

Hitachi Virtual Storage Platform 5000 Series

SVOS RF 9.6.1

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.

© 2019, 2021 Hitachi, Ltd. All rights reserved.

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

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

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

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

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

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

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

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

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

Active Directory, ActiveX, Bing, 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.

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

Contents

Preface	15
Intended audience.....	15
Product version.....	15
Release notes.....	15
Changes in this revision.....	16
Document conventions.....	16
Conventions for storage capacity values.....	17
Accessing product documentation.....	18
Getting help.....	19
Comments.....	19
Chapter 1: Initial setup of the management client	20
Workflow for setting up the management client.....	20
Requirements for management clients.....	20
General requirements.....	21
Requirements for Windows-based management clients.....	21
Requirements for UNIX/Linux-based management clients.....	23
Configuring the network settings on the management client.....	25
Setting up TCP/IP for a firewall.....	25
Setting up IPv4/IPv6 communications.....	26
Configuring IPv6 communication in Windows 7.....	27
Configuring IPv6 communication in Solaris 10.....	27
Registering the SVP host name.....	27
Adding your SVP to the trusted sites zone for Windows Server computers.....	28
Configuring the web browser on the management client.....	29
Enabling JavaScript for Windows.....	30
Installing Storage Device Launcher on the management client.....	31
Configuring the management client for the HDvM - SN secondary window.....	32
Installing and configuring JRE.....	33
Path setting (UNIX).....	33
Configuring JRE.....	34
Using Web Console Launcher to enable the secondary window (Java 11 or later).....	34
Verifying the SVP server certificate.....	35

Registering a certificate on the HDvM - SN management client (Windows).....	36
Viewing a certificate on the HDvM - SN management client (Windows).....	37
Deleting a certificate on the HDvM - SN management client (Windows).....	37
Setting server verification on the HDvM - SN management client (Windows).....	38
Viewing whether server verification is enabled on the HDvM - SN management client (Windows).....	38
Viewing the Help on the HDvM - SN management client (Windows).....	39
Registering a certificate on the HDvM - SN management client (UNIX).....	39
Viewing a certificate on the HDvM - SN management client (UNIX).....	40
Deleting a certificate on the HDvM - SN management client (UNIX).....	41
Setting server verification on the HDvM - SN management client (UNIX).....	41
Viewing whether server verification is enabled on the HDvM - SN management client (UNIX).....	42
Viewing the Help on the HDvM - SN management client (UNIX).....	42
Device Manager - Storage Navigator restrictions.....	43
General restrictions.....	43
Web browser restrictions while using Device Manager - Storage Navigator.....	43
Unsupported actions in Windows version of HDvM - SN.....	45
Unsupported actions in UNIX version of HDvM - SN.....	45
Applying changes made in Device Manager - Storage Navigator.....	46
Updating data after a Volume Migration or Quick Restore operation.....	46
Updating data after operations performed with another application.....	46
Capacities displayed on the Device Manager - Storage Navigator screen..	46
Caution on LUN ID notation.....	47
Chapter 2: Using the Device Manager - Storage Navigator GUI.....	48
Logging in to HDvM - SN in a browser.....	48
Initial superuser login.....	48
User login.....	50
Logging in to HDvM - SN by using AIR.....	50
Changing your initial HDvM - SN password.....	52
Disabling and enabling use of Flash Player with HDvM - SN.....	53
Navigating the Device Manager - Storage Navigator user interface.....	53
Menu bar.....	54
Using the Device Manager - Storage Navigator main window.....	55
Main window controls.....	56

Main window and Modify mode.....	58
Balloon dialog box.....	59
Updating your user view.....	59
Reverting to the default view.....	59
Download/Upload window for HDvM - SN with AIR.....	60
Enabling the HDvM - SN secondary window.....	61
Using Device Manager - Storage Navigator secondary windows.....	62
Secondary windows and wizards.....	62
Secondary window menus and buttons.....	64
HDvM - SN secondary windows and Modify mode.....	65
Resetting the secondary window.....	66
Cautions when using secondary windows.....	66
Java updates.....	66
Troubleshooting secondary windows.....	67
HDvM - SN secondary window blocked.....	78
Saving Java log and trace files.....	79
Creating a login message.....	79
Chapter 3: Configuring the storage system.....	81
Setting storage system information.....	81
Setting up security.....	81
Managing authentication and authorization servers.....	82
External authentication requirements using authentication server.....	83
External authorization requirements using authorization server.....	87
Connecting authentication and authorization servers.....	89
Setting up SSL encryption using Device Manager - Storage Navigator	90
SSL terminology.....	93
Setting up SSL communications.....	93
Notes on updating the signed certificate to the SVP.....	94
Creating a keypair.....	95
Converting the SSL certificates to PKCS#12 format.....	97
Obtaining a signed certificate.....	98
Releasing an SSL certificate passphrase.....	100
Uploading a signed certificate.....	101
Returning the certificate to default.....	103
Blocking HTTP communication to the storage system.....	104
Releasing HTTP communication blocking.....	105
Problems with a website security certificate.....	106
Setting SSL/TLS communications using Device Manager - Storage Navigator.....	106
Configuring certificates for HCS.....	108
Registering certificates for HCS.....	109

Notes on registering certificates for HCS.....	111
Deleting certificates for HCS.....	111
Reporting failure information about storage systems.....	112
Requirements of the Syslog protocol (TLS1.2/RFC5424).....	112
Obtaining a client certificate for the Syslog protocol.....	116
Changing advanced system settings.....	117
Updating Storage Device Launcher on the management client.....	119
Updating Captive Bundle Application on the SVP.....	120
Backing up and restoring HDvM - SN configuration files.....	121
Backing up HDvM - SN configuration files.....	124
Restoring HDvM - SN configuration files.....	124
Using the SMI-S function with a Device Manager - Storage Navigator user account.....	125
Using the SMI-S function.....	125
Uploading a signed certificate to the SMI-S provider.....	126
Returning an SMI-S provider certificate to default.....	128
Uploading an SMI-S provider configuration file.....	129
Returning an SMI-S provider configuration file to default.....	130
Sending SMI-S artificial indication.....	131
Setting up WSUS function	132

Chapter 4: User administration using Device Manager - Storage Navigator..... 134

User administration overview.....	134
Manage roles and permissions.....	134
Roles and user groups.....	135
Resource groups and user groups.....	135
User group registration example.....	136
Precautions when working with user groups.....	137
Naming a user group in Device Manager - Storage Navigator.....	137
Roles and permissions.....	137
Built-in user groups.....	140
Verifying the roles available to a user group.....	142
Verifying the roles available to a user group.....	142
Creating a new user group.....	143
Changing a user group name.....	144
Changing user group permissions.....	144
Changing assigned resource groups.....	145
Deleting a user group.....	145
User accounts.....	146
Creating user accounts.....	146
Character restrictions for user names and passwords.....	147

Changing user passwords.....	149
Changing logged-in user passwords.....	149
Changing user permissions.....	150
Enabling and disabling user accounts.....	151
Deleting user accounts.....	151
Managing resource groups.....	152
About resource groups	152
Resource access requirements for Device Manager - Storage Navigator operations.....	153
Access requirements for Compatible FlashCopy®.....	153
Access requirements for Compatible PAV.....	154
Access requirements for Data Retention Utility.....	154
Access requirements for Dynamic Provisioning and Dynamic Tiering..	154
Access requirements for Encryption License Key	155
Access requirements for global-active device.....	155
Access requirements for LUN Manager.....	156
Access requirements for Performance Monitor.....	159
Access requirements for ShadowImage.....	160
Access requirements for ShadowImage for Mainframe	160
Access requirements for Server Priority Manager.....	160
Access requirements for Thin Image.....	161
Access requirements for TrueCopyTrueCopy for Mainframe.....	162
Access requirements for Universal ReplicatorUniversal Replicator for Mainframe.....	163
Access requirements for Universal Volume Manager.....	165
Access requirements for Virtual LUNVirtual LVI.....	167
Access requirements for Virtual Partition Manager.....	168
Access requirements for Volume Retention Manager.....	168
Access requirements for Volume Shredder.....	168
Examples.....	169
Resource groups sharing a port.....	169
Resource groups not sharing ports.....	170
Resource group assignments.....	171
Resource group rules, restrictions, and guidelines.....	172
Creating resource groups.....	172
Adding resources to a resource group.....	173
Deleting resource groups.....	174
Account lock policy.....	174
Unlock a user account.....	174
Chapter 5: Managing license keys.....	176
License keys overview.....	176

License key types.....	176
Using the permanent key.....	177
Using the term key.....	178
Using the temporary key.....	178
Using the emergency key.....	178
Estimating licensed capacity.....	179
Software and licensed capacity.....	179
Calculating licensed capacity for a normal volume.....	183
Calculating licensed capacity for an external volume.....	184
Calculating pool capacity.....	184
Accelerated compression-enabled parity group capacity.....	185
Installing and uninstalling software.....	185
Installing license keys using Device Manager - Storage Navigator.....	185
When the status is Installed (Disabled).....	186
Enabling a license.....	186
Disabling a license.....	186
Removing a software application.....	186
Updating license status.....	187
Examples of license information.....	187
Cautions on license capacities in license-related windows.....	189
Cautions on licenses.....	189
Resolving errors when removing Data Retention Utility.....	189
License key expiration.....	190
Chapter 6: Viewing and managing the storage system.....	191
Viewing storage system information.....	191
Viewing basic information.....	191
Viewing specific information.....	192
Viewing other system information.....	192
Viewing port conditions.....	193
Status icons for certain resources.....	193
Managing tasks.....	194
Tasks window.....	195
Managing your tasks.....	195
Referencing the detailed task status.....	195
Stalled tasks.....	198
Setting the status refresh interval of the Tasks window.....	198
Chapter 7: Using reports to view storage system information.....	199
Creating configuration reports.....	199
Downloading and viewing the HDvM - SN configuration reports.....	200
Viewing configuration reports in the Reports window.....	201

Deleting configuration reports.....	201
Examples of Device Manager - Storage Navigator storage configuration reports.....	202
Report examples: table view.....	202
CHAP Users report.....	202
Disk Boards report.....	203
Host Groups / iSCSI Targets report.....	204
Hosts report.....	205
Logical Devices report.....	206
LUNs report.....	208
MP Unit report.....	209
MP unit details report.....	210
Parity Groups report.....	211
Physical Devices report.....	213
Ports report.....	215
Power Consumption report.....	218
Spare Drives report.....	220
SSD Endurance report.....	221
Storage System Summary report.....	222
Report examples: graphical view.....	224
Cache Memories report.....	224
Channel Boards report.....	225
Physical View report.....	225
Report examples: CSV files.....	226
AllConf.csv.....	227
CacheInfo.csv.....	227
ChapUserInfo.csv.....	227
ChaStatus.csv.....	228
DeviceEquipInfo.csv.....	228
DkaInfo.csv.....	228
DkaStatus.csv.....	229
DkclInfo.csv.....	229
DkuTempInfo.csv.....	230
DkuTempAveInfo.csv.....	233
DkuTempMaxInfo.csv.....	234
DkuTempMinInfo.csv.....	235
ELunInfo.csv.....	236
EnvMonInfo.csv.....	239
HSNBXTemplInfo.csv.....	240
HduInfo.csv.....	241
IscsiHostInfo.csv.....	242
IscsiPortInfo.csv.....	242

IscsiTargetInfo.csv.....	245
JnlInfo.csv.....	246
LdevCapalInfo.csv.....	246
LdevCountInfo.csv.....	247
LdevInfo.csv.....	248
LdevStatus.csv.....	251
LogPathStatus.csv.....	252
LPartition.csv.....	252
LunInfo.csv.....	253
LunPortInfo.csv.....	255
MfDMInfo.csv.....	256
MicroVersion.csv.....	256
MlcEnduranceInfo.csv.....	257
ModePerLpr.csv.....	258
MpPathStatus.csv.....	259
MpPcbStatus.csv.....	260
PcbRevInfo.csv.....	261
PdevCapalInfo.csv.....	261
PdevInfo.csv.....	262
PdevStatus.csv.....	263
PhyPathStatus.csv.....	264
PkInfo.csv.....	265
PplInfo.csv.....	267
SMfundat.csv.....	268
SsdDriveInfo.csv.....	268
SsidInfo.csv.....	269
SysoptInfo.csv.....	269
WwnInfo.csv.....	270
Chapter 8: Troubleshooting.....	272
General troubleshooting.....	272
Service information messages.....	273
Monitoring SIMs alerts in Device Manager - Storage Navigator.....	274
Login errors.....	275
No-response errors.....	277
Incorrect display errors.....	282
UNIX operation errors.....	284
HDvM - SN secondary window blocked.....	285
Storage Device Launcher errors.....	286
Other errors.....	286
Forcibly fail over the SVP.....	290
Firefox web browser problems on UNIX.....	292

Troubleshooting the SMI-S function.....	292
SMI-S artificial indication errors.....	293
Downloading dump files using the Dump tool.....	293
Saving Java log and trace files.....	295
Appendix A: System option modes (SOMs).....	296
System option modes.....	296
Appendix B: Device Manager - Storage Navigator user management GUI reference.....	367
User Groups window.....	367
Selected User Group Window.....	368
Create User Group wizard.....	372
Create User Group window.....	372
Create User Group confirmation window.....	374
Create User wizard.....	376
Create User window.....	376
Create User confirmation window.....	378
Change Password Wizard.....	379
Change Password window.....	379
Change Password confirmation window.....	380
Edit User wizard.....	380
Edit User window.....	380
Edit User confirmation window.....	382
Add User wizard.....	383
Add Users window.....	383
Add Users confirmation window.....	385
Remove Users window.....	386
Delete Users window.....	388
Release Lockout window	389
Edit User Group wizard.....	389
Edit User Group window.....	389
Edit User Group confirmation window.....	391
Delete User Groups window.....	392
Edit Resource Group Assignment wizard.....	392
Edit Resource Group Assignment window.....	392
Edit Resource Group Assignment confirmation window.....	397
Edit Role Assignment wizard.....	399
Edit Role Assignment window.....	399
Edit Role Assignment confirmation window.....	402
Setup Server wizard.....	403
Select Authentication Server window.....	403

Select Authentication Server confirmation window.....	404
LDAP Properties window.....	404
RADIUS Properties window.....	406
Kerberos Properties window.....	409
Setup Server for LDAP.....	412
LDAP Setup Server window.....	412
LDAP Setup Server confirmation window.....	417
Setup Server for RADIUS.....	419
RADIUS Setup Server window.....	419
RADIUS Setup Server confirmation window.....	425
Setup Server for Kerberos.....	428
Kerberos Setup Server window.....	428
Kerberos Setup Server confirmation window.....	433

Appendix C: Device Manager - Storage Navigator licenses GUI reference..... 436

License Keys window.....	436
Install Licenses wizard.....	439
Install Licenses window.....	439
Install Licenses confirmation window.....	442
Enable Licenses window.....	443
Disable Licenses window.....	445
Remove Licenses window.....	447
Update License Status window.....	449

Appendix D: Configuring storage systems GUI reference..... 452

Login Message window.....	452
Edit Storage System wizard.....	453
Edit Storage System window.....	453
Edit Storage System confirmation window.....	454
Edit Alert Settings wizard.....	454
Edit Alert Settings window.....	455
Add Sending Trap Setting window (SNMP v1 or v2c).....	465
Add Sending Trap Setting window (SNMP v3).....	466
Change Sending Trap Setting window (SNMP v1 or v2c).....	468
Change Sending Trap Setting window (SNMP v3).....	470
Add Request Authentication Setting window (SNMP v1 or v2c).....	472
Add Request Authentication Setting window (SNMP v3).....	473
Change Request Authentication Setting window (SNMP v1 or v2c).....	475
Change Request Authentication Setting window (SNMP v3).....	477
Add Address window.....	479
Change Settings window.....	480

Edit Alert Settings confirmation window.....	482
Column Settings window.....	486
Edit Advanced System Settings wizard.....	487
Edit Advanced System Settings window.....	488
Edit Advanced System Settings confirmation window.....	493
Appendix E: Device Manager - Storage Navigator system GUI reference.....	495
Storage Systems window.....	495
Port Condition window.....	501
Tasks window.....	504
Task Properties window.....	506
Suspend Tasks window.....	506
Resume Tasks window.....	507
Delete Tasks window.....	508
Disable Auto Delete window.....	509
Enable Auto Delete window.....	510
Edit Information Display Settings window.....	511
Reports window.....	513
Create Configuration Report window.....	513
Delete Reports window.....	514
Appendix F: Tool Panel GUI Reference.....	523
Tool Panel.....	523
Control Panel.....	525
Download File window.....	525
Restore File window.....	526
Download Dump Files window.....	527
Update Certificate Files window.....	528
Update Certificate Files for the SMI-S window.....	529
Upload Configuration Files for SMI-S window.....	530
SMI-S Artificial Indication window.....	530
Set or Delete Certificate File for HCS window.....	531
TLS Security Settings window	532
TLS Security Settings Communication Test window	536
Create CSR and Self-Signed Certificate window	537
Flash Enable/Disable window.....	541
CaptiveBundleUpload window.....	542
WSUS Settings.....	542
Appendix G: SMI-S provider configuration file.....	544
Supported TLS versions.....	544
Array-setting-01.properties file.....	544

File description format.....	544
File organization format.....	544
Parameters defined in user configuration files.....	545
VVolForSnapshot parameter.....	545
PoolIDForSnapshot parameter.....	546
ResourceGroup parameter.....	547

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 5000 Series storage system.

Readers of this document should be familiar with the following:

- Data processing and RAID storage systems and their basic functions.
- The VSP 5000 series and the *Hardware Guide* for your storage system.
- The operating system and web browser software on the management client hosting the Device Manager - Storage Navigator software.

Product version

This document applies to the following product versions:

- VSP 5000 series: firmware 90-06-21 or later
- SVOS RF 9.6.1 or later

Release notes

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

Changes in this revision

- Added the locale/language requirement for the management client ([Requirements for Windows-based management clients \(on page 21\)](#), [Requirements for UNIX/Linux-based management clients \(on page 23\)](#)).
- Added instructions for updating Storage Device Launcher on the management client ([Updating Storage Device Launcher on the management client \(on page 119\)](#)).
- Added information about the maximum number of tiers in a certificate chain ([External authentication requirements using authentication server \(on page 83\)](#), [External authorization requirements using authorization server \(on page 87\)](#), [Requirements of the Syslog protocol \(TLS1.2/RFC5424\) \(on page 112\)](#), [Login errors \(on page 275\)](#)).
- Added new system option modes (SOMs) 1222 and 1242 ([System option modes \(on page 296\)](#)).
- Added information about the supported Simple Network Time Protocol (SNTP) version ([Configuring the network settings on the management client \(on page 25\)](#)).
- Added the SVP version requirements for the Flash Disable, SIMSyslog Transfer Information, and TLS Security Settings backup files ([Backing up and restoring HDvM - SN configuration files \(on page 121\)](#)).





Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	<ul style="list-style-type: none"> ▪ Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click OK. ▪ Indicates emphasized words in list items.
<i>Italic</i>	<ul style="list-style-type: none"> ▪ Indicates a document title or emphasized words in text. ▪ Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: <pre>pairdisplay -g group</pre> <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>

Convention	Description
< > angle brackets	<p>Indicates variables in the following scenarios:</p> <ul style="list-style-type: none"> Variables are not clearly separated from the surrounding text or from other variables. Example: <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <pre>Status-<report-name><file-version>.csv</pre> </div> Variables in headings.
[] square brackets	Indicates optional values. Example: [a b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a b } indicates that you must choose either a or b.
vertical bar	<p>Indicates that you have a choice between two or more options or arguments. Examples:</p> <p>[a b] indicates that you can choose a, b, or nothing.</p> <p>{ a b } indicates that you must choose either a or b.</p>

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

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

Conventions for storage capacity values

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

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

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

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

Accessing product documentation

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

Getting help

The [Hitachi Vantara Support Website](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 the Hitachi Vantara Support Website for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

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

Comments

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

Thank you!

Chapter 1: Initial setup of the management client

The management client is the computer used to log in to and manage your storage system. The management client is LAN-attached to the storage system and communicates with the service processor (SVP). You can use Hitachi Device Manager - Storage Navigator (HDvM - SN) as well as other management software such as Hitachi Ops Center Administrator to manage your storage system.

Workflow for setting up the management client

Perform the following tasks to set up the management client for use of Device Manager - Storage Navigator (HDvM - SN).

1. Confirm that the management client meets the hardware and software requirements for running HDvM - SN ([Requirements for management clients \(on page 20\)](#)).
2. Configure the network settings on the management client ([Configuring the network settings on the management client \(on page 25\)](#)).
3. Configure the web browser on the management client ([Configuring the web browser on the management client \(on page 29\)](#)).
4. Install Storage Device Launcher on the management client ([Installing Storage Device Launcher on the management client \(on page 31\)](#)).
5. Configure the management client for the HDvM - SN secondary window ([Configuring the management client for the HDvM - SN secondary window \(on page 32\)](#)).
6. Review the cautions and restrictions before logging in to HDvM - SN for the first time ([Device Manager - Storage Navigator restrictions \(on page 43\)](#)).

Requirements for management clients

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

General requirements

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

Requirements for Windows-based management clients

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

Hardware requirements for the management client (Windows)

Item	Requirement
Processor (CPU)	Pentium 4 640 3.2 GHz or better (Recommended: Core2Duo E6540 2.33 GHz or better)
Memory (RAM)	2 GB or more Recommended: 3 GB
Available storage space	500 MB or more (+ 80 MB for each managed storage system) When HDvM - SN is using Adobe® AIR® from HARMAN™, an additional 80 MB of free space is required for each storage system managed by HDvM - SN.
Monitor	True Color 32-bit or better Resolution: 1280 x 1024 or better
Keyboard and mouse	You cannot use the mouse wheel feature.
Ethernet LAN card for TCP/IP network	100BASE-TX 1000BASE-T

Software requirements for the management client (Windows)

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

On a Windows management client, you can use HDvM - SN with Adobe AIR from HARMAN. The following tables specify the requirements for each method. The combinations and versions of operating system, architecture, browser, Java Runtime Environment (JRE), and Flash Player specified below are fixed requirements. Using other combinations or versions might produce unpredictable results such as the inability to use the HDvM - SN windows.



Note: Adobe will end support of Flash Player by the end of 2020. Make sure you are using HDvM - SN with Adobe AIR from HARMAN before the end of Flash Player support. If desired, you can disable use of HDvM - SN with Flash Player. For details, see [Disabling and enabling use of Flash Player with HDvM - SN \(on page 53\)](#).

You will continue to use a web browser to access and view the Tool Panel dialog box, the storage system configuration reports, and others. These tools are not affected by Flash Player end of support.

Table 1 Requirements for using HDvM with AIR from HARMAN

Operating system	Architecture	Web browser	TLS
Windows 10	64 bit	Internet Explorer 11.0* Google Chrome 63.0 or later	TLS1.2 TLS1.2 must be enabled. AIR does not support TLS1.3.
Windows 8.1	64 bit	Internet Explorer 11.0* Google Chrome 48.0 or later	
* Only the latest version of Internet Explorer that runs on each operating system is supported according to Microsoft® Support Policy.			

Table 2 Requirements for using HDvM - SN with Flash Player

Operating system ¹	Browser	Java Runtime Environment (JRE)	Adobe Flash Player ^{2, 3, 4, 5}
Windows Server 2016	Internet Explorer 11.0 ⁶	OpenJDK 11.0.2+9 or earlier	13 to 32
	Google Chrome 63.0 or later	OpenJDK 11.0.2+9 or earlier	13 to 32
Windows Server 2012 R2	Internet Explorer 11.0 ⁶	OpenJDK 11.0.2+9 or earlier	13 to 32
	Google Chrome 63.0 or later	OpenJDK 11.0.2+9 or earlier	13 to 32

Operating system ¹	Browser	Java Runtime Environment (JRE)	Adobe Flash Player ^{2, 3, 4, 5}
Windows 10	Internet Explorer 11.0 ⁶	OpenJDK 11.0.2+9 or earlier	13 to 32
	Google Chrome 63.0 or later	OpenJDK 11.0.2+9 or earlier	13 to 32
Windows 8.1	Internet Explorer 11.0 ⁶	OpenJDK 11.0.2+9 or earlier	13 to 32
	Google Chrome 48.0 or later	OpenJDK 11.0.2+9 or earlier	13 to 32
Windows 7	Internet Explorer 11.0 ⁶	OpenJDK 11.0.2+9 or earlier	13 to 32

Notes:

1. If the SVP supports IPv6, you can specify IPv6 addresses.
2. Flash Player should use the same architecture (32 bit or 64 bit) as your web browser.
3. Use of a version of Flash Player that is supported as standard on the operating system is supported, even if the version of Flash Player is not listed in this table.
4. Flash Player for Windows is available for Internet Explorer (ActiveX) and non-Internet Explorer (Plugin). Select the Flash Player installer according to the web browser that you use.
5. Flash Player is included and enabled by default for Internet Explorer on Windows Server 2012 and later. You do not need to reinstall Flash Player to use HDvM - SN. If Flash Player is not enabled by default, use the following procedure to enable it.
6. Only the latest version of Internet Explorer that runs on each operating system is supported according to Microsoft support policies.

**Note:**

- Some Device Manager - Storage Navigator operations are performed through the HDvM - SN secondary window that runs within Java.
- When you display an HTML format report saved in your local file system in a web browser that uses Flash Player version 23 or later, add the folder containing the HTML format report to Trusted Location Settings.

Requirements for UNIX/Linux-based management clients

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

Hardware requirements for the management clients (UNIX/Linux)

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

Software requirements for the management clients (UNIX/Linux)

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

The following table specifies the software requirements for using HDvM - SN in a UNIX or Linux environment. The combinations of operating system, architecture, browser, 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 use the HDvM - SN windows.

**Note:**

- Some HDvM - SN operations are performed using the secondary window within Java.
- When you display an HTML format report saved in your local file system in a web browser running with Flash Player version 23 or later, add the folder containing the HTML format report to Trusted Location Settings.

Operating system	Browser	Java Runtime Environment (JRE)	Adobe Flash Player ^{1,2}
Red Hat Enterprise Linux 7.5	Firefox 52.7 or later ³	OpenJDK 11.0.2+9 or earlier	32
	Chrome 67.0 or later	OpenJDK 11.0.2+9 or earlier	32

Operating system	Browser	Java Runtime Environment (JRE)	Adobe Flash Player ^{1,2}
Red Hat Enterprise Linux 7.4	Firefox 58.0 or later ³	OpenJDK 11.0.2+9 or earlier	32
	Chrome 63.0 or later	OpenJDK 11.0.2+9 or earlier	32

Notes:

1. Adobe Flash Player should use the same architecture (32 bit or 64 bit) as your web browser.
2. Using a version of Adobe Flash Player that is supported as standard on the operating system is supported, even if the version of Flash Player is not listed in this table.
3. IPv6 HTTPS connection from Firefox is not supported.

Configuring the network settings on the management client

Before you can use Device Manager - Storage Navigator (HDvM - SN), you must configure the network settings on the management client as follows:

- Set up TCP/IP for a firewall (see [Setting up TCP/IP for a firewall \(on page 25\)](#)).
- Configure IPv4/IPv6 communications (see [Setting up IPv4/IPv6 communications \(on page 26\)](#)).
- Register the SVP host name (see [Registering the SVP host name \(on page 27\)](#)).
- Add the SVP to the trusted sites zone ([Adding your SVP to the trusted sites zone for Windows Server computers \(on page 28\)](#)).



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

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.



Caution: Do not enable ICMP firewall configuration. If ICMP firewall is enabled, alert notifications might not occur. To disable ICMP firewall, contact the administrator who manages the firewall.

Protocol	Port number	Direction of communication
HTTP	80	From the management client to the SVP
HTTPS	443	
HTTPS(raidinf)	5443	
RMI	11099	
RMI	51099	
RMI	51100	
SMI-S	427	
SMI-S	5989	
SNMP ¹	161	
SNMP Trap ¹	162	From the SVP to the management client
Command Control Interface	31xxx through 33xxx ²	From a host to the SVP
Command Control Interface	34xxx through 36xxx ²	From the SVP to a host
Configuration Manager REST API	23454	From the SVP to the Configuration Manager REST API
SVP Connect Utility	7000 ³	From the SVP to the maintenance PC
Hitachi Remote Ops	990 ⁴ , 2056-2059 ⁴	From the SVP to the Remote Ops center
Notes:		
<ol style="list-style-type: none"> 1. Required if you use a Device Manager - Storage Navigator web client as an SNMP manager. 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>. 3. The support personnel use this port number to connect the maintenance PC to the storage system through a firewall. 4. If the remote maintenance by using Remote Ops is not performed, the firewall settings are not required. 		

Setting up IPv4/IPv6 communications

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

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

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

Configuring IPv6 communication in Windows 7

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

Procedure

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

Configuring IPv6 communication in Solaris 10

If the SVP uses IPv6 and you plan to use Device Manager - Storage Navigator (HDvM - SN) in a web browser, you must configure Solaris 10 management clients to use IPv6 for communication. If you plan to run HDvM - SN using Adobe AIR, you do not need to perform this task.

Procedure

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

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

Registering the SVP host name

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



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

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

Enter the SVP host name and IP address in the DNS server or hosts file of the management client. You can register any host name to the DNS server or the hosts file, but there are restrictions on the characters you can use for the host name.

- Registering the IP address and host name of the SVP to the DNS server that manages the network to which the SVP is connected.
- Entering the IP address and host name of the SVP to the hosts file of the management client. The general directory of the hosts file is:
 - For Windows: `C:\Windows\System32\drivers\etc\hosts`
 - For UNIX: `/etc/hosts`



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

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.

Configuring the web browser on the management client

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



Note: If you are using HDvM - SN with Adobe® AIR® from HARMAN™:

- You must configure the web browser as described below because these settings are used by AIR.
- You do not need to install Adobe Flash Player.

Web browser settings

- The browser must allow first-party, third-party, and session cookies.
- The pop-up blocker and plug-ins must be disabled.
- For Windows 8.1, Windows Server 2012, Windows Server 2012 R2 Update, Windows Server 2012 Update, and Windows Server 2016, JavaScript must be enabled. For details, see [Enabling JavaScript for Windows \(on page 30\)](#).

- For Windows Server and Internet Explorer:
 - Internet Explorer must be configured so it does not save encrypted pages to disk (**Tools > Internet Options > Advanced > Do not save encrypted pages to disk**).
 - The URL of the SVP must be registered in Internet Explorer (**Tools > Internet Options > Security**).
 - For Windows Server 2012, the IE security level for the trusted sites must be set to **Medium-high (Tools > Internet Options > Security > Trusted sites > Security level for this zone)**.
- For Firefox and Chrome, Adobe Flash Player must be enabled in your web browser.
- For the Japanese version of Firefox, the browser must be configured to use the C locale (default system language) by using the X Server Emulator.

In a B Shell, enter the following command:

```
LANG=C
export LANG
```

In a C Shell, enter the following command:

```
setenv LANG C
```

Enabling JavaScript for Windows

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

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



Note: This setting is required even if you use Device Manager - Storage Navigator with Adobe AIR because the web browser settings are used by AIR.

Procedure

1. Launch Internet Explorer.
2. On the Internet Explorer menu bar, click **Tools > Internet Options > Security**.
3. Click the **Security** tab.
4. Click **Custom Level**.
5. On the **Security Settings** window, 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. Exit and then restart Internet Explorer.

Installing Storage Device Launcher on the management client

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



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



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

Procedure

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

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



Note: If the SVP firmware version is earlier than 90-04-03, enter the following URL instead:

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

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

- b. In the authentication window, enter the user name and password.
 - c. Download the Web Console Launcher setup file for Windows (WCLauncher_win.zip).
2. Expand the downloaded Web Console Launcher setup file.

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

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



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

- a. Right-click `WCLauncher_win.zip`, and then click **Properties**.
- b. In **Security**, select **Unblock**, and then click **OK**.

3. Install Storage Device Launcher as follows:

- If you are logged in to the management client with administrator permissions, right-click `WCLauncher_win\WCLauncher\Setup_SDLauncher.bat`, and run it by selecting **Run as Administrator**.
- If you are not logged in to the management client with administrator permissions:
 - a. Right-click `WCLauncher_win\WCLauncher\Setup_SDLauncher.bat`, and then click **Create Shortcut**.
 - b. Move the created shortcut onto the desktop.

4. Open `WCLauncher_win\WCLauncher\log\Setup.log` with a text editor, and confirm that "completed" is displayed.



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

Next steps

After installing Storage Device Launcher on the management client, you can log in to HDvM - SN using AIR. For instructions, see [Logging in to HDvM - SN by using AIR \(on page 50\)](#).

Configuring the management client for the HDvM - SN secondary window

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

- Login Message function
- Compatible PAV
- Compatible XRC
- Data Retention Utility
- Volume Retention Manager
- Server Priority Manager

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

Restrictions for using the HDvM - SN secondary window with Google Chrome

When you open the secondary window, Google Chrome displays the following message:

This type of file can harm your computer. Are you sure you want to download <file name>.jnlp? . Click Save in the message window and save the object file. Then open the file. You can continue the operation even though a Java security warning is displayed when you open the file.

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

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

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

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

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.

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

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

- **Web Console Launcher:** This application is required to enable the HDvM - SN secondary window when HDvM - SN is running on a web browser with Java 11 or later installed.
- **Security settings command file:** This command file enables the settings of server certificate on the HDvM - SN management client to enhance communication security.
- **Storage Device Launcher:** This application is required to start HDvM - SN in the Adobe AIR environment. Storage Device Launcher is contained only in the setup file for Windows.

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



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

Procedure

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

Windows: Expand the file, right click `WCLauncher\Setupwin.bat` and execute it by selecting **Run as Administrator**. If the SVP certificate has been updated, run `SecurityToolWin.bat` to register the root certificate or self-signed certificate for the SVP.

UNIX: Enter `tar zxvf WCLauncher_unix.tgz` to expand the file. In the directory to which the file was expanded, enter `sudo sh` and `setupunix.sh` to run the shell script. If the SVP certificate has been updated, run `SecurityToolUnix.sh` to register the root certificate or self-signed certificate for the SVP.



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

Next steps

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



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

Verifying the SVP server certificate

If you updated the initial SVP certificate, you can verify whether the connection destination is correct by registering the server certificate or self-signed certificate for the SVP on the Device Manager - Storage Navigator (HDvM - SN) management client. When verification is enabled, if verification fails, the communication is interrupted, and starting the HDvM - SN secondary window fails. Even when verification is disabled, verification processing is performed. In this case, if verification fails, a confirmation window appears indicating the following message:

```
The certificate security verification for the TLS communication cannot be
performed. Are you sure you want to stop the certificate security
verification to continue the connection?
```

After you click `Confirm`, the communication continues.

If the server certificate registered on the SVP is a signed public key certificate issued by a Certificate Authority (CA), register the root certificate of the CA on the HDvM - SN management client. If the server certificate is a self-signed certificate, register the server certificate registered on the SVP onto the HDvM - SN management client. A certificate that can be registered on the HDvM - SN management client is in X509 PEM or X509 DER format.

Table 3

Verification item	What is verified?	Note
Validity period verification	Verifies whether the server certificate is within the validity period.	Before you verify the validity, ensure that the validity period for the server certificate registered on the SVP is not expired.
Revocation verification	Verifies whether the server certificate is not invalidated by using the CRL (list of digital certificates that were invalidated before the expiration date) or OCSP (online check).	You need a network environment in which the CRL repository or OCSP responder can be accessed from the HDvM - SN management client.

Verification item	What is verified?	Note
SAN/CN verification	Verifies whether the host name (including FQDN) or IP address (IPv4 or IPv6) that is specified for SAN (Subject Alternative Name: additional name that is an extension of CN) or CN (Common Name) in the server certificate is the same as the connection destination.	The host name or IP address of the SVP that you specify as the connection destination on the HDvM - SN management client must be contained in SAN or CN in the server certificate registered on the SVP. For the IP address, specify the IP address displayed in the HDvM - SN main window.
Certificate chain verification	Verifies whether the root certificate, intermediate certificates, and server certificate are correctly associated with each other in the certificate chain.	If the sever certificate is signed by an intermediate CA, all intermediate certificates including the server certificate must be registered in the certificate to be registered on the SVP.



Caution:

If you did not update the initial SVP certificate, disable the verification function to continue the communication as it did before.

If you enable the verification function, verification fails, the communication is interrupted, and starting the HDvM - SN secondary window fails.

Registering a certificate on the HDvM - SN management client (Windows)

If you updated the initial SVP certificate, you must register the root certificate or self-signed certificate for the SVP on the Device Manager - Storage Navigator (HDvM - SN) management client.

Before you begin

You must have logged into the HDvM - SN management client.

Procedure

1. Store the certificate file on the HDvM - SN management client.
2. Open a command prompt with administrator permissions.
3. Move the current directory to the folder to which the downloaded file was expanded.
4. Run the following command.

```
SecurityToolWin.bat import alias-of-the-SVP path-to-the-certificate
```

```
Example: SecurityToolWin.bat import SVP1 "C:\monitor\cert.crt"
```

5. Ensure that the trust store `WCLauncher.dat` exists in the current directory.

Viewing a certificate on the HDvM - SN management client (Windows)

You can view the root certificate or self-signed certificate that is registered on the Device Manager - Storage Navigator (HDvM - SN) management client.

Before you begin

You must have logged into the HDvM - SN management client.

Procedure

1. Open a command prompt with administrator permissions.
2. Move the current directory to the folder to which the downloaded file was expanded.
3. Run the following command:
`SecurityToolWin.bat list`
4. Check the displayed contents

Output example:

```
Alias name: abc
Creation date: 2020/05/14
Entry type: trustedCertEntry
Owner: EMAILADDRESS=svp@str.hitachi.co.jp, CN="Hitachi, Ltd.", OU=IT
Platform
Division Group, O="Hitachi, Ltd.", L=Odawara, ST=Kanagawa, C=JP
Issuer: EMAILADDRESS=svp@str.hitachi.co.jp, CN="Hitachi, Ltd.", OU=IT
Platform
Division Group, O="Hitachi, Ltd.", L=Odawara, ST=Kanagawa, C=JP
Serial number: dc52873fdb5cc76b
Valid from: Fri Apr 18 09:16:04 GMT+09:00 2014 until: Thu Apr 18
09:16:04 GMT
+09:00 2024
Certificate fingerprints:
MD5: B3:A5:60:17:17:91:9D:0E:F7:31:DC:1C:06:FA:51:CA
SHA1: 43:14:DF:80:1D:64:AA:09:B8:F3:1C:13:74:2B:7E:95:1D:2F:E9:6F
SHA256:
9B:A8:68:45:95:91:3C:72:9B:4C:6A:FE:BB:B9:32:F0:04:E5:9E:DF:B1:47:2F:59
:EA:0C:26:1A:
BC:70:E8:15
Signature algorithm name: SHA256withRSA
Version: 1
```

Deleting a certificate on the HDvM - SN management client (Windows)

You can delete the root certificate or self-signed certificate that is registered on the Device Manager - Storage Navigator (HDvM - SN) client.

Before you begin

You must have logged into the HDvM - SN management client.

Procedure

1. Check the alias of the SVP connected by using the root certificate or self-signed certificate that is registered on the HDvM - SN management client.
2. Open a command prompt with administrator permissions.
3. Move the current directory to the folder to which the downloaded file was expanded.
4. Run the following command:

```
SecurityToolWin.bat delete alias-of-the-SVP
```

```
Example: SecurityToolWin.bat delete SVP1
```

5. Ensure that the certificate was deleted.

Setting server verification on the HDvM - SN management client (Windows)

You can enable or disable server verification on the Device Manager - Storage Navigator (HDvM - SN) management client.

Before you begin

You must have logged into the HDvM - SN management client.

Procedure

1. Open a command prompt with administrator permissions.
2. Move the current directory to the folder to which the downloaded file was expanded.
3. Run the following command:

```
SecurityToolWin.bat verify setting-value
```

```
Example: SecurityToolWin.bat verify enable
```



Note:

If you specify *enable*, a security settings command file is created in the folder that stores command files.

If you specify *disable*, the security settings command file is deleted.

Viewing whether server verification is enabled on the HDvM - SN management client (Windows)

You can view whether server verification is enabled on the Device Manager - Storage Navigator management client.

Before you begin

You must have logged into the HDvM - SN management client.

Procedure

1. Open a command prompt with administrator permissions.
2. Move the current directory to the folder to which the downloaded file was expanded.
3. Run the following command:
`SecurityToolWin.bat verifysetting`
4. Check the displayed contents.

Output example:

```
disabled
```

Viewing the Help on the HDvM - SN management client (Windows)

You can view the Help on the Device Manager - Storage Navigator (HDvM - SN) management client.

Before you begin

You must have logged into the HDvM - SN management client.

Procedure

1. Open a command prompt with administrator permissions.
2. Move the current directory to the folder to which the downloaded file was expanded.
3. Run the following command:
`SecurityToolWin.bat help`

Output example:

```
Command Line Syntax
import <alias> <certificate-file-path>
alias: alias of specified certificate
certificate-file-path: relative or absolute certificate file path
delete <alias>
alias: alias of specified certificate
list
verify <value>
value: enable or disable
verifysetting
help
```

Registering a certificate on the HDvM - SN management client (UNIX)

If you updated the initial SVP certificate, you must register the root certificate or self-signed certificate for the SVP on the Device Manager - Storage Navigator (HDvM - SN) management client.

Before you begin

You must have logged into the HDvM - SN management client.

Procedure

1. Store the certificate file on the HDvM - SN management client.
2. Run the shell as superuser.
3. Move the current directory to the directory to which the downloaded file was expanded.
4. Run the following command as superuser:

```
SecurityToolUnix.sh import alias-of-the-SVP path-to-the-certificate
```

Example: `SecurityToolUnix.sh import SVP1 /tmp/cert.crt`

5. Ensure that the trust store `WCLauncher.dat` exists in the current directory.

Viewing a certificate on the HDvM - SN management client (UNIX)

You can view the root certificate or self-signed certificate that is registered on the Device Manager - Storage Navigator (HDvM - SN) management client.

Before you begin

You must have logged into the HDvM - SN management client.

Procedure

1. Run the shell as superuser.
2. Move the current directory to the directory to which the downloaded file was expanded.
3. Run the following command as superuser:

```
SecurityToolUnix.sh list
```

4. Check the displayed contents.

Output example:

```
Alias name: test
Creation date: 2020/05/14
Entry type: trustedCertEntry
Owner: EMAILADDRESS=svp@str.hitachi.co.jp, CN="Hitachi, Ltd.", OU=IT
Platform
Division Group, O="Hitachi, Ltd.", L=Odawara, ST=Kanagawa, C=JP
Issuer: EMAILADDRESS=svp@str.hitachi.co.jp, CN="Hitachi, Ltd.", OU=IT
Platform
Division Group, O="Hitachi, Ltd.", L=Odawara, ST=Kanagawa, C=JP
Serial number: dc52873fdb5cc76b
Valid from: Fri Apr 18 09:16:04 JST 2014 until: Thu Apr 18 09:16:04
JST 2024
Certificate fingerprints:
MD5: B3:A5:60:17:17:91:9D:0E:F7:31:DC:1C:06:FA:51:CA
SHA1: 43:14:DF:80:1D:64:AA:09:B8:F3:1C:13:74:2B:7E:95:1D:2F:E9:6F
SHA256:
9B:A8:68:45:95:91:3C:72:9B:4C:6A:FE:BB:B9:32:F0:04:E5:9E:DF:B1:47:2F:59
:EA:0C:26:1A:
BC:70:E8:15
```



```
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 1
```

Deleting a certificate on the HDvM - SN management client (UNIX)

You can delete the root certificate or self-signed certificate that is registered on the Device Manager - Storage Navigator (HDvM - SN)r management client.

Before you begin

You must have logged into the HDvM - SN management client.

Procedure

1. Check the alias of the SVP connected by using the root certificate or self-signed certificate that is registered on the HDvM - SN management client.
2. Run the shell as superuser.
3. Move the current directory to the directory to which the downloaded file was expanded.
4. Run the following command as superuser:

```
SecurityToolUnix.sh delete alias-of-the-SVP
```


Example:

```
SecurityToolUnix.sh delete SVP1
```
5. Ensure that the certificate was deleted.

Setting server verification on the HDvM - SN management client (UNIX)

You can enable or disable server verification on the Device Manager - Storage Navigator (HDvM - SN) management client.

Before you begin

You must have logged into the HDvM - SN management client.

Procedure

1. Run the shell as superuser.
2. Move the current directory to the directory to which the downloaded file was expanded.
3. Run the following command as superuser:

```
SecurityToolUnix.sh verify setting-value
```


Example:

```
SecurityToolUnix.sh verify enable
```



Note:

If you specify *enable*, a security settings command file is created in the directory that stores command files.

If you specify *disable*, the security settings command file is deleted.

Viewing whether server verification is enabled on the HDvM - SN management client (UNIX)

You can view whether server verification is enabled on the Device Manager - Storage Navigator management client.

Before you begin

You must have logged into the HDvM - SN management client.

Procedure

1. Run the shell as superuser.
2. Move the current directory to the directory to which the downloaded file was expanded.
3. Run the following command as superuser:
`SecurityToolUnix.sh verifysetting`
4. Check the displayed contents

Output example:

```
disabled
```

Viewing the Help on the HDvM - SN management client (UNIX)

You can view the Help on the Device Manager - Storage Navigator (HDvM - SN) management client.

Before you begin

You must have logged into the HDvM - SN management client.

Procedure

1. Run the shell as superuser.
2. Move the current directory to the directory to which the downloaded file was expanded.
3. Run the following command as superuser:
`SecurityToolUnix.sh help`

Output example:

```
Command Line Syntax
import <alias> <certificate-file-path>
alias: alias of specified certificate
certificate-file-path: relative or absolute certificate file path
delete <alias>
alias: alias of specified certificate
list
verify <value>
value: enable or disable
verifysetting
help
```

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 using Device Manager - Storage Navigator (HDvM - SN) in a web browser, observe the following cautions and restrictions:

- When you use a web browser for a long period of time, memory might be heavily used. Make sure to close and log out of HDvM - SN after each use.
- Do not change the web browser settings such as Tools > Folder options in Internet Explorer. If you do and see unexpected results, close the web browser and log in to HDvM - SN again.
- 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 use Back, Next, or web browser shortcut keys such as **F5** and **Esc**, you will be logged out of HDvM - SN. 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 HDvM - SN, click Logout or File > Close in the HDvM - SN menu.
- 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 in the HDvM - SN main window.

In Google Chrome, the window does not close when you log out.
- If you are using HDvM - SN in a web browser, do not disable Flash Player. Flash Player is required to run HDvM - SN in a browser and acts as an add-on to the browser. If you use Internet Explorer, do not change the settings in Tools > Manage Add-ons.

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
Virtual Storage Platform 5000 series	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 \(on page 511\)](#).

Chapter 2: Using the Device Manager - Storage Navigator GUI

The Device Manager - Storage Navigator (HDvM - SN) GUI displays the storage system information and allows you to perform operations on the storage system.

When you use HDvM - SN on a Windows management client, you can use the HDvM - SN GUI either in a web browser or by using Adobe AIR. When you use HDvM - SN on a UNIX/Linux management client, you can only use the HDvM - SN GUI in a web browser.

Logging in to HDvM - SN in a browser

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

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



Note:

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

Initial superuser login

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

**Important:**

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

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

Procedure

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

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

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

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

4. The following actions might be required to open the login window, depending on your environment:
 - If a message indicates that the enhanced security configuration is enabled on the management client, select **In the future, do not show this message** and then click **OK**.
 - If the SVP is configured to support SSL-encrypted communication and security messages appear, make sure the certificate is correct and follow the instructions in the dialog box.
 - If a message indicates that certain websites are blocked, you need to add the SVP to the trusted sites zone (see [Adding your SVP to the trusted sites zone for Windows Server computers \(on page 28\)](#)).
5. Type the superuser ID and password, and then click **Login**.
6. If the **Security Information** dialog box appears, click **Yes**.
After you log in, the Device Manager - Storage Navigator main window opens. You can navigate using the menu, tree, or General Tasks.
7. **Important:** Change the superuser password immediately after you log in to prevent unauthorized use of the superuser account. To change the password, click **Settings > User Management > Change Password**.

User login

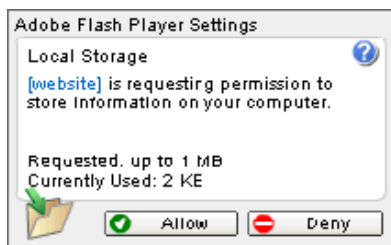
Use the following procedure to log in to Device Manager - Storage Navigator.

Procedure

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

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

3. The following actions might be required to open the login window, depending on your environment:
 - If a message indicates that the enhanced security configuration is enabled on the management client, select **In the future, do not show this message** and then click **OK**.
 - If the SVP is set to support SSL-encrypted communication and security messages appear, make sure the certificate is correct and follow the instructions in the dialog box.
 - If a message indicates that certain web sites are blocked, you need to add the SVP to the trusted sites zone (see [Adding your SVP to the trusted sites zone for Windows Server computers \(on page 28\)](#)).
4. Type the user ID and password, and then 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.



Result

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

Logging in to HDvM - SN by using AIR

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

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

Before you begin

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

Procedure

1. Open the HDvM - SN login dialog box.

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

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

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



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

- b. Enter the IP address or host name of the SVP.
 - c. Specify 443 for the HTTPS port number, and then click **Connect**.

If a security warning message is displayed, verify that the security certificate is correct, and then follow the instructions in the dialog box.
- To open the HDvM - SN login dialog box by opening a web browser and running Storage Device Launcher on the SVP:
 - a. Start the web browser on the management client with administrator permissions.
 - b. Enter the following URL in the web browser:

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

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

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



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

- c. If a security warning message is displayed, verify that the security certificate is correct, and then follow the instructions in the dialog box.
2. Wait about 10 seconds for the CBA file to be downloaded to the management client. When the download is complete, the HDvM - SN login dialog box opens. You can close the web browser.



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

3. Enter the user name and password, and then click **Login**.
If the **Security Information** dialog box opens, click **Yes**.
When the storage system configuration information is finished loading, the HDvM - SN main window opens.

Changing your initial HDvM - SN password

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

Procedure

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

Disabling and enabling use of Flash Player with HDvM - SN

Adobe Flash Player is used to run Device Manager - Storage Navigator (HDvM - SN) in a web browser. If desired, you can disable use of Flash Player with HDvM - SN after you start using HDvM - SN with Adobe AIR from HARMAN. Later, if you need to run HDvM - SN in a web browser, you can re-enable use of Flash Player on the management client.

When you use Hitachi Command Suite (HCS), however, do not disable use of Flash Player to run HDvM - SN. If you disable this function, you will not be able to access HDvM - SN from HCS.

Make sure that the HCS version supports linkage with HDvM - SN running in the AIR environment.



Caution: If you disable Flash Player, you will not be able to access HDvM - SN.



Note: If an alert about an SVP failover (SIM reference code: 7ff3xx) is issued within 24 hours after disabling or enabling use of Flash Player with HDvM - SN, check the setting and change it again if necessary. Depending on the timing of the SVP failover, this setting might not be saved in the SVP after the failover.

Before you begin

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

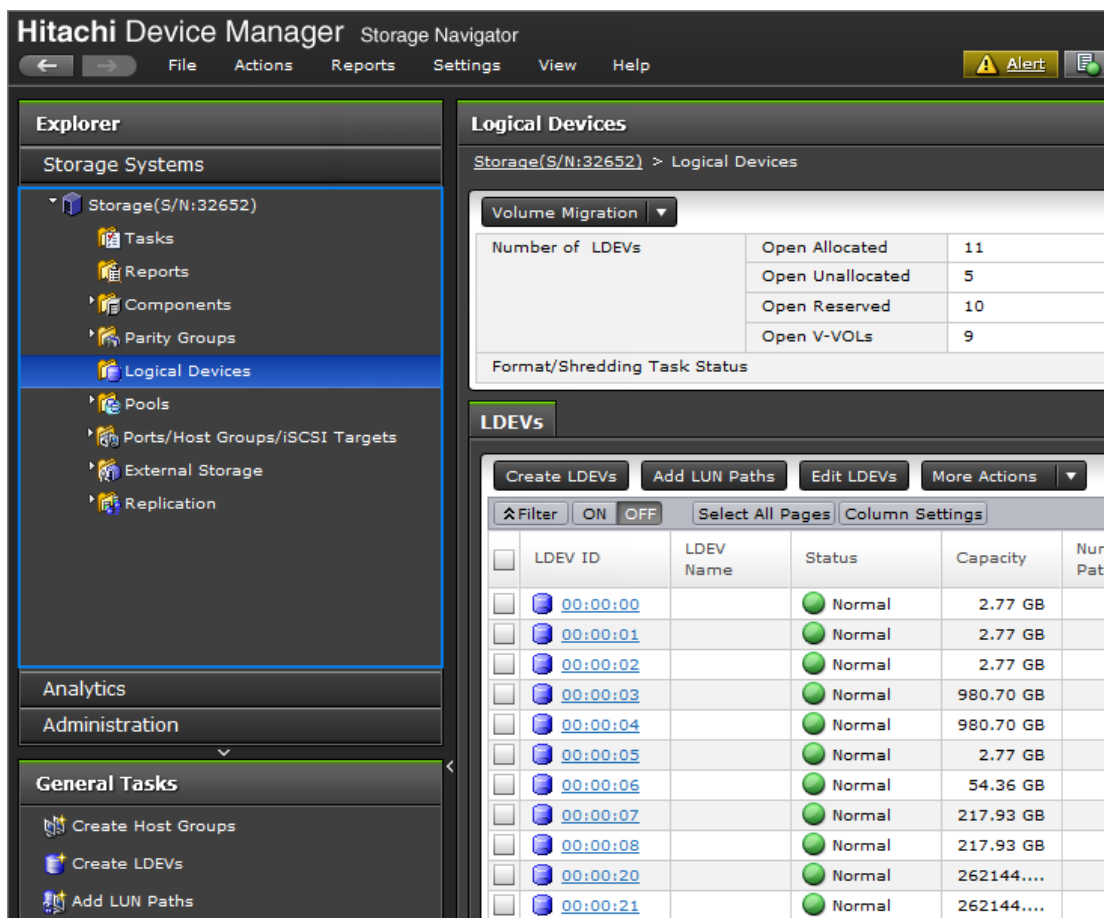
Procedure

1. On the management client, open a web browser.
2. Open the Tool Panel on the SVP by specifying the following URL:

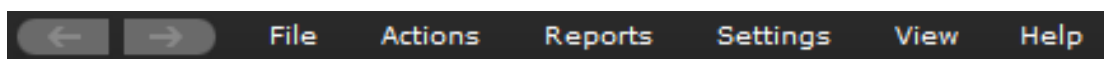

```
https://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi
```
3. Click **Flash Disable/Enable**.
4. On the **Login** dialog box, enter the administrator user ID and password, and then click **Login**.
5. In the **Flash Disable/Enable** dialog box, select **Disable** (or **Enable**), and then click **OK**.
If the **Security Alert** dialog box for the certificate opens before you are returned to the **Login** dialog box, click **View Certificate**, verify that the certificate is correct, and then click **Yes**.

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



Item	Description
	Click to return to the previous window.
	Click to advance to the next window.
File	<ul style="list-style-type: none"> 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. Logout: Logs the current user out of Device Manager - Storage Navigator.
Actions	Provides actions to the storage system such as creating LDEVs or performing replication copy.

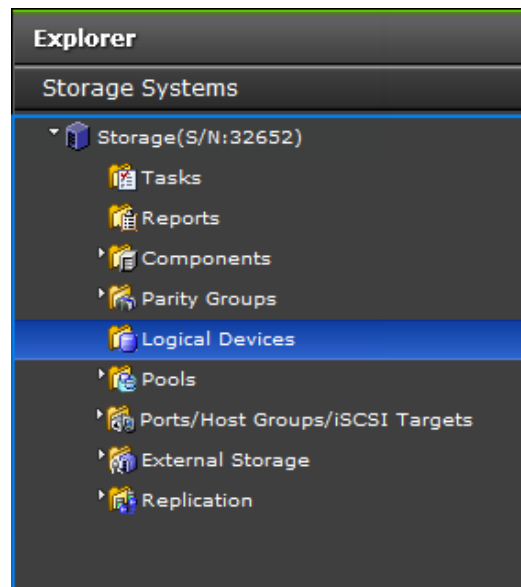
Item	Description
Reports	<ul style="list-style-type: none"> ▪ Task Management: Manages the tasks that will be applied to the storage system. ▪ Configuration Report: Creates and downloads storage system configuration reports. ▪ Performance Monitor: Monitors performance of the storage system. ▪ Shredding Report: Downloads the shredding report.
Settings	<ul style="list-style-type: none"> ▪ User Management: Manages Device Manager - Storage Navigator user accounts, including changing passwords. ▪ Resource management: Performs resource group related operations ▪ Security: Performs audit log or encryption operations ▪ 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.
View	Changes the font size in the window.
Maintenance Utility	Launches the storage system's maintenance work window.
Tool	<ul style="list-style-type: none"> ▪ Download: Displays the dialog box to download the setup files for Web Console Launcher (required to use the HDvM - SN secondary window with Java 11 or later) and Storage Device Launcher (required to start HDvM - SN running with Adobe AIR).
Help	Displays the online help

Using the Device Manager - Storage Navigator main window

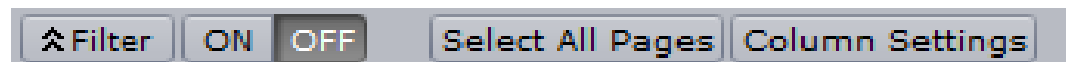
You can perform operations by using the main window and wizards.

Procedure

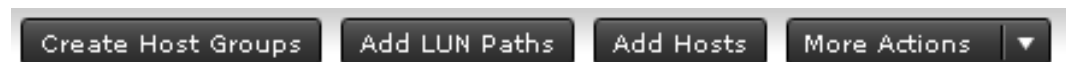
1. Click a function in the resource tree in the Explorer.



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.

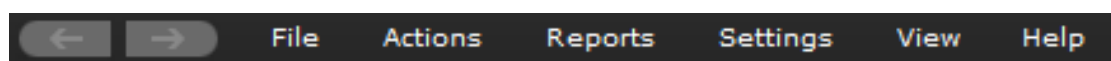


6. Open the task window to verify the result of the operation. A task can be suspended or canceled if the processing of the task is not started.

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.

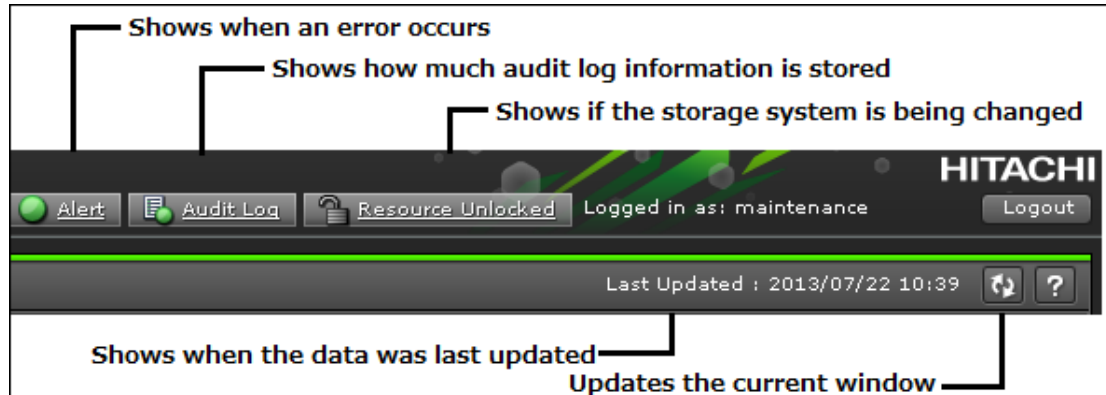
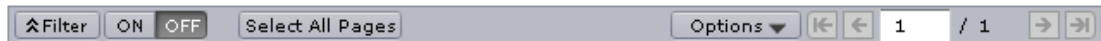


Table Controls

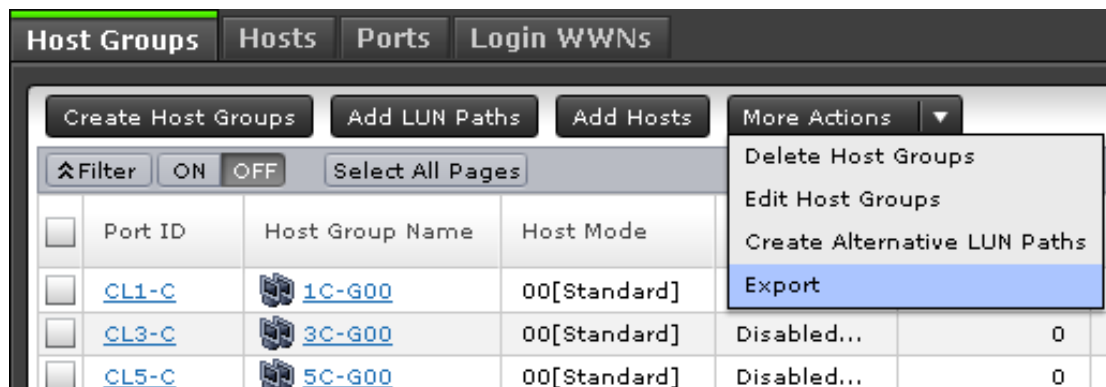
The following figures shows the controls used to view and filter the results in a main window table:



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.

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").

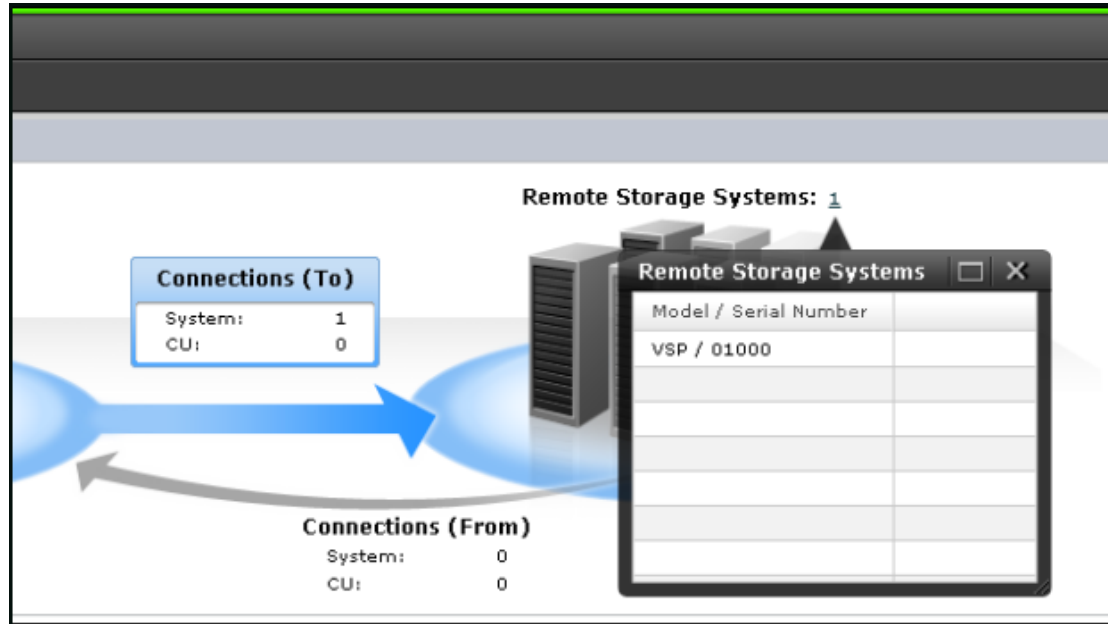
Host Groups Hosts Ports Login WWNs							
Edit Ports Export							
Filter ON OFF Select All Pages							
	Port ID	Internal WWN	Speed	Security	Type	Address (Loop ID)	Fabric
<input type="checkbox"/>	CL1-C	50060E80073...	Auto(1Gbps)	Disabled	Fibre	B2 (32)	OFF
<input type="checkbox"/>	CL3-C	50060E8007303902	Auto(1Gbps)	Disabled	Fibre	B1 (33)	OFF
<input type="checkbox"/>	CL5-C	50060E80073...	Auto(1Gbps)	Disabled	Fibre	AE (34)	OFF
<input type="checkbox"/>	CL7-C	50060E80073...	Auto(1Gbps)	Disabled	Fibre	AD (35)	OFF
<input type="checkbox"/>	CL1-D	50060E80073...	Auto(1Gbps)	Disabled	Fibre	AC (36)	OFF
<input type="checkbox"/>	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.

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.



Updating your user view

If you remain in the same Device Manager - Storage Navigator view while other users make changes to the storage system, these changes do not appear in your view.

- To see how long it has been since your view was updated, check the clock in the title bar to the left of the **Update** button. This clock displays the SVP time, not the time on your local workstation.
- To display the number of minutes that have passed since your view was updated, place the cursor over the clock.
- To refresh your view, click **Update** in the top right corner of the title bar.



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

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.

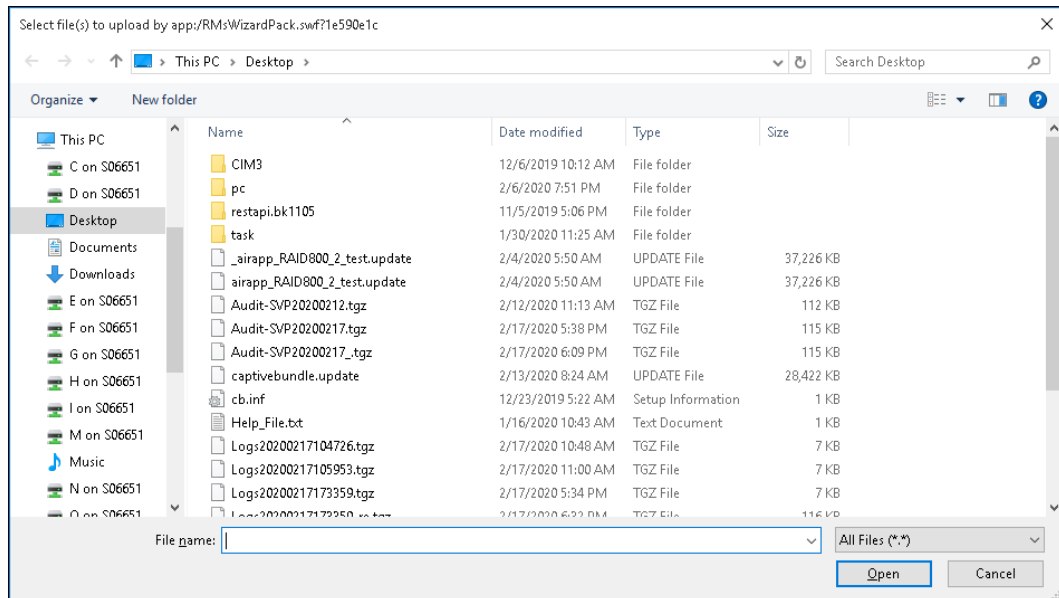
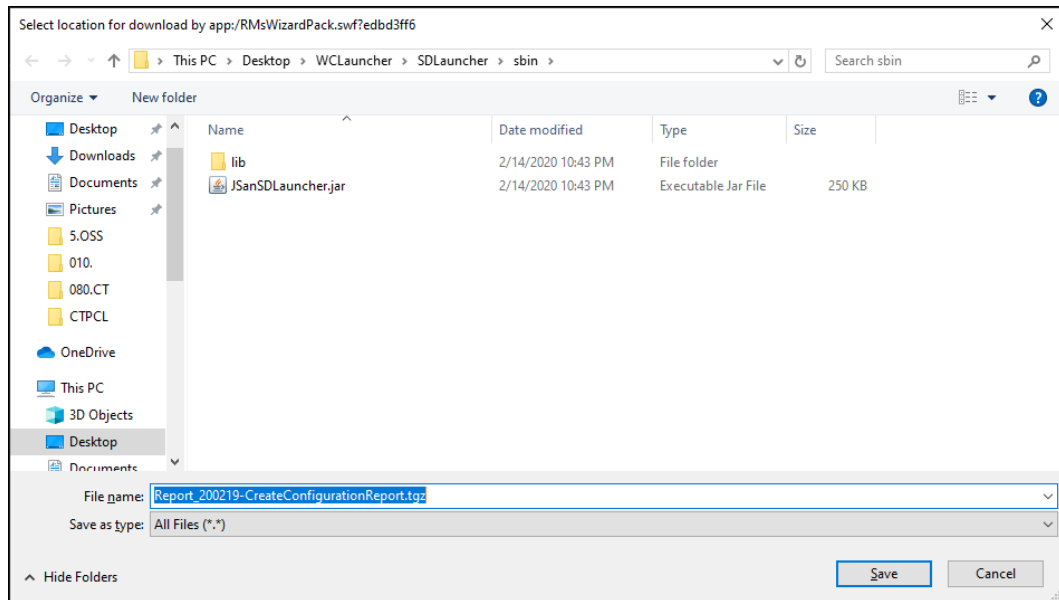
To return your settings to default, select Settings > Environmental Settings > Reset User's View Settings.

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 ¹
	Column	Sort	NA
		Width	Default state ¹
		Order	Default state ¹
	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 ¹
LUN ID notation	-	-	Decimal integer
1. The default state varies from window to window.			

Download/Upload window for HDvM - SN with AIR

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



Enabling the HDvM - SN secondary window

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

- Login Message function
- Data Retention Utility
- Server Priority Manager
- Compatible PAV
- Compatible XRC
- Volume Retention Manager

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

Before you begin

- Required role: Storage Administrator (View Only)

Procedure

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

Using 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.

