:</b> Do not include space characters at the beginning or end.</p>
Authentication - Re-enter Password	Re-enter the same password.
Encryption	<p>Select whether to perform the encryption</p> <ul style="list-style-type: none"> <li>▪ Enable: Encryption is performed.</li> <li>▪ Disable: Encryption is not performed.</li> </ul> <p>Encryption information is displayed only if encryption is enabled.</p>
Encryption - Protocol	<p>If encryption is enabled, select the encryption method</p> <ul style="list-style-type: none"> <li>▪ AES</li> <li>▪ DES</li> </ul>
Encryption - Key	<p>If encryption is enabled, enter a key. The key must be 8 to 180 alphanumeric characters excluding the following symbols:            \, / ; : * ? " &lt; &gt;   &amp; % ^</p> <p><b>Note:</b> Do not include space characters at the beginning or end.</p>
Encryption - Re-enter Key	Re-enter the same key.

## Change Request Authentication Setting window (SNMP v1 or v2c)

Use the Change Request Authentication Setting window to set up an alert notification when using SNMP v1 or SNMP v2c.

This window appears when you click Change on the SNMP tab of the **Set Up Alert Notifications** window if the SNMP protocol version is SNMP v1 or SNMP v2c.

Item	Description
Community	<p>Select an existing community, or create one, permitted to execute GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST*.</p> <p>You can enter up to 180 alphanumeric characters excluding the following symbols:</p> <p>\, / ; : * ? " &lt; &gt;   &amp; % ^ ' </p> <p><b>Note:</b> Do not include space characters at the beginning or end.</p>



Item	Description
Requests Permitted	<p>Specify which users have permission to execute GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST*.</p> <ul style="list-style-type: none"> <li>▪ All: Accepts GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST from all users. If All is selected, the IP address information is not displayed.</li> <li>▪ Specific IP addresses: <ul style="list-style-type: none"> <li>• Select an existing IP address from the pull down menu or enter a new address.</li> <li>• IPv4: Enter a valid IPv4 address in the format <i>XXX.XXX.XXX.XXX</i> (where <i>XXX</i> is a number from 0 to 255)</li> <li>• IPv6: Enter a valid IPv6 address in the format <i>YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY</i> (where <i>YYYY</i> is a hexadecimal number from 0 to FFFF). You can also use an IPv6 address in abbreviated format.</li> <li>• Minus symbol: Removes the IP address in that row.</li> <li>• Add IP Address: Adds an IP address. You can add up to 32 IP addresses.</li> </ul> </li> </ul>
* Only SNMP v2c supports GETBULK REQUEST.	

## Change Request Authentication Setting window (SNMP v3)

Use the Change Request Authentication Setting window to set up an alert notification when using SNMP v3.

This window appears when you click Change on the SNMP tab of the **Set Up Alert Notifications** window if the SNMP protocol version is SNMP v3.

**Change Request Authentication Setting**

Check the box in front of the property you want to edit, and then enter the new value. Click OK.

User Name:   
(Max. 32 Characters)

Authentication:  Enable  Disable

Protocol:

Password:   
(8-180 characters)

Re-enter Password:

Encryption:  Enable  Disable

Protocol:

Key:   
(8-180 characters)

Re-enter Key:

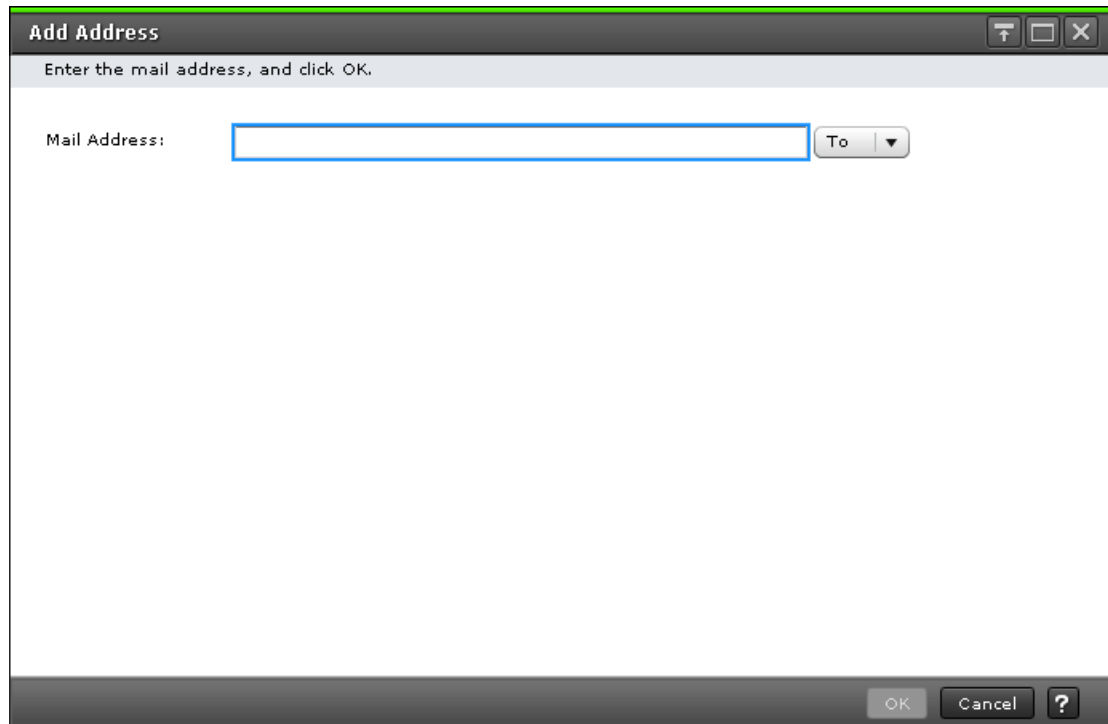
OK Cancel ?

Item	Description
User Name	<p>Enter the name of the user permitted to execute GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST.</p> <p>You can enter up to 32 alphanumeric characters, excluding the following symbols:</p> <p>\, / ; : * ? " &lt; &gt;   &amp; % ^</p> <p><b>Note:</b> Do not include space characters at the beginning or end.</p>
Authentication	<p>Select whether to perform authentication.</p> <ul style="list-style-type: none"> <li>Enable: Authentication is performed.</li> <li>Disable: Authentication is not performed.</li> </ul> <p>Authentication and encryption information is displayed only if authentication is enabled.</p>
Authentication - Protocol	<p>If authentication is enabled, select the authentication method.</p> <ul style="list-style-type: none"> <li>SHA</li> <li>MD5</li> </ul>

Item	Description
Authentication - Password	<p>If authentication is enabled, enter a password. The password must be 8 to 180 alphanumeric characters excluding the following symbols:            \ , / ; : * ? " &lt; &gt;   &amp; % ^</p> <p><b>Note:</b> Do not include space characters at the beginning or end.</p>
Authentication - Re-enter Password	Re-enter the same password.
Encryption	<p>Select whether to perform encryption.</p> <ul style="list-style-type: none"> <li>▪ Enable: Encryption is performed.</li> <li>▪ Disable: Encryption is not performed.</li> </ul> <p>Encryption information is displayed only if encryption is enabled.</p>
Encryption - Protocol	<p>If encryption is enabled, select the encryption method.</p> <ul style="list-style-type: none"> <li>▪ AES</li> <li>▪ DES</li> </ul>
Encryption - Key	<p>If encryption is enabled, enter a key. The key must be 8 to 180 alphanumeric characters excluding the following symbols:            \ , / ; : * ? " &lt; &gt;   &amp; % ^</p> <p><b>Note:</b> Do not include space characters at the beginning or end.</p>
Encryption - Re-enter Key	Re-enter the same key.

## Add Address window

Use the add address window to add an email address to the list of addresses to notify of a system error.

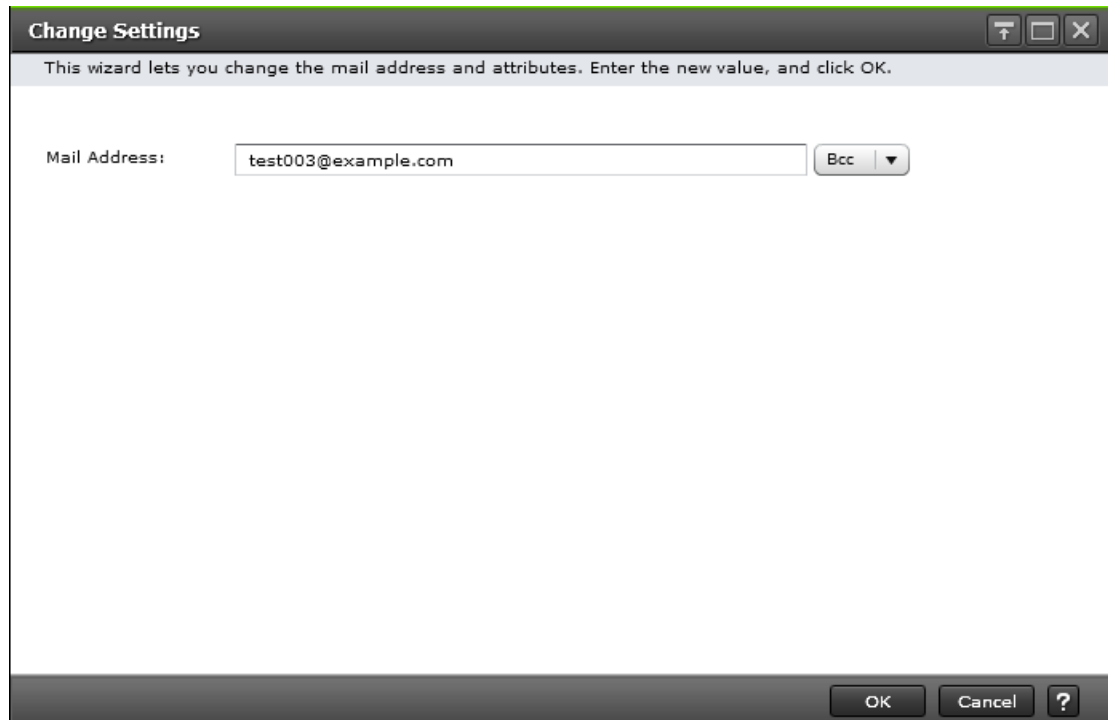


The following table describes the fields and settings in the **Add Address** window.

Item	Description
Mail Address	Enter an email address and select an attribute (To, Cc, or Bcc). Email addresses can contain up to 255 alphanumeric characters, including the following symbols: ! # \$ % & ` + - * / ' ^ { } _ .

## Change Settings window

Use the change settings window to change an email address.



The following table describes the fields and settings in the **Change Settings** window.

Item	Description
Mail Address	<p>Enter an email address after change and select an attribute. You can select more than one email address. When you select more than one email address, you can change only attributes.</p> <p>Email addresses can contain up to 255 alphanumeric characters, including the following symbols: ! # \$ % &amp; ` + - * / ' ^ { } _ .</p>

## Edit Alert Settings confirmation window



**Note:** Only the tables related to the items you edited are displayed in the confirmation window.

The following tables describe the fields and settings in the Edit Alert Settings confirmation window

Item	Description
Notification Alert	Displays the destination of the alert notification.

This table describes the Syslog Server settings.

Item	Description
Primary Server - Syslog Server	Displays whether or not to use the Syslog Server
Primary Server - IP Address	Displays the IP address of the Syslog Server
Primary Server - Port Number	Displays the port number used by the Syslog Server
Primary Server - Client Certificate File Name	Displays the client certificate file name

Item	Description
Primary Server - Password	Displays the client certificate password as asterisks
Primary Server - Root Certificate File Name	Displays the root certificate file name
Secondary Server - Syslog Server	Displays whether or not to use an alternate server for the Syslog Server
Secondary Server - IP Address	Displays the IP address of the alternate server for the Syslog Server
Secondary Server - Port Number	Displays the port number used by the alternate server for the Syslog Server
Secondary Server - Client Certificate File Name	Displays the file name of the client certificate
Secondary Server - Password	Displays the password of the client certificate as asterisks
Secondary Server - Root Certificate File Name	Displays the file name of the root certificate
Location Identification Name	Displays the name for identifying the storage system that transfers SIM to the Syslog Server
Timeout	Displays the time before the timeout for connection to the Syslog Server is detected
Retry Interval	Displays the retry interval when communication with the Syslog Server fails
Number of Retries	Displays the number of retries when communication with the Syslog Server fails

This table describes the SNMP Information settings.

Item	Description
SNMP Agent	Displays whether or not to use the SNMP Agent.
System Group Information - Storage System Name	Displays the storage system name
System Group Information - Contact	Displays the administrator's name or contact information

Item	Description
System Group Information - Location	Displays the storage system location
SNMP Version	Displays the SNMP protocol version.

The following tables describes the Registered Sending Trap Settings for the different SNMP protocol versions.

(when the SNMP protocol version is SNMP v1 or SNMP v2c)

Item	Description
Community	Displays the name of the community for which the SNMP trap information is reported.
Send Trap to	Displays the IP address to which SNMP trap information is reported.

(when the SNMP protocol version is SNMP v3)

Item	Description
Send Trap to	Displays the IP address to which SNMP trap information is reported.
User Name	Displays the user name to which SNMP trap information is reported.
Authentication - Mode	Displays whether the authentication is enabled or not.
Authentication - Protocol	Displays the authentication method if the authentication is enabled.
Authentication - Password	Displays the authentication password as asterisks.
Encryption - Mode	Displays whether the encryption is enabled.
Encryption - Protocol	Displays the encryption method if the encryption is enabled.
Encryption - Key	Displays the encryption key as asterisks.

The following tables describes the Registered Request Authentication Setting for the different SNMP protocol versions.

(when the SNMP protocol version is SNMP v1 or SNMP v2c)



Item	Description
Community	Displays the name of community to which GET REQUEST, GETNEXT REQUEST, or GETBULK REQUEST is accepted.
Requests Permitted	Displays the IP address to which GET REQUEST, GETNEXT REQUEST, or GETBULK REQUEST is accepted.

(when the SNMP protocol version is SNMP v3)

Item	Description
User Name	Displays the user name that accepts GET REQUEST, GETNEXT REQUEST, or GETBULK REQUEST.
Authentication - Mode	Displays whether the authentication is enabled or not.
Authentication - Protocol	Displays the authentication method if the authentication is enabled.
Authentication - Password	Displays the authentication password as asterisks.
Encryption - Mode	Displays whether the encryption is enabled.
Encryption - Protocol	Displays the encryption method if the encryption is enabled.
Encryption - Key	Displays the encryption key as asterisks.

The following table describes the Email Notification settings. (when the SNMP protocol version is SNMP v3)

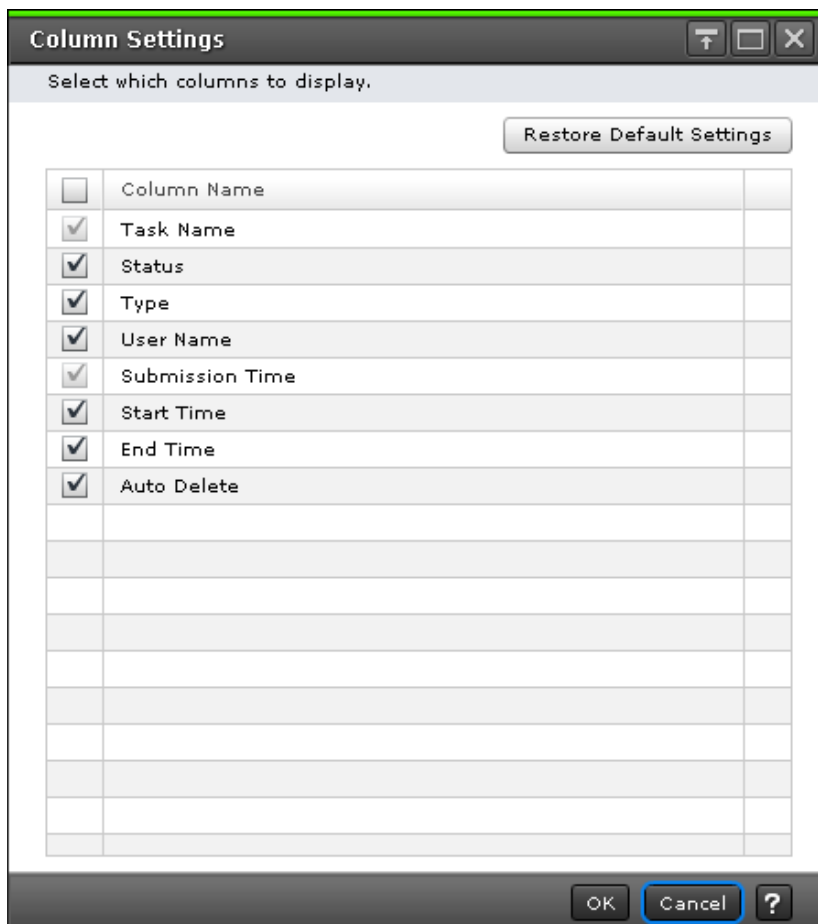
Item	Description
Mail Notice	Displays whether or not to use email to notify users of failure information
Mail Address (From)	Displays the source email address for notification of failure information.
Mail Address (Reply - To)	Displays the email return address
Server Host Name	Displays the email server host name or IP address
SMTP Authentication	Displays whether or not to perform SMTP authentication.
SMTP Authentication - Account	Displays the account used for SMTP authentication.

Item	Description
SMTP Authentication - Password	Displays the SMTP authentication password as asterisks

The following table describes the Email settings. (when the SNMP protocol version is SNMP v3)

Item	Description
Mail Address	Displays the email address after the change
Attribute	Displays the attribute of email for SIM notification

## Column Settings window



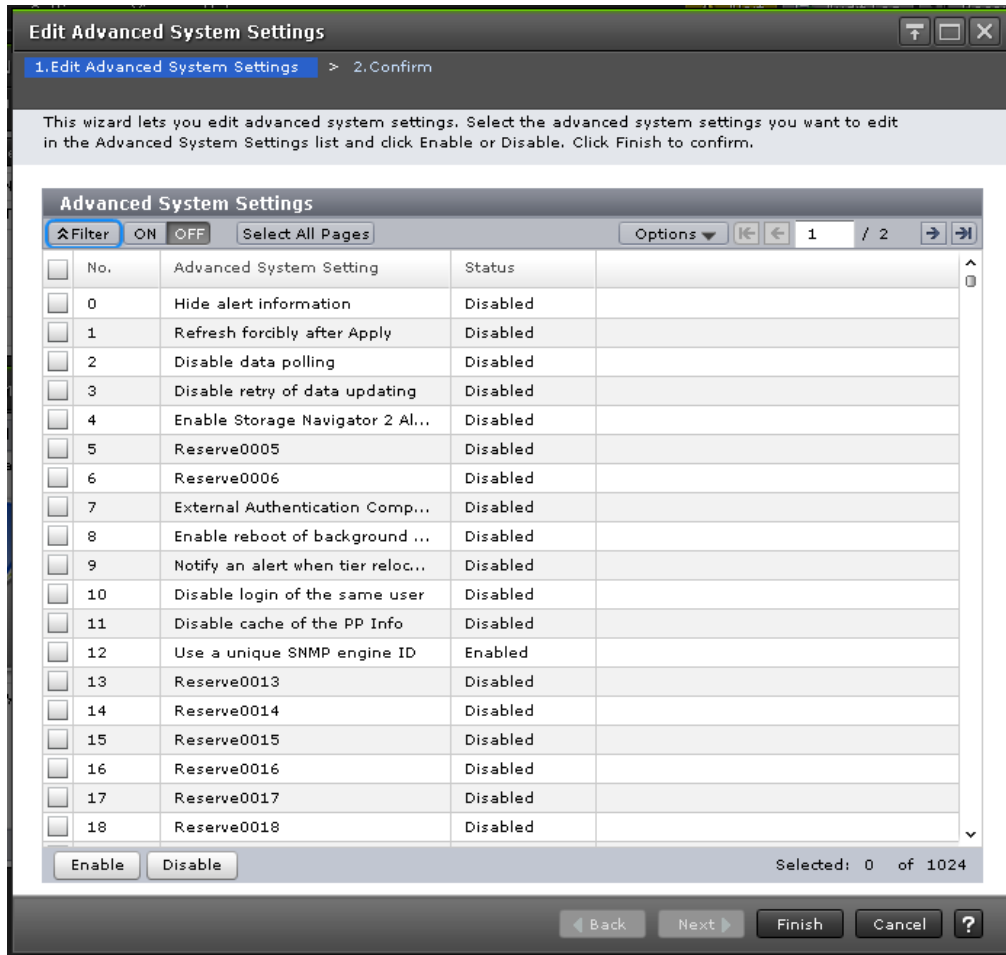
Item	Description
Restore Default Settings	Changes the selection of the displayed columns to the factory default settings.
Checkbox	<p>Selects the columns to display.</p> <p>Click the checkbox next to the name of each column that you want to display. After making the selections, click OK. Only the columns whose checkboxes are selected are displayed. Columns whose checkboxes are not selected are not displayed.</p> <p>Note that you cannot select the checkboxes of the columns that must always be displayed because they are deactivated.</p> <p>When you deselect a checkbox, the filter and sort settings of that column are released. If you display the column again, you must set the filter and sort settings again.</p>
Column Name	Displays the names of the columns in the table. If a column contains two rows, the name of the upper row is shown on the left of the vertical bar ( ). The name of the lower row is shown on the right of the vertical bar.

## Edit Advanced System Settings wizard

Edit Advanced System Settings wizard contains the following topics:

- [Edit Advanced System Settings window \(on page 364\)](#)
- [Edit Advanced System Settings confirmation window \(on page 366\)](#)
- [Column Settings window \(on page 362\)](#)

## Edit Advanced System Settings window



The following table describes the advanced system settings fields and settings in the **Edit Advanced System Settings** window.

Item	Description
No.	Displays the number of function bits for the advanced system settings.
Advanced System Setting	Displays advanced system setting names. <ul style="list-style-type: none"> <li>▪ Hide alert information: The <b>Alert</b> window is not displayed.</li> <li>▪ Refresh forcibly after Apply: The configuration information for the storage system is forcibly updated after the configuration changes are applied to the storage system.</li> <li>▪ Disable data polling: Polling stops.</li> <li>▪ Disable retry of data updating: Retry does not take place even when you fail to acquire data.</li> </ul>

Item	Description
	<ul style="list-style-type: none"> <li>▪ External Authentication Compatibility option. If you enable this option, the authentication method is switched from VSP G1x00 and VSP F1500 to VSP.</li> <li>▪ Enable reboot of background service: If you enable this option, when either of the followings exceeds its threshold value, the background service process for managing configuration information is restarted. Enable this option only when requested. <ul style="list-style-type: none"> <li>• The amount of memory used in the background service process</li> <li>• Time elapsed after the background service process is started</li> </ul> </li> <li>▪ Notify an alert when tier relocation is suspended by system: If you enable this option, when tier relocation is suspended by the system, an alert is issued to users. For details about an alert (SIM) to be issued, see the Troubleshooting chapter of the <i>Provisioning Guide for Open Systems</i> or <i>Provisioning Guide for Mainframe Systems</i>.</li> <li>▪ Disable login of the same user: Set this option only when requested.</li> <li>▪ Disable cache of the PP Info: Set this option only when requested.</li> <li>▪ Use a unique SNMP engine ID: If you enable this option, a unique SNMP engine ID is set. If you disable it, the fixed value is set. When changing the settings for this option, first set SNMP Agent to Disable, then after the completion of the settings, set it back to Enable.</li> </ul>
Status	Displays the statuses of the advanced system settings.
Enable	Enables the selected advanced system settings. You can select more than one advanced system setting.
Disable	Disables the selected advanced system settings. You can select more than one advanced system setting.

## Edit Advanced System Settings confirmation window

1.Edit Advanced System Settings > 2.Confirm

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

Task Name:  (Max. 32 Characters)

No.	Advanced System Setting	Status
0	Hide alert information	Disabled
1	Refresh forcibly after Apply	Disabled
2	Disable data polling	Disabled
3	Disable retry of data updating	Disabled
4	Enable Storage Navigator 2 Al...	Disabled
5	Reserve0005	Disabled
6	Reserve0006	Disabled
7	External Authentication Comp...	Disabled
8	Enable reboot of background ...	Disabled
9	Notify an alert when tier reloc...	Disabled
10	Disable login of the same user	Disabled
11	Disable cache of the PP Info	Disabled
12	Use a unique SNMP engine ID	Enabled
13	Reserve0013	Disabled
14	Reserve0014	Disabled
15	Reserve0015	Disabled
16	Reserve0016	Disabled
17	Reserve0017	Disabled
18	Reserve0018	Disabled

Total: 1024

Go to tasks window for status    Back    Next    Apply    Cancel    ?

Item	Description
No.	Displays the number of function bits for the advanced system setting.
Advanced System Setting	Displays the name of the advanced system setting.
Status	Displays the status of the advanced system setting.