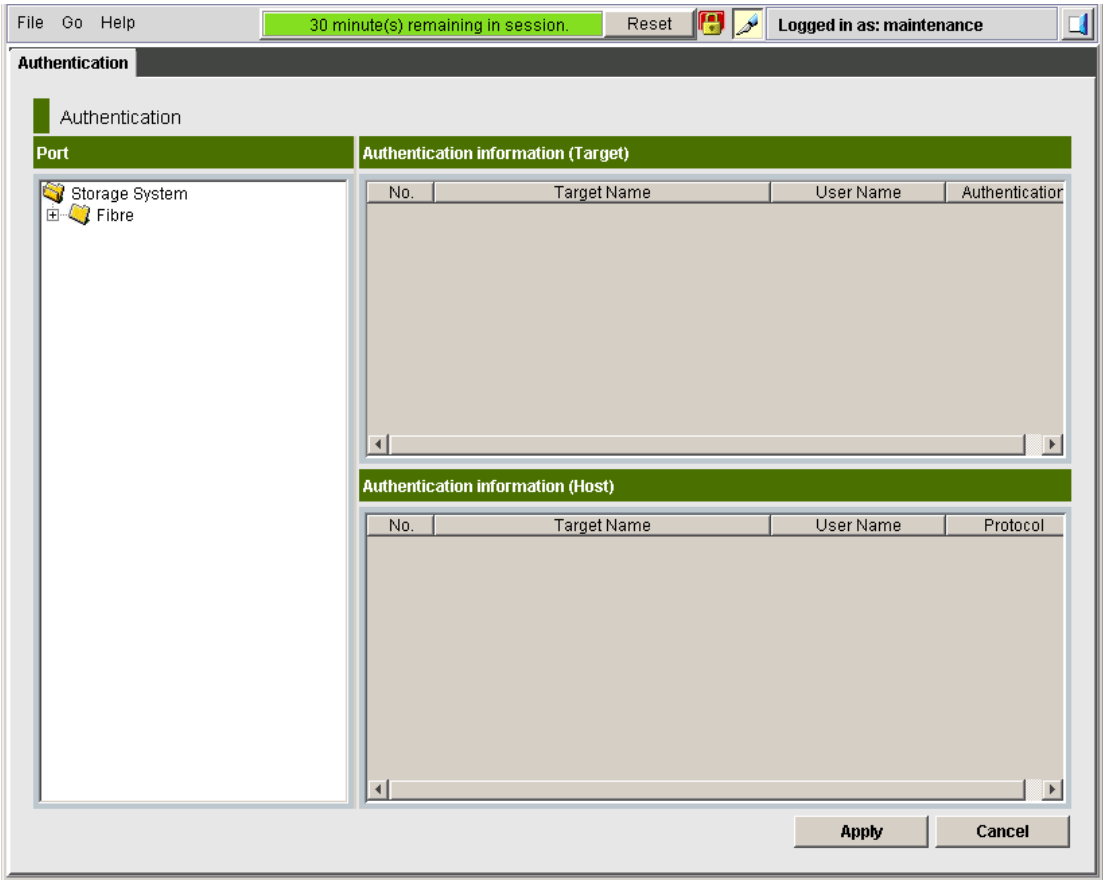


Figure 1 Example of a secondary window

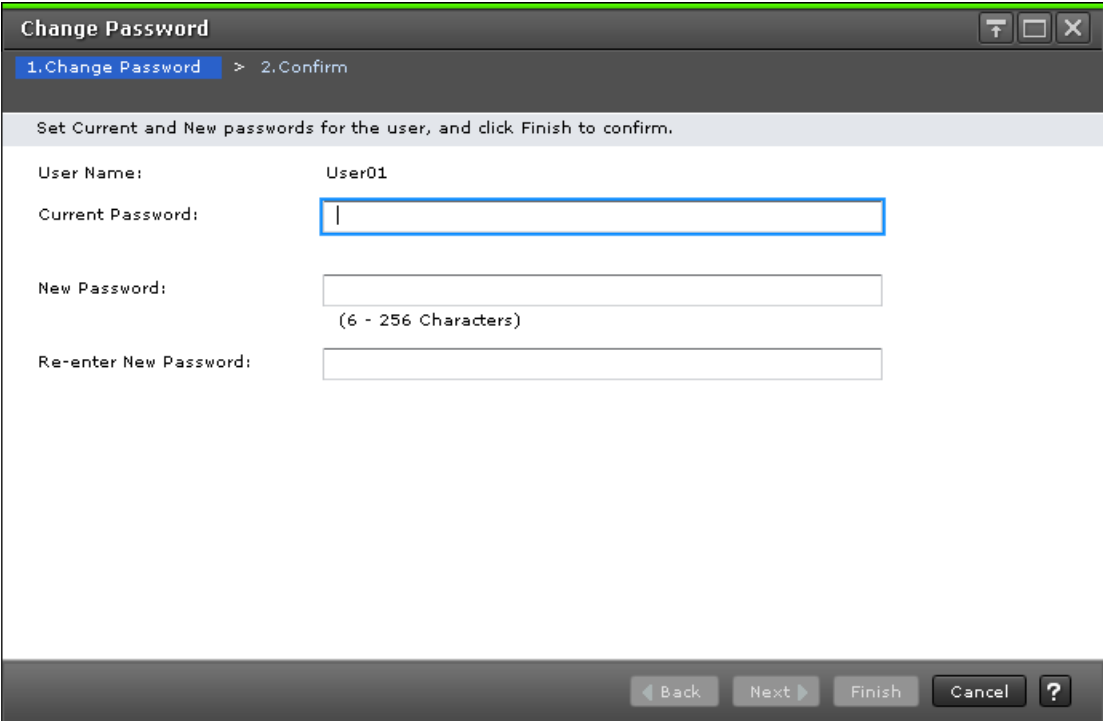
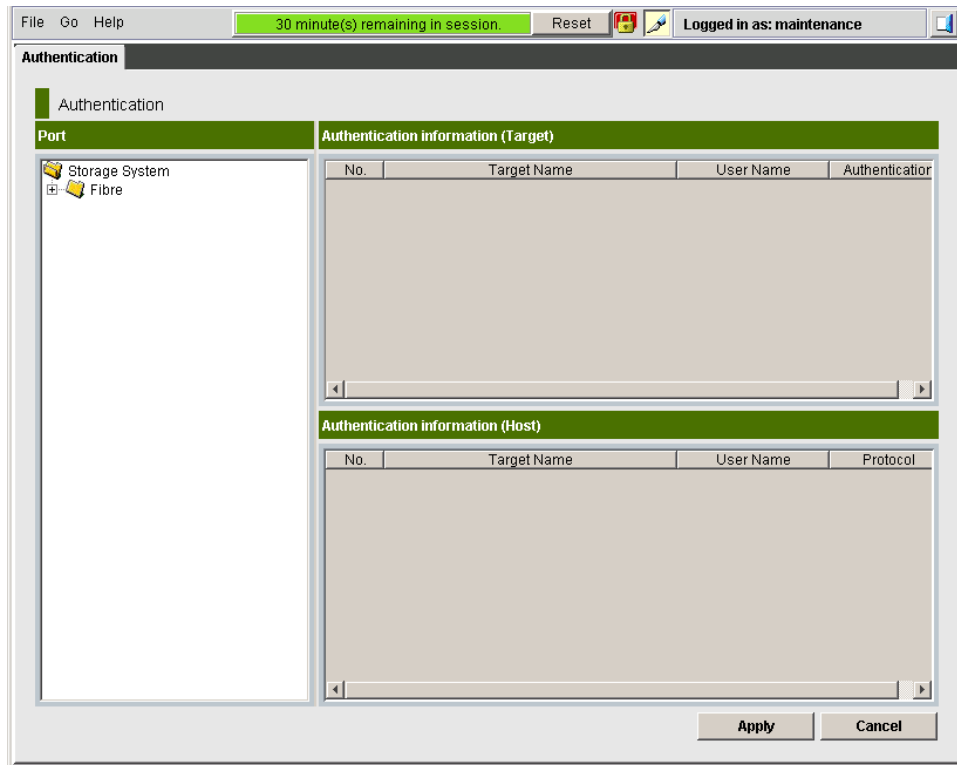


Figure 2 Example of a wizard




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"> ▪ IP indicates the IP address of the SVP. ▪ S/N indicates the serial number. ▪ D/N indicates the device name specified in the Edit storage system window.
File > 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"> ▪ Takes time until the processing has been completed. ▪ 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. ▪ Available only for the user with Storage Administrator (Initial Configuration) role.

Item	Description
	<ul style="list-style-type: none"> ▪ Available only when the user is in Modify mode. ▪ The information may not display correctly if SVP maintenance is in progress. ▪ Try this command if the configuration information displayed on the Device Manager - Storage Navigator differs from the actual configuration information that can be recognized from the host.
File > Refresh	Displays the latest information on Device Manager - Storage Navigator.
File > Close	Closes the Device Manager - Storage Navigator secondary window
Go menu	Indicates software names
Help menu	About: Opens the About dialog box to show the version of the storage system.
 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.</p>
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.

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 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.

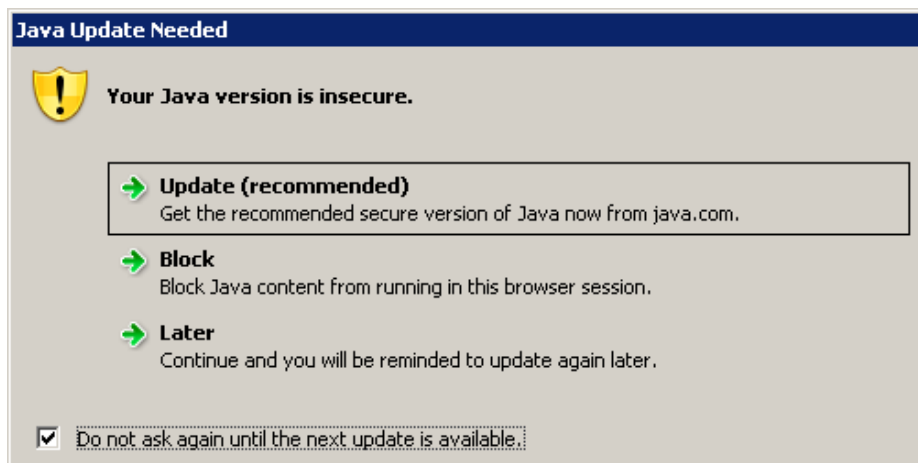
Java updates

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 **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 HDvM - SN secondary window \(on page 61\)](#).
- 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 HDvM - SN secondary window \(on page 61\)](#).
- 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

The following tables list error conditions in the Device Manager - Storage Navigator (HDvM - SN) secondary window and provide recommended actions to resolve the errors:

Table 4 Java application errors

Error condition	Probable cause / recommended action
<p>When you click the HDvM - SN 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 HDvM - SN. 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"> ▪ Disable the pop-up blocker function of your web browser. ▪ Disable the pop-up blocker function of any browser plug-in/add-on. <p>If neither of the above can be performed in Internet Explorer, you can open the window by clicking the HDvM - SN menu while holding down the Ctrl 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>

Error condition	Probable cause / recommended action
<p>When you click the HDvM - SN menu, a message appears asking you to download the file SJsVlSNStartServlet.do or SJsVlAppStartServlet.do. One minute later, the application error (20020-108000) occurs.</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 HDvM - SN 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"> 1. In Internet Explorer, click Tools > Internet options, and then select the Advanced tab. 2. In the Security section, uncheck Do not save encrypted pages to disk. 3. Click OK.
<ul style="list-style-type: none"> ▪ The application errors (20020-108000 and 10-6027) occur when you click the HDvM - SN menu. ▪ The application error (10-6027) occurs and HDvM - SN terminates when you click the HDvM - SN menu. 	<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"> ▪ Java on the HDvM - SN web client might have failed to start due to timeout. Close all other applications and perform the HDvM - SN operation again. ▪ The version of HDvM - SN 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. ▪ The management client might have entered standby or hibernate mode. Restart the management client.

Error condition	Probable cause / recommended action
	<ul style="list-style-type: none"> ▪ If a proxy server is used for network connections, the proxy cache may be storing the older version of the program. If the problem continues after you clear the Java and web browser caches, contact your network administrator. ▪ The network connection between the SVP and the management client might be blocked by a firewall or some kind of device. <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 HDvM - SN.</p>
When you click the HDvM - SN menu, the system does not respond.	If the problem continues after you perform the operation multiple times, close all the HDvM - SN windows and clear the Java and web browser caches.
The application error (1-7050) occurs when you click the HDvM - SN menu.	The version of HDvM - SN 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.
Java console is grayed out and does not start when you try to open the HDvM - SN secondary window (Java application).	<p>Restart the management client, or terminate the HDvM - SN process with one of the following methods:</p> <ul style="list-style-type: none"> ▪ For Windows: Exit all applications using Java, and then terminate the javaw.exe and javaws.exe applications through Task Manager. ▪ For UNIX: Exit all applications using Java, and then terminate javaw and javaws with the kill command.

Error condition	Probable cause / recommended action
<p>A message box remains displayed when opening the HDvM - SN secondary window (Java application). The HDvM - SN secondary window does not appear for a long time.</p>	<p>Restart the management client, or terminate the HDvM - SN process with one of the following methods:</p> <ul style="list-style-type: none"> ▪ For Windows: Exit all applications using Java, and then terminate the javaw.exe and javaws.exe applications through the Task Manager. ▪ For UNIX: Exit all applications using Java, and then terminate javaw and javaws with the kill command.
<p>A message remains displayed when the HDvM - SN 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 Network Configuration dialog box, which is located in the Java Control Panel's General dialog box.</p>
<p>If you open the Java console dialog box by selecting the Java icon on the system tray while opening the HDvM - SN secondary window (Java application), the browser and Java console may stop responding.</p>	<p>Do not open the Java console dialog box while opening the HDvM - SN secondary window. If the browser and Java console stop responding, restart the management client.</p>
<p>When you click the HDvM - SN 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 HDvM - SN process with one of the following methods: For example:</p> <ul style="list-style-type: none"> ▪ You might have clicked Exit on the Security Warning window. ▪ You might have clicked Cancel on the Warning - Security window. <p>Close all the HDvM - SN 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 HDvM - SN dump file and the Java trace file, and send them to HDvM - SN.</p>

Error condition	Probable cause / recommended action
<p>The following message displays in HDvM - SN.</p> <ul style="list-style-type: none"> ▪ Java has discovered application components that could indicate a security concern. ▪ Block potentially unsafe components from being run. (recommended) ▪ The application contains both signed and unsigned code. Contact the application vendor to ensure that it has not been tampered with. 	<p>Select Yes to continue using HDvM - SN. If the problem continues, the cause may be one of the following:</p> <ul style="list-style-type: none"> ▪ The version of HDvM - SN 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 ▪ 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.
<p>In Internet Explorer, the following pop-up window appears when you open the HDvM - SN 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"> 1. In the Windows menu bar, click Tools > Internet Options, and then click the Advanced tab. 2. In the Advanced tab, clear the Enable third-party browser extensions (requires restart) check box. 3. Restart Internet Explorer.
<p>In Internet Explorer, an application error (10-6027) occurs when you open the HDvM - SN 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"> 1. In the Windows menu bar, click Safety > SmartScreen Filter > Turn Off SmartScreen Filter. 2. Restart Internet Explorer.
<p>When you open the HDvM - SN secondary window, an error (22252-005003) occurs.</p>	<p>This problem might occur when the SVP microcode is updated. Download WCLauncher again.</p>

Error condition	Probable cause / recommended action
<p>In Internet Explorer or Google Chrome, either of the following pop-up windows appears when you open the HDvM - SN secondary window.</p> <p>"Application Blocked by Java Security" or "Application Blocked by Security Settings"</p>	<p>Note: The following Java versions do not allow the HDvM - SN secondary window to display.</p> <ul style="list-style-type: none"> ▪ Java 7 Update 55 or later ▪ Java 8 Update 5 or later <p>To start up the window, you need to change Java security settings.</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"> 1. Open the Java Control Panel. 2. Click Edit Site List on the Security tab. Exception Site List displays. 3. Click Add. 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>). 5. Click OK. If Security Warning - HTTP Location displays, click Continue. 6. Click OK on the Java Control Panel and close the window. 7. Restart your web browser.
<p>When you open the HDvM - SN secondary window, an error (22252-005002) occurs.</p>	<p>This problem might occur when the SVP microcode is updated. Download WCLauncher again.</p> <p>If this problem occurs again, collect the HDvM - SN dump files, the Java logs and trace files, and the WCLauncher logs, and then contact customer support.</p>



Table 5 No response errors

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

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

Error condition	Probable cause / recommended action
<p>One of the following sets of errors occurred when starting the HDvM - SN secondary window.</p> <ul style="list-style-type: none"> ▪ 22252-007007 ▪ 10-6071 	<p>SSL communication from the HDvM - SN management client to the SVP failed due to one of the following causes:</p> <ul style="list-style-type: none"> ▪ The initial SVP certificate was not updated, but server verification is enabled. Update the SVP certificate. Otherwise, disable server verification. ▪ The entered host name or IP address is wrong. Specify the correct host name or IP address, and then run the operation again. ▪ The SVP certificate was updated, but the root certificate or self-signed certificate was not registered on the HDvM - SN management client. Register the root certificate or self-signed certificate on the HDvM - SN management client. ▪ One of the following causes occurred: <ul style="list-style-type: none"> • The root certificate or self-signed certificate that was registered on the HDvM - SN management client is wrong. • The host name or IP address of the SVP is different from the one specified for SAN (subjectAltName) or CN (CommonName) in the SVP server certificate. • The SVP server certificate is expired. • The SVP server certificate is invalidated. • The SVP certificate is signed by an intermediate CA, but only the server certificate is registered on the SVP. <p>Contact the issuer of the certificate to obtain a valid certificate, and then update the SVP certificate.</p> <ul style="list-style-type: none"> ▪ In TLS security settings, the selected cipher suite does not match the certificate key type. Select the cipher suite that matches the TLS security settings.

Table 6 Incorrect display errors

Error condition	Probable cause / recommended action
Only the Exit button and the Refresh and Refresh All commands are effective when accessing the SVP from HDvM - SN.	The SVP might not be ready to perform some write processes from the other system. Wait a few minutes and then click File > Refresh. If the SVP is not restored, click Refresh All.
Only the Exit button and the Refresh All command are effective when accessing the SVP from the HDvM - SN.	An error may have occurred in the SVP. Click File > Refresh All. If the SVP is not restored, log in to HDvM - SN again.
The commands in the Go menu are unavailable.	<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"> ▪ Click File > Refresh. ▪ Click File > Refresh All. ▪ Log in to HDvM - SN again.
When you switch windows from one window to the HDvM - SN window, the HDvM - SN window is not displayed.	Close all windows, and then log in to HDvM - SN again.
The items in a list are not synchronized with a scroll bar.	Click the scroll buttons  or  above and below the scroll bar.
The focus disappears from the edit box.	Close all dialog boxes, and then log in to HDvM - SN again.
The web browser does not display correctly, because some GUI items such as labels and icons cannot be loaded properly.	Log out of HDvM - SN, and then log in again. If this error occurs before you log in to the HDvM - SN, close all dialog boxes and then log in to HDvM - SN.
The characters are unreadable because they are overlapped or garbled.	Log out of HDvM - SN, and then log in again.
The characters are garbled in a window where a tree is displayed.	Click File > Refresh.
Even though you have clicked Apply to change storage system settings, the new settings are not displayed in HDvM - SN.	Click File > Refresh.

Error condition	Probable cause / recommended action
<p>The dialog box that says Loading... stays open for a long period of time.</p>	<p>A HDvM - SN message dialog box other than the dialog box that says Loading... might be displayed behind this window. Press Alt+Tab to switch the dialog box.</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 HDvM - SN windows:</p> <ul style="list-style-type: none"> ▪ Information on the storage system, such as ports or HDDs ▪ Information configured with another management client 	<p>Click File > Refresh. If the problem continues, close all HDvM - SN windows, and then clear the Web browser caches.</p>
<p>The HDvM - SN secondary window does not display.</p>	<ul style="list-style-type: none"> ▪ In the Java Control Panel, click the Temporary Internet Files section. In the Disk Space area, enter 1 MB, and then click Delete Files. ▪ Click Security > Java Control Panel. Ensure that Enable Java content in the browser is checked. ▪ Clear the browser cache. ▪ Ensure that Java Plug-in is enabled. <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>
<p>Even when sever verification is disabled, verification is performed. If this verification fails, a confirmation window appears indicating the following message:</p> <p>"The certificate security verification for the TLS communication cannot be performed. Are you sure you want to stop the certificate security verification to continue the connection?"</p> <p>In this window, the Confirm and Cancel buttons are enabled.</p>	<p>To continue the connection by disabling server verification, click Confirm.</p> <p>To cancel the processing, click Cancel .</p>

Table 7 Other errors

Error condition	Probable cause / recommended action
If you click in a HDvM - SN secondary window while a dialog box is open, the dialog box disappears behind the HDvM - SN secondary window.	Click the dialog box again.
An error occurs because a digital signature or security certificate has expired.	You can continue using HDvM - SN even though the digital signature for the HDvM - SN Java application is expired.
You specify IPv6 communication addresses when you start HDvM - SN, but IPv6 is not being used. Instead, IPv4 is being used and IPv4 addresses are output to audit logs for operations on the HDvM - SN secondary window.	IPv4 has higher priority when both IPv4 communication and IPv6 communication can be used. As a result, IPv4 may be used when you specify IPv6 communication addresses. Also, IPv4 addresses may appear in audit logs.
Communication from the HDvM - SN management client to the SVP fails.	The connection destination might be wrong, or server verification during SSL communication might have failed.
A root certificate of the SVP cannot be registered.	<ul style="list-style-type: none"> ▪ Verify the path to the certificate specified in the security setting command. ▪ Verify that the specified certificate must be in X509 PEM or X509 DER format.
The communications cannot be established from the management client to the SVP.	The connection destination might not be correct or the server verification during the SSL communications might have not been performed.
When you run the delete and list command of the security setting command, the following message is issued: "keytool error: java.lang.Exception: the keystore file does not exist: ExportTool.dat".	Keystore has not been created because the import command of the security setting command has not been run. Run the import command, and then rerun the delete and list command.

HDvM - SN secondary window blocked

If Java 7 Update 55 or later or Java 8 Update 5 or later is installed on the management client, execution of the Device Manager - Storage Navigator secondary window application might be blocked. In this case, use the following procedure to change the Java security settings.

Procedure

1. Check the version and update information of Java installed in your management client.
Click **Start > Control Panel > Java**.

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

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


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 HDvM - SN secondary window \(on page 61\)](#).

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.

Setting storage system information

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

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 **Tasks** 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.

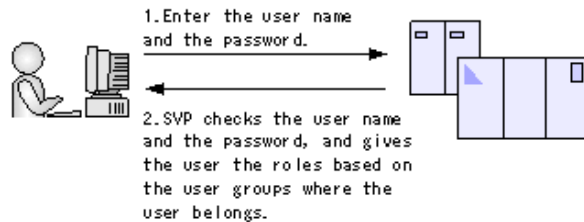
Configure the storage system with the security settings appropriate for your environment.

Managing authentication and authorization servers

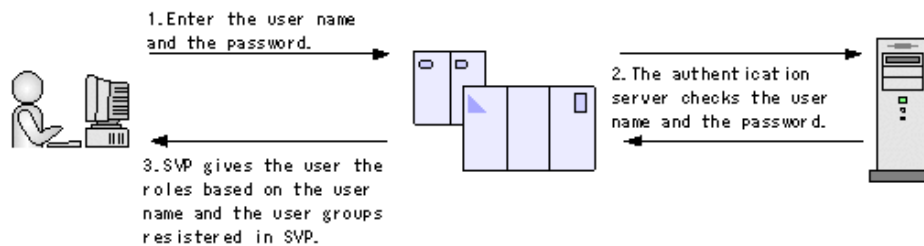
An authentication server enables users to log in to Device Manager - Storage Navigator with the same password as the password that they use for other applications.

The authentication server must be configured for each user.

The following figure shows login workflow without an authentication server:

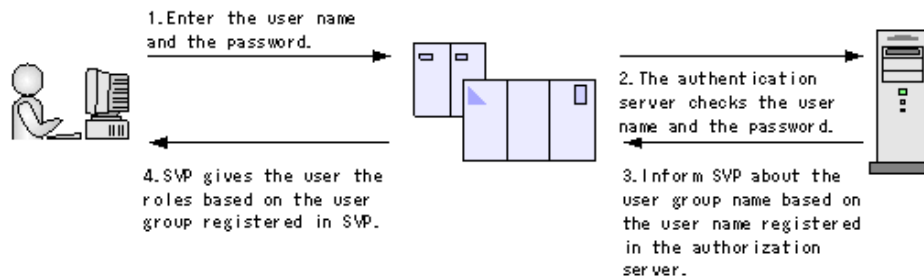


The following figure shows login workflow with an authentication server:



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.



Caution:

- If the affiliated user group registered in the external authentication server and the user group registered locally in the storage system are different, the user group in the storage system has higher priority.
- You cannot create a load balancer between the SVP and the external authentication server.

External authentication requirements using authentication server

Authentication servers support the LDAP, RADIUS, and Kerberos protocols. The following lists explain requirements for each protocol.

LDAP

TLS Security Settings

LDAPv3 simple bind authentication (Note that Bind DN is used for authentication.)

Authentication format

The TLS Security Settings made in Setting SSL communications using Device Manager - Storage Navigator must be supported.

Root certificate file format for Device Manager - Storage Navigator

- X509 DER format
- X509 PEM format

Requirements for root certificate format for Device Manager - Storage Navigator

- If the public key of the certificate to be updated is RSA, the key length must not be less than the key length that is set for **Minimum Key Length (Key Exchange)** in the **TLS Security Settings** dialog box.
- If the public key of the certificate to be uploaded is ECDSA, the public key parameter must be any of the following:
 - ECDSA_P256 (secp256r1)
 - ECDSA_P384 (secp384r1)
 - ECDSA_P521 (secp521r1)
- The signature hash algorithm of the certificate must be SHA-256, SHA-384, or SHA-512.

Requirements for certificate for the connected server

- If the public key of the certificate is RSA, the key length must be 2048 bits or more.
- If the public key of the certificate to be uploaded is ECDSA, the public key parameter must be any of the following:
 - ECDSA_P256 (secp256r1)
 - ECDSA_P384 (secp384r1)
 - ECDSA_P521 (secp521r1)

- The signature hash algorithm of the certificate must be SHA-256, SHA-384, or SHA-512.
- The extended profile fields in the X.509 certificate support the following items as specified in RFC5280:
 - subjectAltName
 - CRLDistributionPoint
 - AuthorityInfoAccess
 - BasicConstraints
 - KeyUsage
 - SubjectKeyIdentifier

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

- When setting an IP address for **Primary Host Name** or **Secondary Host Name** in the **Setup Server** window (Settings > User Management > View External Authentication Server Properties > Setup Server), enter the IP address of the server in *subjectAltName* or *CommonName* of the server certificate.
- When using DNS Lookup to connect to an external authentication server, enter the host name of the server in *subjectAltName* or *CommonName* of the server certificate.
- When you perform a certificate revocation check by using CRL, set the URI of the CRL repository for *cRLDistributionPoint* (CRL distribution point) of the intermediate certificate and server certificate set on the connected server. The CRL repository must be on the network that can be accessed by the SVP so that the SVP can communicate with the CRL repository. If the SVP cannot communicate with the CRL repository, external authentication fails.
- When you perform a certificate revocation check by using OCSP, correctly set the URI of the OCSP responder for *authorityInfoAccess* (Authority Information Access) of the intermediate certificate and server certificate set on the connected server. The OCSP responder must be on the network that can be accessed by the SVP so that the SVP can communicate with the OCSP responder. If the SVP cannot communicate with the OCSP responder, external authentication fails.
- If no DNS server is used, the IP address of the authentication server must be specified for the common name of the certificate.
- Check the number of tiers of the certificate chain to be used. The maximum number supported is 20 tiers. Make sure to use a certificate in a certificate chain with no more than 20 tiers.



Note:

- Acquire the root certificate for the authentication server from the authentication server administrator.
- The certificates has an expiration date. If the certificate expires, you will not be able to connect to the authentication server. Make sure to update the certificate before the expiration date.
- For more information about the certificate management, contact the key management server administrator.

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. For the secondary server, use the same configuration settings as the primary server, except for the host name and the port number.
- If you search for a server using information registered in the SRV records in the DNS server, confirm that the following conditions are satisfied. For RADIUS servers, you cannot use the SRV records.

LDAP server conditions:

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

Kerberos server conditions:

- The host name, port number, and domain name of the Kerberos server are registered in the DNS server.
- Because UDP/IP is used to access the RADIUS server, encrypted communications, including negotiation between processes, are not used. To access the RADIUS server in a secure environment, encryption in the packet level, such as IPsec, is required.
- If you use Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 as an authorization server, the SSL communications might fail by using DHE in the default settings. When you use any of these servers as the authentication server, configure the SSL communication settings by using Device Manager - Storage Navigator to disable the cipher suites that use DHE for key exchange.

External authorization requirements using authorization server

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



Note: Use an operating system that continues to be supported by a vendor. Operations performed using firmware for which vendor support has expired cannot be guaranteed.

Prerequisite OS

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

Prerequisite software

- Active Directory

Authentication protocol for user for searching

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

TLS Security Settings

- The TLS Security Settings made in Setting SSL communications using Device Manager - Storage Navigator must be supported. For the default TLS Security Settings, see [Setting up SSL encryption using Device Manager - Storage Navigator \(on page 90\)](#).

Root certificate file format for Device Manager - Storage Navigator

- X509 DER format
- X509 PEM format

Requirements for root certificate format for Device Manager - Storage Navigator

- If the public key of the certificate to be uploaded is RSA, the key length must not be less than the key length that is set for Minimum Key Length (Key Exchange) in the TLS Security Settings dialog box.
- If the public key of the certificate to be uploaded is ECDSA, the public key parameter must be any of the following:
 - ECDSA_P256 (secp256r1)
 - ECDSA_P384 (secp384r1)
 - ECDSA_P521 (secp521r1)
- The signature hash algorithm of the certificate must be SHA-256, SHA-384, or SHA-512.

Requirements for certificate for the connected server

- If the public key of the certificate is RSA, the key length must be 2048 bits or more.

- If the public key of the certificate to be uploaded is ECDSA, the public key parameter must be any of the following:
 - ECDSA_P256 (secp256r1)
 - ECDSA_P384 (secp384r1)
 - ECDSA_P521 (secp521r1)
- The signature hash algorithm of the certificate must be SHA-256, SHA-384, or SHA-512.
- The extended profile fields in the X.509 certificate support the following items as specified in RFC5280:
 - subjectAltName
 - CRLDistributionPoint
 - AuthorityInfoAccess
 - BasicConstraints
 - KeyUsage
 - SubjectKeyIdentifier

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

- When setting an IP address for **Primary Host Name** or **Secondary Host Name** in the **Setup Server** window (Settings > User Management > View External Authentication Server Properties > Setup Server), enter the IP address of the server in *subjectAltName* or *CommonName* of the server certificate.
- When using DNS Lookup to connect to an external authentication server, enter the host name of the server in *subjectAltName* or *CommonName* of the server certificate.
- When you perform a certificate revocation check by using CRL, set the URI of the CRL repository for *cRLDistributionPoint* (CRL distribution point) of the intermediate certificate and server certificate set on the connected server. The CRL repository must be on the network that can be accessed by the SVP so that the SVP can communicate with the CRL repository. If the SVP cannot communicate with the CRL repository, communication with the authorization server fails.
- When you perform a certificate revocation check by using OCSP, correctly set the URI of the OCSP responder for *authorityInfoAccess* (Authority Information Access) of the intermediate certificate and server certificate set on the connected server. The OCSP responder must be on the network that can be accessed by the SVP so that the SVP can communicate with the OCSP responder. If the SVP cannot communicate with the OCSP responder, communication with the authorization server fails.
- The number of tiers of the certificate chain for the certificate to be uploaded must be 20 tiers or less including the root CA certificate.

- If no DNS server is used, the IP address of the authorization server must be specified for the common name of the certificate.
- Check the number of tiers of the certificate chain to be used. The maximum number supported is 20 tiers. Make sure to use a certificate in a certificate chain with no more than 20 tiers.



Note:

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



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

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

If you use Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 as an authorization server, the SSL communications might fail by using DHE in the default settings. When you use any of these servers as the authorization server, configure the SSL communication settings by using Device Manager - Storage Navigator to disable the cipher suites that use DHE for key exchange.

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 the 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 > User Management > 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.



Note: When the SVP High Reliability Kit is used, the settings are automatically linked to the standby SVP.

Setting up SSL encryption using Device Manager - Storage Navigator

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

In the communication between the Device Manager - Storage Navigator operating PC and the SVP, the SSL/TLS communication settings are applied to the communication of the following protocols and port numbers.

Protocol	Port Number
HTTPS	443
RMI	11099
RMI	51100
SMI-S	5989
HTTPS (raidinf)	5443

When the following servers are used, the above SSL/TLS communication settings are applied to the communication between these servers and the SVP by using TLS Security Settings In the Tool Panel dialog box.


- Syslog Server
- Key management server
- External authentication or authorization server
- Hitachi Command Suite server


The user with the Security Administrator (View & Modify) role can configure the following security settings used for the SSL/TLS communications with the SVP by using the **Tool Panel** dialog box on Device Manager - Storage Navigator:


- Protocol
- Cipher suites
- Minimum key length of keys used for key exchange
- Enabling renegotiation


Device Manager - Storage Navigator must satisfy the following security requirements:

- Protocol
 - TLS1.2
 - TLS1.3
- Cipher suites
 - Cipher suites supported by TLS1.2
 - TLS_RSA_WITH_AES_128_CBC_SHA
 - TLS_RSA_WITH_AES_128_CBC_SHA256
 - TLS_RSA_WITH_AES_256_CBC_SHA256
 - TLS_RSA_WITH_AES_256_GCM_SHA384
 - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
 - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 - Cipher suite supported by TLS1.3
 - TLS_AES_128_GCM_SHA256
 - TLS_AES_256_GCM_SHA384
- Minimum key length supported by key exchange algorithm
 - RSA: Supports the key length of 2048 bits, 3072 bits, or 4096 bits. It can be used when TLS1.2 is enabled.
 - DHE: Supports the key length of 2048 bits. It can be used when TLS1.2 or TLS1.3 is enabled.
 - ECDHE: Supports elliptic curve parameters of secp256r1, secp384r1, or secp521r1. It can be used when TLS1.2 or TLS1.3 is enabled.
- Enabling renegotiation
 - It can be used when TLS1.2 is enabled, however it is recommended to disable renegotiation.

 **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 \(on page 104\)](#).

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

 **Note:** The minimum key length supported by the key exchange algorithm set on the TLS Security Setting dialog box in the Tool Panel dialog box is applied when a certificate with RSA public key is set during the communications between the management client and the SVP.

When the following cipher suites are valid, and when a server certificate, root certificate, or client certificate with an RSA public key is uploaded to the SVP, the key length of the RSA public key of the certificate must be longer than the key length selected on the TLS Security Setting dialog box in the Tool Panel dialog box.

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

When the SVP communicates with a Syslog server, key management server, external authentication and authorization server, or Hitachi Command Suite server, the key length of the key exchange key set on the server must satisfy the following:

- RSA: 2048 bits or more
- DHE: 2048 bits
- ECDHE: secp256r1, secp384r1, or secp521r1

SSL terminology

Note the following SSL terms:

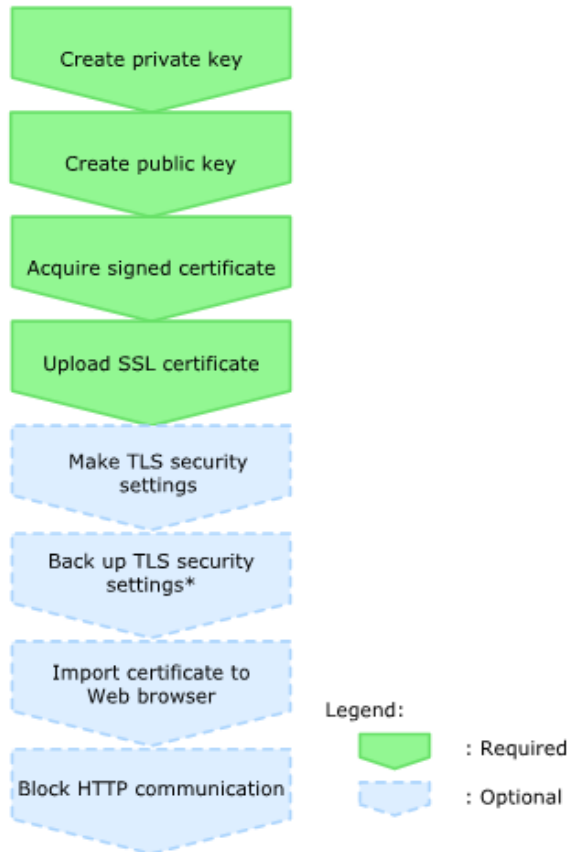
- **Secure Sockets Layer:** SSL is a protocol first developed by Netscape to securely transmit data over the Internet. Two SSL-enabled peers use their private and public keys to establish a secure communication session, with each peer encrypting transmitted data with a randomly generated and agreed-upon 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 owned 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/>).



*It is required if you make the TLS security settings.

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 8.1 as an example.

Creating a private key using the OpenSSL command

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

Before you begin

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



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

Procedure

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

For RSA

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

For ECDSA

```
C:\key>c:\openssl\bin\openssl ecparam -genkey -name key-length -out server.key
```

For `key-length`, you can specify either of the following:

For RSA: 2048, 3072, or 4096

For ECDSA: prime256v1 (secp256r1), secp384r1, or secp521r1

Example command input:

- When the key type is RSA and the key length is 2048 bit:

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

- When the key type is ECDSA and the key length is 256 bit (secp256r1):

```
C:\key>c:\openssl\bin\openssl ecparam -genkey -name prime256v1 -out server.key
```

Creating a public key using the OpenSSL command

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

Before you begin

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

Procedure

1. Open a command prompt with administrator permissions.
2. 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
```



Note: This command uses SHA-256, SHA-384, or SHA-512 as a hash algorithm. MD5 or SHA-1 is not recommended for a hash algorithm due to its low security level.

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.
 - If you update SSL certificates in a batch, conversion is not required.

Procedure

1. Open a command prompt with administrator permissions.
2. Enter the following command: 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 \(on page 98\)](#).
- 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 \(on page 98\)](#).



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.

Creating private and public keys using the Tool Panel dialog box

You can create a CSR (public key), private key, and self-signed certificate using the **Tool Panel** dialog box. If you want the certificate authority to issue a certificate, create a CSR and private key, and then send the CSR to the certificate authority.

**Caution:**

- Creating private and public keys take approximately 6 seconds, which differs depending on your environment.
- Do not use the CSR created in this procedure, the certificate created using the private key, and the self-signed certificate created in this procedure for the purposes other than Device Manager - Storage Navigator.

Before you begin

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

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 **Create CSR and Self-Signed Certificate**. The **Create CSR and Self-Signed Certificate** login dialog box opens.

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**.

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**.
4. In the **Create CSR and Self-Signed Certificate** login dialog box, enter the administrator user ID and password, and click **Login**. The **Create CSR and Self-Signed Certificate** dialog box opens.
5. In the **Create CSR and Self-Signed Certificate** dialog box, enter the required items. After you have completed the entries, perform either of the following operations depending on whether you create a self-signed certificate.
 - When you create a self-signed certificate, go to step 6 without clicking **Create CSR File and Key File**.
 - When you do not create a self-signed certificate, go to step 7 after clicking **Create CSR File and Key File**.

6. If you create a self-signed certificate, select the check box for **Create Self-Signed Certificate**.

In the **Profile** field, select either of **Default** or **Custom**:

- **Default**: If you select **Default**, 365 days is set as the validity period of the certificate, and SHA-256 is set as the hash algorithm of the certificate. If you can accept the default settings, click **Create Self-Signed Certificate File**.
- **Custom**: If you select **Custom**, the .cfg file allows you to specify the number of days that the self-signed certificate is valid and the hash algorithm. Click **Browse** to select the .cfg file, and then click **Create Self-Signed Certificate File**. See **Create CSR and Self-Signed Certificate** dialog box.



Note: It is recommended that the self-signed certificate be valid for less than 825 days (27 months).

7. After step 5 or step 6 is complete, the **Download File** window is displayed.
Click **Save**, and then confirm that the created self-signed certificate file is stored in the specified folder.
8. In the **Create CSR and Self-Signed Certificate** dialog box, click **Close**. The **Create CSR and Self-Signed Certificate** dialog box is closed, and then the **Tool Panel** dialog box is displayed.

Releasing an SSL certificate passphrase

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

Before you begin

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

Procedure

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



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

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

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

Example (when passphrase is set)

- When the key type is RSA:

```
C:\key>C:\openssl\bin\openssl rsa -in server.key -out server.key
Enter pass phrase for server.key:
```

- When the key type is ECDSA:

```
C:\openssl\bin\openssl ec -in server.key -out server.key
read EC key
Enter PEM pass phrase:
```

Example (when passphrase is not set)

- When the key type is RSA:

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

- When the key type is ECDSA:

```
C:\openssl\bin\openssl ec -in server.key -out server.key
read EC key
writing EC 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`.
- 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`.
- You must be an external authentication user whose external user group mapping is disabled, or a local authentication user.
- If the public key of the certificate to be uploaded is RSA, the key length must not be less than the key length that is set for **Minimum Key Length (Key Exchange)** in the **TLS Security Settings** dialog box.

- The signature hash algorithm of the certificate to be uploaded must be SHA-256, SHA-384, or SHA-512.
- The extended profile fields in the X.509 certificate support the following items as specified in RFC5280:
 - subjectAltName
 - CRLDistributionPoint
 - AuthorityInfoAccess
 - BasicConstraints
 - KeyUsage
 - SubjectKeyIdentifier

Enter the host name or the IP address of the SVP in *subjectAltName* or *CommonName* of the certificate to be uploaded.

- If the public key of the certificate to be uploaded is ECDSA, the public key parameter must be any of the following:
 - ECDSA_P256 (secp256r1)
 - ECDSA_P384 (secp384r1)
 - ECDSA_P521 (secp521r1)
- When you perform a certificate revocation check by using CRL, set the CRL repository URI for the cRLDistributionPoint (CRL distribution point) of the intermediate certificate and server certificate.
- When you perform a certificate revocation check by using OCSP, set the OCSP responder URI for authorityInfoAccess (Authority Information Access) of the intermediate certificate and server certificate.
- When you perform a certificate revocation check on the management client, the CRL repository or the OCSP responder must be on the network that can be accessed by the management client so that they can be accessed by the management client. If the management client cannot communicate with the CRL repository or the OCSP responder, the connection to Device Manager - Storage Navigator is established without certificate revocation check.
- If an intermediate certificate exists, prepare a signed public key certificate file (server.crt) that has a certificate chain that includes the intermediate certificate.
- The number of tiers of the certificate chain for the certificate to be uploaded must be 20 tiers or fewer including the root CA certificate.

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 dialog box, confirm the messages about a possible TLS communication failure and recommendations, and then select the check box for **I understood that I canceled HTTP blocking or TLS communication might fail**.
7. In the **Upload** dialog box, click **Upload**. A confirmation dialog box opens.
8. 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.
9. 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 \(on page 101\)](#) to default.

Before you begin

- You must have the Storage Administrator (Initial Configuration) role to perform this task.
- You must be an external authentication user whose external user group mapping is disabled, or a local authentication user.

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 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 **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**.

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.
- You must be an external authentication user whose external user group mapping is disabled.

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.
- You must be an external authentication user whose external user group mapping is disabled.

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.

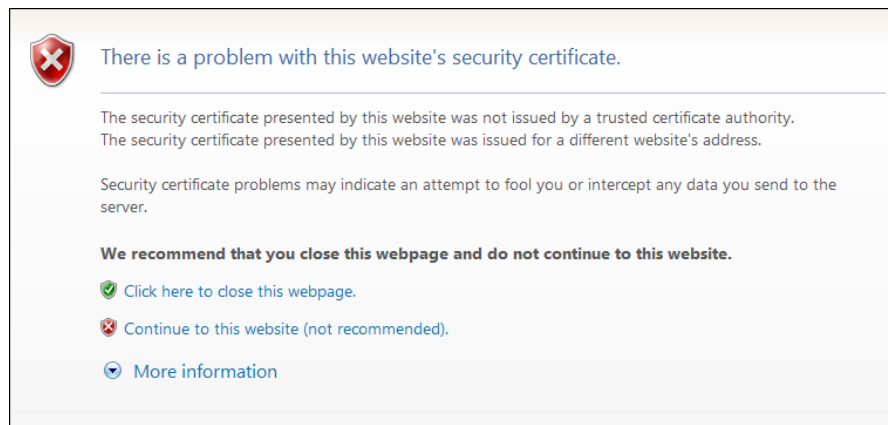

```
https://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi
```
3. In the **Tool Panel** dialog box, click **Release HTTP Blocking**.
4. Enter the User ID and Password for the root storage administrator, then click **Login**. The **Release HTTP Blocking** dialog box opens.
5. Click **OK**. 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.

Problems with a website security certificate

If the following security warning appears, take the actions in accordance with the warning messages. If no action is taken, verify the security certificate sent from the server and make sure that the connection destination is the SVP as expected. After confirmation, click Continue to this website (not recommended).

- If this security warning appears after the microprogram replacement, the SSL certificate has been returned to default. In this case, upload the original SSL certificate. For more information, see [Uploading a signed certificate \(on page 101\)](#).
- The message of "The security certificate presented by this website was not issued by a trusted certificate authority." appears if the security certificate is not issued by a trusted certificate authority when connecting to an SSL-enabled Hitachi Device Manager - Storage Navigator. Register the root certificate in the trusted root certificate authority in the browser.
- The message of "The security certificate presented by this website was issued for a different website's address." appears if an IP address or a host name specified in the URL does not match the CN (Common Name) or subjectAltName described in the security certificate. Verify that the CN (Common Name) or subjectAltName described in the security certificate is the same as the IP address or host name specified in the URL when connecting to Hitachi Device Manager - Storage Navigator. If it is not the same, see [Registering the SVP host name \(on page 27\)](#).



Setting SSL/TLS communications using Device Manager - Storage Navigator

Use the following procedure to create the security settings used for SSL/TLS communications with the SVP.

**Caution:**

- If an SSL/TLS communication setting is not correct, SSL/TLS communication with the SVP might fail. If SSL communication fails, you need to configure the security settings again using the **Tool Panel** dialog box by using HTTP connection. Therefore, it is recommended to release the HTTP communication blocking using the **Tool Panel** dialog box before making security settings. For more information about how to release the HTTP communication blocking, see [Releasing HTTP communication blocking \(on page 105\)](#).
- When you perform this procedure, use HTTPS connection for access. If you access via an HTTP connection, the ID and password used for login are communicated in clear text.

Before you begin

- Verify the security settings of the SVP communication destination before the setting. If the protocol is TLS1.3 only, make sure that the communication destination supports TLS1.3.
If you use Device Manager - Storage Navigator with Adobe AIR, you must enable TLS1.2. Adobe AIR does not support TLS1.3.
- Verify that no other management or maintenance operations are being performed on Device Manager - Storage Navigator.
- You must have Security Administrator (View & Modify) role to perform this task.

Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. On the management client, open a web browser, and then type the following URL to open the **Tool Panel** dialog box by using HTTPS connection.
`https://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi`
3. In the **Tool Panel** dialog box, click **TLS Security Settings** to open the **TLS Security Settings** login dialog box.
If SSL/TLS communication has been established, the **Security Alert** dialog box opens before the login dialog box opens. In the **Security Alert** dialog 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 then click **Yes**.
4. In the **TLS Security Settings** login dialog box, enter the administrator user ID and password, and then click **Login**.
5. In the **TLS Security Settings** dialog box, enter the required items.



Caution: When using TLS1.2, select the cipher suites corresponding to the key type of the certificate uploaded to the SVP.

- If the key type is RSA, select a cipher suite whose name contains “RSA”.
- If the key type is ECDSA, select a cipher suite whose name contains “ECDSA”.

If the cipher suites are not set correctly, the SSL/TLS communications with the SVP fail, and then a problem, such as a Device Manager - Storage Navigator login error, occurs.

When using TLS1.3, you can select both cipher suites regardless of whether the certificate key type is RSA or ECDSA.

6. In the **TLS Security Settings** dialog box, confirm the messages about the possible TLS communication failures and recommendations, and then select the check box for **I understand that I canceled HTTP blocking or TLS communication might fail**.
7. Click **Next** to perform a communication test. The **Communication Test** dialog box for **TLS Security Settings** opens.
8. The communication test using the security settings specified in step 5 starts automatically for the following communication paths:
 - SVP – Syslog Server
 - SVP – Key Management Server
 - SVP – LDAP Server
 - SVP – HCS server
9. Verify the results of the communication test for each communication path performed in the previous step. In the Communication Test dialog box for **TLS Security Settings**, wait until any of the following is displayed as the communication test result:
 - Normal: Communication is complete correctly.
 - Skipped: Connection settings are not made on Device Manager - Storage Navigator.
 - Error : Communication failed.
10. Confirm the communication test result, and then click **Submit** in the **Communication Test** dialog box for TLS Security Settings.
11. When prompted if you are sure you want to change the settings, click **OK**.
The SVP web server restarts to reflect the security settings. When the SVP Web server restart is complete, the setting completion dialog box for **TLS Security Settings** opens.
12. Click **OK** to return to the login dialog box.
13. Back up the new security settings. For details, see [Backing up HDvM - SN configuration files \(on page 124\)](#).

Configuring certificates for HCS

When you want to manage the storage system by using Hitachi Command Suite and perform the HCS external authentication, you need to register the certificate for HCS on the SVP.

When you want to manage the storage system by linking Hitachi Ops Center Administrator and Hitachi Device Manager - Storage Navigator (HDvM - SN), you need to register the certificate for Hitachi Ops Center Administrator on the SVP.

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

Registering certificates for HCS

To manage the storage system by using HCS and perform the 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.
- You must be an external authentication user whose external user group mapping is disabled, or a local authentication user.
- If the public key of the certificate to be uploaded is RSA, the key length must not be less than the key length that is set for Minimum Key Length (Key Exchange) in the **TLS Security Settings** dialog box.
- If the public key of the certificate to be uploaded is ECDSA, the public key parameter must be any of the following:
 - ECDSA_P256 (secp256r1)
 - ECDSA_P384 (secp384r1)
 - ECDSA_P521 (secp521r1)
- The signature hash algorithm of the certificate to be uploaded must be SHA-256, SHA-384, or SHA-512.

- The extended profile fields in the X.509 certificate support the following items as specified in RFC5280:
 - `subjectAltName`
 - `CRLDistributionPoint`
 - `AuthorityInfoAccess`
 - `BasicConstraints`
 - `KeyUsage`
 - `SubjectKeyIdentifier`

Enter the host name or the IP address of the server in *subjectAltName* or *CommonName* of the certificate for the connected server.

- The number of tiers of the certificate chain for the connected server certificate must be 20 tiers or less including the root CA certificate.

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, the storage system is not managed by using HCS and HCS external authentication is not performed.
- Only with registration of the correct certificate, the storage system is managed by using HCS and HCS external authentication operates normally.
- When you perform a certificate revocation check by using CRL, set the URI of the CRL repository for `cRLDistributionPoint` (CRL distribution point) of the intermediate certificate and server certificate set on the connected server. The CRL repository must be on the network that can be accessed by the SVP so that the SVP can communicate with the CRL repository. If the SVP cannot communicate with the CRL repository, HCS external authentication fails.
- When you perform a certificate revocation check by using OCSP, correctly set the URI of the OCSP responder for `authorityInfoAccess` (Authority Information Access) of the intermediate certificate and server certificate set on the connected server. The OCSP responder must be on the network that can be accessed by the SVP so that the SVP can communicate with the OCSP responder. If the SVP cannot communicate with the OCSP responder, HCS external authentication fails.

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, HCS external authentication cannot be performed.

Before you begin

- You must have the Security Administrator (View & Modify) role to perform this task.
- You must be an external authentication user whose external user group mapping is disabled, or a local authentication user.

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**.

Reporting failure information about storage systems

You can report failure information (SIM) about storage systems through Syslog, SNMP trap, and email. Failure information reported through email is the same as SIM displayed on the **Alert** window or reported through SNMP trap. For SNMP trap, the user needs to access the SNMP Manager to check for failure. However, for report through Syslog or email, the user has only to check Syslog or email to know about the occurrence of failure. See the *Hitachi Alert Notification Guide* for methods of notification with SNMP traps.

Requirements of the Syslog protocol (TLS1.2/RFC5424)

The Syslog protocol (TLS1.2/RFC5424) requires the following:

- Operation confirmed Syslog server which supports TLS1.2.
- The server supports communications using the TLS Security Settings that is set in accordance with the procedure in Setting up SSL communications.
- Server certificate that has been set on the Syslog server

The server certificate that meets the following requirements can be used:

Certificate type	Requirements
Server certificate of Syslog server	<ul style="list-style-type: none"> ▪ If the public key of the certificate is RSA, the key length must be 2048 bits or more. ▪ If the public key of the certificate is ECDSA, the public key parameter must be any of the following: <ul style="list-style-type: none"> • ECDSA_P256 (secp256r1) • ECDSA_P384 (secp384r1) • ECDSA_P521 (secp521r1) ▪ The signature hash algorithm of the certificate must be SHA-256, SHA-384, or SHA-512.

Certificate type	Requirements
	<ul style="list-style-type: none"> ▪ The extended profile fields in the X.509 certificate support the following items as specified in RFC5280: <ul style="list-style-type: none"> • subjectAltName • CRLDistributionPoint • AuthorityInfoAccess • BasicConstraints • KeyUsage • SubjectKeyIdentifier <p>The IP address of the Syslog server must be entered in subjectAltName or CommonName. Domain name cannot be specified.</p> ▪ When you perform a certificate revocation check by using CRL, set the URI of the CRL repository for cRLDistributionPoint (CRL distribution point) of the intermediate certificate and the server certificate that have been set on the connected server. The CRL repository must be on the network that can be accessed by the SVP so that the SVP can communicate with the CRL repository. If the SVP cannot communicate with the CRL repository, the communications with the Syslog server fails. ▪ When you perform a certificate revocation check by using OCSP, correctly set the URI of the OCSP responder for authorityInfoAccess (Authority Information Access) of the intermediate certificate and the server certificate that have been set on the connected server. The OCSP responder must be on the network that can be accessed by the SVP so that the SVP can communicate with the OCSP responder. If the SVP cannot communicate with the OCSP responder, the communications with the Syslog server fails. ▪ Check the number of tiers of the certificate chain to be used. The maximum number supported is 20 tiers. Make sure to use a certificate in a certificate chain with no more than 20 tiers.

- Root certificate of the Syslog server

The root certificate that meets the following requirements can be uploaded to the SVP.

Certificate type	Requirements
Certificate format	<ul style="list-style-type: none"> ▪ X509 DER format ▪ X509 PEM format
Root certificate	<ul style="list-style-type: none"> ▪ If the public key of the certificate to be uploaded to the SVP is RSA, the key length must not be less than the key length that is set for Minimum Key Length (Key Exchange) in the TLS Security Settings dialog box. ▪ If the public key of the certificate to be uploaded to the SVP is ECDSA, the public key parameter must be any of the following: <ul style="list-style-type: none"> • ECDSA_P256 (secp256r1) • ECDSA_P384 (secp384r1) • ECDSA_P521 (secp521r1) ▪ The signature hash algorithm of the certificate to be uploaded to the SVP must be SHA-256, SHA-384, or SHA-512

- Client certificate

The client certificate that meets the following requirements can be uploaded to the SVP.

Certificate type	Requirements
Certificate format	PKCS#12 format
TLS security settings	The server supports communications using the TLS Security Settings that is set in accordance with the procedure in Setting up SSL communications. For more information about the default TLS Security Settings, see Setting up SSL encryption using Device Manager - Storage Navigator (on page 90) .
Client certificate	<ul style="list-style-type: none"> ▪ If the public key of the certificate to be uploaded to the SVP is RSA, the key length must not be less than the key length that is set for Minimum Key Length (Key Exchange) in the TLS Security Settings dialog box. ▪ If the public key of the certificate to be uploaded to the SVP is ECDSA, the public key parameter must be any of the following: <ul style="list-style-type: none"> • ECDSA_P256 (secp256r1) • ECDSA_P384 (secp384r1) • ECDSA_P521 (secp521r1) ▪ The signature hash algorithm of the certificate to be uploaded to the SVP must be SHA-256, SHA-384, or SHA-512. ▪ If an intermediate certificate exists, you must prepare a signed public key certificate in a certificate chain that contains the intermediate certificate. ▪ The number of tiers of the certificate chain for the certificate to be uploaded must be 20 tiers or less including the root CA certificate.

Convert the client certificate signed by a CA (Certificate Authority) on the Syslog server to the PKCS#12 format. For more information, see [Obtaining a client certificate for the Syslog protocol \(on page 116\)](#)

If you do not know the password of the client certificate in the PKCS#12 format, contact the Syslog server administrator.



Caution:

- The certificates have expiration dates. If a certificate expires, you will not be able to connect to the Syslog server. Make sure to update the certificate before the expiration date.
- For more information about the certificate management, contact the Syslog server administrator.

Obtaining a client certificate for the Syslog protocol

You must obtain a client certificate from the SVP to enable the Syslog protocol.

Procedure

1. Create a private key (.key file). See [Creating a private key using the OpenSSL command \(on page 95\)](#).
2. Create a public key (.csr file). See [Creating a public key using the OpenSSL command \(on page 96\)](#).
3. Send the new key to the Syslog server Certificate Authority for signature to obtain a certificate. The certificate is used as the client certificate.



Caution: If the certificate expires, you cannot connect to the Syslog server.

4. Open a Windows command prompt, and then set the current directory to the directory where the PKCS#12 format client certificate is output.
5. Store the private key (.key file) and client certificate in this folder, and then execute the command below.

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

Where

- Folder to which the PKCS#12 format client certificate is output: C:\key
 - File name of the private key: client.key
 - File name of the client certificate: client.crt
6. Set the password.

You can use a password of up to 128 alphanumeric characters and 31 of the following symbols:

```
! # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` { | } ~
```

If you use more than 50 letters, use the following command option example, where XXXX...X is the password:

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

Changing advanced system settings

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

Before you begin

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

Procedure

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

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

Option	Description
	that has the user capacity (greater than 4,194,304 MB) when a new TC/TCMF/UR/URMF/GAD pair using the DP-VOL is created.
Manage differential bitmaps in DP pool at pair create operations for 4TB or less TC/TCMF/UR/URMF/GAD pairs	When enabled, the differential data is maintained in a pool with which a DP-VOL that has the user capacity (up to 4,194,304 MB) is linked when a new TC/TCMF/UR/URMF/GAD pair is created using the DP-VOL. Note that differential data is maintained, regardless of this setting, in a pool linked with the DP-VOL that has the user capacity (greater than 4,194,304 MB) when a new pair using the DP-VOL is created.
External Authentication Compatibility option	If you enable this option, the authentication method is switched from VSP 5000 series to VSP.
Enable reboot of background service	<p>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.</p> <ul style="list-style-type: none"> ▪ The amount of memory used in the background service process. ▪ Time elapsed after the background service process is started.
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> .
The consistency time of a Hitachi Universal Replicator software for Mainframe pair shows the time stamp of the data that has just been copied to a restored journal volume	When enabled, the time included in the time stamp of the data that has just been copied to a restored journal volume shows the consistency time.
After delta resync, the pair status remains COPY during journal data copy	If you enable this option, when a delta resync is performed in a 3DC multi-target configuration with TC and UR, the pair status remains COPY during journal data copy.
One minute after remote path failure detection, the mirror is split	If you enable this option, when a remote path failure is detected, the mirror is split if the remote path is not restored within one minute after the detection.

Option	Description
	This setting is enabled only when After remote path failure detection, the mirror is split is enabled. When No. 16 is disabled, the mirror is not split even if a remote path failure is detected.
After remote path failure detection, the mirror is split	When enabled, after a remote path failure is detected, the mirror is split.
The copy pace for mirror option (Medium) becomes one level faster	When enabled, the pace for copying data during initial copy becomes one level faster when the copy pace for journal option is Medium. This item can be used to make the initial copy operation in Medium speed mode perform faster
The copy pace for mirror option (Medium) becomes two level faster	When enabled, the pace for copying data during initial copy becomes two levels faster when the copy pace for journal option is Medium. This item can be used to make the initial copy operation in Medium speed mode perform faster.

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

Updating Storage Device Launcher on the management client

The Storage Device Launcher software on the HDvM - SN management client is not automatically updated. If the Storage Device Launcher version on the SVP is updated (for example, when the SVP firmware is updated), you must download the Storage Device Launcher setup file from the SVP and install the updated Storage Device Launcher software on the HDvM - SN management client.

Use the following procedure to check the Storage Device Launcher version on the management client and SVP. If the versions are different, update the Storage Device Launcher software on the management client.

Procedure

1. Check the Storage Device Launcher version on the management client: In the **Start** menu, select **Storage Device Launcher** to open the **Storage Device Launcher** window.

The **Storage Device Launcher** window displays the Storage Device Launcher version on the management client.

2. Check the Storage Device Launcher version on the SVP by clicking **Tool > Download** to open the download dialog box.

The download dialog box displays the Storage Device Launcher version on the SVP. If the version on the SVP is not the same as the version on the management client, download Storage Device Launcher from the SVP and install it on the management client. For instructions, see [Installing Storage Device Launcher on the management client \(on page 31\)](#).

Updating Captive Bundle Application on the SVP

If Captive Bundle Application (CBA) on the SVP needs to be updated, you need to upload CBA from the management client to the SVP.



Note: Do not remove CBA on the management client before updating CBA on the SVP. If you need to increase the available free space on the management client, you can remove all files stored in the following location while HDvM - SN is not running: `Storage_Device_Launcher_installation_directory\WCLauncher\SDLauncher\micro`.

Before you begin

- You must have the CBA file to be uploaded to the SVP on the management client. If you do not have the CBA file, contact customer support.
- You must have the Security Administrator (View & Modify) role to perform this task.

Procedure

1. On the management client, open a web browser.
2. Open the **Tool Panel** dialog box by specifying the following URL:

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

3. Click **CaptiveBundleUpload**.
4. Enter the administrator user ID and password, and then click **Login**.
5. Click **Browse**, navigate to and select the CBA file on the management client, and then click **Upload**.
 - If the CBA version to be uploaded is earlier than the CBA version on the SVP, a message asking if you want to downgrade CBA is displayed. If you are sure about downgrading the CBA version, click **OK** to continue. If you are not sure, click **Cancel** to cancel the upload, and then contact customer support.
 - If the SVP firmware version and the CBA version to be uploaded are not compatible, a message is displayed. Click **OK** to cancel the upload, and then contact customer support.
6. Verify the CBA version on the SVP and the CBA version to be uploaded, and then click **OK** to upload CBA to the SVP.

Wait up to 10 minutes for the upload to complete.

- When the version confirmation message is displayed, click **OK**.

You are returned to the **Login** dialog box.

If the **Security Alert** dialog box for the certificate opens before you are returned to the **Login** dialog box, click **View Certificate**, verify that the certificate is correct, and then click **Yes**.



Caution: On the management client, do not delete the CBA file that you uploaded to the SVP. This CBA file might be required for SVP failure recovery or other purposes.

- Log in to HDvM - SN by using AIR, and then verify that the CBA version in the **Storage Systems** window is correct (same as the CBA version you uploaded).

Backing up and restoring HDvM - SN configuration files

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

The following table lists the backup file items that have SVP version requirements. If you need to restore these settings on an SVP that does not meet the minimum SVP version requirement, first download the configuration file without selecting these backup file items, perform the restore operation using the configuration file, and then perform the operation in the following table to restore these settings.

Backup file item	Minimum SVP version	Operation to restore the setting
Flash Disable File	90-04-0x	None (not applicable).
SIMSyslog Transfer Information	90-04-0x	Configure the SIMSyslog transfer settings on the Syslog tab of the Edit Alert Settings window.
TLS Security Settings	90-02-0x	Configure the TLS settings.

The following table lists the items that are not backed up and provides the required action to save and re-register each item.

Item	Action
Configuration reports of the storage system	See Using reports to view storage system information (on page 199) .
Configuration to block HTTP communication to SVP	See Blocking HTTP communication to the storage system (on page 104) .

Item	Action
Interval for the automatic updates of the Tasks window of Device Manager - Storage Navigator	See Setting the status refresh interval of the Tasks window (on page 198) .
Audit logs saved in SVP	See Hitachi Audit Log User Guide .
Private key and certificate used for SSL communication between the SVP and the management client	See Uploading a signed certificate (on page 101) .
Advanced system settings	See Changing advanced system settings (on page 117) .
Storage system information	See Setting storage system information (on page 81) .
Certificates for SMI-S provider	See Uploading a signed certificate to the SMI-S provider (on page 126) .
Configuration files for SMI-S provider	See Uploading an SMI-S provider configuration file (on page 129) .
Certificates for Hitachi Command Suite	See Registering certificates for HCS (on page 109) .
Mail notice settings	See Email tab in Edit Alert Settings window (on page 455) .

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 HDvM - SN	Security Administrator (View Only)	Security Administrator (View & Modify)
Environment Parameter List	Parameter information in the entire system	Storage Administrator (Initial Configuration)	Storage Administrator (Initial Configuration)
Log Transfer Information	Settings made in the Edit Audit Log Settings and Edit Alert Settings windows	Audit log Administrator (View Only)	Audit log Administrator (View & Modify)
SIMSyslog Transfer Information	Settings made in the Edit Alert Settings window	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)	Security Administrator (View & Modify)
Key Management Server	<p>Connection to the Key Management Server*</p> <p>* 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 (KMS) to determine the best way to use the server to manage and back up the certificate.</p>	Security Administrator (View & Modify)	Security Administrator (View & Modify)
TLS Security Settings	Security settings used for communications with SVP	Storage Administrator (Initial Configuration) or Security Administrator (View & Modify)	Storage Administrator (Initial Configuration) or Security Administrator (View & Modify)
REST API Configurations	<p>Remote storage information and job history information*</p> <p>* While downloading or restoring the REST API configuration files, the REST services are stopped. The REST services might be stopped for a few minutes due to the configuration file sizes because the download or restoration can take some time depending on the configuration file sizes.</p>	Storage Administrator (Initial Configuration)	Storage Administrator (Initial Configuration)
Flash Disable File	Settings to disable or enable use of Adobe Flash Player with HDvM - SN	Security Administrator (View & Modify)	Security Administrator (View & Modify)

Configuration file	Description	Required role to back up a file	Required role to restore a file
WSUS Settings	Settings to disable or enable use of Windows Server Update Services (WSUS), and settings for the WSUS server URL and the active hours* * If the SVP High Reliability Kit (standby SVP) is installed, the WSUS setting file cannot be downloaded.	Security Administrator (View & Modify)	Security Administrator (View & Modify)

Backing up HDvM - SN configuration files

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

Before you begin

- You must be an external authentication user whose external user group mapping is disabled.

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.

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

The 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 SVP
 - **Protocol**: specify **HTTPS**

- **Port: 5989**
- **Namespace:root/hitachi/smis or interop**



Note: If you cannot access the storage system with error message "An error (20121-107097) occurs and the Device Manager - Storage Navigator login fails", you might not have selected the cipher suites corresponding to the key type of the certificate on the **TLS Security Settings** dialog box.

- a. Connect to the **Tool Panel** dialog box via an HTTP connection, and enable all cipher suites.
- b. Make sure you can log in to Device Manager - Storage Navigator.
- c. Verify the settings of the cipher suites.

If this problem occurs again, verify the network environment and the access destination. If you still cannot access to the storage system after taking actions, contact customer support.

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 using the OpenSSL command \(on page 95\)](#).
- The passphrase for the private key (server.key file) is released.
- A signed public key certificate (.crt file) has been acquired. Change the file name to server.crt unless the file is already named that. See [Creating a public key using the OpenSSL command \(on page 96\)](#).
- When using TLS1.2, you must set the cipher suites corresponding to the key type of the certificate that is uploaded to the SVP or the SMI-S provider.

Verify the settings of the cipher suites on the **TLS Security Settings** dialog box using the **Tool Panel** dialog box:

- If the key type is RSA, select a cipher suite whose name contains "RSA".
- If the key type is ECDSA, select a cipher suite whose name contains "ECDSA".

If the cipher suites corresponding to the key type of the certificate are not set, you cannot connect the storage system using the management software.

- You must be an external authentication user whose external user group mapping is disabled, or a local authentication user.

- If the public key of the certificate to be uploaded is RSA, the key length must not be less than the key length that is set for Minimum Key Length (Key Exchange) in the **TLS Security Settings** dialog box.
- If the public key of the certificate to be uploaded is ECDSA, the public key parameter must be any of the following:
 - ECDSA_P256 (secp256r1)
 - ECDSA_P384 (secp384r1)
 - ECDSA_P521 (secp521r1)
- The signature hash algorithm of the certificate to be uploaded must be SHA-256, SHA-384, or SHA-512.
- The extended profile fields in the X.509 certificate support the following items as specified in RFC5280:
 - subjectAltName
 - CRLDistributionPoint
 - AuthorityInfoAccess
 - BasicConstraints
 - KeyUsage
 - SubjectKeyIdentifier

Enter the host name or the IP address of the SVP in *subjectAltName* or *CommonName* of the certificate to be uploaded.

- When you perform a certificate revocation check by using CRL, set the CRL repository URI for the cRLDistributionPoint (CRL distribution point) of the intermediate certificate and server certificate.
- When you perform a certificate revocation check by using OCSP, set the OCSP responder URI for authorityInfoAccess (Authority Information Access) of the intermediate certificate and server certificate.
- When you perform a certificate revocation check on the management client, the CRL repository or the OCSP responder must be on the network that can be accessed by the management client so that they can be accessed by the management client. If the management client cannot communicate with the CRL repository or the OCSP responder, the connection to Device Manager - Storage Navigator is established without certificate revocation check.
- If an intermediate certificate exists, prepare a signed public key certificate file (server.crt) that has a certificate chain that includes the intermediate certificate.
- The number of tiers of the certificate chain for the certificate to be uploaded must be 20 tiers or less including the root CA certificate.

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 \(on page 126\)](#) 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 \(on page 129\)](#).

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.

Setting up WSUS function

Windows Server Update Services (WSUS) provides centralized management for applying updates provided by the Microsoft Corporation. When the WSUS server works with the SVP, Security Updates for which our operation verification has been complete can automatically apply to the SVP .

This allows customers to centrally manage the application of Security Updates to the SVP, which was previously performed as a maintenance operation. To use this function, perform the following procedure for enabling the WSUS function.

Before you begin

- The WSUS server must be prepared by the customer.
- Configure the network so that the WSUS server can communicate with the SVP.
- Set the WSUS server so that Security Updates can be received by the SVP.
- Set the WSUS server so that only Security Updates for which our operation verification has been complete applies to the SVP.
- You must have the Security Administrator (View & Modify) role to perform this task.
- A single SVP configuration must be created. In a duplex SVP configuration with the SVP High Reliability Kit installed, the WSUS function cannot be enabled.
- To enter the host name in the WSUS server URL, set the host name and the domain name of the WSUS server for the DNS server.



Caution: Applying Security Updates for which our operation verification has not been complete to the SVP might produce unpredictable results such as the inability to operate the SVP.



Note: Make a note of the settings during the following operating procedure, which might be useful if you reconfigure the WSUS settings to replace the SVP.

Procedure

1. On the management client, open a web browser.
2. Open the **Tool Panel** dialog box by specifying the following URL:

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

3. Click **WSUS Settings**.
4. Enter the administrator user ID in the User ID field and the password in the Password field, and click **Login**. The **WSUS Settings** dialog box opens.
5. Select a radio button.



Caution: Even if you change the WSUS settings from **Enable** to **Disable**, the downloaded Security Updates might apply to the SVP.

6. To enable the WSUS function, enter the WSUS server URL.
Example: `http://wsus.example.com`, `http://192.0.2.0`
7. Set the active hours between 6 and 18 hours .
8. Click **Next** to open the dialog box opens to confirm the WSUS settings updates.
9. Click **OK**.
10. Check the following audit logs to verify whether Security Updates are applied by using the WSUS function.

Function name: BASE

Operation Name: WindowsServerUpdateServices

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 \(on page 145\)](#).
- 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 ¹
User A	user group 10	Storage Administrator ²	Resource group 10
User B	user group 20	Storage Administrator ²	Resource group 20
Notes:			
<ol style="list-style-type: none"> 1. For the user group that is assigned the Security Administrator role, All Resource Groups Assigned is automatically set to Yes. 2. There are a few types of storage administrators. For more information, see Roles and permissions (on page 137). 			

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 groups and user groups

Resource groups determine the resources that users can manage. The resource groups are associated with user groups rather than individual users.

There are two ways to change the resources that a user has permission to manage:

- Move the user to another user group.
- Change the resource groups assigned to the user group to which the user belongs.

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 ¹
User A	user group 10	Storage Administrator ²	Resource group 10
User B	user group 20	Storage Administrator ²	Resource group 20
<p>Notes:</p> <ol style="list-style-type: none"> 1. For the user group that is assigned the Security Administrator role, All Resource Groups Assigned is automatically set to Yes. 2. There are a few types of storage administrators. For more information, see Roles and permissions (on page 137). 			

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.

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

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

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

Role	Permissions
	<ul style="list-style-type: none"> ▪ Viewing, deleting, and downloading storage configuration reports ▪ Acquiring all the information about the storage system and updating Device Manager - Storage Navigator window by clicking Refresh All
Storage Administrator (System Resource Management)	<ul style="list-style-type: none"> ▪ Configuring settings for CLPR ▪ Configuring settings for MP unit ▪ Deleting tasks and releasing exclusive locks of resources ▪ Completing SIMs¹ ▪ Configuring attributes for ports ▪ Configuring LUN security ▪ Configuring Server Priority Manager ▪ Configuring tiering policies
Storage Administrator (Provisioning)	<ul style="list-style-type: none"> ▪ Configuring caches ▪ Configuring LDEVs, pools, and virtual volumes ▪ Formatting and shredding LDEVs ▪ Configuring external volumes ▪ Configuring alias volumes for Compatible PAV ▪ Configuring Dynamic Provisioning ▪ Configuring host groups, paths, and WWN ▪ Configuring Volume Migration except splitting Volume Migration pairs when using CCI ▪ Configuring access attributes for LDEVs ▪ Configuring LUN security ▪ Creating and deleting quorum disk used with global-active device ▪ Creating and deleting global-active device pairs ▪ Completing SIMs¹ ▪ Editing virtual management settings ▪ Setting reserved attributes for global-active device.
Storage Administrator (Performance Management)	<ul style="list-style-type: none"> ▪ Configuring monitoring ▪ Starting and stopping monitoring
Storage Administrator (Local Copy)	<ul style="list-style-type: none"> ▪ Performing pair operations for local copy ▪ Configuring environmental settings for local copy ▪ Splitting Volume Migration V2 pairs when using CCI

Role	Permissions
Storage Administrator (Remote Copy)	<ul style="list-style-type: none"> ▪ Remote copy operations in general ▪ Operating global-active device pairs (except for creation and deletion)
Support Personnel ² (Vendor Only)	Configuring the SVP <ul style="list-style-type: none"> ▪ Normally, this role is for service representatives. ▪ Downloading dump files using the Dump tool
Notes: <ol style="list-style-type: none"> 1. Completing SIMs is permitted for users who are assigned to both the Storage Administrator (System Resource Management) role and Storage Administrator (Provisioning) role. 2. Normally, the Support Personnel role is reserved for service representatives. However, 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"> ▪ Security Administrator (View & Modify) ▪ Audit Log Administrator (View & Modify) ▪ Storage administrator (Initial Configuration) ▪ Storage Administrator (System Resource Management) ▪ Storage Administrator (Provisioning) ▪ Storage Administrator (Performance Management) ▪ Storage Administrator (Local Copy) ▪ Storage Administrator (Remote Copy) 	All Resource Groups Assigned

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

Built-in group	Role	Resource group
	<ul style="list-style-type: none"> ▪ Storage Administrator (Performance Management) ▪ Storage Administrator (Local Copy) ▪ Storage Administrator (Remote Copy) 	
Support Personnel	<ul style="list-style-type: none"> ▪ Storage Administrator (Initial Configuration) ▪ Storage Administrator (System Resource Management) ▪ Storage Administrator (Provisioning) ▪ Storage Administrator (Performance Management) ▪ Storage Administrator (Local Copy) ▪ Storage Administrator (Remote Copy) ▪ Support Personnel 	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 **Tasks** window opens to show the status of the task.

Changing a user group name

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

Before you begin

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

Procedure

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

Changing user group permissions

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

Before you begin

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

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, select **User Groups**.
2. In the **User Groups** tab, select the user group whose permission you want to change.
3. Click the **Roles** tab.
4. Click **Edit Role Assignment**.

5. In the **Edit Role Assignment** window, change roles to be assigned to the user group.
 - Select roles to add, and then click **Add**.
 - Select a role to remove, and then click **Remove**.
6. Click **Finish**.
7. In the **Confirm** window, check the settings and enter a task name in **Task Name**.
8. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Tasks** window opens.

Changing assigned resource groups

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

Before you begin

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

Procedure

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

Deleting a user group

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

Before you begin

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

Procedure

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

User accounts

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

For more information about roles, permissions, and user groups, see [Roles and permissions \(on page 137\)](#).

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

**Important:**

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

Creating user accounts

When you create a user account, you register the user to the applicable user groups with appropriate permissions. The storage system supports a maximum of 512 user accounts, including the built-in user accounts. To prevent unauthorized access to the storage system, users must change their password immediately after logging in for the first time.



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

Before you begin

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

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, select **User Groups**.
2. On the **User Groups** tab, select a user group to which to add a user. This is dependent on which permissions you want to give to the user.
Support representatives must have the Support Personnel (Vendor Only) role to log in.
3. On the **Roles** tab, confirm that the displayed permissions are appropriate for the user.
4. On the **Users** tab, click **Create**.
5. Enter the user name.
6. Select **Enable** or **Disable** for the account.
If you select **Disable**, the user of this account is disabled and cannot log in to Device Manager - Storage Navigator.
7. To use an authentication server, select **External**. To authenticate users with only Device Manager - Storage Navigator, select **Local**.
8. If you select **Local**, enter the password for this user account in two places.
You can use all alphanumeric characters and symbols for the password. The password must be between 6 and 256 characters.
9. Click **Finish**.
10. In the **Confirm** window, check the settings.
11. Click **Apply**. The task is now registered. If **Go to tasks window for status** is checked, the **Tasks** window opens to display the status of the task.

Character restrictions for user names and passwords

The user account you created for Device Manager - Storage Navigator can also be used for SVP and CCI. 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. 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



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.

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

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

User name and password for logging in to CCI

Item	Length in characters	Characters that can be used
User name	1-63	<ul style="list-style-type: none"> Alphanumeric (ASCII code) characters The following symbols¹: - . @ _
Password	6- 63	<ul style="list-style-type: none"> Alphanumeric (ASCII code) characters The following symbols²: - , . : @ _
Note:		

Item	Length in characters	Characters that can be used
1.	If the host on which CCI is installed is running on UNIX, a slash (/) can be specified.	
2.	If the host on which CCI is installed is running on Windows, a back slash (\) can be specified.	

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 **Tasks** window opens to show the status of the task.

Changing logged-in user passwords

You can change or reissue your own password when currently logging in to 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

- 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. Enter your current password to change your own password.
6. In the **Change Password** dialog box, specify a new password for the user in the two password fields.
7. Click **Finish**
8. In the **Confirm** window, check the settings and enter a task name in **Task Name**.
9. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Tasks** window opens to show the status of the task.



Note: To automatically open the Tasks window after closing the wizard, click **Apply** in the wizard, select **Go to tasks window for status**, and then click **Apply**.

10. In the Tasks window, verify the result of the operation. A task can be suspended or canceled if the processing of the task is not started.

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 **Tasks** window opens to show the status of the task.

Enabling and disabling user accounts

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

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 **Tasks** window opens to show the status of the task.

Deleting user accounts

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

Before you begin

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

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, select **User Groups**.
2. On the **User Groups** tab, click a user group to which a user belongs.
3. On the **Users** tab, select the user whose account you want to delete.
4. Click **More Actions > Delete Users**.
5. In the **Delete Users** window, select the user to be deleted, then click **Finish**.
6. In the Confirm window, check the settings.
7. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Tasks** window opens to show the status of the task.

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.

Operation 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 Operation Locked.



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

Resource access requirements for Device Manager - Storage Navigator operations

When you log on to Device Manager - Storage Navigator, your user access privileges determine the resources you can view and the operations you can perform. User access privileges are determined by the user groups to which a user belongs and the resources assigned to those user groups. To perform an operation on the storage system, you must have access to the resources (for example, volumes, pools, ports) that are required for the operation.

These tables specify the resource access requirements for Device Manager - Storage Navigator operations.

Access requirements for Compatible FlashCopy[®]

This table specifies the resource access requirements for Compatible FlashCopy[®] operations.

Operation name	Condition
Create LDEVs	If TSE-VOLs are created, LDEV IDs must be assigned to the Storage Administrator group that is permitted to manage them.

Operation name	Condition
Expand V-VOLs	You can expand only TSE-VOLs that are assigned to the Storage Administrator group permitted to manage them.

Access requirements for Compatible PAV

This table specifies the resource access requirements for Compatible PAV operations.

Operation name	Condition
Assign aliases	The specified base volumes and free volumes must be assigned to the Storage Administrator group permitted to manage them.
Remove aliases	The specified base volumes and alias volumes must be assigned to the Storage Administrator group permitted to manage them.

Access requirements for Data Retention Utility

This table specifies the resource access requirements for Data Retention Utility operations.

Operation name	Condition
Set access attributes	The specified LDEV must be assigned to users.

Access requirements for Dynamic Provisioning and Dynamic Tiering

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

Operation name	Condition
Create LDEVs	If DP-VOLs are created, these items must be assigned to the Storage Administrator group that is permitted to manage them. <ul style="list-style-type: none"> ▪ LDEV ID ▪ Pool-VOL of the pool
Delete LDEVs	If DP-VOLs are deleted, these items must be assigned to the Storage Administrator group that is permitted to manage them. <ul style="list-style-type: none"> ▪ LDEV ID ▪ Pool-VOL of the pool

Operation name	Condition
Create pools Expand pools	Volumes to be specified as pool-VOLs must be assigned to the Storage Administrator group permitted to manage them. All the volumes that are specified when creating a pool must belong to the same resource group.
Edit pools Delete pools	Pool-VOLs of the specified pool must be assigned to the Storage Administrator group permitted to manage them.
Expand V-VOLs	You can expand only the DP-VOLs that are assigned to the Storage Administrator group permitted to manage them.
Reclaim zero pages Stop reclaiming zero pages	You can reclaim or stop reclaiming zero pages only for the DP-VOLs that are assigned to the Storage Administrator group permitted to manage them.

Access requirements for Encryption License Key

This table specifies the resource access requirements for Encryption License Key operations.

Operation name	Condition
Edit encryption keys	When you specify a parity group and open the Edit Encryption window, the specified parity group and LDEVs carved from the parity group must be assigned to the Storage Administrator group permitted to manage them. When you open the Edit Encryption window without specifying a parity group, more than one parity group and LDEVs carved from the parity group must be assigned to the Storage Administrator group permitted to manage them.

Access requirements for global-active device

This table specifies the resource access requirements for global-active device operations.

Operation name	Condition
Edit Ports	Specified ports must be assigned to the user.
Add Remote Connection	Specified ports must be assigned to the user.
Edit Remote Connection Options	Operation can be performed with no conditions.
Create Pairs	Primary volumes must be assigned to the user.

Operation name	Condition
	Ports of remote paths that are connected with the primary volume in the remote storage must be assigned to the user.
Split Pairs	Specified primary volumes or secondary volumes must be assigned to the user.
Resync Pairs	Primary volumes must be assigned to the user.
Delete Pairs	Specified volumes must be assigned to the user. If primary volumes are specified, the ports of remote paths that are connected with the primary volume in the remote storage must be assigned to the user.
Edit Pair Options	Primary volumes must be assigned to the user.
Add Remote Paths	Specified ports must be assigned to the user.
Remove Remote Paths	Specified ports must be assigned to the user.
Edit Remote Connection Options	Ports of remote paths that are connected to a specified remote storage must be assigned to the user.
Remove Remote Connections	Ports of remote paths that are connected to a specified remote storage must be assigned to the user.
Force Delete Pairs	Specified primary volumes or secondary volumes must be assigned to the user.
Add Quorum Disks	LDEVs to be set as quorum disks must be assigned to the user.
Remove Quorum Disks	LDEVs set as quorum disks to be deleted must be assigned to the user.

Access requirements for LUN Manager

These tables specify the resource access requirements for LUN Manager operations.

For Fibre Channel

Operation name	Condition
Add LUN paths	When you specify host groups and open the Add LUN Paths window, the specified host groups must be assigned to the Storage Administrator group permitted to manage them. When you specify LDEVs and open the Add LUN paths window, the specified LDEVs must be assigned to the Storage Administrator group permitted to manage them.

Operation name	Condition
Delete LUN paths	<p>When you specify a host group and open the Delete LUN Paths window, the specified host group must be assigned to the Storage Administrator group permitted to manage them.</p> <p>When you specify LDEVs and open the Delete LUN Paths window, the specified LDEVs must be assigned to the Storage Administrator group permitted to manage them.</p> <p>When selecting the Delete all defined LUN paths to above LDEVs check box, the host groups of all the alternate paths in the LDEV displayed on the Selected LUNs table must be assigned to the Storage Administrator group permitted to manage them.</p>
Edit host groups	The specified host groups and ports must be assigned to the Storage Administrator group permitted to manage them.
Add hosts	The specified host groups must be assigned to the Storage Administrator group permitted to manage them.
Edit hosts	<p>The specified host group must be assigned to the Storage Administrator group permitted to manage them.</p> <p>When you select the Apply same settings to the HBA WWN of all ports check box, all the host groups where the specified HBA WWNs are registered must be assigned to the Storage Administrator group permitted to manage them.</p>
Remove hosts	When you select the Remove hosts from all host groups containing the hosts in the storage system check box, all the host groups where the HBA WWNs displayed in the Selected Hosts table are registered must be assigned to the Storage Administrator group permitted to manage them.
Edit ports	The specified port must be assigned to the Storage Administrator group permitted to manage them.
Create alternative LUN paths	The specified host groups and all the LDEVs where the paths are set to the host groups must be assigned to the Storage Administrator group permitted to manage them.
Copy LUN paths	The specified host groups and the LDEVs where the paths are set must be assigned to the Storage Administrator group permitted to manage them.
Edit command devices	LDEVs where the specified paths are set must be assigned to the Storage Administrator group permitted to manage them.
Edit UUIDs	The specified LDEV must be assigned to the Storage Administrator group permitted to manage them.

Operation name	Condition
Delete UUIDs	The specified LDEV must be assigned to the Storage Administrator group permitted to manage them.
Create host groups	When you open the Create Host Groups window by specifying host groups, the specified host groups must be assigned to the Storage Administrator group permitted to manage them.
Delete host groups	The specified host groups and all the LDEVs where the paths are set to the host groups must be assigned to the Storage Administrator group permitted to manage them.
Release Host-Reserved LUNs	LDEVs where the specified paths are set must be assigned to you.

For iSCSI

Operation name	Condition
Add LUN paths	<p>When you specify host groups and open the Add LUN Paths window, the specified iSCSI target must be assigned to the Storage Administrator group permitted to manage them.</p> <p>When you specify LDEVs and open the Add LUN paths window, the specified LDEVs must be assigned to the Storage Administrator group permitted to manage them.</p>
Delete LUN paths	<p>When you specify an iSCSI target and open the Delete LUN Paths window, the specified iSCSI target must be assigned to the Storage Administrator group permitted to manage them.</p> <p>When you specify LDEVs and open the Delete LUN Paths window, the specified LDEVs must be assigned to the Storage Administrator group permitted to manage them.</p> <p>When selecting the Delete all defined LUN paths to above LDEVs check box, the iSCSI target of all the alternate paths in the LDEV displayed on the Selected LUNs table must be assigned to the Storage Administrator group permitted to manage them.</p>
Add hosts	The specified iSCSI target must be assigned to the Storage Administrator group permitted to manage them.
Edit hosts	The specified iSCSI target must be assigned to the Storage Administrator group permitted to manage them.

Operation name	Condition
	When you select the Apply same settings to the HBA WWN of all ports check box, all the iSCSI targets where the specified HBA WWNs are registered must be assigned to the Storage Administrator group permitted to manage them.
Remove hosts	The specified iSCSI target must be assigned to the Storage Administrator group permitted to manage them.
Edit ports	The specified port must be assigned to the Storage Administrator group permitted to manage them.
Create alternative LUN paths	The specified iSCSI target and all the LDEVs where the paths are set to the iSCSI target must be assigned to the Storage Administrator group permitted to manage them.
Copy LUN paths	The specified iSCSI target and the LDEVs where the paths are set must be assigned to the Storage Administrator group permitted to manage them.
Edit command devices	LDEVs where the specified paths are set must be assigned to the Storage Administrator group permitted to manage them.
Edit UUIDs	The specified LDEV must be assigned to the Storage Administrator group permitted to manage them.
Delete UUIDs	The specified LDEV must be assigned to the Storage Administrator group permitted to manage them.
Release Host-Reserved LUNs	LDEVs where the specified paths are set must be assigned to you.
Create iSCSI targets	When you open the Create iSCSI targets window by specifying iSCSI targets, the specified iSCSI targets must be assigned to the Storage Administrator group permitted to manage them.
Edit iSCSI targets	The specified iSCSI targets and ports must be assigned to the Storage Administrator group permitted to manage them.
Delete iSCSI targets	The specified iSCSI targets and all the LDEVs where the paths are set to the iSCSI targets must be assigned to the Storage Administrator group permitted to manage them.

Access requirements for Performance Monitor

This table specifies the resource access requirements for Performance Monitor operations.

Operation name	Condition
Add to ports	The specified ports must be assigned to the Storage Administrator group permitted to manage them.
Add new monitored WWNs	
Edit WWNs	

Access requirements for ShadowImage

This table specifies the resource access requirements for ShadowImage operations.

Operation name	Condition
Create pairs	Both primary volume and secondary volumes must be assigned to the Storage Administrator group permitted to manage them.
Split pairs	Primary volumes must be assigned to the Storage Administrator group permitted to manage them.
Suspend pairs	
Resynchronize pairs	
Release pairs	

Access requirements for ShadowImage for Mainframe

This table specifies the resource access requirements for ShadowImage for Mainframe operations.

Operation name	Condition
Create pairs	Both primary volumes and secondary volumes must be assigned to the Storage Administrator group permitted to manage them.
Split pairs	Primary volumes must be assigned to the Storage Administrator group permitted to manage them.
Suspend pairs	
Resynchronize pairs	
Release pairs	

Access requirements for Server Priority Manager

This table specifies the resource access requirements for Server Priority Manager operations.

Operation name	Conditions
Set priority of ports (attribute/threshold/upper limit)	The specified ports must be assigned to the Storage Administrator group permitted to manage them.
Release settings on ports by the decrease of ports	
Set priority of WWNs (attribute/upper limit)	
Change WWNs and SPM names	
Add WWNs (add WWNs to SPM groups)	
Delete WWNs (delete WWNs from SPM groups)	
Add SPM groups and WWNs	
Delete SPM groups	
Set priority of SPM groups (attribute/upper limit)	
Rename SPM groups	
Add WWNs	
Delete WWNs	
Initialization	
Set threshold	

Access requirements for Thin Image

This table specifies the resource access requirements for Thin Image operations.

Operation name	Condition
Create LDEVs	<p>If LDEVs for Thin Image are created, these items must be assigned to the Storage Administrator group that is permitted to manage them.</p> <ul style="list-style-type: none"> ▪ LDEV ID ▪ Pool VOL of the pool

Operation name	Condition
Delete LDEVs	If LDEVs for Thin Image are deleted, these items must be assigned to the Storage Administrator group that is permitted to manage them. <ul style="list-style-type: none"> ▪ LDEV ID ▪ Pool VOL of the pool
Create pools Expand Pool	Volumes that are specified when creating or expanding pools must be assigned to the Storage Administrator group that is permitted to manage them. All the volumes that are specified when creating pools must belong to the same resource group.
Edit Pools Delete Pools	Pool-VOLs of the specified pools must be assigned to the Storage Administrator group that is permitted to manage them.
Create pairs	Both primary volumes and secondary volumes must be assigned to the Storage Administrator group that is permitted to manage them.
Split pairs	Primary volumes must be assigned to the Storage Administrator group that is permitted to manage them.
Suspend pairs	
Resynchronize pairs	
Release pairs	

Access requirements for TrueCopyTrueCopy for Mainframe

This table specifies the resource access requirements for TrueCopyTrueCopy for Mainframe operations.

Operation name	Condition
Edit Ports	Specified ports must be assigned to the user.
Add Remote Connection	Specified ports must be assigned to the user.
Edit Remote Connection Options	Operation can be performed with no conditions.
Create Pairs	Primary volumes must be assigned to the user. Ports of remote paths that are connected with the primary volume in the remote storage must be assigned to the user.

Operation name	Condition
Split Pairs	Specified primary volumes or secondary volumes must be assigned to the user.
Resync Pairs	Primary volumes must be assigned to the user.
Delete Pairs	Specified volumes must be assigned to the user. If primary volumes are specified, the ports of remote paths that are connected with the primary volume in the remote storage must be assigned to the user.
Edit Pair Options	Primary volumes must be assigned to the user.
Add Remote Paths	Specified ports must be assigned to the user.
Remove Remote Paths	Specified ports must be assigned to the user.
Edit Remote Connection Options	Ports of remote paths that are connected to a specified remote storage must be assigned to the user.
Add SSIDs	Ports of remote paths that are connected to a specified remote storage must be assigned to the user.
Remove SSIDs	Ports of remote paths that are connected to a specified remote storage must be assigned to the user.
Remove Remote Connections	Ports of remote paths that are connected to a specified remote storage must be assigned to the user.
Force Delete Pairs	Specified primary volumes or secondary volumes must be assigned to the user.

Access requirements for Universal ReplicatorUniversal Replicator for Mainframe

This table specifies the resource access requirements for Universal ReplicatorUniversal Replicator for Mainframe operations.

Operation name	Condition
Edit Ports	Specified ports must be assigned to the user.
Add Remote Connection	Specified ports must be assigned to the user.
Add Remote Paths	Specified ports must be assigned to the user.
Create Journals	All LDEVs that are specified when creating a journal must belong to the same resource group. Volumes to be assigned to a journal must be assigned to the user.

Operation name	Condition
Assign Journal Volumes	Volumes to be assigned to a journal must be assigned to the user. All volumes to be assigned to a journal must belong to a same resource group to which the existing journal volumes belong.
Assign MP Unit	Journal volumes must be assigned to the user.
Edit Remote Connection Options	Operation can be performed with no conditions.
Create Pairs	Journal volumes for pair volumes and primary volumes must be assigned to the user. Ports of remote paths that are connected with the primary volume in the remote storage must be assigned to the user.
Split Pairs	Specified primary volumes or secondary volumes must be assigned to the user.
Split Mirrors	All data volumes configured to a mirror must be assigned to the user.
Resync Pairs	Primary volumes must be assigned to the user.
Resync Mirrors	All data volumes configured to a mirror must be assigned to the user.
Delete Pairs	Specified volumes or secondary volume must be assigned to the user. Ports of remote paths that are connected with the primary volume in the remote storage must be assigned to the user.
Delete Mirrors	All data volumes configured to a mirror must be assigned to the user.
Edit Pair Options	Primary volumes must be assigned to the user.
Force Delete Pairs	Specified volumes must be assigned to the user.
Edit Journal Options	All data volumes consisting of the specified journal must be assigned to the user. Journal volumes must be assigned to the user.
Edit Mirror Options	All data volumes configuring the specified journal must be assigned to the user. Journal volumes must be assigned to the user.
Remove Journals	Journal volumes must be assigned to the user.

Operation name	Condition
Edit Remote Connection Options	Ports of remote paths that are connected to a specified remote storage must be assigned to the user.
Remove Remote Paths	Specified ports must be assigned to the user.
Move LDEVs to other resource groups	When you move LDEVs used for journal volumes to other resource groups, you must specify all the journal volumes of the journal to which the LDEVs belong.
Assign Remote Command Devices	Journal volumes must be assigned to the user. Specified remote command devices must be assigned to the user.
Release Remote Command Devices	Journal volumes must be assigned to the user. Specified remote command devices must be assigned to the user.

Access requirements for Universal Volume Manager

This table specifies the resource access requirements for Universal Volume Manager operations.

Operation name	Condition
Add external volumes	When creating an external volume, a volume is created in the resource group where the port belongs. When you specify a path group and open the Add External Volumes window, all the ports that compose the path group must be assigned to the Storage Administrator group permitted to manage them.
Delete external volumes	The specified external volume and all the LDEVs allocated to that external volume must be assigned to the Storage Administrator group permitted to manage them.
Disconnect external storage systems	All the external volumes belonging to the specified external storage system and all the LDEVs allocated to those external volumes must be assigned to the Storage Administrator group permitted to manage them.
Reconnect external storage systems	All the external volumes belonging to the specified external storage system and all the LDEVs allocated to those external volumes must be assigned to the Storage Administrator group permitted to manage them.

Operation name	Condition
Disconnect external volumes	The specified external volumes and all the LDEVs allocated to those external volume must be assigned to the Storage Administrator group permitted to manage them.
Reconnect external volumes	The specified external volumes and all the LDEVs allocated to those external volumes must be assigned to the Storage Administrator group permitted to manage them.
Edit external volumes	The specified external volumes must be assigned to the Storage Administrator group permitted to manage them.
Assign MP Unit	The specified external volumes and all the ports of the external paths connecting the external volumes must be assigned to the Storage Administrator group permitted to manage them.
Disconnect external paths	<p>Ports of the specified external paths and all the external volumes connecting with the external path must be assigned to the Storage Administrator group permitted to manage them.</p> <p>When you specify By Ports, all the external paths connecting with the specified ports and all the external volumes connecting with the external paths must be assigned to the Storage Administrator group permitted to manage them.</p> <p>When you specify By External WWNs, all the ports of the external paths connecting to the specified external WWN and all the external volumes connecting with those external paths must be assigned to the Storage Administrator group permitted to manage them.</p>
Reconnect external paths	<p>Ports of the specified external paths and all the external volumes connecting with those external paths must be assigned to the Storage Administrator group permitted to manage them.</p> <p>When you specify By Ports, all the external paths connecting with the specified ports and all the external volumes connecting with the external paths must be assigned to the Storage Administrator group permitted to manage them.</p> <p>When you specify By External WWNs, all the ports of the external paths connecting to the specified external WWN and all the external volumes connecting with those external paths must be assigned to the Storage Administrator group permitted to manage them.</p>
Edit external WWNs	All the ports of the external paths connecting to the specified external WWN and all the external volumes connecting with the external paths must be assigned to the Storage Administrator group permitted to manage them.

Operation name	Condition
Edit external path configuration	Ports of all the external paths composing the specified path group and all the external volumes that belong to the path group must be assigned to the Storage Administrator group permitted to manage them.

Access requirements for Virtual LUNVirtual LVI

This table specifies the resource access requirements for Virtual LUNVirtual LVI operations.

Operation name	Condition
Create LDEVs	<p>When you specify a parity group and open the Create LDEVs window, the parity group must be assigned to the Storage Administrator group permitted to manage them.</p> <p>When you create an internal or external volumes, the parity groups to which the LDEVs belong and the IDs of the new LDEVs must be assigned to the Storage Administrator group permitted to manage them.</p>
Delete LDEVs	When deleting an internal or external volume, the deleted LDEV and parity groups where the LDEV belongs must be assigned to the Storage Administrator group permitted to manage them.
Edit LDEVs	The specified LDEV must be assigned to the Storage Administrator group permitted to manage them.
Restore LDEVs	<p>When you specify LDEVs and open the Restore LDEVs window, the specified LDEVs must be assigned to the Storage Administrator group permitted to manage them.</p> <p>When you specify a parity group and open the Restore LDEVs window, the specified parity group and all the LDEVs in the parity group must be assigned to the Storage Administrator group permitted to manage them.</p>
Block LDEVs	<p>When you specify LDEVs and open the Block LDEVs window, the specified LDEVs must be assigned to the Storage Administrator group permitted to manage them.</p> <p>When you specify a parity group and open the Block LDEVs window, the specified parity group and all the LDEVs in the parity group must be assigned to the Storage Administrator group permitted to manage them.</p>
Format LDEVs	When you specify LDEV and open the Format LDEVs window, the specified LDEV must be assigned to the Storage Administrator group permitted to manage them.

Operation name	Condition
	When you specify a parity group and open the Format LDEVs window, the specified parity group and all the LDEVs in the parity group must be assigned to the Storage Administrator group permitted to manage them.

Access requirements for Virtual Partition Manager

This table specifies the resource access requirements for Virtual Partition Manager operations.

Operation name	Condition
Migrate parity groups	When you specify virtual volumes, the specified LDEV must be assigned to the Storage Administrator group permitted to manage them. When you specify a parity group, the specified parity group must be assigned to the Storage Administrator group permitted to manage them.

Access requirements for Volume Retention Manager

This table specifies the resource access requirements for Volume Retention Manager operations.

Operation name	Condition
Set access attributes	The specified LDEV must be assigned to users.

Access requirements for Volume Shredder

This table specifies the resource access requirements for Volume Shredder operations.

Operation name	Condition
Shred LDEVs	When you specify LDEVs and open the Shred LDEVs window, the specified LDEVs must be assigned to the Storage Administrator group permitted to manage them. When you specify a parity group and open the Shred LDEVs window, the specified parity group and all the LDEVs in the parity group must be assigned to the Storage Administrator group permitted to manage them.

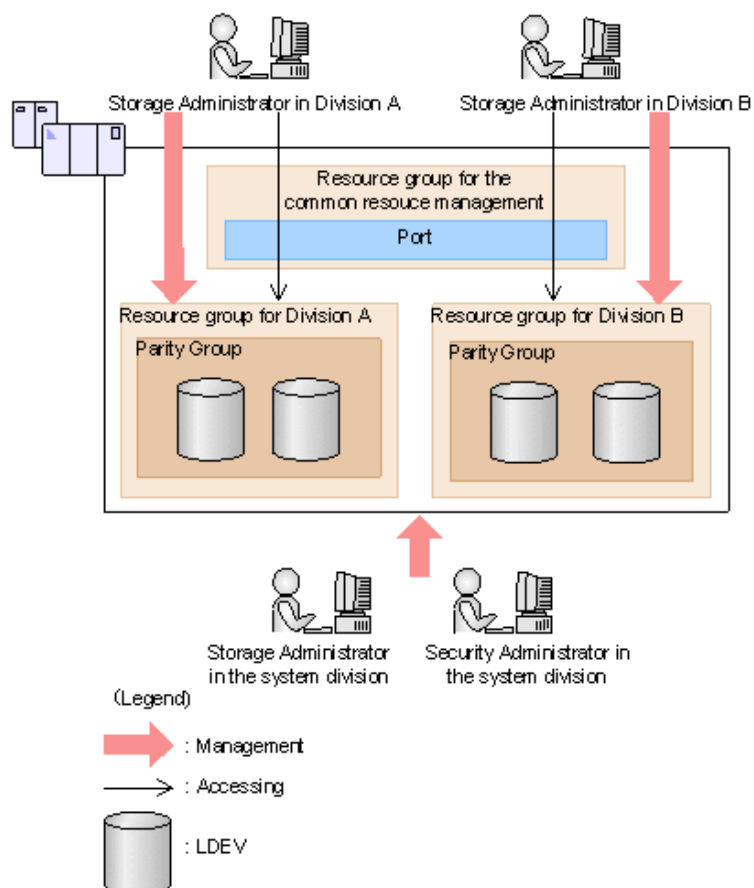
Examples

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

Resource groups sharing a port

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

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



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

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

Configuration workflow for resource groups sharing a port

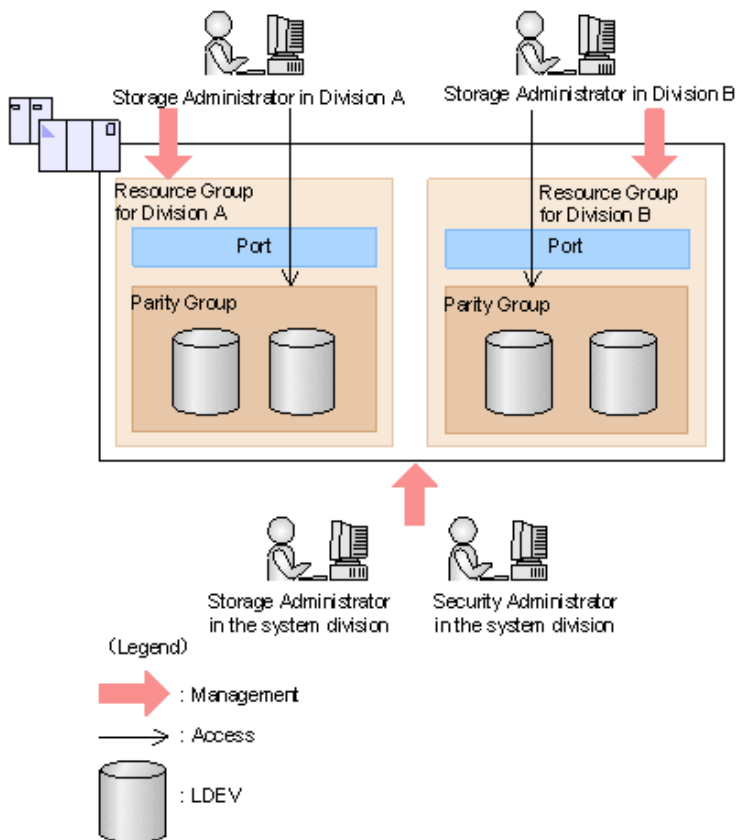
1. The system division forms a plan about the resource group creation and assignment of the resources.
2. The Security Administrator creates the resource groups.
3. The Security Administrator creates the user groups.
4. The Security Administrator assigns the resource groups to the user groups.
5. The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

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

Resource groups not sharing ports

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

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



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

Configuration workflow for resource groups not sharing a port

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

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

Resource group assignments

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

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

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

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

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

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

Resource group rules, restrictions, and guidelines

Rules

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

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

Creating resource groups

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

Before you begin

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

Procedure

1. In the **Explorer** pane, expand the **Storage Systems** tree, click the **Administration** tab, and then select **Resource Groups**.
2. In the **Explorer** pane, expand the **Storage Systems** tree, and then click the **Administration** tab.
3. Select **Resource Groups**, and then click **Create Resource Groups**.
4. In the **Create Resource Groups** window, enter the name for the new group, select the desired resources for the new group, and click **Add** to add the new group to list of resource groups to be added.

Naming guidelines:

- A resource group name can use alphanumeric characters, spaces, and the following symbols: ! # \$ % & ' () + - . = @ [] ^ _ ` { } ~
 - The characters in a resource group name are case-sensitive.
 - Duplicate occurrences of the same name are not allowed.
 - You cannot use the following names: `meta_resource`
5. Repeat the previous step for each new resource group to be added. If you need to remove a group from the list of resource groups to be added, select the group, and click **Remove**.



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

6. When you are finished configuring new resource groups in the **Create Resource Groups** window, click **Next**.

7. Enter a task name or accept the default, and then click **Submit**.
If you select **View task status**, the **Tasks & Alerts** tab opens.

Adding resources to a resource group

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

Note the following restrictions for editing resource groups:

- Only resources allocated to meta_resource can be added to resource groups.
- Resources removed from a resource group are returned to meta_resource.
- No resource can be added to or removed from meta_resource.
- The name of the meta_resource group cannot be changed or used for any resource group other than the meta_resource group.
- The system does not allow duplicate names.
- LDEVs with the same pool ID or journal ID cannot be added to multiple resource groups or partially removed from a resource group. For example, if two LDEVs belong to the same pool, you must allocate both to the same resource group. You cannot allocate them separately.

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

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

- 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 \(on page 176\)](#). 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 \(on page 178\)](#). Explains that you can conserve the term key when you are not using it.
- [Using the temporary key \(on page 178\)](#). Explains that you can conserve the temporary key when you are not using it.
- [Estimating licensed capacity \(on page 179\)](#). Provides information and instructions for calculating license capacity according to your system and organization requirements.
- [Installing and uninstalling software \(on page 185\)](#). Provides instructions for installing, disabling, enabling, and removing keys.
- [License key expiration \(on page 190\)](#) 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 ¹	Estimating licensed capacity
Permanent	For purchase	No limit	Required
Term	For purchase	365 days	Required
Temporary	For trial use before purchase (try and buy)	120 days	Not required
Emergency	For emergency use	30 days	Not required
<p>Notes:</p> <p>1. When you log in to Device Manager - Storage Navigator, a warning message appears if 45 days or less remain before the expiration.</p>			

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

The following table describes the three types of licensed capacity: used capacity, mounted capacity, and unlimited capacity. The type you select depends on the software application.

Table 8 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"> ▪ Normal volumes (volumes) ▪ External volumes mapped to the storage system ▪ Pools <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 options and specifies the licensed capacity type for each option.

Option name	Licensed capacity	Notes
Device Manager - Storage Navigator	Mounted capacity	
SNMP Agent	Mounted capacity	
JAVA API	Mounted capacity	
SMI-S Provider	Unlimited	
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	
Performance Monitor	Mounted capacity	
Server Priority Manager	Mounted capacity	To use Server Priority Manager, first install Performance Monitor.
Volume Quality of Service	Unlimited	blank
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*	Default state*
TrueCopy for Mainframe	Used capacity for normal volumes*	
Universal Replicator	Used capacity for normal volumes*	To use Universal Replicator, first install TrueCopy.

Option name	Licensed capacity	Notes
Universal Replicator for Mainframe	Used capacity for normal volumes*	To use Universal Replicator for Mainframe, first install TrueCopy for Mainframe.
Remote Replication Extended	Unlimited	To use Remote Replication 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*	
ShadowImage for Mainframe	Used capacity for normal volumes*	
Compatible FlashCopy® V2	Used capacity for normal volumes*	
Hitachi Compatible FlashCopy®	Used capacity for normal volumes*	
Thin Image	Used capacity for normal volumes* + 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.
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.

Option name	Licensed capacity	Notes
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	
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	
Nondisruptive migration	Used capacity for external volumes	
Encryption License Key	Unlimited	

Option name	Licensed capacity	Notes
Global-active device	Used capacity for normal volumes*	
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.
Hybrid mode activation license	Unlimited	- (hyphen)
VSP 5500 model activation license	Unlimited	- (hyphen)
<p>* 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"> ▪ ShadowImage ▪ Thin Image ▪ TrueCopy ▪ Universal Replicator ▪ ShadowImage for Mainframe ▪ TrueCopy for Mainframe ▪ Universal Replicator for Mainframe ▪ Compatible FlashCopy® ▪ Global-active device 		

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 9 Formulas for calculating capacity of a normal volume

Volume emulation type	Formula for calculating capacity of a normal volume
3390-x ¹	870 KB × <i>number-of-user-cylinders</i>

Volume emulation type	Formula for calculating capacity of a normal volume
OPEN-x ¹	Same as the capacity specified when creating the volume
Notes:	
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 10 Example of calculating license capacity

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

Calculating licensed capacity for an external volume

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

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

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 **Tasks** 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	-

License key status (example)	Status	Key type	Licensed capacity	Term (Days)
Installed with the term key and set to Enabled	Installed	term	Permitted	Number of remaining days before expiration
Installed with the term key and set to Disabled	Installed (Disabled)	term	Permitted	-
Installed with the temporary key.	Installed	temporary	-	Number of remaining days before expiration
Installed with the emergency key.	Installed	emergency	-	Number of remaining days before expiration
A temporary key was installed, but has expired.	Expired	temporary	-	Number of remaining days before expiration
A term key or an emergency key was installed, but has expired.	Not installed	blank	Blank	Blank
Installed with the permanent key or the term key, but the licensed capacity was insufficient.	Not Enough License	permanent or term	Permitted and Used	-
Installed with the permanent or term key, and then LDEVs are added, but the license capacity was insufficient.	Grace Period	permanent or term	Permitted and Used	Number of remaining days before expiration
Installed with the temporary key, and then reinstalled with the permanent key, but the license capacity was insufficient.	Installed	temporary	Permitted and Used	Number of remaining days before expiration
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®, 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 System Name:** VSP 5000 series(S/N:1)
- Storage System Type:** VSP 5500H
- Serial Number:** 1
- IP Address:** localhost
- Contact:** localhost
- Location:** localhost
- Software Version:** Main
- SVP:** 90-04-00/00
- CBA:** 90-04-00/00-0001
- RMI Server:** 10_01_03
- Total Cache Size:** 166.00 GB

Allocation Summary:

Internal/External	Total	Open/MainFrame	Total	Capacity Unit	Appropriate
Physical Summary					
Allocated	542.60 GB	[7%]		Physical Capacity	542.60 GB
Reserved	0.00 MB	[0%]			94
Used DP Pool	0.00 MB	[0%]			94
Unused DP Pool	0.00 MB	[0%]			-
Other	294.91 GB	[4%]			2
Available Space	157.20 GB	[1%]			236
Unallocated	6.70 TB	[88%]			-
Free Space	6.70 TB	[88%]			-
Physical Total	7.68 TB			Physical Capacity	856
Virtual Summary					
DP Allocated	120.96 GB			Virtual Capacity	84
DP Unallocated	361.75 GB				114
Other	768.00 MB				16
Virtual Total	483.46 GB				214

General Tasks:

- Create Host Groups
- Create (SCSI) Targets
- Create LDEVs
- Add LUN Paths
- Create Pools
- Add External Volumes

Analytics:

- Administration

General Tasks:

- Create Host Groups
- Create (SCSI) Targets
- Create LDEVs
- Add LUN Paths
- Create Pools
- Add External Volumes

Summary:

- Total Efficiency: - (Data Reduction: - / Software Saving: - (Compression: - / Deduplication: - / Pattern Matching: - / FMD Saving: - (Compression: - / Provisioning: 0%) [-]
- Snapshot: - / Provisioning: 0% [-]
- Total Saving: 0.99:1 (-) Total DP Subscription Rate: 0% Total Number of LDEVs: 1070 (Max Allowed: 65280)

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
CL1-C	1C-G00	00[Standard]	Disabled...	0	0	me
CL3-C	3C-G00	00[Standard]	Disabled...	0	0	me
CL5-C	5C-G00	00[Standard]	Disabled...	0	0	me
CL7-C	7C-G00	00[Standard]	Disabled...	0	0	me
CL1-D	1D-G00	00[Standard]	Disabled...	0	0	me
CL3-D	3D-G00	00[Standard]	Disabled...	0	0	me
CL5-D	5D-G00	00[Standard]	Disabled...	0	0	me
CL7-D	7D-G00	00[Standard]	Disabled...	0	0	me
CL2-C	2C-G00	00[Standard]	Disabled...	0	0	me
CL4-C	4C-G00	00[Standard]	Disabled...	0	0	me
CL6-C	6C-G00	00[Standard]	Disabled...	0	0	me
CL8-C	8C-G00	00[Standard]	Disabled...	0	0	me
CL2-D	2D-G00	00[Standard]	Disabled...	0	0	me
CL4-D	4D-G00	00[Standard]	Disabled...	0	0	me
CL6-D	6D-G00	00[Standard]	Disabled...	0	0	me
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 device DKC0. It features a 'Refresh' button and a summary table of port counts:

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

Below the summary is a graphical representation of port racks. Racks 1PB, 1PC, 1PE, 2PE, and 2PB are labeled as 'Not Installed'. Racks 1PC, 1PE, 2PE, and 2PB show individual port status icons (green circles with white dots for 'Available (Connected)', green circles with grey dots for 'Available (Not Connected)', and grey circles for 'Not Available').

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' button (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"> ▪ The resource can be used, but has a limit on I/O performance and so on. ▪ The status of the resource is changing. ▪ The status of the resource is being confirmed. ▪ The resource has subresources of different status. <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"> ▪ The resource cannot be used because it is blocked due to a failure or maintenance operations. ▪ The status of the resource is unknown. <p>Restore the resource to the normal status.</p>

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 **Tasks** 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.

When an operation that contains several connected tasks is set as one task, you can still check the status of each task in the Tasks window. You can also check which task has failed. The following example shows that an error has occurred for the task action number 2.


Task Status ↑ □ ×

Task Name: 130530-CreatePools



Task Failed

An error occurred during the task (Create Pools) processing.



Specified LDKC:CU:LDEV has already been used.

Check the setting of LDKC, CU, and LDEV.

(03205-066504)

Actions			
No.	Action Name	Status	
1	Create Pools	Completed	
2	Create LDEVs	Failed	
3	Add LUN Pa...	Waiting	
Total: 3			

Close

In the LDEV creations or LUN operations, some tasks are processed as one and the individual result may not be reported. Some of the settings may not be applied because internal processing has been stopped due to the error displayed in the following 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)

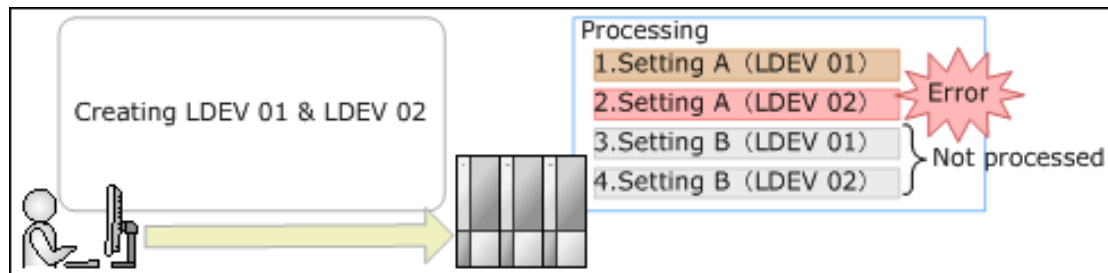
Selected LDEVs					
Error Code	LDEV ID	LDEV Name	Pool Name(ID)	Drive Type/RPM	RAID
03205-058474	00:03:34		HDT0(0)	SSD/-	6(140
03205-006537	00:03:35		HDT0(0)	SSD/-	6(140
03205-006537	00:03:36		HDT0(0)	SSD/-	6(140
03205-006537	00:03:37		HDT0(0)	SSD/-	6(140
03205-006537	00:03:38		HDT0(0)	SSD/-	6(140
03205-006537	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 Operation 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

By default, the **Tasks** window in Device Manager - Storage Navigator is set to refresh automatically every 60 seconds. You can change this refresh time interval or, if desired, you can disable the automatic refresh for the **Tasks** window.

Procedure

1. In the Device Manager - Storage Navigator main window, click **Settings > Environmental Settings > Edit Information Display Settings**.
2. For **Task Screen Refresh Interval**, specify the desired refresh interval (range: 10 - 3600 seconds) or select **No Update**.
If you select **No Update**, the **Tasks** window will not be automatically updated after it has been opened. In this case, you must use **Refresh** or **File > Refresh All** to update the **Tasks** window while it is open.
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 board, and disk board. 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.

If you log in as the user who created the report, you can download / delete only the report created by the user. If you log in as a user with the Storage Administrator (Initial Configuration) role, you can download / delete the reports created by all users.

Creating configuration reports

You can create and store up to 20 configuration reports for each storage system. There are two types of reports:

- Configuration Reports, which are generated in HTML format
- Detail Configuration Reports, which are generated in CSV format

Before you begin

- You must have the Storage Administrator (Initial Configuration) role to create a configuration report.
- Verify that there are less than 20 reports listed on the **Reports** window. If there are already 20 reports, you must delete one or more existing reports before you can create a new report.

Procedure

1. If CCI has been used to create parity groups or LDEVs, click **File > Refresh All** to update the configuration information before creating a configuration report.
2. In the Device Manager - Storage Navigator main menu, click **Reports > Configuration Report > Create Configuration Report**.
3. In the **Create Configuration Report** window, specify a task name or accept the default task name (**yymmdd-CreateConfigurationReport**).

This task name is used as the report name in the **Reports** window.

4. In the **Selected Reports** table, select the desired report type: **Configuration Reports** (HTML) or **Detail Configuration Reports** (CSV).
5. If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status** (selected by default).
6. Click **Apply** to create the selected report.

The create configuration report process takes approximately 10 minutes to complete.

When the process is complete, the new report is displayed on the **Reports** window. If necessary, click **Refresh** to update the list of reports.

Downloading and viewing the HDvM - SN configuration reports

The configuration report created on Device Manager - Storage Navigator (HDvM - SN) can be archived by downloading it to the management client.



Note:

- Adobe Flash Player is required to display configuration reports created with SVP firmware version 90-03-xx and earlier.
- Configuration reports created with SVP firmware version 90-04-01 or later might not be displayed depending on the web browser version on the management client. You must use the latest version of the web browser. (Use the management client running an OS that supports the latest version of the web browser.)
- If you use Google Chrome, specify the Start Option `-allow-file-access-from-files`.
- If you use Google Chrome, the window used to specify the folder in which the report will be saved might not appear when downloading the report. In this case, click Chrome Menu > Settings > Show advanced settings, and then under Privacy clear the check box for Protect you and your device from dangerous sites.

Before you begin

- Users can view the reports that they created.
- Users who have the Storage Administrator (Initial Configuration) role can view all reports.

Procedure

1. Expand the **Storage Systems** tree, and then click **Reports**.
2. Specify the report to download.
3. Click **Download Reports**.



Note: If you are running HDvM - SN with Adobe AIR, a character string that depends on the AIR environment is displayed in the title of the download window.

4. Specify the folder in which to save the `.tgz` file.
5. Extract the downloaded `.tgz` file.
6. Display the report.
 - For HTML reports, open the file `extracted-folder\html\index.html`.

The following warning message might appear when you open the HTML file: An ActiveX control on this page might be unsafe to interact with other parts of the page. Do you want to allow this interaction? This message appears when the program embedded in the report accesses a local file. Click **Yes** to continue the operation.

- For CSV reports, open the CSV file in the folder `extracted-folder\csv`.

Viewing configuration reports in the Reports window

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



Note:

- Adobe Flash Player is required to display configuration reports created with SVP firmware version 90-03-XX or earlier.
- If you use Google Chrome, specify the Start Option `-allow-file-access-from-files`.

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 (20).



Caution: Do not perform Device Manager - Storage Navigator or CCI operations while you are deleting configuration reports. If you perform such operations, deletion of configuration reports might fail.

Before you begin

- You must have the Storage Administrator (Initial Configuration) role to delete a configuration report.

Procedure

1. Expand the **Storage Systems** tree, and then click **Reports**.

2. In the **Reports** window, select the report to delete, and then click **Delete Reports**.
3. In the **Delete Reports** window, specify a task name or accept the default task name (**yymmdd-DeleteReports**).
4. If you want the **Tasks** window to open after you click **Apply**, select **Go to tasks window for status** (selected by default).
5. Click **Apply**.


Examples of Device Manager - Storage Navigator storage configuration reports



















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

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

Report examples: table view

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

The following figure provides examples of reports in table format. The  icons are displayed before the names of the reports in table view. If the icons are not displayed correctly, update the window. To sort data in table reports, click any column header.

Configuration Reports																																																																																																																																																																							
Report Types	Ports																																																																																																																																																																						
<ul style="list-style-type: none">  Storage System Summary  Physical View  Cache Memories  Channel Boards  Ports  Host Groups / iSCSI Targets  Hosts  LUNs  CHAP Users  Logical Devices  Physical Devices  Parity Groups  MP Units  MP Unit Details  Disk Boards  SSD Endurance  Spare Drives  Power Consumption 	<p>This report is about ports. A record is created for each port.</p> <table border="1"> <thead> <tr> <th>CHB</th> <th>Type</th> <th>Port Location</th> <th>Port Attribute</th> <th>iSCSI Virtual Port Mode</th> <th>TCP Port Number</th> <th>Internal WWN / Internal iSCSI Name</th> </tr> </thead> <tbody> <tr><td>CHB-01A</td><td>4HF32R(Fibre)</td><td>1A</td><td>Target</td><td>-</td><td>-</td><td>50060E8008000100</td></tr> <tr><td>CHB-01A</td><td>4HF32R(Fibre)</td><td>3A</td><td>Target</td><td>-</td><td>-</td><td>50060E8008000120</td></tr> <tr><td>CHB-01A</td><td>4HF32R(Fibre)</td><td>5A</td><td>Target</td><td>-</td><td>-</td><td>50060E8008000140</td></tr> <tr><td>CHB-01A</td><td>4HF32R(Fibre)</td><td>7A</td><td>Bidirectional</td><td>-</td><td>-</td><td>50060E8008000160</td></tr> <tr><td>CHB-01B</td><td>2HS10S(iSCSI)</td><td>1C</td><td>Bidirectional</td><td>-</td><td>-</td><td>-</td></tr> <tr><td>CHB-01B</td><td>2HS10S(iSCSI)</td><td>3C</td><td>Bidirectional</td><td>-</td><td>-</td><td>-</td></tr> <tr><td>CHB-01E</td><td>4Mx16(Mfibre)</td><td>1E</td><td>HTP</td><td>-</td><td>-</td><td>50060E8008000104</td></tr> <tr><td>CHB-01E</td><td>4Mx16(Mfibre)</td><td>3E</td><td>HTP</td><td>-</td><td>-</td><td>50060E8008000124</td></tr> <tr><td>CHB-01E</td><td>4Mx16(Mfibre)</td><td>5E</td><td>HTP</td><td>-</td><td>-</td><td>50060E8008000144</td></tr> <tr><td>CHB-01E</td><td>4Mx16(Mfibre)</td><td>7E</td><td>HTP</td><td>-</td><td>-</td><td>50060E8008000164</td></tr> <tr><td>CHB-02A</td><td>4HF32R(Fibre)</td><td>1B</td><td>Bidirectional</td><td>-</td><td>-</td><td>50060E8008000101</td></tr> <tr><td>CHB-02A</td><td>4HF32R(Fibre)</td><td>3B</td><td>Bidirectional</td><td>-</td><td>-</td><td>50060E8008000121</td></tr> <tr><td>CHB-02A</td><td>4HF32R(Fibre)</td><td>5B</td><td>Bidirectional</td><td>-</td><td>-</td><td>50060E8008000141</td></tr> <tr><td>CHB-02A</td><td>4HF32R(Fibre)</td><td>7B</td><td>Bidirectional</td><td>-</td><td>-</td><td>50060E8008000161</td></tr> <tr><td>CHB-02E</td><td>4Mx16(Mfibre)</td><td>1F</td><td>HTP</td><td>-</td><td>-</td><td>50060E8008000105</td></tr> <tr><td>CHB-02E</td><td>4Mx16(Mfibre)</td><td>3F</td><td>HTP</td><td>-</td><td>-</td><td>50060E8008000125</td></tr> <tr><td>CHB-02E</td><td>4Mx16(Mfibre)</td><td>5F</td><td>HTP</td><td>-</td><td>-</td><td>50060E8008000145</td></tr> <tr><td>CHB-02E</td><td>4Mx16(Mfibre)</td><td>7F</td><td>HTP</td><td>-</td><td>-</td><td>50060E8008000165</td></tr> <tr><td>CHB-11A</td><td>4HF32R(Fibre)</td><td>2A</td><td>Target</td><td>-</td><td>-</td><td>50060E8008000110</td></tr> <tr><td>CHB-11A</td><td>4HF32R(Fibre)</td><td>4A</td><td>Target</td><td>-</td><td>-</td><td>50060E8008000130</td></tr> <tr><td>CHB-11A</td><td>4HF32R(Fibre)</td><td>6A</td><td>Target</td><td>-</td><td>-</td><td>50060E8008000150</td></tr> <tr><td>CHB-11A</td><td>4HF32R(Fibre)</td><td>8A</td><td>Target</td><td>-</td><td>-</td><td>50060E8008000170</td></tr> </tbody> </table> <p>Total:36</p>						CHB	Type	Port Location	Port Attribute	iSCSI Virtual Port Mode	TCP Port Number	Internal WWN / Internal iSCSI Name	CHB-01A	4HF32R(Fibre)	1A	Target	-	-	50060E8008000100	CHB-01A	4HF32R(Fibre)	3A	Target	-	-	50060E8008000120	CHB-01A	4HF32R(Fibre)	5A	Target	-	-	50060E8008000140	CHB-01A	4HF32R(Fibre)	7A	Bidirectional	-	-	50060E8008000160	CHB-01B	2HS10S(iSCSI)	1C	Bidirectional	-	-	-	CHB-01B	2HS10S(iSCSI)	3C	Bidirectional	-	-	-	CHB-01E	4Mx16(Mfibre)	1E	HTP	-	-	50060E8008000104	CHB-01E	4Mx16(Mfibre)	3E	HTP	-	-	50060E8008000124	CHB-01E	4Mx16(Mfibre)	5E	HTP	-	-	50060E8008000144	CHB-01E	4Mx16(Mfibre)	7E	HTP	-	-	50060E8008000164	CHB-02A	4HF32R(Fibre)	1B	Bidirectional	-	-	50060E8008000101	CHB-02A	4HF32R(Fibre)	3B	Bidirectional	-	-	50060E8008000121	CHB-02A	4HF32R(Fibre)	5B	Bidirectional	-	-	50060E8008000141	CHB-02A	4HF32R(Fibre)	7B	Bidirectional	-	-	50060E8008000161	CHB-02E	4Mx16(Mfibre)	1F	HTP	-	-	50060E8008000105	CHB-02E	4Mx16(Mfibre)	3F	HTP	-	-	50060E8008000125	CHB-02E	4Mx16(Mfibre)	5F	HTP	-	-	50060E8008000145	CHB-02E	4Mx16(Mfibre)	7F	HTP	-	-	50060E8008000165	CHB-11A	4HF32R(Fibre)	2A	Target	-	-	50060E8008000110	CHB-11A	4HF32R(Fibre)	4A	Target	-	-	50060E8008000130	CHB-11A	4HF32R(Fibre)	6A	Target	-	-	50060E8008000150	CHB-11A	4HF32R(Fibre)	8A	Target	-	-	50060E8008000170
CHB	Type	Port Location	Port Attribute	iSCSI Virtual Port Mode	TCP Port Number	Internal WWN / Internal iSCSI Name																																																																																																																																																																	
CHB-01A	4HF32R(Fibre)	1A	Target	-	-	50060E8008000100																																																																																																																																																																	
CHB-01A	4HF32R(Fibre)	3A	Target	-	-	50060E8008000120																																																																																																																																																																	
CHB-01A	4HF32R(Fibre)	5A	Target	-	-	50060E8008000140																																																																																																																																																																	
CHB-01A	4HF32R(Fibre)	7A	Bidirectional	-	-	50060E8008000160																																																																																																																																																																	
CHB-01B	2HS10S(iSCSI)	1C	Bidirectional	-	-	-																																																																																																																																																																	
CHB-01B	2HS10S(iSCSI)	3C	Bidirectional	-	-	-																																																																																																																																																																	
CHB-01E	4Mx16(Mfibre)	1E	HTP	-	-	50060E8008000104																																																																																																																																																																	
CHB-01E	4Mx16(Mfibre)	3E	HTP	-	-	50060E8008000124																																																																																																																																																																	
CHB-01E	4Mx16(Mfibre)	5E	HTP	-	-	50060E8008000144																																																																																																																																																																	
CHB-01E	4Mx16(Mfibre)	7E	HTP	-	-	50060E8008000164																																																																																																																																																																	
CHB-02A	4HF32R(Fibre)	1B	Bidirectional	-	-	50060E8008000101																																																																																																																																																																	
CHB-02A	4HF32R(Fibre)	3B	Bidirectional	-	-	50060E8008000121																																																																																																																																																																	
CHB-02A	4HF32R(Fibre)	5B	Bidirectional	-	-	50060E8008000141																																																																																																																																																																	
CHB-02A	4HF32R(Fibre)	7B	Bidirectional	-	-	50060E8008000161																																																																																																																																																																	
CHB-02E	4Mx16(Mfibre)	1F	HTP	-	-	50060E8008000105																																																																																																																																																																	
CHB-02E	4Mx16(Mfibre)	3F	HTP	-	-	50060E8008000125																																																																																																																																																																	
CHB-02E	4Mx16(Mfibre)	5F	HTP	-	-	50060E8008000145																																																																																																																																																																	
CHB-02E	4Mx16(Mfibre)	7F	HTP	-	-	50060E8008000165																																																																																																																																																																	
CHB-11A	4HF32R(Fibre)	2A	Target	-	-	50060E8008000110																																																																																																																																																																	
CHB-11A	4HF32R(Fibre)	4A	Target	-	-	50060E8008000130																																																																																																																																																																	
CHB-11A	4HF32R(Fibre)	6A	Target	-	-	50060E8008000150																																																																																																																																																																	
CHB-11A	4HF32R(Fibre)	8A	Target	-	-	50060E8008000170																																																																																																																																																																	

CHAP Users report

The following figure shows an example of a CHAP Users report. The table following the figure describes the items in the report.

CHAP Users			
This report is about chap users. A record is created for each chap user.			
Port Location	User Name	iSCSI Target Alias	iSCSI Target Name
1B	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000	iqn.1994.04.jp.co.hitachi:rsd.r50.t.62510.2a.02	iqn.1994.04.jp.co.hitachi:rs
3B	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.3b000	iqn.1994.04.jp.co.hitachi:rsd.r50.t.62510.2a.02	iqn.1994.04.jp.co.hitachi:rs
2B	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.2b000	iqn.1994.04.jp.co.hitachi:rsd.r50.t.62510.2a.02	iqn.1994.04.jp.co.hitachi:rs
4B	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.4b000	iqn.1994.04.jp.co.hitachi:rsd.r50.t.62510.2a.02	iqn.1994.04.jp.co.hitachi:rs
Total:4			

Item	Description
Port Location	Name of the port
User Name	Name of the CHAP user for authentication
iSCSI Target Alias	Alias of the iSCSI target
iSCSI Target Name	Name of the iSCSI target

Disk Boards report

The following illustration shows an example of a disk boards 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
DKB	Location of the disk board (also called a back-end director). <ul style="list-style-type: none"> "External" is displayed when the storage system has an external storage system. "External (FICON DM)" is displayed when the storage system has volumes for FICON DM.
Number of PGs	The number of the parity groups that the disk board controls. <ul style="list-style-type: none"> If "DKB" is "External", this item indicates the number of parity groups mapped to external volumes. If "DKB" is "External (FICON DM)", this item indicates the number of parity groups mapped to volumes for FICON DM.
Number of LDEVs (Total)	The number of the logical volumes belonging to the parity groups that the disk board controls.

Item	Description
Number of LDEVs (Unallocated)	The number of the logical volumes that are inaccessible from the host and belong to the parity groups controlled by the disk board.
Total LDEV Capacity (MB)	Total capacity of the logical volumes belonging to the parity groups that the disk board controls.
Unallocated LDEV Capacity (MB)	Total capacity of the logical volumes that are inaccessible from the host and belong to the parity groups controlled by the disk board.

Host Groups / iSCSI Targets report

The following figure shows an example of a Host Groups / iSCSI Targets report. The table following the figure describes the items in the report.

Host Groups / iSCSI Targets				
This report is about host groups and iSCSI Targets. A record is created for each host group or iSCSI Target.				
Port Location	Type	Host Group Name / iSCSI Target Alias	Host Group ID / iSCSI Target ID	iSCSI Target Name
1A	4FC16(CHB)	1A-G00		-
3A	4FC16(CHB)	3A-G00		-
1B	ISCSI(OPT)	1B-G00	00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
3B	ISCSI(OPT)	3B-G00	00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
2A	4FC16(CHB)	2A-G00		-
4A	4FC16(CHB)	4A-G00		-
2B	ISCSI(OPT)	2B-G00	00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
4B	ISCSI(OPT)	4B-G00	00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
Total: 8				

Item	Description
Port Location	Name of the port
Type	Type of the host group
Host Group Name / iSCSI Target Alias	Name of the host group / alias of the iSCSI target
Host Group ID / iSCSI Target ID	Number of the host group / ID of the iSCSI target
iSCSI Target Name	Name of the iSCSI target
Resource Group Name	Resource Group Name where the host group belongs
Resource Group ID	Resource Group ID where the host group belongs
Number of LUNs	The number of LU paths defined to the host group
Number of LDEVs	The number of logical volumes that are accessible from the hosts in the host group

Item	Description
Number of PGs	The number of parity groups with logical volumes that are accessible from the hosts in the host group
Number of DKBs	The number of disk boards controlling the parity groups where the logical volumes that are accessible from the hosts in the host group belong
Total LDEV Capacity (MB)	Total capacity of the logical volumes accessible from the hosts in the host group. This is the total capacity of LDEVs referred to in "Number of LDEVs".
Port Security	Security of the port
Authentication : Method	iSCSI target method authentication settings <ul style="list-style-type: none"> ▪ CHAP ▪ None ▪ Comply with Host Setting
Authentication : Mutual CHAP	Enable or disable the iSCSI target mutual CHAP <ul style="list-style-type: none"> ▪ Enabled ▪ Disabled
Authentication : User Name	Authenticated iSCSI target user name
Authentication : Number of Users	The number of authenticated users registered in the iSCSI target
Host Mode	Host mode of the host group
Host Mode Option	Host mode option of the host group. Host mode options are separated by semicolons (;) when more than one option is specified.
Number of Hosts	The number of the hosts in the host group.

Hosts report

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

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

Item	Description
Port Location	Name of the port
Type	Port type
Port Internal WWN	Port WWN
Port Security	Port security setting
Host Group Name / iSCSI Target Alias	Name of the host group / alias of the iSCSI target
iSCSI Target Name	Name of the iSCSI target
Host Mode	Host mode of the host group
Host Mode Option	Host group host mode option. When more than one host mode option is specified, they are separated by semicolons (;)
Host Name	Name of the host that can access the LU path through the port
HBA WWN / iSCSI Name	Host WWN / host iSCSI name. The name is in 16-digit hex format.

Logical Devices report

The following figure shows an example of a Logical Devices report. The table following the figure describes the items in the report.

Logical Devices								
This report is about logical volumes. A record is created for each logical volume.								
LDEV ID	LDEV Name	Capacity(MB)	Emulation Type	Resource Group Name	Resource Group ID	PG	RAID Level	Drive 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	Name of the resource group to which the LDEV belongs
Resource Group ID	ID of the resource group to which the LDEV belongs

Item	Description
PG	Number of the parity group to which the LDEV belongs. <ul style="list-style-type: none"> ▪ If the number starts with "E" (for example, E1-1), the parity group contains external volumes. ▪ If the number starts with "M" (for example, M1-1), the parity group contains FICON DM volumes. A hyphen (-) is displayed for Dynamic Provisioning and Thin Image V-VOLs.
RAID Level	RAID level of the parity group to which the LDEV belongs ¹
Drive Type/ Interface/RPM	Drive type, drive control name, and revolutions-per-minute (RPM) of the drive of the parity group to which the LDEV belongs. A hyphen (-) is displayed as RPM when the drive is not HDD. ¹
Drive Type-Code	Type code of the drives in the parity group to which the logical volume belongs ¹
Drive Capacity	Capacity of the drives in the parity group to which the LDEV belongs ¹
PG Members	Drive locations of the parity group to which the LDEV belongs ¹
Allocated	Information about whether the host can access the LDEV: <ul style="list-style-type: none"> ▪ Y: For open-systems volumes, Y indicates that the host can access the volume. For mainframe volumes and multi-platform volumes, Y is displayed unless the volume is in the reserved status. ▪ N: For opens-systems volumes, N indicates that the host cannot access the volume. For mainframe volumes and multi-platform volumes, N indicates that the volume is in the reserved status.
SSID	SSID of the LDEV
CVS	Information about whether the LDEV is a custom-size volume
OCS	Oracle checksum
Attribute	Attribute of the LDEV
Provisioning Type	Provisioning type of the LDEV

Item	Description
Pool Name	<ul style="list-style-type: none"> ▪ For V-VOLs of Dynamic Provisioning, the name of the pool related to the logical volume is displayed¹. ▪ If the logical volume attribute is Pool, the name of the pool to which the logical volume belongs is displayed. ▪ When neither of the above is displayed, the pool name is blank.
Pool ID	ID of the pool indicated by "Pool Name". A hyphen (-) is displayed for volumes other than pool-VOLs or V-VOLs.
Current MPU	MP unit currently controlling the LDEV
Setting MPU	MP unit that you specified to control the LDEV
Command Device: Security	Indicates whether Security is specified as the attribute for the command device. A hyphen (-) is displayed when "Attribute" is not "CMDDEV".
Command Device: User Authentication	Indicates whether User Authentication is specified as the attribute for the command device. A hyphen (-) is displayed when "Attribute" is not "CMDDEV".
Command Device: Device Group Definition	Indicates whether Device Group Definition is specified as the attribute for the command device. A hyphen (-) is displayed when "Attribute" is not "CMDDEV".
Encryption	Indicates whether the parity group to which the LDEV belongs is encrypted: <ul style="list-style-type: none"> ▪ For internal volumes: Enabled (encrypted) or Disabled (not encrypted) ▪ For external volumes: blank
Notes: 1. A hyphen (-) is displayed if the LDEV is an external volume or a FICON DM volume.	

LUNs report

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

LUNs			
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
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"> ▪ Active/Optimized: Prioritized ▪ Active/Non-Optimized: Lower priority

MP Unit report

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

MP Units

This report is about MP units. A record is created for each MP unit.