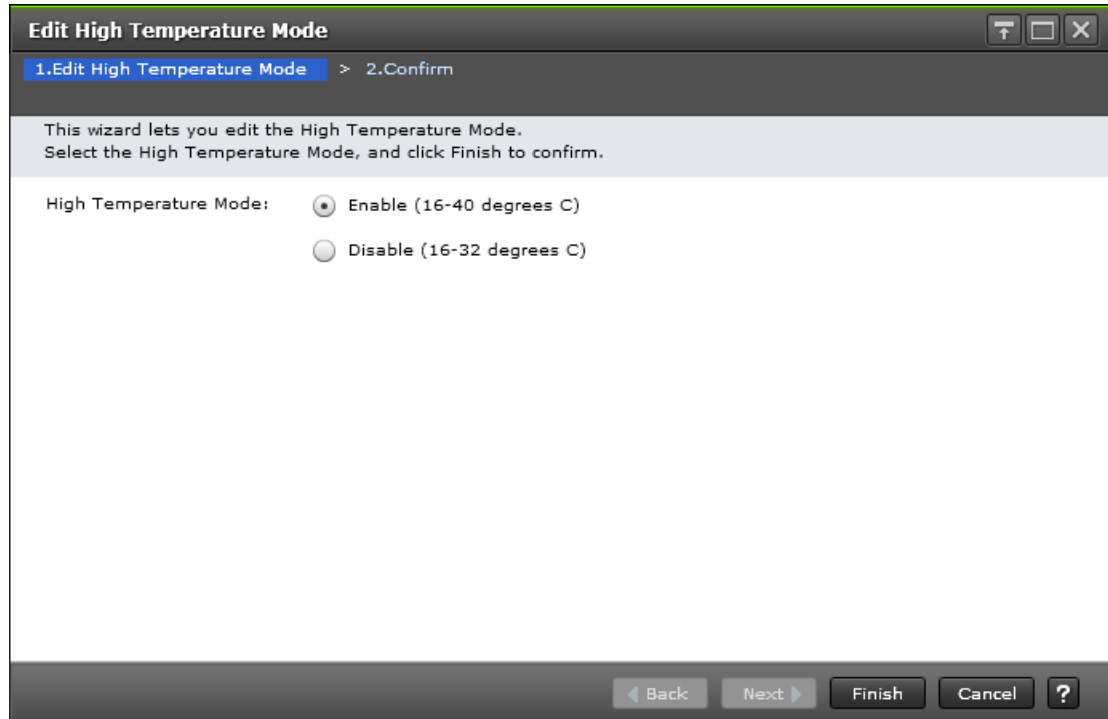
## Edit High Temperature Mode wizard

### Prerequisites

- You must install the software and activate the license to use the high temperature mode feature.

## Edit High Temperature Mode window

Use this window to set the allowable operating temperature of the storage system.



Item	Description
High Temperature Mode	<p>Enables the high temperature mode so that the storage system can run in a high temperature environment.</p> <ul style="list-style-type: none"> <li>▪ Enable (16-40 degrees C): Turns the high temperature mode on. The system can run in the temperature range of (60.8°F to 104°F / 16°C to 40°C). A SIM is displayed when the internal storage system temperature exceeds 40°C.</li> <li>▪ Disable (16-32 degrees C): Turns the high temperature mode off. The system can run in the temperature range of (60.8°F to 89.6°F / 16°C to 32°C). A SIM is displayed when the internal storage system temperature exceeds 32°C.</li> </ul>

## Edit High Temperature Mode confirmation window

Use this window to confirm the allowable storage system operating temperature settings made in the Edit High Temperature **Mode** window.

**Edit High Temperature Mode**

1.Edit High Temperature Mode > 2.Confirm

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

Task Name:   
(Max. 32 Characters)

Selected High Temperature Mode	
High Temperature Mode	
Enable (16-40 degrees C)	

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

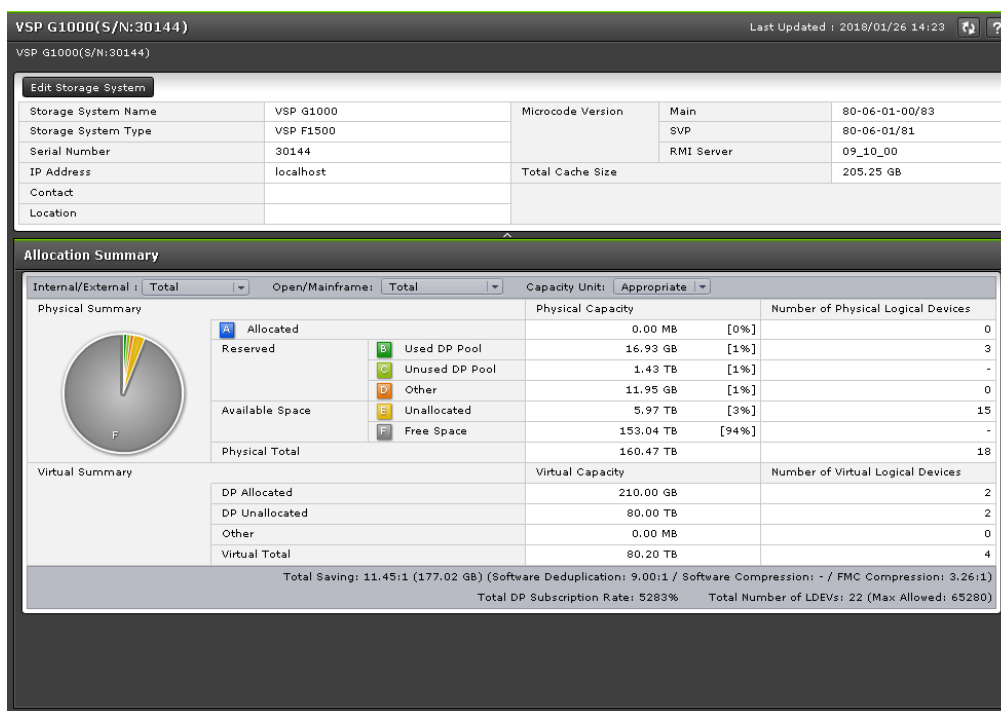


<b>Item</b>	<b>Description</b>
High Temperature Mode	Displays the high temperature mode settings. <ul style="list-style-type: none"><li data-bbox="750 310 1409 415">▪ Enable (16-40 degrees C): The system operates in high temperature mode (60.8°F to 104°F / 16°C to 40°C).</li><li data-bbox="750 430 1409 535">▪ Disable (16-32 degrees C): The system is operating in standard temperature mode (60.8°F to 89.6°F / 16°C to 32°C).</li></ul>

# Appendix D: Device Manager - Storage Navigator system GUI reference

This section explains the Device Manager - Storage Navigator windows used to view and manage storage system tasks, reports, and alerts.

## Storage Systems window



### Hardware summary

The following table describes the fields and settings in the hardware summary section of the **Storage Systems** window.

Item	Description
Edit Storage System	Allows editing of the storage system name, contact, and location.

Item	Description
Storage System Name	Device name of the storage system.
Contact	Contact information such as personnel and telephone number where you can inquire about the storage system.
Location	Location of the connected storage system.
Storage System Type	Model type of the storage system.
Serial Number	Serial number of the storage system.
IP Address	IP address of the SVP.
Microcode Version	This item displays the version of the microcode. <ul style="list-style-type: none"> <li>▪ Main: Version of the microcode installed in the connected storage system</li> <li>▪ SVP: Version of the Device Manager - Storage Navigator installed in the SVP</li> <li>▪ RMI Server: Version of the RMI server installed in the SVP</li> </ul>
Total Cache Size	Total size of the cache memory in the storage system. The capacity used as the shared memory is not included.

### Allocation summary

The following table describes the fields and settings in the allocation summary section of the **Storage Systems** window.

Item	Description
Internal / External	This item switches the displayed items. <ul style="list-style-type: none"> <li>▪ Total: Displays information on both the internal volumes and the external volumes.</li> <li>▪ Internal Only: Displays information on only the internal volumes.</li> <li>▪ External Only: Displays information on only the external volumes.</li> </ul>
Open/ Mainframe	This item switches the displayed capacity units. <ul style="list-style-type: none"> <li>▪ Total: Displays all the open-systems, mainframe-systems and multi-platform volumes</li> <li>▪ Open Only: Displays only open-systems volumes</li> <li>▪ Mainframe Only: Displays mainframe-systems and multi-platform volumes.</li> </ul>

Item	Description
Capacity Unit	<p>This item switches the displayed units of the capacity.</p> <ul style="list-style-type: none"> <li>▪ Appropriate: Displays the capacity in appropriate unit depending on the capacity of each item.</li> <li>▪ TB/GB/MB: Displays the capacity of the specified unit.</li> </ul>
Physical Summary	<p>This item displays the capacity of physical logical devices and the number of devices. It displays different information for open-systems and mainframe-systems. For details about this item, see the Physical Summary table.</p>
Virtual Summary	<p>This item displays capacity of virtual logical devices and the number of devices. It displays different information for open-systems and mainframe-systems. For details about this item, see the table below about virtual summary.</p>
Total Saving (Software Deduplication/ Software Compression/ FMC Compression)	<p>Total Saving: Displays the ratio and capacity reduced by the capacity saving function against all data in a storage system.</p> <p>Software Deduplication: Displays the ratio reduced by the deduplication function against all data in a storage system.</p> <p>Note that the following data is contained in the deduplicated capacity. Therefore, Software Deduplication might be lower than the actual value:</p> <ul style="list-style-type: none"> <li>▪ Data in a virtual volume whose capacity saving setting is Compression.</li> <li>▪ Data which is queued for deduplication processing (Not deduplicated yet).</li> </ul> <p>Software Compression: Displays the ratio reduced by the software compression function against all data in a storage system.</p> <p>FMC Compression: For the total data capacity in a storage system, displays the ratio of before and after the FMC compression function is executed.</p>
Total Number of LDEVs	<p>The number of LDEVs. The information displayed in this field depends on the type of system. See the following table.</p>

### Physical summary

The following table describes the fields and settings in the physical summary section of the **Storage Systems** window.

Item	Description
Allocated	<p>When Open is selected from Open / Mainframe, this item displays the capacity of path-defined open system volumes (LDEVs) and the number of logical devices that the host can recognize. This capacity does not include the control cylinder.</p> <p>When Mainframe is selected from Open / Mainframe, this item displays the capacity of path-defined mainframe and multiplatform volumes and the number of logical devices that the host can recognize. The Reserved - Used DP Pool, Reserved - Unused DP Pool, and Reserved - Other volumes are not included. This capacity does not include the control cylinder.</p>
Reserved - Used DP Pool	<p>When Total is selected in Internal / External, this item displays the total capacity of the pages that are actually used in pool of Dynamic Provisioning and the number of logical devices. The total capacity does not include the control cylinder.</p> <p>For a DP pool in which Thin Image pairs are created, the total page capacity includes the snapshot data capacity.</p> <p>When an item other than Total is selected in Internal / External, this item displays the number of logical devices that are actually used in the Dynamic Provisioning pool. The capacity does not display in this item, but is counted as part of Reserved - Other.</p>
Reserved - Unused DP Pool	<p>When the total is selected in Internal / External, this item displays the capacity remaining after subtracting the Used DP Pool value from the total capacity of pool of Dynamic Provisioning. Control cylinder is not included in the capacity. The number of logical devices does not display.</p> <p>When an item other than Total is selected in Internal / External, the capacity and the number of logical devices are not displayed in this item, and the capacity is counted as part of Reserved - Other.</p>
Reserved - Other	<p>When Open is selected from Open / Mainframe, this item displays the total capacity and the number of logical devices of the following volumes:</p> <ul style="list-style-type: none"> <li>▪ Thin Image pool volumes</li> <li>▪ Journal volumes</li> </ul> <p>The control cylinder is not included in the capacity.</p> <p>The total capacity includes:</p> <ul style="list-style-type: none"> <li>▪ The pool-VOL capacity that is not used as pool capacity</li> <li>▪ The capacity of the system pool-VOL management area (approx. 4.1 GB per pool)</li> </ul>

Item	Description
	<p>When Mainframe is selected from Open / Mainframe, this item displays the total capacity of journal volumes and the number of logical devices of the mainframe and multi-platform volumes.</p> <p>The control cylinder is not included in the capacity.</p> <p>The total capacity includes:</p> <ul style="list-style-type: none"> <li>▪ The pool-VOL capacity that is not used as pool capacity</li> <li>▪ The capacity of the system pool-VOL management area (approx. 3.7 GB per pool)</li> </ul> <p>For both open and mainframe, when an item other than Total is selected in Internal / External, the capacities for Reserved - Used DP Pool and Reserved - Unused DP Pool are also counted as part of this item.</p>
Available Space - Unallocated	<p>When Open or Total is selected from Open / Mainframe, this item displays the volume capacity and the number of logical devices from the open volumes that are not defined paths. The Reserved - Used DP Pool, Reserved - Unused DP Pool, and Reserved - Other volumes are not included. The control cylinder is also not included in the capacity.</p> <p>When Mainframe is selected from Open / Mainframe, the capacity and the number of logical devices do not display.</p>
Available Space - Free Space	<p>When Open is selected from Open / Mainframe, this item displays the free space in which users can create Open volumes.</p> <p>When Mainframe is selected from Open / Mainframe, this item displays the free space in which users can create Mainframe-systems and multi-platform volumes.</p> <p>In both Open and Mainframe, the control cylinder is not included in the capacity, and the number of logical devices does not display.</p>
Physical Total	<p>This item displays the total capacity of physical logical devices and the number of logical devices. Control cylinder is not included in the capacity.</p>

### Virtual summary

The following table describes the fields and settings in the virtual summary section of the **Storage Systems** window.

Item	Description
DP Allocated *	When total is selected in Internal / External, this item displays the capacity of path-defined virtual volumes of Dynamic Provisioning, and the number of logical devices. Virtual volumes for Thin Image are not included. Control cylinder is not included in the capacity.
DP Unallocated*	When total is selected in Internal / External, this item displays the capacity of virtual volumes of Dynamic Provisioning that are not path-defined, and the number of logical devices. Virtual volumes for Thin Image are not included. Control cylinder is not included in the capacity.
Other*	When total is selected in Internal / External, the item displays the virtual volumes of other than Dynamic Provisioning and the number of logical devices. Control cylinder is not included in the capacity.
Virtual Total	This item displays the total capacity of virtual logical devices and the number of logical devices. Control cylinder is not included in the capacity.
* When an item other than Total is selected in Internal / External, the capacity and the number of logical devices are not displayed.	

## Port Condition window

The screenshot shows the 'Port Condition' window for DKC0. It features a 'Refresh' button at the top right. Below the window title, there is a summary table for 'Number of Ports' and a grid of port status indicators.

Number of Ports	Condition	Count
<input checked="" type="checkbox"/>	Available (Connected)	14
<input type="checkbox"/>	Available (Not Connected)	13
<input type="checkbox"/>	Not Available	13
Not Installed		

The port status grid shows various ports (e.g., 1PB, 1PC, 1PE, 2PE, 2PC, 2PB) with their respective conditions (e.g., Available (Connected), Available (Not Connected), Not Available) and whether they are installed.

Below the grid is a detailed 'Port Condition' table with columns: Channel Adapter, Adapter Type, Port ID, Attribute, Condition, and Speed. The table lists 14 rows of port data.

Channel Adapter	Adapter Type	Port ID	Attribute	Condition	Speed
CHA-1PC	8FC16 (Fibre)	CL1-A	External	Not Available	Auto(-)
CHA-1PC	8FC16 (Fibre)	CL3-A	Initiator	<input type="checkbox"/> Available (Not Connected)	Auto(-)
CHA-1PC	8FC16 (Fibre)	CL1-B	Target	<input type="checkbox"/> Available (Not Connected)	Auto(-)
CHA-1PC	8FC16 (Fibre)	CL3-B	Target	<input checked="" type="checkbox"/> Available (Connected)	Auto(-)
CHA-1PE	16FC8 (Fibre)	CL1-E	Target	<input checked="" type="checkbox"/> Available (Connected)	Auto(-)
CHA-1PE	16FC8 (Fibre)	CL3-E	Initiator	Not Available	Auto(-)
CHA-1PE	16FC8 (Fibre)	CL5-E	Target	<input type="checkbox"/> Available (Not Connected)	Auto(-)
CHA-1PE	16FC8 (Fibre)	CL7-E	Target	<input checked="" type="checkbox"/> Available (Connected)	Auto(-)
CHA-1PE	16FC8 (Fibre)	CL1-F	Target	Not Available	Auto(-)
CHA-1PE	16FC8 (Fibre)	CL3-F	External	<input type="checkbox"/> Available (Not Connected)	Auto(-)
CHA-1PE	16FC8 (Fibre)	CL5-F	Target	<input checked="" type="checkbox"/> Available (Connected)	Auto(-)

The window also includes an 'Export' button and a 'Total: 40' indicator at the bottom right.

You can switch between information for DKC-0 and DKC-1 through a tab. When DKC-1 is not installed, the DKC-1 tab is not displayed.



### Note:

- Ports not allocated to the user are indicated with Not Available.
- Except for the Condition column, there may be a difference between the actual device configuration and the displayed information depending on the update timing of the storage system.

Refresh: Updates the window display to the latest status.

### Number of Ports



The following table describes the fields and settings in **Number of Ports**.



Item	Description
Available (Connected)	Number of ports in use
Available (Not Connected)	Number of ports that are installed but not in use
Not Available	Total number of ports that are installed but blocked
Not Installed	Ports not installed

### Port Condition

The following table describes the fields and settings in the **Port Condition** window.

Item	Description
Channel Adapter	Name of the channel adapter (channel adapter is also called a front-end director)
Adapter Type	Type of the channel adapter
Port ID	Port identifier
Attribute	Port attribute <ul style="list-style-type: none"> <li>▪ Channel adapter type is Fibre or FCoE: Initiator, Target, RCU Target, or External</li> <li>▪ Channel adapter type is Mfibre: HTP or FNP</li> <li>▪ When no port is assigned to the user, a hyphen (-) is displayed.</li> </ul>
Condition	Port Condition icon and port status <ul style="list-style-type: none"> <li>▪  Available (Connected): The port is installed and in use.</li> <li>▪  Available (Not Connected): The port is installed and available</li> <li>▪ Not Available: The port is either blocked or not assigned to the user.</li> </ul>
Speed	Data transfer speed of the port is displayed in gigabits per second as follows: <ul style="list-style-type: none"> <li>▪ 2 Gbps</li> <li>▪ 4 Gbps</li> <li>▪ 8 Gbps</li> <li>▪ 10 Gbps</li> </ul>

Item	Description
	<ul style="list-style-type: none"> <li>▪ 16 Gbps</li> <li>▪ 32 Gbps</li> </ul> <p>If Auto is set for Port Speed in the <b>Edit Ports</b> window, this item is displayed as follows:</p> <ul style="list-style-type: none"> <li>▪ Auto (2 Gbps)</li> <li>▪ Auto (4 Gbps)</li> <li>▪ Auto (8 Gbps)</li> <li>▪ Auto (10 Gbps)</li> <li>▪ Auto (16 Gbps)</li> <li>▪ Auto (32 Gbps)</li> </ul> <p>The values in the parentheses are set by the storage system. If linkup is not made, a hyphen (-) displays.</p> <p>Port speed is fixed at 10 Gbps for Fibre Channel over Ethernet (FCoE).</p> <p>For details of the <b>Edit Ports</b> window, see the <i>Provisioning Guide for Open Systems</i>.</p> <p>For information about the availability of the 32 Gbps SFPs, contact customer support.</p>
WWN/iSCSI Name	WWN/iSCSI name of the port
Export	Displays a window for outputting table information

## Tasks window

Tasks window screenshot showing a summary table and a detailed task list.






Task Name	Status	Type	User Name	Submission Time	Start Time	End Time	Auto Delete
130131-Cre...	Completed	Create Res...	mainten...	2013/01/31 11:19:55	2013/01/31 11:19:56	2013/01/31 11:20:11	Enabled
130130-Cre...	Failed	Create LDEVs	mainten...	2013/01/30 15:34:16	2013/01/30 15:34:22	2013/01/30 15:34:48	Disabled
130129-Res...	Failed	Restore LDE...	mainten...	2013/01/29 20:35:39	2013/01/29 20:35:39	2013/01/29 20:35:52	Disabled
130129-Cre...	Completed	Create User	mainten...	2013/01/29 12:01:11	2013/01/29 12:01:12	2013/01/29 12:01:18	Enabled
130129-Cre...	Completed	Create User...	mainten...	2013/01/29 12:00:29	2013/01/29 12:00:29	2013/01/29 12:00:31	Enabled

This window displays a list of tasks performed on the storage system. Up to 384 tasks can display, including 256 that are Completed and/or Failed. Up to 128 tasks whose statuses are In Progress, Waiting, and Suspended can also display.

### Summary

Item	Description
Completed	Number of completed tasks.
In Progress	Number of tasks in progress.
Waiting	Number of tasks waiting.
Suspended	Number of suspended tasks.
Failed	Number of tasks in which an error occurred.

### Tasks tab

Item	Description
Task Name	Task name specified by a user when the user performed the task. Click to view the detail of the task.
Status	<p>Task status. Click to view more details about status or errors.</p> <ul style="list-style-type: none"> <li>▪  Completed or Completed(Request): The task completed normally.</li> <li>▪  In progress: The task is being processed by the system.</li> <li>▪  Waiting: The task is not yet started.</li> <li>▪  Suspended: The task has been suspended.</li> <li>▪  Failed: The task ended abnormally.</li> </ul>
Type	General name of the task.
User Name	User name who performed the task.
Submission Time	Date and time when the task was submitted.
Start Time	Date and time when the task was started. Blank indicates the task has not started yet.
End time	Date and time when the task completed. Blank indicates the task has not completed yet.

Item	Description
Auto Delete	<p>Enabled: A task is automatically deleted when the following two events occur:</p> <ul style="list-style-type: none"> <li>▪ The task is completed</li> <li>▪ The number of tasks in the Task list reaches the maximum number the window can display (384)</li> </ul> <p>Disabled: Tasks will remain displayed until users delete them. Tasks whose status is Failed are automatically Disabled by the system.</p>
Suspend Tasks button	Suspends the selected tasks. They will not be started even if the storage system is ready. Only waiting tasks can be suspended.
Resume Tasks button	Resume the selected tasks. The status goes back to waiting.
Delete Tasks button	<p>Deletes the selected tasks from the window.</p> <ul style="list-style-type: none"> <li>▪ The waiting or suspended tasks will be cancelled.</li> <li>▪ The failed or aborted tasks can be deleted from the window.</li> <li>▪ Tasks in progress cannot be deleted.</li> <li>▪ If the maximum number of tasks displayed on the window is reached when Auto Delete is enabled, execution of a new task will result in automatic deletion of a task starting with the oldest one.</li> </ul>
Disable Auto Delete *	When disabled, the selected task remains in the task list after the task is completed.
Enable Auto Delete *	<p>When enabled, the selected task is deleted from the Task list when the following two events occur:</p> <ul style="list-style-type: none"> <li>▪ The task is completed</li> <li>▪ The number of tasks in the Task list reaches the maximum number the window can display (384)</li> </ul>
Export *	Displays a window that shows the information in the table
* Appears when you click More Actions.	

## Task Properties window

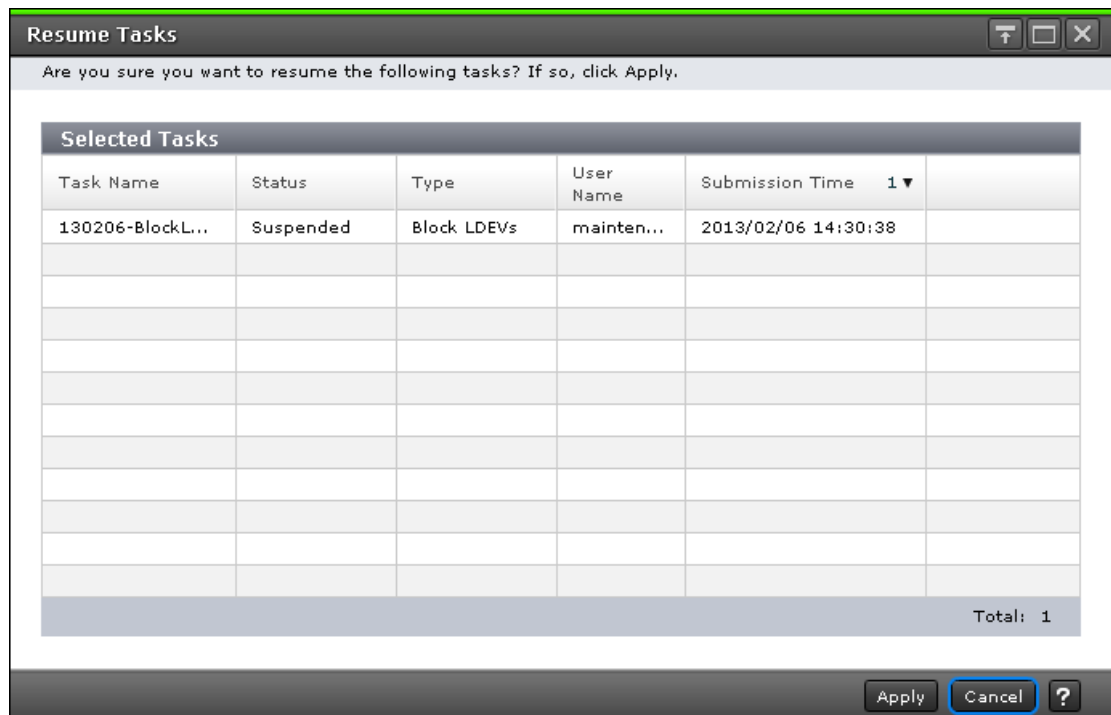
This window displays details about a task performed on the storage system. The content of the window depends on the task you executed.