MP Unit ID	Auto Assignment	Number of Resources(LDEV)	Number of Resources(Journal)	Number of Resources(External Volume)	Number of Resources(Total)
MPU-010	Enabled	4576	32	8	4616
MPU-020	Enabled	4570	32	8	4610
MPU-110	Enabled	4564	32	8	4604
MPU-120	Enabled	4574	32	8	4614

Total:4

Item	Description
MP Unit ID	MP unit ID
Auto Assignment	Auto assignment attribute for the MP unit
Number of Resources (LDEV)	The number of logical volumes that the MP unit controls
Number of Resources (Journal)	The number of journals that the MP unit controls
Number of Resources (External Volume)	The number of external volumes that the MP unit controls, including FICON DM volumes
Number of Resources (Total)	The total number of resources that the MP unit controls The sum of "Number of Resources (LDEV)", "Number of Resources (Journal)", and "Number of Resources (External Volume)"

MP unit details report

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

MP Unit Details

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

MP Unit ID	Auto Assignment	Resource ID	Resource Name	Type
MPU-010	Enabled	00:02:00	DP-GAD	LDEV
MPU-010	Enabled	00:02:04	DP-GAD	LDEV
MPU-010	Enabled	00:02:08	DP-GAD	LDEV
MPU-010	Enabled	00:02:0C	DP-GAD	LDEV
MPU-010	Enabled	00:02:10	DP-GAD	LDEV
MPU-010	Enabled	00:02:14	DP-GAD	LDEV
MPU-010	Enabled	00:02:18	DP-GAD	LDEV
MPU-010	Enabled	00:02:1C	DP-GAD	LDEV
MPU-010	Enabled	00:02:20	DP-GAD	LDEV
MPU-010	Enabled	00:02:24	DP-GAD	LDEV
MPU-010	Enabled	00:02:28	DP-GAD	LDEV
MPU-010	Enabled	00:02:2C	DP-GAD	LDEV
MPU-010	Enabled	00:02:30	DP-GAD	LDEV
MPU-010	Enabled	00:02:34	DP-GAD	LDEV

Total:18444

Item	Description
MP Unit ID	MP unit ID
Auto Assignment	Auto assignment attribute for the MP unit
Resource ID	ID of this resource that the MP unit controls
Resource Name	The name of the resource that the MP unit controls. If "Type" is LDEV, the LDEV name that is set is displayed. A hyphen (-) displays for journal volumes or external volumes.
Type	The type of the resource that the MP unit controls

Parity Groups report

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

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"> If the number starts with "E" (for example, E1-1), the parity group contains external volumes (Hitachi Universal Volume Manager User Guide). If the number starts with "M" (for example, M1-1), the parity group contains volumes for FICON DM.
DKB	Name of the disk board that controls the parity group ¹
RAID Level	RAID level of the parity group ¹
Resource Group Name	Name of the resource group in which the parity group belongs
Resource Group ID	ID for the resource group in which the parity group belongs
Emulation Type	Emulation type of the parity group
Number of LDEVs (Total)	The number of the logical volumes in the parity group

Item	Description
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	<p>The type code of the drive in the parity group.</p> <ul style="list-style-type: none"> ▪ The type code of the first drive in the parity group. ▪ If the parity group contains external volumes, the drive type code displays the vendor, the model, and the serial number of the storage system. ▪ A hyphen (-) displays if the parity group contains volumes for FICON DM.
Drive Type/ Interface/RPM	<p>Drive type, drive control name, and revolutions-per-minute (RPM) of the drive in the parity group where the LDEV belongs¹</p> <p>A hyphen (-) is displayed instead of the RPM when the drive is not HDD.</p>
Drive Capacity	Capacity of the drive in the parity group ¹
RAID Concatenation #0	The number indicating a parity group #0 connected to this parity group ^{1,2}
RAID Concatenation #1	The number indicating a parity group #1 connected to this parity group ^{1,2}
RAID Concatenation #2	The number indicating a parity group #1,2 connected to this parity group ^{1,2}
Encryption	<p>Indicates whether the parity group is encrypted.</p> <ul style="list-style-type: none"> ▪ For internal volumes: Enabled (encrypted) or Disabled (not encrypted) ▪ For external volumes: A hyphen (-) is displayed
Accelerated Compression	<p>Accelerated compression of the parity group</p> <ul style="list-style-type: none"> ▪ If accelerated compression is supported, Enabled or Disabled is displayed. ▪ If accelerated compression is not supported, a hyphen (-) is displayed.
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"> ▪ When accelerated compression is supported, Enabled (the area is managed automatically) or Disabled (the area is not managed automatically) is displayed ▪ If accelerated compression is not supported, a hyphen (-) is displayed.

Item	Description
Notes:	
<ol style="list-style-type: none"> 1. A hyphen is displayed if the parity group contains external volumes or FICON DM volumes. 2. A hyphen is displayed if the parity group is not connected with another parity group or if the parity group contains external volumes including volumes for FICON DM. 	

Physical Devices report

The following table describes the items in the PDEVs report.

Item	Description
Location	PDEV name
CR#	<p>C# and R# (2-digit hexadecimal numbers that identify the PDEV Output in the format XX/YY, where:</p> <ul style="list-style-type: none"> ▪ XX: C# ▪ YY: R#
PG	PDEVs parity group
Emulation Type	PDEVs emulation type
Drive Type	<p>PDEVs drive type</p> <p>Output example: HDD, FMD DC2, SCM, SSD</p>
Interface	<p>PDEVs control type</p> <p>Output example: SAS, SATA, NVMe</p>
RPM	<p>Revolutions per minute</p> <p>Output example: 7200, 10000, 15000</p> <p>A hyphen (-) indicates that the drive is not a hard disk drive (HDD).</p>
Drive Type-Code	<p>Drive type code of the drive to which the parity group belongs</p> <p>Output example: SLB5E-M19RSS;SLB5G-M19RSS</p> <p>If multiple drive types are configured, they are separated by semicolons (;).</p>
Drive Size	<p>Drive size (inches)</p> <p>Output example: 2.5, 3.5</p>
Drive Capacity	Physical drive capacity (GB or TB)
Drive Version	Drive firmware version

Item	Description
DKB1	Name of the DKB1 controlling the PDEV
DKB2	Name of the DKB2 controlling the PDEV
DKB3	Name of the DKB3 controlling the PDEV
DKB4	Name of the DKB4 controlling the PDEV
Serial Number#	Serial number of this PDEV
RAID Level	RAID level of PDEVs Output example: RAID1(2D+2D), RAID5(7D+1P), RAID6(14D+2P)
RAID Concatenation#0	Number of parity group (#0) being concatenated to Physical drive Output example: 2-1, 3-1, 4-1
RAID Concatenation#1	Number of parity group (#1) being concatenated to Physical drive Output example: 2-1, 3-1, 4-1
RAID Concatenation#2	Number of parity group (#2) being concatenated to Physical drive Output example: 2-1, 3-1, 4-1
Resource Group Name	Name of the resource group to which the PDEV parity group belongs
Resource Group ID	ID of the resource group to which the PDEV parity group belongs (0 to 1023, decimal number)
Encryption	Encryption status of the parity group to which the PDEV belongs: <ul style="list-style-type: none"> ▪ Enabled: Encryption is enabled ▪ Disabled: Encryption is disabled

Ports report

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

Ports							
This report is about ports. A record is created for each port.							
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
CHB	Name of the channel board (also called a front-end director)
Type	Package type of the channel board
Port Location	Name of the port on the channel board
Port Attribute	Attribute of the port
iSCSI Virtual Port Mode	Mode of the iSCSI virtual port
TCP Port Number	Port number to use for a socket (decimal)
Internal WWN / Internal iSCSI Name	WWN / iSCSI name of the port
Fabric	One of the Fibre topology settings indicating the setting status of the Fabric switch ¹
Connection Type	One of the Fibre topology settings ¹ <ul style="list-style-type: none"> ▪ Point to Point ▪ FC-AL

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"> ▪ Enabled ▪ Disabled
IPv6 : Link Local Address	IPv6 link local address of the port (16-digit hexadecimal)
IPv6 : Global Address	IPv6 global address of the port. Output example: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (hexadecimal)
IPv6 : Global Address 2	IPv6 global address 2 of the port. Output example: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (hexadecimal)
IPv6 : Assigned Default Gateway	Assigned IPv6 default gateway
Selective ACK	Selective ACK mode <ul style="list-style-type: none"> ▪ Enabled ▪ Disabled
Ethernet MTU Size (Byte)	MTU settings (binary) <ul style="list-style-type: none"> ▪ 1,500
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"> ▪ Enabled ▪ Disabled
VLAN : ID	Number of VLAN set to the port (1 to 4,094)
CHAP User Name	User name for the CHAP authentication
iSNS Server : Mode	iSNS mode settings <ul style="list-style-type: none"> ▪ ON ▪ OFF

Item	Description
iSNS Server : IP Address	IP address of the iSNS server (30 to 65,535)
iSNS Server : TCP Port Number	Number of the TCP port used in iSNS (binary)
Address (Loop ID)	Fibre port address and Loop ID of the port ¹
Port Security	Security of the port ¹ <ul style="list-style-type: none"> ▪ Enabled ▪ Disabled
Speed	Data transfer speed of the port ¹
SFP Data Transfer Rate	Maximum transfer rate of SFP which the mounted package supports. <ul style="list-style-type: none"> ▪ 10G ▪ 16G ▪ 32G A hyphen (-) is displayed if "Type" is "2HS10S".
T10 PI Mode	Indicates whether the T10 PI mode can be applied to the port. <ul style="list-style-type: none"> ▪ Enabled ▪ Disabled ▪ Blank if the port type is a Fibre port other than 16FC2(CHB). For iSCSI ports, a hyphen (-) is displayed.
Resource Group Name	Name of the resource group to which the port belongs
Resource Group ID	ID for the resource group to which the port belongs (0 to 1023)
Number of Hosts	The number of the hosts registered to the port ¹
Number of LUNs	The number of the LU paths defined to the port ¹
Number of LDEVs	The number of the logical volumes that can be accessed through the port ¹
Number of PGs	The number of the parity groups having the logical volumes that can be accessed through the port ¹
Number of DKBs	The number of the disk boards controlling the parity group that contains the logical volumes that can be accessed through the port ¹
Notes: 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 if the storage system is 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.

A hyphen(-) is displayed if the power and temperature information cannot be acquired due to a unit or network failure.

Power Consumption				
This report is about power consumption and temperature. A record is created for each power consumption and temperature monitoring data.				
Date and Time	Power Consumption Average (W)	Power Consumption Maximum (W)	Power Consumption Minimum (W)	TEMP:DKCO
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
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:HSNBX0-HSNPANEL0 Average (degrees C)	Average temperature of HSNBX0:HSNPANEL0
TEMP:HSNBX0-HSNPANEL0 Maximum (degrees C)	Maximum temperature of HSNBX0:HSNPANEL0
TEMP:HSNBX0-HSNPANEL0 Minimum (degrees C)	Minimum temperature of HSNBX0:HSNPANEL0
TEMP:HSNBX1-HSNPANEL1 Average (degrees C)	Average temperature of HSNBX1:HSNPANEL1
TEMP:HSNBX1-HSNPANEL1 Maximum (degrees C)	Maximum temperature of HSNBX1:HSNPANEL1
TEMP:HSNBX1-HSNPANEL1 Minimum (degrees C)	Minimum temperature of HSNBX1:HSNPANEL1

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

Table 11 Power Consumption report for DKU00

Item	Description
TEMP:DKU00-DBS000-1 Average (Temperature in degrees C) , TEMP:DKU00-DBS000-1 Maximum (Temperature in degrees C) , TEMP:DKU00-DB000-1 Minimum (Temperature in degrees C) , ... ,TEMP:DKU00-DB007-2 Average (Temperature in degrees C) , TEMP:DKU00-DB-2 Maximum (Temperature in degrees C) , TEMP:DKU00-DB-2 Minimum (Temperature in degrees C)	Average temperature, maximum temperature, and minimum temperature of the drive box (DB) for the two-hour period. Outputs in the following format:

	<p>TEMP:DKUXX-DBYYY-DBPSYYY-A Average, Maximum, or Minimum (Temperature in degrees Celsius)</p> <ul style="list-style-type: none"> ▪ DKUXX: DKU location number (decimal) ▪ DBYYY or DBYYY&ZZZ: DB location number <p>The display format of DB location numbers differs depending on the type of DB.</p> <ul style="list-style-type: none"> • DBYYY: DBL location number (decimal) • DBYYY&ZZZ: Location number of DBS2, DBF3, or DBN (decimal) <p>Two DB numbers are written together, and then displayed as one DB location.</p> <ul style="list-style-type: none"> ▪ DBPSYYY-A: DBPS location number • YYY: DB location number (decimal) • A: DBPS number (1, 2)
--	--

Spare Drives report

The following figure shows an example of a spare drives report. The table following the figure describes the items in the report.

Spare Drives		
This report is about spare drives. A record is created for each spare drive.		
Drive Type-Code	Drive Capacity	Location
DKS5C-K300SS	300GB	HDD010-23
DKS5C-K300SS	300GB	HDD012-23
DKS5C-K300SS	300GB	HDD014-23
DKS5C-K300SS	300GB	HDD016-23
DKR5D-J900SS	900GB	HDD011-23
DKR5D-J900SS	900GB	HDD013-23
DKR5D-J900SS	900GB	HDD015-23
DKR5D-J900SS	900GB	HDD017-23
Total:8		

Item	Description
Drive Capacity	Capacity of the spare drive
Drive Type-Code	Type code of the spare drive
Location	Location of the spare drive

SSD Endurance report

The following figure shows an example of an SSD/SCM endurance report. The table following the figure describes the items in the report.

SSD Endurance			
This report is about endurance information of SSD. A record is created for each SSD.			
Drive Type-Code	Drive Capacity	Location	Used Endurance Indicator (%)
SLB5A-M800SS	800GB	HDD100-00	0
SLB5A-M800SS	800GB	HDD100-01	0
SLB5A-M800SS	800GB	HDD100-02	0
SLB5A-M800SS	800GB	HDD102-00	0
SLB5A-M800SS	800GB	HDD102-01	0
SLB5A-M800SS	800GB	HDD102-02	0
SLB5A-M800SS	800GB	HDD104-00	0
SLB5A-M800SS	800GB	HDD104-01	0
SLB5A-M800SS	800GB	HDD104-02	0
SLB5A-M800SS	800GB	HDD106-00	0
SLB5A-M800SS	800GB	HDD106-01	0
SLB5A-M800SS	800GB	HDD106-02	0
SLB5A-M400SS	400GB	HDD101-00	0
SLB5A-M400SS	400GB	HDD101-01	0
SLB5A-M400SS	400GB	HDD101-02	0
SLB5A-M400SS	400GB	HDD103-00	0
SLB5A-M400SS	400GB	HDD103-01	0
SLB5A-M400SS	400GB	HDD103-02	0
SLB5A-M400SS	400GB	HDD105-00	0
SLB5A-M400SS	400GB	HDD105-01	0
SLB5A-M400SS	400GB	HDD105-02	0
SLB5A-M400SS	400GB	HDD107-00	0
SLB5A-M400SS	400GB	HDD107-01	0
SLB5A-M400SS	400GB	HDD107-02	0
Total:24			

Item	Description
Drive Type-Code	Type code of the drive

Item	Description
Drive Capacity	Capacity of the drive
Location	Location of the drive
Used Endurance Indicator (%)	The used endurance of SSD life (0 to 100) The value of this indicator increases due to drive operation associated with internal processing of the storage system, and the host I/O. Even when no data is copied due to a drive failure, the value of this indicator increases because the spare drive also performs internal processing.

Storage System Summary report

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.

Storage System Summary

This report shows a summary of the storage system.

Storage System Type

VSP G1000

Serial Number

50

IP Address

126.10.50.15

Microcode Versions

Main	8003300805
HTP	800220
FHTP	800303
FCHF	800403
FOEF	800121
ISCF	800101
DKAF	800932
SVP	80033000
SSVP	80030000
FCDG	800003
FPCDG	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

Number of CUs

255

Shared Memory Size(GB)


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.
Software Versions	Version of the following programs. <ul style="list-style-type: none"> ▪ DKCMAIN ▪ HTP ▪ ISCF ▪ FCBK ▪ ISW ▪ DKB ▪ DKBN ▪ SVP ▪ CBA ▪ SSVP ▪ GUM ▪ FCDG ▪ ROMBOOT ▪ RAMBOOT ▪ Expander ▪ NSW ▪ CONFIG ▪ CFM ▪ HDD ▪ HDD (SVP) ▪ Printout Tool ▪ EDKBN
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 DKBs	The number of disk boards on the module

Item	Description
System Options	List of the system options specified for the storage system
Drive Capacity (TB)	Total capacity of drives in the storage system except for external volumes
Spare Drive Capacity (TB)	Total capacity of the spare drives in the storage system
Free Drive Capacity(TB)	Total capacity of the free drives in the storage system
OPEN Volume Capacity (GB) ¹	List of the capacity of the open volumes
M/F Volume Capacity (GB) ¹	The list of the capacity of the mainframe volumes and multi-platform volumes
Number of LDEVs ¹	<p>List of the numbers of the volumes in the following status.</p> <ul style="list-style-type: none"> ▪ allocated ▪ unallocated ▪ reserved ▪ free <p>The list for open-systems and the list for mainframe-systems are separate.</p>
Notes:	
1. You cannot sort this list.	

Report examples: graphical view

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

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

Cache Memories report

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

Cache Memories

This report shows cache memory data, including controller boards and DIMMs.

Shared Memory Size: 172GB

<DKC-0> Cache Size: 256GB																	
CTL01 <table border="1"> <tr><td>32GB</td></tr> <tr><td>32GB</td></tr> <tr><td>32GB</td></tr> <tr><td>32GB</td></tr> <tr><td>Not Installed</td></tr> <tr><td>Not Installed</td></tr> <tr><td>Not Installed</td></tr> <tr><td>Not Installed</td></tr> </table>	32GB	32GB	32GB	32GB	Not Installed	Not Installed	Not Installed	Not Installed	CTL02 <table border="1"> <tr><td>32GB</td></tr> <tr><td>32GB</td></tr> <tr><td>32GB</td></tr> <tr><td>32GB</td></tr> <tr><td>Not Installed</td></tr> <tr><td>Not Installed</td></tr> <tr><td>Not Installed</td></tr> <tr><td>Not Installed</td></tr> </table>	32GB	32GB	32GB	32GB	Not Installed	Not Installed	Not Installed	Not Installed
32GB																	
32GB																	
32GB																	
32GB																	
Not Installed																	
Not Installed																	
Not Installed																	
Not Installed																	
32GB																	
32GB																	
32GB																	
32GB																	
Not Installed																	
Not Installed																	
Not Installed																	
Not Installed																	

Channel Boards report

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

Channel Boards

This report shows channel boards, ports, types of channel boards.

<DKC-0> Number of Ports: 8			
Not Installed	CHB-02B 4HF32R(Fibre) 1D 3D 5D 7D	Not Installed	Not Installed
Not Installed	Not Installed	Not Installed	Not Installed
Not Installed	CHB-01B 4HF32R(Fibre) 1C 3C 5C 7C	Not Installed	Not Installed
Not Installed	Not Installed	Not Installed	Not Installed

Physical View report

This report shows controller chassis and drive box, and includes channel boards (also called front-end directors), disk boards (also called back-end directors), data drives, spare drives, and free drives

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

Physical View

This report shows controller chassis and drive boxes, and includes channel boards, disk boards, data drives, free drives, and spare drives.

Storage System Type: VSP 5000 series, Serial Number: 90620, Software Version = 9001400000

- [DKC-0](#)
- DKC-1
- DKC-2
- DKC-3
- DKC-4
- DKC-5
- [DKU00:DB-0&1](#)
- [DKU00:DB-2&3](#)
- [DKU00:DB-4&5](#)
- [DKU00:DB-6&7](#)
- DKU01:DB-8
- DKU01:DB-9
- DKU01:DB-10
- DKU01:DB-11
- DKU01:DB-12
- DKU01:DB-13
- DKU01:DB-14
- DKU02:DB-15
- DKU02:DB-16
- DKU02:DB-17
- DKU02:DB-18
- DKU02:DB-19
- DKU02:DB-20
- DKU02:DB-21
- DKU02:DB-22
- DKU02:DB-23
- DKU03:DB-24
- DKU03:DB-25
- DKU03:DB-26
- DKU03:DB-27
- DKU03:DB-28
- DKU03:DB-29
- DKU03:DB-30
- DKU03:DB-31
- DKU04:DB-32
- DKU04:DB-33
- DKU04:DB-34
- DKU04:DB-35
- DKU04:DB-36
- DKU04:DB-37
- DKU04:DB-38
- DKU04:DB-39
- DKU05:DB-40
- DKU05:DB-41
- DKU05:DB-42
- DKU05:DB-43
- DKU05:DB-44
- DKU05:DB-45
- DKU05:DB-46
- DKU05:DB-47
- DKU06:DB-48
- DKU06:DB-49
- DKU06:DB-50
- DKU06:DB-51
- DKU06:DB-52

DKC-0		
Not Installed	CHB-02B	DKB-02D
Not Installed	Not Installed	DKB-02H
Not Installed	CHB-01B	DKB-01D
Not Installed	Not Installed	DKB-01H

DKC-1

Not Installed

DKC-2

Not Installed

DKC-3

Not Installed

DKC-4

Not Installed

DKC-5

Not Installed

< Drive Box >

DKU-00

DB-0&1													
Free	Free	Free	Free	Free	Free	Free	Free	Free	Free	Free	Free	Free	Free

 HDD	 SSD	 Spare	 Free	 Not Installed
--	--	---	--	--

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 12 CacheInfo.csv file (Title: <<Cache>>)

Item	Content
Location	Name of cache package
CMG#0 Size(GB)	Cache memory capacity (in GB) of CMG(#0) in CTL
CMG#1 Size(GB)	Cache memory capacity (in GB) of CMG(#1) in CTL
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.
CFM#0 Type	CFM(#0) type in Cluster
CFM#1 Type	CFM(#1) type in Cluster

ChapUserInfo.csv

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

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

ChaStatus.csv

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

Item	Content
CHB Location	CHB name
PCB Status	Status of this CHB*
Port#00, #01, ..., #07	Status of ports on this CHB*
* 1: Normal, 0: Abnormal	

DeviceEquipInfo.csv

This CSV file contains information about equipment and devices that are part of the storage system, including power supplies and batteries for DKC, DB, and SVP. A record is created for each device.

Item	Content
Module#	Module number
Device Location	Device location name.
Equip Status	Equipment status of the device: <ul style="list-style-type: none"> ▪ Equipped ▪ Not Equipped
Status	Status of the device: <ul style="list-style-type: none"> ▪ Normal ▪ Abnormal ▪ Blank if "Equip Status" is Not Equipped

DkInfo.csv

This CSV file contains information about disk boards (DKBs). A record is created for each DKB.

Table 13 DkInfo.csv file (Title: <<DKA Information>>)

Item	Content
DKB Location	DKB name

Item	Content
Package Type	DKB type Example: <ul style="list-style-type: none"> ▪ DKB (2Port) ▪ EDKB (2Port) ▪ DKBN (2Port)

DkaStatus.csv

This CSV file contains information about the status of disk boards (DKBs). A record is created for each DKB.

Table 14 DkaStatus.csv file (Title: <<DKA Status>>)

Item	Content
DKB Location	DKB name
PCB Status	Status of this DKB ¹
BECON#00, #01	Status of BECON on this DKB ¹
BEPOR#0000, #0001, ..., #0003.	Status of BEPORT on this DKB. ¹ Items are output in the format of "BEPOR#XXYY". XX: BE controller number (2-digit hexadecimal (00)) YY: BE port number (2-digit hexadecimal (00 to 03))
Notes:	
1. 1: Normal, 0: Abnormal	

DkclInfo.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 15 DkclInfo.csv file (Title: <<DKC Information>>)

Item	Content
Storage System Type	Storage system type. Output example: VSP 5000 series
Serial Number #	Serial product number (in the decimal format, from 1 to 99999)

Item	Content
IP Address	IP address ¹ Output example: xxx.xxx.xxx.xxx (xxx is in decimal format)
Subnet Mask	Subnet mask ¹ Output example: xxx.xxx.xxx.xxx (xxx is in decimal format)
Number of CUs	Number of CUs (number in the decimal format) ¹
Number of DKBs	Number of DKBs (number in the decimal format) ²
Configuration Type	Configuration type ¹ Output example: PCM
DKC#	DKC Number
Notes: <ol style="list-style-type: none"> 1. The same value is output for all DKCs. 2. Different values are output for all DKCs. 	

DkuTempInfo.csv

This CSV file contains information about DB temperature for every two hours. The acquisition interval of temperature data cannot be changed from two hours. A record is DB temperature information obtained from the environment monitor. A record output to the first line shows the latest temperature information. Because DB temperature information is measured by DBPS, items are displayed in this unit*.

DkuTempInfo.csv shows the average temperature as DB temperature data. The total number of items is 1153.

The DB temperature data displayed in DkuTempAveInfo.csv (average temperature only), DkuTempMaxInfo.csv (maximum temperature only), and DkuTempMinInfo.csv (minimum temperature only) is the same value as the DB temperature data for DkuTempInfo.csv.

No records are created if the DKC is turned off. If the system is in maintenance mode or the SVP is rebooted, the data that is output every two hours might not contain data for the period.

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

Table 16 DkuTempInfo.csv file (Title: <<DKU temperature Information>>)

Item	Description
Date	Year, month, and date when temperature data was acquired in the format: YYYY/MM/DD hh:mm:ss

Item	Description
DKU00 DB000 DBPS0001 Temperature average	Average temperature (°C) for the two-hour period of DKU00 DB000 DBPS0001
DKU00 DB000 DBPS0001 Temperature maximum value	Maximum temperature (°C) for the two-hour period of DKU00 DB000 DBPS0001
DKU00 DB000 DBPS0001 Temperature minimum value	Minimum temperature (°C) for the two-hour period of DKU00 DB000 DBPS0001
DKU27 DB191 DBPS1912 Temperature average	Average temperature (°C) for the two-hour period of DKU27 DB191 DBPS1912
DKU27 DB191 DBPS1912 Temperature maximum value	Maximum temperature (°C) for the two-hour period of DKU27 DB191 DBPS1912
DKU27 DB191 DBPS1912 Temperature minimum value	Minimum temperature (°C) for the two-hour period ofDKU27 DB191 DBPS1912

Note: An item name is displayed as "DKU DByyy DBPSyyyya" or "DKUxx DByyy&zzz DBPSyyyya".

- DKUxx: DKU location number (decimal)
- DByyy or DByyy&zzz: DB location number
 - The display format of DB location numbers differs depending on the type of DB.
 - DByyy: DBL location number (decimal)
 - DByyy&zzz: Location number of DBS2, DBF3, or DBN (decimal)
 - Two DB numbers are written together, and then displayed as one DB location.
- DBPSyyyya: DBPS location number
 - yyy: DB location number (decimal)
 - a: DBPS number (1, 2)

The following table shows the locations and values for DKUxx, DByyy, and DByyy&zzz.

If DB is not implemented, the item name is displayed with the same as DBL, and the data part is blank. In the case of DBS2, DBF3, and DBN, the data of the same item is displayed twice in duplicate by DB location.

DKU #	0	1	2	3	4	5
x	0	1	0	1	0	1
y	0	0	1	1	2	2

DKU #	0	1	2	3	4	5
DKU _{xy}	DKU00	DKU10	DKU01	DKU11	DKU02	DKU12
DKUPS _{xy} zc	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
DKU _{xx}	DKU03	DKU13	DKU04	DKU14	DKU05	DKU15
DKU _{xy}	DKU03zc	DKU13zc	DKU04zc	DKU14zc	DKU05zc	DKU15zc

The following tables list DKUPS_{xyzc}: zc values (where DKC# is 0 and xy is 00)

DKU location number	DKU location number (DBS2/DBF3/DBN)			
DKU00	DB000&001	DB002&003	DB004&005	DB006&007
DKU01	DB008&009	DB010&011	DB012&013	DB014&015
DKU26	DB176&177	DB178&179	DB180&181	DB182&183
DKU27	DB184&185	DB186&187	DB188&189	DB190&191

DKU location number	DKU location number (DBS2/DBF3/DBN)							
DKU00	DB000	DB001	DB002	DB003	DB004	DB005	DB006	DB007
DKU01	DB008	DB009	DB010	DB011	DB012	DB013	DB014	DB015
DKU26	DB176	DB177	DB178	DB179	DB180	DB181	DB182	DB183
DKU27	DB184	DB185	DB186	DB187	DB188	DB189	DB190	DB191

A hyphen(-) is displayed if the power and temperature information cannot be acquired due to a unit or network failure.

DkuTempAveInfo.csv

This CSV file contains information about DB temperature for every two hours. The acquisition interval of temperature data cannot be changed from two hours. A record is DB temperature information obtained from the environment monitor. A record output to the first line shows the latest temperature information. Because DB temperature information is measured by DBPS, items are displayed in this unit*.

DkuTempAveInfo.csv shows the average temperature as DB temperature data. The total number of items is 385.

The DB temperature data displayed in DkuTempAveInfo.csv (average temperature only), DkuTempMaxInfo.csv (maximum temperature only), and DkuTempMinInfo.csv (minimum temperature only) is the same value as the DB temperature data for DkuTempInfo.csv.

No records are created if the DKC is turned off. If the system is in maintenance mode or the SVP is rebooted, the data that is output every two hours might not contain data for the period.

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

Table 17 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>YYYYMMDD hh:mm:ss</i>
DKU00 DB000 DBPS0001 Temperature average	Average temperature (°C) for the two-hour period of DKU00 DB000 DBPS0001
DKU27 DB191 DBPS1912 Temperature average	Average temperature (°C) for the two-hour period of DKU27 DB191 DBPS1912

Note: An item name is displayed as "DKU DByyy DBPSyyyya" or "DKUxx DByyy&zzz DBPSyyyya".

- DKUxx: DKU location number (decimal)
- DByyy or DByyy&zzz: DB location number

The display format of DB location numbers differs depending on the type of DB.

- DByyy: DBL location number (decimal)
- DByyy&zzz: Location number of DBS2, DBF3, or DBN (decimal)

Two DB numbers are written together, and then displayed as one DB location.

- DBPSyyyya: DBPS location number
 - yyy: DB location number (decimal)
 - a: DBPS number (1, 2)

See [DkuTempInfo.csv \(on page 230\)](#) for locations and values for DKUxx, DByyy, and DByyy&zzz.

A hyphen(-) is displayed if the power and temperature information cannot be acquired due to a unit or network failure.

DkuTempMaxInfo.csv

This CSV file contains information about DB temperature for every two hours. The acquisition interval of temperature data cannot be changed from two hours. A record is DB temperature information obtained from the environment monitor. A record output to the first line shows the latest temperature information. Because DB temperature information is measured by DBPS, items are displayed in this unit*.

DkuTempMaxInfo.csv shows the maximum temperature as DB temperature data. The total number of items is 385.

The DB temperature data displayed in DkuTempAveInfo.csv (average temperature only), DkuTempMaxInfo.csv (maximum temperature only), and DkuTempMinInfo.csv (minimum temperature only) is the same value as the DB temperature data for DkuTempInfo.csv.

No records are created if the DKC is turned off. If the system is in maintenance mode or the SVP is rebooted, the data that is output every two hours might not contain data for the period.

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

Table 18 DkuTempMaxInfo.csv file (Title: <<DKU temperature maximum value Information>>)

Item	Description
Date	Year, month, and date when temperature data was acquired in the format: YYYY/MM/DD hh:mm:ss
DKU00 DB000 DBPS0001 Temperature maximum value	Maximum temperature (°C) for the two-hour period of DKU00 DB000 DBPS0001
DKU27 DB191 DBPS1912 Temperature maximum value	Maximum temperature (°C) for the two-hour period of DKU27 DB191 DBPS1912

Note: An item name is displayed as "DKU DByyy DBPSyyyya" or "DKUxx DByyy&zzz DBPSyyyya".

- DKUxx: DKU location number (decimal)
- DByyy or DByyy&zzz: DB location number

The display format of DB location numbers differs depending on the type of DB.

- DByyy: DBL location number (decimal)
- DByyy&zzz: Location number of DBS2, DBF3, or DBN (decimal)

Two DB numbers are written together, and then displayed as one DB location.

- DBPSyyyya: DBPS location number
 - yyy: DB location number (decimal)
 - a: DBPS number (1, 2)

See [DkuTempInfo.csv \(on page 230\)](#) for locations and values for DKUxx, DByyy, and DByyy&zzz.

A hyphen(-) is displayed if the power and temperature information cannot be acquired due to a unit or network failure.

DkuTempMinInfo.csv

This CSV file contains information about DB temperature for every two hours. The acquisition interval of temperature data cannot be changed from two hours. A record is DB temperature information obtained from the environment monitor. A record output to the first line shows the latest temperature information. Because DB temperature information is measured by DBPS, items are displayed in this unit*.

DkuTempMinInfo.csv shows the minimum temperature as DB temperature data. The total number of items is 385.

The DB temperature data displayed in DkuTempAveInfo.csv (average temperature only), DkuTempMaxInfo.csv (maximum temperature only), and DkuTempMinInfo.csv (minimum temperature only) is the same value as the DB temperature data for DkuTempInfo.csv.

No records are created if the DKC is turned off. If the system is in maintenance mode or the SVP is rebooted, the data that is output every two hours might not contain data for the period.

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

Table 19 DkuTempMinInfo.csv file (Title: <<DKU temperature minimum value Information>>)

Item	Description
Date	Year, month, and date when temperature data was acquired in the format: YYYYIMMIDD hh:mm:ss
DKU00 DB000 DBPS0001 Temperature minimum value	Minimum temperature (°C) for the two-hour period of DKU00 DB000 DBPS0001

Item	Description
DKU27 DB191 DBPS1912 Temperature minimum value	Minimum temperature (°C) for the two-hour period of DKU27 DB191 DBPS1912

Note: An item name is displayed as "DKU DByyy DBPSyyyya" or "DKUxx DByyy&zzz DBPSyyyya".

- DKUxx: DKU location number (decimal)
- DByyy or DByyy&zzz: DB location number
The display format of DB location numbers differs depending on the type of DB.
 - DByyy: DBL location number (decimal)
 - DByyy&zzz: Location number of DBS2, DBF3, or DBN (decimal)
Two DB numbers are written together, and then displayed as one DB location.
- DBPSyyyya: DBPS location number
 - yyy: DB location number (decimal)
 - a: DBPS number (1, 2)

See [DkuTempInfo.csv \(on page 230\)](#) for locations and values for DKUxx, DByyy, and DByyy&zzz.

A hyphen(-) is displayed if the power and temperature information cannot be acquired due to a unit or network failure.

ELunInfo.csv

This CSV file contains information about external volumes. Information about one external volume is output to multiple records according to the number of prioritized paths between the local and the external storage systems.

For details about external volumes, see the *Hitachi Universal Volume Manager User Guide*.

Item	Content
VDEV#	Virtual device number to which the external volume is mapped
Characteristic1	Identification number of the external volume If the character string contains a comma, the comma is converted to a tab.
Characteristic2	Extended information for identifying the external volume
Device	Product name reported to the host by the external volume If the character string contains a comma, the comma is converted to a tab.
Capacity(blocks)	Capacity of the external volume (in blocks)

Item	Content
Cache Mode	<p>Indicates whether the write data from the host to the external storage system is reflected synchronously or asynchronously</p> <ul style="list-style-type: none"> ▪ Enabled: Asynchronously ▪ Disabled: Synchronously
ECC Group	<p>Number of parity group to which the external volume is mapped.</p> <p>If the number starts with "E" (for example, E1-1), the parity group contains external volumes.</p>
Current MPU	<p>Number of a current MP unit controlling the parity group to which the external volume is mapped</p>
Setting MPU	<p>Number of an MP unit configured to control the external volume indicated by ECC Group</p>
Vendor	<p>Vendor name of the external storage system</p>
Product Name	<p>Product name of the external storage system</p>
Serial Number#	<p>Serial product number of the external storage system</p>
Path Mode	<p>Mode which indicates how the paths between local and external storage systems operate</p> <ul style="list-style-type: none"> ▪ Multi ▪ Single ▪ ALUA
Port	<p>Name of a local port from which the external path is connected to the external storage system</p>
WWN	<p>Port identifier number of the external storage system</p> <p>This item is blank when the "Package Type" is iSCSI.</p>
LUN	<p>LU number set for the external volume.</p>
Priority	<p>Priority of the paths between the storage systems to be used for connection with the external volume.</p> <p>"1" indicates the path with the highest priority.</p>
Status	<p>Status of the path between storage systems.</p> <ul style="list-style-type: none"> ▪ Normal ▪ Blocked
IO TOV	<p>I/O timeout value for the external volume</p>

Item	Content
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	<p>I/O load balance distribution logic specified for external volume:</p> <ul style="list-style-type: none"> ▪ Normal Round-robin ▪ Extended Round-robin ▪ Disabled ▪ - (hyphen): Single is specified in Path Mode.
Path Mode on Profile	<p>Path mode on profile information of the external storage system:</p> <ul style="list-style-type: none"> ▪ Multi ▪ Single
ALUA Settable	<p>Indicates whether ALUA mode can be set as path mode on the external storage system</p> <ul style="list-style-type: none"> ▪ Yes: ALUA mode can be set ▪ No: ALUA mode cannot be set
ALUA Permitted	<p>Indicates whether ALUA is used as path mode on the local storage system:</p> <ul style="list-style-type: none"> ▪ Enabled: ALUA mode is used ▪ Disabled: ALUA mode is not used
Target Port Asymmetric Access State	<p>Status of the port on the external storage system when the path mode is ALUA:</p> <ul style="list-style-type: none"> ▪ Active/Optimized ▪ Active/Non-Optimized ▪ Blank: The path mode is other than ALUA.
Package Type	<p>Type of CHB to which a port of the local storage system connecting to the external storage system belongs:</p> <ul style="list-style-type: none"> ▪ Output example for FC: 4HF32R(Fibre) ▪ Output example for iSCSI: 2HS10S(iSCSI) ▪ Output example for FICON: 4Mx16(Mfibre)

Item	Content
IP Address	<p>IP address for an iSCSI target of an external storage system</p> <ul style="list-style-type: none"> ▪ IPv6: (XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX) XX: 00 to FF (hexadecimal) ▪ IPv4: (XXX.XXX.XXX.XXX) XXX: 0 to 255 (decimal) ▪ Blank: The "Package Type" is other than iSCSI.
TCP Port Number	<p>TCP port number (1 through 65535) for the iSCSI target of an external storage system</p> <p>This item is blank when the "Package Type" is other than iSCSI.</p>
iSCSI Target Name	<p>iSCSI target name of an external storage system</p> <p>This item is blank when the "Package Type" is other than iSCSI.</p>
Virtual Port ID	<p>Virtual port number of own storage system to which external storage system is connected.</p> <p>If Virtual Port Mode is Disabled, this column to be blanked.</p>

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 if the DKC is 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	<p>Year, month, and date when record data was acquired for the two-hour period in the format:</p> <p>YYYY/MM/DD HH:MM:SS</p>
Electric power average	Average value of electric power (W)
Electric power maximum value	Maximum value of electric power (W)

Item	Description
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"> ▪ When the storage system is starting up ▪ Right after replacing storage system parts ▪ During or after microcode update
DKC0 CLT01 Temperature average	DKC0: Average temperature of CLT01 (°C)
DKC0 CLT01 Temperature maximum value	DKC0: Maximum temperature of CLT011 (°C)
DKC0 CLT01 Temperature minimum value	DKC0: Minimum temperature of CLT01 (°C)
DKC5 CLT52 Temperature average	DKC5 CLT52: Average temperature of CL2 (°C)
DKC5 CLT52 Temperature maximum value	DKC5 CLT52: Maximum temperature of CL2 (°C)
DKC5 CLT52 Temperature minimum value	DKC5 CLT52: Minimum temperature of CL2 (°C)

A hyphen(-) is displayed if the power and temperature information cannot be acquired due to a unit or network failure.

HSNBXTemplInfo.csv

This CSV file contains information about HSNBX temperature for every two hours. The acquisition interval of temperature data cannot be changed from two hours. A record is HSNBX temperature information obtained from the environment monitor. A record output to the first line shows the latest temperature information.

No records are created if the DKC is 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: YYYY/MM/DD HH:MM:SS
HSNBX0 HSNPANEL0 Temperature average	HSNBX0: Average temperature of CLT01 (°C)
HSNBX0 HSNPANEL0 Temperature maximum value	HSNBX0: Maximum temperature of CLT01 (°C)
HSNBX0 HSNPANEL0 Temperature minimum value	HSNBX0: Minimum temperature of CLT01 (°C)
HSNBX1 HSNPANEL1 Temperature average	HSNBX1: Average temperature of CL2 (°C)
HSNBX1 HSNPANEL1 Temperature maximum value	HSNBX1: Maximum temperature of CL2 (°C)
HSNBX1 HSNPANEL1 Temperature minimum value	HSNBX1: Minimum temperature of CL2 (°C)

A hyphen(-) is displayed if the power and temperature information cannot be acquired due to a unit or network failure.

HdulInfo.csv

This CSV file contains information about drive boxes (DBs). A record is created for each DB.

Table 20 HdulInfo.csv file (Title: <<HDU Information>>)

Item	Content
DB Location	DB location name Output example: HDU000
DB Status	Information about whether this DB is installed or not <ul style="list-style-type: none"> ▪ Installed ▪ Not Installed

Item	Content
Slot Size	Slot size (inches) <ul style="list-style-type: none"> ▪ 2.5 ▪ 3.5 ▪ Blank when DB is DBF3(FMD DC2)
DB Type	DB type of HDU <ul style="list-style-type: none"> ▪ DBL (DB for 3.5-inch drive) ▪ DBS2 (2.5 inch SAS DB) ▪ DBF3 (DB for FMD DC2) ▪ DBN (2.5-inch NVMe DB)

IscsiHostInfo.csv

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

Item	Content
Port	Port name
iSCSI Name	iSCSI host name
Host Name	Nickname for iSCSI host name
iSCSI Target ID ¹	iSCSI target number (hexadecimal format, 00 to fe)
Notes:	
1. For the target information, see the record information with the same iSCSI target ID in IscsiTargetInfo.csv.	

IscsiPortInfo.csv

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

Item	Content
Port	Port name
IPv4 IP Address	IPv4 address Output example: xxx.xxx.xxx.xxx (decimal)

Item	Content
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"> ▪ Enabled ▪ Disabled
IPv6 Link Local Address	Port IPv6 link local address <ul style="list-style-type: none"> ▪ Output example: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (hexadecimal) ▪ Output example: Auto Auto is displayed if the link local address is automatically set. Blank if "IPv6 Mode" is Disabled.
IPv6 Global Address	IPv6 global address of the port <ul style="list-style-type: none"> ▪ Output example: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (hexadecimal) ▪ Output example: Auto Auto is displayed if the global address is automatically set. Blank if "IPv6 Mode" is Disabled.
IPv6 Assigned Default Gateway	Port IPv6 assigned default gateway <ul style="list-style-type: none"> ▪ Output example: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (hexadecimal) Blank if "IPv6 Mode" is Disabled.
Channel Speed	Data transfer speed of the port (for example, 1G, 10G, Auto)
Security Switch	Port security switch settings <ul style="list-style-type: none"> ▪ On ▪ Off
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"> ▪ 1500 ▪ 4500 ▪ 9000
Keep Alive Timer (sec.)	Keep alive timer value of iSCSI (30 to 64800) (sec)

Item	Content
Selective ACK	Selective ACK mode <ul style="list-style-type: none"> ▪ Enabled ▪ Disabled
Delayed ACK	Delayed ACK mode <ul style="list-style-type: none"> ▪ Enabled ▪ Disabled
Maximum Window Size (KB)	Window scale option settings <ul style="list-style-type: none"> ▪ 64KB ▪ 128KB ▪ 256KB ▪ 512KB ▪ 1024KB
iSNS Server Mode	iSNS mode settings <ul style="list-style-type: none"> ▪ On ▪ Off
iSNS Server IP Address	IP address of the iSNS server <ul style="list-style-type: none"> ▪ IPv4: xxx.xxx.xxx.xxx (decimal) ▪ IPv6: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (hexadecimal) ▪ Blank if "iSNS Server Mode" is Off.
iSNS Server TCP Port Number	Port number of TCP used for iSNS (1 to 65535). Blank if "iSNS Server Mode" is Off.
VLAN Tagging Mode	VLAN tagging mode set to the port <ul style="list-style-type: none"> ▪ On ▪ Off
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

Item	Content
CHAP User Name	Authenticated user name of the port
IPv6 Global Address 2	<p>IPv6 global address 2 of the port</p> <ul style="list-style-type: none"> ▪ Output example: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (hexadecimal) ▪ Output example: Auto <p>Auto is displayed if the global address 2 is automatically set. Blank if "IPv6 Mode" is Disabled.</p>
Virtual Port Mode	<p>Virtual port mode of the port</p> <ul style="list-style-type: none"> ▪ Enabled ▪ Disabled

IscsiTargetInfo.csv

This CSV file contains information about iSCSI target information set to the channel board port. A record is created for each iSCSI target.

Item	Content
Port	Port name
iSCSI Target Alias	iSCSI target alias
iSCSI Target ID	Number of the iSCSI target (00 to fe, hexadecimal)
iSCSI Target Name	Name of the iSCSI target
Host Mode	Host mode set to the iSCSI target (hexadecimal)
Host Mode Option	<p>Host mode option set to the iSCSI target (decimal)</p> <p>Separated with a semicolon (;) if multiple host mode options are set.</p>
Security Switch	<p>Security switch status set to the iSCSI target port</p> <ul style="list-style-type: none"> ▪ On ▪ Off
Authentication Method	<p>Authentication method settings of the iSCSI target</p> <ul style="list-style-type: none"> ▪ CHAP ▪ None ▪ Comply with Host Setting

Item	Content
Authentication Mutual CHAP	Mutual CHAP authentication function settings of the iSCSI target <ul style="list-style-type: none"> ▪ Enabled ▪ Disabled
Authentication User Name	User name set when iSCSI target was authenticated
Resource Group ID (iSCSI Target)	Resource group ID of the iSCSI target (0 to 1023)
Resource Group Name (iSCSI Target)	Resource group name of the iSCSI target

JnlInfo.csv

This CSV file contains information about Journals. A record is created for each journal.

Table 21 JnlInfo.csv file (Title: <<JNL Information>>)

Item	Content
JNL#	Journal number (in the hexadecimal format)
Current MPU	Number of MP unit currently controlling the journal
Setting MPU	Number of MP unit 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"> ▪ Internal OPEN Volumes ▪ Internal Mainframe Volumes ▪ External OPEN Volumes ▪ External Mainframe Volumes ▪ Total OPEN Volumes ▪ Total Mainframe Volumes

Item	Content
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"> ▪ Internal Volumes ▪ External Volumes ▪ Total Volumes
Allocated OPEN LDEVs	Number of allocated open-system volumes (LDEVs)
Unallocated OPEN LDEVs	Number of unallocated open-system volumes (LDEVs)
Reserved OPEN LDEVs	Number of reserved open-system volumes (LDEVs)
Allocated Mainframe LDEVs	Number of allocated mainframe and multi-platform volumes (LDEVs)
Reserved Mainframe LDEVs	Number of reserved mainframe and multi-platform volumes (LDEVs)
V-VOL	Number of virtual volumes This item is output only when "Volume Kind" is Total Volumes. This item is blank when "Volume Kind" is Internal Volumes or External Volumes.

Item	Content
Total(All LDEVs)	Total number of LDEVs
ECC Groups	Total number of parity groups

LdevInfo.csv

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

For details about LDEVs, see the *Provisioning Guide*.

Item	Content
ECC Group	Number of parity group to which the LDEV belongs <ul style="list-style-type: none"> ▪ If the number starts with "E" (for example, E1-1), the parity group contains external volumes. ▪ If the number starts with "M" (for example, M1-1), the parity group contains FICON[®] DM volumes. ▪ If "LDEV Type" is Dynamic Provisioning, Thin Image, or ALU (Administrative Logical Unit), a hyphen (-) is output.
LDEV#	LDEV number
LDEV Name	LDEV name If the character string contains a comma, the comma is converted to a tab.
LDEV Emulation	LDEV emulation type
LDEV Type	LDEV type: <ul style="list-style-type: none"> ▪ Basic ▪ Dynamic Provisioning ▪ External ▪ Thin Image (Thin Image virtual volume) ▪ ALU
LDEV Attribute	LDEV Attribute: <ul style="list-style-type: none"> ▪ CMDDEV (Command device) ▪ CMDDEV* (Remote command device) ▪ Journal (Journal volume) ▪ Pool (Pool volume) ▪ Reserve (Reserved volume)

Item	Content
	<ul style="list-style-type: none"> ▪ Quorum disk (Quorum Disk used with global-active device) ▪ TSE (Volume for Hitachi Compatible FlashCopy[®]) ▪ ALU ▪ SLU (Subsidiary Logical Unit) ▪ Deduplication system data volume ▪ Regular (Others)
Volume Size(Cyl)	LDEV capacity (in cylinders)
Volume Size(MB)	LDEV capacity (in MB)
Volume Size(Blocks)	LDEV capacity (in blocks)
CVS	<p>Information about whether the LDEV is a custom-sized volume:</p> <ul style="list-style-type: none"> ▪ On: The volume is a custom-sized volume. ▪ Off: "Off" is output for all other volumes.
Pool ID	<p>Pool number</p> <p>The pool number is output in the following cases:</p> <ul style="list-style-type: none"> ▪ "LDEV Type" is Dynamic Provisioning ▪ LDEV Attribute is Pool <p>This item is blank for all other cases.</p>
RAID Concatenation#0	<p>Number of parity group to be concatenated to parity group (#0) identified by ECC Group</p> <p>This item is blank when the parity group is not concatenated to another parity group.</p>
RAID Concatenation#1	<p>Number of parity group to be concatenated to parity group (#1) identified by ECC Group</p> <p>This item is blank when the parity group is not concatenated to another parity group.</p>
RAID Concatenation#2	<p>Number of parity group to be concatenated to parity group (#2) identified by ECC Group</p> <p>This item is blank when the parity group is not concatenated to another parity group.</p>
ORACLE CHECK SUM	<p>Information about whether this LDEV is Oracle check sum target:</p> <p>For open-systems and multi-platform volumes:</p> <ul style="list-style-type: none"> ▪ On ▪ Off

Item	Content
	For mainframe volumes, this item is blank.
Current MPU	Number of MP unit currently controlling the LDEV
Setting MPU	Number of MP unit configured to control LDEV
Allocated	<p>Information about whether this LDEV is allocated to a host:</p> <ul style="list-style-type: none"> ▪ For open-systems volumes, Y indicates that the volume is accessible to the host. For mainframe and multi-platform volumes, Y is output for all volumes except Reserved volumes. ▪ For open-systems volumes, N indicates that the volume is not accessible to the host. For mainframe and multi-platform volumes, N indicates that the volume is Reserved.
Pool Name	<p>Name of the pool indicated by Pool ID</p> <p>If the character string contains a comma, the comma is converted to a tab.</p>
CmdDevSecurity	<p>Indicates whether Security is specified as the attribute for the command device:</p> <ul style="list-style-type: none"> ▪ Enabled: Command device security is set. ▪ Disabled: Command device security is not set. ▪ Blank: "LDEV Attribute" is not CMDDEV.
CmdDevUserAuth	<p>Indicates whether User Authentication is specified as the attribute for the command device:</p> <ul style="list-style-type: none"> ▪ Enabled: User authentication is set. ▪ Disabled: User authentication is not set. ▪ Blank: "LDEV Attribute" is not CMDDEV.
CmdDevDevGrpDef	<p>Indicates whether Device Group Definition is specified as the attribute for the command device:</p> <ul style="list-style-type: none"> ▪ Enabled: Device group definition is set. ▪ Disabled: Device group definition is not set. ▪ Blank: "LDEV Attribute" is not CMDDEV.
Resource Group ID (LDEV)	LDEV resource group ID (decimal number)
Resource Group Name (LDEV)	LDEV resource group name

Item	Content
Encryption	Indicates whether the parity group identified by ECC Group is encrypted: For internal volumes: <ul style="list-style-type: none"> ▪ Enabled (encrypted) ▪ Disabled (not encrypted) For external volumes, this item is blank.
ALUA Mode	Indicates whether the ALUA mode is enabled: <ul style="list-style-type: none"> ▪ Enabled ▪ Disabled ▪ Blank: The volume is a mainframe volume.
T10 PI	Indicates the T10 PI attribute set for the LDEV: <ul style="list-style-type: none"> ▪ Enabled ▪ Disabled ▪ Blank: The "LDEV Emulation" is not OPEN-V.
Accelerated Compression	Indicates whether accelerated compression is enabled: For internal volumes: <ul style="list-style-type: none"> ▪ Enabled: Accelerated compression is enabled. ▪ Disabled: Accelerated compression is disabled. ▪ Blank: The parity group with LDEV does not support accelerated compression. For external volumes, this item is blank.

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"> ▪ 1: Normal ▪ 0: Abnormal
HDEV#	LDEV number

Item	Content
HDEV Status	LDEV status <ul style="list-style-type: none"> ▪ 1: Normal ▪ 0: Abnormal
LDEV Emulation	LDEV emulation type
ECC Group	Number of the parity group where the LDEV belongs. <ul style="list-style-type: none"> ▪ If the number starts with "E" (for example, E1-1), the parity group contains external volumes. ▪ If the type of the LDEV is a Dynamic Provisioning, Thin Image, or ALU virtual volume, a hyphen is output. Refer to "LdevInfo.csv" for information about the LDEV type.

LogPathStatus.csv

This CSV file contains information about mainframe logical paths.

Table 22 LogPathStatus.csv file (Title: <<Main Frame Logical Path Status>>)

Item	Content
LPN#	Logical path number (in the hexadecimal format)
CHB Location	CHB 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 about the cache logical partitioning function, see the *Performance Guide*.

Item	Content
CLPR#	CLPR ID (decimal number)
CLPR Name	Name of the CLPR
Cache Size(MB)	Cache size (in MB) allocated to this CLPR ID
Cache Residency Size(MB)	Cache Residency Manager cache size (in MB) allocated to this CLPR ID
ECC Group	Number of parity group allocated to this CLPR ID
LDEV#(V-VOL)	Number of LDEVs allocated to this CLPR ID The type of this LDEV is Dynamic Provisioning, Thin Image, or ALU. This item is blank when no LDEVs are assigned to the CLPR ID.

LunInfo.csv

This CSV file contains information about LU path definitions. A record is created for each LU path definition. When only the port name (Port) is output, it indicates that no LU path is defined for the port (which is used only for a remote path or an external path). For details about LU path definitions, see the *Provisioning Guide for Open Systems*. For information about iSCSI targets, see *lscsiTargetInfo.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 (;). This item is blank when no host mode option has been specified.
LUN#	LUN number for this LU path definition (hexadecimal) This item is blank when no LU path is defined for the host group.
LDEV#	LDEV number for this LU path definition This item is blank when no LU path is defined for the host group.

Item	Description
Command Device	Information about whether the LDEV is a command device: <ul style="list-style-type: none"> ▪ On: Command Device ▪ On*: Remote Command Device ▪ Off: Others ▪ Blank: No LU path is defined for the host group.
Command Security	Information about whether the command device is secured: <ul style="list-style-type: none"> ▪ On ▪ Off ▪ Blank: No LU path is defined for the host group.
CVS	Information about whether the LDEV is a custom-sized volume: <ul style="list-style-type: none"> ▪ On: Customized volume ▪ Off: Other volumes ▪ Blank: No LU path is defined for the host group.
CHB Location	Name of the CHB on which this port is installed
Package Type	CHB type for CHB Location Output example for Fibre: 4HF32R(Fibre) Output example for iSCSI: 2HS10S(iSCSI) Output example for FICON [®] : 4Mx16(Mfibre)
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"> ▪ Enabled ▪ Disabled ▪ Blank: "Package Type" does not support T10 PI mode.
T10 PI	Information about the T10 PI attribute which is set for the LDEV number of the LU path definition. <ul style="list-style-type: none"> ▪ Enabled ▪ Disabled ▪ Blank: The LDEV# is blank.

Item	Description
Asymmetric Access State	Asymmetric access status (output only for an open-systems CHB that is FC or FCoE) Indicates the asymmetric access status: <ul style="list-style-type: none"> ▪ Active/Optimized: Prioritized ▪ Active/Non-Optimized: Lower priority ▪ Blank: "Package Type" is iSCSI

LunPortInfo.csv

This CSV file contains information about LU path definition. A record is created for each port.

For details of LU path definition, see the *Provisioning Guide 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"> ▪ On ▪ Off
Port Address	Port address (2-digit hexadecimal number) 00 to ff This item is blank when "Package Type" is iSCSI.
Loop ID	Port address (0 - 125, decimal) This item is blank when "Package Type" is iSCSI.
Fabric	Setting status of the Fabric switch: <ul style="list-style-type: none"> ▪ On ▪ Off ▪ Blank: "Package Type" is iSCSI.
Connection	Fibre topology setting: <ul style="list-style-type: none"> ▪ Point to Point ▪ FC-AL ▪ Blank: "Package Type" is iSCSI.
Channel Speed	Channel speed of this port (for example, 4G, 10G, 32G)
WWN	WWN of this port (hexadecimal number)

Item	Content
	This item is blank when "Package Type" is iSCSI.
CHB Location	CHB on which the port is installed.
Package Type	CHB type for CHB Location Output example for Fibre: 4HF32R(Fibre) Output example for iSCSI: 2HS10S(iSCSI) Output example for FICON®: 4Mx16(Mfibre)
T10 PI Mode	Indicates whether the T10 PI mode can be applied to the port: <ul style="list-style-type: none"> ▪ Enabled ▪ Disabled

MfDMInfo.csv

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

Table 23 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 MPU	Number of the MP unit that is controlling the migration volume
Setting MPU	Number of the MP unit 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 24 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)

Item	Content
DKB	DKB microcode version (6 digits)
SVP	The version of the microcode installed on the service processor (8 digits)
CBA	CBA version (12 digits)
SSVP	SSVP microcode version (6 digits)
FCDG	FCDG microcode version (6 digits)
ROM BOOT	ROM BOOT microcode version (6 digits)
RAM BOOT	RAM BOOT 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
ISCF	ISCF version (8 digits)
GUM	GUM firmware version (8 digits)
FCBK	FCBK version (8 digits)
ISW	ISW firmware version (8 digits)
DKBN	DKBN version (6 digits)
NSW	NSW version (6 digits)
EDKBN	EDKBN version (6 digits)

MlcEnduranceInfo.csv

This CSV file contains information about endurance information of SSD, SCM, or FMD DC2. A record is created for each SSD, SCM, or FMD DC2 endurance information.

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

Item	Content
ECC Group	Number of parity groups.
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 (%)	The current used endurance of SSD life (0 to 100) The value of this indicator increases due to drive operation associated with internal processing of the storage system, and the host I/O. Even when no data is copied due to a drive failure, the value of this indicator increases because the spare drive also performs internal processing.
History1 (date)	Date on which the used endurance of SSD life was acquired (1 month ago)
History1 (%)	The used endurance of SSD life (0 to 100)(1 month ago)
History2 (date)	Date on which the used endurance of SSD life was acquired (2 months ago)
History2 (%)	The used endurance of SSD life (0 to 100) (2 months ago)
History3 (%) ... History 119 (%)	Life (0 to 100) (3 months ago ...119 months ago)
History120 (date)	Date on which the used endurance of SSD life was acquired (120 months ago)
History120 (%)	The used endurance of SSD life (0 to 100) (120 months ago)

ModePerLpr.csv

This CSV file contains information about system option modes. A record is created for each system option mode.

Item	Content
System Option Mode#	System option mode # (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"> ▪ If the system option mode is on: On ▪ If the system option mode is not on: Blank

MpPathStatus.csv

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

Table 25 MpPathStatus.csv file (Title: <<MP Path Status>>)

Item	Content
MPU#/CTL#	MP unit number or CTL number (2-digit hexadecimal numbers): <ul style="list-style-type: none"> ▪ For MP unit number MPU#00 to MPU#0b ▪ For CTL number CTL#00 to CTL #0b
CMG#00-00 to CMG#00-0b CMG#01-00 to CMG#01-0b CMG#02-00 to CMG#02-0b CMG#03-00 to CMG#03-0b	Cache module path status for MP unit number in the format of "CMG#XX-YY". ¹ (CMG#XX-YY) XX: I path (00 to 03), YY: CMG# (00 to 0b)
MPU#00-00 to MPU#00-0b MPU#01-00 to MPU#01-0b MPU#02-00 to MPU#02-0b MPU#03-00 to MPU#03-0b	MP unit path status for MP unit number in the format of "MPU#XX-YY". ¹ MPU#XX-YY) XX: I path (00 to 03), YY: MPU# (00 to 0b)

Item	Content
CMG#00-00 to CMG#00-0b CMG#01-00 to CMG#01-0b CMG#02-00 to CMG#02-0b CMG#03-00 to CMG#03-0b	Cache module path status for CTL number in the format of "CMG#XX-YY". ¹ (CMG#XX-YY) XX: I path (00 to 03), YY: CMG# (00 to 0b): MSW number in one module (2-digit number in the hexadecimal format)
MPU#00-00 to MPU#00-0b MPU#01-00 to MPU#01-0b MPU#02-00 to MPU#02-0b MPU#03-00 to MPU#03-0b	MP unit path status for CTL number in the format of "MPU#XX-YY". ¹ (MPU#XX-YY) XX: I path (00 to 03), YY: MPU# (00 to 0b)
Notes:	
1. 1=Normal, 0=Abnormal	

MpPcbStatus.csv

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

Table 26 MpPcbStatus.csv file (Title: <<MP PCB Status>>)

Item	Content
MPU ID	MP unit ID
Auto Assignment	Information about whether this MP unit is set to be automatically assigned to each resource or not <ul style="list-style-type: none"> ▪ Enabled Set to be automatically assigned ▪ Disabled Not set to be automatically assigned
PCB Status	MP unit status ¹
MP#00, #01, #02..., #13	MP status on MP unit #0 to #13 ¹

Item	Content
Notes:	
1. 1=Normal, 0=Abnormal	

PcbRevInfo.csv

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

Item	Content
Location	Part name
FRU number	Product name of the package or some other name
PK Revision	Revision of the package
Factory	Factory manufacturing the package
Number	Serial number of the package
MAC Address	MAC address of the package

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"> ▪ OPEN System (TB) ▪ Mainframe System (TB) ▪ Total Capacity (TB) ▪ Number of PDEVs
HDD Drive	HDD drive capacity (TB)
Spare Drive	Spare drive capacity (TB)
SSD Drive	SSD/SCM capacity (TB)
Free Drive	Free drive capacity (TB)

PdevInfo.csv

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

Item	Content
ECC Group	Number of parity group of which this PDEV is a component: <ul style="list-style-type: none"> Spare Drive: For spare drives
Emulation Type	Emulation type for the parity group indicated by "ECC Group" This item is blank when the ECC Group is Spare Drive.
CR#	C# and R# (2-digit hexadecimal numbers that identify the PDEV) Output in the format XX/YY, where: <ul style="list-style-type: none"> XX: C# YY: R#
PDEV Location	PDEV location name
Device Type	Drive type (for example, HDD, SSD, FMD, SCM)
Interface	Drive control name (for example, NVMe, SAS, SATA)
RPM	Revolutions per minute A hyphen (-) is output when the drive type is not HDD.
Device Type-Code	Device type code of this drive (for example, DKR5D-J600SS)
Device Size	Drive size (inches) (for example, 2.5, 3.5) This item is blank when the drive type is FMD.
Device Capacity	Drive capacity (GB or TB)
Drive Version	Drive firmware version
DKB1	Name of the DKB (1) controlling the PDEV
DKB2	Name of the DKB (2) controlling the PDEV
DKB3	Name of the DKB (3) controlling the PDEV
DKB4	Name of the DKB (4) controlling the PDEV
Serial Number #	Serial number of this drive
RAID Level	RAID level of the parity group indicated by "ECC Group" This item is blank when the "ECC Group" is Spare Drive
RAID Concatenation #0	Number of parity group to be concatenated to parity group (#0) identified by "ECC Group"

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

PdevStatus.csv

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

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

PhyPathStatus.csv

This CSV file contains information about mainframe physical paths.

Table 27 PhyPathStatus.csv file (Title: <<Main Frame Physical Path Status>>)

Item	Content
Module#	Module number
CHB Location	CHB 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"> ▪ VALID (CUR) ▪ INVALID
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"> ▪ 2 Gbps ▪ 4 Gbps ▪ 8 Gbps

PkInfo.csv

This CSV file contains information about channel boards (CHBs). A record is created for each CHB.

Table 28 PkInfo.csv file (Title: <<PK>>)

Item	Content
CHB Location	CHB name
DKC Emulation	DKC emulation type
Port#	Number of the port installed on the CHB (2-digit number in the hexadecimal format)
Port	Name of port installed on the CHB
Package Type	CHB type CHB for CHB location: <ul style="list-style-type: none"> ▪ Fibre: 4HF32R (Fibre) ▪ iSCSI: 2HS10S (iSCSI) ▪ FICON: 4Mx16 (Mfibre)
SFP Kind	SFP (Small Form factor Pluggable) kind: <ul style="list-style-type: none"> ▪ Short Wave ▪ Long Wave

Item	Content
SFP Status	SFP status: <ul style="list-style-type: none"> ▪ Normal ▪ Failed ▪ Not Fix
Port Type	Port type Output example: <ul style="list-style-type: none"> ▪ Bidirectional ▪ Target ▪ HTP ▪ FNP
Fabric	One of the Fibre topology settings indicating the setting status of the Fabric switch (output only for an open system CHB that is Fibre or FCoE): <ul style="list-style-type: none"> ▪ On ▪ Off
Connection	One of the Fibre topology settings (output only for an open system CHB that is Fibre or FCoE) <ul style="list-style-type: none"> ▪ Point to Point ▪ FC-AL
Port Address	Port address (2-digit number in the hexadecimal format) Output only for an open system CHB that is Fibre or FCoE
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 CHB 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"> ▪ Enabled ▪ Disabled
SFP Data Transfer Rate	Maximum SFP data transfer rate that is supported by installed packages: <ul style="list-style-type: none"> ▪ 8G ▪ 10G

Item	Content
	<ul style="list-style-type: none"> ▪ 16G ▪ 32G

PplInfo.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 \(on page 176\)](#).

Item	Content
Program Product Name	Software name
Install	<p>Information about whether the installed license key is enabled:</p> <ul style="list-style-type: none"> ▪ Enabled: Installed and the software can be used. ▪ Disabled: Installed but the software cannot be used.
Key Type	<p>Installed license key type:</p> <ul style="list-style-type: none"> ▪ Permanent ▪ Temporary ▪ Emergency ▪ Term ▪ Not Installed: No license key is installed.
Permitted Volumes(TB)	<p>Permitted volume capacity for this software (in TB). (The used volume capacity is not output.)</p> <p>If no upper limit value is set for the capacity, "Unlimited" is output.</p> <p>This item is blank in either of the following cases:</p> <ul style="list-style-type: none"> ▪ A new license key whose "Key Type" is Temporary or Emergency has been installed. ▪ No license key has been installed.
Expiration Date	<p>Expiration date of the software</p> <p>The format is <i>mm/dd/yyyy</i> (month/day/year).</p> <p>This item is blank in either of the following cases:</p> <ul style="list-style-type: none"> ▪ The effective term of the license key is unlimited. ▪ No license key has been installed.

Item	Content
Status	License key status of the software: <ul style="list-style-type: none"> ▪ Installed ▪ Not Enough License ▪ Grace Period ▪ Expired ▪ Not Installed ▪ Installed (Disabled)

SMfundat.csv

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

Item	Content
SM Install function	The following classifications are output: <ul style="list-style-type: none"> ▪ Base ▪ Extension1 ▪ Extension2 ▪ Extension3
Availability	Information about whether the function of "SM Install function" is enabled <ul style="list-style-type: none"> ▪ Enabled ▪ Disabled

SsdDriveInfo.csv

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

Item	Content
ECC Group	Number of the parity group to which this SSD belongs
CR#	C# and R# (2-digit hexadecimal numbers that identify the PDEV) Output in the format XX/YY, where: <ul style="list-style-type: none"> ▪ XX: C# ▪ YY: R#

Item	Content
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 (for example, SSD, SSD(RI), FMD, SCM)
Used Endurance Indicator (%)	Used endurance of SSD life (0 to 100)
Used Endurance Indicator Threshold (%)	Drive life threshold (0 to 100)
Used Endurance Indicator Warning SIM (%)	Warning SIM threshold (0 to 100)
FMD Battery Life Indicator Warning SIM (%)	Threshold of battery life warning SIM (0 to 100) This item is blank if the SSD is other than FMD.
FMD Battery Life Indicator (%)	Used battery life (0 to 100) This item is blank if the SSD is other than FMD.

SsidInfo.csv

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

Item	Content
DEV# Start	First LDEV number for the SSID
DEV# End	Last LDEV number for the SSID
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"> ▪ Interleave mode ▪ Full Speed mode
Dynamic Sparing	Information about whether to perform automatic copy to a spare drive if the occurrences of drive failures exceed the threshold. <ul style="list-style-type: none"> ▪ On ▪ Off
Correction Copy	Information about whether to perform correction copy to a spare drive if a drive is blocked. <ul style="list-style-type: none"> ▪ On ▪ Off
Disk Copy pace	Speed of copying the spare drive in the Interleave mode. <ul style="list-style-type: none"> ▪ Faster ▪ Medium ▪ Slower
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"> ▪ On ▪ Off
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"> ▪ On ▪ Off

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`.

Item	Content
Port	Port name
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 (hexadecimal number) Multiple options are separated by semicolons (;). This item is blank when no host mode option is specified.
WWN	World Wide Name of the host bus adapter registered to the host group (hexadecimal number) This item is blank when no valid WWN is specified or when Package Type is iSCSI.
Nickname	Nickname of the host This item is blank when no nickname is specified or when Package Type is iSCSI.
Host Group#	Host group number (hexadecimal) If "Package Type" is iSCSI, the iSCSI target alias is output.
CHB Location	CHB on which the port is installed
Package Type	CHB type for CHB Location Output example for Fibre: 4HF32R (Fibre) Output example for iSCSI: 2HS10S (iSCSI) Output example for FICON®: 4Mx16 (Mfibre)
T10 PI Mode	Indicates whether the T10 PI mode can be applied to the port: <ul style="list-style-type: none"> ▪ Enabled ▪ Disabled

Chapter 8: Troubleshooting

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

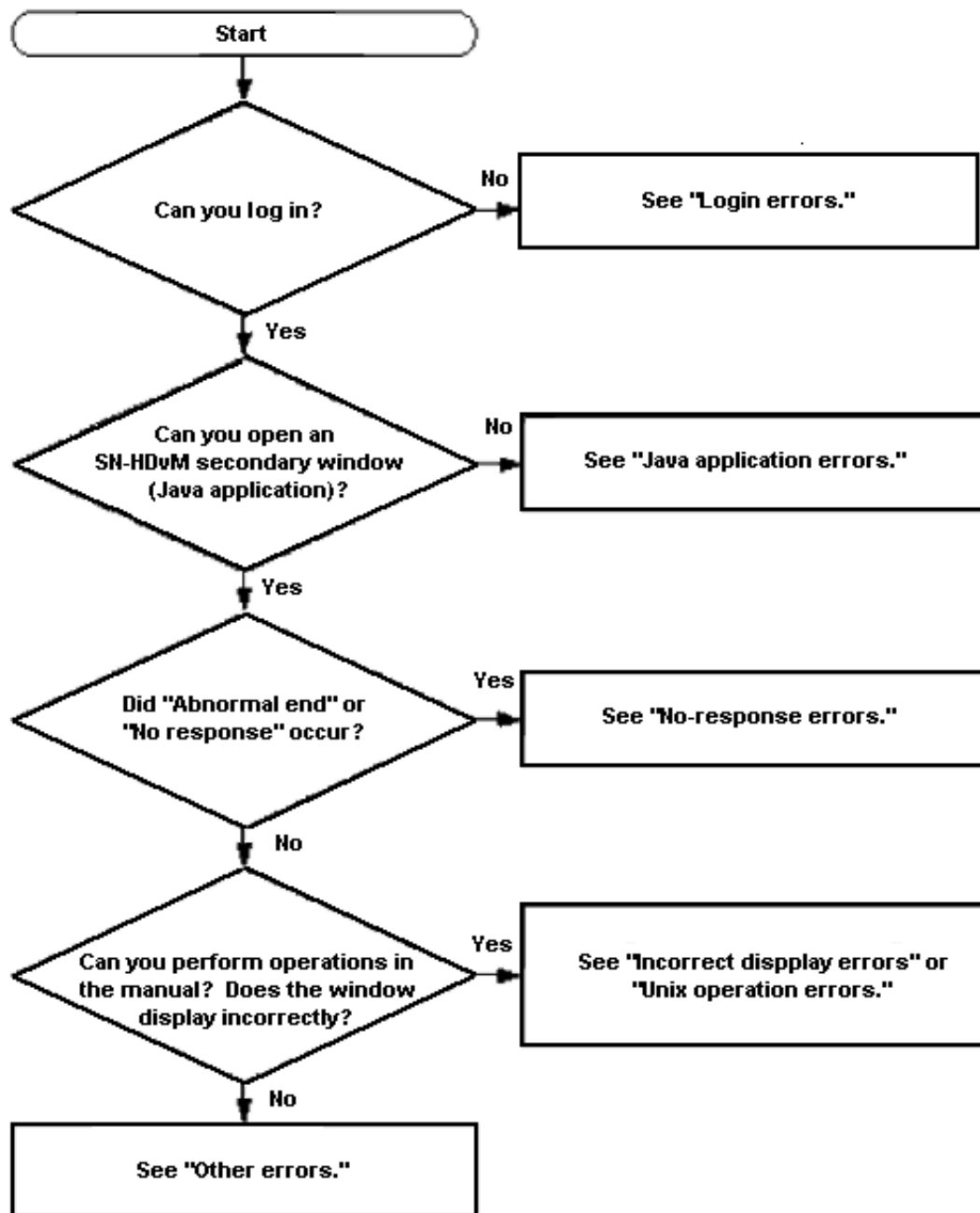
This section provides information for identifying and correcting problems with Device Manager - Storage Navigator for your storage system.

General troubleshooting

If you have a problem with Device Manager - Storage Navigator, check the following items. If you cannot resolve an error condition, contact customer support.

- Check the cabling and the LAN. Verify that both the management client and LAN cabling are firmly attached, and that the LAN is operating properly.
- Close any programs on the management client that are not responding. If necessary, reboot the management client and restart a Device Manager - Storage Navigator web client session.
- Clear the Java and web browser caches to solve the problem. To clear the Java cache, click Delete the temporary files in the **General** dialog box of the Java Control Panel.
- Check for other general error conditions. For a complete list of Device Manager - Storage Navigator error codes, see the *Hitachi Device Manager - Storage Navigator Messages*.
- Check the alert icon. Confirm the severity level of the storage system alert by clicking Alert in the Device Manager - Storage Navigator main window.

Troubleshooting workflow



Service information messages

The storage systems generate service information messages (SIM) to identify normal operations. For example, TrueCopy pair status change, as well as service requirements and errors or failures. For assistance with SIMs, contact customer support.

SIMs can be generated by the front-end directors, back-end directors, and the SVP. All SIMs generated by the storage system are stored on the SVP for use by Hitachi Vantara personnel, displayed by the Device Manager - Storage Navigator software, and reported over SNMP to the open-systems host. The SIM display on Device Manager - Storage Navigator enables users to remotely view the SIMs reported by the attached storage systems. Each time a SIM is generated, the amber Message LED on the control panel turns on. The Hitachi Remote Ops also reports all SIMs to the support center.

SIMs are classified in four severity levels: service, moderate, serious, and acute. The service and moderate SIMs (lowest severity) do not require immediate attention and are addressed during routine maintenance. The serious and acute SIMs (highest severity) are reported to the host system once every eight hours.



Note: If a serious-level or high-level SIM is reported, contact the support center immediately to ensure the problem is being addressed.

The following figure illustrates a typical 32-byte SIM from the storage system. The SIMs are displayed by reference code (RC) and severity. The six-digit RC comprises bytes 22, 23, and 13, identifies the possible error and determines the severity. The SIM type, located in byte 28, indicates which component experienced the error.

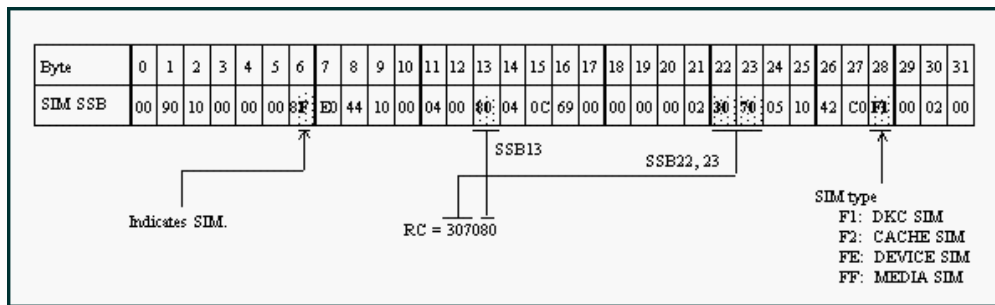


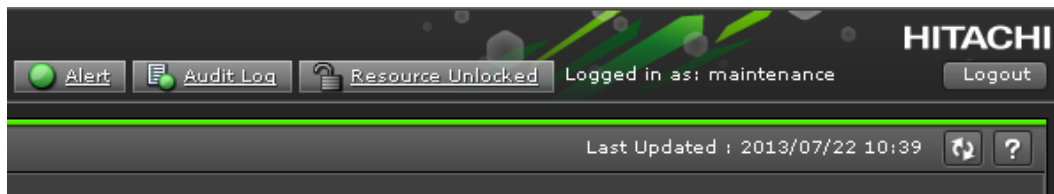
Figure 3 Service information message

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 Alert Properties 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 and provides recommended actions for each error condition.

Error condition	Probable cause / Recommended action
Failed to login is displayed.	Check that the user name and password are correct. If you forget your password, log in with the Security Administrator (View & Modify) and set a new password.

Error condition	Probable cause / Recommended action
	<p>When you are using an external authentication server such as LDAP, check the following:</p> <ul style="list-style-type: none"> ▪ The authentication server has been started. ▪ The authentication server can be accessed from the SVP via the network ▪ The user account has been established on the authentication server ▪ The connection information for the authentication server that has set on the SVP is correct. ▪ The certificate used for the communication with the external authentication server satisfies the requirements. <p>If the symptom recurs even after you correct the above settings, use the dump tool to collect HDvM - SN normal dump files to some recording media and then contact customer support.</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 Internet Options dialog box.
The HDvM - SN window is not displayed.	Make sure that the TLS setting of SVP and that of the browser are correct.
HDvM - SN 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 HDvM - SN.	Close all dialog boxes and log in to the HDvM - SN again. If the same error occurs, check the network environment.
The login to a storage system from the Hitachi Command Suite server fails.	<p>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.</p> <p>Check the number of tiers of the certificate chain to be used in Hitachi Command Suite. The maximum number supported is 20 tiers. Make sure to use a certificate in a certificate chain with no more than 20 tiers.</p>


Error condition	Probable cause / Recommended action
The login dialog box for HDvM - SN running in a web browser is not displayed.	You might be using Internet Explorer 11 with Adobe Flash Player version 10 or earlier. Update Adobe Flash Player if needed.
An error (20121-107097) occurs and the HDvM - SN login fails.	<p>You might not have selected the cipher suites corresponding to the key type of the certificate on the TLS Security Settings dialog box.</p> <ol style="list-style-type: none"> 1. Connect to the Tool Panel dialog box via an HTTP connection, and enable all cipher suites. 2. Make sure you can log in to Device Manager - Storage Navigator. 3. Verify the settings of the cipher suites. 4. The maximum number of tiers of the certificate chain is 20 tiers. Make sure to use a certificate in a certificate chain with no more than 20 tiers.


No-response errors



The following table lists no-response errors and provides the probable cause and recommended actions for each error.

Error condition	Probable cause / Recommended action
<p>The following error occurs when using Device Manager - Storage Navigator:</p> <ul style="list-style-type: none"> ▪ 20121-107024 	The SVP web server might have been restarted. Close HDvM - SN, wait 10 minutes, and then restart HDvM - SN.
<p>The following error occurs when using Device Manager - Storage Navigator:</p> <ul style="list-style-type: none"> ▪ 20121-107022 ▪ 20121-107025 	The session information might not be stored correctly. Set to enable cookies for your web browser. For more information, see Configuring the web browser on the management client (on page 29)
Error (20121-107096) occurs repeatedly while you are using Device Manager - Storage Navigator.	<p>A timeout error may have occurred in Adobe Flash Player or Adobe AIR.</p> <p>Close the HDvM - SN window. Click X in the corner of the browser window or click the window and press Alt+F4.</p>

Error condition	Probable cause / Recommended action
<p>The following errors occur when using Device Manager - Storage Navigator:</p> <ul style="list-style-type: none"> ▪ 20121-107024 ▪ 20121-107025 ▪ 20121-107096 ▪ 20121-107097 	<p>This error may occur if the load to the management client is high, or if you start multiple instances of HDvM - SN by using multiple tabs in a tab browser or multiple browsers.</p> <p>Close the other applications which cause the high load, or make sure to start only one HDvM - SN</p>
<p>The following application error occurs when using Device Manager - Storage Navigator:</p> <ul style="list-style-type: none"> ▪ 20020-108000 	<p>Retry the operations on HDvM - SN. If the problem occurs again, take the following actions:</p> <ul style="list-style-type: none"> ▪ The version of HDvM - SN installed on the management client might not match the SVP version. Close all the browser windows and then clear the browser cache. ▪ The management client might have entered standby or hibernate mode. Restart HDvM - SN. ▪ If a proxy server is used for network connections, the proxy server cache may be storing the older version of the program. If the problem continues after you clear the browser cache, contact your network administrator. ▪ 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"> 1. From Windows, open the Java Control Panel. 2. In the Java Control Panel, click the Security tab. 3. If Enable Java content in the browser is checked, uncheck it and click Apply. 4. The User Account Control dialog box opens. Click Yes. The confirmation window opens. Click OK. 5. Restart the browser. ▪ The JRE used by the secondary window might not support the protocols or cipher suites used in TLS communications. Check whether your JRE supports the protocols and cipher suites used in TLS communications. If not, install a new JRE that supports these protocols and cipher suites.

Error condition	Probable cause / Recommended action
	If none of the above actions solves the problem, save the HDvM - SN dump file and send it to customer support. Then restart the web browser.
<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"> ▪ The HDvM - SN main window is grayed out and does not display the percentage of progress, and you cannot perform any operation for a long period of time. ▪ You cannot perform any operation for a long period of time and the dialog box that says Loading... is not displayed. ▪ The dialog box that says Loading... opens when the window switches. However, you cannot move the dialog box or perform any operation for a long period of time. ▪ The login window does not appear and the white screen continues. ▪ You clicked the cross mark  or Close, however the window cannot be closed. 	<p>Close the web browser and reopen it. When using the HDvM - SN secondary window, exit HDvM - SN by pressing Ctrl+Alt+Shift+D all at once.</p> <p>If you close the web browser but you cannot exit HDvM - SN, reboot the management client or restart HDvM - SN after forcibly closing HDvM - SN as follows:</p> <ul style="list-style-type: none"> ▪ In Windows: <ul style="list-style-type: none"> 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). ▪ In UNIX: <ul style="list-style-type: none"> Exit the web browser, and then terminate firefox-bin with the kill command. ▪ If the problem continues, ask your maintenance personnel to restart the SVP.
A network error occurred. There is no response to any operation even after 30 minutes.	Restart the management client. An operation can take over 30 minutes depending on the use condition. For example, when several HDvM - SN web clients are running, an operation might take a long time.
An internal error occurs, or a web browser ended abnormally.	Close all dialog boxes, and then log in to HDvM - SN again. If the same error occurs, restart the management client.
During a Device Manager - Storage Navigator operation, the web browser suddenly disappears.	Restart the management client.
An error (1-4011) occurs while you are using Device Manager - Storage Navigator.	The clock time of the management client may have been changed. Log in to HDvM - SN again.
The management client reboots on its own.	Restart the management client.
A Device Manager - Storage Navigator window is forcibly closed during a time-consuming process, such as LDEV formatting.	Close all windows, wait until processing finishes, and then restart HDvM - SN.

Error condition	Probable cause / Recommended action
<p>A Device Manager - Storage Navigator window is incorrectly closed when you do one of the following:</p> <ul style="list-style-type: none"> ▪ Click  ▪ Use commands such as File > Close on the web browser ▪ Press the Alt and F4 keys 	<p>Restart HDvM - SN. If you cannot log in, wait for one minute and try again.</p>
<p>During a Device Manager - Storage Navigator operation, an add-on (Flash10e.ocx) error occurs.</p>	<p>Restart the management client. If this error occurs repeatedly, reinstall Adobe Flash Player on the management client.</p>
<p>When you log out of Device Manager - Storage Navigator, an Internet Explorer error occurs.</p>	<p>The probable causes are as follows:</p> <ul style="list-style-type: none"> ▪ Internet Explorer has not been updated. Action: Install the latest updates. ▪ Internet Explorer may be configured incorrectly. Action: Re-install Internet Explorer.
<p>When you click File > 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"> ▪ Another application such as Command Control Interface may be changing configuration. The window will be updated shortly after the configuration change ends. ▪ Volume Migration operations, Quick Restore operations or Thin Image operations may be in progress. The window will be updated shortly after the operations end.
<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"> ▪ 20123-107027 ▪ 20123-108004 ▪ 00002-058578 ▪ 00003-002003 ▪ xxxx-065740 ▪ xxxx-068800 <p>where xxxx indicates any code.</p>	<ul style="list-style-type: none"> ▪ Another application such as Command Control Interface may be changing configuration. ▪ Volume Migration operations, Quick Restore operations, or Thin Image operations may be in progress. ▪ The configuration data may not be matched if a communication error occurs between the storage system and SVP.


Error condition	Probable cause / Recommended action
	<p>Wait a few minutes and then click File > Refresh All to reload the configuration information. Then run HDvM - SN again. If a configuration change operation was performed, check that all the configuration changes that caused the error were applied, and then set the settings that were not applied again.</p> <p>When using Encryption License Key, do the following:</p> <ul style="list-style-type: none"> ▪ If a failure (00002-058578) occurs when you set the Encryption Environment for the first time from the Edit Encryption Environmental Settings window, do the following: <ol style="list-style-type: none"> 1. Wait a few minutes and then click File > Refresh All to reload the configuration information. 2. Initialize the Encryption Environment Settings. 3. Set the Encryption Environment again. ▪ If a failure (00002-058578) occurs when you set the Encryption Environment again from the Edit Encryption Environmental Settings window, do the following: <ol style="list-style-type: none"> 1. Wait a few minutes and then click File > Refresh All to reload the configuration information. 2. Set the Encryption Environment again.
<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>Icon in Internet Explorer: </p> <p>Icon in Google Chrome: </p>	<p>Restart the management client.</p>

Error condition	Probable cause / Recommended action
Operations cannot be performed due to a problem with the Device Manager - Storage Navigator main window. For example, tables are not displayed correctly or some buttons are not displayed. Logging out and back in does not solve the problem.	The HDvM - SN window setting information may have been saved with an incorrect value. Click Settings > Environmental Settings > Reset View to Settings in the HDvM - SN main window to clear the window setting information. Then click any button in the HDvM - SN window and check that it operates correctly. You do not need to log out and back in.
Device Manager - Storage Navigator closes automatically when operating the IPv6 address setting from Device Manager - Storage Navigator.	<p>When the symptom occurs, the resource group status remains locked.</p> <p>Open the Operation Lock Properties window and release the locked resource group caused by the symptom. Suspend other operations when releasing the resource group, as other resource groups are also released the lock. See Operation Lock Properties window (on page 519).</p> <p>If you use HDvM - SN in a web browser, update Adobe Flash Player to version 13 or later.</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"> ▪ When the question mark appears in the View Tier Properties window, see the topic describing this window in the <i>Provisioning Guide for Open Systems</i>. If the problem still persists, contact customer support. ▪ When the question mark appears in the Add External Volumes 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. ▪ 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.
The product name, vendor name, and function name displayed in HDvM - SN are incorrect.	Contact customer support.

Error condition	Probable cause / Recommended action
A part of the HDvM - SN window is not displayed.	You 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 HDvM - SN.
The display on HDvM - SN's main window is not updated to the latest information. "Last Updated" on HDvM - SN's main window is not updated.	Volume Migration operations, Quick Restore operations, or Thin Image operations may be in progress. The window will be updated shortly after the operations end.
<p>The following message is displayed when connected to HDvM - SN on Internet Explorer or Google Chrome.</p> <p>This content requires Adobe Flash Player.</p> <ul style="list-style-type: none"> ▪ Get and install Adobe Flash Player from the Adobe web site. ▪ Enable Adobe Flash Player. ▪ Adjust the browser security settings. 	<p>This message displays when Adobe Flash Player is not installed. Do the following:</p> <ul style="list-style-type: none"> ▪ Install Adobe Flash Player ▪ Disable ActiveX Filtering <p>If you are using Internet Explorer 9 or later, click  Tools > Safety and uncheck ActiveX Filtering.</p> <ul style="list-style-type: none"> ▪ When a message appears indicating that the specific site was blocked, perform the procedure described in Adding your SVP to the trusted sites zone for Windows Server computers (on page 28). ▪ When using HDvM - SN with Flash Player, do not change the local storage area value in Adobe Flash Player. ▪ When using HDvM - SN with Flash Player, do not disable Adobe Flash Player. ▪ If you use Internet Explorer, do not change the settings in Tools > Manage add-ons.
When many items are set, some items might not be displayed even if you scroll through the table.	<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"> ▪ Increase the resolution so that more areas of the table can be shown. ▪ Use the zoom in or zoom out function of your browser to adjust the viewing area. <p>Note: Text might become too small.</p> <p>If you still cannot solve the problem, contact customer support.</p>
The Tools panel of Google Chrome is not displayed correctly in Japanese.	<p>Click the Chrome menu > Settings > Show advanced settings > Languages > Language and input settings.</p> <ol style="list-style-type: none"> 1. If you do not have Japanese in the list, click Add to add Japanese.

Error condition	Probable cause / Recommended action
	<ol style="list-style-type: none"> 2. From the list, select Japanese, and then click Display Google Chrome in this language > Done. 3. To apply the changes, close all Google Chrome windows. 4. Click the Chrome menu > Settings > Show advanced settings > Languages > Language and input setting. 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. 6. Click Done to close the window.
<p>The message "Unable to launch the application" appears on the secondary window, then operation ends abnormally.</p>	<p>Perform the following:</p> <p>If you use JRE 8, Solaris is not supported.</p> <p>Confirm Use TLS 1.2 for Java is enabled.</p> <p>If this problem still persists after performing the above actions, click Detail in the window to collect information displayed in the window by copying and pasting it or by capturing the screen shot, and then contact customer support.</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"> ▪ B Shell: <pre>LANG=C</pre>

Error condition	Probable cause / Recommended action
	<pre>export LANG</pre> <ul style="list-style-type: none"> ▪ C Shell: <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.
<p>The following error occurs when using Device Manager - Storage Navigator with Firefox:</p> <ul style="list-style-type: none"> ▪ 20020-107094 	<p>The server certificate might not be appropriate. Obtain either of the following certificates to perform the operations:</p> <ul style="list-style-type: none"> ▪ Certificate issued by the certificate authority that is used by your company. ▪ Official certificate issued by an SSL certificate authority such as VeriSign to which you need to send a certificate signing request.

HDvM - SN secondary window blocked

If Java 7 Update 55 or later or Java 8 Update 5 or later is installed on the management client, execution of the Device Manager - Storage Navigator secondary window application might be blocked. In this case, use the following procedure to change the Java security settings.

Procedure

1. Check the version and update information of Java installed in your management client. Click **Start > Control Panel > Java**.
2. On the **General** tab, click **About**.
3. Check the version and update information of Java, and then close the **About Java** dialog box. If your PC uses either Java 7 update 55 or later, or Java 8 Update 5 or later, you need to change Java security settings referring to Step 4 and after.
4. Select the **Security** tab.
5. Click **Edit Site List**.
6. In **Exception Site List**, specify the URL of the SVP as follows, and then click **Add**.

```
http://IP-address-of-SVP or https://IP-address-of-SVP
```
7. Click **OK**.
8. Select the **Advanced** tab.
9. For **Perform signed code certificate revocation checks on**, select **Do not check (not recommended)**, and then click **OK**.
10. Close the **Control Panel**.

Storage Device Launcher errors

Error condition	Probable cause / Recommended action
<ul style="list-style-type: none"> ▪ Storage Device Launcher cannot start. Or a message appears asking if you have entered the name correctly because <code>..\..\bundle\jre_win\bin\javaw</code> cannot be found. ▪ HDvM - SN that can run in the Adobe AIR environment cannot start from a web browser. 	<p>After installing Storage Device Launcher, the <code>WCLauncher_win</code> folder used for the installation might have been deleted or moved. If the <code>WCLauncher_win</code> folder remains, restore it to the location where it was installed. Or, reinstall Storage Device Launcher in the new location to which it has been moved.</p> <p>If you cannot find the <code>WCLauncher_win</code> folder, download the setup file and reinstall Storage Device Launcher. For details, see Installing Storage Device Launcher on the management client (on page 31).</p> <p>The maximum number of tiers of the certificate chain is 20 tiers. Make sure to use a certificate in a certificate chain with no more than 20 tiers.</p>

Other errors

The following table lists other errors that occur in Device Manager - Storage Navigator (HDvM - SN) and the Tool Panel utilities and provides recommended actions for resolving the errors.

Error condition	Probable cause / Recommended action
<ul style="list-style-type: none"> ▪ Error about insufficient capacity when creating an LDEV with sufficient capacity. ▪ Operation error about an LDEV that does not exist when creating a pair for an LDEV that does exist. 	<p>Configuration information displayed in HDvM - SN and controller configuration information might not match.</p> <p>Click File > 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 HDvM - SN 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.

Error condition	Probable cause / Recommended action
HDvM - SN processing is temporarily delayed.	Internal processing (for example, configuration change, P.P. check, operational information acquisition) might be running on the SVP.
HDvM - SN processing is delayed.	<p>If you use HDvM - SN in a browser, the local storage value for Adobe Flash Player might have decreased. Follow these steps:</p> <ol style="list-style-type: none"> 1. Right-click on the HDvM - SN main window and click Settings to open the Adobe Flash Player Settings window. 2. In the local storage settings, move the slider until Unlimited appears and then click Close. 3. Close HDvM - SN. 4. Restart HDvM - SN. 5. If the local storage confirmation dialog box appears, click Allow. 6. If this problem persists, there might be a problem with the SVP performances. Contact customer support.
Installing of signed SSL certificate fails.	The passphrase for the SSL certificate might be set. Release the passphrase. If needed, see Releasing an SSL certificate passphrase (on page 100) .
<i>Failed in the certification of the user.</i> appears when you create a configuration report of a storage system and try to view it in a browser.	<p>Close the tab of the configuration report or the window, and then open it again.</p> <p>If the problem cannot be solved, address mismatch of SSL certificates between the SVP and the management client might have occurred. To reconfigure SSL communication, see Setting up SSL communications (on page 93).</p> <p>Otherwise, you can display the configuration report by logging in to HDvM - SN using HTTP.</p> <p>Note: You cannot connect HDvM - SN that operates on Adobe AIR by using HTTP (only HTTPS connection is available).</p>

Error condition	Probable cause / Recommended action
<p>A message is displayed indicating that the exclusive setting cannot be released, a different user is using the resource, or a different user is locking the resource.</p>	<p>Take the following actions:</p> <ul style="list-style-type: none"> ▪ This operation cannot be performed while a different user is changing the configurations. Wait for a while, and then retry the operation. ▪ This operation might not be performed while a task is running. Wait for a while, and then retry the operation. If a task is waiting to run, suspend the task so that the waiting task does not run. <p>In other cases, ask the storage administrator to perform Force Release System Lock. After the system lock is forcibly released, retry the operation.</p> <p>If this problem persists, ask maintenance personnel to restart the SVP.</p>
<p>When the Operation Lock Properties window is displayed, the status of System Lock is displayed as <i>Locked</i>, and the status of Resource group is displayed as <i>Unlocked</i>.</p>	<p>Ask maintenance personnel to restart the SVP, and then retry the operation in HDvM - SN.</p>
<p>HDvM - SN operation is slow, although the hardware requirements for the SVP are satisfied.</p>	<p>Verify that no anti-virus software runs on the SVP.</p>
<p>You cannot resolve an error condition.</p>	<ol style="list-style-type: none"> 1. Copy the HDvM - SN detailed dump files onto recording media using the Dump tool. 2. Obtain the Java log and trace files. 3. Contact customer support.
<p>HDvM - SN cannot be displayed after setting SSL communication using HDvM - SN.</p>	<p>Your browser might not allow the protocol selected in the TLS Security Settings dialog box. Take the following measures:</p> <ul style="list-style-type: none"> ▪ Check whether your browser supports the protocol selected in the TLS Security Settings dialog box. If your browser does not support the protocol, change the browser that supports the protocol, and then change the TLS security settings. ▪ Access the Tool Panel dialog box by using HTTP connection, and then change the TLS settings that satisfies the requirements or prerequisites again.

Error condition	Probable cause / Recommended action
HDvM - SN cannot be displayed after setting a certificate.	The configured certificate might not be consistent with the cipher suite selected in the TLS Security Settings. Connect to the Tool Panel dialog box via an HTTP connection, and then change the cipher suite in the TLS Security Settings that satisfies the requirements or prerequisites.
After the certificate for Syslog, key management server, or external authentication server is set, you cannot communicate with each server.	<p>The possible causes are as follows:</p> <ul style="list-style-type: none"> ▪ The set certificate might not satisfy the requirements or prerequisites for the certificate. If the requirements or prerequisites are not satisfied, set a certificate that satisfies the requirements or prerequisites again. ▪ The set certificate might not consistent with the cipher suites that were selected in the TLS Security Settings dialog box. Select cipher suites that are consistent with the certificate, or set a certificate that suits the cipher suites again. ▪ Check the number of tiers of the certificate chain to be used. The maximum number supported is 20 tiers. Make sure to use a certificate in a certificate chain with no more than 20 tiers.
No audit log for WindowsServerUpdateServices has been output for more than two weeks even though Security Updates were approved	<ul style="list-style-type: none"> ▪ Verify that the server URL in the WSUS Settings dialog box is correct. ▪ Verify the operation status on the WSUS server. <p>If this problem persists, ask a Support Personnel to perform the following operations:</p> <ol style="list-style-type: none"> 1. Collect the dump file with dump type: WSUS information dump from Autodump on the SVP. 2. Restart the SVP.
An audit log for WindowsServerUpdateServices is output, while a log indicating the successful installation of Security Updates has not been output.	<p>Verify the settings of the WSUS server. If this problem persists after at least 27 hours, ask a Support Personnel to perform the following operations:</p> <ol style="list-style-type: none"> 1. Collect the dump file with dump type: WSUS information dump from Autodump on the SVP. 2. Restart the SVP. <p>If restarting the SVP does not solve the problem after at least 27 hours, contact customer support.</p>

Forcibly fail over the SVP

When you are requested by the support personnel to manually change the SVP to the standby SVP, change the SVP by using the following procedure.

Perform this task only when requested by the support personnel.

Before you begin

- The standby SVP is installed on the storage system.
- Check the IP addresses or the host names of both the master SVP and the standby SVP in advance.
- You must have the Storage Administrator (Initial Configuration) role to perform this task.

Procedure

1. Verify that you can use the standby SVP. On the Device Manager - Storage Navigator computer, open a web browser and enter the following URL to open the **Tool Panel** dialog box for the standby SVP.

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

- When the **Tool Panel** dialog box is displayed, you can change the SVP. Proceed to step 2.
 - When the **Tool Panel** dialog box is not displayed, the message "This page cannot be displayed." or "dns_server_failure" appears and you cannot change the SVP. Close the web browser, and then contact customer support.
2. Close the web browser
 3. Verify that you can connect to the master SVP. On the Device Manager - Storage Navigator computer, open a web browser and enter the following URL to open the **Tool Panel** dialog box for the master SVP.

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

- When the **Tool Panel** dialog box is displayed, proceed to step 4.
 - When the **Tool Panel** dialog box is not displayed, proceed to step 10.
4. In the **Tool Panel** dialog box, click **Forcibly disable SVP**. The login dialog box for **Forcibly disable SVP** opens.
 5. In the login dialog box for **Forcibly disable SVP**, enter the administrator user ID in the User ID field and the password in the Password field, and then click **Login**. The **Forcibly disable SVP** dialog box opens.
 6. Click **OK**. A confirmation dialog box opens.
 7. Click **OK**. The **Forcibly disable SVP** dialog box opens again.

8. Click **OK**. The operation to forcibly disable the SVP starts. Wait up to five minutes to complete the processing of forcibly disable the SVP. After the forcibly disable the SVP operation is complete, the **Forcibly disable SVP** dialog box does not appear again.
9. Reload the web browser and check that the **Tool Panel** dialog box does not appear. If the **Tool Panel** dialog box cannot be displayed, the message “This page cannot be displayed” or “dns_server_failure” appears.
10. Close the web browser.
11. On the Device Manager - Storage Navigator computer, open a web browser and enter the following URL to open the **Tool Panel** dialog box for the standby SVP.

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

12. In the **Tool Panel** dialog box for the standby SVP, click **Forcibly Fail Over SVP**. The login dialog box for **Forcibly Fail Over SVP** opens.
13. In the login dialog box for **Forcibly Fail Over SVP**, enter the administrator user ID in the User ID field and the password in the Password field, and then click **Login**. The **Forcibly Fail Over SVP** dialog box opens.
14. Click **OK**. A confirmation dialog box opens.
15. Click **OK**. The **Forcibly Fail Over SVP** dialog box opens again.
16. Click **OK**. The operation to forcibly fail over the SVP starts. Wait up to five minutes for the forcibly fail over the SVP operation to complete processing. The forcibly fail over the SVP operation takes over the IP address or the host name of the master SVP to the standby SVP. After the forcibly fail over the SVP operation is complete, the **Tool Panel** dialog box does not appear again.
17. Reload the web browser and check that the **Tool Panel** dialog box does not appear. If the **Tool Panel** dialog box cannot be displayed, the message “This page cannot be displayed” or “dns_server_failure” appears.
18. Verify that forcibly fail over the SVP operation is completed correctly. On the Device Manager - Storage Navigator computer, open a web browser and enter the following URL to open the **Tool Panel** dialog box for the master SVP.

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

- When the **Tool Panel** dialog box is displayed, the forcibly fail over the SVP operation is complete correctly. Proceed to step 19.
 - When the **Tool Panel** dialog box is not displayed, the forcibly fail over the SVP operation could not be performed. Close the web browser, and then contact customer support.
19. Close the web browser. Wait up to 10 minutes before you can log in.
 20. Verify that you can log in to Device Manager - Storage Navigator. If you cannot log in, contact customer support.

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.

When you use Device Manager - Storage Navigator with Firefox, the files might not be uploaded depending on the type of server certificate. In this case, you must obtain either of the following certificates provided in [Obtaining a signed and trusted certificate \(on page 98\)](#):

- Certificate issued by the certificate authority that is used by your company.
- Official certificate issued by an SSL certificate authority such as VeriSign to which you need to send a certificate signing request.

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 \(on page 126\)](#).

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. Check the number of tiers of the certificate chain to be used. The maximum number supported is 20 tiers. Make sure to use a certificate in a certificate chain with no more than 20 tiers. If this problem occurs again, collect Device Manager - Storage Navigator normal dump file using the dump tool.
No listeners are subscribed to the provider. (00190 77304)	The listeners are not subscribed to the SMI-S provider. Have the listeners subscribe to the provider, and retry.
The artificial indication cannot be sent to some listeners. (00190 77305)	The artificial indication cannot be sent to some listeners. Use the dump tool to collect and save Device Manager - Storage Navigator normal dump files. Then contact 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.

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 to provide to customer support.
- Check the system configuration. Click File > Refresh All to update the configuration information, and then use the Dump tool to download the dump files.

Before you begin

- Verify that all other users (including the SVP user) have stopped using the Dump tool.
- Stop all maintenance operations.
- You must have Support Personnel role to log in.
- You must be an external authentication user whose external user group mapping is disabled.

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.

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

Appendix A: System option modes (SOMs)

System option modes allow the storage system to be configured to specific customer operating requirements.

System option modes

To provide greater flexibility, the storage systems have additional operational parameters called system option modes (SOMs) that allow you to tailor the storage system to your unique operating requirements. The SOMs are set on your storage system by your service representative.

The following table lists and describes the SOMs for DKCMAIN microcode version 90-06-21. Review the SOMs for your storage system, and work with your service representative to ensure that the appropriate SOMs for your operational environment are configured on your storage system.



Note: The SOM information might have changed since this document was published. For the latest SOM information, contact customer support.

Table 29 System option modes for VSP 5000 series

Mode	Category	Description	Default	MCU/RCU
15	Common	This SOM can reduce the host response time to be within about 6 seconds.	ON	-

Mode	Category	Description	Default	MCU/RCU
		<p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is used on a storage system where slow or delayed drive response may affect business operations. 2. When Dynamic Sparing or Auto Correction Mode is used, because host I/Os conflict with copy processing, the I/O watching time is 30 seconds even when this SOM is set to ON. 3. Even though SOM 15 is set to ON, the function does not apply to SATA or NL-SAS drives. 4. When SOM 771 or SOM 797 is set to ON, the setting of SOM 771/797 is prioritized for the read I/O watching time. 5. For additional details about this SOM (interaction with other SOMs, operational details), contact customer support (see SOM015 sheet). 		
20	TrueCopy for Mainframe Universal Replicator for Mainframe	<p>S-VOL read only function (secondary system only).</p> <p>Mode 20 = ON: The S-VOL accepts host read operations while the pair is split.</p> <p>Mode 20 = OFF (default): 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>Mode 22 = ON: If ECCs/LRC PINs (up to 64) have been set on the track of copy source HDD, ECCs/LRC PINs (up to 64) will be created on the track of copy target HDD so that the copy processing will continue. If the number of ECCs/LRC PINs exceeds 64, the corresponding copy processing will be interrupted.</p> <p>Mode 22 = OFF: If ECCs/LRC PINs have been set on the track of copy source HDD, the copy processing will be interrupted. (First recover ECCs/LRC PINs by using the PIN recovery flow, and then perform the correction copy or the drive copy again).</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>Mode 36 = ON: CRIT=Y(ALL) => equivalent to Primary Volume Fence Level = Data.</p> <p>Mode 36 = OFF (default): CRIT=Y(PATHS) => equivalent to Primary Volume Fence Level = Status.</p>	OFF	MCU
64	TrueCopy for Mainframe	<p>Mode 64 = ON:</p> <ul style="list-style-type: none"> ▪ 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. ▪ When receiving the RUN command, the SCP status of the pairs that fulfill the conditions below is released. ▪ 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. <p>Conditions:</p> <ul style="list-style-type: none"> ▪ TCz P-VOL ▪ Mainframe volume ▪ Pair status: Duplex/Pending <p>Mode 64 = OFF (default):</p> <ul style="list-style-type: none"> ▪ 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. ▪ When receiving the RUN command, the SCP status of the pairs that fulfill the conditions below is released. ▪ 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. 	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p>Conditions:</p> <ul style="list-style-type: none"> ▪ TCz P-VOL ▪ Mainframe volume ▪ Pair status: Duplex/Pending ▪ A pair whose RCU# is identical to the RCU for which the Freeze command is specified. <p>Notes:</p> <ol style="list-style-type: none"> 1. General use: SOM 64 = OFF (default). 2. When all the following conditions are met, set SOM 64 to ON: <ul style="list-style-type: none"> ▪ Customer requests to stop the update I/O operation to the RCU of a TCz pair for the whole storage system. ▪ 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. ▪ Only Peer-to-Peer-Remote-Copy operation. (Do not use it in combination with Business Continuity Manager.) 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. 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. 		
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>Mode 80 = ON: Normal Restore / Reverse Copy is performed.</p> <p>Mode 80 = OFF (default): Quick Restore is performed.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied when the specification for Restore of SI is switched between Quick (default) and Normal. 2. The performance of Restore differs depending on the Normal or Quick specification. 		
87	ShadowImage	<p>Determines whether NormalCopy or QuickResync, if not specified, is performed at the execution of pairresync by CCI.</p> <p>Mode 87 = ON: QuickResync is performed.</p> <p>Mode 87 = OFF (default): 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>Mode 114 = ON: Initiator ports automatically change to RCU target ports, and RCU target ports automatically change to Initiator ports.</p> <p>Mode 114 = OFF (default): Automatic port switching during ESTPATH/DELPATH is disabled.</p> <p>Notes:</p> <ol style="list-style-type: none"> 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. 2. Set this SOM to OFF before using TPC-R or CSM (IBM® software for disaster recovery). 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. 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. 	OFF	MCU
122	ShadowImage ShadowImage for Mainframe	For Split or Resync request from the Mainframe host and Device Manager - Storage Navigator.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>Mode 122 = ON: By specifying Split or Resync, Steady/Quick Split or Normal/Quick Resync is respectively executed in accordance with Normal/Quick setting.</p> <p>Mode 122 = OFF (default): By specifying Split or Resync, Steady/Quick Split or Normal/Quick Resync is respectively executed in accordance with Normal/Quick setting.</p> <p>For details about pairsplit/pairresync command behavior, contact customer support (see SOM122 sheet).</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Executing the pairresync command from CCI may be related to the SOM 87 setting. 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. 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. 		
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>Mode 142 = ON (default*): The threshold value of blocking a drive port due to command time-out is changed to the half of the normal threshold.</p> <p>Mode 142 = OFF: The threshold value of blocking a drive port due to command time-out does not change.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM should always be set to ON. This SOM can be set to OFF only when the customer does not allow to set this SOM to ON for a storage system already in production. 2. This SOM is effective for the entire storage system. 	ON	-

Mode	Category	Description	Default	MCU/RCU
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>Mode 190 = ON: 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>Mode 190 = OFF (default): 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
305	Mainframe	<p>This SOM enables the pre-label function (creation of VTOC including VOLSER).</p> <p>Mode 305 = ON: Pre-label function is enabled.</p> <p>Mode 305 = OFF (default): Pre-label function is disabled.</p> <p>Notes:</p> <ol style="list-style-type: none"> 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. 2. Processing time of LDEV format increases by as much as full initialization takes. 3. The following functions and conditions are not supported: <ul style="list-style-type: none"> ▪ Quick format ▪ 3390-A (Dynamic Provisioning attribute) ▪ Volume Shredder 4. Full initialization is required in actual operation. 	OFF	-
308	TrueCopy for Mainframe Universal Replicator for Mainframe	Allows you to specify whether the Remote Copy Path status, SIM218x, is reported to the host or not.	OFF	MCU

Mode	Category	Description	Default	MCU/RCU
		<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>Mode 308 = ON: SIM RC 2180 is reported, which is compatible with older Hitachi specification.</p> <p>Mode 308 = OFF (default): SIM RC 2180 is not reported. Reporting is compatible with IBM - Sense Status report of F5.</p>		
310	Common	<p>Mode 310 = ON: The monitoring timer for MP hang-up is 6 seconds and returning a response to the host within 8 seconds is guaranteed.</p> <p>Mode 310 = OFF (default): The monitoring timer for MP hang-up is 8 seconds.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM applies to a site where strict host response performance is required. 2. If a hardware failure occurs when this SOM is set to ON, the time until MPB blockage is determined is shorter than usual. 	OFF	-
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>Mode 454 = OFF (default): The amount of the entire destage processing is periodically determined by using the highest workload of all CLPRs (*a). (The larger the workload is, the larger the amount of the entire destage processing becomes.)</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>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<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> <p>Mode 454 = ON:</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>Caution: Because the destage processing would not be accelerated even if CLPR has high workload, when the workload in a specific CLPR increases, the risk of host I/O halt would be increased. Therefore, set SOM 454 to ON only when a CLPR has constant high workload and the I/O performance in a CLPR with low workload has higher priority than host I/O halt in the CLPR with high workload.</p> <p>Notes:</p> <ol style="list-style-type: none"> 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. <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"> 2. Because the destage processing will have a lower priority in the overloaded CLPR, the overloaded state of the overloaded CLPR is not removed, and TOV(MIH) might occur. 		

Mode	Category	Description	Default	MCU/RCU
457	Universal Volume Manager	<p>This SOM has two purposes: High-Speed LDEV Format for External Volumes, and Support for Mainframe Control Block Write GUI.</p> <p>Mode 457 = ON:</p> <ol style="list-style-type: none"> High-Speed LDEV Format for External Volumes. 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. Support for Mainframe Control Block Write GUI. Control Block Write of the external LDEVs in mainframe emulation is supported by Device Manager - Storage Navigator (GUI). <p>Mode 457 = OFF (default): High-speed LDEV format for external volumes and support for mainframe control block write GUI are not available.</p> <p>Notes:</p> <ul style="list-style-type: none"> If the LDEV is not written with data "0" before performing the function, the LDEV format might fail. After the format processing, make sure to set SOM 457 to OFF. 	OFF	Both
459	ShadowImage 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>Mode 459 = ON: 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>Mode 459 = OFF (default): 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
467	ShadowImage ShadowImage for Mainframe Compatible FlashCopy® V2 Compatible FlashCopy® SE 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"> ▪ SI ▪ Slz ▪ FCv2, FCSE ▪ UVM ▪ Volume Migration <p>Mode 467 = ON (default): Copy overload prevention. Copy processing stops when the percentage of “dirty” data reaches 60% or higher. When the percentage falls below 60%, copy processing restarts.</p> <p>Mode 467 = OFF: Normal operation. The copy processing slows down if the dirty percentage is 60% or larger, and it stops if the dirty percentage is 75% or larger.</p> <p>Caution: This SOM must always be set to ON when using an external volume as the secondary volume of any of the applicable replication products.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. It takes longer to finish the copy processing because it stops for prioritizing the host I/O performance. 2. This SOM supports background copy only. The processing to copy the pre-update data to the S-VOL, which occurs when overwriting data to uncopied slots of P-VOL in Split processing or reading or writing data to uncopied slots of S-VOL, is not supported. 3. Check the write pending rate of each CLPR per MP unit. Even though there is some free cache capacity in the entire system, if the write pending rate of an MP unit to which pairs* belong exceeds the threshold, the copy operation is stopped. <p>*Applies to pairs of SI, Slz, FCv2, FCSE, and Volume Migration.</p>	ON	-

Mode	Category	Description	Default	MCU/RCU
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>Mode 471 = ON: These SIM-RCs are reported to maintenance personnel.</p> <p>Mode 471 = OFF (default): These SIM-RCs are not reported to maintenance personnel.</p> <p>Note: 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> <p>Mode 474 = ON: For a suspended UR pair, a TC (Sync) pair can be created with the same P-VOL/S-VOL so that UR initial copy time can be reduced by using the dedicated script.</p> <p>Mode 474 = OFF (default): For a suspended UR pair, a TC (Sync) pair cannot be created with the same P-VOL/S-VOL. For this, the dedicated script cannot be used.</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>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p>Notes:</p> <ol style="list-style-type: none"> 1. Set this SOM for both primary and secondary storage systems. 2. When this SOM is set to ON: <ul style="list-style-type: none"> ▪ Execute all pair operations from CCI/BCM. ▪ Use a dedicated script. ▪ Initial copy operation is prioritized over update I/O. Therefore, the processing speed of the update I/O slows down. 3. If this SOM is set to ON, the processing speed of update I/O slows down by about 15 μs per command, version downgrade is disabled, and Take Over is not available. 4. If this SOM is not set to ON for both sides, the behavior is as follows: <ul style="list-style-type: none"> ▪ OFF in primary and secondary storage systems: Normal UR initial copy performance. ▪ ON in the primary storage system/OFF in the secondary storage system: TC Sync pair creation fails. ▪ OFF in the primary storage system/ON in the secondary storage system: The update data is copied to the S-VOL synchronously. 5. While this SOM is set to ON, make sure not to perform microcode downgrade to an unsupported version. 6. While this SOM is set to ON, make sure not to perform the Take Over function. 7. This SOM cannot be applied to a UR pair that is the second mirror in a URxUR multi-target configuration, URxUR cascade configuration, or 3DC multi-target or cascading configuration of three UR sites. If applied, TC pair creation is rejected with SSB=CBED output. 8. Before setting SOM 474 to ON, make sure that SOM 1091 is set to OFF. If SOM 1091 is set to ON, set it to OFF first, and then set SOM 474 to ON. 		
484	TrueCopy for Mainframe	The IBM [®] -compatible PPRC FC path interface was supported with TagmaStore USP 50-06-11. As the	OFF	Both

Mode	Category	Description	Default	MCU/RCU
	ShadowImage for Mainframe	<p>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"> ▪ Mode 484 = ON: The status of path using the Fibre Channel interface is displayed. WWNN is indicated. ▪ Mode 484 = OFF (default): The status of path using an ESCON[®] interface is displayed. WWNN is invalid. <p>Notes:</p> <ol style="list-style-type: none"> 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. 2. When an old model or a TagmaStore USP that does not support this SOM is connected using TCz, set this SOM to OFF. 3. If the display specification is different between MCU and RCU, it may cause malfunction of host. 4. When IBM[®] TPC-R or CSM software for disaster recovery is used, set this SOM to ON. 		
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>Mode 506 = ON:</p> <ul style="list-style-type: none"> ▪ Without update I/O: Delta Resync is enabled. ▪ With update I/O: Delta Resync is enabled. <p>Mode 506 = OFF:</p> <ul style="list-style-type: none"> ▪ Without update I/O: Total data copy of Delta Resync is performed. ▪ With update I/O: Delta Resync is enabled. 	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		Note: Even when SOM 506 is set to ON, the Delta Resync may fail and only the total data copy of the Delta Resync function is allowed if the necessary journal data does not exist on the primary storage system used for the Delta Resync operation.		
531	Common	When PIN data is generated, the SIM currently stored in SVP is reported to the host. Mode 531 = ON: The SIM for PIN data generation is stored in SVP and reported to the host. Mode 531 = OFF (default): The SIM for PIN data generation is stored in SVP only, not reported to the host, the same as the current specification.	OFF	Both
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. Mode 548 = ON: Pair operations of TCz, URz, or Slz via online Command Device are not available. SSB=0x64fb is output. Mode 548 = OFF (default): Pair operations of TCz, URz, or Slz via online Command Device are available. SIM is output. Notes: 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. 2. This SOM is applied to operations from BCM that is operated on MVS.	OFF	Both
556	Open	Prevents an error code from being set in the 8 - 11th bytes in the standard 16-byte sense byte. Mode 556 = ON: An error code is not set in bytes 8 - 11 in the standard 16-byte sense byte. Mode 556 = OFF (default): 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. Mode 561 = ON: Quick Restore for external volumes with different Cache Mode settings is prevented.	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		Mode 561 = OFF (default): Quick Restore for external volumes with different Cache Mode settings is allowed.		
573	TrueCopy for Mainframe ShadowImage for Mainframe	<p>For the CU emulation type 2105/2107, specifying the CASCADE option for the ICKDSF ESTPAIR command is allowed.</p> <p>Mode 573 = ON: The ESTPAIR CASCADE option is allowed.</p> <p>Mode 573 = OFF (default): The ESTPAIR CASCADE option is not allowed. (When specified, the option is rejected.)</p> <p>Notes:</p> <ol style="list-style-type: none"> 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 2. This SOM is applied when building an environment using the Metro Mirror F.O./F.B. function with TPC-R or CSM. 3. The CASCADE option can be specified in the TSO environment also. 4. Although the CASCADE option can be specified for the ESTPAIR command, the PPRC-XD function is not supported. 5. Perform thorough pre-check for any influence on GDPS/PPRC. 6. The SOM must be enabled only when the CASCADE option is specified for the ESTPAIR command for the CU emulation type 2105/2107. 	OFF	Both 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>Mode 589 = ON: For each external volume, progress is updated only when the progress rate is 100%.</p> <p>Mode 589 = OFF (default): Progress is updated when the progress rate exceeds the previous level.</p> <p>Notes:</p>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<ol style="list-style-type: none"> 1. Set this SOM to ON when disconnecting an external volume while the specific host IO operation is online and its performance requirement is severe. 2. Whether the disconnecting status for each external volume is progressed or not cannot be confirmed on Device Manager - Storage Navigator (It indicates “-“until just before the completion and at the last it changes to 100%). 		
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>Mode 598 = ON: SIMs (RC=DCE0 to DEC3) to warn that a JNL is full are reported to SVP and the host.</p> <p>Mode 598 = OFF (default): SIMs (RC=DCE0 to DEC3) to warn that a JNL is full are reported to SVP only.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied if SIMs (RC=DCE0 to DCE3) need to be reported to a Mainframe host. 2. The SIMs are not reported to the Open server. 3. SIMs for JNL full (RC=DCE0 and DCE1) on MCU are reported to the host connected with MCU. 4. SIMs for JNL full (RC=DCE2 and DCE3) on RCU are reported to the host connected with RCU. 	OFF	Both
632	TrueCopy for Mainframe	<p>By setting this mode to ON/OFF when the PPRC ESTPAIR CRIT option is "NO" (fence level = NEVER) and VPD (SOM 36) is ON, Byte1,Bit5 (VPD flag) of PPRC QUERY is changed. PPRC QUERY display is not changed (CRIT (NO)).</p> <p>Mode 632 = ON: Byte1,Bit5 (VPD flag) = ON</p> <p>Mode 632 = OFF (default): Byte1,Bit5 (VPD flag) = OFF</p> <p>The mode is applied if reporting Byte1,Bit5 (VPD flag) = ON when the PPRC ESTPAIR CRIT option is "NO" (Fence level = NEVER) and VPD (SOM36) is ON is required.</p>	OFF	Both
640	TrueCopy for Mainframe	Vary Online can be run from the host for a volume shared by a TCz S-VOL (SwapSuspend or S-VOL	OFF	RCU

Mode	Category	Description	Default	MCU/RCU
	ShadowImage for Mainframe	<p>write access permitted) and an Slz P-VOL. This mode changes the behavior of the Sense SubSystem command from its current behavior to its previous behavior.</p> <p>Mode 640 = ON: . The Slz pair information is returned for the Sense SubSystem command that runs when either a TCz pair is in SSWS status or when write access to the S-VOL is permitted in a configuration where the TCz pair is combined with an Slz pair.</p> <p>Mode 640 = OFF (default): . The Slz pair information is not returned for the Sense SubSystem command that runs when either a TCz pair is in SSWS status or when write access to the S-VOL is permitted in a configuration where the TCz pair is combined with an Slz pair.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. The mode is applied to obtain the Slz pair information by the SenseSubSystem command when a TCz pair is in SSWS status or write access to the S-VOL is permitted in a configuration where the TCz pair is combined with an Slz pair. 2. When SOM 640 is ON, Vary Online cannot be run for a volume shared by a TCz S-VOL and anSlz P-VOL volume. 		
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>Mode 665 = ON (default): The auto dump collection function is disabled.</p> <p>Mode 665 = OFF: The auto dump collection function is enabled.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied when disabling the automatic log dump collection function is required at a failure. 2. This SOM is effective for the entire storage system. 	ON	-

Mode	Category	Description	Default	MCU/RCU
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>Mode 689 = ON: 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>Mode 689 = OFF (default): The initial copy and resync copy operations are not slowed down when the Write Pending rate on RCU exceeds 60% (the same as before).</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM can be set online. 2. The micro-programs on both MCU and RCU must support this SOM. 3. This SOM should be set when requested by the user. 4. Setting this SOM to ON is recommended when GAD is installed, as the performance degradation is more likely to occur due to active-active I/Os. 5. If the write-pending status remains at 60% or higher on the RCU for a long time, it takes extra time for the initial copy and resync copy to be completed due to the slower copy operations. 6. If the write pending rate of CLPR to which the initial copy target S-VOL belongs is not over 60% but that of MP PCB to which the S-VOL belongs is over 60%, the initial copy operation is slowed down. 	OFF	Both
690	Universal Replicator 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"> ▪ When CLPR of JNL-Volume exceeds 60%, Read JNL is prevented. ▪ When CLPR of Data (secondary)-Volume exceeds 60%, JNL Restore is prevented. 	OFF	RCU

Mode	Category	Description	Default	MCU/RCU
		<p>Mode 690 = ON: Read JNL or JNL Restore is prevented when the Write Pending rate on RCU exceeds 60%.</p> <p>Mode 690 = OFF (default): Read JNL or JNL Restore is not prevented when the Write Pending rate on RCU exceeds 60% (the same as before).</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM can be set online. 2. This SOM should be set per customer's requests. 3. If the Write Pending status long keeps 60% or more on RCU, it takes extra time for the initial copy to be completed by making up for the prevented copy operation. 4. If the Write Pending status long keeps 60% or more on RCU, the pair status may become Suspend due to the JNL-Vol being full. 		
701	Universal Volume Manager	<p>Issues the Read command at the logical unit discovery operation using UVM.</p> <p>Mode 701 = ON: The Read command is issued at the logical unit discovery operation.</p> <p>Mode 701 = OFF (default): The Read command is not issued at the logical unit discovery operation.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>Notes:</p> <ol style="list-style-type: none"> 1. When the external storage is TagmaStore USP/NSC and the Open LDEV Guard attribute (VMA) is defined on an external device, set this SOM to ON. 2. When this SOM is set to ON, it takes longer time to complete the LU discovery. The amount of time depends on external storages. 3. With this SOM OFF, if searching for external devices with VMA is set, the VMA information cannot be read. 4. When this SOM is set to ON while the following conditions are met, the external volume is blocked: <ul style="list-style-type: none"> ▪ An external volume to which Nondisruptive migration (NDM) attribute is set exists. ▪ The external volume is reserved by the host 5. As the VMA information is TagmaStore USP/NSC-specific, this SOM does not need to be ON when the external storage is other than TagmaStore USP/NSC. 6. Set this SOM to OFF when an external volume to which nondisruptive migration (NDM) attribute is set exists. 		
704	ShadowImage 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>Mode 704 = ON: Copy processing requested is registered into a newly created queue so that the processing is scheduled with lower priority than host I/O.</p> <p>Mode 704 = OFF (default): 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>Notes:</p> <ol style="list-style-type: none"> 1. Apply this SOM when the load of host I/O to an ECC that uses ShadowImage or Volume Migration is high and the host I/O processing is delayed. 2. If the PDEV is highly loaded, the priority of Read/Write processing made by ShadowImage, Volume Migration, or Resync may become lower. As a consequence the copy speed may be slower. 		
721	Common	<p>When a parity group is uninstalled or installed, the following operation is performed according to the setting of SOM 721.</p> <p>Mode 721 = ON: When a parity group is uninstalled or installed, the LED of the drive for uninstallation is not illuminated, and the instruction message for removing the drive does not appear. Also, the windows other than that of parity group, such as DKA or DKU, are unavailable to select.</p> <p>Mode 721 = OFF (default): When a parity group is uninstalled or installed, the operation is as before: the LED of the drive is illuminated, and the drive must be unmounted and remounted.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. When the RAID level or emulation type is changed for the existing parity group, this SOM should be applied only if the drive mounted position remains the same at the time of the parity group uninstallation or installation. 2. After the operation using this SOM is completed, this SOM must be set back to OFF; otherwise, the LED of the drive to be removed will not be illuminated at subsequent parity group uninstalling operations. 	OFF	-
725	Universal Volume Manager	<p>This SOM determines the action that will be taken when the status of an external volume is Not Ready.</p> <p>Mode 725 = ON: When Not Ready is returned, the external path is blocked and the path status can be automatically recovered (Not Ready blockade). Note that the two behaviors, automatic recovery and block, may be repeated.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>When the status of a device is Not Ready blockade, Device Health Check is executed after 30 seconds.</p> <p>Mode 725 = OFF (default): When Not Ready is returned three times in three minutes, the path is blocked and the path status cannot be automatically recovered (Response error blockade).</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Applying this SOM is prohibited when USP V/VM is used as an external storage system and its external volume is DP-VOL. 2. Applying this SOM is recommended when the above condition (1) is not met and SUN storage is used as an external storage. 3. Applying this SOM is recommended when the above condition (1) is not met and EMC CX series or Fujitsu Fibre CAT CX series is used as an external storage. 4. Applying this SOM is recommended if the above condition (1) is not met and a maintenance operation such as firmware update causing controller reboot is executed on the external storage side while a storage system other than Hitachi product is used as an external storage system. 5. While USP V/VM is used as an external storage system and its volume is DP-VOL, if some Pool-VOLs constituting the DP-VOL are blocked, external path blockade and recovery occurs repeatedly. 6. When a virtual volume mapped by UVM is set to pool-VOL and used as DP-VOL in local storage system, this SOM can be applied without problem. 		
729	Dynamic Provisioning Data Retention Utility	<p>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.</p> <p>Mode 729 = ON: Set the DRU Protect attribute for the target DP-VOL when any write operation is requested to the area where the page allocation is not provided at a time when the DP pool is full. (Not to set in the case of Read request.)</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>Mode 729 = OFF (default): Do not set the DRU Protect attribute for the target DP-VOL when any write operation is requested to the area where the page allocation is not provided at a time when DP pool is full.</p> <p>For details, contact customer support (see SOM729 & 803 sheet).</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied when: <ul style="list-style-type: none"> ▪ The threshold of pool is high (for example, 95%) and the pool may be full. ▪ File system is used. ▪ Data Retention Utility is installed. 2. Since the Protect attribute is set for V-VOL, the Read operation cannot be allowed as well. 3. When Data Retention Utility is not installed, the desired effect is not achieved. 4. Protect attribute can be released from the Data Retention window of Device Manager - Storage Navigator after releasing the full status of the pool by adding a Pool-VOL. 5. VVP can be enabled/disabled for each pool. With SOM 729 disabled, VVP is also disabled by default, but you can enable VVP for each pool as needed. With SOM 729 enabled, VVP is also enabled automatically (by default) when you create a new pool. Caution: A pool is NOT protected by ANY FUNCTION if you deliberately turn VVP for the pool from ON (default) to OFF, even with SOM 729 enabled. 6. When HMO 63 or 73 is set to ON, the setting of the HMO is prioritized over the SOM 729 setting, so that the behavior remains the same as when SOM 729 is OFF even when it is set to ON. 		
734	Dynamic Provisioning Dynamic Provisioning for Mainframe	When exceeding the pool threshold, the SIM is reported as follows:	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>Mode 734 = ON: A SIM is reported at the time when the pool usage rate exceeds the pool threshold (warning, system, or depletion). Once the pool usage rate falls below the pool threshold, and then exceeds again, the SIM is reported again. If the pool usage rate continues to exceed the warning threshold and the depletion threshold, the SIM (SIM-RC625000) is repeatedly reported every eight (8) hours until the pool usage rate falls below the depletion threshold.</p> <p>Mode 734 = OFF (default): A SIM is reported at the time when the pool usage rate exceeds the pool threshold (warning, system, or depletion). Once the pool usage rate falls below the pool threshold, and then exceeds again, the SIM is reported again. The SIM is not reported while the pool usage rate continues to exceed the warning threshold and the depletion threshold.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is turned ON to prevent the write I/O operation from being unavailable due to pool full. 2. If the exceeding pool threshold SIM occurs frequently, other SIMs may not be reported. 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. 4. Turning on SOM 741 can provide the SIM report to both the users and the service personnel. 		
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>Mode 741 = ON: SIM is reported to the service personnel.</p> <p>Mode 741 = OFF (default): SIM is not reported to the service personnel.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is set to ON to have SIM for users reported to the service personnel: <ul style="list-style-type: none"> ▪ For the system where SNMP and E-mail notification are not set. ▪ If Device Manager - Storage Navigator is not periodically activated. 2. When SOM 734 is turned OFF, SIM-RC625000 is not reported; accordingly the SIM is not reported to the service personnel even though this SOM is ON. 		
745	Universal Volume Manager	<p>Enables to change the area where the information is obtained as the Characteristic1 item from SYMMETRIX.</p> <p>Mode 745 = ON:</p> <ul style="list-style-type: none"> ▪ The area where the information is obtained as the Characteristic1 item from SYMMETRIX is changed. ▪ When CheckPaths or Device Health Check (1/ hour) is performed, the information of an already-mapped external volume is updated to the one after change. <p>Mode 745 = OFF (default):</p> <ul style="list-style-type: none"> ▪ The area where the information is obtained as the Characteristic1 item from SYMMETRIX is set to the default. ▪ When CheckPaths or Device Health Check (1/ hour) is performed, the information of an already-mapped external volume is updated to the default. 	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied when the EMC SYMMETRIX is connected using UVM. 2. Enable the setting of EMC SCSI Flag SC3 for the port of the EMC SYMMETRIX storage connected with the storage system and disable the setting of Flag SPC2. If the setting of EMC SCSI Flag SC3 is not enabled or the setting of Flag SPC2 is enabled, the effect of this SOM may not be achieved. 3. If you want to enable this SOM immediately after setting, perform Check Paths on each path one by one for all the external ports connected to the EMC SYMMETRIX storage. But, without doing Check Paths, the display of Characteristic1 can automatically be changed by the Device Health Check to be performed once an hour. If SSB=AD02 occurs and a path is blocked, perform Check Paths on this path again. 4. If the Check Paths is performed while ShadowImage for Mainframe pair and FlashCopy[®] 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[®] Mirror pair are defined in the specified volume, do not perform Check Paths but wait until the display is automatically changed. 		
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>Mode 749 = ON: The HDP Rebalance function and the HDT Tier relocation function are disabled.</p> <p>Mode 749 = OFF (default): The HDP Rebalance function and the HDT Tier relocation function are enabled.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied when no change in performance characteristic is desired. 2. When a pool is newly installed, the load may be concentrated on the installed pool volumes. 3. When 0 data discarding is executed, load may be unbalanced among pool volumes. 4. Pool VOL deletion while this SOM is set to ON fails. To delete pool VOLs, set this SOM to OFF. 		
757	Common	<p>Enables/disables output of in-band audit logs.</p> <p>Mode 757 = ON: In-band audit log is not output.</p> <p>Mode 757 = OFF (default): In-band audit log is output.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Mode 757 applies to the sites where outputting the In-band audit logs is not needed. 2. When this SOM is set to ON: <ul style="list-style-type: none"> ▪ There is no access to SM for the In-band audit logs, which can avoid the corresponding performance degradation. ▪ SM is not used for the In-band audit logs. 3. If outputting the In-band audit log is desired, set this SOM to OFF. 	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>Mode 762 = ON: The data is settled to RCU according to the time stamp specified in the command.</p> <p>Mode 762 = OFF (default): The data is settled to RCU according to the time stamp that RCU has received.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied under the following conditions. <ul style="list-style-type: none"> ▪ Universal Replicator for Mainframe. ▪ EXCTG configuration. 	OFF	Both (On RCU side, consideration in Takeover is required for setting)

Mode	Category	Description	Default	MCU/RCU
		<ul style="list-style-type: none"> ▪ Flush suspension with an EXCTG specified is executed. ▪ BCM is installed on the host where the time stamping function is available. ▪ (In the case of multiple-host configuration, SYSPLEX timer is available on the system) <p>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.</p> <p>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).</p>		
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[®] function of TPC-R or CSM is used. The Basic HyperSwap[®] 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> <p>Mode 769 = ON: The retry operation is disabled when the path creation operation is executed (retry operation is not executed).</p> <p>Mode 769 = OFF (default): The retry operation is enabled when the path creation operation is executed (retry operation is executed).</p>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p>Notes:</p> <ol style="list-style-type: none"> 1. Apply this SOM when the following three conditions are met: <ul style="list-style-type: none"> ▪ SOM 114 is set to OFF (operation of automatically switching the port is disabled). ▪ HMO 49 and HMO 50 are set to OFF (60-07-51-00/00 and later, 70-02-31-00/00 and later). ▪ TPC-R or CSM is used (it is not applied in normal operation). 2. When SOM 769 is set to ON, SOM 114, HMO 49 and HMO 50 must not be set to ON. 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"> ▪ SOM 114 is set to ON. ▪ HMO 49 and HMO 50 are set to ON. 		
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>Mode 776 = ON: 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>Mode 776 = OFF (default): 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>Notes:</p> <ol style="list-style-type: none"> 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. 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. 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. 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. 		
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>Mode 784 = ON: The MIH time of RIO is internally reduced so that, even though a path failure occurs between storage systems in the environment where host MIH time is set to 15 seconds, update I/Os can be processed by using an alternate path promptly, lowering the possibility of host MIH occurrence.</p> <p>Mode 784 = OFF (default): The operation is processed in accordance with the TC, TCz, or GAD specification.</p>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied to the environment where Mainframe host MIH time is set to 15 seconds. 2. This SOM is applied to the environment where OPEN host time-out time is set to 15 seconds or less. 3. This SOM is applied to reduce RI/O MIH time to 5 seconds. 4. This function is available for all the TC, TCz, and GAD pairs on the storage system, unable to specify the pairs that are using this function or not. 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. 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. 7. If a failure occurs on the switched path between storage systems, Mainframe host MIH or Open server time-out may occur. 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. 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. 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 or time-out may 		

Mode	Category	Description	Default	MCU/RCU
		<p>occur due to a path failure between storage systems.</p> <ol style="list-style-type: none"> 11. Operation commands are not available for promptly switching to an alternate path. 12. This SOM works for the pair for which initial pair creation or Resync operation is executed. 13. Micro-program downgrade to an unsupported version cannot be executed unless all the TC, TCz, and GAD pairs are suspended or deleted. 14. For operational specifications in each combination of MCU and RCU of TCz/TC, contact customer support (see SOM784 sheet). 15. For GAD pairs, this SOM is effective if the microcode version supports GAD. 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. 		
787	Compatible FlashCopy® V2	<p>This SOM enables the batch prefetch copy.</p> <p>Mode 787 = ON: The batch prefetch copy is executed for an FCv2 pair and a Preserve Mirror pair</p> <p>Mode 787 = OFF (default): The batch prefetch copy is not executed.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. When this SOM is set to ON, the performance characteristic regarding sequential I/Os to the FCv2 target VOL changes. 2. This SOM is applied only when SOM 577 is set to OFF. 3. This SOM is applied if response performance for a host I/O issued to the FCv2 target VOL is prioritized. 	OFF	-

Mode	Category	Description	Default	MCU/RCU
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>Mode 803 = ON: While a DP pool VOL is blocked, if a read or write I/O is issued to the blocked pool VOL, the DRU attribute is set to Protect.</p> <p>Mode 803 = OFF (default): While a DP pool VOL is blocked, if a read or write I/O is issued to the blocked pool VOL, the DRU attribute is not set to Protect.</p> <p>For more details, contact customer support (see SOM729 & 803 sheet).</p> <p>Notes:</p> <ol style="list-style-type: none"> This SOM is applied when: <ul style="list-style-type: none"> A file system using DP pool VOLs is used. Data Retention Utility is installed. Because the DRU attribute is set to Protect for the V-VOL, a read I/O is also disabled. If Data Retention Utility is not installed, the expected effect cannot be achieved. The Protect attribute of DRU for the DP V-VOL can be released on the Data Retention window of Device Manager - Storage Navigator after recovering the blocked pool VOL. VVP can be enabled/disabled for each pool. With SOM 803 disabled, VVP is also disabled by default, but you can enable VVP for each pool as needed. With SOM 803 enabled, VVP is also enabled automatically (by default) when you create a new pool. Caution: A pool is NOT protected by ANY FUNCTION if you deliberately turn VVP for the pool from ON (default) to OFF, even with SOM 803 enabled. 	OFF	-
855	ShadowImage for Mainframe Volume Migration	By switching this SOM to ON/OFF when ShadowImage is used with SOM 467 set to ON, copy processing is continued or stopped as follows.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>Mode 855 = ON: When the amount of dirty data is within the range from 58% to 63%, the next copy processing is continued after the dirty data created in the previous copy is cleared to prevent the amount of dirty data from increasing (copy after destaging). If the amount of dirty data exceeds 63%, the copy processing is stopped.</p> <p>Mode 855 = OFF (default): 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> <p>Notes:</p> <ol style="list-style-type: none"> This SOM is applied when all the following conditions are met <ul style="list-style-type: none"> ShadowImage is used with SOM 467 set to ON. Write pending rate of an MP unit that has LDEV ownership of the copy target is high Usage rate of a parity group to which the copy target LDEV belongs is low. ShadowImage copy progress is delayed. This SOM is available only when SOM 467 is set to ON. If the workload of the copy target parity group is high, the copy processing may not be improved even if this SOM is set to ON. 		
867	Dynamic Provisioning Dynamic Tiering	<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> <p>Mode 867 = ON (default): LDEV format of the DP-VOL is performed with page reclamation.</p> <p>Mode 867 = OFF:LDEV format of the DP-VOL is performed with 0 data writing.</p>	ON	-

Mode	Category	Description	Default	MCU/RCU
		<p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied from factory shipment. 2. Do not change the setting of this SOM during DP-VOL format. 3. If the setting of this SOM is changed during DP-VOL format, the change is not reflected to the format of the DP-VOL being executed but the format continues in the same method. 		
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>Mode 895 = ON (default): When the FICON[®]/FC link up speed is 8 Gbps/16 Gbps, the link type with transfer speed of 8 Gbps/16 Gbps is reported.</p> <p>Mode 895 = OFF: 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>Notes:</p> <ol style="list-style-type: none"> 1. To apply this SOM, the RMF version of mainframe z/OS[®] to be connected must be 1.12 or higher. 2. If the OS does not use a supported version, the transfer speed cannot be displayed correctly. 3. If all RMF versions of mainframe z/OS connected are 1.12 or higher, set this SOM to ON. 4. If any version of mainframe z/OS connected is lower than 1.12, set this SOM to OFF. 	ON	Both
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>Mode 896 = ON (default): The background format function is enabled.</p> <p>Mode 896 = OFF: The background format function is disabled.</p>	ON	-

Mode	Category	Description	Default	MCU/RCU
		<p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied when you need to disable the background format for a DP/DT/TI pool due to a concern of performance degradation of other functions in an environment where a DP-VOL is used by other functions. 2. When the background format function is enabled, because up to 42 MB/s of ECCG performance is used, local copy performance may degrade by about 10%. Therefore, confirm whether the 10% performance degradation is acceptable or not before enabling the function. 3. When a Dynamic Provisioning VOL on an external storage system, which is used as an external VOL, is used as a pool VOL, if the external pool on the external storage side becomes full due to the background format, the external VOL may be blocked. If the external pool capacity is smaller than the external VOL capacity (Dynamic Provisioning VOL of external storage system), do not enable the background format function. 4. If the background format function is disabled by changing this SOM setting, the format progress is initialized and the entire area becomes unformatted. 		
899	Volume Migration	<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>Mode 899 = ON:</p> <ul style="list-style-type: none"> ▪ SOM 900 is ON: I/O synchronous copy starts without retrying Volume Migration. ▪ SOM 900 is OFF: I/O synchronous copy starts when the threshold of Volume Migration retry is exceeded. (Recommended) <p>Mode 899 = OFF (default):</p> <ul style="list-style-type: none"> ▪ SOM 900 is ON: I/O synchronous copy starts when the number of retries reaches half of the threshold of Volume Migration retry. ▪ SOM 900 is OFF: Volume Migration is retired and I/O synchronous copy is not executed. 	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied when improvement of Volume Migration success rate is desired under the condition that there are many updates to a migration source volume of Volume Migration. 2. During I/O synchronous copy, host I/O performance degrades. 		
900	Volume Migration	<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>Mode 900 = ON:</p> <ul style="list-style-type: none"> ▪ SOM 899 is ON: I/O synchronous copy starts without retrying Volume Migration. ▪ SOM 899 is OFF: I/O synchronous copy starts when the number of retries reaches half of the threshold of Volume Migration retry. <p>Mode 900 = OFF (default):</p> <ul style="list-style-type: none"> ▪ SOM 899 is ON: I/O synchronous copy starts when the threshold of Volume Migration retry is exceeded. (Recommended) ▪ SOM 899 is OFF: Volume Migration is retired and I/O synchronous copy is not executed. <p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied when improvement of Volume Migration success rate is desired under the condition that there are many updates to a migration source volume of Volume Migration. 2. During I/O synchronous copy, host I/O performance degrades. 	OFF	-
901	Dynamic Tiering 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>Mode 901 = ON: For tier1 (drive type is SSD), pages are allocated until the capacity reaches the limit. Without consideration of exceeding performance limitation, allocation is done from highly loaded pages until reaching the capacity limit</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<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> <p>Mode 901 = OFF (default): For tier1 (drive type is SSD), page allocation is performed based on performance potential limitation. With consideration of exceeding performance limitation, allocation is done from highly loaded pages but at the point when the performance limitation is reached, pages are not allocated any more even there is free space.</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>Notes:</p> <ol style="list-style-type: none"> 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. 2. When Tier1 is SSD while SOM 901 is set to ON, the effect of SOM 897 and 898 to the gray zone of Tier1 and Tier2 is disabled and the SOM 901 setting is enabled instead. In addition, the settings of SOM 897 and 898 are effective for Tier2 and Tier3. 3. The following is recommended when applying SOM 901. actual I/O value (total number of I/Os of all tiering policies) < performance potential value of Tier1* × 0.6 * The performance potential value of Tier1 displayed on Monitor information by using Dx-ray. <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	By setting this SOM to ON or OFF, the number of pages to be migrated per unit time at tier relocation is changed.	OFF	-

Mode	Category	Description	Default	MCU/RCU
	Dynamic Tiering for Mainframe	<p>Mode 904 = ON: The number of pages to be migrated at tier relocation is set to up to one page per second.</p> <p>Mode 904 = OFF (default):No restriction on the number of pages to be migrated at tier relocation (existing specification).</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied when: <ul style="list-style-type: none"> ▪ Dynamic Tiering for Mainframe is used (including multi-platform configuration). ▪ The requirement for response time is severe. 2. The number of pages to be migrated per unit time at tier relocation decreases. 		
908	Universal Replicator Universal Replicator for Mainframe	<p>This SOM can change CM capacity allocated to MPBs with different workloads.</p> <p>Mode 908 = ON: The difference in CM allocation capacity among MPBs with different workload is large.</p> <p>Mode 908 = OFF (default): 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>Notes:</p> <ol style="list-style-type: none"> 1. If a CLPR is used by only some MPBs among all the installed MPBs, set this SOM to ON for the CLPR to increase CM capacity allocated to the MPBs that use the CLPR. Example: (a) A CLPR only for UR JNLG. (b) A configuration where MPBs and CLPRs are separately used for Open and Mainframe systems. 2. Since CM capacity allocated to MPBs with low load is small, the performance is affected by a sudden increase in load. 3. SOM 908 cannot be used with SOM 933. When SOM 933 is set to ON, the function of SOM 908 is canceled even though SOM 908 is ON. 4. This SOM is effective for a CLPR. Therefore, when setting this SOM to ON/OFF, select target "LPRXX (XX=00 to 31)". For example, even when CLPR0 is defined (any of CLPR1 to 31 are not defined), select "LPR00" first and then set this SOM to ON/OFF. 		
930	Dynamic Provisioning Dynamic Tiering ShadowImage	<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>Mode 930 = ON: All of the zero data page reclamation operations in processing are stopped at once. (Also the zero data reclamation cannot be newly started.)</p> <p>Mode 930 = OFF (default): 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>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied when stopping or disabling zero data page reclamation by user request is required. 2. When this SOM is set to ON, the zero data page reclamation does not work at all. <ul style="list-style-type: none"> * Zero data page reclamation by WriteSame and UNMAP, IO synchronous page reclamation, program product synchronous page reclamation, and UDSR page reclamation can work. 3. When downgrading micro-program to a version that does not support this SOM while this SOM is set to ON, set this SOM to OFF after the downgrade. <ul style="list-style-type: none"> * Because the zero data page reclamation does not work at all while this SOM is set to ON. 4. When the mode is set to ON, zero data page reclamation by WriteSame function, UNMAP function, I/O synchronous page reclamation, program product synchronous page reclamation, and UDSR page reclamation can work. 5. This SOM is related to SOM 755 and SOM 859. 		
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. Mode 937 = ON: HDT monitoring data is collected even if the pool is a DP pool. Only Manual execution mode and Period mode are supported. Mode 937 = OFF (default): HDT monitoring data is not collected if the pool is a DP pool	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied when HDT monitoring data collection is required in DP environment. 2. When HDT is already used, do not set this SOM to ON. 3. For HDT monitoring data collection, shared memory for HDT must be installed. For details, contact customer support (see SOM937 sheet). 4. If monitoring data collection is performed without shared memory for HDT installed, an error is reported and the monitoring data collection fails. 5. Before removing the shared memory for HDT, set this SOM to OFF and wait for 30 minutes. 6. Tier relocation with monitoring data collected when this SOM is set to ON is disabled. 7. When DP is converted into HDT (after purchase of software license), the collected monitoring data is discarded. 8. Before downgrading the micro-program to an unsupported version, set SOM 937 to OFF and wait for at least 30 minutes. 		
972	Common	<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>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied when a delay in host I/O response due to reclamation processing occurs in a customer environment. 2. Reclamation processing is delayed. 3. This SOM is to prioritize host I/O response over reclamation processing in VxVM environment, so that the time required for reclamation processing may increase when this SOM is set to ON. <p>For details about the interaction between this SOM and SOM 1069, contact customer support (see SOM1069 sheet).</p>	OFF	-
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</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>details, contact customer support (see SOM972_973 sheet).</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied when a delay in host I/O response due to reclamation processing occurs in a customer environment. 2. When this SOM is set to ON, reclamation processing is delayed. 3. This SOM is to prioritize host I/O response over reclamation processing in VxVM environment, so that the time required for reclamation processing may increase when this SOM is set to ON. <p>For details about the interaction between this SOM and SOM 1069, contact customer support (see SOM1069 sheet).</p>		
1021	Universal Volume Manager	<p>This SOM can enable or disable the auto-recovery for external volumes of an EMC storage system.</p> <p>Mode 0121 = ON: An external volume that is blocked due to Not Ready status can be recovered automatically regardless of the type of external storage system.</p> <p>Mode 1021 = OFF (default): An external volume that is blocked due to Not Ready status might not be recovered automatically depending on the type of external storage system.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied when the auto-recovery of external volumes that are blocked due to Not Ready status is desired in UVM connection using an ECM storage system as an external storage system. 2. When this SOM is set to ON and the connected external storage system is not in stable status (such as failure and recovery from failure), a blockage due to Not Ready status and auto-recovery might occur repeatedly. 	OFF	-
1043	Universal Replicator	<p>This SOM disables journal copy.</p> <p>Mode 1043 = ON: When the following conditions are met at the UR secondary site, the journal copy is disabled.</p>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
	Universal Replicator for Mainframe	<p>The following conditions (1) and (2) or (1) and (3) are met:</p> <ol style="list-style-type: none"> 1. 4,096 or more journals are accumulated at the secondary site. 2. The CLPR write pending rate for journal volumes of MP unit for which journal ownership at the RCU is defined is 25% or higher (including the write pending rate for other than journal volumes). 3. It takes 15 seconds or longer to start restore after journal copy at the RCU. <p>Note: Even though the above conditions are met, journal copy is not disabled when all time stamps of the journals accumulated are the same in a consistency group containing multiple journals.</p> <p>Mode 1043 = OFF (default): The journal copy is not disabled.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM applies when one of the following conditions is met: <ol style="list-style-type: none"> a. Multiple journals are registered in a consistency group of CCI. b. Multiple journals are registered in an extended consistency group. 		