Item	Description
Task Name	Task name specified by a user when the user performed the task.
Status	Task status.
Type	General name of the task.
User Name	User name who performed the task.
Submission Time	Date and time when the task was submitted.

## Resume Tasks window

Use this window to resume suspended tasks.

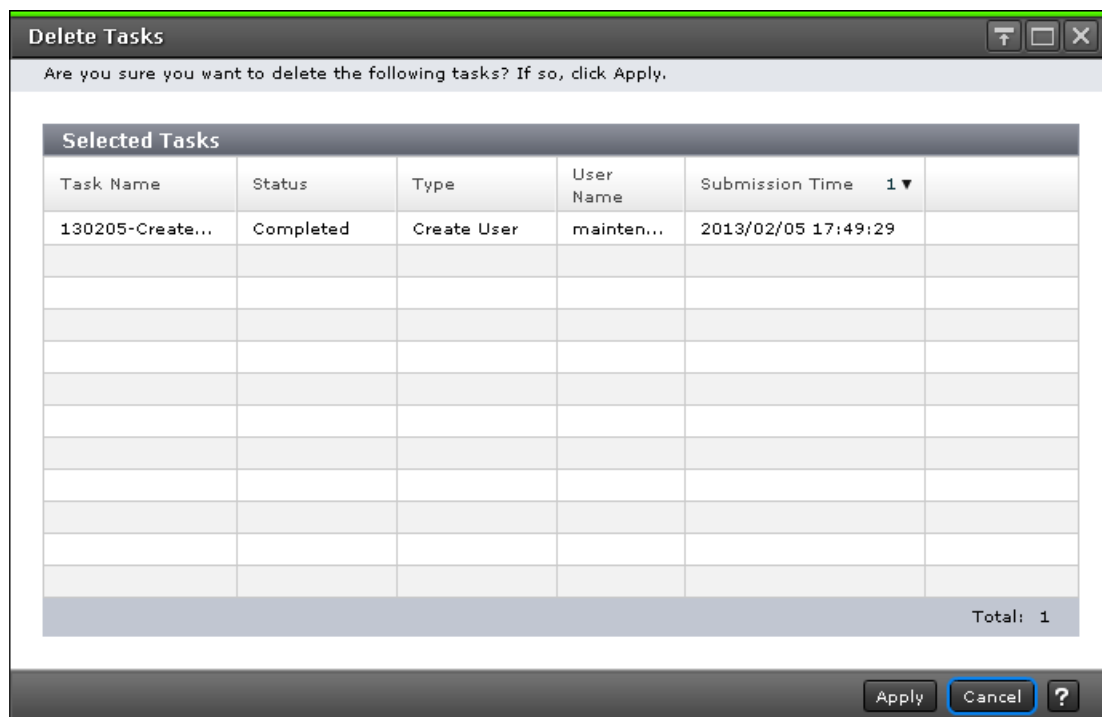


Item	Description
Task Name	Task name specified by a user when the user performed the task.
Status	Task status.
Type	General name of the task.

Item	Description
User Name	User name who performed the task.
Submission Time	Date and time when the task was submitted.

## Delete Tasks window

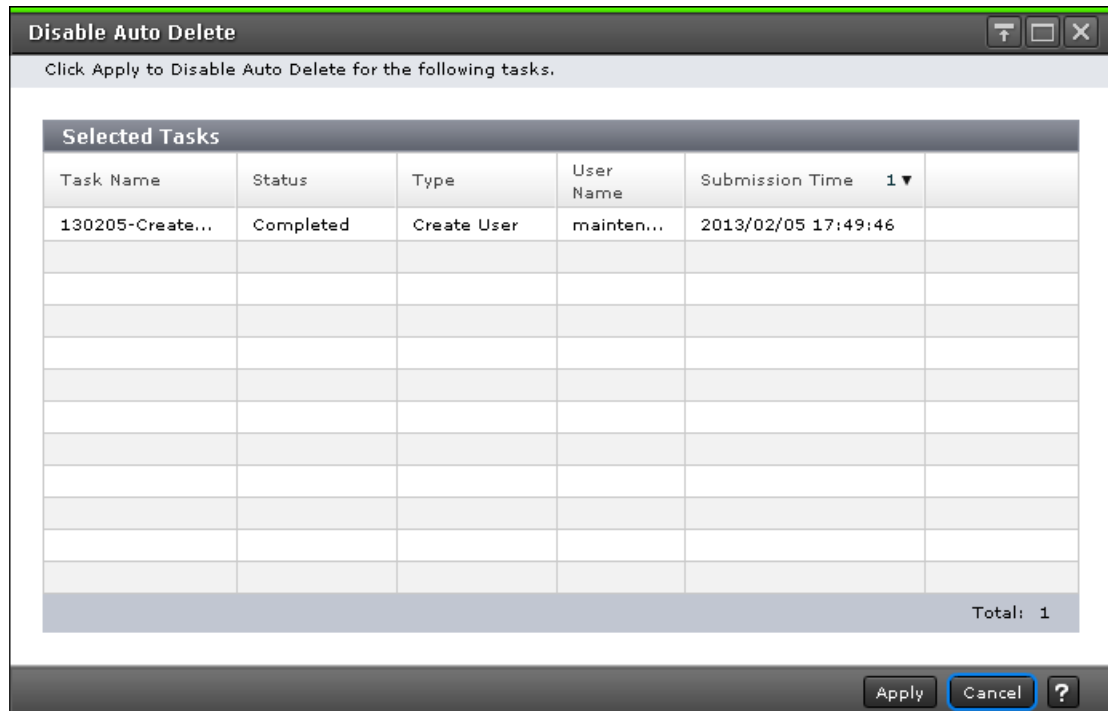
Use this window to delete tasks. If you delete a waiting task, the task will be cancelled.



Item	Description
Task Name	Task name specified by a user when the user performed the task.
Status	Task status.
Type	General name of the task.
User Name	User name who performed the task.
Submission Time	Date and time when the task was submitted.

## Disable Auto Delete window

Use this window to prevent a task from being automatically deleted from the task window.

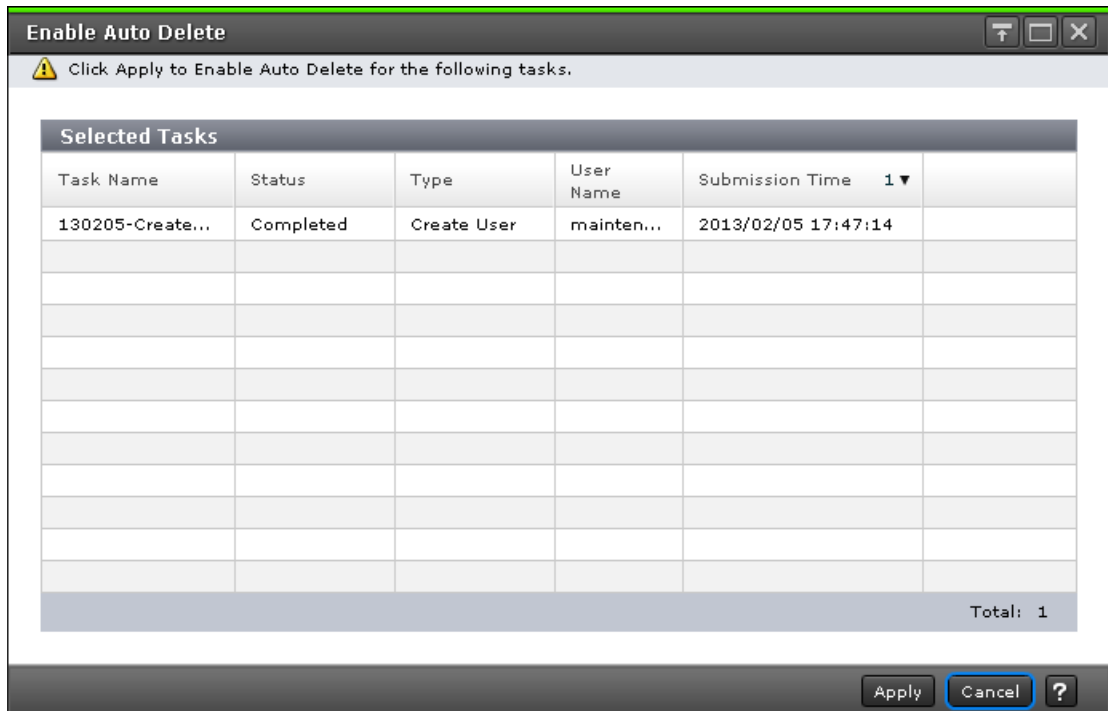


Item	Description
Task Name	Task name specified by a user when the user performed the task.
Status	Task status.
Type	General name of the task.
User Name	User name of the person who performed the task.
Submission Time	Date and time when the task was submitted.

## Enable Auto Delete window

Use this window to automatically delete completed tasks from the task window when the number of displayed tasks reaches the maximum (384 tasks).

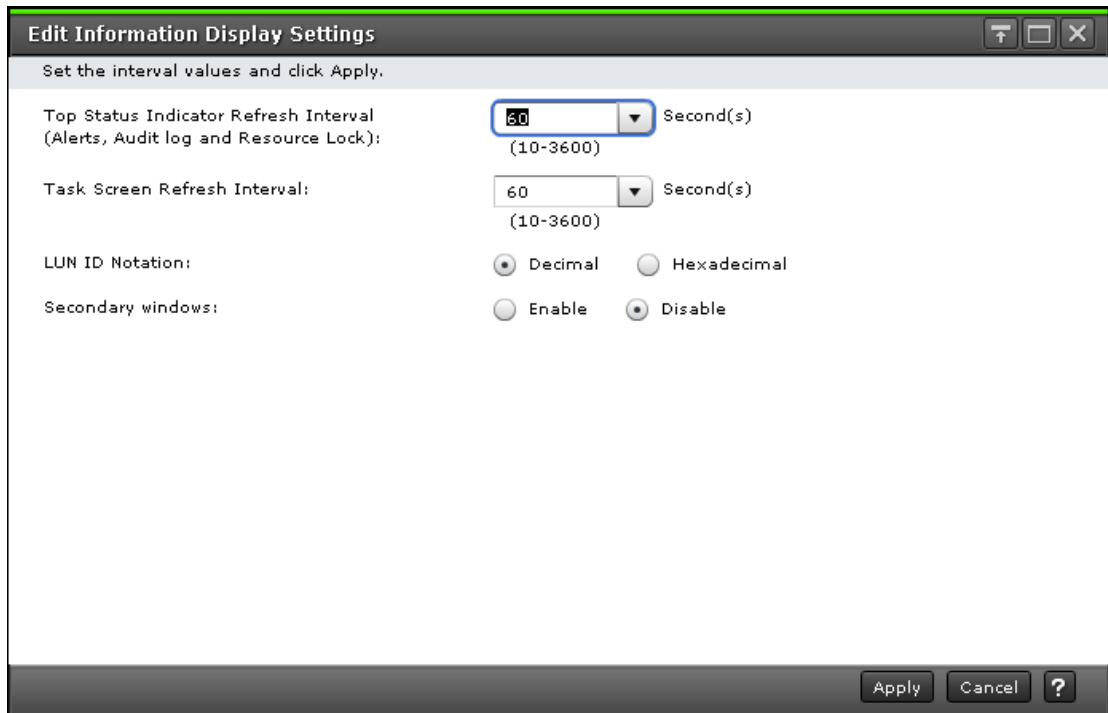




Item	Description
Task Name	Task name specified by a user when the user performed the task.
Status	Task status.
Type	General name of the task.
User Name	User name of the person who performed the task.
Submission Time	Date and time when the task was submitted.

## Edit Information Display Settings window

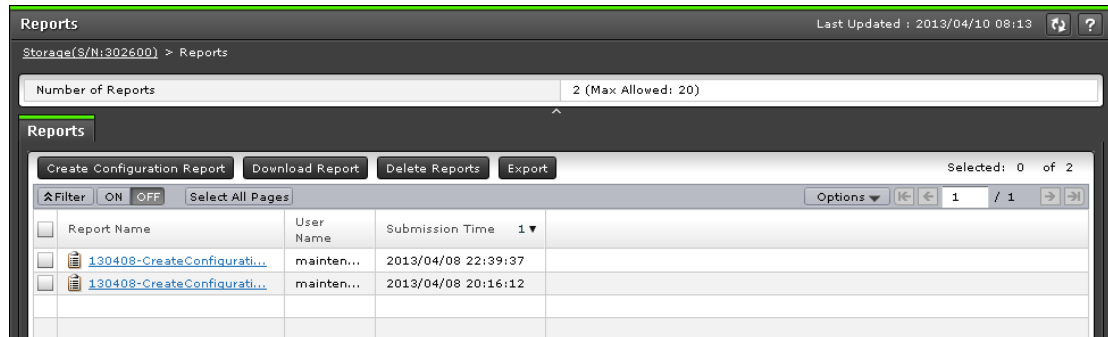
Use this window to change the display parameters.



Item	Description
Top Status Indicator Refresh Interval (Alerts, Audit log, and Resource Lock)	Interval for the automatic updates of the icons on the upper-right corner of the Device Manager - Storage Navigator main window. You can specify 10-3600 seconds. The default value is 60 seconds.
Task Screen Refresh Interval	Interval for the automatic updates of the task window. You can specify 10-3600 seconds, or No Update. The default value is 60 seconds. No Update indicates that the task window will be updated only when a user clicks Refresh or File > Refresh All.
LUN ID Notation	Select whether to display the LUN ID in decimal or hexadecimal notation. The default is decimal. Regardless of the setting, LUN IDs are displayed in decimal format on Device Manager - Storage Navigator's secondary window.
Secondary windows	Specify whether to enable or disable Device Manager - Storage Navigator's secondary window. Enable: Enables Device Manager - Storage Navigator's secondary window. Disable: Disables Device Manager - Storage Navigator's secondary window.

## Reports window

This window lists configuration reports about the storage system.



You can create up to 20 reports.

### Summary

Item	Description
Number of Reports	Number of created reports.

### Reports tab

Item	Description
Report Name	Task name specified when users created a report. Click to view the report in HTML format.
User Name	User name of the person who created the report.
Submission Time	Date and time when the report was created.
Create Configuration Report	Creates a new report.
Download Reports	Downloads the created report in both HTML and CSV format.
Delete Reports	Deletes the selected report.
Export	Displays a window that shows the information in the table Window for outputting table information.

## Create Configuration Report window

Use this window to create storage system configuration reports.











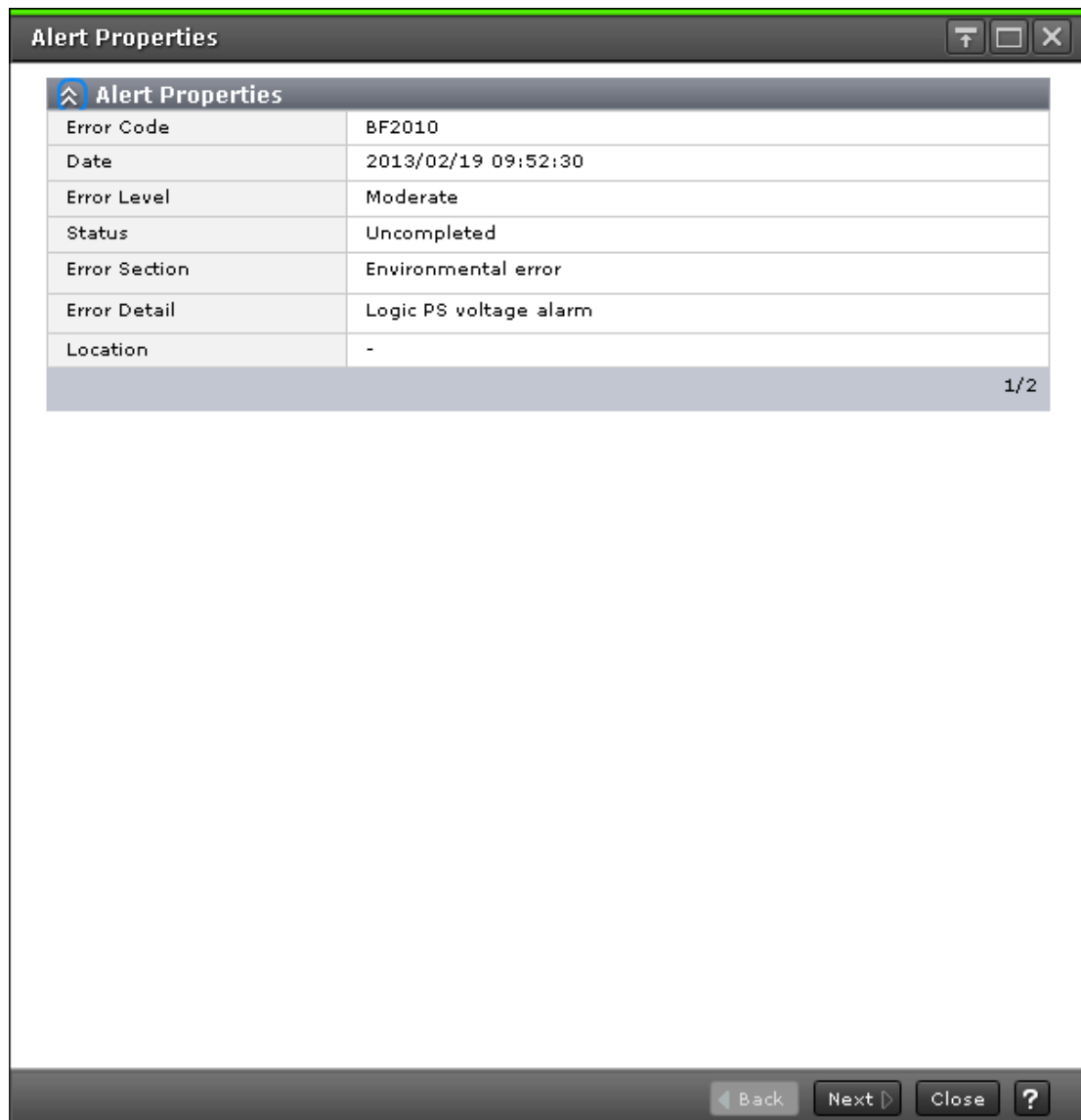
Item	Description
	<ul style="list-style-type: none"> <li>▪ Service: Displays total number of Service level alerts that are not authenticated yet.</li> <li>▪ Total: Total number of above is displayed.</li> </ul>

## Alerts

Item	Description
Error Code	<p>Displays reference code of SIM. For details about reference code, contact the customer support.</p> <p>For information about errors that need to be solved, see <a href="#">Monitoring SIMs alerts in Device Manager - Storage Navigator (on page 226)</a>.</p>
Date	Displays the date when alerts occurred.
Error Level	<p>Displays error level of alerts.</p> <ul style="list-style-type: none"> <li>▪  Service: No need to deal with immediately. Errors that are dealt with within periodical maintenance.</li> <li>▪  Moderate: No need to deal with immediately. Errors that are dealt with within periodical maintenance.</li> <li>▪  Serious: Contact the customer support. Take adequate measure as instructed, report and solve the problem.</li> <li>▪  Acute: Contact the customer support. Take adequate measure as instructed, report and solve the problem.</li> </ul>
Status	If status alert remains, Uncompleted displays. If alert is removed by SVP, Completed displays.
Detail	Displays the details of alert that is selected in the list.

## Alert Properties window





This window shows details of an alert (SIM) that has occurred in the storage system.



When you select multiple alerts in the **Alert** window, click Back and Next to change alert that is displayed.

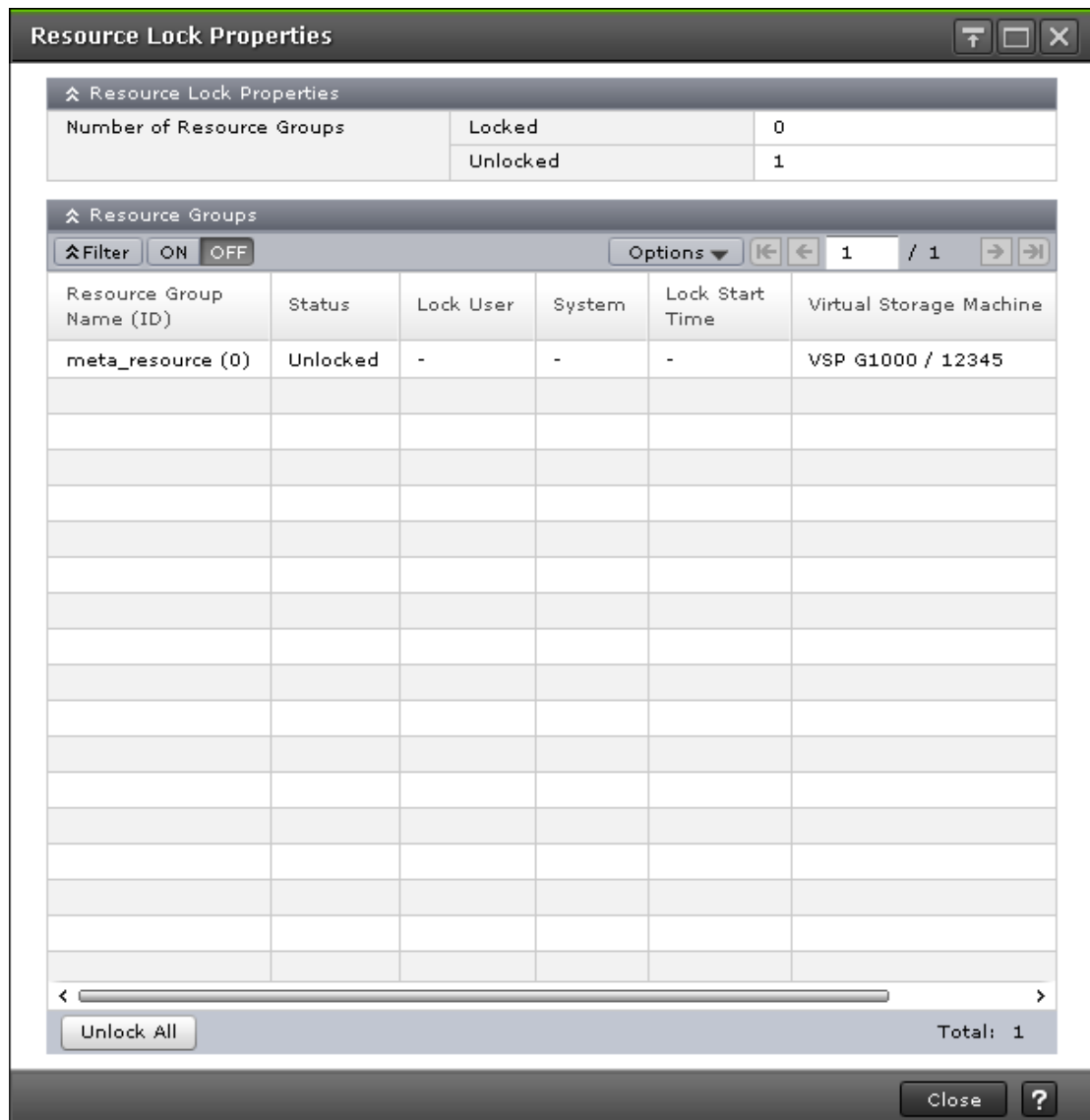
Item	Description
Error Code	Displays reference codes of SIM. For details about reference codes, contact the customer support. For information about errors that need to be solved, see <a href="#">Monitoring SIMs alerts in Device Manager - Storage Navigator (on page 226)</a> .
Date	Displays the date when alerts occurred.



Item	Description
Error Level	Displays error level of alerts. <ul style="list-style-type: none"> <li data-bbox="618 317 1416 394">▪  Service: No need to deal with immediately. These errors are dealt with during periodical maintenance.</li> <li data-bbox="618 415 1416 493">▪  Moderate: No need to deal with immediately. These errors are dealt with during periodical maintenance.</li> <li data-bbox="618 514 1416 592">▪  Serious: Contact the customer support. Take adequate measures as instructed, report and solve the problem.</li> <li data-bbox="618 613 1416 690">▪  Acute: Contact the customer support. Take adequate measures as instructed, report and solve the problem.</li> </ul>
Status	If status alert remains, Uncompleted displays. If alert is removed by SVP, Completed displays.
Error Section	Displays overview of the error where the alert occurred.
Error Detail	Displays more detail on the error.
Location	Displays where the error occurred. It differs according to the error code.

## Resource Lock Properties window

This window displays information about the user who locks the storage system.