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"> 2. If SOM 690 is set to ON and the Write Pending rate is 60% or higher, the journal copy is disabled regardless of the setting of this SOM. 3. When the host write speed is faster than the JNL copy speed, the usage rate of the master journal increases. 4. This SOM is effective within the range of each CLPR. Therefore, an operation target LPRxx (xx= 00 to 31) needs to be selected before setting this SOM to ON/OFF. <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"> 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.) 		
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>Mode 1061 = ON: The CAW function works.</p> <p>Mode 1061 = OFF (default): The CAW function does not work. (COW works.)</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied when the CAW function is enabled. 2. The cache write pending rate may increase. 		
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>Mode 1067 = ON: Even when a UR pair has been registered, downgrading the microcode to a version that does not support URxUR (including delta) is allowed.</p> <p>Mode 1067 = OFF (default): If any UR pair has been registered, downgrading the microcode to a version that does not support URxUR (including delta) is not allowed.</p> <p>Notes:</p> <ol style="list-style-type: none"> 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). 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. 	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p>Phenomena:</p> <ul style="list-style-type: none"> 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. b. When the pair between I site and R site in cascade configuration is resynchronized, the pair status cannot change from COPY to PAIR. c. When the microcode is downgraded at R site in cascade configuration, the pair between I site and R site cannot be resynchronized. 		
1068	Common	<p>This mode can detect and report a minor drive response delay early by severely checking drives.</p> <p>Mode 1068 = ON: 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>Mode 1068 = OFF: 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>Notes:</p> <ol style="list-style-type: none"> 1. Apply this mode to detect a minor delay in drive response. 2. When a delay is suspected, a processing to refer to the statistics data and determine the delay works. 3. If SOM 157 is set to ON, the output prevention status of SSB=A4CE is not cleared in one-day cycle. 4. When applying this mode only, a SIM for delay detection is reported but the HDD is not blocked. To block the HDD, SOM 144 also needs to be applied. 	OFF	-
1069	Common	<p>By setting this SOM, the INQUIRY Page E3h field is changed. The field varies depending on the</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>combination of SOMs 972, 973, and 1069. For details, contact customer support (see SOM1069 sheet).</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied when the page problem occurs in an environment where Symantec ASL 6.0.5 or higher is used and SOM 972 and/or 973 is set to ON. 2. When this SOM is set to ON, reclamation processing is delayed. 3. The priority of setting when SOMs are set at the same time is SOM 1069, 972, and then 973. The setting of higher priority SOM is enabled. 		
1070	Global-active device	<p>This SOM changes the processing for a group operation with GAD consistency group (CTG).</p> <p>Mode 1070 = ON: The status change of all pairs in a consistency group. is performed for 50 msec.</p> <p>Mode 1070 = OFF (default): The status change of all pairs in a consistency group is performed for 1 msec.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied when reducing the time to complete status change of all pairs in a consistency group at a group operation (suspension and resync operation) with the GAD CTG function. In a system configuration where host I/O performance is prioritized, do not use this SOM because setting this SOM may affect the host I/O performance. 2. The MP usage rate increases during status change of all pairs in a consistency group. For details about approximate percentage increase in MP usage rate, contact customer support (see SOM1070 sheet). 	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> <p>Mode 1079 = ON: The Proprietary ANCHOR command is unavailable.</p> <p>Mode 1079 = OFF (default): The Proprietary ANCHOR command is available.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>Notes:</p> <ol style="list-style-type: none"> 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. 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"> a. SOM 1079 setting ON/HMO 97 setting ON --> Proprietary ANCHOR command Unavailable b. SOM 1079 setting ON/HMO 97 setting OFF --> Proprietary ANCHOR command Unavailable c. SOM 1079 setting OFF/HMO 97 setting ON --> Proprietary ANCHOR command Available d. SOM 1079 setting OFF/HMO 97 setting OFF --> Proprietary ANCHOR command Unavailable 		
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>Mode 1080 = ON: The time to run the reset command for the quorum disk on the external system is 15 seconds to eliminate the impacts on commands run for the other external devices that share the Target port with the quorum disk on the external system.</p> <p>If a response to ABTS is delayed for 12 seconds or longer, the quorum disk may be blocked.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>Mode 1080 = OFF (default): The time to run a reset command for the quorum disk when performance of a path degrades is 3 seconds so that a retry is performed by an alternate path to avoid quorum disk blockage.</p> <p>Notes:</p> <ol style="list-style-type: none"> 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. <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"> When connection performance degradation occurs, the quorum disk blockage is more likely to occur. 		
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>Mode 1083 = ON: DP-VOL deletion is enabled.</p> <p>Mode 1083 = OFF (default): DP-VOL deletion is disabled.</p> <p>Notes:</p> <ol style="list-style-type: none"> This SOM is applied when the following conditions are met. <ul style="list-style-type: none"> A DP-VOL with data direct mapping attribute is deleted. The data of external volume with data direct mapping attribute associated with a deletion target DP-VOL with data direct mapping attribute will not be used again. When SOM 1083 is set to ON, the data of external volumes cannot be guaranteed. When DP-VOL deletion is performed without disconnecting an external volume, the data of the external volume cannot be guaranteed. 	OFF	-

Mode	Category	Description	Default	MCU/RCU
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>Mode 1086 = ON (default): The performance improvement is enabled.</p> <p>Mode 1086 = OFF: The performance improvement is disabled.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied when the IOPS performance of an external storage system is higher than $80k \times$ the number of installed MPBs, which is the value of IOPS that an entire local storage system sends to an external storage system. 2. When it is required to set this SOM to OFF, if IOPS sent from the local storage system to the external storage system is higher than $80k \times$ the number of installed MPBs, reduce the IOPS to lower than $80k \times$ the number of installed MPBs, and then set this SOM to OFF. (Otherwise CWP increases and cache is overloaded.) 	ON	-
1091	Compatible FlashCopy® V2 TrueCopy for Mainframe Universal Replicator for Mainframe	<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> <p>Mode 1091 = ON: The zHyperWrite function is enabled. (ReadFeatureCode setting for the zHyperWrite function)</p> <p>Mode 1091 = OFF (default): The zHyperWrite function is disabled.</p>	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM can be applied when DKCMAIN version that supports the zHyperWrite function is used. 2. To use the zHyperWrite function, a HyperSwap environment is required. 3. To enable the zHyperWrite function, set this SOM to ON on both MCU and RCU. 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. 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. 6. Do not set this SOM to ON if SOM 474 is set to ON. 7. Do not set this SOM to ON if Preserve Mirror configuration is created. 8. Do not set this SOM to ON if the TCz Function Switch 12 is set to ON. 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. 		
1093	Dynamic Provisioning Dynamic Tiering Thin Image	<p>(VSP G130, G/F350, G/F370, G/F700, G/F900) 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>Mode 1093 = ON: Background unmap cannot work.</p> <p>Mode 1093 = OFF (default): Background unmap can work.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>Notes:</p> <ol style="list-style-type: none"> 1. 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. 2. When pool capacity shrinking is performed for an FMD parity group while the mode is set to ON, the pool capacity shrinking cannot be completed. Make sure to set the mode to OFF prior to performing pool capacity shrinking for an FMD parity group. 		
1096	Universal Replicator Universal Replicator for Mainframe	<p>This SOM disables read-journal frequency reduction.</p> <p>Mode 1096 = ON: The read-journal frequency reduction does not work.</p> <p>Mode 1096 = OFF (default): The read-journal frequency reduction works.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. This SOM is applied when a significant delay, which is about 200 msec or longer, occurs in the line between MCU and RCU. 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. 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. 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. 	OFF	Both
1097	Common	<p>This SOM disables the warning LED to blink when specific SIMs are reported.</p> <p>Mode 1097 = ON (default): When SIM=452XXX, 462XXX, 3077XY, 4100XX, or 410100 is reported, the warning LED does not blink.</p>	ON	-

Mode	Category	Description	Default	MCU/RCU
		<p>Mode 1097 = OFF: When SIM=452XXX, 462XXX, 3077XY, 4100XX, or 410100 is reported, the warning LED blinks.</p> <p>Note: This SOM disables the warning LED to blink when specific SIMs are reported.</p>		
1099	TrueCopy for Mainframe	<p>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.</p> <p>Mode 1099 = ON: 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"> ▪ After Hyperswap is performed, SSB=8BD8 and 8BD9 are logged for a pair where the Hyperswap is performed. <p>Mode 1099 = OFF (default): The completion of path deletion for every path is reported.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Apply this mode when a storage system with over 32 CUs is used in a TCz environment in which PPRC FREEZE is available. 2. The mode is effective for the entire storage system. 3. FREEZE using Sync CTG is performed without path deletion, so it is not subject to this change in FREEZE behavior. 	OFF	MCU
1106	Dynamic Provisioning Dynamic Provisioning for Mainframe Dynamic Tiering Dynamic Tiering for Mainframe	This SOM is used to perform rebalance even when the number of reclaimed pages is 0 after 0 data page reclamation.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>Mode 1106 = ON: The rebalance (the same as the rebalance that works at pool expansion or after 0 data page reclamation) (*3) works one of the following conditions is met:</p> <ol style="list-style-type: none"> 1. The usage rate is checked for parity groups in a pool once a day, and the usage rate is not balanced (*1) among parity groups. 2. After 0 data page reclamation, the number of reclaimed pages is 0 (*2). <p>Mode 1106 = OFF (default): The rebalance does not work even when the usage rate is not balanced.</p> <p>*1: How to determine whether usage rate is unbalanced among parity groups</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> <p>Note: The term "page usage rate" refers to the percentage of the number of assigned pages in each PG compared to the total number of pages in the pool. For HDT pools, the term "total number of pages" is the number of pages assigned within each specific tier.</p> <p>Examples:</p> <ol style="list-style-type: none"> 1. In an HDP pool, if the usage rates of PG1, PG2, and PG3 are 50%, 40%, and 30% respectively, it is not determined as unbalanced. Because the average parity group usage rate is $(50\% + 40\% + 30\%) / 3 = 40\%$ and the difference in the rate between each parity group and the average is 10% at the maximum. 2. In an HDP pool, if the usage rates of PG1, PG2, and PG3 are 80%, 40%, and 30% respectively, it is determined as unbalanced. Because the average parity group usage rate is $(80\% + 40\% + 30\%) / 3 = 50\%$ and the difference in the rate between each parity group and the average is 30% at the maximum. 3. In an HDT pool, if the usage rates of PG1, PG2, and PG3 are 80% (SSD), 40% (SAS15K) and 		

Mode	Category	Description	Default	MCU/RCU
		<p>30% (SAS15K), it is not determined as unbalanced, because:</p> <ul style="list-style-type: none"> ▪ The average parity group usage rate of Tier1 is $(80\%) / 1 = 80\%$ and the difference in the rate between the parity group and the average is 0%. ▪ The average parity group usage rate of Tier2 is $(40\% + 30\%) / 2 = 35\%$ and the difference in the rate between the parity group and the average is 5% at the maximum. <p>*2: Condition for rebalance after 0 data page reclamation</p> <p>When the mode is set to ON, rebalance works even when reclaimed page is 0 at 0 data page reclamation.</p> <p>*3: Rebalance (the same as the rebalance that works at pool expansion or after 0 data page reclamation) works according to the SOM1195 setting (default OFF).</p> <p>Note: This SOM is applied when balancing the usage rate is required at a customer site where the usage rate is not even.</p>		
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>Mode 1113 = ON: The asynchronous processing of host I/Os by the capacity saving function, other than garbage collection and de-staging, is stopped.</p> <p>Note: While the capacity reduction processing is not working, the capacity saving rate might degrade.</p> <p>Mode 1113 = OFF (default): The capacity saving function fully works.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>Relationship between SOM 1113 and SOM 1112: When both modes are set to ON, the setting of SOM 1112 is prioritized over that of SOM 1113. When SOM 1112 is set to ON, all asynchronous processing for host I/Os among those related to the capacity saving function are stopped, including garbage collection and de-staging, so that write I/Os to V-VOLs with Compression or Deduplication and Compression set are disabled.</p>		
1115	Deduplication and Compression	<p>When LDEV format is performed for a virtual volume with capacity saving (Compression, or Deduplication and Compression, the same hereinafter) enabled, data is initialized without using metadata regardless of the mode setting.</p> <p>Mode 1115 = ON: When LDEV format is performed for a virtual volume with capacity saving enabled, the data is initialized without using the metadata.</p> <p>Mode 1115 = OFF (default): When LDEV format is performed for a virtual volume with capacity saving enabled, normal formatting is performed, but if one of the following conditions is met, the data is initialized without using metadata.</p> <ul style="list-style-type: none"> ▪ There is a pinned slot. ▪ The capacity saving status is "Failed". ▪ The virtual volume is blocked (Normal restore cannot be performed). <p>The processing time increases with increase in pool capacity. Estimate of processing time:</p> $\text{Processing time (minutes)} = (\text{pool capacity (TB)} / 40) + 5$ <p>If the result of dividing the pool capacity by 40 has decimal places, round it up to the next integer.</p> <p>The processing finishes early if there is less capacity of allocated pages. For example, in the case of a 4-PB pool, normal formatting (SOM 1115 OFF) is faster if the LDEV capacity is 50 GB or less, therefore the performance of LDEV format without using metadata is better.</p>	ON	-
1118	Open	This SOM is used to disable the ENC reuse function.	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>Mode 1118 = ON: When a failure occurs in the Expander chip mounted on a controller board (CTLS, CTLSE) or an ENC board, the reuse function does not work but SIM=CF12XX is reported and the ENC is blocked.</p> <p>Mode 1118 = OFF (default): When a failure occurs in the Expander chip mounted on a controller board (CTLS, CTLSE) or an ENC board, the reuse function works.</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>Note: The ENC reuse function is enabled as default. This SOM is applied when you want to disable the ENC reuse function.</p>		
1169	Deduplication and Compression	<p>This mode can enable or disable the deduplication processing that works during resync processing from P-VOL to S-VOL by the copy function for DP-VOLs with capacity saving in Inline mode enabled.</p> <p>Mode 1169 = ON: Deduplication processing is not performed during resync processing.*</p> <p>Mode 1169 = OFF: Deduplication processing is performed during resync processing.</p> <p>* To reduce the capacity consumption in the case that the pool capacity is almost depleted for example, the deduplication processing might be performed during the resync processing. In particular, the following cases apply:</p> <ul style="list-style-type: none"> ▪ The usage rate exceeds the warning threshold. ▪ Free capacity is smaller than about 240 GB. 	ON (90-03-01 and later)	-

Mode	Category	Description	Default	MCU/RCU
		<p>Notes:</p> <ol style="list-style-type: none"> 1. When SOM 1280 is ON, deduplication processing is performed even when SOM 1169 is ON. 2. If conditions to disable deduplication processing by SOM 1191 are met, deduplication processing is not performed even when SOM 1169 is OFF. For details about the conditions to disable deduplication processing, contact customer support (see SOM1191 sheet). 3. When SOM 1169 is set to ON, like the post mode, estimating and reserving the capacity of a temporary storing area in the copy target DP volume or pool in advance is necessary. 4. SOM 1169 is not effective for the initial copy at pair creation, but there are some exceptional cases for SI and VM, such as pair creation using a used volume for S-VOL. In this case, deduplication processing is performed or not performed according to the mode setting. 5. SOM 1169 is not related to determining whether to perform deduplication processing in synchronization with initial write. For example, the setting of SOM 1169 does not contribute to a reduction in time to migrate data to a newly defined volume. 		
1174	Open Universal Volume Manager	<p>This SOM is used to disable a path that is logged in from a host or an external storage system (host path and external path) to be used as an external path.</p> <p>Mode 1174 = ON: A path logged in from a host or an external storage system is excluded from the WWN discovery target.</p> <p>Mode 1174 = OFF: A path logged in from a host or external storage system is included in the WWN discovery target.</p>	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>Notes:</p> <ol style="list-style-type: none"> 1. Apply SOM 1174 when discovery is performed while specifying a universal port that is being logged in from a host or an external storage system. 2. If SOM 1174 is set to ON, external volumes cannot be created using the paths being logged in from hosts and external storage systems. 3. If WWN discovery is performed while SOM 1174 is set to ON, the storage system being logged in from hosts and external storage systems are displayed as [Unknown] in the discovery result. 		
1175	Universal Replicator for Mainframe	<p>This SOM enables the CFW data that the P-VOL of a URz pair created from BCM or CCI to be transferred to the S-VOL.</p> <p>Mode 1175 = ON: The CFW data written to the URz P-VOL is transferred to the S-VOL.</p> <p>Mode 1175 = OFF: The CFW data written to the URz P-VOL is not transferred to the S-VOL.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Apply SOM 1175 if the CFW data transfer from the URz P-VOL to the S-VOL is required. When a pair is created with SOM 1175 set ON, the CFW data that the P-VOL receives is transferred to the S-VOL. It can apply to pair creation from BCM or CCI only. If a pair is created from Device Manager - Storage Navigator, transferring the CFW data can be selected, as usual. 2. If SOM 1175 is set to OFF, to transfer the CFW data to the S-VOL, a journal ceation is performed as an extension of CFW write, which causes the CFW write performance to degrade compared to that when SOM 1175 is set to ON. 3. The mode setting, whether ON or OFF, can be changed regardless of the URz pair status, but to transfer the CFW data to the S-VOL, a new pair must be created after setting SOM 1175 to ON. 	ON	Both
1182	Universal Replicator	<p>This SOM is used to enable replacement of the journal volume on the primary storage system of the UR delta resync pair in a GAD 3DC delta resync (GAD+UR) configuration.</p>	OFF	MCU (MCU of delta UR pair, L site in GAD)

Mode	Category	Description	Default	MCU/RCU
		<p>Mode 1182 = ON: If a reserve journal is added to the journal on the primary storage system of the delta resync pair, the status of the journal changes to HLD.</p> <p>Mode 1182 = OFF:</p> <p>Deletion of the journal whose status is HOLD, HOLDING, or HLDE is guarded on the primary storage system of the UR delta resync pair.</p> <p>If a reserve journal volume has already been added, delete the reserve journal volume, and then add a reserve journal volume again while the system option mode 1182 is set to ON.</p> <p>After the journal volume is replaced, restore the delta resync pair status from Device Manager - Storage Navigator (you cannot perform this operation from CCI).</p>		+UR config.)
1191	Deduplication and Compression	<p>When online data migration is performed on volumes whose capacity saving mode is set to deduplication and compression and inline, setting SOM 1191 to ON can mitigate the I/O performance degradation caused by the deduplication processing.</p> <p>Mode 1191 = ON: Inline deduplication processing is disabled when the average of MP usage rates on the entire storage system is 50% or higher. When SOM 1191 is ON, SOM 1191 applies to the entire storage system.</p> <p>Mode 1191 = OFF: Inline deduplication processing is not disabled regardless of the average MP usage rate.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Before setting this mode to ON, estimate the temporary area in a pool and then reserve it in advance. For details, see the Caution* below. 2. By setting the mode to ON, the inline deduplication processing is disabled when the average MP usage is 50% or higher even though SOM 1280 is set to ON. 3. When SOM 1169 is set to ON, the inline deduplication at copy processing is disabled regardless of SOM 1191 setting. 	OFF	-

Mode	Category	Description	Default	MCU/RCU
		<p>* Caution: When SOM 1191 is ON and MP usage (entire storage system) reaches or exceeds 50%, the pool used capacity increases due to consumption of temporary area for post-process deduplication processing. Before enabling this SOM, verify that there is enough pool capacity by using the following conditional expressions, and then set SOM 1191 to ON only when the applicable conditional expression is met:</p> <ul style="list-style-type: none"> ▪ If SOM 1191 is set to ON during data migration: $\frac{\text{pool-capacity} \times \text{depletion-threshold} [\%]}{100} > \text{current-pool-used-capacity} + (\text{data-capacity-to-be-migrated} \times (100 - \text{estimated-compression-ratio} [\%])^*) / 100$ ▪ If SOM 1191 is set to ON during normal operations: $\frac{\text{pool-capacity} \times \text{depletion-threshold} [\%]}{100} > \text{current-pool-used-capacity} + (\text{data-capacity-to-be-written-to-non-write-area} \times (100 - \text{estimated-compression-ratio} [\%])^*) / 100$ <p>where <i>estimated-compression-ratio</i> is the ratio of the estimated compression reduction effect. To convert the compression ratio in the N:1 format to percentage, use the following equation:</p> $\text{compression-ratio} [\%] = (1 - 1 \div N) \times 100$ <p>If the estimated compression ratio is not specified, use 0% to calculate.</p>		
1198	TrueCopy Universal Replicator Global-active device	To expand TC, UR, and GAD pair capacity, the difference management method must be changed from shared memory (SM) difference management to hierarchical difference management. This mode is used to enable changing the difference management method by using CCI. The difference management method is changed at the first TC, UR, or GAD pair creation or resync operation after setting this mode.	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p>Mode 1198 = ON: The difference management method for volumes of 4 TB or less used in TC, UR, or GAD pairs is changed to hierarchical difference management regardless of SOM 5, SOM 6, and SOM 1199 settings.</p> <p>Mode 1198 = OFF:</p> <ul style="list-style-type: none"> ▪ When SOM 1198 is OFF and SOM 1199 is ON, the difference management method for volumes of 4 TB or less used in TC, UR, or GAD pairs is changed to SM difference management. ▪ When both SOM 1198 and SOM 1199 are OFF, the difference management method is not changed. <p>Notes:</p> <ol style="list-style-type: none"> 1. Apply this mode when the storage system does not have an SVP and you want to expand the capacity of volumes used in TC, UR, or GAD pairs. 2. Changing the difference management method can affect the I/O response performance depending on the I/O pattern. 3. Changing the difference management method can affect the initial copy time depending on the conditions. 		
1199	TrueCopy Universal Replicator Global-active device	This mode is used to enable changing the difference management method from hierarchical difference management back to SM difference management if necessary for some reasons after the method was changed to hierarchical difference management by setting SOM 1198 to ON. The difference management method is changed at the first TC, UR, or GAD pair creation or resync operation after setting this mode.	OFF	Both

Mode	Category	Description	Default	MCU/RCU
		<p>Mode 1199 = ON:</p> <ul style="list-style-type: none"> ▪ When both SOM 1199 and SOM 1198 are ON, the difference management method for volumes of 4 TB or less used in TC, UR, or GAD pairs is changed to hierarchical difference management regardless of SOM 5 and 6 settings. ▪ When SOM 1199 is ON and SOM 1198 is OFF, the difference management method for volumes of 4 TB or less used in TC, UR, or GAD pairs is changed to SM difference management regardless of SOM 5 and 6 settings. <p>Mode 1199 = OFF:</p> <ul style="list-style-type: none"> ▪ When SOM 1199 is OFF and SOM 1198 is ON, the difference management method for volumes of 4 TB or less used in TC, UR, or GAD pairs is changed to hierarchical difference management regardless of SOM 5 and 6 settings. ▪ When both SOM 1199 and SOM 1198 are OFF, the difference management method is not changed. <p>Notes:</p> <ol style="list-style-type: none"> 1. Apply this mode when the storage system does not have an SVP and you want to expand the capacity of volumes used in TC, UR, or GAD pairs. 2. Changing the difference management method can affect the I/O response performance depending on the I/O pattern. 3. Changing the difference management method can affect the initial copy time depending on the conditions. 		
1202	Common	This mode is to disable the improvement for responses to host I/Os during FMD and SSD firmware replacement. I/Os are disabled during reboot in drive firmware replacement by the specification. This mode allows users to enable the host I/Os to mitigate the impact on the performance during drive firmware replacement.	OFF	--

Mode	Category	Description	Default	MCU/RCU
		<p>Mode 1202 = ON:</p> <ul style="list-style-type: none"> ▪ Synchronous read I/O: Disabled. ▪ Other than synchronous read I/O: Disabled. ▪ Write I/O: Disabled. <p>Caution: When the mode is set to ON, the host I/O performance might be degraded during FMD and SSD firmware replacement.</p> <p>Mode 1202 = OFF:</p> <ul style="list-style-type: none"> ▪ Correction read: Enabled. ▪ Other than synchronous read I/O: Disabled. ▪ Write I/O: Disabled. 		
1204	Dynamic Provisioning Dynamic Provisioning for Mainframe Dynamic Tiering Dynamic Tiering for Mainframe Thin Image	<p>This mode is intended to improve the page migration performance when the MP usage rate is within the range from 30% to 50%.</p> <p>Mode 1204 = ON: When the MP usage rate is within the range 30 to 50%, the processing interval is shortened to improve the page migration throughput.</p> <p>Mode 1204 = OFF: There is no change for the processing interval.</p> <p>For details, see sheet SOM 1204.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Apply this mode when the following conditions are met: <ul style="list-style-type: none"> ▪ The MP usage rate constantly exceeds 30%. ▪ Prioritizing the page migration processing over the I/O processing is required. 2. When SOM 1204 is set to ON, the operation frequency of the relocation processing increases so that the host I/O response performance is degraded. 3. When SOM 904 is set to ON, the SOM 904 setting is prioritized. 4. By setting SOM 1204 to ON, the MP usage rate increases by 3 to 10% due to the asynchronous processing, and the host I/O response may be degraded. 	OFF	-
1205	Dynamic Provisioning	Changes the background unmap processing speed for FMC drives.	OFF	-

Mode	Category	Description	Default	MCU/RCU
	Dynamic Tiering Thin Image	<p>Mode 1205 = ON: Background unmap runs at up to 42 MB/s.</p> <p>Mode 1205 = OFF: Background unmap runs at up to 10 GB/s.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. The mode is applied to prevent the host response performance from being degraded due to background unmap. 2. When SOM 1122 is set to ON, the SOM 1122 setting is prioritized. 3. As releasing physical areas runs at the normal speed, the following phenomena may occur, though the phenomena are solved immediately after the physical area release is complete: <ul style="list-style-type: none"> ▪ The used pool capacity does not decrease immediately after DP volume deletion. ▪ The saving ratio seems to be lower temporarily. ▪ The used pool capacity may increase due to rebalance. 		
1211	Universal Replicator Universal Replicator for Mainframe	<p>This mode is to change the threshold for the write pending rate that is a condition to determine whether to disable journal data copy or not. By setting the mode to ON, the threshold of write pending rate that is a condition to disable journal data copy is changed from 25% to 50%.</p> <p>Journal data copy is disabled when the following conditions (1) and (2), or (1) and (3) are met:</p> <ol style="list-style-type: none"> 1. 4096 or more journal data sets are accumulated on RCU. 2. The write pending rate of a journal volume in an MPB that has the ownership of the journal on RCU exceeds the threshold, 25% (mode OFF) or 50% (mode ON). (Including the write pending rate of those other than the journal volume) 3. On RCU, it takes 15 seconds or longer to start a restore operation after the copy processing of journals is complete. 	OFFOFF F	BothBoth

Mode	Category	Description	Default	MCU/RCU
		<p>Note: Even when the above conditions are met, if the time stamp of accumulated journal datasets is the same in a configuration where multiple journals are added to a consistency group, journal data copy is not disabled.</p> <p>Mode 1211 = ON: The threshold for the write pending rate is 50%.</p> <p>Mode 1211 = OFF: The threshold for the write pending rate is 25%.</p> <p>Apply this mode when all of the following conditions are met:</p> <ol style="list-style-type: none"> 1. Disabling journal data copy is enabled by meeting one of the following conditions: <ul style="list-style-type: none"> SOM1043 is set to ON for each CLPR on the secondary site. A configuration where multiple journals are added to a CCI consistency group (open and mainframe). A configuration where multiple journals are added to an extended consistency group (mainframe). 2. The write pending rate of a CLPR containing a journal on the secondary site exceeds 25%. <p>The mode is effective for a CLPR.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Though the mode can work on UR/URz RCU, apply it to both MCU and RCU assuming Disaster Recovery operation. 2. This mode is related to SOM 1043. 3. If SOM 690 is set to ON and the write pending rate is 60% or higher, journal data copy is disabled regardless of the setting of this mode. 4. This mode is effective per CLPR. Therefore, select a target LPR xx (xx= 00 to 31), and then set the mode to ON or OFF. For example, when setting the mode to CLPR0 (CLPR 1 to 31 are not defined), select LPR00, and then set the mode to ON or OFF. When setting the mode by selecting System, the mode cannot be enabled for any CLPRs. 		

Mode	Category	Description	Default	MCU/RCU
1222	Dynamic Provisioning Dynamic Provisioning for Mainframe Deduplication and Compression	<p>This mode is used to enable the gray zone promotion processing at HDT/HDTz tier relocation on compressed pages of a virtual volume with capacity saving enabled. The gray zone promotion processing promotes pages applicable to the gray zone from a lower tier to a free space in the upper tier after performing optimal allocation according to the number of I/Os in tier relocation.</p> <p>Mode 1222 = ON: The gray zone promotion processing is performed on compressed pages.</p> <p>Mode 1222 = OFF: The gray zone promotion processing is not performed on compressed pages.</p> <p>Apply this mode when the performance is prioritized over the reduction ratio. In an ADR with HDT/HDTz environment, if the usage rate of the second lowest tier is lower than the upper limit of the setting value, the usage rate can be increased by setting this mode to ON.</p>	OFF	--
1223	Dynamic Provisioning	<p>This mode is used to disable the mapping consistency check processing that runs at Write Same command. The mapping consistency check processing causes response performance degradation if the transfer length is short, so this mode is available to prevent the performance degradation by disabling the processing.</p> <p>Mode 1223 = ON: The mapping consistency check processing does not run at Write Same command.</p> <p>Mode 1223 = OFF: The mapping consistency check processing runs at Write Same command.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Apply the mode when all the following conditions are met: <ol style="list-style-type: none"> a. The microcode that supports the mode is applied.(90-04-08 and later in 90-04-0x range, 90-05-03 and later) b. The response time of Write Same command increase about 0.1 msec. c. The length of Write Same command is short. (less than 256KiB) 2. The mode is effective for the entire storage system. 	OFF	--

Mode	Category	Description	Default	MCU/RCU
1224	Thin Image, ShadowImage, ShadowImage for Mainframe, TrueCopy, TrueCopy for Mainframe, Universal Replicator, Universal Replicator for Mainframe, Volume Migration	<p>Prevents the MP usage rate from increasing by disabling ownership migration that takes place. In particular, when there is an LDEV used as an S-VOL whose ownership has been migrated to an MPU with the ownership of the P-VOL at pair creation, the LDEV ownership is not migrated back to the migration source MPU at pair deletion by setting the mode to ON.</p> <p>Use this mode to enable and disable ownership migration to migrate the ownership of an LDEV whose ownership has been migrated to the MPU with P-VOL ownership at pair creation back to the previous MPU at pair deletion.</p> <p>Mode 1224 = ON: Ownership migration at program product pair deletion is disabled.</p> <p>Mode 1224 = OFF: Ownership migration at program product pair deletion is performed.</p> <p>Different from other program products, the ownership in an MPU with the journal group ownership is migrated as follows in a UR configuration:</p> <ul style="list-style-type: none"> ▪ Ownership migration target: LDEV (journal volume, remote CMDDEV) ▪ Timing when ownership migration takes place: Journal volume deletion, journal group deletion from EXCTG, and mirror allocation release. <p>Notes:</p> <ol style="list-style-type: none"> 1. Apply the mode when preventing the MP usage rate increase is required. 2. The mode is effective for the entire storage system. 	OFF	Both
1242	Universal Replicator, Universal Replicator for Mainframe	This mode is used to report SIM=DCF6XX (XX=JNLG number) as a warning for an omission of setting a remote command device for delta resync in a TC/TCz-UR/URz delta resync configuration or a UR/URz-UR/URz delta resync configuration. The SIM is reported once 24 hours after the pair for delta resync is created in the target journal group.	OFF	Both

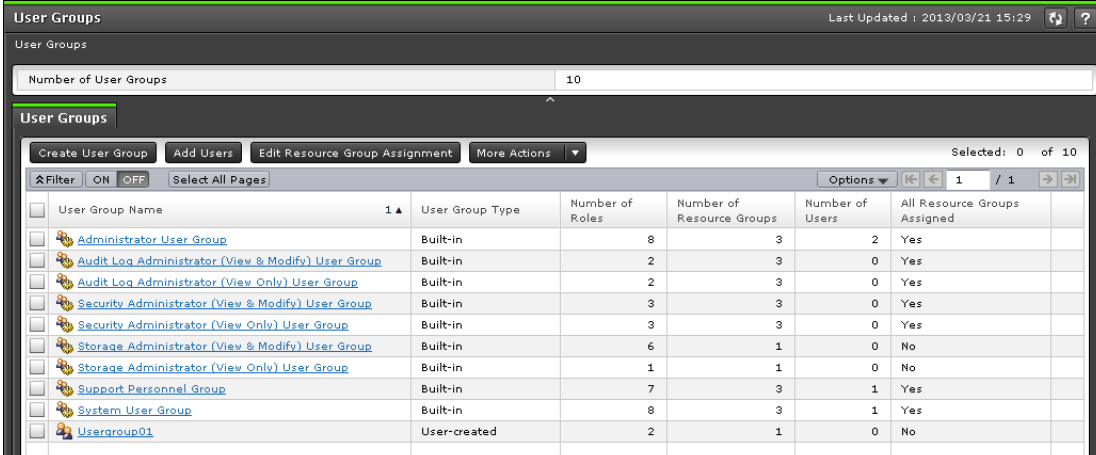
Mode	Category	Description	Default	MCU/RCU
		<p>When a delta resync operation is performed after a GDPS update and then a second delta resync operation is performed within one minute after the previous delta resync operation in a TC-UR delta resync configuration for which a remote command device was not added, the second delta resync operation fails (SSB=EBE6 or EBE7) because the second delta resync operation is performed before the delta resync internal information was defined.</p> <p>Mode 1242 = ON: SIM=DCF6XX is reported regularly if a remote command device for delta resync was not added in the target configuration. The SIM is reported for each journal group to which a remote command device for delta resync was not added.</p> <p>Mode 1242 = OFF: SIM=DCF6XX is not reported.</p>		

Appendix B: 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

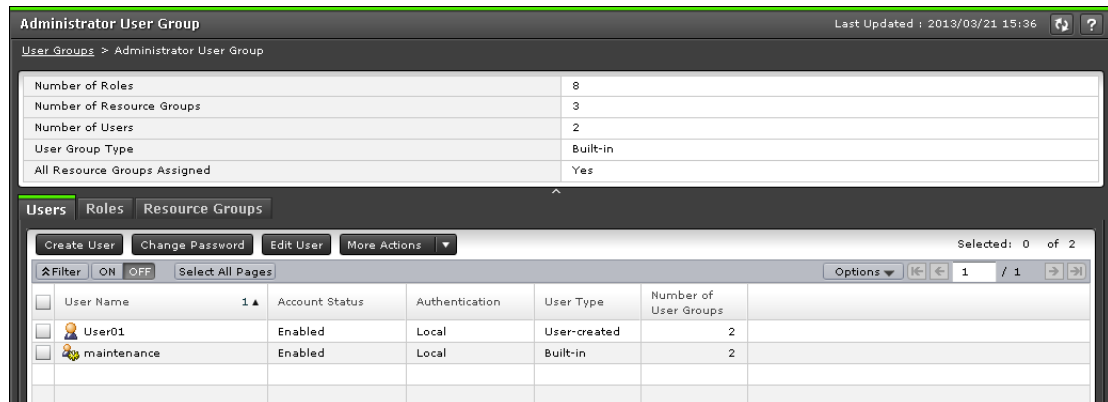
The following table describes the fields in the User Groups tab in the **User Groups** window.

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.

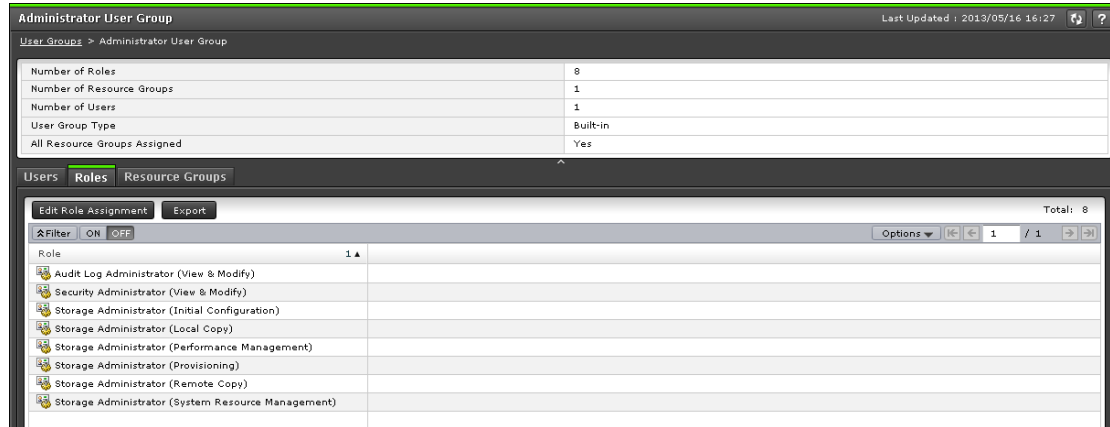
Users tab

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	<p>Account status. The following statuses are available:</p> <p>Enabled: The user can use the account.</p> <p>Disabled: The user cannot use the account or log in to Device Manager - Storage Navigator.</p>
Lockout ¹	<p>Indicates whether the status is locked.</p> <ul style="list-style-type: none"> ▪ Yes: The user account is locked, so login to Device Manager - Storage Navigator is not possible. ▪ No: The user can use the account.
Authentication	<p>Authentication method. The following methods are available:</p> <p>Local: Does not use authentication server. Uses a dedicated password for Device Manager - Storage Navigator.</p> <p>External: Uses authentication server.</p>
User Type	<p>User type. The following types are available:</p> <p>Built-in or User-created</p>
Number of User Groups	Displays the number of the user groups where the user belongs.
Create User	Creates a new user account.
Change Password	<p>Changes your own password if you click this.</p> <p>Changes the password of other users if you select a user and then click this.</p>
Edit User	<p>Changes the setting for authentication or for the account status.</p> <p>You can set the password of the selected user if you change Authentication from External to Local.</p>
Add Users ²	Adds the created users to the selected user group.
Remove Users ²	Removes the selected user from the user group. The user account itself will not be deleted.
Delete Users ²	Deletes the selected users.
Export ²	Displays a window for outputting table information.
<p>Notes:</p> <ol style="list-style-type: none"> 1. This content is not displayed by default. To display it, change the settings in the Column Settings window in the table options. 2. Appears when you click More Actions. 	

Roles tab

The following illustration shows the Roles tab of the selected user group window.

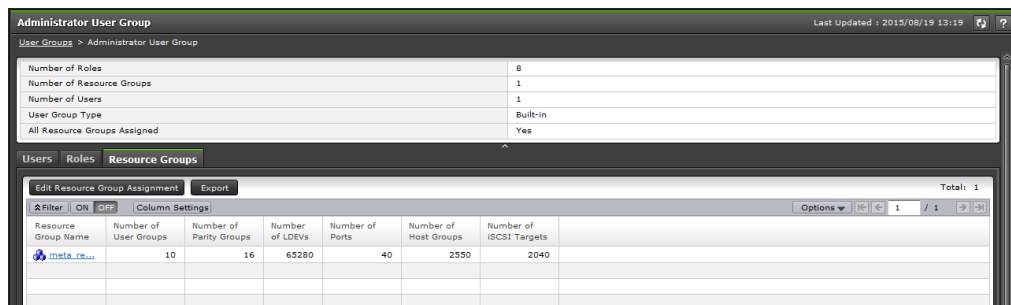


The following table describes the fields and settings in the Roles tab of the selected user group window. Role displays the roles assigned to the user group, which determines the operations the user can perform.

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 Column Settings 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.

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 ?

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

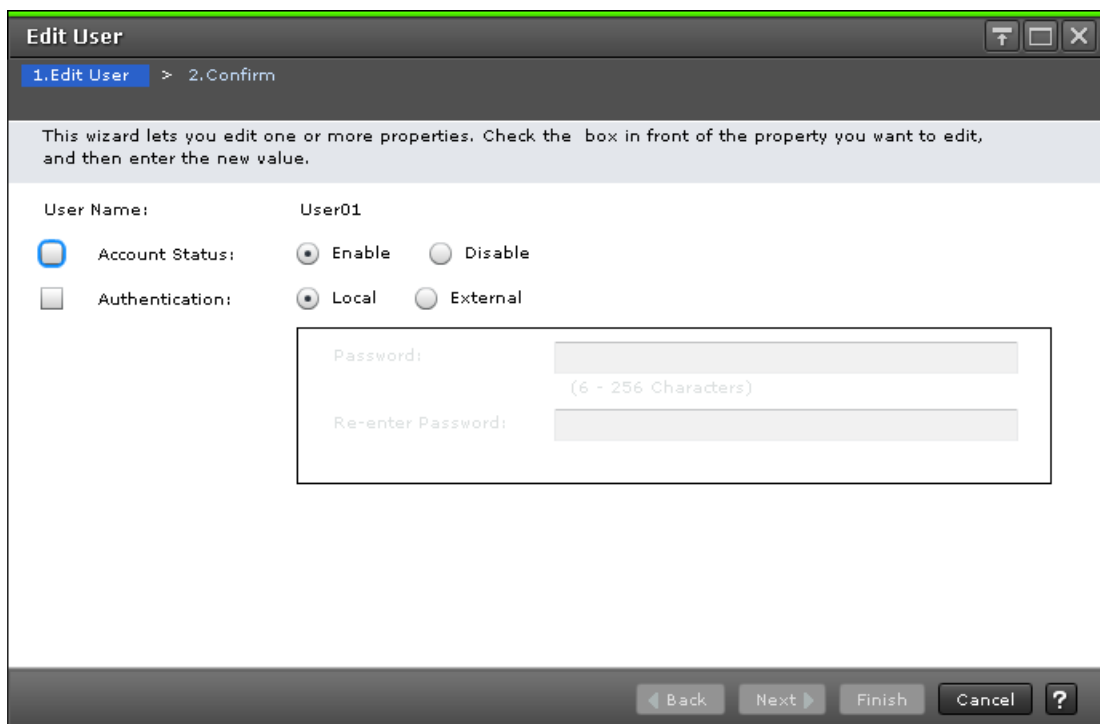
The following table describes the fields and settings used to change user passwords.

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 Back Next Apply Cancel ?

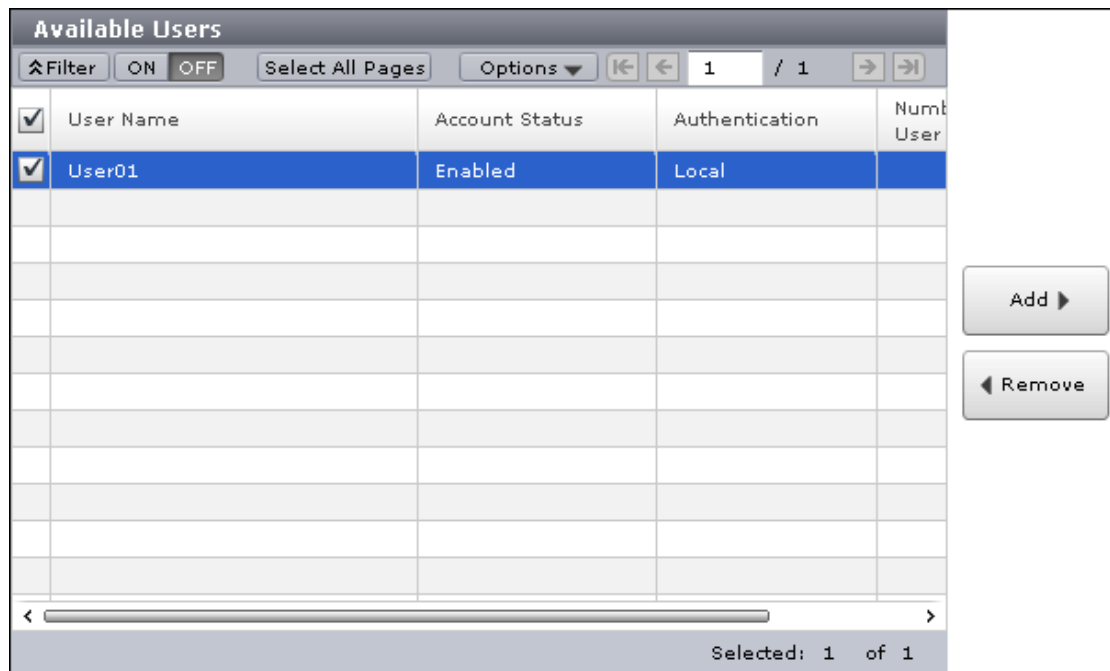
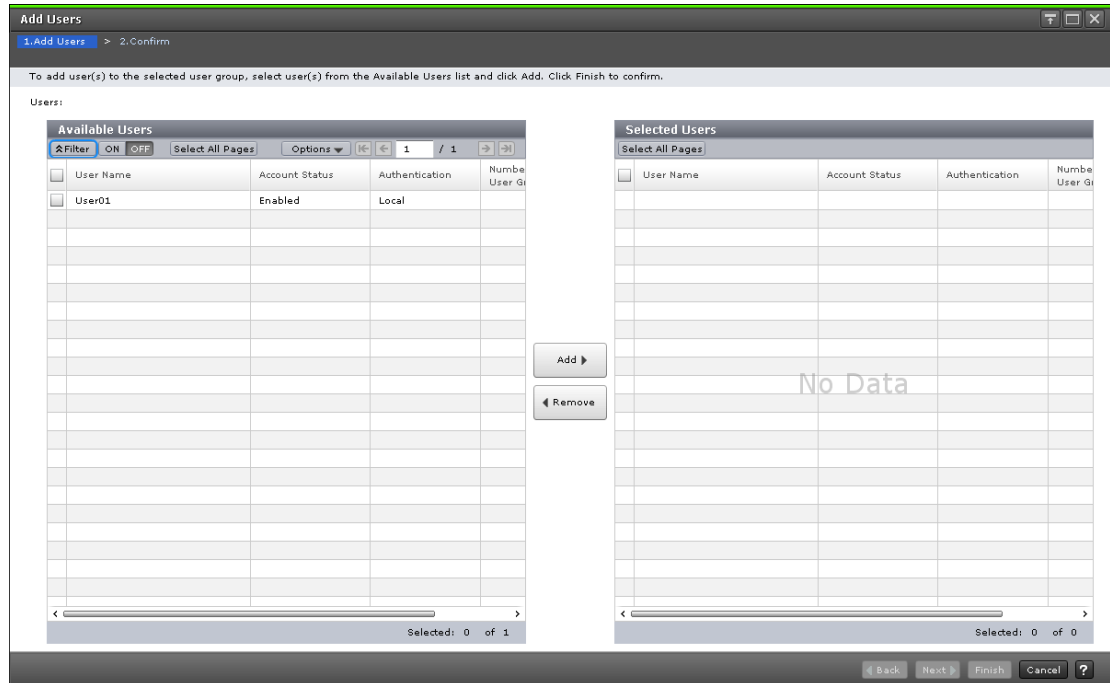
The following table describes the fields and settings in the **Edit Users** window.

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.

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: 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 \(on page 151\)](#).

Remove Users

1. Confirm

⚠ The authorization of User Group can not be used for this user. Are you sure to continue?

Task Name: (Max. 32 Characters)

Selected User Group	
User Group Name	
Administrator User Group	

Selected Users				
User Name	Account Status	Authentication	Number of User Groups	
User01	Enabled	Local	2	
				Total: 1

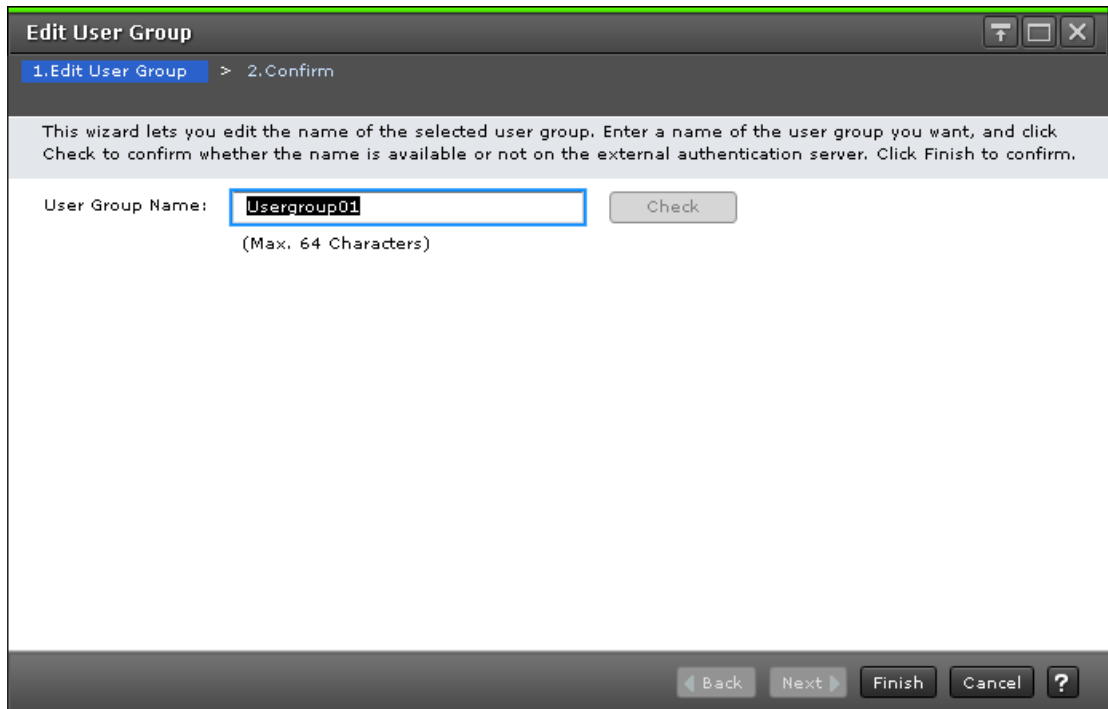
Go to tasks window for status Back Next Apply Cancel ?

Selected User Group 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.



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.

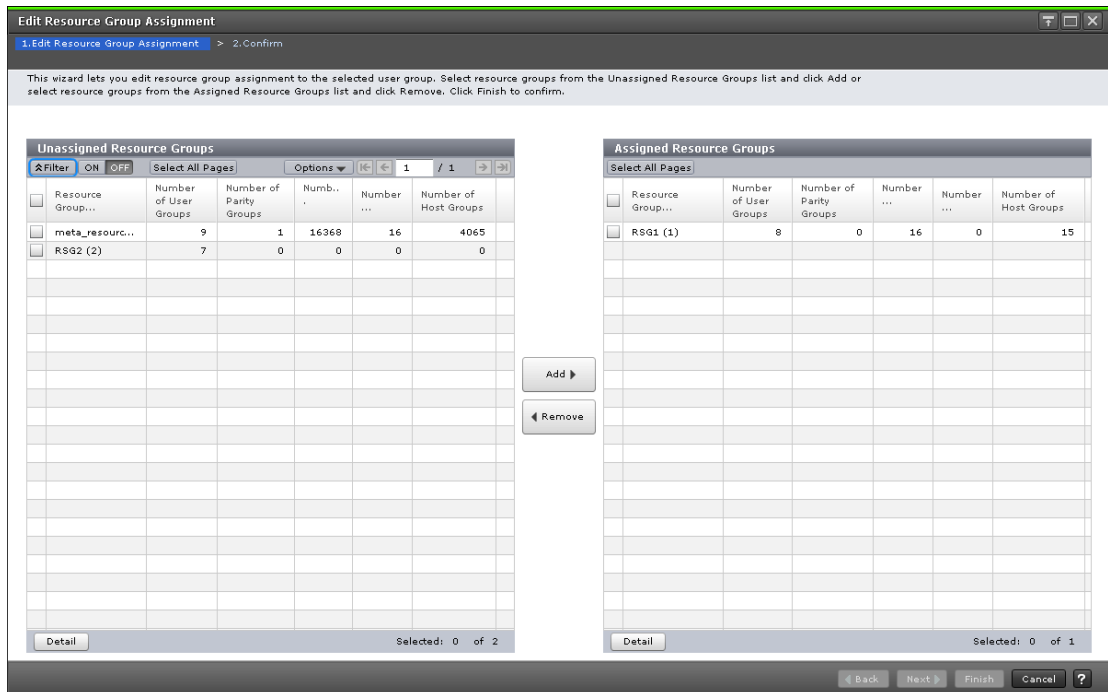
Task Name: (Max. 32 Characters)

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.



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 Assign Roles window.</p> <ul style="list-style-type: none"> ▪ Security Administrator (View Only) ▪ Security Administrator (View & Modify) ▪ Audit log Administrator (View Only) ▪ Audit log Administrator (View & Modify) ▪ Support Personnel (Vendor Only) <p>When this item is set to Yes, Unassigned Resource Groups table, Assigned Resource Groups table, Add button, and Remove button are disabled.</p>

Lists the resource groups to be assigned to the user group.

Item	Description
Resource Group Name (ID)	Displays the name and ID of the resource group assigned to the user group to be created.
Number of User Groups	Displays the number of user groups that are assigned to the resource group.
Number of Parity Groups	Displays the number of parity groups that are assigned to the resource group.
Number of LDEVs	Displays the number of LDEVs that are assigned to the resource group.
Number of Ports	Displays the number of ports that are assigned to the resource group.
Number of Host Groups	Displays the number of host groups that are assigned to the resource group.
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.

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

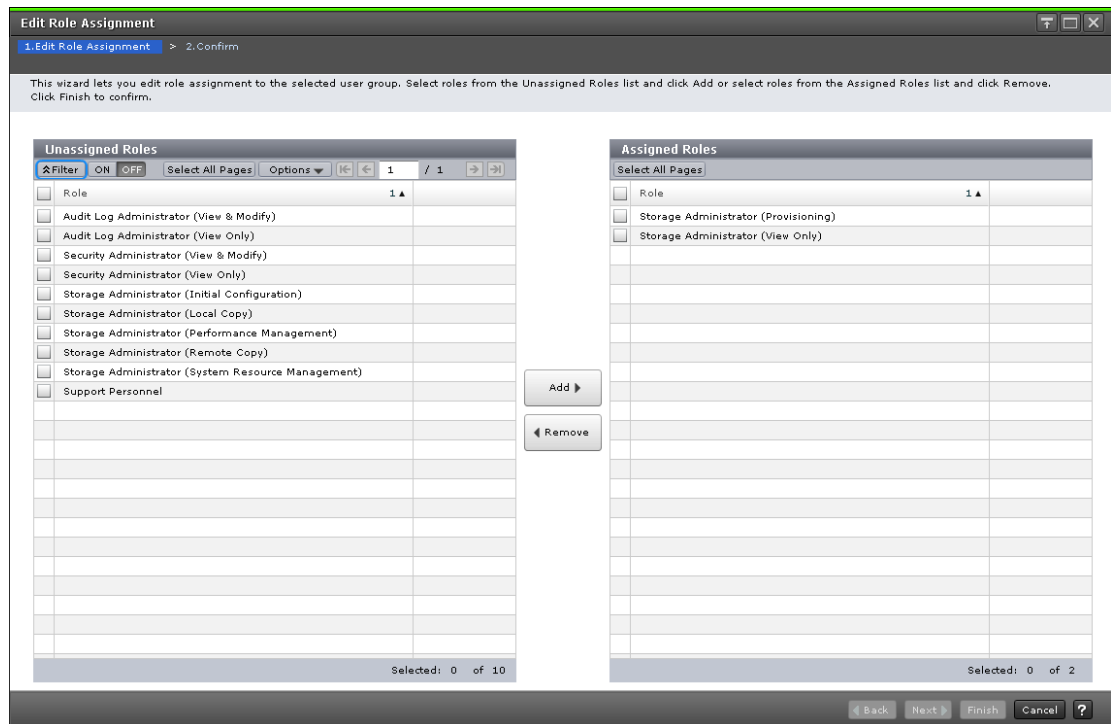
The following table lists the resource groups that are not assigned to the user group.

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.
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.

Item	Description
Detail	Displays the detail of the selected resource group.

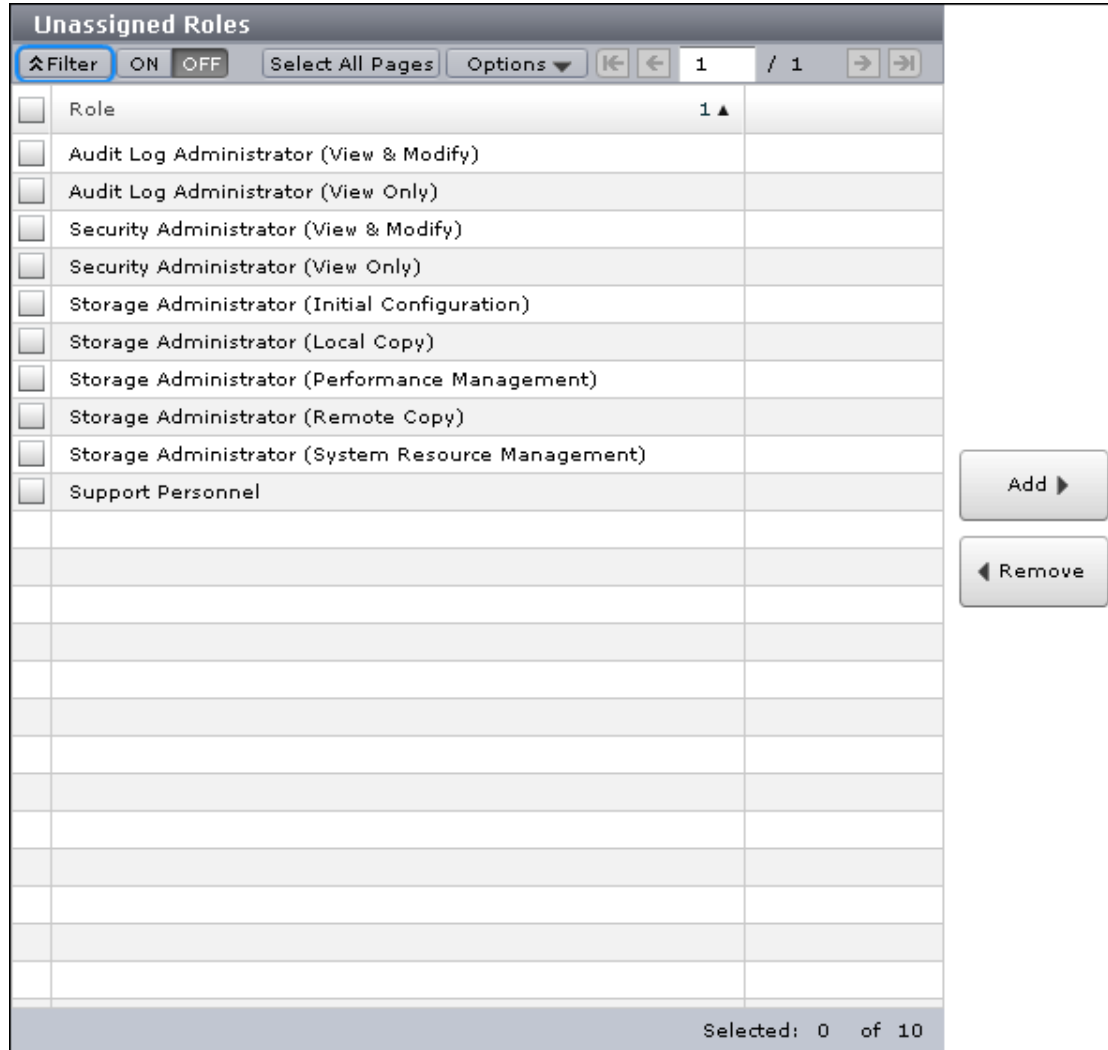
Edit Role Assignment wizard

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

1. Edit Role 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	All Resource Groups Assigned
usergroup01	No

Selected Roles as Assigned	
Role	
Storage Administrator (Initial Configuration)	
Total: 1	

Selected Roles as Unassigned	
Role	
Storage Administrator (Provisioning)	
Total: 1	

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

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.

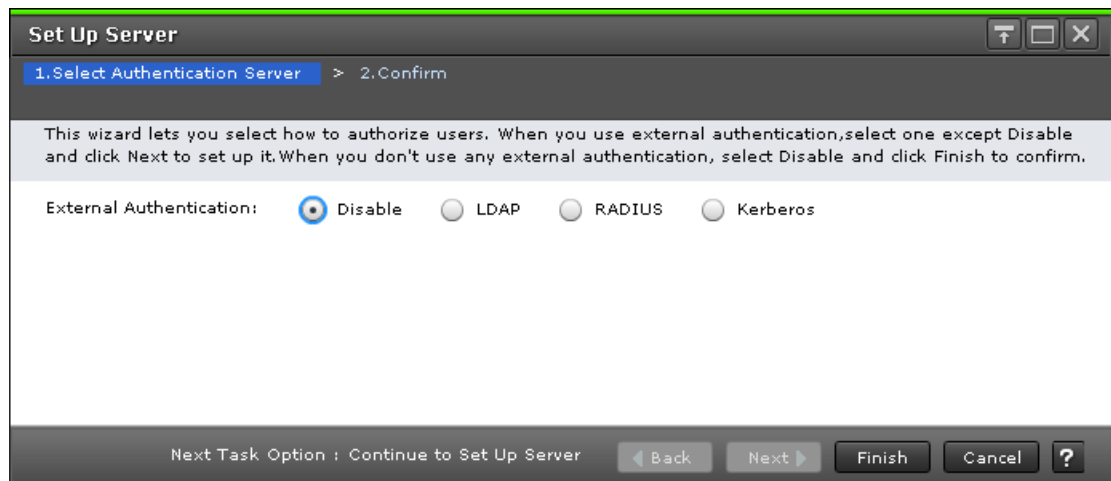
Selected Unassigned Roles

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.



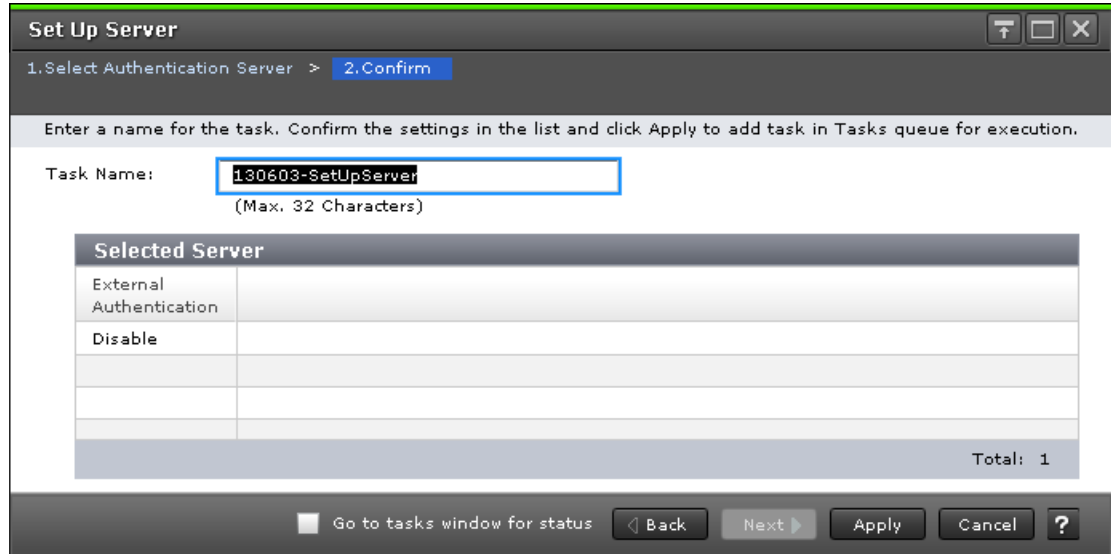
The following tables describe the fields and settings used to set up external authentication in the **Select Authentication Server** window.

Item	Description
External Authentication	<p>Select the type of authentication server.</p> <ul style="list-style-type: none"> ▪ Disable: Does not use any authentication server. Users are authenticated with user information registered in the SVP. ▪ LDAP: Users are authenticated with user information registered in the LDAP server. ▪ RADIUS: Users are authenticated with user information registered in the RADIUS server. ▪ Kerberos: Users are authenticated with user information registered in the Kerberos server. <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 Setup Server 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"> Disable: Does not use any authentication server. Users are authenticated with user information registered in the SVP. LDAP: Users are authenticated with user information registered in the LDAP server. RADIUS: Users are authenticated with user information registered in the RADIUS server. Kerberos: Users are authenticated with user information registered in the Kerberos server.

LDAP Properties window

To open this window, select LDAP in the **External Authentication** window.

The screenshot shows a window titled "LDAP Properties" with a standard Windows-style title bar (minimize, maximize, close buttons). The window contains a table of configuration settings. At the bottom right of the table is a "Set Up Server" button. At the bottom right of the window is a "Close" button and a help icon (question mark).

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	-

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"> ▪ Enable: Performs the search using information registered in the SRV records in the DNS server. ▪ Disable: Performs the search using the host name and the port number.
Authentication Protocol	Displays the LDAP protocol to use.

Item	Description
External User Group Mapping	Displays whether to connect an authentication server to an authorization server. <ul style="list-style-type: none"> ▪ Enable: Connects an authentication server to an authorization server. ▪ Disable: Does not connect an authentication server to an authorization server.
Primary Host Name	Displays the host name of the LDAP server.
Primary Port Number	Displays the port number of the LDAP server.
Domain Name	Displays the domain name that the LDAP server manages.
User Name Attribute	Displays the attribute name to identify a user, such as a user ID.
Base DN	Displays the Base DN for searching for users to authenticate.
Search User's DN	Displays the DN of the user for searching.
Password	Displays asterisks (*) to mask the password of the user for searching.
Timeout	Displays the number of seconds before connection to the LDAP server times out.
Retry Interval	Displays the retry interval in seconds when the connection to the LDAP server fails.
Number of Retries	Displays the retry times when the connection to the LDAP server fails.
Secondary Host Name	Displays the host name of the secondary LDAP server.
Secondary Port Number	Displays the port number of the secondary LDAP server.
Setup Server	Displays the Setup Server window.

RADIUS Properties window

This window opens when you select RADIUS in External Authentication.

The screenshot shows the 'RADIUS Properties' window with the following configuration:

RADIUS Properties		
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	Authentication Protocol	-
	DNS Lookup	-
	Host Name	-
	Port Number	-
	Domain Name	-
	Base DN	-
	Search User's DN	-
	Password	-
	Timeout	-
Retry Interval	-	
Number of Retries	-	

Buttons: Set Up Server, Close, ?

The following table describes the fields and settings in the RADIUS properties window.

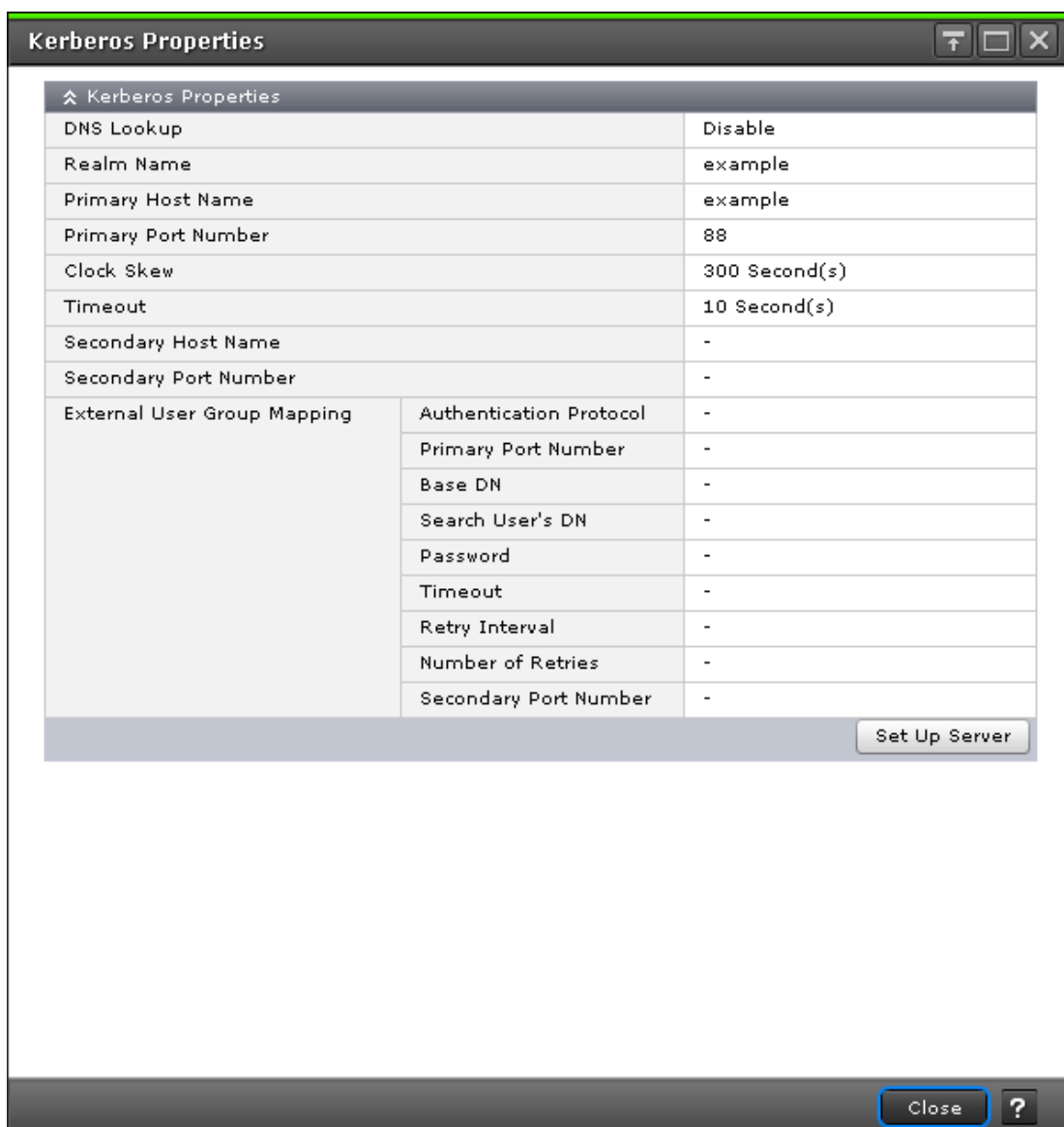
Item	Description
Authentication Protocol	Displays the RADIUS protocol to use. <ul style="list-style-type: none"> ▪ PAP: Password authentication protocol that transmits plaintext user ID and password. ▪ CHAP: Challenge-handshake authentication protocol that transmits encrypted password.
Primary Host Name	Displays the host name, the IPv4 address, or the IPv6 address of the RADIUS server.
Secret	Displays asterisks (*) to mask the RADIUS secret key used for the PAP or CHAP authentication.

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"> ▪ Enable: Performs the search using information registered in the SRV records in the DNS server. ▪ Disable: Performs the search using the host name and the port number.
External User Group Mapping - Host Name	Displays the host name, the IPv4 address, or the IPv6 address of the LDAP server.
External User Group Mapping - Port Number	Displays the port number of the LDAP server.
External User Group Mapping - Domain Name	Displays the domain name of the LDAP server.
External User Group Mapping - Base DN	Displays 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 Setup Server 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"> Enable: Performs the search using information registered in the SRV records in the DNS server. Disable: Performs the search using the host name and the port number.
Realm Name	Displays the default realm name.
Primary Host Name	Displays the name of the Kerberos server.

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 Setup Server 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"> ▪ Enable: Do not select the search using information registered in the SRV records in the DNS server. ▪ Disable: Select the search using the host name and the port number.
Authentication Protocol	<p>Specify an LDAP protocol to use. Available protocols are as follows.</p> <ul style="list-style-type: none"> ▪ Select LDAP over SSL/TLS ▪ Do not select STARTTLS <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"> ▪ Enable: Connects an authentication server to an authorization server. ▪ Disable: Does not connect an authentication server to an authorization server.
External User Group Mapping - Host Name	<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>! # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~</p> <ul style="list-style-type: none"> ▪ Hierarchical model Specify an attribute name where the value that can identify a user is stored. ▪ Flat model Specify an attribute name for a user entry's RDN. sAMAccountName is used for Active Directory.
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	<p>Search for users to authenticate by specifying a base DN. Available characters: Alphanumeric characters (ASCII characters) and all symbols.</p> <ul style="list-style-type: none"> ▪ Hierarchical model: Specify a DN of hierarchy that includes all of the targeted users for searching. ▪ Flat model: Specify a DN of hierarchy that is one level above the targeted user for searching. <p>To use symbols such as + ; , < = and > in the basedn field, type a backslash (\) before each symbol. When using multiple symbols, each symbol must have a backslash (\) before it. For example, to enter abc++, type abc\+\+.</p> <p>To use backslash (\) , forward slash (/), or quotation mark (") in the basedn field, type a backslash (\) followed by the ASCII code in hex for the symbol:</p> <ul style="list-style-type: none"> ▪ Type \5c to enter a backslash (\). ▪ Type \2f to enter a forward slash (/). ▪ Type \22 to enter a quotation mark (").
External User Group Mapping - Search User's DN	<p>Search for a user by specifying a DN. Available characters: Alphanumeric characters (ASCII characters) and all symbols.</p> <p>If you specify sAMAccountName in External User Group Mapping - User Name Attribute, or if you select Enable in External User Group Mapping, this item must be specified.</p>

Item	Description
	<p>To use symbols such as + ; , < = and > in the searchdn field, type a backslash (\) before each symbol. When using multiple symbols, each symbol must have a backslash (\) before it. For example, to enter abc++, type abc\+\+.</p> <p>To use backslash (\) , forward slash (/), or quotation mark (") in the searchdn field, type a backslash (\) followed by the ASCII code in hex for the symbol:</p> <ul style="list-style-type: none"> ▪ Type \5c to enter a backslash (\). ▪ Type \2f to enter a forward slash (/). ▪ Type \22 to enter a quotation mark (").
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>! # \$ % & ' () * + - . = @ \ ^ _ </p> <p>If you specify sAMAccountName in External User Group Mapping - User Name Attribute, or if you select Enable in External User Group Mapping, this item must be specified.</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>! # \$ % & ' () * + - . = @ \ ^ _ </p> <p>If you enter any password in External User Group Mapping - Password, you must specify this item.</p>
Secondary Server	<p>Specify whether to use a secondary LDAP server.</p> <ul style="list-style-type: none"> ▪ Enable: Uses a secondary LDAP server. ▪ Disable: Does not use a secondary LDAP server. <p>If you select Enable in DNS Lookup, this item is disabled.</p>
Secondary Server - Host Name	<p>Specify a host name of the secondary LDAP 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 LDAP server.</p> <p>If you select Disable in Secondary Server, this item is disabled.</p>

Item	Description
Test User Name	<p>Specify a user name for a server connection test.</p> <p>You can specify ASCII code characters and the following symbols:</p> <p>! # \$ % & ' * + - . / = ? @ ^ _ ` { } ~</p>
Password	<p>Specify a password of the user name for a server connection test.</p> <p>You can specify ASCII code characters and the following symbols:</p> <p>! # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~</p>
Server Configuration Test	<p>Click Check to conduct a server connection test for the authentication server and the authorization server based on the specified settings.</p>
Server Configuration Test - Result	<p>Displays a result of the server connection test for the authentication server and the authorization server.</p>

Item	Description
	<ul style="list-style-type: none"> ▪ RADIUS: Users are authenticated with user information registered in the RADIUS server. ▪ Kerberos: Users are authenticated with user information registered in the Kerberos server.

Setup Server

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"> ▪ Enable: Performs the search using information registered in the SRV records in the DNS server. ▪ Disable: Performs the search using the host name and the port number.
Authentication Protocol	Displays the LDAP protocol.
External User Group Mapping	<p>Displays whether to connect an authentication server to an authorization server.</p> <ul style="list-style-type: none"> ▪ Enable: Connects an authentication server to an authorization server. ▪ Disable: Does not connect an authentication server to an authorization server.
Primary Host Name	Displays the host name of the LDAP server.
Primary Port Number	Displays the port number of the LDAP server.
Domain Name	Displays the domain name that the LDAP server manages.
User Name Attribute	Displays the attribute name to identify a user.
Base DN	Displays the base DN for searching for users to authenticate.
Search User's DN	Displays the DN of a user for searching.
Password	Displays asterisks (*) to mask the password of the user for searching.
Timeout	Displays the number of seconds before connection to the LDAP server times out.

Item	Description
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"> ▪ PAP: Password authentication protocol that transmits plaintext user ID and password. ▪ CHAP: Challenge-handshake authentication protocol that transmits encrypted password.
Host Name	Specify a name of the RADIUS server. You can specify ASCII code characters, hyphens (-), and periods (.).

Item	Description
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: ! # \$ % & ' () * + - . = @ \ ^ _ </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: ! # \$ % & ' () * + - . = @ \ ^ _ </p>
NAS Address	<p>Specify an identifier for the RADIUS server to find SVP.</p> <ul style="list-style-type: none"> ▪ To specify a host name, select Identifier and enter the host name. You can specify ASCII code characters and the following symbols: ! " # \$ % & ' () * + , - . / ; : < > = ? @ [\] ^ _ { } ~ ▪ To specify an IPv4 address, select IPv4 and enter 4 numbers (0-255). For example: XXX.XXX.XXX.XXX (X indicates a digit) Specify only numbers. Do not specify any periods. ▪ To specify an IPv6 address, select IPv6 and enter 8 hexadecimal numbers (0-FFFF). For example: YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY (Y indicates a hexadecimal digit) Enter 0 to omit a segment.
Port Number	Specify a port number of the RADIUS server.
Timeout	Specify the number of seconds before connection to the RADIUS server times out.
Number of Retries	Specify the retry times when the connection to the RADIUS server fails.
Secondary Server	<p>Specify whether to use a secondary RADIUS server and a secondary LDAP server.</p> <ul style="list-style-type: none"> ▪ Enable: Uses secondary servers. ▪ Disable: Does not use secondary servers.

Item	Description
Secondary Server - Host Name	Specify a name of the secondary RADIUS server. You can specify ASCII code characters, hyphens (-), and periods (.). If you select Disable in Secondary Server, this item is disabled.
Secondary Server - Port Number	Specify a port number of the secondary RADIUS server. If you select Disable in Secondary Server, this item is disabled.
External User Group Mapping	Specify whether to connect an authentication server to an authorization server. <ul style="list-style-type: none"> ▪ Enable: Connects an authentication server to an authorization server. ▪ Disable: Does not connect an authentication server to an authorization server.
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.
External User Group Mapping - DNS Lookup	Specify whether to search for the LDAP server using the information registered in the SRV records in the DNS server. <ul style="list-style-type: none"> ▪ Enable: Do not select the search using information registered in the SRV records in the DNS server. ▪ Disable: Select the search using the host name and the port number. If you select Disable in External User Group Mapping, this item is disabled.
External User Group Mapping - Authentication Protocol	Specify an LDAP protocol to use. Available protocols are as follows. <ul style="list-style-type: none"> ▪ Select LDAP over SSL/TLS ▪ Do not select STARTTLS If you select Enable in DNS Lookup, you cannot select LDAP over SSL/TLS. If you select Disable in External User Group Mapping, this item is disabled.
External User Group Mapping - Host Name	Specify a host name of the LDAP server. You can specify ASCII code characters, hyphens (-), and periods (.). If you select Enable in DNS Lookup, or if you select Disable in External User Group Mapping, this item is disabled.

Item	Description
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"> ▪ Hierarchical model: Specify a DN of hierarchy that includes all the targeted users for searching. ▪ Flat model: Specify a DN of hierarchy that is one level up of the targeted user for searching. <p>If this field is blank, the value specified for the defaultNamingContext attribute of Active Directory is assumed as the base DN.</p> <p>If you select Disable in External User Group Mapping, this item is disabled.</p> <p>To use symbols such as + ; , < = and > in the basedn field, type a backslash (\) before each symbol. When using multiple symbols, each symbol must have a backslash (\) before it. For example, to enter abc++, type abc\+\+.</p> <p>To use backslash (\) , forward slash (/), or quotation mark (") in the basedn field, type a backslash (\) followed by the ASCII code in hex for the symbol:</p> <ul style="list-style-type: none"> ▪ Type \5c to enter a backslash (\). ▪ Type \2f to enter a forward slash (/). ▪ Type \22 to enter a quotation mark (").
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> <p>If you select Disable in External User Group Mapping, this item is disabled.</p>

Item	Description
	<p>To use symbols such as + ; , < = and > in the searchdn field, type a backslash (\) before each symbol. When using multiple symbols, each symbol must have a backslash (\) before it. For example, to enter <code>abc++</code>, type <code>abc\+\+</code>.</p> <p>To use backslash (\) , forward slash (/), or quotation mark (") in the searchdn field, type a backslash (\) followed by the ASCII code in hex for the symbol:</p> <ul style="list-style-type: none"> ▪ Type <code>\5c</code> to enter a backslash (\). ▪ Type <code>\2f</code> to enter a forward slash (/). ▪ Type <code>\22</code> to enter a quotation mark (").
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>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>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> <p>If you select Disable in External User Group Mapping, this item is disabled.</p>
Test User Name	<p>Specify a user name for a server connection test.</p>

Item	Description
	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.)	Nu 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"> ▪ Disable: Does not use any authentication server. Users are authenticated with user information registered in the SVP. ▪ LDAP: Users are authenticated with user information registered in the LDAP server. ▪ RADIUS: Users are authenticated with user information registered in the RADIUS server. ▪ Kerberos: Users are authenticated with user information registered in the Kerberos server.

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	<p>Displays the RADIUS protocol to use.</p> <ul style="list-style-type: none"> ▪ PAP: Password authentication protocol that transmits plaintext user ID and password. ▪ CHAP: Challenge-handshake authentication protocol that transmits encrypted password.
Primary Host Name	Displays the name of the RADIUS server.
Secret	Displays asterisks (*) to mask the RADIUS secret key used for the PAP authentication or the CHAP authentication.
NAS Address	Displays the identifier for the RADIUS server to find SVP.
Primary Port Number	Displays the port number of the RADIUS server.
Timeout	Displays the number of seconds before connection to the RADIUS server times out.
Number of Retries	Displays the retry times when the connection to the RADIUS server fails.
Secondary Host Name	Displays the name of the secondary RADIUS server.

Item	Description
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	<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"> ▪ Enable: Performs the search using information registered in the SRV records in the DNS server. ▪ Disable: Performs the search using the host name and the port number.
External User Group Mapping - Host Name	Displays the 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.

Item	Description
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.

Set Up Server

1. Select Authentication Server > **2. Set Up Server** > 3. Confirm

Enter the information to set up the authentication server (Kerberos). Click Finish to confirm.

DNS Lookup: Enable Disable

Realm Name:
(Max. 255 Characters)

Host Name:
(Max. 255 Characters)

Port Number:
(1-65535)

Clock Skew: Second(s)
(1-300)

Timeout: Second(s)
(1-120)

Secondary Server: Enable Disable

Host Name:
(Max. 255 Characters)

Port Number:
(1-65535)

External User Group Mapping: Enable Disable

Certificate File Name:

Authentication Protocol:

Primary Port Number:

Secondary Port Number:

Base DN:

The following table describes the fields and settings in the Setup Server section of Kerberos window.

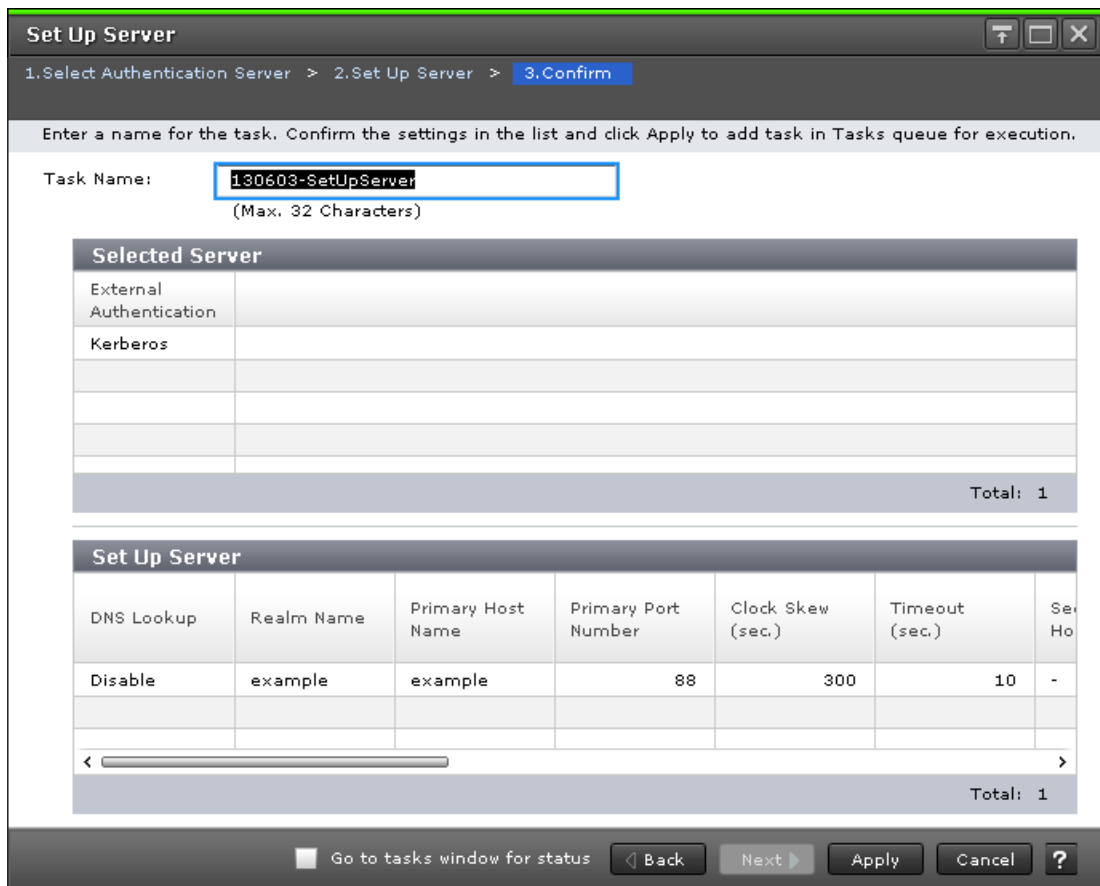
Item	Description
DNS Lookup	Specify whether to search for the Kerberos server using the information registered in the SRV records in the DNS server. <ul style="list-style-type: none"> ▪ Enable: Do not select the search using information registered in the SRV records in the DNS server. ▪ Disable: Select the search using the host name and the port number.
Realm Name	Specify a default realm name. You can specify ASCII code characters and hyphens (-).
Host Name	Specify a host name of the Kerberos server. You can specify ASCII code characters, hyphens (-), and periods (.). If you select Enable in DNS Lookup, this item is disabled.
Port Number	Specify a port number of the Kerberos server. If you select Enable in DNS Lookup, this item is disabled.
Clock Skew	Specify an acceptable range of time difference between the SVP and the Kerberos server.
Timeout	Specify the number of seconds before connection to the Kerberos server times out.
Secondary Server	Specify whether to use a secondary Kerberos server. <ul style="list-style-type: none"> ▪ Enable: Uses the secondary server. ▪ Disable: Does not use the secondary server. If you specify Enable in DNS Lookup, this item is disabled.
Secondary Server - Host Name	Specify a name of the secondary Kerberos server. You can specify ASCII code characters, hyphens (-), and periods (.). If you select Enable in DNS Lookup, or if you select Disable in Secondary Server, this item is disabled.
Secondary Server - Port Number	Specify a port number of the secondary Kerberos server. If you select Enable in DNS Lookup, or if you select Disable in Secondary Server, this item is disabled.

Item	Description
External User Group Mapping	<p>Specify whether to connect an authentication server to an authorization server.</p> <ul style="list-style-type: none"> ▪ Enable: Connects an authentication server to an authorization server. ▪ Disable: Does not connect an authentication server to an authorization server.
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 - Authentication Protocol	<p>Specify an LDAP protocol to use. Available protocols are:</p> <ul style="list-style-type: none"> ▪ Select LDAP over SSL/TLS ▪ Do not select STARTTLS <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"> ▪ Hierarchical model: Specify a DN of hierarchy that includes all the targeted users for searching. ▪ Flat model: Specify a DN of hierarchy that is one level up of the targeted user for searching. <p>If this field is blank, the value specified for the defaultNamingContext attribute of Active Directory is assumed as the base DN.</p> <p>If you select Disable in External User Group Mapping, this item is disabled.</p>

Item	Description
	<p>To use symbols such as + ; , < = and > in the basedn field, type a backslash (\) before each symbol. When using multiple symbols, each symbol must have a backslash (\) before it. For example, to enter abc++, type abc\+\+.</p> <p>To use backslash (\) , forward slash (/), or quotation mark (") in the basedn field, type a backslash (\) followed by the ASCII code in hex for the symbol:</p> <ul style="list-style-type: none"> ▪ Type \5c to enter a backslash (\). ▪ Type \2f to enter a forward slash (/). ▪ Type \22 to enter a quotation mark (").
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> <p>If you select Disable in External User Group Mapping, this item is disabled.</p> <p>To use symbols such as + ; , < = and > in the searchdn field, type a backslash (\) before each symbol. When using multiple symbols, each symbol must have a backslash (\) before it. For example, to enter abc++, type abc\+\+.</p> <p>To use backslash (\) , forward slash (/), or quotation mark (") in the searchdn field, type a backslash (\) followed by the ASCII code in hex for the symbol:</p> <ul style="list-style-type: none"> ▪ Type \5c to enter a backslash (\). ▪ Type \2f to enter a forward slash (/). ▪ Type \22 to enter a quotation mark (").
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>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>If you enter any password in External User Group Mapping - Password, you must specify this item.</p>

Item	Description
	If you select Disable in External User Group Mapping, this item is disabled.
External User Group Mapping - Timeout	Specify the number of seconds before connection to the LDAP server times out. If you select Disable in External User Group Mapping, this item is disabled.
External User Group Mapping - Retry Interval	Specify a retry interval in seconds when the connection to the LDAP server fails. If you select Disable in External User Group Mapping, this item is disabled.
External User Group Mapping - Number of Retries	Specify retry times when the connection to the LDAP server fails. If you select Disable in External User Group Mapping, this item is disabled.
Test User Name	Specify a user name for a server connection test. You can specify ASCII code characters and the following symbols: ! # \$ % & ' * + - . / = ? @ ^ _ ` { } ~
Password	Specify a password of the user name for a server connection test. You can specify ASCII code characters and the following symbols: ! # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~
Server Configuration Test	Click Check to conduct a server connection test for the authentication server and the authorization server based on the specified settings.
Server Configuration Test - Result	Displays a result of the server connection test for the authentication server and the authorization server.

Kerberos Setup Server confirmation window



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"> ▪ Disable: Does not use any authentication server. Users are authenticated with user information registered in the SVP. ▪ LDAP: Users are authenticated with user information registered in the LDAP server. ▪ RADIUS: Users are authenticated with user information registered in the RADIUS server. ▪ Kerberos: Users are authenticated with user information registered in the Kerberos server.

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"> ▪ Enable: Performs the search using information registered in the SRV records in the DNS server. ▪ Disable: Performs the search using the host name and the port number.
Realm Name	Displays the default realm name.
Primary Host Name	Displays the name of the Kerberos server.
Primary Port Number	Displays the port number of the Kerberos server.
Clock Skew	Displays the acceptable range of time difference between the SVP and the Kerberos server.
Timeout	Displays the number of seconds before connection to the Kerberos server times out.
Secondary Host Name	Displays the name of the secondary Kerberos server.
Secondary Port Number	Displays the port number of the secondary Kerberos server.
External User Group Mapping - 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.
External User Group Mapping - Search User's DN	Displays the search user's domain name.

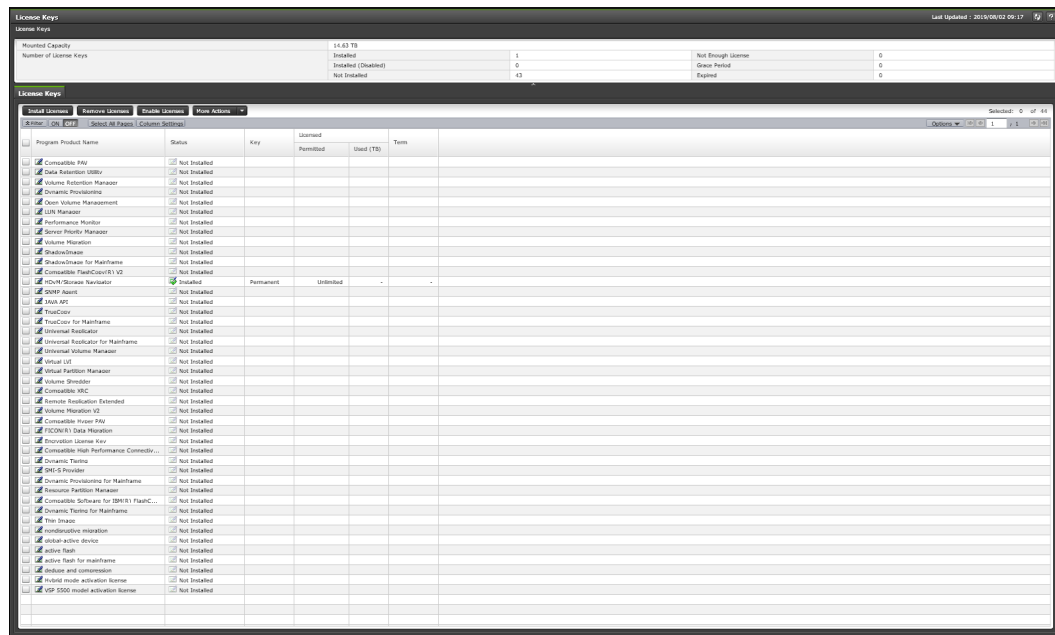
Item	Description
External User Group Mapping - Password	Displays asterisks (*) to mask the password of the user for searching.
External User Group Mapping - Timeout	Displays the number of seconds before connection to the LDAP server times out.
External User Group Mapping - Retry Interval	Displays the 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 C: 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.
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"> ▪ Installed: The software is available. ▪ Installed (Disabled): Installation is complete, but the license is set to Disabled. This status might appear if an error occurs after you install software. Resolve the error and enable the license. This status also appears when the license key of this software is installed but the license key of the prerequisite software has expired. ▪ Not Installed: The software is not installed. ▪ Not Enough License: Installation is complete, but the license capacity is insufficient. Not Enough License might remain displayed when the licensed capacity exceeds the mounted capacity after you reduce the number of LDEVs, or when the licensed capacity exceeds the used capacity after you delete pairs or pool volumes. In these cases, you can update the license status by selecting Update License Status and then installing the software.

Item	Description
	<ul style="list-style-type: none"> ▪ 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. ▪ Expired: The term has already expired for the temporary key. When the status is Expired, you cannot re-install the temporary key.
Key Type	<p>The license key type:</p> <ul style="list-style-type: none"> ▪ permanent ▪ term ▪ temporary ▪ emergency <p>This field is blank if no license key is installed.</p>
Licensed Capacity	<ul style="list-style-type: none"> ▪ 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. ▪ 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. <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	<p>Opens the Install Licenses window</p>

Item	Description
Uninstall Licenses	Opens the Uninstall Licenses window
Enable	Opens the Enable Licenses window
Disable*	Opens the Disable Licenses window
Update License Status*	Opens the Update License Status 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

Install Licenses

1. Install Licenses > 2. Confirm

This wizard lets you install licenses. Enter the key code, or select the file, and then click Add. Click Finish to confirm.

License Key:

Key Code:

File:

Selected License Keys

Select All Pages

	Program Product Name	Status	Key Type	Licensed Capacity		Term (days)
				Permitted (TB)	Used (TB)	
No Data						

Selected: 0 of 0

Item	Description
License Key	Select whether to enter a key code or specify a license key file. <ul style="list-style-type: none"> ▪ Key Code: Enter a key code to install the software. Use the license key code for the software to be installed. ▪ File: Specify a license key file to install software. Click Browse and specify the license key file.
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	The current status of the software <ul style="list-style-type: none"> ▪ Installed: The software is available. ▪ Installed (Disabled): Installation is complete, but the license is set to Disabled. This status might appear if an error occurs after you install software. Resolve the error and enable the license. This status also appears when the license key of this software is installed but the license key of the prerequisite software has expired. ▪ Not Installed: The software is not installed. ▪ Not Enough License: Installation is complete, but the license capacity is insufficient. Not Enough License might remain displayed when the licensed capacity exceeds the mounted capacity after you reduce the number of LDEVs, or when the licensed capacity exceeds the used capacity after you delete pairs or pool volumes. In these cases, you can update the license status by selecting Update License Status and then installing the software.

Item	Description
	<ul style="list-style-type: none"> ▪ 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. ▪ Expired: The term has already expired for the temporary key. When the status is Expired, you cannot re-install the temporary key.
Key Type	<p>The license key type:</p> <ul style="list-style-type: none"> ▪ permanent ▪ term ▪ temporary ▪ emergency <p>This field is blank if no license key is installed.</p>
Licensed Capacity	<ul style="list-style-type: none"> ▪ 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. ▪ 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. <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	<p>Installs license keys in Enabled status. You can select more than one software product.</p>

Item	Description
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 ?

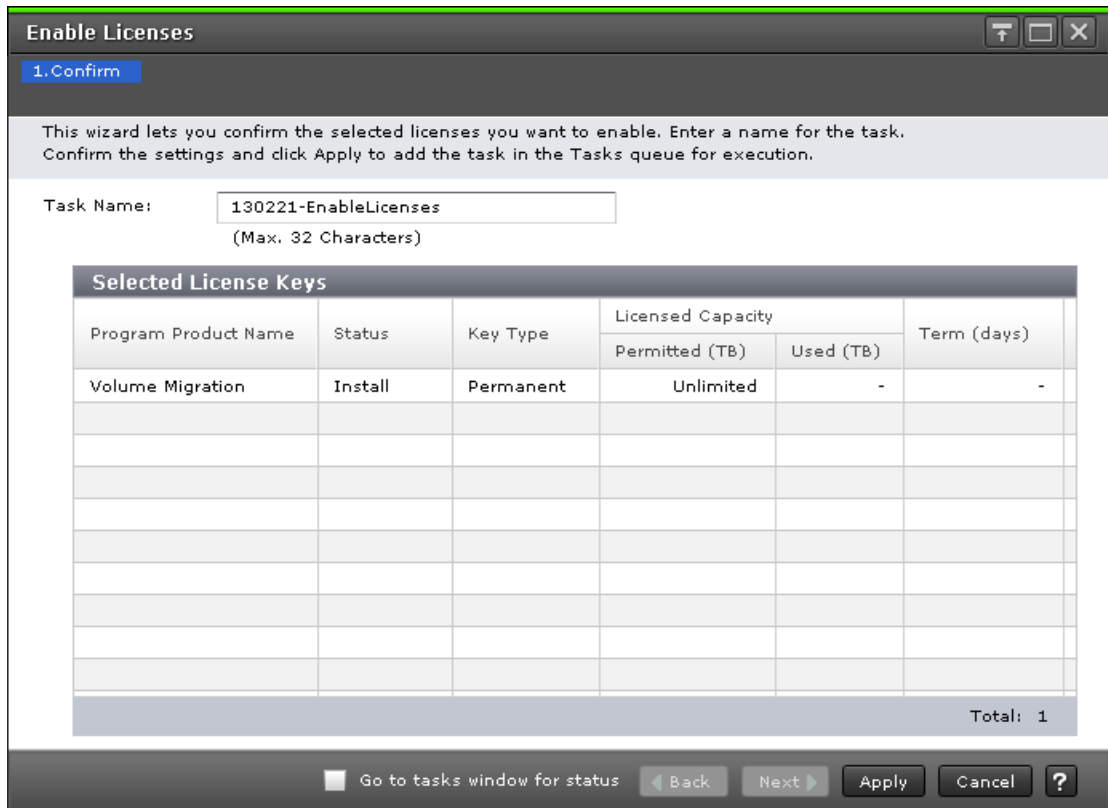
This topic describes the Install Licenses confirmation window.

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 Install Licenses window (on page 439) .

Item	Description
Key Type	<p>The license key type:</p> <ul style="list-style-type: none"> ▪ permanent ▪ term ▪ temporary ▪ emergency <p>This field is blank if no license key is installed.</p>
Licensed Capacity	<ul style="list-style-type: none"> ▪ 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. ▪ 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. <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.



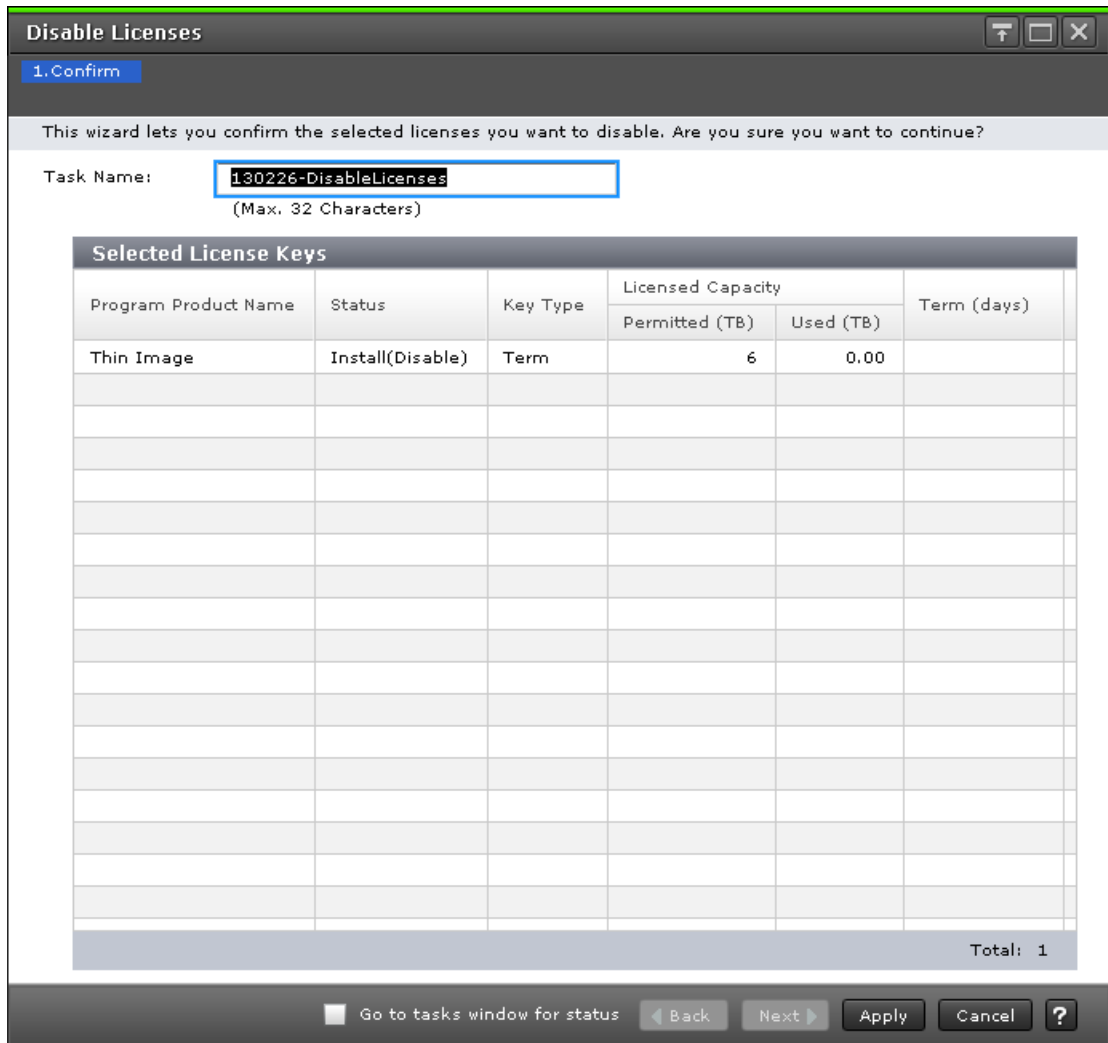
The following table describes the fields and settings in the **Enable Licenses** window.

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 Install Licenses window (on page 439) .
Key Type	<p>The license key type:</p> <ul style="list-style-type: none"> ▪ Permanent ▪ Term ▪ Temporary ▪ Emergency <p>This field is blank if no license key is installed.</p>

Item	Description
Licensed Capacity (TB)	<ul style="list-style-type: none"> ▪ 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. ▪ 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. <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 Install Licenses window (on page 439) .
Key Type	<p>The license key type:</p> <ul style="list-style-type: none"> ▪ Permanent ▪ Term ▪ Temporary ▪ Emergency <p>This field is blank if no license key is installed.</p>

Item	Description
Licensed Capacity (TB)	<ul style="list-style-type: none"> ▪ 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. ▪ 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. <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"> ▪ 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. ▪ 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. <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 the If there is no limit on validity, a hyphen (-) displays. This field is blank if no license is installed.</p>

Update License Status window

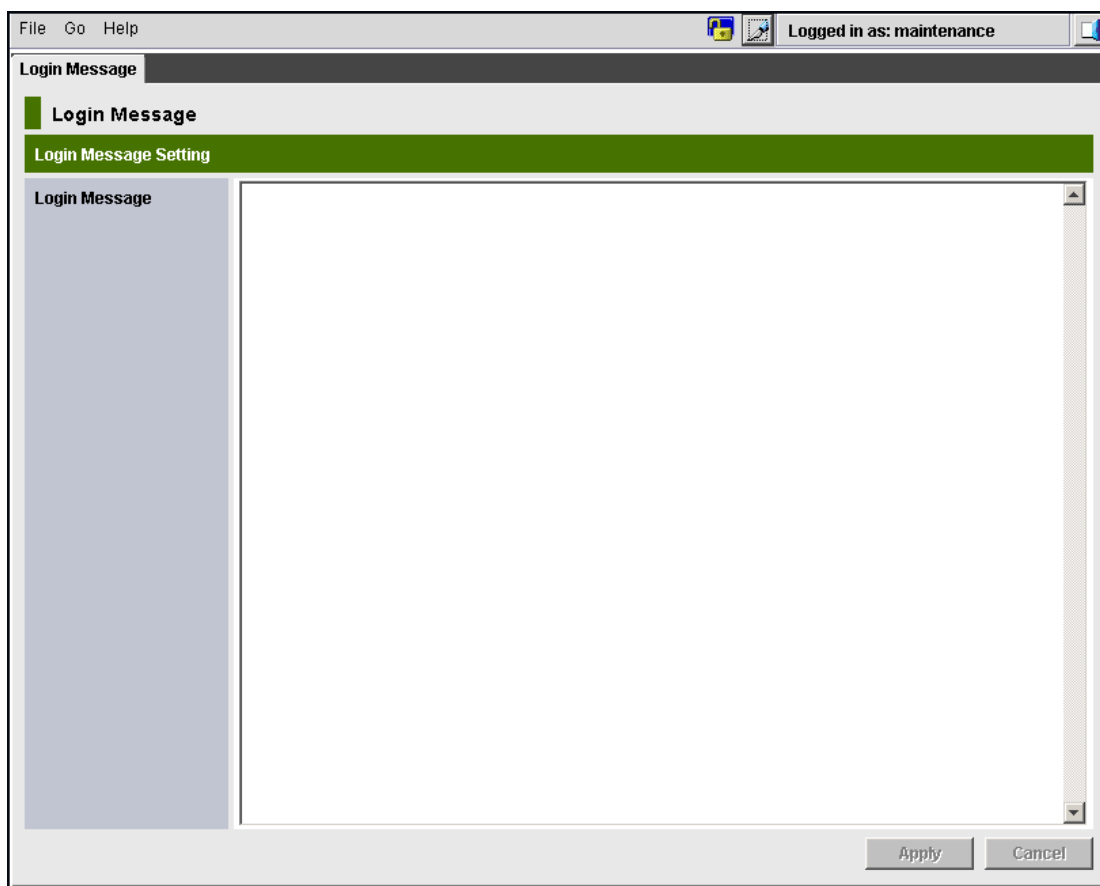
This topic describes the **Update License Status** window.

Item	Description
Licensed Capacity	<ul style="list-style-type: none"> ▪ 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. ▪ 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. <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 D: 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 Storage System confirmation window

The following table describes the fields and settings in the Confirm window (Edit Storage System).

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 wizard

This section describes the **Edit Alert Settings** wizard.

Edit Alert Settings window


Item	Description
Notification Alert	<p>Select the destination of the alert notification.</p> <ul style="list-style-type: none"> All: Sends alerts of all SIMs. Host Report: Sends alerts only of SIMs that report to hosts. <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' sub-tab, the 'Transfer Protocol' is set to 'New Syslog Protocol (TLS1.2/RFC5424)'. The 'Primary Server' is enabled, with 'Identifier' set to '127.0.0.1' and 'Port Number' set to '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.

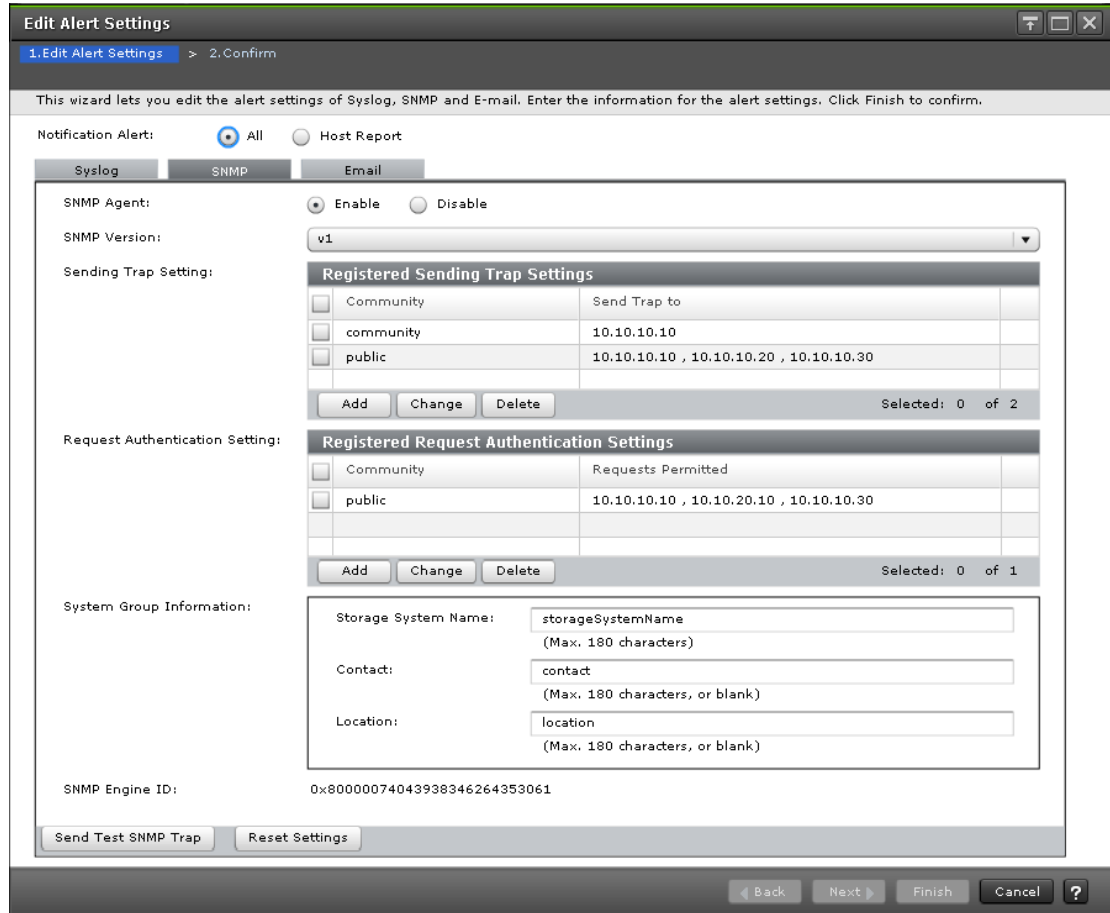
The following table describes the fields and settings in the Syslog tab.

Item	Description
Transfer Protocol	<p>Select the protocol for Syslog transfer.</p> <ul style="list-style-type: none"> New Syslog Protocol (TLS1.2/RFC5424) Old Syslog Protocol (UDP/RFC3164)

Item	Description
Primary Server	<p>Select whether or not to use the Syslog Server.</p> <ul style="list-style-type: none"> ▪ Enable: Reports SIM to the Syslog Server through Syslog. ▪ Does not report SIM to the Syslog Server through Syslog.
Primary Server - Server Setting	<p>Enter the IPv4 or IPv6 address, or the host name of the server that you want to set as the Syslog Server. You cannot set an address with all 0s.</p> <p>To specify a host name, select Identifier, and then enter a host name with no more than 255 characters by using alphanumeric characters and symbols: ! \$ % - . @ _ ` ~.</p> <p>Use this field only when you select Enable in Primary Server.</p> <div style="background-color: #e0f2f1; padding: 5px; border: 1px solid #ccc;"> <p> Note: If SIMs are not transferred to the Syslog server, verify the settings in the Syslog tab. If all settings are correct, verify the settings and operating conditions of the Syslog Server itself, and the operating conditions of the Management LAN.</p> </div>
Primary Server - Port Number	<p>Enter the port number used by the Syslog Server. Use this field only when you selected Enable in Primary Server.</p>
Primary Server - Client Certificate File Name	<p>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.</p>
Primary Server - Password	<p>Enter a password for the client certificate. You can enter up to 128 alphanumeric characters and the following symbols:</p> <p>! # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~</p> <p>Use this field only when you specified Client Certificate File Name.</p>
Primary Server - Root Certificate File Name	<p>Specify a certificate file. Click Browse and specify the certificate file.</p> <p>Use this field only when you select New Syslog Protocol (TLS1.2/RFC5424) in Transfer Protocol and selected Enable in Primary Server.</p>
Secondary Server	<p>Select whether or not to use an alternate server for the Syslog Server.</p> <ul style="list-style-type: none"> ▪ Enable: Reports SIM to the alternate server for the Syslog Server through Syslog. ▪ Disable: Does not report SIM to the alternate server for the Syslog Server through Syslog.
Secondary Server - Server Setting	<p>Enter the IPv4 or IPv6 address, or the host name of the server that you want to set as the alternate server for the Syslog Server. You cannot set an address with all 0s.</p> <p>To specify a host name, select Identifier, and then enter a host name with no more than 255 characters by using alphanumeric characters and symbols: ! \$ % - . @ _ ` ~.</p>

Item	Description
	Use this field only when you select Enable in Secondary Server.
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	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 specify Client Certificate File Name.
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	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: ! # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~ Spaces are not allowed.
Timeout	Enter a value as the time before the timeout for connection to the Syslog Server is detected. The default is 10. Use this field only when you selected New Syslog Protocol (TLS1.2/RFC5424) in Transfer Protocol.
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.
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. Verify that the log Detailed data: "RefCode: 7FFFFFFF, This is Test Report." has been transferred to the Syslog server.
Reset settings	Cancels the changes within the tab

SNMP tab (when the SNMP protocol version is SNMP v1 or SNMP v2c)



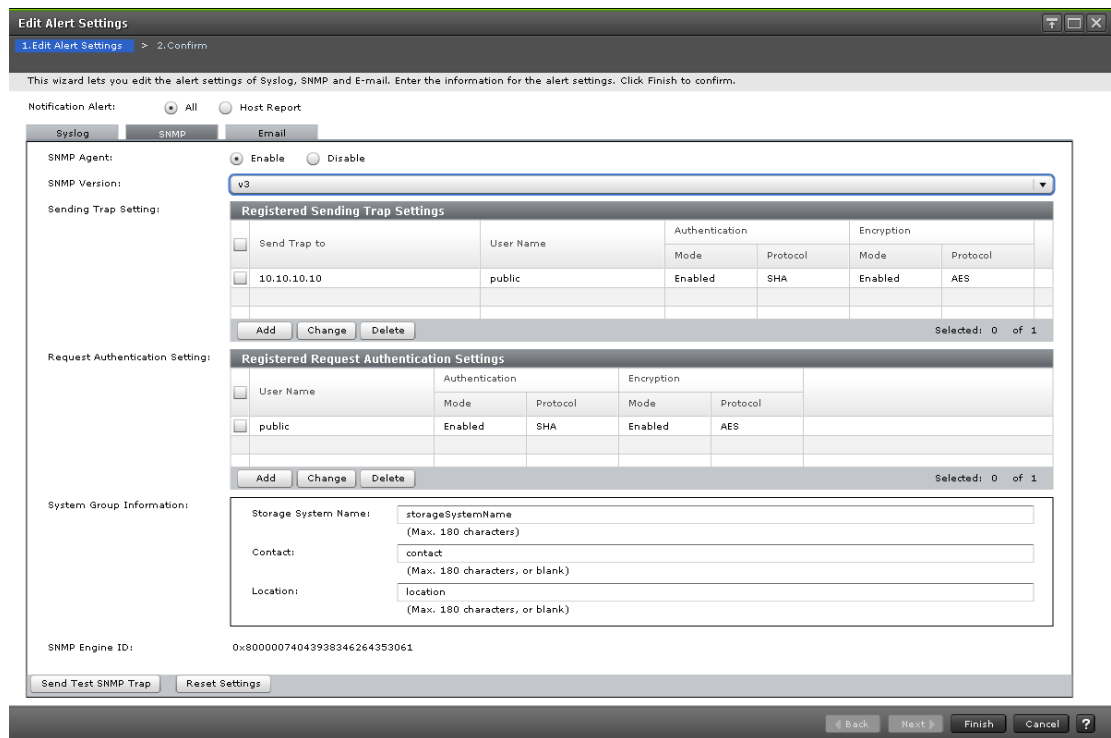
The following table describes the fields and settings in the SNMP tab when the SNMP protocol version is v1 or v2c.

Item	Description
SNMP Agent	Select whether to use the SNMP agent. <ul style="list-style-type: none"> ▪ Enable: Reports SIM through SNMP trap that permits GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST* ▪ Disable: Does not report SIM through SNMP or permit GET REQUEST, GETNEXT REQUEST, or GETBULK REQUEST*
SNMP Version	Select the SNMP protocol version.

Item	Description
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"> ▪ Community: Displays the community for which SNMP trap information is reported. ▪ Send Trap to: Displays the IP address to which SNMP trap information is reported ▪ Add: Opens the Add Sending Trap Setting window. You can register up to 32 communities. ▪ Change: To change a community, select it, and then click this button to open the Change Sending Trap Setting window. ▪ Delete: To delete a community, select it, and then click this button.
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"> ▪ Community: Displays the community names that permit GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST* ▪ Requests Permitted: Displays the IP addresses that permit GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST* ▪ Add: The Add Request Authentication Setting window opens. You can register up to 32 communities. ▪ Change: To change a community, select it, and then click this button. ▪ Delete: To delete a community, select it, and then click this button
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>Note: Do not include space characters at the beginning or end.</p> <p>Caution: 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: \ , / ; : * ? " < > & % ^</p> <p>Note: 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: \ , / ; : * ? " < > & % ^</p> <p>Note: Do not include space characters at the beginning or end.</p>

Item	Description
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. Note: 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)



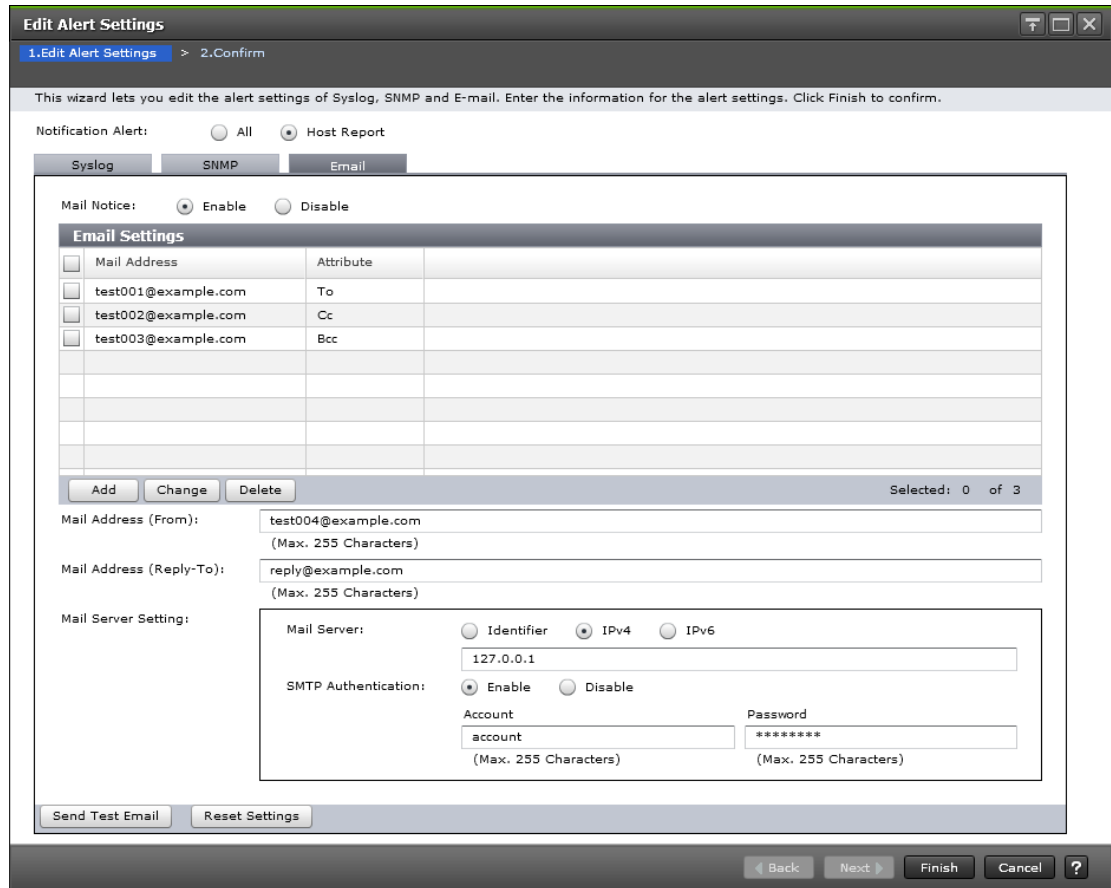
The following table describes the fields and settings in the SNMP tab when the SNMP protocol version is v3.

Item	Description
SNMP Agent	<p>Select whether to use the SNMP agent.</p> <ul style="list-style-type: none"> ▪ Enable: Reports SIM through SNMP trap that permits GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST ▪ Disable: Does not report SIM through SNMP or permit GET REQUEST, GETNEXT REQUEST, or GETBULK REQUEST
SNMP Version	Select the SNMP protocol version.
Sending Trap Setting	<p>Displays, in the Registered Sending Trap Settings table, the community names and IP addresses for which SNMP trap information is reported.</p> <ul style="list-style-type: none"> ▪ Send Trap to: Displays the IP address to which SNMP trap information is reported ▪ User Name: Displays the user used for reporting SNMP trap information ▪ Authentication - Mode: Displays whether authentication is enabled ▪ Authentication - Protocol: If authentication is enabled, the authentication method is displayed ▪ Encryption - Mode: Displays whether encryption is enabled ▪ Encryption - Protocol: If encryption is enabled, the encryption method is displayed ▪ Add: Opens the Add Sending Trap Setting window. You can register up to eight IP addresses. ▪ Change: To change a destination, select it, and then click this button to open the Change Sending Trap Setting window. ▪ Delete: To delete a destination, select it, and then click this button.


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"> ▪ User Name: Displays the user names that permit GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST ▪ Authentication - Mode: Displays whether authentication is enabled ▪ Authentication - Protocol: If authentication is enabled, the authentication method is displayed ▪ Encryption - Mode: Displays whether encryption is enabled ▪ Encryption - Protocol: If encryption is enabled, the encryption method is displayed ▪ Add: Opens the Add Request Authentication Setting window. You can register up to 8 users. ▪ Change: To change a user, select it, and then click this button to open the Change Request Authentication Setting window. ▪ Delete: To delete a user, select it, and then click this button.
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>Note: Do not include space characters at the beginning or end.</p> <p>Caution: 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: \ , / ; : * ? " < > & % ^</p> <p>Note: 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: \ , / ; : * ? " < > & % ^</p> <p>Note: Do not include space characters at the beginning or end.</p>
SNMP Engine ID	Displays the SNMP engine identifier.
Send Test SNMP Trap	<p>Reports test trap to IP addresses that are already registered in the storage system.</p> <p>Note: 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.</p>

Item	Description
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"> ▪ Enable: Reports SIM through email. ▪ Disable: Does not report SIM through email.
Email Settings	This field is mandatory when you selected Enable in Mail Notice. <ul style="list-style-type: none"> ▪ Mail Address: The email address displays. ▪ Attribute: Adds email addresses. The Add Address window opens. ▪ Add: Adds email addresses. The Add Address window opens

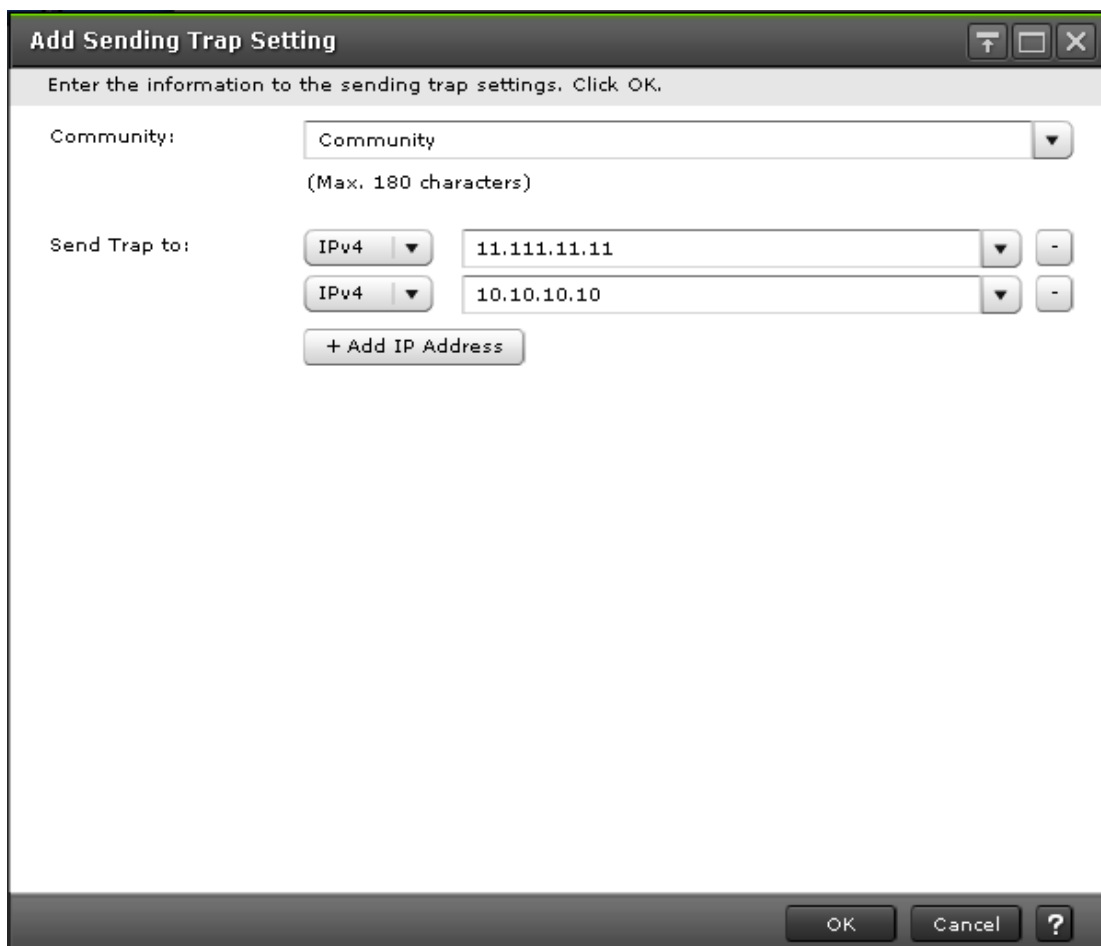
Item	Description
	<ul style="list-style-type: none"> ▪ Change: Changes the selected email address and attribute. The opens. You can select more than one email address. When you select more than one email address, you can change only attributes. ▪ Delete: Deletes the selected email address. You can select more than one email address.
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>! # \$ % & ` + - * / ' ^ { } _ . = ? @ ~</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>! # \$ % & ` + - * / ' ^ { } _ . = ? @ ~</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"> ▪ Identifier: To specify a host name, select Identifier. You can enter a name of up to 63 characters and the following symbols: ! \$ % () ' - _ . @ ~ ▪ IPv4: Enter a valid IPv4 address in the format XXX.XXX.XXX.XXX (where XXX is a number from 0 to 255) ▪ IPv6: Enter a valid IPv6 address in the format YYYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY: (where YYYYY is a hexadecimal number from 0 to FFFF). You can also use an IPv6 address in abbreviated format. <p>This field is mandatory when you select Enable in Mail Notice.</p> <div style="background-color: #e0f2f1; padding: 5px; border: 1px solid #ccc;"> <p> Note: If SIMs are not transferred through email, verify the settings in the Email tab. If all settings are correct, verify the settings and operating conditions of the mail server itself, and the operating conditions of the Management LAN.</p> </div>
Mail Server Setting - SMTP Authentication	<p>Select whether or not to perform SMTP authentication.</p> <ul style="list-style-type: none"> ▪ Enable: Performs SMTP authentication. ▪ Disable: Does not perform SMTP authentication. <p>When you select Enable, enter values in Account and Password.</p>

Item	Description
	You can enter up to 255 alphanumeric characters and the following symbols: ! \$ % () ' - _ . @ ~ 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	<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>\, / ; : * ? " < > & % ^ ' </p> <p>Note: 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"> ▪ IPv4: Enter a valid IPv4 address in the format XXX.XXX.XXX.XXX (where XXX is a number from 0 to 255) ▪ IPv6: Enter a valid IPv6 address in the format YYYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY: (where YYYYY is a hexadecimal number from 0 to FFFF). You can also use an IPv6 address in abbreviated format. ▪ Minus symbol: Removes the IP address in that row. ▪ Add IP Address: Adds an IP address. You can add up to 32 IP addresses.

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	<p>Specify the IP address to which SNMP traps are reported.</p> <ul style="list-style-type: none"> IPv4: Enter a valid IPv4 address in the format XXX.XXX.XXX.XXX (where XXX is a number from 0 to 255) IPv6: Enter a valid IPv6 address in the format YYYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY: (where YYYYY is a hexadecimal number from 0 to FFFF). You can also use an IPv6 address in abbreviated format.
User Name	<p>Enter the user name to be used for reporting SNMP traps.</p> <p>You can enter up to 32 alphanumeric characters, excluding the following symbols: \, / ; : * ? " < > & % ^</p> <p>Note: 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"> Enable: Authentication is performed. Disable: Authentication is not performed.

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"> ▪ SHA ▪ MD5
Authentication - Password	If authentication is enabled, enter a password. The password must be 8 to 180 alphanumeric characters, including the following symbols: \ , / ; : * ? " < > & % ^ Note: Do not include space characters at the beginning or end.
Encryption	Select whether to perform encryption. <ul style="list-style-type: none"> ▪ Enable: Encryption is performed. ▪ Disable: Encryption is not performed. 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"> ▪ AES ▪ DES
Encryption - Key	If encryption is enabled, enter a key. The key must be 8 to 180 alphanumeric characters, including the following symbols: \ , / ; : * ? " < > & % ^ Note: 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>\, / ; : * ? " < > & % ^</p> <p>Note: Do not include space characters at the beginning or end.</p>
Send Trap to	Specify the IP address to which SNMP traps are reported.

Item	Description
	<p>Select an existing IP address from the pull down menu or enter a new address.</p> <ul style="list-style-type: none"> ▪ IPv4: Enter a valid IPv4 address in the format XXX.XXX.XXX.XXX (where XXX is a number from 0 to 255) ▪ IPv6: Enter a valid IPv6 address in the format YYYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY: (where YYYYY is a hexadecimal number from 0 to FFFF). You can also use an IPv6 address in abbreviated format. ▪ Minus symbol: Removes the IP address in that row. ▪ Add IP Address: Adds an IP address. You can add up to 32 IP addresses.

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.

Change Sending Trap Setting

Check the box in front of the property you want to edit, and then enter the new value. Click OK.

Send Trap to: IPv4 10.10.10.10

User Name: public
(Max. 32 Characters)

Authentication: Enable Disable

Protocol: SHA

Password: *****
(8-180 characters)

Encryption: Enable Disable

Protocol: AES

Key: *****
(8-180 characters)

Re-enter Key: *****

OK Cancel ?

Item	Description
Send Trap to	<p>Specify the IP address to which SNMP traps are reported.</p> <ul style="list-style-type: none"> ▪ IPv4: Enter a valid IPv4 address in the format XXX.XXX.XXX.XXX (where XXX is a number from 0 to 255) ▪ IPv6: Enter a valid IPv6 address in the format YYYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY: (where YYYYY is a hexadecimal number from 0 to FFFF). You can also use an IPv6 address in abbreviated format.
User Name	<p>Enter the user name to be used for reporting SNMP traps.</p> <p>You can enter up to 32 alphanumeric characters, excluding the following symbols: \ , / ; : * ? " < > & % ^</p> <p>Note: 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"> ▪ Enable: Authentication is performed. ▪ Disable: Authentication is not performed. <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"> ▪ SHA ▪ MD5
Authentication - Password	<p>If authentication is enabled, enter a password. The password must be 8 to 180 alphanumeric characters, including the following symbols: \ , / ; : * ? " < > & % ^</p> <p>Note: Do not include space characters at the beginning or end.</p>
Encryption	<p>Select whether to perform the encryption</p> <ul style="list-style-type: none"> ▪ Enable: Encryption is performed. ▪ Disable: Encryption is not performed. <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"> ▪ AES ▪ DES

Item	Description
Encryption - Key	<p>If encryption is enabled, enter a key. The key must be at least 8 alphanumeric characters, including the following symbols:</p> <p>\ , / ; : * ? " < > & % ^</p> <p>Note: Do not include space characters at the beginning or end.</p>
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.