### Resource Lock Properties

Item	Description
Number of Resource Groups - Locked	Displays the number of locked resource groups.
Number of Resource Groups - Unlocked	Displays the number of unlocked resource groups.

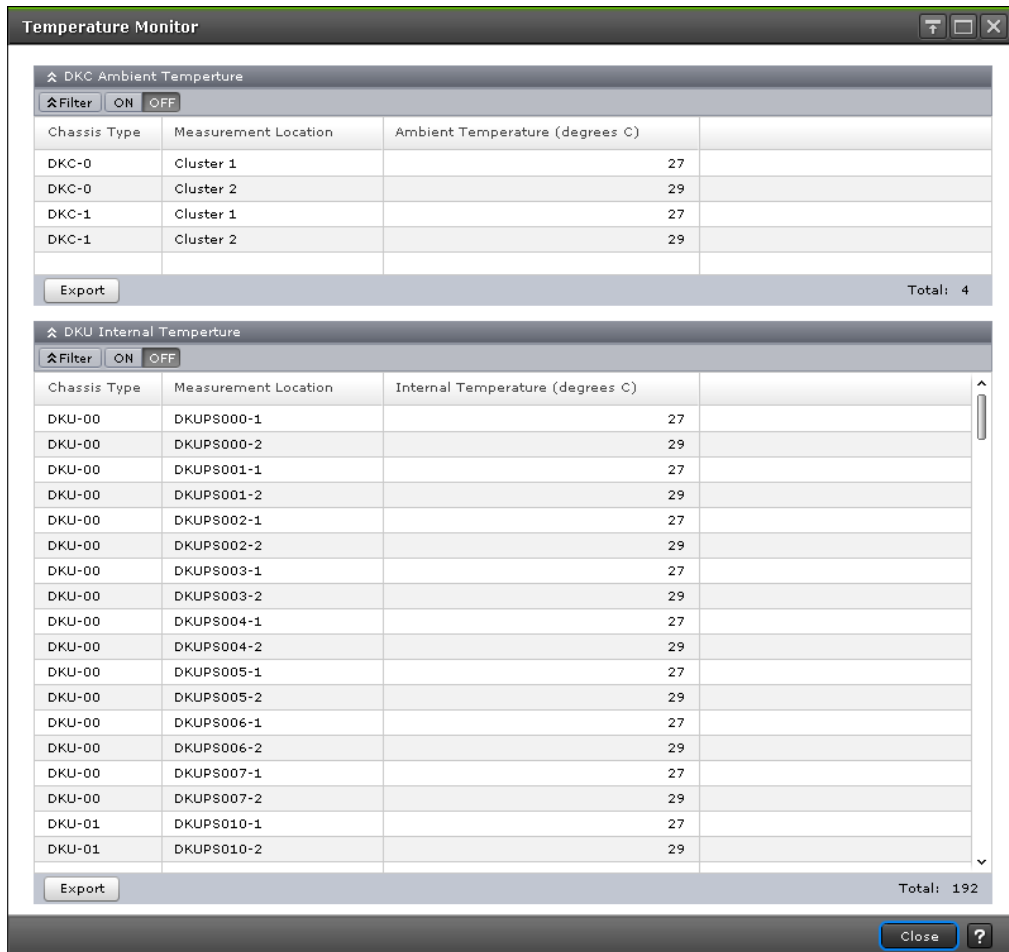
### Resource Groups

The following table describes the items in the Resource Groups table section of the **Resource Lock Properties** window.

Item	Description
Resource Group Name (ID)	Displays the name and ID of the resource group that user can control
Status	Displays the lock status of the resource groups Locked: Locked user exists Unlocked: Locked user does not exist
Lock User	Displays the user name of the person who locked the resource
System	Displays the name of the system that the locked user is using
Lock Start Time	Displays the time when the lock started
Unlock All	Forcibly unlocks all locked resource groups
Virtual Storage Machine	Displays the model type of the virtual storage machine and serial number set for the resource group

## Temperature Monitor window

Displays the temperature information for DKC and DKU.



### DKC Ambient Temperature table

Item	Description
Chassis Type	Displays the chassis ID of the storage system.
Measurement Location	Displays the measurement location.
Ambient Temperature (degrees C)	Displays the ambient temperature in degrees Celsius. A hyphen (-) is displayed when the temperature information cannot be acquired due to a unit or network failure
Export button	Displays a window for outputting table information.

**DKU Internal Temperature table**

<b>Item</b>	<b>Description</b>
Chassis Type	Displays the chassis ID of the storage system.
Measurement Location	Displays the measurement location.
Internal Temperature (degrees C)	Displays the internal temperature in degrees Celsius. A hyphen (-) is displayed when the temperature information cannot be acquired because the chassis is not installed, or a unit or network failure occurred.
Export button	Displays a window for outputting table information.

## Appendix E: Tool Panel GUI Reference

This section describes the windows and features of the SVP **Tool Panel**.

### Control Panel

This section describes the **Tool Panel** windows and controls.

#### Environment Parameter window

This section describes the **Environment Parameter** window features and controls.

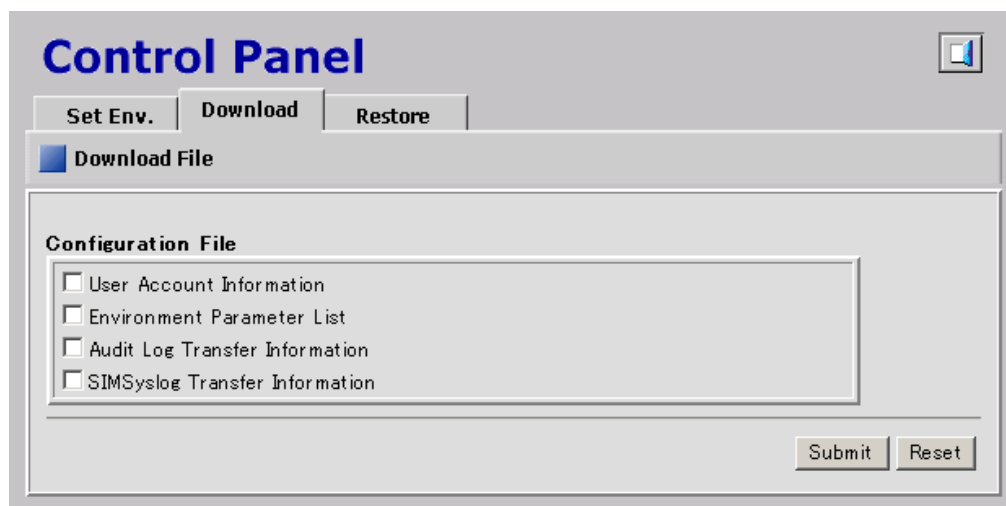
Item	Description
RMI time-out period	This parameter specifies the time-out period for forcible logout when a user performs no operation for a certain period of time because of a network error, etc.
RMI time-out period for Modify	This parameter specifies the time-out period for forcible release of Modify mode when the user is in Modify mode but does not make any changes that access the RMI server for a certain period of time.

Item	Description
RMI time-out period	This parameter specifies the time-out period for forcible logout when a user performs no operation for a certain period of time because of a network error, etc.
RMI time-out period for Modify	This parameter specifies the time-out period for forcible release of Modify mode when the user is in Modify mode but does not make any changes that access the RMI server for a certain period of time.

Item	Description
Polling period for checking exclusive lock	This parameter specifies the polling period for monitoring who is changing information while in Modify mode when other users are viewing the storage system information in View mode.
Polling period for checking obstacles	This parameter specifies the time interval to monitor failure within the storage system.
Submit	Applies the environment parameters to the storage system.
Reset	Resets the environment parameter settings

## Download File window

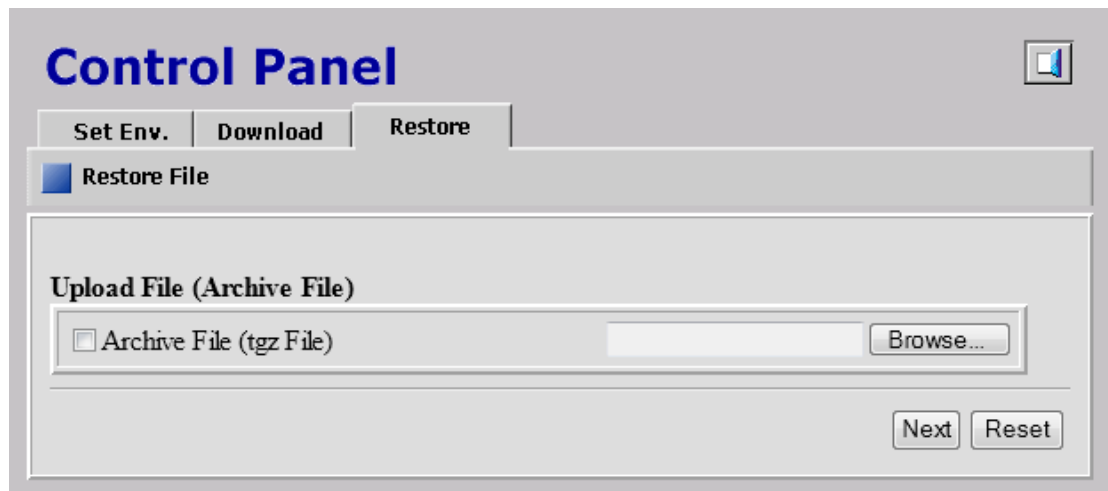
This section describes the **Download File** window features and controls.



Item	Description
Configuration File	Select the checkbox for the file to be downloaded. Downloadable configuration files differ according to the system configuration.
Submit	Downloads the configuration file.
Reset	Cancels downloading the configuration file.

## Restore File window

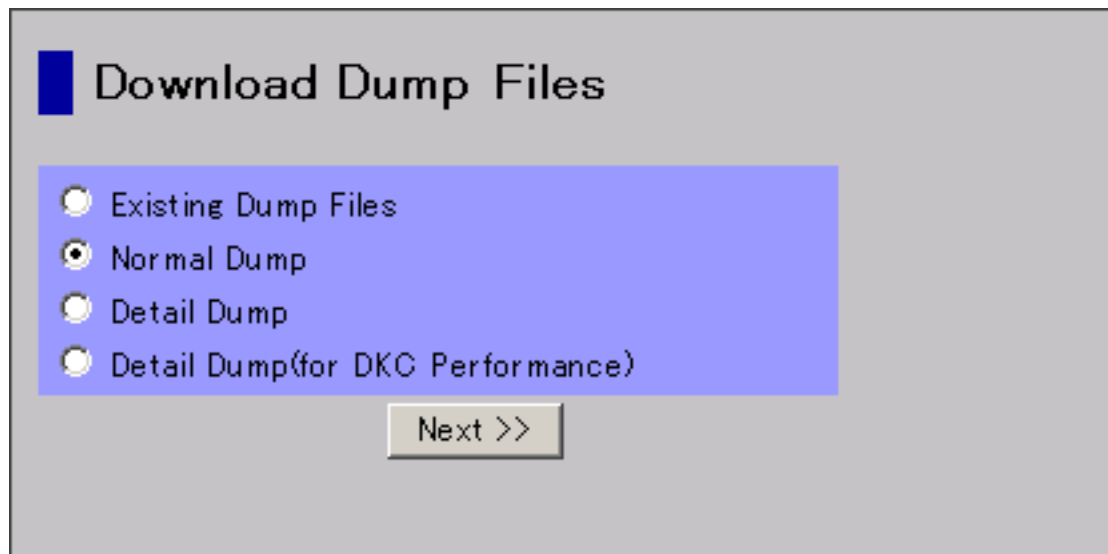
This section describes the **Restore File** window features and controls.



Item	Description
Upload File (Archive File)	Click Browse... and specify the configuration file you want to restore.
Next	Displays a window for confirming the configuration file to be restored.
Reset	Cancels restoring the configuration file.

## Download Dump Files window

This section describes the **Download Dump Files** window features and controls.





Item	Description
Existing Dump Files	Select this when you want to re-download a previously downloaded dump file. This item displays only when one or more compressed dump files exist. If you have not downloaded any dump files, this item does not display even though you have acquired dump files via SVP.
Normal Dump	Contains all information about the SVP and minimum information about the storage system. Select Normal Dump when there is no fatal problem such as a problem with the display of Device Manager - Storage Navigator.
Detail Dump	Contains all information about the storage system in addition to the content of Normal Dump. Select this when you cannot start Device Manager - Storage Navigator or when you check for problems with the storage system.
Detail Dump (for DKC Performance)	Contains information about I/O performance, such as collecting Performance Monitor information in addition to the content of Detail Dump. Select this when you check for problems with the I/O performance.
Next	Displays a dialog box for confirm that the downloading of the dump file can start.

## Update Certificate Files window

This section describes the **Update Certificate Files** window features and controls.

## Update Certificate Files

**Specify the certificate files.**

Certificate file (.crt file)

Key file (.key file)

Item	Description
Certificate file (.crt file)	Click Browse... and specify the certificate file (server.crt file).
Key file (.key file)	Click Browse... and specify the key file (server.key file).
Return to the default certificate	Returns the SSL certificate to default.
Upload	Uploads the SSL certificate.
Reset	Cancels the upload of the SSL certificate.

## Update Certificate Files for the SMI-S window

This section describes the **Update Certificate Files for the SMI-S** window features and controls.

## Update Certificate Files for SMI-S

**Specify the certificate files.**

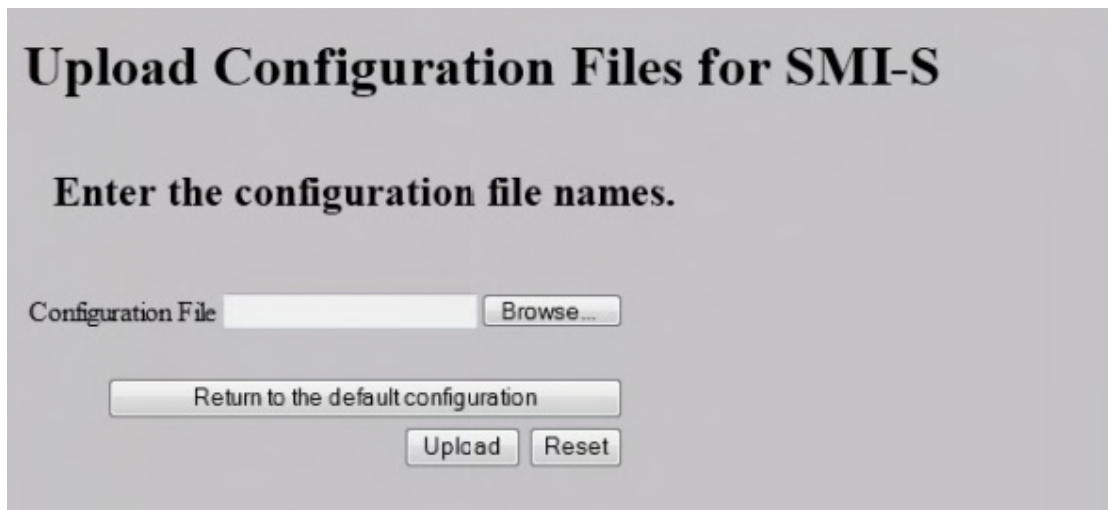
Certificate file (.crt file)

Key file (.key file)

Item	Description
Certificate file (.crt file)	Click Browse... and specify the certificate file (server.crt file).
Key file (.key file)	Click Browse... and specify the key file (server.key file).
Return to the default certificate	Returns the SSL certificate to default.
Upload	Uploads the certificate to the SMI-S provider.
Reset	Cancels the upload of the SMI-S provider certificate.

## Upload Configuration Files for SMI-S window

This section describes the **Upload Configuration Files for SMI-S** window features and controls.



Item	Description
Configuration file	Click Browse... and specify the configuration file you want to upload.
Return to the default configuration	Returns the SMI-S provider configuration file to default
Upload	Uploads the configuration file to SMI-S provider.
Reset	Cancels the upload of the SMI-S provider configuration file.

## SMI-S Artificial Indication window

This section describes the **SMI-S Artificial Indication** window features and controls.



Item	Description
User ID	Enter user ID.
Password	Enter password.
Test	Sends the artificial indication.
Reset	Resets user ID and password.

## Set or Delete Certificate File for HCS window

This section describes the Set or Delete Certificate File for HCS window features and controls.

**Set or Delete Certificate File for HCS**

**Set Certificate File for HCS**

**Specify the certificate file.**

Certificate file (.crt file)

**Delete Certificate File for HCS**

Item	Description
Certificate file (.crt file)	Click Browse... and specify the certificate file (server.crt file).
Register	Registers the certificate for HCS.

<b>Item</b>	<b>Description</b>
Delete	Deletes the certificate for HCS.

---

## Appendix F: SMI-S provider configuration file

To use this SMI-S function you must create a SMI-S provider configuration file. This section describes the SMI-S provider configuration files.

### Array-setting-01.properties file

The array-setting-01.properties file is an SMI-S provider user configuration file. This section describes the description format and organization format of SMI-S provider user configuration files and parameters to be defined.

#### File description format

The format of the array-setting-01.properties file includes the following items:

- File format: text
- Character code: ISO 8859-1
- Line-end symbol: \n, \r, or \r\n
- Comment: Line on which # or ! is the first non-space character

#### File organization format

The organization of the array-setting-01.properties file is shown here:

```
# comment line
parameter1= parameter1_setting_value
parameter2= parameter2_setting_value
# comment line
```

#### Parameters defined in user configuration files

The following table describes the parameters can be specified in user configuration files.

Parameter name	Description
VVolForSnapshot	Specifies virtual volumes that can be used by the SMI-S provider. For parameter details, see <a href="#">VVolForSnapshot parameter (on page 408)</a> .
PoolIDForSnapshot	Specifies pools that can be used by the SMI-S provider. For parameter details, see <a href="#">PoolIDForSnapshot parameter (on page 409)</a> .
ResourceGroup	Specifies the resource groups that the SMI-S provider can use. For parameter details, see <a href="#">ResourceGroup parameter (on page 410)</a> .

All parameters are optional. If no value is specified for a parameter, the default value applies. However, if you specify `VVolForSnapshot`, you must also specify `PoolIDForSnapshot`. Also note that, if you specify `ResourceGroup`, `VVolForSnapshot` and `PoolIDForSnapshot` are ignored.

## VVolForSnapshot parameter

Use the `VVolForSnapshot` parameter to specify virtual volumes that the SMI-S provider can use when you operate Thin Image from `CreateElementReplica` of `HITACHI_ReplicationService`.

All virtual volumes are specified by default.

### Setting up the VVolForSnapshot parameter

Set up the parameter by using `<RangeOfVVol>` and `<SingleVVol>` with a comma (,) as a delimiter:

- `<RangeOfVVol>`: Specifies a range of virtual volumes
- `<SingleVVol>`: Specifies a single virtual volume

#### <RangeOfVVol> format

`<S2HexLDKC>:<S2HexCU>:<S2HexLDEV>to<E2HexLDKC>:<E2HexCU>:<E2HexLDEV>`

- `<S2HexLDKC>`: LDKC number (two-digit hexadecimal) of the first virtual volume in the specified range
- `<S2HexCU>`: CU number (two-digit hexadecimal) of the first virtual volume in the specified range
- `<S2HexLDEV>`: LDEV number (two-digit hexadecimal) of the first virtual volume in the specified range
- `<E2HexLDKC>`: LDKC number (two-digit hexadecimal) of the last virtual volume in the specified range



- <E2HexCU>: CU number (two-digit hexadecimal) of the last virtual volume in the specified range
- <E2HexLDEV>: LDEV number (two-digit hexadecimal) of the last virtual volume in the specified range

#### <SingleVVol> format

<2HexLDKC>:<2HexCU>:<2HexLDEV>

- <2HexLDKC>: LDKC number (two-digit hexadecimal) of the single virtual volume to be specified
- <2HexCU>: CU number (two-digit hexadecimal) of the single virtual volume to be specified
- <2HexLDEV>: LDEV number (two-digit hexadecimal) of the single virtual volume to be specified

#### Example

```
VVolForSnapshot=00:00:00to00:00:FF,00:02:00,00:04:00to00:04:FF
```

In this example, a virtual volume having one of the following LDEV IDs is used as the snapshot target:

- From 00:00:00 (LDKC=0, CU=0, LDEV=0) to 00:00:FF (LDKC=0, CU=0, LDEV=255)
- 00:02:00 (LDKC=0, CU=2, LDEV=0)
- From 00:04:00 (LDKC=0, CU=4, LDEV=0) to 00:04:FF (LDKC=0, CU=4, LDEV=255)

## PoolIDForSnapshot parameter

Use the PoolIDForSnapshot parameter to specify pools that the SMI-S provider can use when you run Thin Image from CreateElementReplica of HITACHI\_ReplicationService.

All pools are specified by default.

#### Setting up the PoolIDForSnapshot parameter

Set up the parameter by using <RangeOfPoolID> and <SinglePoolID> with a comma (,) as a delimiter:

- <RangeOfPoolID>: Specifies a range of pool IDs
- <SinglePoolID>: Specifies a single pool ID

#### <RangeOfPoolID> format

<Start PoolID>to<End PoolID>

- <Start PoolID>: ID of the first pool in the specified range
- <End PoolID>: ID of the last pool in the specified range

**<SinglePoolID> format**

<PoolID>

- <PoolID>: ID of the pool to be specified

**Example**

PoolIDForSnapshot=1to2,4,6to8

In this example, pools having one of the following pool IDs are used as snapshot pools:

- 1 to 2
- 4
- 6 to 8

**ResourceGroup parameter**

Use the ResourceGroup parameter to specify resource groups that the SMI-S provider can use.

All resource groups are specified by default.

**Setting up the ResourceGroup parameter**

Set up the parameter by using <RangeOfResourceGroupID> and <SingleResourceGroupID> with a comma (,) as a delimiter:

- <RangeOfResourceGroupID>: Specifies a range of resource group IDs
- <SingleResourceGroupID>: Specifies a single resource group ID

**<RangeOfResourceGroupID> format**

<Start ResourceGroupID>to<End ResourceGroupID>

- <Start ResourceGroupID>: ID of the first resource group in the specified range
- <End ResourceGroupID>: ID of the last resource group in the specified range

**<SingleResourceGroupID> format**

<ResourceGroupID>

- <ResourceGroupID>: ID of the resource group to be specified

**Example**

ResourceGroup=1to2,4,6to8

In this example, resource groups having one of the following resource group IDs are used:

- 1, 2, 4, 6, and 8

---

## Appendix G: System option modes (SOMs)

System option modes allow the storage systems 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 storage system 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 microcode version 80-06-61.



**Note:** The SOM information might have changed since this document was published. For the latest SOM information, contact customer support.

**Table 28 System option modes for VSP G1x00 and VSP F1500**

Mode	Category	Description	Default	MCU/RCU
15	Common	This SOM can reduce the host response time to be within about 6 seconds.	ON	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is used on a storage system where slow or delayed drive response may affect business operations.</li> <li>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.</li> <li>3. Even though SOM 15 is set to ON, the function does not apply to SATA or NL-SAS drives.</li> <li>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.</li> <li>5. For additional details about this SOM (interaction with other SOMs, operational details), contact customer support (see SOM015 sheet).</li> </ol>		
20	TrueCopy for Mainframe Universal Replicator for Mainframe	<p>S-VOL read only function (secondary system only).</p> <p><b>Mode 20 = ON:</b> The S-VOL accepts host read operations while the pair is split.</p> <p><b>Mode 20 = OFF (default):</b> The S-VOL does not accept host read operations while the pair is split.</p>	OFF	RCU
22	Common	<p>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.</p> <p><b>Mode 22 = ON:</b> 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.</p> <p><b>Mode 22 = OFF:</b> 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).</p> <p>One of the controlling option for correction/drive copy.</p>	OFF	None

Mode	Category	Description	Default	MCU/RCU
36	TrueCopy for Mainframe	<p>Selects function of CRIT=Y(ALL) or CRIT=Y(PATHS).</p> <p><b>Mode 36 = ON:</b> CRIT=Y(ALL) =&gt; equivalent to Primary Volume Fence Level = Data.</p> <p><b>Mode 36 = OFF (default):</b> CRIT=Y(PATHS) =&gt; equivalent to Primary Volume Fence Level = Status.</p>	OFF	MCU
64	TrueCopy for Mainframe	<p><b>Mode 64 = ON:</b></p> <ul style="list-style-type: none"> <li>▪ When receiving the Freeze command, pair volumes in the storage system that fulfill the conditions below are suspended and the status change pending (SCP) that holds write I/Os from the host is set. The path between MCU and RCU is not deleted. Query is displayed only but unusable.</li> <li>▪ When receiving the RUN command, the SCP status of the pairs that fulfill the conditions below is released.</li> <li>▪ When a Failure Suspend occurs when Freeze Option Enable is set, except the pair in which the Failure Suspend occurs, other pairs that fulfill the conditions below go into SCP state.</li> </ul> <p>Conditions:</p> <ul style="list-style-type: none"> <li>▪ TCz P-VOL</li> <li>▪ Mainframe volume</li> <li>▪ Pair status: Duplex/Pending</li> </ul> <p><b>Mode 64 = OFF (default):</b></p> <ul style="list-style-type: none"> <li>▪ When receiving the Freeze command, pairs that fulfill the conditions below are suspended and the SCP is set. In the case of CU emulation type 2105/2017, the path between MCU and RCU is deleted, while the path is not deleted but unusable with Query displayed only in the case of CU emulation type 3990.</li> <li>▪ When receiving the RUN command, the SCP status of the pairs that fulfill the conditions below is released.</li> <li>▪ When a Failure Suspend occurs while the Freeze Option Enable is set, except the pair in which the Failure Suspend occurs, other pairs that fulfill the conditions below go into SCP state.</li> </ul>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p>Conditions:</p> <ul style="list-style-type: none"> <li>▪ TCz P-VOL</li> <li>▪ Mainframe volume</li> <li>▪ Pair status: Duplex/Pending</li> <li>▪ A pair whose RCU# is identical to the RCU for which the Freeze command is specified.</li> </ul> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. General use: SOM 64 = OFF (default).</li> <li>2. When all the following conditions are met, set SOM 64 to ON: <ul style="list-style-type: none"> <li>▪ Customer requests to stop the update I/O operation to the RCU of a TCz pair for the whole storage system.</li> <li>▪ Disaster Recovery function such as GDPS, HyperSwap, or Fail Over/ Fail Back, which requires compatibility with IBM® storage, is not used as SOM 64 operates without having compatibility with IBM® storage.</li> <li>▪ Only Peer-to-Peer-Remote-Copy operation. (Do not use it in combination with Business Continuity Manager.)</li> </ul> </li> <li>3. Even though the Failover command is not an applicable criterion, when executing the Failover command while SOM 114 is ON, since ports are not automatically switched, the Failover command fails.</li> <li>4. With increase of Sync pairs in storage system, the time period to report the completion of Freeze command and RUN command gets longer (estimate of time to report completion: 1 second per 1000 pairs), and MIH may occur.</li> </ol>		
80	ShadowImage	<p>In response to the Restore instruction from the host, if neither Quick nor Normal is specified, the following operation is performed.</p> <p><b>Mode 80 = ON:</b> Normal Restore / Reverse Copy is performed.</p> <p><b>Mode 80 = OFF (default):</b> Quick Restore is performed.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied when the specification for Restore of SI is switched between Quick (default) and Normal.</li> <li>2. The performance of Restore differs depending on the Normal or Quick specification.</li> </ol>		
87	ShadowImage	<p>Determines whether NormalCopy or QuickResync, if not specified, is performed at the execution of pairresync by CCI.</p> <p><b>Mode 87 = ON:</b> QuickResync is performed.</p> <p><b>Mode 87 = OFF (default):</b> NormalCopy is performed.</p>	OFF	-
104	TrueCopy for Mainframe	Changes the default of the CGROUP Freeze option.	OFF	MCU
114	TrueCopy for Mainframe Universal Replicator for Mainframe	<p>Allows dynamic port mode setting (Initiator/RCU target for Fibre Channel) through PPRC CESTPATH and CDELPATH commands.</p> <p><b>Mode 114 = ON:</b> Initiator ports automatically change to RCU target ports, and RCU target ports automatically change to Initiator ports.</p> <p><b>Mode 114 = OFF (default):</b> Automatic port switching during ESTPATH/DELPATH is disabled.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. If you select an incorrect port while this SOM is set to ON, and if ESTPATH is executed when no logic path exists, the port is switched to RCP.</li> <li>2. Set this SOM to OFF before using TPC-R or CSM (IBM® software for disaster recovery).</li> <li>3. For Fibre Channel interface, do not use the CESTPATH and CDELPATH commands at the same time as the SCSI path definition function of LUN Manager. Fibre Channel interface ports need to be configured as initiator ports or RCU target ports before the CESTPATH and CDELPATH commands are issued.</li> <li>4. If you use the FCoE port (16FE10 package), you cannot switch the initiator port and the RCU target port automatically, even if SOM 114 is ON.</li> </ol>	OFF	MCU

Mode	Category	Description	Default	MCU/RCU
122	ShadowImage ShadowImage for Mainframe	<p>For Split or Resync request from the Mainframe host and Storage Navigator.</p> <p><b>Mode 122 = ON:</b> By specifying Split or Resync, Steady/Quick Split or Normal/Quick Resync is respectively executed in accordance with Normal/Quick setting.</p> <p><b>Mode 122 = OFF (default):</b> By specifying Split or Resync, Steady/Quick Split or Normal/Quick Resync is respectively executed in accordance with Normal/Quick setting.</p> <p>For details about pairsplit/pairresync command behavior, contact customer support (see SOM122 sheet).</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. Executing the pairresync command from CCI may be related to the SOM 87 setting.</li> <li>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.</li> <li>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.</li> </ol>	OFF	-
142	Common	<p>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.</p> <p><b>Mode 142 = ON (default*):</b> The threshold value of blocking a drive port due to command time-out is changed to the half of the normal threshold.</p> <p><b>Mode 142 = OFF:</b> The threshold value of blocking a drive port due to command time-out does not change.</p>	ON	-



Mode	Category	Description	Default	MCU/RCU
		<p>*The default setting for this SOM depends on the microcode level:</p> <ul style="list-style-type: none"> <li>▪ Default = ON: 80-04-27 and later (within 80-04-xx range), 80-05-05 and later</li> <li>▪ Default = OFF: earlier than 80-04-27 (within 80-04-xx range), earlier than 80-05-05 (within 80-05-0x range)</li> </ul> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>2. This SOM is effective for the entire storage system.</li> </ol>		

Mode	Category	Description	Default	MCU/RCU
144	Common	<p>This mode is intended to detect and block an HDD whose response is permanently delayed to keep reliability.</p> <p><b>1. Normal response delay detection logic</b></p> <p>Mode 144 = ON: When a response delay drive is detected, SSB=A4CE and A4DE are logged, the drive with response delay is blocked, and SSB=AE4A and SIM=EF0XXX or EF1XXX are reported.</p> <p>The behavior varies depending on the combinations of SOM settings. For details, contact customer support (see SOM144 sheet).</p> <p>Mode 144 = OFF: When a response delay drive is detected, SSB=A4CE is logged, and SIM=DFFXXX is reported.</p> <p>The behavior varies depending on the combinations of SOM settings. For details, contact customer support (see SOM144 sheet).</p> <p><b>2. Early response delay detection logic</b></p> <p>When the logic that detects a minor drive response delay early, which is enabled or disabled by setting SOM1068 to ON or OFF, detects a drive response delay, the drive with response delay is blocked.</p> <p>SOM144 works with the logic and determines whether to block a drive or not when the logic detects a response delay.</p> <p>Mode 144 = ON: When a response delay is detected by the logic, SSB=A4CF is logged, the drive with response delay is blocked, and then SSB=AE4A and SIM=EF0XXX or EF1XXX are reported.</p> <p>The behavior varies depending on the combinations of SOM settings. For details, contact customer support (see sheet SOM144).</p> <p>Mode 144 = OFF: When a response delay is detected by the logic, SSB=A4CF is logged and SIM=DFFXXX is reported.</p>	<p>ON 80-04-27 and later (within 80-04-xx range), 80-05-05 and later but earlier than 80-06-05 OFF (80-06-05 and later)</p>	-

Mode	Category	Description	Default	MCU/RCU
		<p>The behavior varies depending on the combinations of SOM settings. For details, contact customer support (see sheet SOM144).</p> <p><b>Note:</b> The mode is applied if a stable host response is prioritized by separating a drive whose response is permanently delayed at early stage when the drive delay is detected. To apply the mode, note that separating the drive causes decrease in redundancy.</p>		
190	TrueCopy for Mainframe Universal Replicator for Mainframe	<p>Allows you to update the VOLSER and VTOC of the S-VOL while the pair is suspended if both SOM 20 and SOM 190 are ON.</p> <p><b>Mode 190 = ON:</b> When SOM 20 (S-VOL read-only option) and this SOM are both ON, you can update the VOLSER and VTOC of the S-VOL while the pair is suspended. When the pair is resumed, the VOLSER and VTOC of the S-VOL are overwritten with the VOLSER and VTOC of the P-VOL.</p> <p><b>Mode 190 = OFF (default):</b> Even when SOM 20 (S-VOL read-only option) is ON, you cannot update the VOLSER or VTOC of the S-VOL while the pair is suspended.</p>	OFF	RCU
269	Virtual LVI/LUN	<p>High Speed Format for CVS (Available for all device emulation types)</p> <ol style="list-style-type: none"> <li>High Speed Format support When redefining all LDEVs included in an ECC group using Volume Initialize or Make Volume on CVS setting panel, LDEV format, as the last process, will be performed in high speed.</li> <li>Make Volume feature enhancement In addition, with supporting the feature, the Make Volume feature (re-creating new CVs after deleting all volumes in a VDEV), which so far was supported for OPEN-V only, is available for all emulation types.</li> </ol> <p><b>Mode 269 = ON:</b> The High Speed format is available when performing LDEV format on the <b>Maintenance</b> window of the SVP for all LDEVs in a parity group. Note that the High Speed format is not available when performing CVS operations on Storage Navigator for all LDEVs in a parity group.</p>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 269 = OFF (default):</b> As usual, only the low speed format is available when performing CVS operations on Storage Navigator. In addition, the LDEV specifying format on the <b>Maintenance</b> window of the SVP is in low speed as well.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. For additional details about SOM 269, contact customer support (see SOM269 sheet).</li> <li>2. In case of creating a small volume using CVS, the format takes longer time.</li> <li>3. When performing an LDEV format for all LDEVs in a parity group with SOM 269 ON, the format is in high speed, but in the case of VSP/HUS VM and later models, LDEV format performed on Storage Navigator for all LDEVs in a parity group is in low speed.</li> <li>4. For SATA drive, the format is not in high speed.</li> </ol>		
292	TrueCopy for Mainframe	<p>Issuing OLS when Switching Port. In case the mainframe host (FICON<sup>®</sup>) is connected with the CNT-made FC switch (FC9000 etc.) and is using along with the TrueCopy for Mainframe with Open Fibre connection, the occurrence of Link Incident Report for the mainframe host from the FC switch will be deterred when switching the CHT port attribute (including automatic switching when executing CESTPATH and CDELPATH in case of Mode114=ON).</p> <p><b>Mode 292=ON:</b> When switching the port attribute, issue the OLS (100ms) first, and then reset the Chip.</p> <p><b>Mode 292=OFF (default):</b> When switching the port attribute, reset the Chip without issuing the OLS.</p>	OFF	Both
305	Mainframe	<p>This SOM enables the pre-label function (creation of VTOC including VOLSER).</p> <p><b>Mode 305 = ON:</b> Pre-label function is enabled.</p> <p><b>Mode 305 = OFF (default):</b> Pre-label function is disabled.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. Set SOM 305 to ON before performing LDEV Format for a mainframe volume if you want to perform OS IPL (volume online) without fully initializing the volume after the LDEV Format. However, full initialization is required in actual operation.</li> <li>2. Processing time of LDEV format increases by as much as full initialization takes.</li> <li>3. The following functions and conditions are not supported: <ul style="list-style-type: none"> <li>▪ Quick format</li> <li>▪ 3390-A (Dynamic Provisioning attribute)</li> <li>▪ Volume Shredder</li> </ul> </li> <li>4. Full initialization is required in actual operation.</li> <li>5. Microcode versions earlier than 80-05-32-00/00 or earlier than 80-05-47-00/00 (within 80-05-4x range) have a bug. Refer to BID=RAID800-XXXX (SR# HDS04414070). Make sure to use the workaround or the fixed code when SOM 305 is ON.</li> </ol>		
308	TrueCopy for Mainframe Universal Replicator for Mainframe	<p>Allows you to specify whether the Remote Copy Path status, SIM218x, is reported to the host or not.</p> <p>SIM RC=2180 (RIO path failure between MCU and RCU) is not reported to host. The storage system reports SSB with F/M=F5 instead of reporting SIM RC=2180 in case of RIO path failure between MCU and RCU. Micro-program is modified to report SIM RC=2180 with this SOM as individual function for specific customers.</p> <p><b>Mode 308 = ON:</b> SIM RC 2180 is reported, which is compatible with older Hitachi specification.</p> <p><b>Mode 308 = OFF (default):</b> SIM RC 2180 is not reported. Reporting is compatible with IBM - Sense Status report of F5.</p>	OFF	MCU
310	Common	<p><b>Mode 310 = ON:</b> The monitoring timer for MP hang-up is 6 seconds and returning a response to the host within 8 seconds is guaranteed.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 310 = OFF (default):</b> The monitoring timer for MP hang-up is 8 seconds.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM applies to a site where strict host response performance is required.</li> <li>2. If a hardware failure occurs when this SOM is set to ON, the time until MPB blockage is determined is shorter than usual.</li> </ol>		
448	Universal Replicator Universal Replicator for Mainframe	<p><b>Mode 448 = ON:</b> After a physical path failure (such as path disconnection) is detected, a mirror is split (suspended) one minute after the detection. On the MCU side, the mirror is suspended one minute after read journal commands from the RCU stop. On the RCU side, the mirror is suspended one minute after read journal commands fail.</p> <p><b>Mode 448 = OFF (default):</b> After a physical path failure (such as path disconnection) is detected, a mirror is split (suspended) if the path is not restored within the path monitoring time set by the mirror option.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. The mode is applied when pairs need to be suspended one minute after a communication error between UR MCU and RCU is detected.</li> <li>2. When SOM 449 is set to ON, SOM 448 does not function.</li> </ol>	OFF	-
449	Universal Replicator Universal Replicator for Mainframe	<p>This mode is used to enable and disable detection of communication failures between the MCU and RCU. The default setting is ON.</p> <p><b>Mode 449 = ON (default):</b> When a physical path failure is detected, the pair is not suspended. On the MCU side, checking read journal command disruption from the RCU is disabled, and monitoring read journal command failures is disabled on the RCU side.</p> <p><b>Mode 449 = OFF:</b> When a physical path failure is detected, the pair is suspended after the path monitoring time set by the mirror option has passed or after one minute. Detecting communication failures between the MCU and RCU is enabled. When this mode is set to OFF, SOM 448 can be enabled.</p>	ON	MCU

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied when disabling the detection of communication failures between the MCU and RCU in UR/URz configuration is required.</li> <li>2. When this SOM is set to ON, SOM 448 does not work.</li> <li>3. This SOM setting is not changed by microcode upgrade.</li> <li>4. This SOM is not effective for remote paths between an Initiator port on the MCU and a Target port on the RCU.</li> <li>5. While a path from the RCU to MCU is disconnected, if the UR/URz pair remains in Suspending or Deleting status, recover it in accordance with the procedure in Recovery from UR/URz Failure in TROUBLE SHOOTING section of Maintenance Manual.</li> </ol>		
454	Virtual Partition Manager	<p>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.</p> <p><b>Mode 454 = OFF (default):</b> 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.)</p> <p>*a: (Write Pending capacity of CLPR#x of concerned MPB) ÷ (Cache capacity of CLPR#x of concerned MPB), x=0 to 31</p> <p>CLPR whose value above is the highest of all CLPRs</p> <p>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.</p> <p>Therefore, set SOM 454 to OFF in most cases.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 454 = ON:</b></p> <p>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.)</p> <p>*b: (Write Pending capacity of the entire system of concerned MPB) ÷ (Cache capacity of the entire system of concerned MPB)</p> <p><b>Caution:</b> 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.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>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.</li> </ol> <p>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.</p> <ol style="list-style-type: none"> <li>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.</li> </ol>		
457	Universal Volume Manager	This SOM has two purposes: High-Speed LDEV Format for External Volumes, and Support for Mainframe Control Block Write GUI.	OFF	Both



Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 457 = ON:</b></p> <ol style="list-style-type: none"> <li data-bbox="513 302 1024 359">1. High-Speed LDEV Format for External Volumes.</li> </ol> <p>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.</p> <ol style="list-style-type: none"> <li data-bbox="513 716 1089 772">2. Support for Mainframe Control Block Write GUI.</li> </ol> <p>Control Block Write of the external LDEVs in mainframe emulation is supported by Device Manager - Storage Navigator (GUI).</p> <p><b>Mode 457 = OFF (default):</b> High-speed LDEV format for external volumes and support for mainframe control block write GUI are not available.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li data-bbox="513 1125 1130 1224">▪ If the LDEV is not written with data "0" before performing the function, the LDEV format might fail.</li> <li data-bbox="513 1245 1097 1302">▪ After the format processing, make sure to set SOM 457 to OFF.</li> </ul>		
459	ShadowImage ShadowImage for Mainframe	<p>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:</p> <p><b>Mode 459 = ON:</b> When suspending an SI/Siz pair: Waits for the copy data in cache memory to completely destage to the external volume S-VOL before changing the pair status to SUSPEND.</p> <p><b>Mode 459 = OFF (default):</b> When suspending an SI/Siz pair: The status changes to SUSPEND as soon as all of the delta data is copied to S-VOL cache. The status does not wait for cache to destage to the S-VOL external volume.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
466	Universal Replicator Universal Replicator for Mainframe	<p>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.</p> <p><b>Mode 466 = ON:</b> Data transfer speeds of 10 Mbps and higher are supported. The JNL read is performed with 4-multiplexed read size of 256 KB.</p> <p><b>Mode 466 = OFF (default):</b> 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.</p> <p><b>Note:</b> The data transfer speed can be changed using the Change JNL Group options.</p>	OFF	-
467	ShadowImage ShadowImage for Mainframe Compatible FlashCopy® V2 Compatible FlashCopy® SE Snapshot Universal Volume Manager Volume Migration	<p>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.</p> <ul style="list-style-type: none"> <li>▪ SI</li> <li>▪ SIz</li> <li>▪ FCv2, FCSE</li> <li>▪ Snapshot</li> <li>▪ UVM</li> <li>▪ Volume Migration</li> </ul> <p><b>Mode 467 = ON (default):</b> 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.</p> <p><b>Mode 467 = OFF:</b> 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.</p>	ON	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Caution:</b> This SOM must always be set to ON when using an external volume as the secondary volume of any of the applicable replication products.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. It takes longer to finish the copy processing because it stops for prioritizing the host I/O performance.</li> <li>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.</li> <li>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.</li> </ol> <p>*Applies to pairs of SI, Slz, FCv2, FCSE, Snapshot, and Volume Migration.</p>		
471	Thin Image	<p>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.</p> <p>The SIM-RCs reported by setting the SOM to ON are: 601xxx (Pool utilization threshold exceeded), 603000 (SM space warning).</p> <p><b>Mode 471 = ON:</b> These SIM-RCs are reported to maintenance personnel.</p> <p><b>Mode 471 = OFF (default):</b> These SIM-RCs are not reported to maintenance personnel.</p> <p><b>Note:</b> Set this SOM to ON when it is required to inform maintenance personnel of these SIM-RCs.</p>	OFF	-
474	Universal Replicator Universal Replicator for Mainframe	<p>UR initial copy performance can be improved by issuing a command from CCI/Business Continuity Manager (BCM) to execute a dedicated script consisting of UR initial copy (Nocopy), UR suspend, TC Sync initial copy, TC Sync delete, and UR resync.</p>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 474 = ON:</b> 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.</p> <p><b>Mode 474 = OFF (default):</b> 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.</p> <p>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.</p>		

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. Set this SOM for both primary and secondary storage systems.</li> <li>2. When this SOM is set to ON: <ul style="list-style-type: none"> <li>▪ Execute all pair operations from CCI/BCM.</li> <li>▪ Use a dedicated script.</li> <li>▪ Initial copy operation is prioritized over update I/O. Therefore, the processing speed of the update I/O slows down.</li> </ul> </li> <li>3. If this SOM is set to ON, the processing speed of update I/O slows down by about 15 <math>\mu</math>s per command, version downgrade is disabled, and Take Over is not available.</li> <li>4. If this SOM is not set to ON for both sides, the behavior is as follows: <ul style="list-style-type: none"> <li>▪ OFF in primary and secondary storage systems: Normal UR initial copy performance.</li> <li>▪ ON in the primary storage system/OFF in the secondary storage system: TC Sync pair creation fails.</li> <li>▪ OFF in the primary storage system/ON in the secondary storage system: The update data is copied to the S-VOL synchronously.</li> </ul> </li> <li>5. While this SOM is set to ON, make sure not to perform microcode downgrade to an unsupported version.</li> <li>6. While this SOM is set to ON, make sure not to perform the Take Over function.</li> <li>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.</li> <li>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.</li> </ol>		

Mode	Category	Description	Default	MCU/RCU
484	TrueCopy for Mainframe ShadowImage for Mainframe	<p>The IBM®-compatible PPRC FC path interface was supported with TagmaStore USP 50-06-11. As the specification of QUERY display using FC interface (hereinafter called New Spec) is different from the ESCON® specification (hereinafter called Previous Spec), this SOM enables to display the PPRC path QUERY with New Spec or Previous Spec.</p> <ul style="list-style-type: none"> <li>▪ <b>Mode 484 = ON:</b> The status of path using the Fibre Channel interface is displayed. WWNN is indicated.</li> <li>▪ <b>Mode 484 = OFF (default):</b> The status of path using an ESCON® interface is displayed. WWNN is invalid.</li> </ul> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. Set this SOM to ON when you want to maintain compatibility with the Previous Spec for PPRC path QUERY display under the environment where IBM host function (such as PPRC and GDPS) is used.</li> <li>2. When an old model or a TagmaStore USP that does not support this SOM is connected using TCz, set this SOM to OFF.</li> <li>3. If the display specification is different between MCU and RCU, it may cause malfunction of host.</li> <li>4. When IBM® TPC-R or CSM software for disaster recovery is used, set this SOM to ON.</li> </ol>	OFF	Both
495	NAS	<p>Function: That the secondary volume where S-VOL Disable is set means the NAS file system information is imported in the secondary volume. If the user has to take a step to release the S-VOL Disable attribute in order to perform the restore operation, it is against the policy for the guard purpose and the guard logic to have the user uninvolved. In this case, in the NAS environment, SOM 495 can be used to enable the restore operation.</p> <p><b>Mode 495 = ON:</b> The restore operation (Reverse Copy, Quick Restore) is allowed on the secondary volume where S-VOL Disable is set.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<b>Mode 495 = OFF (default):</b> The restore operation (Reverse Copy, Quick Restore) is not allowed on the secondary volume where S-VOL Disable is set.		
506	Universal Replicator Universal Replicator for Mainframe	<p>This SOM is used to enable Delta Resync with no host update I/O by copying only differential JNL instead of copying all data.</p> <p>The UR Delta Resync configuration is required.</p> <p><b>Mode 506 = ON:</b></p> <ul style="list-style-type: none"> <li>▪ Without update I/O: Delta Resync is enabled.</li> <li>▪ With update I/O: Delta Resync is enabled.</li> </ul> <p><b>Mode 506 = OFF (default):</b></p> <ul style="list-style-type: none"> <li>▪ Without update I/O: Total data copy of Delta Resync is performed.</li> <li>▪ With update I/O: Delta Resync is enabled.</li> </ul> <p><b>Note:</b> 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.</p>	OFF	Both
530	Universal Replicator for Mainframe	<p>When a Universal Replicator for Mainframe pair is in the Duplex state, this SOM switches the display of Consistency Time (C/T) between the values at JNL restore completion and at JNL copy completion.</p> <p><b>Mode 530 = ON:</b> C/T displays the value of when JNL copy is completed.</p> <p><b>Mode 530 = OFF (default):</b> C/T displays the value of when JNL restore is completed.</p> <p><b>Note:</b> At the time of Purge suspend or RCU failure suspend, the C/T of Universal Replicator for Mainframe displayed by Business Continuity Manager or Storage Navigator may show earlier time than the time showed when the pair was in the Duplex state.</p>	OFF	RCU
531	Common	<p>When PIN data is generated, the SIM currently stored in SVP is reported to the host.</p> <p><b>Mode 531 = ON:</b> The SIM for PIN data generation is stored in SVP and reported to the host.</p>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<b>Mode 531 = OFF (default):</b> The SIM for PIN data generation is stored in SVP only, not reported to the host, the same as the current specification.		
548	ShadowImage for Mainframe from BCM TrueCopy for Mainframe from BCM Universal Replicator for Mainframe from BCM	This SOM prevents pair operations of TCz, URz, or Slz via Command Device online. <b>Mode 548 = ON:</b> Pair operations of TCz, URz, or Slz via online Command Device are not available. SSB=0x64fb is output. <b>Mode 548 = OFF (default):</b> Pair operations of TCz, URz, or Slz via online Command Device are available. SIM is output. <b>Notes:</b> <ol style="list-style-type: none"><li>1. When Command Device is used online, if a script containing an operation via Command Device has been executed, the script may stop if this SOM is set to ON. As described in the BCM user's guide, the script must be performed with Command Device offline.</li><li>2. This SOM is applied to operations from BCM that is operated on MVS.</li></ol>	OFF	Both
556	Open	Prevents an error code from being set in the 8 - 11th bytes in the standard 16-byte sense byte. <b>Mode 556 = ON:</b> An error code is not set in bytes 8 - 11 in the standard 16-byte sense byte. <b>Mode 556 = OFF (default):</b> An error code is set in bytes 8 - 11 in the standard 16-byte sense byte.	OFF	Both
561	ShadowImage Universal Volume Manager	Allows Quick Restore for external volumes with different Cache Mode settings. <b>Mode 561 = ON:</b> Quick Restore for external volumes with different Cache Mode settings is prevented. <b>Mode 561 = OFF (default):</b> Quick Restore for external volumes with different Cache Mode settings is allowed.	OFF	Both
573	TrueCopy for Mainframe ShadowImage for Mainframe	For the CU emulation type 2105/2107, specifying the CASCADE option for the ICKDSF ESTPAIR command is allowed. <b>Mode 573 = ON:</b> The ESTPAIR CASCADE option is allowed.	OFF	Both



Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 573 = OFF (default):</b> The ESTPAIR CASCADE option is not allowed. (When specified, the option is rejected.)</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. When CU emulation type is 2105/2107, this SOM is applied in the case where pair creation in TCz – Slz cascading configuration in the ICKDSF environment fails with the following message output. Message: ICK30111I DEVICE SPECIFIED IS THE SECONDARY OF A DUPLEX OR PPRC PAIR</li> <li>2. This SOM is applied when building an environment using the Metro Mirror F.O./F.B. function with TPC-R or CSM.</li> <li>3. The CASCADE option can be specified in the TSO environment also.</li> <li>4. Although the CASCADE option can be specified for the ESTPAIR command, the PPRC-XD function is not supported.</li> <li>5. Perform thorough pre-check for any influence on GDPS/PPRC.</li> <li>6. The SOM must be enabled only when the CASCADE option is specified for the ESTPAIR command for the CU emulation type 2105/2107.</li> </ol>		The unit for which TCz and Slz in a cascading configuration use the same volume.
589	Universal Volume Manager	<p>When this SOM is ON, the frequency of progress update of disconnection is changed.</p> <p><b>Mode 589 = ON:</b> For each external volume, progress is updated only when the progress rate is 100%.</p> <p><b>Mode 589 = OFF (default):</b> Progress is updated when the progress rate exceeds the previous level.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>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.</li> </ol>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p>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%).</p>		
598	Universal Replicator for Mainframe	<p>This SOM is used to report SIMs (RC=DCE0 to DCE3) to a Mainframe host to warn that a URz journal is full.</p> <p><b>Mode 598 = ON:</b> SIMs (RC=DCE0 to DEC3) to warn that a JNL is full are reported to SVP and the host.</p> <p><b>Mode 598= OFF (default):</b> SIMs (RC=DCE0 to DEC3) to warn that a JNL is full are reported to SVP only.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied if SIMs (RC=DCE0 to DCE3) need to be reported to a Mainframe host.</li> <li>2. The SIMs are not reported to the Open server.</li> <li>3. SIMs for JNL full (RC=DCE0 and DCE1) on MCU are reported to the host connected with MCU.</li> <li>4. SIMs for JNL full (RC=DCE2 and DCE3) on RCU are reported to the host connected with RCU.</li> </ol>	OFF	Both
664	Server Priority Manager	<p>This mode changes SPM upper limit control method for WWN control.</p> <p>In a host configuration in which the queue depth is greater than 8, multi-path software is used, or the striping function is used, traffic might be controlled much lower than the upper limit set for non-prioritized WWNs. This mode is used to improve the upper limit control method.</p> <p><b>Mode 664 = ON (default):</b> The new upper limit control (managing the total number of I/Os) is applied for I/O control. The control works by monitoring the performance of non-prioritized WWNs in real time.</p>	ON	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Note:</b> Even when SOM 664 is ON, some workloads that exceed an upper limit might not be adequately controlled (for example, when the Adaptive multipath policy of Veritas Volume Manager or the Dynamic Multipathing function of Red Hat Enterprise Linux is used). In this case, consider setting the multipath I/O policy to round-robin instead of other policies.</p> <p><b>Mode 664 = OFF:</b> The current upper limit control (assigning upper limit in advance) is applied for I/O control. The control works based on the non-prioritized WWNs performance monitored immediately before.</p> <p><b>Caution:</b> Setting SOM 664 to OFF can result in overthrottling of workloads and significant impact. Make sure SOM 664 is set to ON to ensure proper SPM operations.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. Set this mode to ON when all of the following conditions are met: <ol style="list-style-type: none"> <li>a. The upper limit is set for traffic of non-prioritized WWNs.</li> <li>b. The queue depth is greater than 8, multipath software is used, or the striping function is used in a host configuration.</li> </ol> </li> <li>2. To downgrade the microcode from the support version to an unsupported version below, set this mode to OFF. If the microcode is downgraded from a support version to an unsupported version while this mode is set to ON, I/Os exceeding the upper limit might be received or I/Os might be kept lower than the upper limit. <ul style="list-style-type: none"> <li>▪ Earlier than 80-03-39-00/00</li> <li>▪ Earlier than 80-04-05-00/00 (within 80-04-0x range)</li> <li>▪ Earlier than 80-04-22-00/00 (within 80-04-2x range)</li> </ul> </li> <li>3. For several seconds at SOM setting change (ON/OFF), I/Os exceeding the upper limit might be received.</li> </ol>		

Mode	Category	Description	Default	MCU/RCU
665	Common	<p>Disables the automatic log dump collection function that is executed when a hardware failure occurs to reduce the time to start failure analysis. A failure log created on a storage system triggers the function to start at a hardware failure.</p> <p><b>Mode 665 = ON (default):</b> The auto dump collection function is disabled.</p> <p><b>Mode 665 = OFF:</b> The auto dump collection function is enabled.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied when disabling the automatic log dump collection function is required at a failure.</li> <li>2. This SOM is effective for the entire storage system.</li> </ol>	ON	-
689	TrueCopy TrueCopy for Mainframe global-active device	<p>Allows you to slow the initial copy and resync operations when the write-pending rate on the RCU exceeds 60%.</p> <p><b>Mode 689 = ON:</b> The initial copy and resync copy operations are slowed down when the Write Pending rate on RCU exceeds 60%.</p> <p>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.</p> <p><b>Mode 689 = OFF (default):</b> The initial copy and resync copy operations are not slowed down when the Write Pending rate on RCU exceeds 60% (the same as before).</p>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM can be set online.</li> <li>2. The micro-programs on both MCU and RCU must support this SOM.</li> <li>3. This SOM should be set when requested by the user.</li> <li>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.</li> <li>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.</li> <li>6. If the write pending rate of CLPR to which the initial copy target S-VOL belongs is not over 60% but that of MP PCB to which the S-VOL belongs is over 60%, the initial copy operation is slowed down.</li> <li>7. Do not set this SOM if the primary or secondary system is connected to USP V/VM with microcode earlier than 60-02-xx. If this SOM is applied and the write-pending rate reaches 60%, pair suspend might occur.</li> </ol>		
690	Universal Replicator Universal Replicator for Mainframe	<p>This SOM is used to prevent Read JNL or JNL Restore when the Write Pending rate on RCU exceeds 60% as follows:</p> <ul style="list-style-type: none"> <li>▪ When CLPR of JNL-Volume exceeds 60%, Read JNL is prevented.</li> <li>▪ When CLPR of Data (secondary)-Volume exceeds 60%, JNL Restore is prevented.</li> </ul> <p><b>Mode 690 = ON:</b> Read JNL or JNL Restore is prevented when the Write Pending rate on RCU exceeds 60%.</p> <p><b>Mode 690 = OFF (default):</b> Read JNL or JNL Restore is not prevented when the Write Pending rate on RCU exceeds 60% (the same as before).</p>	OFF	RCU

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM can be set online.</li> <li>2. This SOM should be set per customer's requests.</li> <li>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.</li> <li>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.</li> <li>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.</li> </ol>		
696	Open	<p>This SOM is available to enable or disable the QoS function.</p> <p><b>Mode 696 = ON:</b> QoS is enabled. (In accordance with the Share value set to SM, I/Os are scheduled. The Share value setting from RMLIB is accepted)</p> <p><b>Mode 696 = OFF (default):</b> QoS is disabled. (The Share value set to SM is cleared. I/O scheduling is stopped. The Share value setting from host is rejected.)</p> <p><b>Note:</b> Set this SOM to ON when you want to enable the QoS function.</p>	OFF	-
701	Universal Volume Manager	<p>Issues the Read command at the logical unit discovery operation using UVM.</p> <p><b>Mode 701 = ON:</b> The Read command is issued at the logical unit discovery operation.</p> <p><b>Mode 701 = OFF (default):</b> The Read command is not issued at the logical unit discovery operation.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>2. When this SOM is set to ON, it takes longer time to complete the LU discovery. The amount of time depends on external storages.</li> <li>3. With this SOM OFF, if searching for external devices with VMA is set, the VMA information cannot be read.</li> <li>4. When this SOM is set to ON while the following conditions are met, the external volume is blocked: <ul style="list-style-type: none"> <li>▪ An external volume to which Nondisruptive migration (NDM) attribute is set exists.</li> <li>▪ The external volume is reserved by the host</li> </ul> </li> <li>5. As the VMA information is USP/NSC specific, this SOM does not need to be ON when the external storage is other than USP/NSC.</li> <li>6. Set this SOM to OFF when an external volume to which nondisruptive migration (NDM) attribute is set exists.</li> </ol>		
704	ShadowImage ShadowImage for Mainframe  Compatible FlashCopy®  Volume Migration	<p>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.</p> <p><b>Mode 704 = ON:</b> Copy processing requested is registered into a newly created queue so that the processing is scheduled with lower priority than host I/O.</p> <p><b>Mode 704 = OFF (default):</b> Copy processing requested is not registered into a newly created queue. Only the existing queue is used.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>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.</li> </ol>		
721	Common	<p>When a parity group is uninstalled or installed, the following operation is performed according to the setting of SOM 721.</p> <p><b>Mode 721 = ON:</b> 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.</p> <p><b>Mode 721 = OFF (default):</b> 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.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>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.</li> </ol>	OFF	-
725	Universal Volume Manager	This SOM determines the action that will be taken when the status of an external volume is Not Ready.	OFF	-



Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 725 = ON:</b> 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.</p> <p>When the status of a device is Not Ready blockade, Device Health Check is executed after 30 seconds.</p> <p><b>Mode 725 = OFF (default):</b> 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).</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. Applying this SOM is prohibited when USP VVM is used as an external storage system and its external volume is DP-VOL.</li> <li>2. Applying this SOM is recommended when the above condition (1) is not met and SUN storage is used as an external storage.</li> <li>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.</li> <li>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.</li> <li>5. While USP VVM 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.</li> <li>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.</li> </ol>		
729	Dynamic Provisioning Data Retention Utility	When a DP pool is full, if any write operation is requested to the area where the page allocation is not provided, this SOM can enable the DRU Protect attribute for the target DP-VOL.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 729 = ON:</b> 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.)</p> <p><b>Mode 729 = OFF (default):</b> 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.</p> <p>For details, contact customer support (see SOM729 &amp; 803 sheet).</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied when: <ul style="list-style-type: none"> <li>▪ The threshold of pool is high (for example, 95%) and the pool may be full.</li> <li>▪ File system is used.</li> <li>▪ Data Retention Utility is installed.</li> </ul> </li> <li>2. Since the Protect attribute is set for V-VOL, the Read operation cannot be allowed as well.</li> <li>3. When Data Retention Utility is not installed, the desired effect is not achieved.</li> <li>4. Protect attribute can be released from the <b>Data Retention</b> window of Device Manager - Storage Navigator after releasing the full status of the pool by adding a Pool-VOL.</li> <li>5. With 80-02-01-00/01 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. <b>Caution:</b> 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.</li> </ol>		

Mode	Category	Description	Default	MCU/RCU
		<p>6. With 80-02-41-00/00 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.</p>		
733	ShadowImage ShadowImage for Mainframe Volume Migration	<p>This SOM enables to suspend Volume Migration or Quick Restore operation during LDEV-related maintenance.</p> <p><b>Mode 733 = ON:</b> Volume Migration or Quick Restore operation during LDEV-related maintenance is not suspended.</p> <p><b>Mode 733 = OFF (default):</b> Volume Migration or Quick Restore operation during LDEV-related maintenance is suspended.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>Note that behavior when this SOM is set to ON and OFF is reversed between USP V/VM and VSP/HUS VM and later.</li> <li>This SOM should be applied to perform Volume Migration or Quick Restore during maintenance operation.</li> <li>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.</li> <li>An LDEV-related maintenance operation such as LDEV installation/removal may fail when Volume Migration or Quick Restore takes place.</li> </ol>	OFF	-
734	Dynamic Provisioning  Dynamic Provisioning for Mainframe	<p>When exceeding the pool threshold, the SIM is reported as follows:</p> <p><b>Mode 734 = ON:</b> 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.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 734 = OFF (default):</b> 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.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is turned ON to prevent the write I/O operation from being unavailable due to pool full.</li> <li>2. If the exceeding pool threshold SIM occurs frequently, other SIMs may not be reported.</li> <li>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.</li> <li>4. Turning on SOM 741 can provide the SIM report to both the users and the service personnel.</li> </ol>		
741	Dynamic Provisioning Dynamic Provisioning for Mainframe	<p>This SOM enables to switch over whether to report the following SIM for users to the service personnel:</p> <p>SIM-RC 625000 (DP pool usage rate continues to exceed the threshold)</p> <p><b>Mode 741 = ON:</b> SIM is reported to the service personnel.</p> <p><b>Mode 741 = OFF (default):</b> SIM is not reported to the service personnel.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is set to ON to have SIM for users reported to the service personnel: <ul style="list-style-type: none"> <li>▪ For the system where SNMP and E-mail notification are not set.</li> <li>▪ If Device Manager - Storage Navigator is not periodically activated.</li> </ul> </li> <li>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.</li> </ol>		
745	Universal Volume Manager	<p>Enables to change the area where the information is obtained as the Characteristic1 item from SYMMETRIX.</p> <p><b>Mode 745 = ON:</b></p> <ul style="list-style-type: none"> <li>▪ The area where the information is obtained as the Characteristic1 item from SYMMETRIX is changed.</li> <li>▪ 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.</li> </ul> <p><b>Mode 745 = OFF (default):</b></p> <ul style="list-style-type: none"> <li>▪ The area where the information is obtained as the Characteristic1 item from SYMMETRIX is set to the default.</li> <li>▪ When CheckPaths or Device Health Check (1/ hour) is performed, the information of an already-mapped external volume is updated to the default.</li> </ul>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied when the EMC SYMMETRIX is connected using UVM.</li> <li>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.</li> <li>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.</li> <li>4. If the Check Paths is performed while ShadowImage for Mainframe pair and FlashCopy<sup>®</sup> Mirror pair are defined in the specified volume, the Check Paths operation is rejected with a message, "605 2518". If ShadowImage for Mainframe pair and FlashCopy<sup>®</sup> Mirror pair are defined in the specified volume, do not perform Check Paths but wait until the display is automatically changed.</li> </ol>		
749	Dynamic Provisioning Dynamic Provisioning for Mainframe Dynamic Tiering Dynamic Tiering for Mainframe Thin Image	<p>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.</p> <p><b>Mode 749 = ON:</b> The HDP Rebalance function and the HDT Tier relocation function are disabled.</p> <p><b>Mode 749 = OFF (default):</b> The HDP Rebalance function and the HDT Tier relocation function are enabled.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied when no change in performance characteristic is desired.</li> <li>2. When a pool is newly installed, the load may be concentrated on the installed pool volumes.</li> <li>3. When 0 data discarding is executed, load may be unbalanced among pool volumes.</li> <li>4. Pool VOL deletion while this SOM is set to ON fails. To delete pool VOLs, set this SOM to OFF.</li> </ol>		
757	Common	<p>Enables/disables output of in-band audit logs.</p> <p><b>Mode 757 = ON:</b> In-band audit log is not output.</p> <p><b>Mode 757 = OFF (default):</b> In-band audit log is output.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. Mode 757 applies to the sites where outputting the In-band audit logs is not needed.</li> <li>2. When this SOM is set to ON: <ul style="list-style-type: none"> <li>▪ There is no access to SM for the In-band audit logs, which can avoid the corresponding performance degradation.</li> <li>▪ SM is not used for the In-band audit logs.</li> </ul> </li> <li>3. If outputting the In-band audit log is desired, set this SOM to OFF.</li> </ol>	OFF	-
762	Universal Replicator for Mainframe	<p>This SOM enables to settle the data to RCU according to the time stamp specified in the command when a Flush suspension for an EXCTG is performed from BCM.</p> <p><b>Mode 762 = ON:</b> The data is settled to RCU according to the time stamp specified in the command.</p> <p><b>Mode 762 = OFF (default):</b> The data is settled to RCU according to the time stamp that RCU has received.</p>	OFF	Both (On RCU side, consideration in Takeover is required for setting)

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied under the following conditions. <ul style="list-style-type: none"> <li>▪ Universal Replicator for Mainframe.</li> <li>▪ EXCTG configuration.</li> <li>▪ Flush suspension with an EXCTG specified is executed.</li> <li>▪ BCM is installed on the host where the time stamping function is available.</li> <li>▪ (In the case of multiple-host configuration, SYSPLEX timer is available on the system)</li> </ul> </li> <li>2. If this SOM is set to ON while the BCM does not exist in the environment where the time stamping function is available (In the case of multiple-host configuration, SYSPLEX timer is available on the system), the pair status may not become Suspend after Flush suspension for an EXCTG.</li> <li>3. Do not set this SOM to ON if the BCM does not exist in the environment where the time stamping function is available (In the case of multiple-host configuration, SYSPLEX timer is available on the system).</li> </ol>		
769	TrueCopy TrueCopy for Mainframe Universal Replicator Universal Replicator for Mainframe	<p>Controls whether the retry operation is executed or not when a path creation operation is executed. (The function applies to both of CU FREE path and CU single path for Open and Mainframe).</p> <p>Apply this SOM when the Basic HyperSwap<sup>®</sup> function of TPC-R or CSM is used. The Basic HyperSwap<sup>®</sup> function can allow the CESTPATH operation to establish a path to several secondary systems at the same time. Because attributes of a port are switched if the CESTPATH operation is performed with SOM 144 ON, the path status between the primary and secondary systems is changed to linkdown. If the CESTPATH operation is performed to two or more secondary systems at the same time, MIH may be reported to a host as the other CESTPATH operation, which has detected the linkdown path, retries the CESTPATH operation. To disable an MIH report to a host, set this SOM to ON to disable the CESTPATH to retry the operation when a linkdown is detected.</p>	OFF	Both



Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 769 = ON:</b> The retry operation is disabled when the path creation operation is executed (retry operation is not executed).</p> <p><b>Mode 769 = OFF (default):</b> The retry operation is enabled when the path creation operation is executed (retry operation is executed).</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. Apply this SOM when the following three conditions are met: <ul style="list-style-type: none"> <li>▪ SOM 114 is set to OFF (operation of automatically switching the port is disabled).</li> <li>▪ HMO 49 and HMO 50 are set to OFF (60-07-51-00/00 and later, 70-02-31-00/00 and later).</li> <li>▪ TPC-R or CSM is used (it is not applied in normal operation).</li> </ul> </li> <li>2. When SOM 769 is set to ON, SOM 114, HMO 49 and HMO 50 must not be set to ON.</li> <li>3. In either of the following cases, the path creation operation might fail after automatic port switching is executed. <ul style="list-style-type: none"> <li>▪ SOM 114 is set to ON.</li> <li>▪ HMO 49 and HMO 50 are set to ON.</li> </ul> </li> </ol>		
776	TrueCopy for Mainframe Business Continuity Manager	<p>Allows you to select whether to output the F/M = FB message to the host of primary system when the split or the release operation is performed from Business Continuity Manager to the S-VOL of a TCz pair in Duplex status.</p> <p><b>Mode 776 = ON:</b> When the status of P-VOL changes to Suspend during a TCz S-VOL pair suspend or deletion operation from BCM, the F/M=FB message is not output to the host.</p> <p><b>Mode 776 = OFF (default):</b> When the status of P-VOL changes to Suspend during a TCz S-VOL pair suspend or deletion operation from BCM, the F/M=FB message is output to the host.</p>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. Set this SOM to ON in the environment where TCz is used from BCM and the MCU host does not need the F/M=FB message output during an S-VOL pair suspend or deletion operation from BCM.</li> <li>2. If this SOM is set to ON, the F/M=FB message is not output to the host when the status of P-VOL changes to Suspend during an S-VOL pair suspend or deletion operation from BCM.</li> <li>3. If the PPRC item of CU option is set to NO, the F/M=FB message is not output to the host regardless of setting of this SOM.</li> <li>4. If the function switch#07 is set to "enable", the F/M=FB message is not output to the host regardless of setting of this SOM.</li> </ol>		
784	TrueCopy TrueCopy for Mainframe Global-active device	<p>This SOM can reduce the MIH watch time of RI/O for a TC, TCz, 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, TCz, or GAD. (Not effective by just setting this SOM to ON.)</p> <p>This SOM is applied to TC, TCz, and GAD. This SOM supports Fibre remote copy paths but not iSCSI.</p> <p><b>Mode 784 = ON:</b> 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.</p> <p><b>Mode 784 = OFF (default):</b> The operation is processed in accordance with the TC, TCz, or GAD specification.</p>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied to the environment where Mainframe host MIH time is set to 15 seconds.</li> <li>2. This SOM is applied to the environment where OPEN host time-out time is set to 15 seconds or less.</li> <li>3. This SOM is applied to reduce RI/O MIH time to 5 seconds.</li> <li>4. This function is available for all the TC, TCz, and GAD pairs on the storage system, unable to specify the pairs that are using this function or not.</li> <li>5. To apply this SOM to TCz, MCU and RCU must be USP V/VM or later models and micro-program must be the support version on both sides.</li> <li>6. For a TC, TCz, 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.</li> <li>7. If a failure occurs on the switched path between storage systems, Mainframe host MIH or Open server time-out may occur.</li> <li>8. If an MP to which the path between storage systems belongs is overloaded, switching to an alternate path delays and host MIH or time-out may occur.</li> <li>9. 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.</li> <li>10. 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</li> </ol>		

Mode	Category	Description	Default	MCU/RCU
		<p>or time-out may occur due to a path failure between storage systems.</p> <ol style="list-style-type: none"> <li data-bbox="500 327 1084 394">11. Operation commands are not available for promptly switching to an alternate path.</li> <li data-bbox="500 405 1125 472">12. This SOM works for the pair for which initial pair creation or Resync operation is executed.</li> <li data-bbox="500 483 1133 583">13. Micro-program downgrade to an unsupported version cannot be executed unless all the TC, TCz, and GAD pairs are suspended or deleted.</li> <li data-bbox="500 594 1060 730">14. For operational specifications in each combination of MCU and RCU of TCz/TC, contact customer support (see SOM784 sheet).</li> <li data-bbox="500 741 1068 808">15. For GAD pairs, this SOM is effective if the microcode version supports GAD.</li> <li data-bbox="500 819 1125 1329">16. 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.</li> </ol>		
787	Compatible FlashCopy® V2	<p>This SOM enables the batch prefetch copy.</p> <p><b>Mode 787 = ON:</b> The batch prefetch copy is executed for an FCv2 pair and a Preserve Mirror pair</p> <p><b>Mode 787 = OFF (default):</b> The batch prefetch copy is not executed.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. When this SOM is set to ON, the performance characteristic regarding sequential I/Os to the FCv2 target VOL changes.</li> <li>2. This SOM is applied only when SOM 577 is set to OFF.</li> <li>3. This SOM is applied if response performance for a host I/O issued to the FCv2 target VOL is prioritized.</li> </ol>		
803	Dynamic Provisioning Data Retention Utility	<p>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.</p> <p><b>Mode 803 = ON:</b> 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.</p> <p><b>Mode 803 = OFF (default):</b> 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.</p> <p>For more details, contact customer support (see SOM729 &amp; 803 sheet).</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied when: <ul style="list-style-type: none"> <li>▪ A file system using DP pool VOLs is used.</li> <li>▪ Data Retention Utility is installed.</li> </ul> </li> <li>2. Because the DRU attribute is set to Protect for the V-VOL, a read I/O is also disabled.</li> <li>3. If Data Retention Utility is not installed, the expected effect cannot be achieved.</li> <li>4. The Protect attribute of DRU for the DP V-VOL can be released on the <b>Data Retention</b> window of Device Manager - Storage Navigator after recovering the blocked pool VOL.</li> <li>5. With 80-02-01-00/01 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. <b>Caution:</b> 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.</li> </ol>		
855	ShadowImage ShadowImage for Mainframe Volume Migration	<p>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.</p> <p><b>Mode 855 = ON:</b> 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.</p> <p><b>Mode 855 = OFF (default):</b> The copy processing is stopped when the amount of dirty data is over 60%.</p> <p>For details, contact customer support (see SOM855 sheet).</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>This SOM is applied when all the following conditions are met <ul style="list-style-type: none"> <li>ShadowImage is used with SOM 467 set to ON.</li> <li>Write pending rate of an MP blade that has LDEV ownership of the copy target is high</li> <li>Usage rate of a parity group to which the copy target LDEV belongs is low.</li> <li>ShadowImage copy progress is delayed.</li> </ul> </li> <li>This SOM is available only when SOM 467 is set to ON.</li> <li>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.</li> </ol>		
857	Common	<p>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.</p> <p><b>Mode 857 = ON:</b> The cache allocation capacity is limited to within the prescribed capacity*.</p> <p><b>Mode 857 = OFF (default):</b> The cache allocation capacity is not limited to within the prescribed capacity*.</p> <p>*Prescribed capacity:</p> <ul style="list-style-type: none"> <li>VSP G1000, VSP G1500, VSP F1500: 256 GB</li> </ul> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>The cache hit rate may decrease.</li> <li>The cache allocation capacity per MPB/MPU is limited to within the prescribed capacity.</li> </ol>	OFF	-
867	Dynamic Provisioning Dynamic Tiering	<p>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.</p>	ON	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 867 = ON (default):</b> LDEV format of the DP-VOL is performed with page reclamation.</p> <p><b>Mode 867 = OFF:</b>LDEV format of the DP-VOL is performed with 0 data writing.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied from factory shipment.</li> <li>2. Do not change the setting of this SOM during DP-VOL format.</li> <li>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.</li> </ol>		
872	Universal Volume Manager	<p>When this SOM is applied, the order of data transfer slots is guaranteed at the destaging from the storage system to an external storage system.</p> <p><b>Mode 872 = ON (default*):</b> The order of data transfer slots from the storage system to an external storage is guaranteed.</p> <p><b>Mode 872 = OFF:</b> The order of data transfer slots from the storage system to an external storage is not guaranteed.</p> <p>*The default is OFF for microcode earlier than 80-03-31. In 80-03-31 and later versions, this SOM is set to ON before shipment. If the micro-program is exchanged to a supported version (80-03-31 or later), the setting remains OFF and needs to be set to ON manually.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied when performance improvement at sequential write in UVM configuration is required.</li> <li>2. By setting this SOM to ON, the usage rate of MPs in MPB may become imbalanced, but the processing is balanced in the MPB and the performance per MPB is not affected.</li> </ol>	ON	-
895	TrueCopy for Mainframe	<p>Setting this SOM to ON or OFF, the link type with transfer speed of 8 Gbps/16 Gbps or 4 Gbps is reported respectively.</p> <p><b>Mode 895 = ON (default*):</b> When the FICON<sup>®</sup>/FC link up speed is 8 Gbps/16 Gbps, the link type with transfer speed of 8 Gbps/16 Gbps is reported.</p>	ON	Both



Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 895 = OFF:</b> The link type with transfer speed of up to 4 Gbps is reported , even when the actual transfer speed is 8 Gbps/16 Gbps.</p> <p>* The default value depends on the microcode version as follows:</p> <ul style="list-style-type: none"> <li>▪ 80-05-23 to 80-05-32, 80-06-01 and later: default = ON</li> <li>▪ 80-05-22 and earlier, 80-05-4x, 80-05-61: default = OFF</li> </ul> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. To apply this SOM, the RMF version of mainframe z/OS<sup>®</sup> to be connected must be 1.12 or higher.</li> <li>2. If the OS does not use a supported version, the transfer speed cannot be displayed correctly.</li> <li>3. If all RMF versions of mainframe z/OS connected are 1.12 or higher, set this SOM to ON.</li> <li>4. If any version of mainframe z/OS connected is lower than 1.12, set this SOM to OFF.</li> </ol>		
896	Dynamic Provisioning Dynamic Provisioning for Mainframe Dynamic Tiering Dynamic Tiering for Mainframe Thin Image	<p>This SOM enables or disables the background format function performed on an unformatted area of a DP/DT/TI pool.</p> <p>For information regarding operating conditions, see the <i>Provisioning Guide</i>.</p> <p><b>Mode 896 = ON (default):</b> The background format function is enabled.</p> <p><b>Mode 896 = OFF:</b> The background format function is disabled.</p>	ON	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>3. When a Dynamic Provisioning VOL on an external storage system, which is used as an external VOL, is used as a pool VOL, if the external pool on the external storage side becomes full due to the background format, the external VOL may be blocked.  If the external pool capacity is smaller than the external VOL capacity (Dynamic Provisioning VOL of external storage system), do not enable the background format function.</li> <li>4. If the background format function is disabled by changing this SOM setting, the format progress is initialized and the entire area becomes unformatted.</li> <li>5. The background format for FMC drives is not disabled. When FMC drives are used, use SOM 1093.</li> </ol>		
897	Dynamic Tiering  Dynamic Tiering for Mainframe	<p>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.</p> <p><b>Mode 897 = ON:</b></p> <ul style="list-style-type: none"> <li>▪ SOM 898 is OFF: 110%+0IO</li> <li>▪ SOM 898 is ON: 110%+2IO</li> </ul>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 897 = OFF (default):</b></p> <ul style="list-style-type: none"> <li>▪ SOM 898 is OFF: 110%+5IO (default)</li> <li>▪ SOM 898 is ON: 110%+1IO</li> </ul> <p>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.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. Apply this SOM when the upper tier usage is low and lower tier usage is high.</li> <li>2. This SOM must be used with SOM 898.</li> <li>3. Narrowing the gray zone increases the number of pages to migrate between tiers per relocation.</li> <li>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.</li> </ol> <p>For more details about the interactions between SOMs 897, 898, and 901, contact customer support (see SOM897_898_901 sheet).</p>		
898	Dynamic Tiering Dynamic Tiering for Mainframe	<p>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.</p> <p><b>Mode 898 = ON:</b></p> <ul style="list-style-type: none"> <li>▪ SOM 897 is OFF: 110%+1IO</li> <li>▪ SOM 897 is ON: 110%+2IO</li> </ul> <p><b>Mode 898 = OFF (default):</b></p> <ul style="list-style-type: none"> <li>▪ SOM 897 is OFF: 110%+5IO (default)</li> <li>▪ SOM 897 is ON: 110%+0IO</li> </ul> <p>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.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. Apply this SOM when the usage of upper tier is low and that of lower tier is high.</li> <li>2. This SOM must be used with SOM 897.</li> <li>3. Narrowing the gray zone increases the number of pages to migrate between tiers per relocation.</li> <li>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.</li> </ol> <p>For more details about the interactions between SOMs 897, 898, and 901, contact customer support (see SOM897_898_901 sheet).</p>		
899	Volume Migration	<p>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.</p> <p><b>Mode 899 = ON:</b></p> <ul style="list-style-type: none"> <li>▪ SOM 900 is ON: I/O synchronous copy starts without retrying Volume Migration.</li> <li>▪ SOM 900 is OFF: I/O synchronous copy starts when the threshold of Volume Migration retry is exceeded. (Recommended)</li> </ul> <p><b>Mode 899 = OFF (default):</b></p> <ul style="list-style-type: none"> <li>▪ SOM 900 is ON: I/O synchronous copy starts when the number of retries reaches half of the threshold of Volume Migration retry.</li> <li>▪ SOM 900 is OFF: Volume Migration is retired and I/O synchronous copy is not executed.</li> </ul> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>2. During I/O synchronous copy, host I/O performance degrades.</li> </ol>	OFF	-

Mode	Category	Description	Default	MCU/RCU
900	Volume Migration	<p>In combination with SOM 899 setting, this SOM determines whether to execute and when to start the I/O synchronous copy change as follows.</p> <p><b>Mode 900 = ON:</b></p> <ul style="list-style-type: none"> <li>▪ SOM 899 is ON: I/O synchronous copy starts without retrying Volume Migration.</li> <li>▪ SOM 899 is OFF: I/O synchronous copy starts when the number of retries reaches half of the threshold of Volume Migration retry.</li> </ul> <p><b>Mode 900 = OFF (default):</b></p> <ul style="list-style-type: none"> <li>▪ SOM 899 is ON: I/O synchronous copy starts when the threshold of Volume Migration retry is exceeded. (Recommended)</li> <li>▪ SOM 899 is OFF: Volume Migration is retired and I/O synchronous copy is not executed.</li> </ul> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>2. During I/O synchronous copy, host I/O performance degrades.</li> </ol>	OFF	-
901	Dynamic Tiering Dynamic Tiering for Mainframe	<p>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.</p> <p><b>Mode 901 = ON:</b> 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</p> <p>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.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 901 = OFF (default):</b> 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.</p> <p>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 <i>boundary-value</i> × 110% + 5 [IOPH].</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied when pages with the maximum capacity need to be allocated to tier1 (drive type is SSD) with Dynamic Tiering or Dynamic Tiering for Mainframe.</li> <li>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.</li> <li>3. The following is recommended when applying SOM 901. actual I/O value (total number of I/Os of all tiering policies) &lt; performance potential value of Tier1* × 0.6  * The performance potential value of Tier1 displayed on Monitor information by using Dx-ray.</li> </ol> <p>For more details about the interactions between SOMs 897, 898, and 901, contact customer support (see SOM897_898_901 sheet).</p>		
904	Dynamic Tiering Dynamic Tiering for Mainframe	<p>By setting this SOM to ON or OFF, the number of pages to be migrated per unit time at tier relocation is changed.</p> <p><b>Mode 904 = ON:</b> The number of pages to be migrated at tier relocation is set to up to one page per second.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 904 = OFF (default):</b>No restriction on the number of pages to be migrated at tier relocation (existing specification).</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied when: <ul style="list-style-type: none"> <li>▪ Dynamic Tiering for Mainframe is used (including multi-platform configuration).</li> <li>▪ The requirement for response time is severe.</li> </ul> </li> <li>2. The number of pages to be migrated per unit time at tier relocation decreases.</li> </ol>		
908	Universal Replicator  Universal Replicator for Mainframe	<p>This SOM can change CM capacity allocated to MPBs with different workloads.</p> <p><b>Mode 908 = ON:</b> The difference in CM allocation capacity among MPBs with different workload is large.</p> <p><b>Mode 908 = OFF (default):</b> The difference in CM allocation capacity among MPBs with different workload is small (existing operation) .</p>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. If a CLPR is used by only some MPBs among all the installed MPBs, set this SOM to ON for the CLPR to increase CM capacity allocated to the MPBs that use the CLPR.  Example: (a) A CLPR only for UR JNLG. (b) A configuration where MPBs and CLPRs are separately used for Open and Mainframe systems.</li> <li>2. Since CM capacity allocated to MPBs with low load is small, the performance is affected by a sudden increase in load.</li> <li>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.</li> <li>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.</li> </ol>		
930	Dynamic Provisioning Dynamic Tiering ShadowImage	<p>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.)</p> <p>* Zero data page reclamation by WriteSame and UNMAP functions, and IO synchronous page reclamation are not disabled.</p> <p><b>Mode 930 = ON:</b> All of the zero data page reclamation operations in processing are stopped at once. (Also the zero data reclamation cannot be newly started.)</p> <p><b>Mode 930 = OFF (default):</b> The zero data page reclamation is performed.</p> <p>For details about interactions with SOM 755 and SOM 859, contact customer support (see SOM930 sheet).</p>	OFF	-



Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied when stopping or disabling zero data page reclamation by user request is required.</li> <li>2. When this SOM is set to ON, the zero data page reclamation does not work at all. <ul style="list-style-type: none"> <li>* Zero data page reclamation by Write Same and UNMAP, and IO synchronous page reclamation can work.</li> </ul> </li> <li>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. <ul style="list-style-type: none"> <li>* Because the zero data page reclamation does not work at all while this SOM is set to ON.</li> </ul> </li> <li>4. This SOM is related to SOM 755 and SOM 859.</li> </ol>		
937	Dynamic Provisioning  Dynamic Provisioning for Mainframe  Dynamic Tiering  Dynamic Tiering for Mainframe	By setting this SOM to ON, HDT monitoring data is collected even if the pool is a DP pool.  <b>Mode 937 = ON:</b> HDT monitoring data is collected even if the pool is a DP pool.  Only Manual execution mode and Period mode are supported.  <b>Mode 937 = OFF (default):</b> HDT monitoring data is not collected if the pool is a DP pool	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied when HDT monitoring data collection is required in DP environment.</li> <li>2. When HDT is already used, do not set this SOM to ON.</li> <li>3. For HDT monitoring data collection, shared memory for HDT must be installed. For details, contact customer support (see SOM937 sheet).</li> <li>4. If monitoring data collection is performed without shared memory for HDT installed, an error is reported and the monitoring data collection fails.</li> <li>5. Before removing the shared memory for HDT, set this SOM to OFF and wait for 30 minutes.</li> <li>6. Tier relocation with monitoring data collected when this SOM is set to ON is disabled.</li> <li>7. When DP is converted into HDT (after purchase of software license), the collected monitoring data is discarded.</li> <li>8. Before downgrading the micro-program to an unsupported version, set SOM 937 to OFF and wait for at least 30 minutes.</li> </ol>		
972	Common	<p>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).</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied when a delay in host I/O response due to reclamation processing occurs in a customer environment.</li> <li>2. Reclamation processing is delayed.</li> <li>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.</li> </ol> <p>For details about the interaction between this SOM and SOM 1069, contact customer support (see SOM1069 sheet).</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
973	Common	<p>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).</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied when a delay in host I/O response due to reclamation processing occurs in a customer environment.</li> <li>2. When this SOM is set to ON, reclamation processing is delayed.</li> <li>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.</li> </ol> <p>For details about the interaction between this SOM and SOM 1069, contact customer support (see SOM1069 sheet).</p>	OFF	-
1015	Universal Replicator Universal Replicator for Mainframe	<p>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.</p> <p>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 performed, the setting is not applied.</p> <p><b>Mode 1015 = ON:</b> The pair status changes to COPY/Pending and then to PAIR/Duplex when a delta resync is performed in a 3DC multi-target configuration.</p> <p><b>Mode 1015 = OFF (default):</b> The pair status changes directly to PAIR/Duplex when a delta resync is performed in a 3DC multi-target configuration.</p> <p><b>Notes:</b></p>	OFF	MCU

Mode	Category	Description	Default	MCU/RCU
		<ol style="list-style-type: none"> <li data-bbox="513 254 1117 422">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.</li> <li data-bbox="513 432 1117 562">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.</li> <li data-bbox="513 573 1117 779">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.</li> <li data-bbox="513 789 1117 926">4. Regardless of the remote command device setting, the copy status does not change to COPY/Pending and then the delta resync is completed.</li> <li data-bbox="513 936 1117 1073">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.</li> <li data-bbox="513 1083 1117 1318">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.</li> <li data-bbox="513 1329 1117 1503">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.</li> <li data-bbox="513 1514 1117 1612">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.</li> <li data-bbox="513 1623 1117 1856">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.</li> </ol>		

Mode	Category	Description	Default	MCU/RCU
1017	Universal Replicator for Mainframe	<p>This SOM can be used to advance arbitration processing of an extended consistency group and restore journal data on storage systems at the secondary site even when a Mainframe host continues to issue I/Os with invalid time stamps.</p> <p><b>Mode 1017 = ON:</b> When Mainframe host I/Os with invalid time stamp continue, the time stamp is replaced with the latest time stamp in those of journal data that storage systems at secondary site in a consistency group receive, so that the arbitration processing makes progress and journal data in storage systems at secondary site can be restored.</p> <p><b>Mode 1017= OFF (default):</b> The above function does not work.</p>	OFF	RCU

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. When a Mainframe host issues I/Os with invalid time stamps, SSB=4874 and SSB=CD58 are logged on storage systems at primary and secondary sites respectively. In this case, verify that the LDEV# of the primary volume reported in SSB=4874 and the LDEV# of the secondary volume reported in SSB=CD58 are the primary and secondary volumes of a pair respectively. If the combination of the reported volumes matches the exact pair, apply this SOM to all storage systems at secondary site so as to advance the arbitration processing and to restore journal data on storage systems at secondary site.</li> <li>2. This SOM works only when the timer type of journal option on MCU and RCU is system.</li> <li>3. Set the SOM to ON for all storage systems at secondary site in Universal Replicator for Mainframe MxN configuration (EXCTG).</li> <li>4. To use the SOM, microcode must be the support version and the SOM must be set to ON for all storage systems at the secondary site. To fail over, microcode must be the support version and the SOM must be set to ON for all storage systems at the primary site too.</li> <li>5. The function is applied to time stamps that storage systems at secondary site receive after setting the SOM.</li> <li>6. If a Mainframe host issues I/Os with invalid time stamps, SSB=CD58 is logged on the target storage system at secondary site. If the SOM is set to ON, SSB=CD57 is logged on the target storage system at secondary site.</li> </ol>		
1021	Universal Volume Manager	<p>This SOM can enable or disable the auto-recovery for external volumes of an EMC storage system.</p> <p><b>Mode 0121 = ON:</b> An external volume that is blocked due to Not Ready status can be recovered automatically regardless of the type of external storage system.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 1021 = OFF (default):</b> An external volume that is blocked due to Not Ready status might not be recovered automatically depending on the type of external storage system.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>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.</li> </ol>		
1043	Universal Replicator Universal Replicator for Mainframe	<p>This SOM disables journal copy.</p> <p><b>Mode 1043 = ON:</b> When the following conditions are met at the UR secondary site, the journal copy is disabled.</p> <p>For versions 80-02-05-00/00 and later, the following conditions (1) and (2) or (1) and (3) are met:</p> <ol style="list-style-type: none"> <li>1. 4,096 or more journals are accumulated at the secondary site.</li> <li>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).</li> <li>3. It takes 15 seconds or longer to start restore after journal copy at the RCU.</li> </ol>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p>For versions earlier than 80-02-05-00/00, the following conditions (1) and (2) or (1) and (3) are met:</p> <ol style="list-style-type: none"> <li>1. 4,096 or more journals are accumulated at the secondary site.</li> <li>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).</li> <li>3. The initiator operating rate of the MP blade/unit for which journal ownership at the RCU is defined is 40% or higher.</li> </ol> <p><b>Note:</b> 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.</p> <p><b>Mode 1043 = OFF (default):</b> The journal copy is not disabled.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM applies when one of the following conditions is met: <ol style="list-style-type: none"> <li>a. Multiple journals are registered in a consistency group of CCI.</li> <li>b. Multiple journals are registered in an extended consistency group.</li> </ol> </li> </ol>		



Mode	Category	Description	Default	MCU/RCU
		<p>c. Journals are accumulated at the secondary site, causing the system performance to decrease.</p> <ol style="list-style-type: none"> <li>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.</li> <li>3. When the host write speed is faster than the JNL copy speed, the usage rate of the master journal increases.</li> <li>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.</li> </ol> <p>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.</p> <ol style="list-style-type: none"> <li>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.)</li> </ol>		
1050	Global-active device TrueCopy TrueCopy for Mainframe Universal Replicator Universal Replicator for Mainframe	<p>This SOM enables creation of pairs using user capacity in excess of 1.8 PB per system by managing differential BMP in hierarchical memory for pair volumes whose capacity is 4 TB (open) or 262,668 cyl (mainframe) or less.</p> <p><b>Mode 1050 = ON:</b> For pair volumes of 4 TB (open)/262,668 cyl (mainframe) or less, differential BMP is managed in hierarchical memory that performs caching to CM/PM using HDD as a master and enables creation of pairs using user capacity in excess of 1.8 PB per system.</p> <p>For microcode 80-02-4x and later, you should use hierarchical memory for all remote copy pairs. Using SOMs 1050 and 1058 enables the use of hierarchical memory for volumes of 4 TB or less, which increases the total amount of replicated capacity above 1.8 PB.</p>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p><b>WARNING:</b> If you allocate more than 1.8 PB of replicated capacity for volumes of 4 TB or less and then later want to return to using shared memory, you will have to delete some pairs to reduce the total replicated capacity for volumes of 4 TB or less to below 1.8 PB.</p> <p><b>Mode 1050= OFF (default):</b> For pair volumes of 4 TB (open)/262,668 cyl (mainframe) or less, differential BMP is managed in SM as usual so that the user capacity to create pairs is limited to 1.8 PB per system. Also, differential MPB management can be switched from the hierarchical memory to SM by performing a resync operation for pairs whose volume capacity is 4 TB (open)/ 262,668 cyl (mainframe) or less.</p>		

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is related to SOM 1058.</li> <li>2. The hierarchical memory is used for volumes over 4 TB (open)/262,668 cyl (mainframe) even when this SOM is set to OFF.</li> <li>3. When this SOM is turned OFF after operating with this SOM set to ON, if resynchronizing pairs whose volume capacity is 4 TB (open)/262,668 cyl (mainframe) or less managed in the hierarchical memory, the pair resync operation might fail due to lack of the SM capacity.</li> <li>4. If a pair resync operation fails, the pairs exceeding 1.8 PB of user capacity need to be deleted.</li> <li>5. Open non-DP-VOLs do not support hierarchical memory differential management so that this SOM cannot be applied.</li> <li>6. To downgrade the microcode, the procedure described in Maintenance Manual (Function ID 01:03 described in 03 MICRO-FC) is required. Refer to the manual before applying this SOM.</li> <li>7. Apply this SOM when you want to create pairs using user capacity exceeding 1.8 PB per system.</li> <li>8. Depending on the I/O pattern, I/O response might be affected.</li> <li>9. Depending on the condition, initial copy time might be affected.</li> <li>10. The differential BMP managed in hierarchical memory does not use the shared memory, but the differential data is managed in a pool with which the volumes are associated. For the pool capacity necessary for the differential data management, refer to the "Differential data" section in the user guide.</li> <li>11. Before using this SOM to increase pair volumes on the storage system, check the resources on the storage system to make sure all performance requirements are met.</li> </ol>		

Mode	Category	Description	Default	MCU/RCU
1058	Global-active device TrueCopy TrueCopy for Mainframe Universal Replicator Universal Replicator for Mainframe	<p>This SOM can change differential BMP management from SM to hierarchical memory so that the number of pairs to be created on a system and user capacity used for pairs increase.</p> <ul style="list-style-type: none"> <li>▪ For mainframe systems, all pairs can be managed in hierarchical memory so that pairs can be created by all LDEVs.</li> <li>▪ For open systems, pairs that can only be managed in SM use SM so that the number of pairs that can be created using non-DP-VOLs increases.</li> </ul> <p><b>Mode 1058 = ON:</b></p> <p>When SOM 1050 is ON:</p> <ul style="list-style-type: none"> <li>▪ By resynchronizing mainframe VOLs of 262,668 cyl or less, the differential BMP management is switched from SM to hierarchical memory. Hierarchical memory management remains as is.</li> <li>▪ By resynchronizing open VOLs (DP-VOLs only) of 4 TB or less, the differential BMP management is switched from SM to hierarchical memory. Hierarchical memory management remains as is.</li> </ul> <p>When SOM 1050 is OFF:</p> <ul style="list-style-type: none"> <li>▪ By resynchronizing mainframe VOLs of 262,668 cyl or less, the differential BMP management is switched from hierarchical memory to SM. SM management remains as is.</li> <li>▪ By resynchronizing open VOLs (DP-VOLs only) of 4 TB or less, the differential BMP management is switched from hierarchical memory to SM. SM management remains as is.</li> </ul> <p><b>Mode 1058 = OFF (default):</b></p> <p>When SOM 1050 is ON: The differential BMP management does not change by resynchronizing pairs.</p>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p>When SOM 1050 is OFF:</p> <ul style="list-style-type: none"> <li>▪ By resynchronizing mainframe VOLs of 262,668 cyl or less, the differential BMP management is switched from hierarchical memory to SM. SM management remains as is.</li> <li>▪ By resynchronizing open VOLs (DP-VOLs only) of 4 TB or less, the differential BMP management is switched from hierarchical memory to SM. SM management remains as is.</li> </ul> <p>For microcode 80-02-4x and later, you should use hierarchical memory for all remote copy pairs. Using SOMs 1050 and 1058 enables the use of hierarchical memory for volumes of 4 TB or less, which increases the total amount of replicated capacity above 1.8 PB.</p> <p><b>WARNING:</b> If you allocate more than 1.8 PB of replicated capacity for volumes of 4 TB or less and then later want to return to using shared memory, you will have to delete some pairs to reduce the total replicated capacity for volumes of 4 TB or less to below 1.8 PB.</p>		

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. Depending on the I/O pattern, I/O response might be affected.</li> <li>2. Depending on the condition, initial copy time might be affected.</li> <li>3. This SOM is related to SOM 1050.</li> <li>4. Open non-DP-VOLs do not support hierarchical memory differential management so that this SOM cannot be applied.</li> <li>5. To downgrade the microcode, the procedure described in Maintenance Manual Function ID 01:03 described in 03 MICRO-FC. is required. Refer to the manual before applying this SOM.</li> <li>6. This SOM is applied when increasing the number of pairs that can be created on a system or the user capacity for pairs is desired.</li> <li>7. The differential BMP managed in hierarchical memory does not use the shared memory, but the differential data is managed in a pool with which the volumes are associated. For the pool capacity necessary for the differential data management, refer to "Differential data" in the manuals for TC, UR, and GAD. Before using this SOM to increase pair volumes on the storage system, reexamine the resource on the storage system to make sure all performance requirements are met.</li> <li>8. Before using this SOM to increase pair volumes on the storage system, re-examine the resource on the storage system to make sure all performance requirements are met.</li> </ol>		
1061	Compatible FlashCopy® V2 Compatible FlashCopy® SE	<p>This SOM is used to enable the copy after write (CAW) function of FlashCopy®.</p> <p>By setting this SOM to ON, CAW (While copy processing is withheld, command response is returned first and then the copy is done in asynchronous manner) can work so as to improve random write response performance. (In the case of sequential write, as an improvement to copy data in advance has been implemented, the equal performance can be achieved without CAW.)</p> <p><b>Mode 1061 = ON:</b> The CAW function works.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 1061 = OFF (default):</b> The CAW function does not work. (COW works.)</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied when the CAW function is enabled.</li> <li>2. The cache write pending rate may increase.</li> </ol>		
1067	Universal Replicator Universal Replicator for Mainframe	<p>This SOM is used to enable microcode downgrade to a version that does not support URxUR (including delta).</p> <p><b>Mode 1067 = ON:</b> Even when a UR pair has been registered, downgrading the microcode to a version that does not support URxUR (including delta) is allowed.</p> <p><b>Mode 1067 = OFF (default):</b> If any UR pair has been registered, downgrading the microcode to a version that does not support URxUR (including delta) is not allowed.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>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).</li> <li>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.</li> </ol>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p>Phenomena:</p> <ul style="list-style-type: none"> <li>a. 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.</li> <li>b. When the pair between I site and R site in cascade configuration is resynchronized, the pair status cannot change from COPY to PAIR.</li> <li>c. When the microcode is downgraded at R site in cascade configuration, the pair between I site and R site cannot be resynchronized.</li> </ul>		
1068	Common	<p>This mode can detect and report a minor drive response delay early by severely checking drives.</p> <p><b>Mode 1068 = ON:</b> Drive response delay is checked and detected with conditions that are more severe than current conditions.</p> <p>When SOM 144 is set to ON, the drive with response delay is blocked.</p> <p>Target drive: HDD, FMD, SSD</p> <p><b>Mode 1068 = OFF:</b> Drive response delay is checked and detected with current conditions.</p> <p>The behavior varies depending on the combinations of SOM settings. For details, contact customer support (see SOM144 sheet).</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. Apply this mode to detect a minor delay in drive response.</li> <li>2. When a delay is suspected, a processing to refer to the statistics data and determine the delay works.</li> <li>3. If SOM 157 is set to ON, the output prevention status of SSB=A4CE is not cleared in one-day cycle.</li> <li>4. When applying this mode only, a SIM for delay detection is reported but the HDD is not blocked. To block the HDD, SOM 144 also needs to be applied.</li> </ol>	OFF	-



Mode	Category	Description	Default	MCU/RCU
1069	Common	<p>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).</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>2. When this SOM is set to ON, reclamation processing is delayed.</li> <li>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.</li> </ol>	OFF	-
1070	Global-active device	<p>This SOM changes the processing for a group operation with GAD consistency group (CTG).</p> <p><b>Mode 1070 = ON:</b> The status change of all pairs in a consistency group. is performed for 50 msec.</p> <p><b>Mode 1070 = OFF (default):</b> The status change of all pairs in a consistency group is performed for 1 msec.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>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).</li> </ol>	OFF	Both
1079	Dynamic Provisioning Dynamic Tiering	<p>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.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 1079 = ON:</b> The Proprietary ANCHOR command is unavailable.</p> <p><b>Mode 1079 = OFF (default):</b> The Proprietary ANCHOR command is available.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>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: <ol style="list-style-type: none"> <li>a. SOM 1079 setting ON/HMO 97 setting ON --&gt; Proprietary ANCHOR command Unavailable</li> <li>b. SOM 1079 setting ON/HMO 97 setting OFF --&gt; Proprietary ANCHOR command Unavailable</li> <li>c. SOM 1079 setting OFF/HMO 97 setting ON --&gt; Proprietary ANCHOR command Available</li> <li>d. SOM 1079 setting OFF/HMO 97 setting OFF --&gt; Proprietary ANCHOR command Unavailable</li> </ol> </li> </ol>		
1080	Global-active device Universal Volume Manager	<p>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.</p> <p><b>Mode 1080 = ON:</b> 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.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>If a response to ABTS is delayed for 12 seconds or longer, the quorum disk may be blocked.</p> <p><b>Mode 1080 = OFF (default):</b> 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.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>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.</li> </ol> <p>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.</p> <ol style="list-style-type: none"> <li>2. When connection performance degradation occurs, the quorum disk blockage is more likely to occur.</li> </ol>		
1083	Dynamic Provisioning Universal Volume Manager	<p>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.</p> <p><b>Mode 1083 = ON:</b> DP-VOL deletion is enabled.</p> <p><b>Mode 1083 = OFF (default):</b> DP-VOL deletion is disabled.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>This SOM is applied when the following conditions are met. <ul style="list-style-type: none"> <li>A DP-VOL with data direct mapping attribute is deleted.</li> <li>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.</li> </ul> </li> <li>When SOM 1083 is set to ON, the data of external volumes cannot be guaranteed.</li> <li>When DP-VOL deletion is performed without disconnecting an external volume, the data of the external volume cannot be guaranteed.</li> </ol>		
1086	Dynamic Provisioning Dynamic Provisioning for Mainframe Universal Volume Manager	<p>This SOM enables or disables the performance improvement for Dynamic Provisioning volumes that are Universal Volume Manager volumes used as pool volumes.</p> <p><b>Mode 1086 = ON (default):</b> The performance improvement is enabled.</p> <p><b>Mode 1086 = OFF:</b> The performance improvement is disabled.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>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.)</li> </ol>	ON	-
1091	Compatible FlashCopy® V2	<p>This SOM enables or disables the IBM® zHyperWrite function. When this SOM setting is changed to ON or OFF, SCI is reported to the host and the zHyperWrite function is enabled or disabled.</p>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
	TrueCopy for Mainframe Universal Replicator for Mainframe	<p><b>Mode 1091 = ON:</b> The zHyperWrite function is enabled. (ReadFeatureCode setting for the zHyperWrite function)</p> <p><b>Mode 1091 = OFF (default):</b> The zHyperWrite function is disabled.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM can be applied when DKCMAIN version 80-04-21-00/00 or higher that supports the zHyperWrite function is used.</li> <li>2. To use the zHyperWrite function, a HyperSwap environment is required.</li> <li>3. To enable the zHyperWrite function, set this SOM to ON on both MCU and RCU.</li> <li>4. To downgrade the microcode to a version that does not support the zHyperWrite function, set this SOM to OFF prior to downgrading the microcode.</li> <li>5. Even when this SOM is set to ON for a storage system in 3DC configuration, the zHyperWrite function does not work for volumes in 3DC configuration.</li> <li>6. Do not set this SOM to ON if SOM 474 is set to ON.</li> <li>7. Do not set this SOM to ON if Preserve Mirror configuration is created.</li> <li>8. Do not set this SOM to ON if the TCz Function Switch 12 is set to ON.</li> <li>9. To use the zHyperWrite function, make sure that the CFW Data setting for the PPRC/TCz pairs is set to Secondary Volume Copy so that CFW data is copied to the S-VOL. If CFW Data is set to Primary Volume Only, zHyperWrite will not function.</li> </ol>		
1093	Dynamic Provisioning Dynamic Tiering Thin Image	<p>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.</p> <p><b>Mode 1093 = ON:</b> Background unmap cannot work.</p> <p><b>Mode 1093 = OFF (default):</b> Background unmap can work.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<b>Note:</b> 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.		
1096	Universal Replicator  Universal Replicator for Mainframe	<p>This SOM disables read-journal frequency reduction.</p> <p><b>Mode 1096 = ON:</b> The read-journal frequency reduction does not work.</p> <p><b>Mode 1096 = OFF (default):</b> The read-journal frequency reduction works.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. This SOM is applied when a significant delay, which is about 200 msec or longer, occurs in the line between MCU and RCU.</li> <li>2. When this SOM is set to ON while round-trip delay time is small (about less than 20 msec), the usage rate of RCU Initiator increases by 10% x the number of journals.</li> <li>3. Even though this SOM is supposed to be applied to UR RCU, apply it to both MCU and RCU on the premise of DR operation.</li> <li>4. This SOM is effective for each CLPR, so that select the operation target LPRxx (xx=00 to 31), and then set this SOM to ON/OFF. For example, when only CLPR0 is defined (CLPR1 to 31 are not defined), select LPR00 and then set this SOM to ON/OFF. This SOM is not effective for any CLPRs if "System" is selected even when this SOM is set to ON.</li> </ol>	OFF	Both
1099	TrueCopy for Mainframe	When PPRC FREEZE using GDPS works, the FREEZE might time out if the storage system has more than 32 CUs. This SOM changes the FREEZE behavior to prevent time-out for a storage system with more than 32 CUs.	OFF	MCU

Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 1099 = ON:</b> When FREEZE is received, the completion of path deletion for those other than the last path is not reported but only the completion of path deletion for the last path is reported. If multiple CUs share an RCU path, path deletion does not work at FREEZE per CU, so that the following phenomenon may occur:</p> <ul style="list-style-type: none"> <li>▪ After Hyperswap is performed, SSB=8BD8 and 8BD9 are logged for a pair where the Hyperswap is performed.</li> </ul> <p><b>Mode 1099 = OFF (default):</b> The completion of path deletion for every path is reported.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. Apply this mode when a storage system with over 32 CUs is used in a TCz environment in which PPRC FREEZE is available.</li> <li>2. The mode is effective for the entire storage system.</li> <li>3. To set this mode to ON, the microcode must be 80-04-24-00/00 or later on both the MCU and the RCU.</li> <li>4. FREEZE using Sync CTG is performed without path deletion, so it is not subject to this change in FREEZE behavior.</li> </ol>		
1106	Dynamic Provisioning Dynamic Provisioning for Mainframe Dynamic Tiering Dynamic Tiering for Mainframe	<p>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.</p> <p><b>Mode 1106 = ON:</b> The usage rate is checked once a day and the rebalance works if the rate is not even.</p> <p><b>Mode 1106 = OFF (default):</b> The rebalance does not work even when the usage rate is not balanced.</p> <p>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.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Note:</b> 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.</p> <p>Examples:</p> <ol style="list-style-type: none"> <li>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. <p>Because the average parity group usage rate is <math>(50\% + 40\% + 30\%) / 3 = 40\%</math> and the difference in the rate between each parity group and the average is 10% at the maximum.</p> </li> <li>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. <p>Because the average parity group usage rate is <math>(80\% + 40\% + 30\%) / 3 = 50\%</math> and the difference in the rate between each parity group and the average is 30% at the maximum.</p> </li> <li>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: <ul style="list-style-type: none"> <li>▪ The average parity group usage rate of Tier1 is <math>(80\%) / 1 = 80\%</math> and the difference in the rate between the parity group and the average is 0%.</li> <li>▪ The average parity group usage rate of Tier2 is <math>(40\% + 30\%) / 2 = 35\%</math> and the difference in the rate between the parity group and the average is 5% at the maximum.</li> </ul> </li> </ol> <p><b>Note:</b> This SOM is applied when balancing the usage rate is required at a customer site where the usage rate is not even.</p>		



Mode	Category	Description	Default	MCU/RCU
1113	Deduplication and Compression	<p>If a problem occurs while the capacity saving function is enabled and the MP usage rate needs to be reduced to identify the failure, use this mode to stop asynchronous processing of host I/Os by the capacity saving function other than garbage collection and de-staging.</p> <p><b>Mode 1113 = ON:</b> The asynchronous processing of host I/Os by the capacity saving function, other than garbage collection and de-staging, is stopped.</p> <p><b>Note:</b> While the capacity reduction processing is not working, the capacity saving rate might degrade.</p> <p><b>Mode 1113 = OFF (default):</b> The capacity saving function fully works.</p> <p><b>Relationship between SOM 1113 and SOM 1112:</b> When both modes are set to ON, the setting of SOM 1112 is prioritized over that of SOM 1113. When SOM 1112 is set to ON, all asynchronous processing for host I/Os among those related to the capacity saving function are stopped, including garbage collection and de-staging, so that write I/Os to V-VOLs with Compression or Deduplication and Compression set are disabled.</p>	OFF	-
1115	Deduplication and Compression	<p>When this SOM is set to ON, data is initialized without using metadata at LDEV format for a virtual volume with capacity saving enabled.</p> <p><b>Caution:</b> Use SOM 1115 only when performing recovery procedures. This SOM is used only when performing recovery procedures described in the Maintenance Manual.</p> <p><b>Mode 1115 = ON:</b> When LDEV format is performed for a virtual volume whose capacity saving setting is Compression, the data is initialized without using the metadata.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 1115 = OFF (default):</b> 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.</p> <ul style="list-style-type: none"> <li>▪ There is a pinned slot.</li> <li>▪ The capacity saving status is "Failed".</li> <li>▪ The virtual volume is blocked (Normal restore cannot be performed).</li> </ul> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. Apply this SOM only when performing recovery procedures. For details about when to turn SOM 1115 on and off, see the instructions in the Maintenance Manual.</li> <li>2. The processing time increases with increase in pool capacity.  Estimate of processing time:  Processing time (minutes) = ceiling(pool capacity (TB)/40) + 5  ceiling: The value enclosed in ceiling( ) must be rounded up to the nearest whole number.  The processing finishes early if there is less capacity of allocated pages.</li> <li>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.</li> <li>4. This SOM is effective only for LDEV format for a virtual volume whose capacity saving setting is 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, do not use this SOM for cases other than pool volume blockage recovery.</li> </ol>		
1118	Open	This SOM is used to disable the ENC reuse function.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Mode 1118 = ON:</b> 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.</p> <p><b>Mode 1118 = OFF (default):</b> When a failure occurs in the Expander chip mounted on a controller board (CTLS, CTLSE) or an ENC board, the reuse function works.</p> <p>If the ENC is reusable, SIM=CF12XX and then CF14XX are reported, and the ENC is reused.</p> <p>If the ENC is not reusable, SIM=CF12XX is reported, and the ENC is blocked.</p> <p><b>Note:</b> The ENC reuse function is enabled as default. This SOM is applied when you want to disable the ENC reuse function.</p>		
1119	Deduplication and Compression	<p>This SOM is used to downgrade the microcode as follows while capacity saving is enabled: from 80-05-05-00/00 or later to 80-05-01-00/00 or later.</p> <p>New control information is added with 80-05-05 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 80-05-01 or later. This SOM disables the control information added with 80-05-05 when capacity saving is enabled to enable microcode downgrade.</p> <p><b>Mode 1119 = ON:</b> The control information is not used when capacity saving is enabled.</p> <p><b>Mode 1119 = OFF (default):</b> The control information is used when capacity saving is enabled.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>2. After the microcode downgrade is complete, make sure to set this SOM to OFF.</li> <li>3. This SOM is effective for the entire storage system.</li> <li>4. The write performance might degrade when this SOM is ON.</li> </ol>		
1120	Dynamic Provisioning Thin Image	<p>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.</p> <p><b>Mode 1120 = ON:</b> 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.</p> <p><b>Mode 1120 = OFF (default):</b> No action.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. Set this SOM to ON when the microcode downgrade described above is performed while there is a DP pool in the storage system.</li> <li>2. Set this SOM to ON only when downgrading the microcode.</li> <li>3. Before setting this SOM to ON, delete all TI pairs in DP pools.</li> <li>4. After the microcode downgrade is complete, make sure to set this SOM to OFF.</li> </ol>	OFF	-
1147	Universal Replicator for Mainframe	<p>This mode is used to prevent the performance of write I/O to a URz P-VOL from degrading when the path condition is unstable or the RCU site is overloaded in a configuration where high-speed drives (HAF/SSD) are used for journal volumes.</p> <p>Apply this mode when:</p> <ul style="list-style-type: none"> <li>▪ Drives constituting a URz journal volume are HAF/SSD(*), and</li> <li>▪ Host I/Os are prioritized and accumulating journal is required (suspending is acceptable).</li> </ul>	OFF	MCU

Mode	Category	Description	Default	MCU/RCU
		<p>* If the drives constituting the URz journal volume are HDDs, the mode can be applied when the staging performance outweighs the amount of read journal transfer.</p> <p><b>Mode 1147 = ON</b> The caching rate of journal data created at a write I/O to a URz P-VOL is limited to 50% (equal to Open environment). (The URz pair might be suspended as journal data tends to accumulate compared to the OFF setting.)</p> <p><b>Mode 1147 = OFF (default)</b> The caching rate of journal data created at a write I/O to a URz P-VOL is limited to 70% (same as usual). (Compared to the ON setting, the performance of host write I/Os tends to be affected when CWP reaches 70%.)</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. Do not set this mode to ON if HDDs whose staging performance is lower than the amount of read journal transfer are used for the journal volume.</li> <li>2. This mode is effective for CLPR. To set the mode, select an operation target LPRxx (xx=00 to 31), and then set the mode to ON or OFF.</li> </ol> <p>When defining CLPR0 only (for example, when CLPR 1 to 31 are not defined), select LPR00 and then set the mode to ON or OFF. If System is selected and then the mode is set to ON, the mode is not effective for any CLPRs.</p>		

---

# Index

## A

- accelerated compression 137
- account 127
- account lock policy 127
- Add Request Authentication Setting window
  - SNMP v1 or SNMP v2c 347
  - SNMP v3 349
- Add Sending Trap Setting window
  - SNMP v1 or v2c 341
  - SNMP v3 342
- adding SVP to trusted zone 25
- administration guide 67, 68, 93, 128, 156, 177, 179, 411
- advanced system settings 88
- Advanced System Settings wizard 363
- alert properties 391
- alert settings window 331
- alerts 389, 391
- alerts function 226
- alerts window 389
- audience 14
- authentication server 70
- Authentication server 70
- Authorization server 70
- Authorization servers
  - requirements 72

## B

- backing up Stor. Nav. settings 90
- backup 92
- Blocking HTTP communications 83
- built-in groups 108
- built-in user 39

## C

- Cache Memories report 177
- capacity, calculating 136
- capacity, estimating for license 131
- certificate 80, 81, 93

- certificated 93
- certificates
  - obtaining 78
- certificates, obtaining 78
- Change Request Authentication Setting window
  - SNMP v3 353
  - v1 or v2c 351
- Change Sending Trap Setting window
  - SNMP v1 or v2c 344
  - SNMP v3 346
- changing a user's password 117
- Changing assigned resource groups 113
- changing permissions 118
- Channel Adapters report 178
- clearing
  - cache 238
- client computer
  - Windows requirements 20
- configuration files 92, 93, 98, 407
- creating
  - resource groups 124
  - user accounts 114
- Creating a keypair 75
- creating a report 154
- creating a user account 111
- csv 179, 219

## D

- data acquisition settings 88
- deleting a report 155
- deleting a user account 119
- Device Manager- Storage Navigator
  - client setup for 24
- disable 118
- Disable Licenses window 321
- display errors 233
- display settings 88
- DkuTempAveInfo.csv 186
- DkuTempInfo.csv 184
- DkuTempMaxInfo.csv 187
- DkuTempMinInfo.csv 188

downloading trace files,FD Dump Tool 240

## E

edit settings 331

Edit Storage System wizard 329

editing 363

emergency key 128

enable 319

environmental parameters 26

environmental settings 68

errors

clearing 238

login 227

UNIX 236

external volume 128

external volume, calculating capacity 137

## F

FD Dump Tool

downloading trace files 240

Firefox

clearing cache 238

Firefox problems on UNIX, troubleshooting 239

firewall configuration 69

## G

graphical view 177

## H

Hitachi Virtual Storage Platform F1500 67, 68, 93, 128, 156, 177, 179

Hitachi Virtual Storage Platform G1000 67, 68, 93, 128, 156, 177, 179

Hitachi Virtual Storage Platform G1500 67, 68, 93, 128, 156, 177, 179

Hitachi Virtual Storage Platform G1x00 67, 68, 93, 128, 156, 177, 179

Hosts report 160

## I

Internet Explorer

clearing cache 238

IPv6, configuring communications 23

## J

java 31, 53

Java

Java (*continued*)

clearing cache 238

JavaScript for Windows

enabling 239

JRE

configuring 33

## K

key 128

## L

LDEV 137

licence status 325

license 128, 318, 321, 323

license capacities

unlicensed software 141

license capacity

software 131

license key

estimating capacity 131

License key status disabled 138

license keys

expiration 142

permanent 129

term 130

types 128

viewing information 140

License keys

disabling 139

emergency 130

temporary 130

licenses window 319

logging in 39, 40

Logical Devices report 160

login errors 227

login message 67

LUN ID 38

LUNs report 163

## M

main window 42, 43

management client

setup 24

managing 102

menu bar 42

MP Blade Details report 164

MP Blades report 164

## N

no response 229  
normal volume 128

## O

obtain certificate 78

## P

parity group 137  
Parity Groups report 165, 173  
password  
    allowable characters and symbols 114  
    changing a user's 117  
permanent key 128  
permissions, changing 118  
Physical View report 178  
PKCS#12 format 77  
pool capacity  
    calculating 137  
port locations 146  
Ports report 168  
Power Consumption report 170  
PpInfo.csv 219  
precautions 105  
preface 14  
primary SVP 100  
private key 78  
product version 14  
public key 78

## R

registration 104  
release lock 127  
Release Lockout window 265  
removing a software application 139  
report 179  
**Report Viewer** window 155  
reports  
    Cache Memories 177  
    Channel Adapters 178  
    CHAP Users 156  
    Disk Adapters 157  
    downloading 154  
    Host Groups 158  
    Hosts 160  
    iSCSI Targets 158  
    Logical Devices 160  
    LUNs 163

reports (*continued*)

    MP Blade Details 164  
    MP Blades 164  
    Parity Groups 165, 173  
    Physical View 178  
    Ports 168  
    power consumption 170  
    Spare Drives 172  
    Storage System Summary 174  
    using 154  
requirements  
    management clients 20  
resource group 121  
resource groups  
    adding resources to 125  
    assignments 124  
    creating 124  
    deleting 126  
    deleting resources from 125  
    editing 125  
    example not sharing a port 122  
    example sharing a port 121  
    renaming 125  
    rules, restrictions, and guidelines 124  
Resource groups  
    changing 113  
revisions 15  
roles 104, 108  
Roles 105

## S

secondary window 31, 50  
secondary windows 54  
security 68, 83  
security settings 31  
self-signed certificate 78  
Servers  
    authentication 70  
    authorization 70  
session timeout 65  
setting up management client 24  
settings 26  
setup workflow 19  
signed certificates 78, 93  
Signed certificates 78  
signed private key 78  
signed public key 78  
SIM 389, 391  
SIMs  
    checking 226



- smi-s 93
- SMIs 93, 98, 242
- SMIS 95
- software installation 137
- SOMs 411
- Spare Drives report 172
- SsdDriveInfo.csv 222
- SSdDriveInfo.csv 221
- SSL 74, 93
- SSL certificate passphrase 79
- SSL certificates
  - converting 77
- SSL communication settings 74
- SSL-encrypted communications
  - blocking HTTP communications 83
  - creating a private keypair 76
  - creating a public key 76
  - overview 73
- stalled tasks 153
- status refresh interval 153
- status, port 145
- storage navigator 39, 43, 102
- Storage Navigator
  - backing up settings 90
  - browser restrictions 34
  - creating a user account 111
  - reports 154
  - saving changes 37
  - setting time periods 27
  - setup 19
  - unsupported actions on Windows 36
- storage system
  - applying changes to 37
- storage system information 68
- Storage System Summary report 174
- storage system, viewing 144
- Storage Systems window 370
- SVP
  - host name 100
- SVP, adding to trusted sites 25
- System configuration 68
- system information 68
- system option modes 411
- system settings 364

## T

- table view 156
- tasks
  - about 149
  - managing 150

- Tasks windows 378
- temporary key 128
- term key 128
- TLSv1.0 83
- TLSv1.1 83
- TLSv1.2 83
- troubleshooting 54, 225, 242

## U

- UNIX
  - errors 236
- UNIX requirements 22
- user accounts
  - creating 111, 114
  - deleting 119
  - managing 114
- user administration
  - overview 102
- user group 244
- User group 243
- User group window 244
- user groups
  - deleting 113
  - names 112
  - roles 105, 108, 110
- User groups
  - permissions 112

## V

- viewing a report 154
- Virtual Storage Platform F350 411
- Virtual Storage Platform F370 411
- Virtual Storage Platform F700 411
- Virtual Storage Platform F900 411
- Virtual Storage Platform G350 411
- Virtual Storage Platform G370 411
- Virtual Storage Platform G700 411
- Virtual Storage Platform G900 411
- VSP F1500 67, 68, 93, 128, 156, 177, 179
- VSP F350 411
- VSP F370 411
- VSP F700 411
- VSP F900 411
- VSP Fx00 models 411
- VSP G1000 67, 68, 93, 128, 156, 177, 179
- VSP G1500 67, 68, 93, 128, 156, 177, 179
- VSP G1x00 67, 68, 93, 128, 156, 177, 179
- VSP G350 411
- VSP G370 411
- VSP G700 411

VSP G900 [411](#)  
VSP Gx00 models [411](#)

## **W**

Web browser  
    [configuring 25](#)  
    [restrictions 34](#)  
Windows requirements [20](#)  
Windows server  
    [configuration 24](#)