Add Request Authentication Setting

Enter the information to the request authentication settings. Click OK.

Community: (Max. 180 characters)

Requests Permitted: All

IPv4 -

IPv4 -

+ Add IP Address

OK Cancel ?

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>\, / ; : * ? " < > & % ^ ' </p> <p>Note: Do not include space characters at the beginning or end.</p>
Requests permitted	<p>Specify which users have permission to execute GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST*.</p> <ul style="list-style-type: none"> ▪ All: Accepts GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST from all users. <p>If All is selected, the IP address information is not displayed.</p> <ul style="list-style-type: none"> ▪ Specific IP addresses: <ul style="list-style-type: none"> • Select an existing IP address from the pull down menu or enter a new address. • IPv4: Enter a valid IPv4 address in the format XXX.XXX.XXX.XXX (where XXX is a number from 0 to 255) • IPv6: Enter a valid IPv6 address in the format YYYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY: (where YYYYY is a hexadecimal number from 0 to FFFF). You can also use an IPv6 address in abbreviated format. • Minus symbol: Removes the IP address in that row. • Add IP Address: Adds an IP address. You can add up to 32 IP addresses.
* 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.

Add Request Authentication Setting [Maximize] [Close]

Enter the information to the request authentication settings. 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>Note: 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"> ▪ Enable: Authentication is performed. ▪ Disable: Authentication is not performed. <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"> ▪ SHA ▪ MD5

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:</p> <p>\, / ; : * ? " < > & % ^</p> <p>Note: Do not include space characters at the beginning or end.</p>
Authentication - Re-enter Password	<p>Re-enter the same password.</p>
Encryption	<p>Select whether to perform the encryption</p> <ul style="list-style-type: none"> ▪ Enable: Encryption is performed. ▪ Disable: Encryption is not performed. <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"> ▪ AES ▪ DES
Encryption - Key	<p>If encryption is enabled, enter a key. The key must be 8 to 180 alphanumeric characters excluding the following symbols:</p> <p>\, / ; : * ? " < > & % ^</p> <p>Note: Do not include space characters at the beginning or end.</p>
Encryption - Re-enter Key	<p>Re-enter the same key.</p>

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>\, / ; : * ? " < > & % ^ ' </p> <p>Note: 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"> ▪ All: Accepts GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST from all users. If All is selected, the IP address information is not displayed. ▪ Specific IP addresses: <ul style="list-style-type: none"> • Select an existing IP address from the pull down menu or enter a new address. • IPv4: Enter a valid IPv4 address in the format XXX.XXX.XXX.XXX (where XXX is a number from 0 to 255) • IPv6: Enter a valid IPv6 address in the format YYYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY: (where YYYYY is a hexadecimal number from 0 to FFFF). You can also use an IPv6 address in abbreviated format. • Minus symbol: Removes the IP address in that row. • Add IP Address: Adds an IP address. You can add up to 32 IP addresses.
* 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.

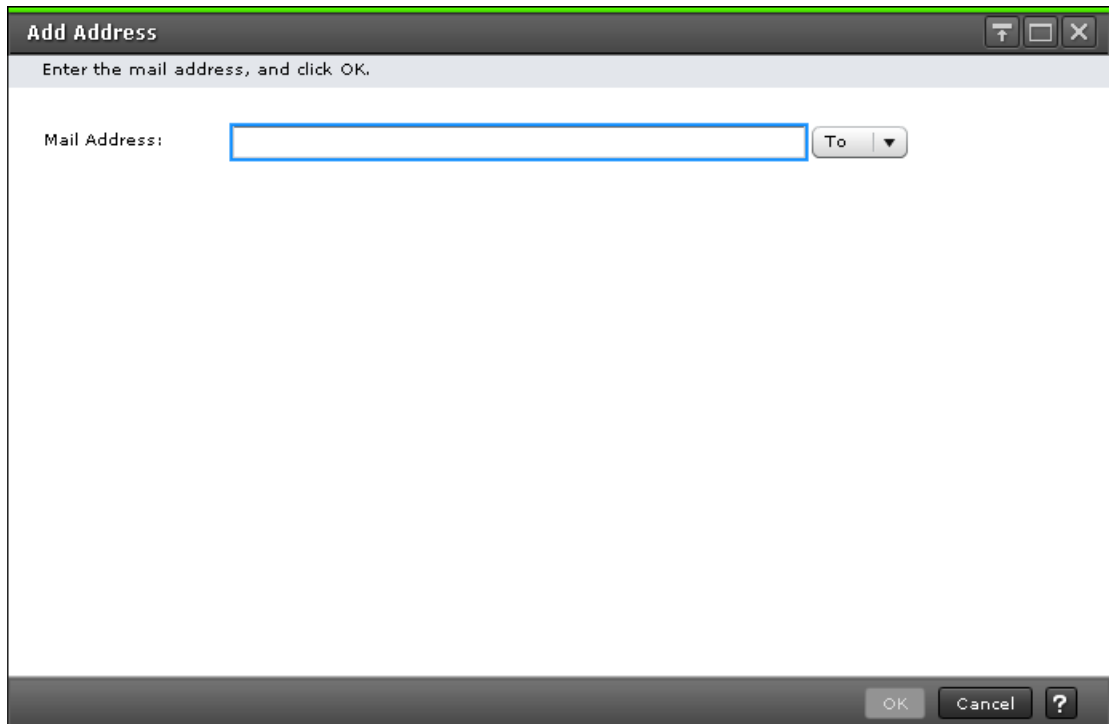
This window appears when you click Change on the SNMP tab of the **Set Up Alert Notifications** window if the SNMP protocol version is SNMP v3.

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>Note: 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"> ▪ Enable: Authentication is performed. ▪ Disable: Authentication is not performed. <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"> ▪ SHA ▪ MD5

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:</p> <p>\ , / ; : * ? " < > & % ^</p> <p>Note: 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"> ▪ Enable: Encryption is performed. ▪ Disable: Encryption is not performed. <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"> ▪ AES ▪ DES
Encryption - Key	<p>If encryption is enabled, enter a key. The key must be 8 to 180 alphanumeric characters excluding the following symbols:</p> <p>\ , / ; : * ? " < > & % ^</p> <p>Note: 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.

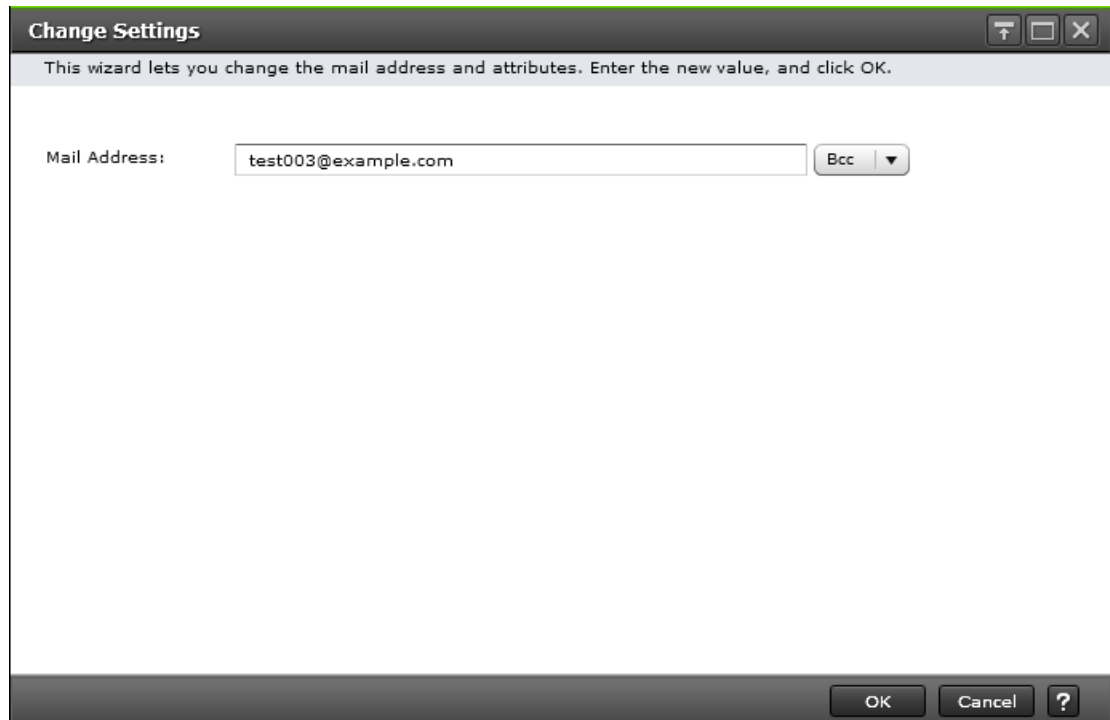


The following table describes the fields and settings in the **Add Address** window.

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: ! # \$ % & ` + - * / ' ^ { } _ = ? @ ~.</p>

Edit Alert 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	Manage differential bitmaps i...	Disabled
6	Manage differential bitmaps i...	Disabled
7	External Authentication Comp...	Disabled
8	Enable reboot of background ...	Disabled
9	Notify an alert when tier reloc...	Disabled
10	Reserve0010	Disabled
11	Reserve0011	Disabled
12	Reserve0012	Disabled
13	The consistency time of a Uni...	Disabled
14	After delta resync, the pair st...	Disabled
15	One minute after remote pat...	Disabled
16	After remote path failure dete...	Disabled
17	The copy pace for mirror opti...	Disabled
18	The copy pace for mirror opti...	Disabled

Total: 1024

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



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 - Host Name/IP Address	Displays the host name or 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
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 - Host Name/IP Address	Displays the host name or 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
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)

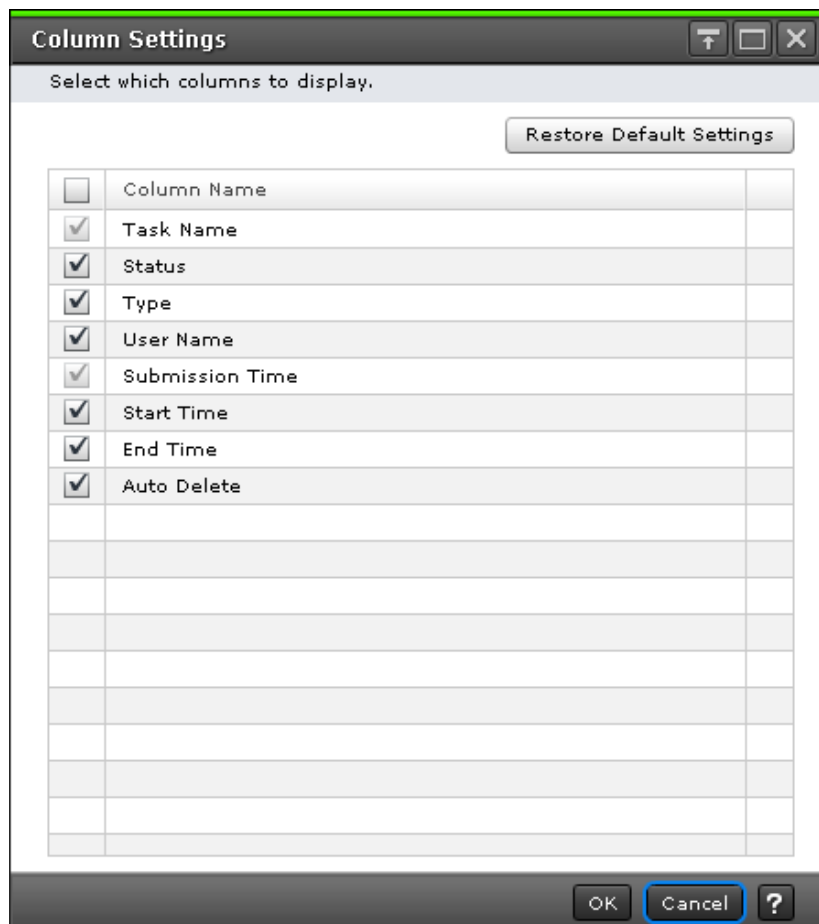
Item	Description
Mail Notice	Displays whether or not to use email to notify users of failure information
Mail Address (From)	Displays the source email address for notification of failure information.
Mail Address (Reply - To)	Displays the email return address
Server Host Name	Displays the email server 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



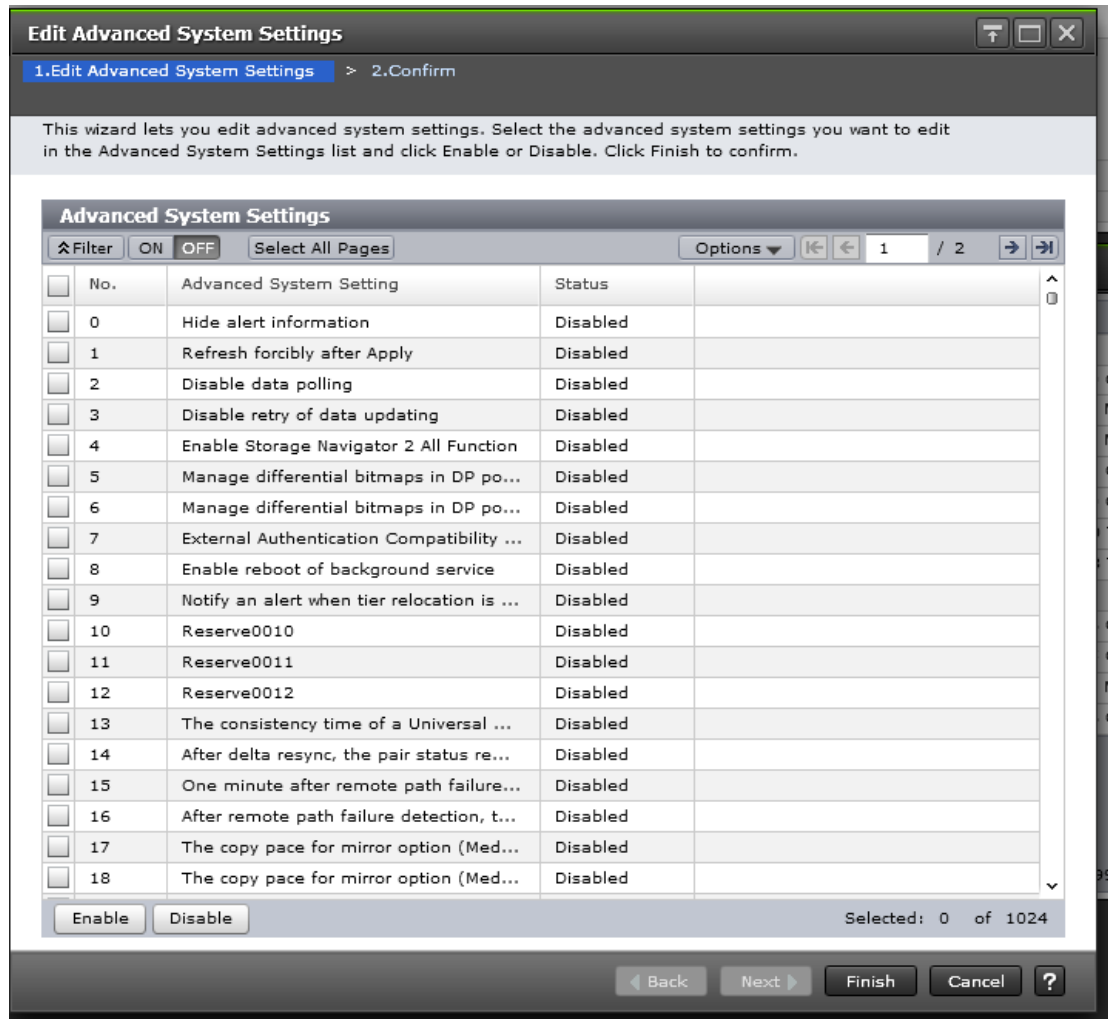
Item	Description
Restore Default Settings	Changes the selection of the displayed columns to the factory default settings.
Checkbox	<p>Selects the columns to display.</p> <p>Click the checkbox next to the name of each column that you want to display. After making the selections, click OK. Only the columns 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 \(on page 488\)](#)
- [Edit Advanced System Settings confirmation window \(on page 493\)](#)
- [Column Settings window \(on page 486\)](#)


Edit Advanced System Settings window



Item	Description
No.	Number of function bits for the advanced system setting
Advanced System Setting	Name of the advanced system setting <ul style="list-style-type: none"> ▪ Hide alert information: The Alert window is not displayed. ▪ Refresh forcibly after Apply: The configuration information for the storage system is forcibly updated after the configuration changes are applied to the storage system. ▪ Disable data polling: Polling stops. ▪ Disable retry of data updating: Retry does not take place even when you fail to acquire data.

Item	Description
	<ul style="list-style-type: none"> <li data-bbox="630 258 1424 422">▪ Enable Storage Navigator 2 All Function : 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. <li data-bbox="630 443 1424 747">▪ Manage differential bitmaps in DP pool at pair create and resync operations for 4TB or less TC/TCMF/UR/URMF/GAD pairs: Differential data is maintained in a pool with which a DP-VOL that has the user capacity (up to 4,194,304 MB) is linked when a new TC/TCMF/UR/URMF/GAD pair is created or resynchronized using the DP-VOL. Note that differential data is maintained, regardless of this setting, in a pool linked with the DP-VOL that has the user capacity (greater than 4,194,304 MB) when a new pair using the DP-VOL is created. <li data-bbox="630 768 1424 1041">▪ Manage differential bitmaps in DP pool at pair create operations for 4TB or less TC/TCMF/UR/URMF/GAD pairs: Differential data is maintained in a pool with which a DP-VOL that has the user capacity (up to 4,194,304 MB) is linked when a new pair is created using the DP-VOL. Note that differential data is maintained, regardless of this setting, in a pool linked with the DP-VOL that has the user capacity (greater than 4,194,304 MB) when a new pair using the DP-VOL is created. <li data-bbox="630 1062 1424 1516"> <ul style="list-style-type: none"> <li data-bbox="630 1062 1424 1157">▪ External Authentication Compatibility option: When enabled, the authentication method is switched from VSP 5000 series to VSP. <p data-bbox="667 1178 1424 1272">This setting enables the acceleration of external authentication, however only top-level user groups can be searched. Therefore, this setting is not recommended.</p> <ul style="list-style-type: none"> <li data-bbox="667 1293 1424 1388">▪ VSP authentication method: When external authentication (LDAP) is performed, only top-level user groups are searched. Nested groups are not searchable. <li data-bbox="667 1409 1424 1516">▪ VSP authentication method: When external authentication (LDAP) is performed, nested groups are enabled as well as top-level user groups.


Item	Description
	<ul style="list-style-type: none"> <li data-bbox="630 254 1419 453"> <p>▪ Enable reboot of background service: This option must be enabled only when you are requested to enable it. When this option is enabled, the SVP starts monitoring the background service process. When either of the following values exceeds its threshold, the background service process for managing configuration information is restarted.</p> <ul style="list-style-type: none"> <li data-bbox="667 474 1357 537">• The amount of memory used in the background service process <li data-bbox="667 558 1333 621">• Time elapsed after the background service process is started <li data-bbox="630 663 1419 863"> <p>▪ 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>.</p> <li data-bbox="630 884 1419 1188"> <p>▪ The consistency time of a URMF pair shows the time stamp of the data that has just been copied to a restored journal volume.</p> <ul style="list-style-type: none"> <li data-bbox="667 968 1373 1062">• Enabled: The time included in the time stamp of the data that has just been copied to a restored journal volume shows the consistency time. <li data-bbox="667 1083 1406 1178">• Disabled: The time included in the time stamp of the data that has just been copied to a secondary volume shows the consistency time. <li data-bbox="630 1209 1419 1503"> <p>▪ After delta resync, the pair status remains COPY during journal data copy.</p> <ul style="list-style-type: none"> <li data-bbox="667 1293 1419 1388">• Enabled: When a delta resync is performed in a 3DC multi-target configuration with TC and UR, the pair status remains COPY during journal data copy. <li data-bbox="667 1409 1419 1503">• Disabled: When a delta resync is performed in a 3DC multi-target configuration with TC and UR, the pair status changes directly to PAIR.

Item	Description
	<ul style="list-style-type: none"> ▪ One minute after remote path failure detection, the mirror is split. <ul style="list-style-type: none"> • Enabled: When a remote path failure is detected, the mirror is split if the remote path is not restored within one minute after the detection. • Disabled: When a remote path failure is detected, the mirror is split if the remote path is not restored within the path monitoring time set by the mirror option. <p>This setting is enabled only when After remote path failure detection, the mirror is split is enabled. When After remote path failure detection, the mirror is split is disabled, the mirror is not split even if a remote path failure is detected.</p> ▪ After remote path failure detection, the mirror is split. <ul style="list-style-type: none"> • Enabled: After a remote path failure is detected, the mirror is split. • Disabled: Even if a remote path failure is detected, the mirror is not split. <div style="border: 1px solid black; background-color: #e0f7fa; padding: 5px; margin: 10px 0;">  Note: See table below for After remote path failure detection settings. </div> ▪ The copy pace for mirror option (Medium) becomes one level faster. <ul style="list-style-type: none"> • Enabled: The pace for copying data during initial copy becomes one level faster when the copy pace for journal option is Medium. This item can be used to make the initial copy operation in Medium speed mode perform faster. ▪ The copy pace for mirror option (Medium) becomes two levels faster. <ul style="list-style-type: none"> • Enabled: The pace for copying data during initial copy becomes two levels faster when the copy pace for journal option is Medium. This item can be used to make the initial copy operation in Medium speed mode perform faster.
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.

The following tables show how advanced system setting 5 works with advanced system setting 6 and how advanced system setting 15 works with advanced system setting 16.

Table 30 Advanced system settings 5 and 6

No. 5	No. 6	Description	
		Create operation	Resync operation
Disabled	Disabled	Change the management method from hierarchical differences to SM differences.	Change the management method from hierarchical differences to SM differences.
	Enabled	Change the management method from SM differences to hierarchical differences.	The differential data management method is not changed.
Enabled	Disabled	Change the management method from SM differences to hierarchical differences.	Change the management method from SM differences to hierarchical differences.
	Enabled	Change the management method from SM differences to hierarchical differences.	The differential data management method is not changed.



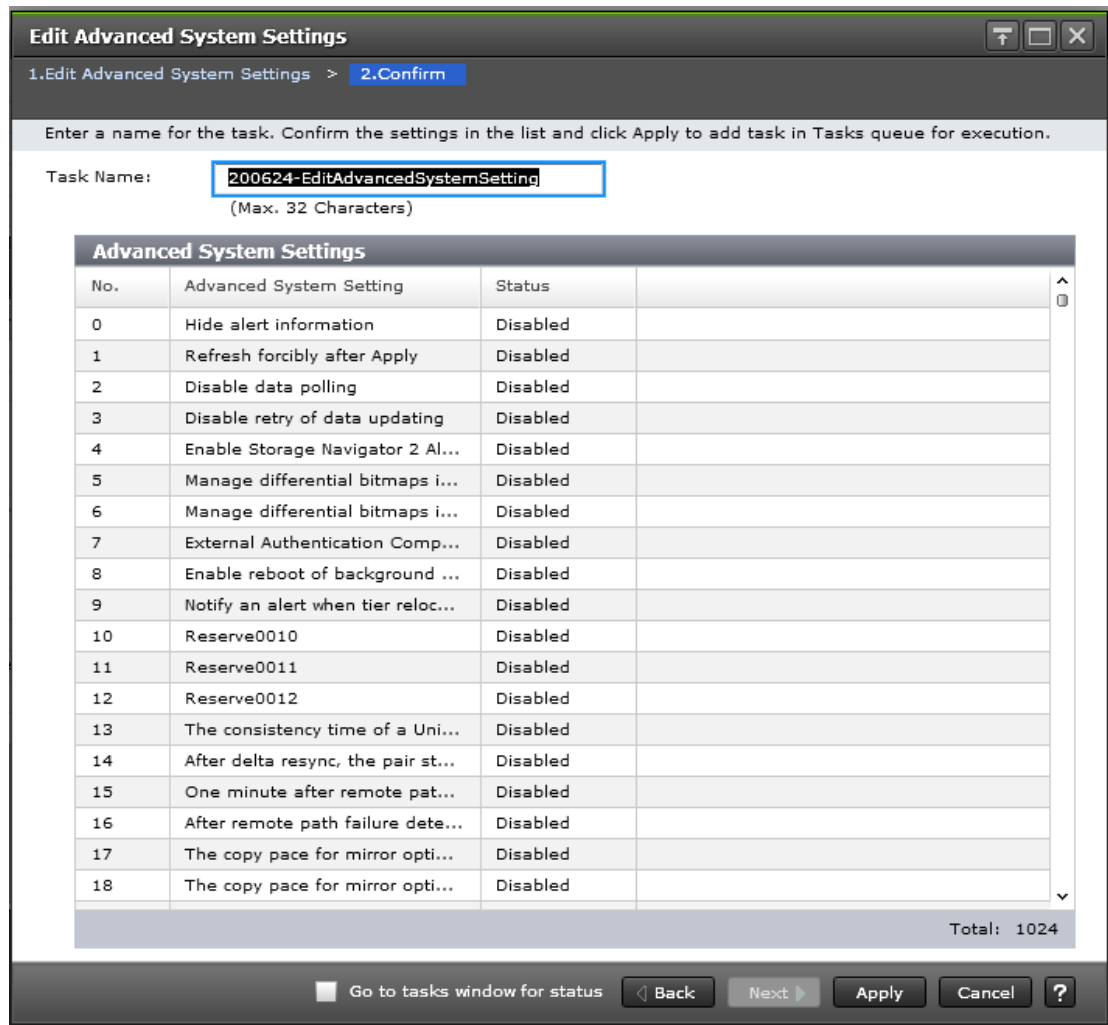
Note: If the LDEV capacity exceeds 4 TB (for open)/262,668 Cyl (for mainframe), the hierarchical memory management method is used regardless of whether advanced system settings 5 or 6 are enabled.

Table 31 Advanced system settings 15 and 16

No. 15	No. 16	Description
Disabled	Disabled	Even if a remote path failure is detected, the mirror is not split.
Enabled	Disabled	Even if a remote path failure is detected, the mirror is not split.

No. 15	No. 16	Description
Disabled	Enabled	After remote path failure detection, the mirror is split if the remote path is not restored within the path monitoring time.
Enabled	Enabled	After remote path failure detection, the mirror is split if the remote path is not restored within one minute after the detection.

Edit Advanced System Settings confirmation window



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.

Appendix E: 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

The screenshot displays the Storage Navigator interface for a VSP 5000 series storage system. The top window, titled 'Edit Storage System', contains a table with the following data:

Storage System Name	VSP 5500H	Software Version	Main	90-04-00/00
Storage System Type		SVP	CBA	90-04-00/00-0001
Serial Number	1	RMI Server		10_01_03
IP Address	localhost	Total Cache Size		166.00 GB
Contact				
Location				

The bottom window, titled 'Allocation Summary', provides a detailed breakdown of storage capacity and usage. It includes a pie chart for physical capacity and a table for virtual capacity. The physical capacity table is as follows:

Category	Physical Capacity	Percentage	Number of Physical Logical Devices
Allocated	542.60 GB	[7%]	504
Reserved	0.00 MB	[0%]	94
Used DP Pool	0.00 MB	[0%]	-
Unused DP Pool	0.00 MB	[0%]	-
Other	294.91 GB	[4%]	2
Available Space	157.20 GB	[1%]	256
Unallocated	6.70 TB	[88%]	-
Free Space	-	-	-
Physical Total	7.68 TB		856

The virtual capacity table is as follows:

Category	Virtual Capacity	Number of Virtual Logical Devices
DP Allocated	120.96 GB	84
DP Unallocated	361.75 GB	114
Other	768.00 MB	16
Virtual Total	483.46 GB	214

Additional summary information at the bottom of the Allocation Summary window includes:

- Total Efficiency: - [Data Reduction: - / Software Saving: - (Compression: - / Deduplication: - / Pattern Matching: -) / FMD Saving: - (Compression: - / Pattern Matching: -) / Snapshot: - / Provisioning: 0%] [-]
- Total Saving: 0.99:1 (-)
- Total DP Subscription Rate: 0%
- Total Number of LDEVs: 1070 (Max Allowed: 65280)

Hardware summary

Item	Description
Edit Storage System	Allows editing of the storage system name, contact, and location.
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.

Item	Description
Storage System Type	Model type of the storage system.
Serial Number	Serial number of the storage system.
IP Address	IP address of the SVP.
Software Version	Version of the following software: <ul style="list-style-type: none"> ▪ Main: Version of the storage system firmware ▪ SVP: Version of HDvM - SN installed in the SVP ▪ CBA: Version of Captive Bundle Application (used for running HDvM - SN with Adobe AIR) ▪ RMI Server: Version of the RMI server installed in the SVP
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

Item	Description
Internal / External	This item switches the displayed items. <ul style="list-style-type: none"> ▪ Total: Displays information on both the internal volumes and the external volumes. ▪ Internal Only: Displays information on only the internal volumes. ▪ External Only: Displays information on only the external volumes.
Open/ Mainframe	This item switches the displayed capacity units. <ul style="list-style-type: none"> ▪ Total: Displays all the open-systems, mainframe-systems and multi-platform volumes ▪ Open Only: Displays only open-systems volumes ▪ Mainframe Only: Displays mainframe-systems and multi-platform volumes.
Capacity Unit	This item switches the displayed units of the capacity. <ul style="list-style-type: none"> ▪ Appropriate: Displays the capacity in appropriate unit depending on the capacity of each item. ▪ TB/GB/MB: Displays the capacity of the specified unit.
Physical Summary	This item displays the capacity of physical logical devices and the number of devices. The information for open systems and mainframe systems is different. For details about this item, see the Physical Summary table.

Item	Description
Virtual Summary	This item displays capacity of virtual logical devices and the number of devices. The information for open systems and mainframe systems is different. For details about this item, see the table below about virtual summary.
Total Efficiency	<p>This field is blank if the calculation for items below is not complete. A hyphen (-) is displayed if the information is not valid. For details, see the <i>Provisioning Guide</i>.</p> <ul style="list-style-type: none"> ▪ Total Efficiency: Displays the ratio of the total saving effect achieved by accelerated compression, capacity saving (compression and deduplication), snapshot, and Hitachi Dynamic Provisioning. The ratio of the system data is not included. ▪ Data Reduction: Displays the data reduction ratio before and after performing the accelerated compression function and the capacity saving function (compression and deduplication). The ratio of the system data is not included. ▪ Software Saving: Displays the capacity reduction ratio for data which is before and after performing the capacity saving function. The ratio of the system data is not included. <ul style="list-style-type: none"> • Compression: Displays the capacity compression ratio for data which is before and after performing the capacity saving function. • Deduplication: Displays the capacity deduplication ratio for data which is before and after performing the capacity saving function. • Pattern Matching: Displays the capacity reduction ratio for data before and after performing pattern matching of the capacity saving function. ▪ FMD Saving: Displays the capacity reduction ratio for data which is before and after performing the accelerated compression function. The ratio of the system data is not included. <ul style="list-style-type: none"> • Compression: Displays the capacity compression ratio for data which is before and after performing the accelerated compression function. • Pattern Matching: Displays the capacity reduction ratio for data before and after performing pattern matching of the accelerated compression function. ▪ Snapshot: Displays the efficiency ratio achieved by snapshot. The ratio of the system data is not included. ▪ Provisioning: Displays the efficiency ratio achieved by Hitachi Dynamic Provisioning. The ratio of the system data is not included. ▪ Date and time for calculation: The start date and time and the end date and time for the calculation are displayed within the square brackets.

Item	Description
	<p>Note: The date and time in the square brackets are the system date and time (date, time, and timezone) of the storage system. For Last Updated in HDvM - SN, the date and time based on the system date and time (date, time, and timezone) of the SVP are displayed. Therefore, if the settings of the system date and time for the storage system and the ones for the SVP are different, the date and time in the square brackets in this window and the date and time displayed for Last Updated are also different.</p>
Total Saving (Software Deduplication, Software Compression, FMD Compression)	<p>Total Saving: Displays the ratio and capacity reduced by the capacity saving function against all data in a storage system.</p> <p>When you use the capacity saving function, the saving ratio is calculated against metadata, garbage data, and parity data generated by the storage system in addition to user data. If the amount of used data volume before the capacity saving function is executed is smaller than the used pool capacity, a value which is invalid and smaller than the actually saved capacity might be displayed as the saved capacity.</p> <p>Software Deduplication: Displays the ratio reduced by the deduplication function against all data in a storage system.</p> <p>Software Compression: Displays the ratio reduced by the software compression function against all data in a storage system.</p> <p>FMD Compression: Displays the ratio reduced by the FMD compression function against all data in a storage system.</p>
Total DP Subscription Rate	<p>This item displays the ratio of virtual logical device capacity to physical logical device capacity in the pool volume of Dynamic Provisioning.</p> <p>For a Dynamic Provisioning pool in which Thin Image pairs are created, the virtual logical device capacity includes the snapshot data capacity.</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

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> <p>The control cylinder is not included in the capacity.</p> <p>The total capacity includes:</p> <ul style="list-style-type: none"> ▪ The pool-VOL capacity that is not used as pool capacity ▪ The capacity of the system pool-VOL management area (approx. 4.1 GB per pool) <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>

Item	Description
	<p>The control cylinder is not included in the capacity.</p> <p>The total capacity includes:</p> <ul style="list-style-type: none"> ▪ The pool-VOL capacity that is not used as pool capacity ▪ The capacity of the system pool-VOL management area (approx. 3.7 GB per pool) <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

Item	Description
DP Allocated *	<p>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.</p>
DP Unallocated*	<p>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.</p>

Item	Description
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

Port Condition DKC-0

Refresh

Number of Ports	Available (Connected)	2
	Available (Not Connected)	3
	Not Available	3
	Not Installed	0

Port Condition

Filter ON OFF

Channel Board	Board Type	Port ID	Attribute	Condition	Speed	SI	Tr	R
CHB-01B	4HF32R (Fi...	CL1-A	Target	Not Available	Auto(-)	10		
CHB-01B	4HF32R (Fi...	CL3-A	Target	Available (Not Connected)	Auto(-)	10		
CHB-01B	4HF32R (Fi...	CL5-A	Target	Available (Connected)	Auto(-)	10		
CHB-01B	4HF32R (Fi...	CL7-A	Target	Not Available	Auto(-)	10		
CHB-02B	4HF32R (Fi...	CL1-E	Target	Available (Not Connected)	Auto(-)	10		
CHB-02B	4HF32R (Fi...	CL3-E	Target	Available (Connected)	Auto(-)	10		
CHB-02B	4HF32R (Fi...	CL5-E	Target	Not Available	Auto(-)	10		
CHB-02B	4HF32R (Fi...	CL7-E	Target	Available (Not Connected)	Auto(-)	10		

Export Total: 8

Close ?

You can switch between information about DKC-0 and DKC-1 through DKC-5 with a tab. When DKC-1 through DKC-5 is not installed, the target 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 Board	Name of the channel board (Channel board is also called a front-end director.)
Board Type	Type of the channel board
Port ID	Port identifier
Attribute	Port attribute <ul style="list-style-type: none"> ▪ Channel board type is Fibre: Bidirectional or Target ▪ When no port is assigned to the user, a hyphen (-) is displayed.
Condition	Port Condition icon and port status <ul style="list-style-type: none"> ▪  Available (Connected): The port is installed and in use. ▪  Available (Not Connected): The port is installed and available

Item	Description
	<ul style="list-style-type: none"> ▪ Not Installed: The port is either not installed or cannot be used. ▪ Not Available: The port is either blocked or not assigned to the user.
Speed	<p>Data transfer speed of the port is displayed in gigabits per second as follows:</p> <ul style="list-style-type: none"> ▪ 1 Gbps ▪ 2 Gbps ▪ 4 Gbps ▪ 8 Gbps ▪ 10 Gbps ▪ 16 Gbps ▪ 32 Gbps <p>If Auto is set for Port Speed in the Edit Ports window, this item is displayed as follows:</p> <ul style="list-style-type: none"> ▪ Auto (1 Gbps) ▪ Auto (2 Gbps) ▪ Auto (4 Gbps) ▪ Auto (8 Gbps) ▪ Auto (10 Gbps) ▪ Auto (16 Gbps) ▪ Auto (32 Gbps) <p>The values in the parentheses are set by the storage system. If linkup is not made, a hyphen (-) is displayed.</p> <p>A hyphen (-) is displayed for the ports not assigned to the user.</p> <p>For details of the Edit Ports 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>
SFP Data Transfer Rate	Displays the maximum transfer rate of SFP which the mounted package supports.
WWN/iSCSI Name	WWN/iSCSI name of the port
Export	Displays a window for outputting table information

Tasks window




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

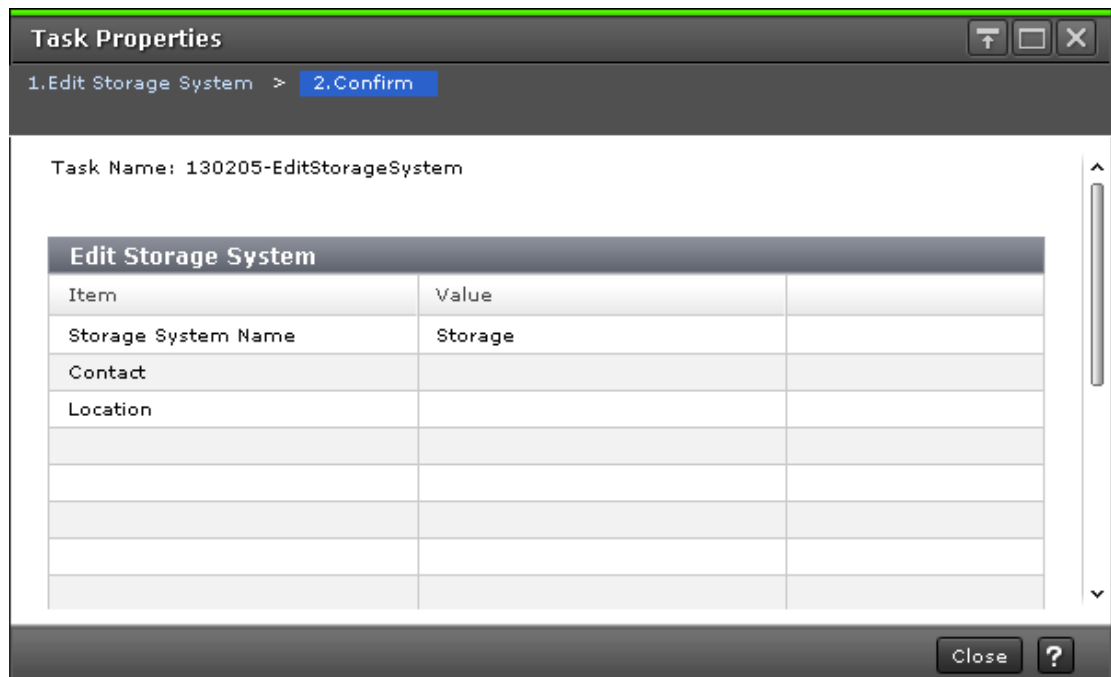
Item	Description
Task Name	Task name specified by a user when the user performed the task. Click to view the detail of the task.
Status	<p>Task status. Click to view more details about status or errors.</p> <ul style="list-style-type: none">  Completed or Completed(Request): The task completed normally.  In progress: The task is being processed by the system.  Waiting: The task is not yet started.

Item	Description
	<ul style="list-style-type: none"> ▪  Suspended: The task has been suspended. ▪  Failed: The task ended abnormally.
Type	General name of the task.
User Name	User name who performed the task.
Submission Time	Date and time when the task was submitted.
Start Time	Date and time when the task was started. Blank indicates the task has not started yet.
End time	Date and time when the task completed. Blank indicates the task has not completed yet.
Auto Delete	<p>Enabled: A task is automatically deleted when the following two events occur:</p> <ul style="list-style-type: none"> ▪ The task is completed ▪ The number of tasks in the Task list reaches the maximum number the window can display (384) <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"> ▪ The waiting or suspended tasks will be cancelled. ▪ The failed or aborted tasks can be deleted from the window. ▪ Tasks in progress cannot be deleted. ▪ 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.
Disable Auto Delete *	When disabled, the selected task remains in the task list after the task is completed.

Item	Description
Enable Auto Delete *	When enabled, the selected task is deleted from the Task list when the following two events occur: <ul style="list-style-type: none"> The task is completed The number of tasks in the Task list reaches the maximum number the window can display (384)
Export *	Displays a window that shows the information in the table
* Appears when you click More Actions.	

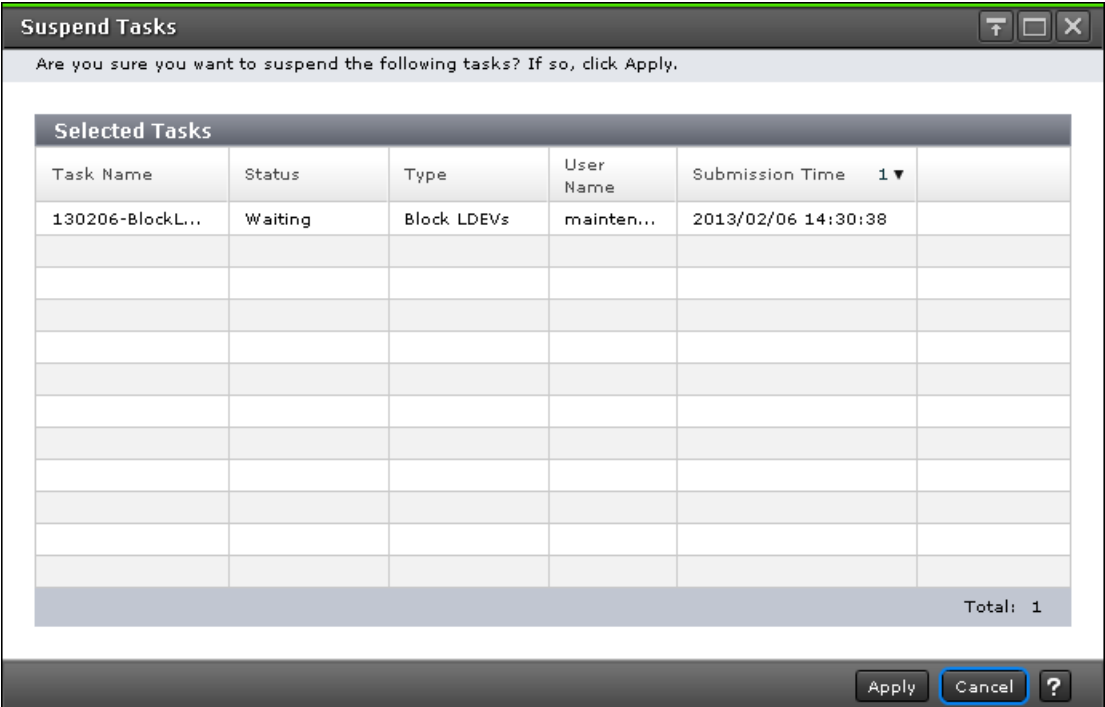
Task Properties window

This window displays details about a task performed on the storage system. The content of the window depends on the task you executed.



Suspend Tasks window

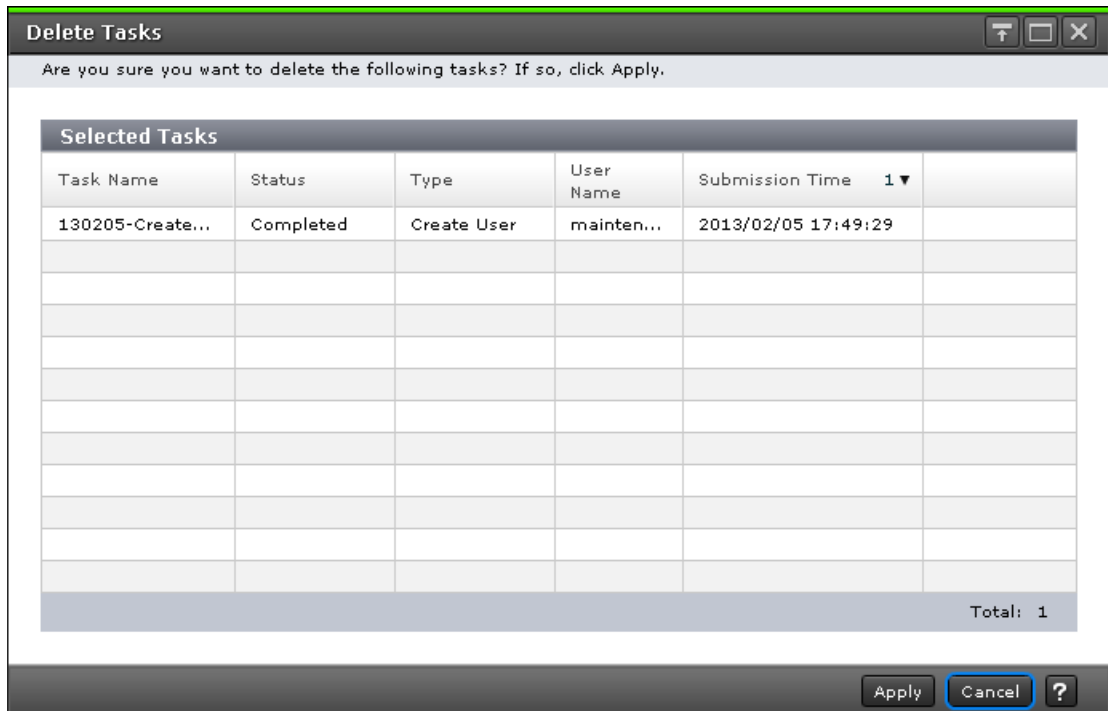
Use this window to suspend waiting tasks.



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 who performed the task.
Submission Time	Date and time when the task was submitted.

Resume Tasks window

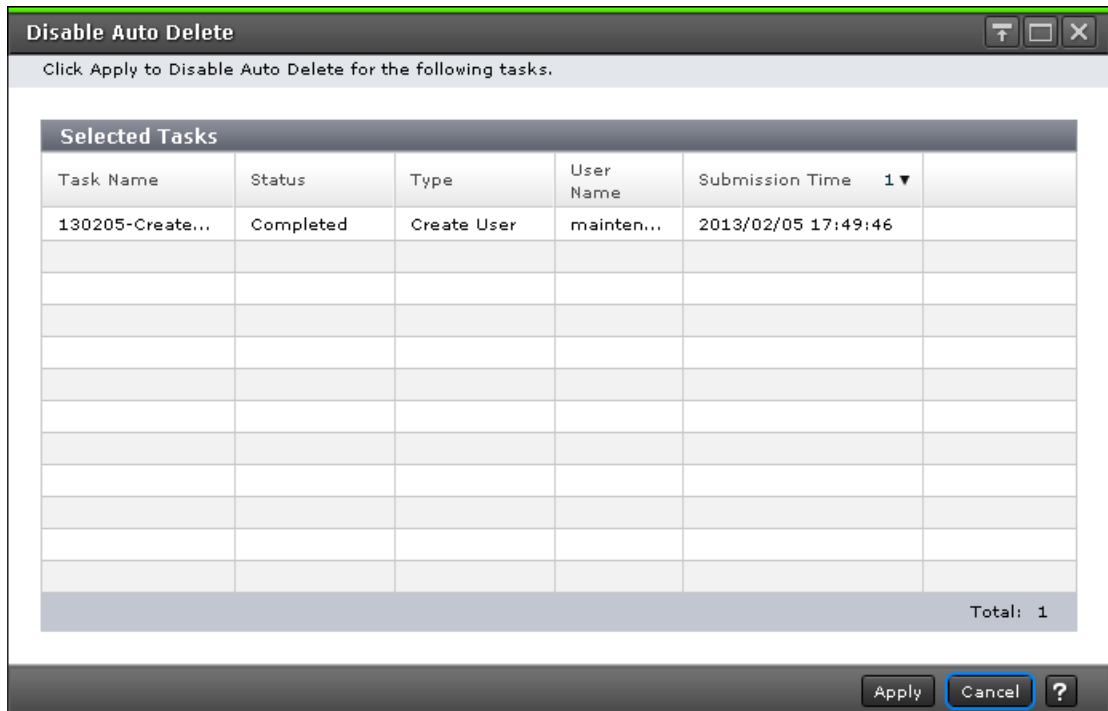
Use this window to resume suspended tasks.



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.
User Name	User name who performed the task.
Submission Time	Date and time when the task was submitted.

Disable Auto Delete window

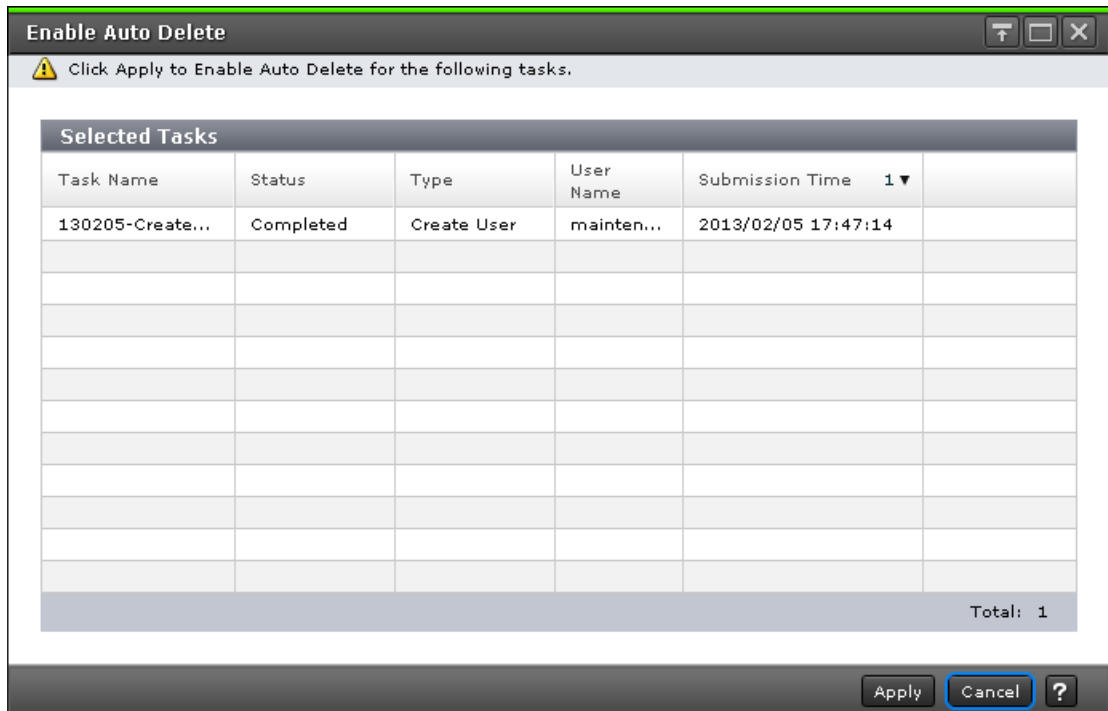
Use this window to prevent a task from being automatically deleted from the task window.



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

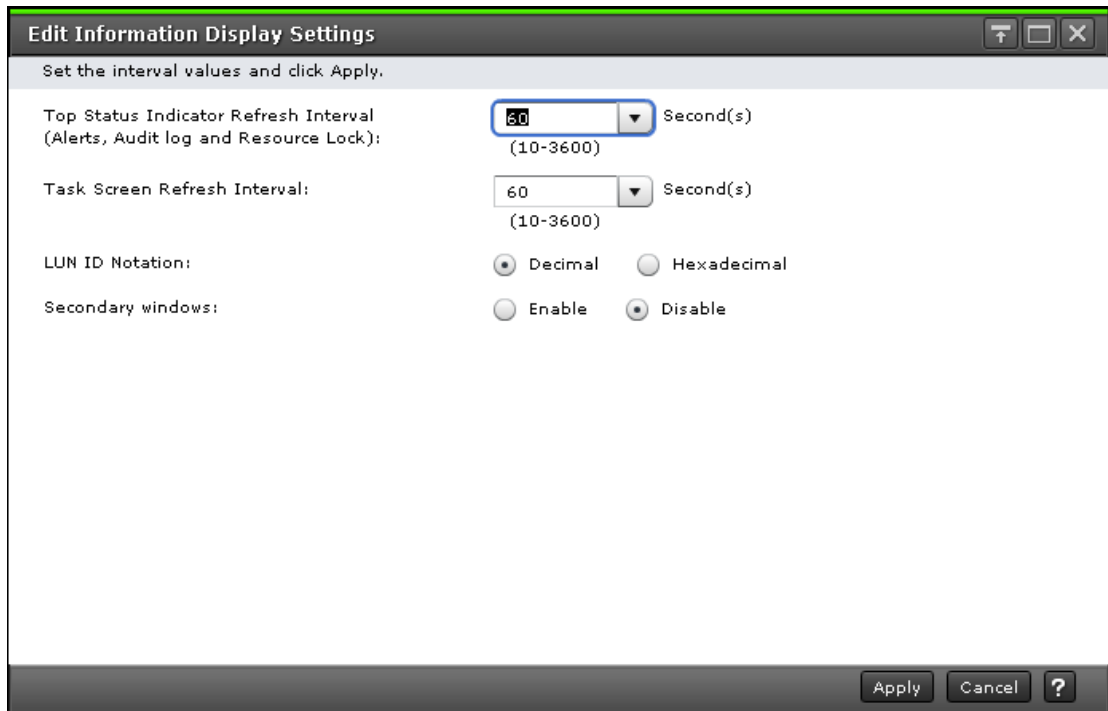
Use this window to automatically delete completed tasks from the task window when the number of displayed tasks reaches the maximum (384 tasks).



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

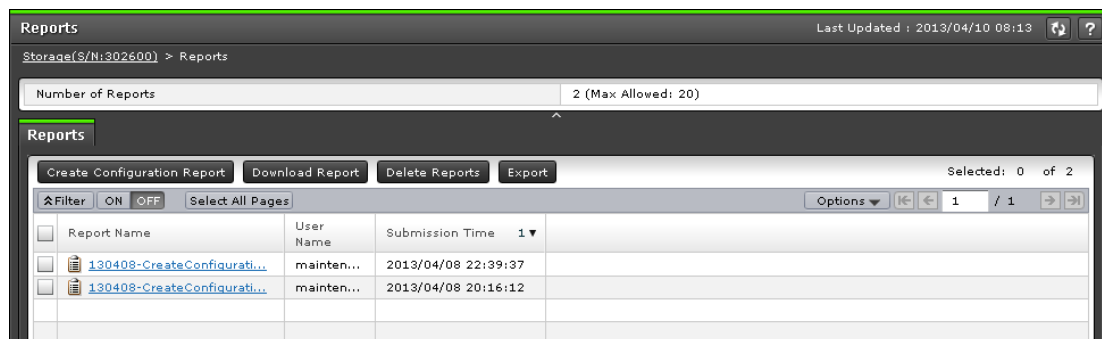
Use this window to change the display parameters.



Item	Description
Top Status Indicator Refresh Interval (Alerts, Audit log, and Operation 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. This setting can be enabled only during logged in. 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.

1. 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 Reports	
Report Type	Format
Configuration Reports	HTML
Detail Configuration Reports	CSV
Total: 2	

Go to tasks window for status Back Next Apply Cancel ?

Item	Description
Report Type	Type of the report to be created.
Format	File format.

Delete Reports window

Use this window to delete configuration reports.

The screenshot shows the Alerts window with a summary table and a list of alerts. The summary table shows the following data:

Summary		
Number of Uncompleted Alerts	Acute	0
	Serious	0
	Moderate	2
	Service	0
	Total	2

The Alerts list shows the following data:

Error Code	Date	Error Level	Status
<input type="checkbox"/> BF2010	2013/02/19 09:52:30	Moderate	Uncompleted
<input type="checkbox"/> 47E700	2013/02/19 09:51:37	Moderate	Uncompleted





At the bottom of the window, there is a 'Detail' button and a status bar showing 'Selected: 0 of 2'. A 'Close' button and a help icon are also visible.

Summary

Item	Description
Number of Uncompleted Alerts	<p>Displays the number of alerts that are not authenticated yet.</p> <ul style="list-style-type: none"> ▪ Acute: Displays total number of Acute level alerts that are not authenticated yet. ▪ Serious: Displays total number of Serious level alerts that are not authenticated yet. ▪ Moderate: Displays total number of Moderate level alerts that are not authenticated yet.

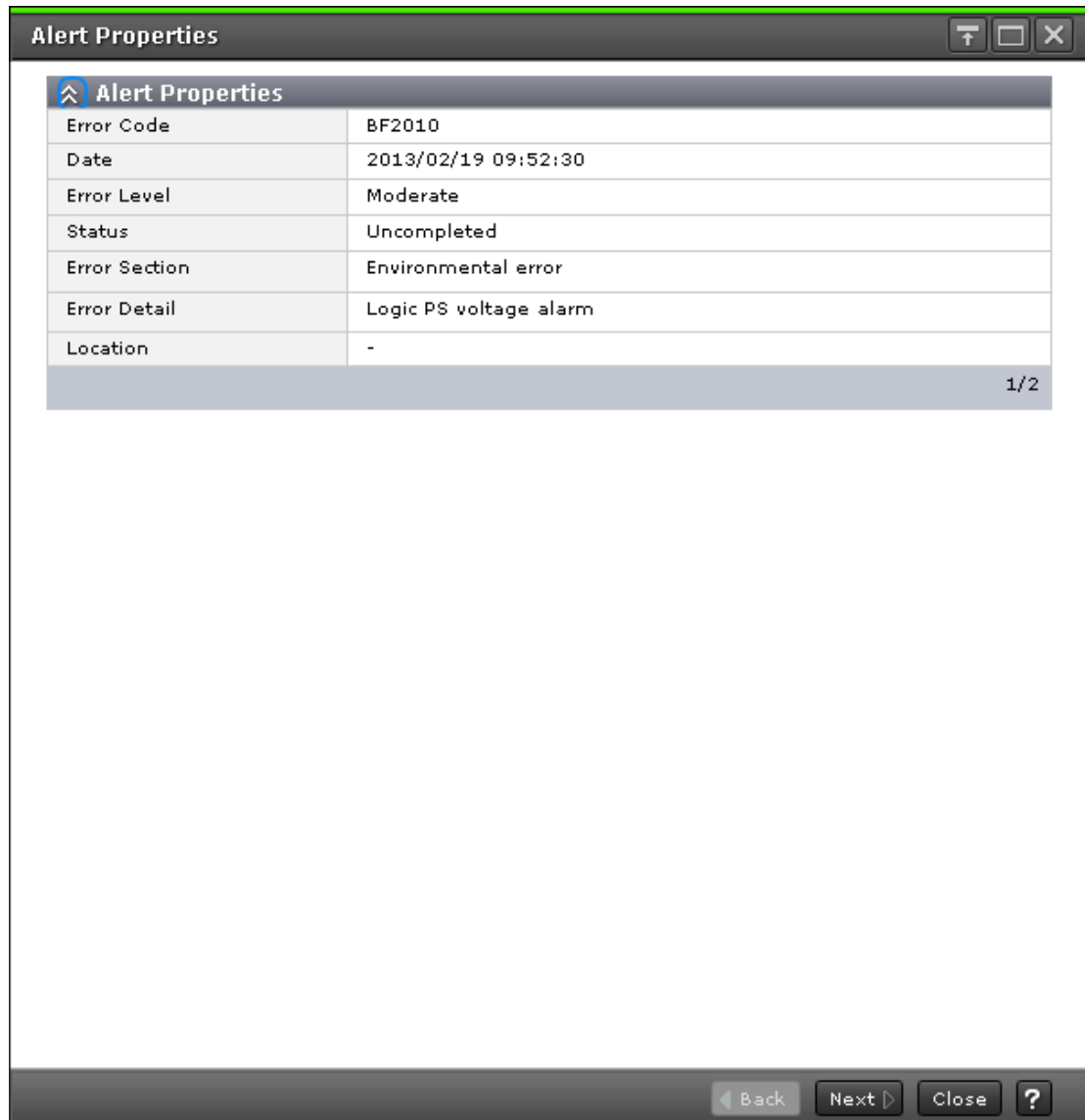
Item	Description
	<ul style="list-style-type: none"> ▪ Service: Displays total number of Service level alerts that are not authenticated yet. ▪ Total: Total number of above is displayed.

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 Monitoring SIMs alerts in Device Manager - Storage Navigator (on page 274).</p>
Date	Displays the date when alerts occurred.
Error Level	<p>Displays error level of alerts.</p> <ul style="list-style-type: none"> ▪  Service: No need to deal with immediately. Errors that are dealt with within periodical maintenance. ▪  Moderate: No need to deal with immediately. Errors that are dealt with within periodical maintenance. ▪  Serious: Contact the customer support. Take adequate measure as instructed, report and solve the problem. ▪  Acute: Contact the customer support. Take adequate measure as instructed, report and solve the problem.
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.



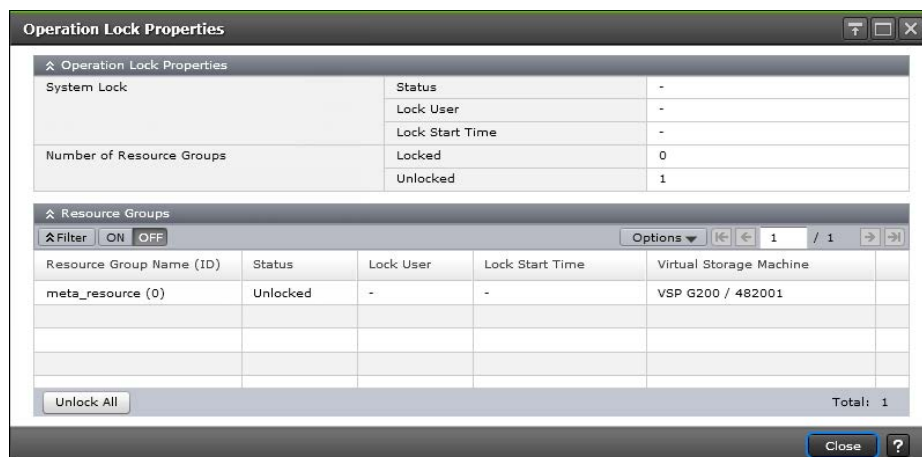
When you select multiple alerts in the **Alert** window, click Back and Next to change alert that is displayed.

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 Monitoring SIMs alerts in Device Manager - Storage Navigator (on page 274) .
Date	Displays the date when alerts occurred.

Item	Description
Error Level	<p>Displays error level of alerts.</p> <ul style="list-style-type: none"> ▪  Service: No need to deal with immediately. These errors are dealt with during periodical maintenance. ▪  Moderate: No need to deal with immediately. These errors are dealt with during periodical maintenance. ▪  Serious: Contact the customer support. Take adequate measures as instructed, report and solve the problem. ▪  Acute: Contact the customer support. Take adequate measures as instructed, report and solve the problem.
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.

Operation Lock Properties window

This window displays the lock status of the entire system and the lock status of the resource groups that can be operated.



Operation Lock Properties

Item	Description
System Lock - Status	Displays lock status of the entire system. Locked: System locked user exists. Hyphen (-): System locked user does not exist.
System Lock - Lock User	Displays the user that locked the entire system. A hyphen (-) indicates that there is no user who locked the entire system.
System lock - Lock Start Time	Displays the time when the entire system was locked. A hyphen (-) indicates that the entire system is not locked.
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 **Operation 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: The resource group is locked Unlocked: The resource group is not locked System Locked: The entire system is locked
Lock User	Displays the user name of the person who locked the resource
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 DB.

The screenshot shows the Temperature Monitor window with three sections:

- HSNBX Ambient Temperature:** A table with columns 'HSN Box', 'Measurement Location', and 'Ambient Temperature (degrees C)'. It shows one entry for HSNBX-0 at HSNPANEL0 with a temperature of 28. An 'Export' button and 'Total: 1' are at the bottom.
- DKC Ambient Temperature:** A table with columns 'Chassis ID', 'Measurement Location', and 'Ambient Temperature (degrees C)'. It shows two entries for DKC-0 at CTL01 and CTL02, both with a temperature of 26. An 'Export' button and 'Total: 2' are at the bottom.
- DB Internal Temperature:** A table with columns 'Disk Unit', 'Drive Box', 'Measurement Location', and 'Internal Temperature (degrees C)'. It shows two entries for DKU-0 at DB-000, with temperatures of 31 and 30. An 'Export' button and 'Total: 2' are at the bottom.

The window has a title bar 'Temperature Monitor' and standard window controls. At the bottom right, there are 'Close' and '?' buttons.

DKC Ambient Temperature table

Item	Description
Chassis ID	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 if the DKC is turned off, or the temperature information cannot be acquired due to a unit or network failure.
Export button	Displays a window for outputting table information.

DB Internal Temperature table

Item	Description
Disk Unit	Displays the disk unit of the storage system.
Drive Box	Displays the drive box.
Measurement Location	Displays the measurement location.
Internal Temperature (degrees C)	Displays the internal temperature in degrees Celsius. Nothing is displayed in the DB internal temperature table when the DKC is turned off. The DB is not displayed in the DB internal temperature table when the temperature information cannot be acquired because the chassis is not installed, the DB is blocked for maintenance, or a unit or network failure occurred.
Export button	Displays a window for outputting table information.

HSNBX Ambient Temperature table

Item	Description
HSN Box	Displays the HSN box of the storage system.
Measurement Location	Displays the measurement location.
Ambient Temperature (degrees C)	Displays the ambient temperature in degrees Celsius. Nothing is displayed in the HSNBX ambient temperature table when the DKC is turned off. The HSNBX is not displayed in the HSNBX ambient temperature table when the temperature information cannot be acquired because the HSNBX is blocked for maintenance, or a unit or network failure occurred.
Export button	Displays a window for outputting table information.

Appendix F: Tool Panel GUI Reference

This section describes the windows and features of the SVP **Tool Panel**.

Tool Panel

This section describes the **Tool Panel** window features and controls.





Item	Description
Control Panel	Downloads and restores configuration files.
Download Dump Files	Download dump files onto a Hitachi Device Manager - Storage Navigator(HDvM - SN) computer.
Update Certificate Files	Updates and uploads the private key and the signed server certificate (Public Key) to the SVP.
Set Up HTTP Blocking	Allows you to block access to port 80.
Release HTTP Blocking	Allows you to unblock access to port 80.
Update Certificates Files for SMI-S	Updates and uploads the private key and the signed server certificate (public key) to the SMI-S provider to update the certificate.
Upload Configuration Files for SMI-S	Controls the SMI-S function using the SMI-S provider configuration file that you create.
SMI-S Artificial Indication	Send an SMI-S artificial indication to determine whether the communication between the listeners and the SMI-S provider succeeds or fails.
Set or Delete Certificates for HCS	Sets or deletes the HCS public key certificate.

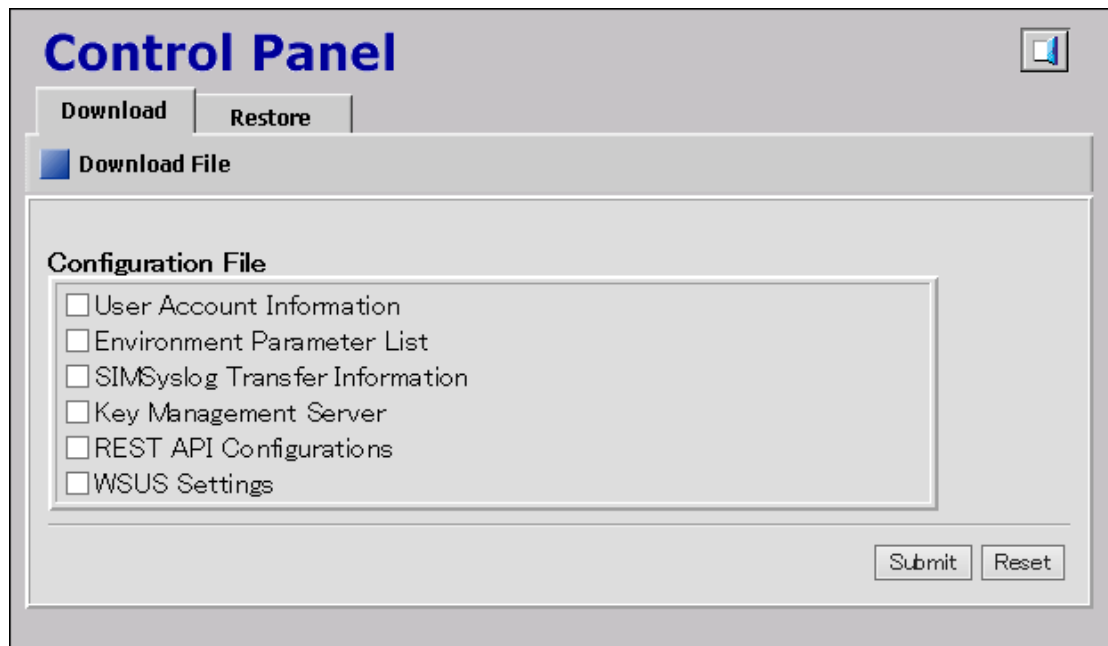
Item	Description
TLS Security Settings	Creates the security settings used for SSL/TLS communications with the SVP.
Create CSR and Self-Signed Certificate	Creates a CSR (public key), private key, and self-signed certificate.
Forcibly Disable SVP	Used to manually change the SVP to the standby SVP.
Forcibly Fail Over SVP	Used to manually change the SVP to the standby SVP.
Flash Disable/Enable	Enables or Disables HDvM - SN to run in the Adobe Flash Player environment.
CaptiveBundleUpload	Enables HDvM - SN to run in the Adobe AIR environment.
WSUS Settings	Sets up Windows Server Update Services (WSUS).

Control Panel

This section describes the **Tool Panel** windows and controls.

Download File window

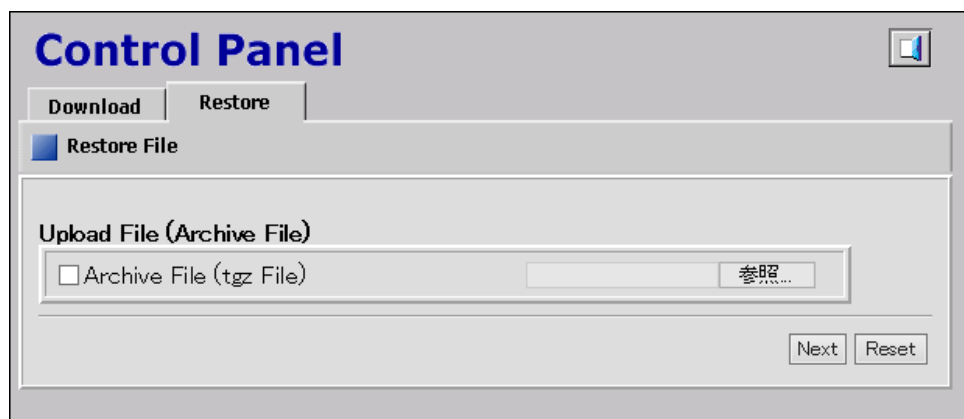
This section describes the **Download File** window of the Control Panel.



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

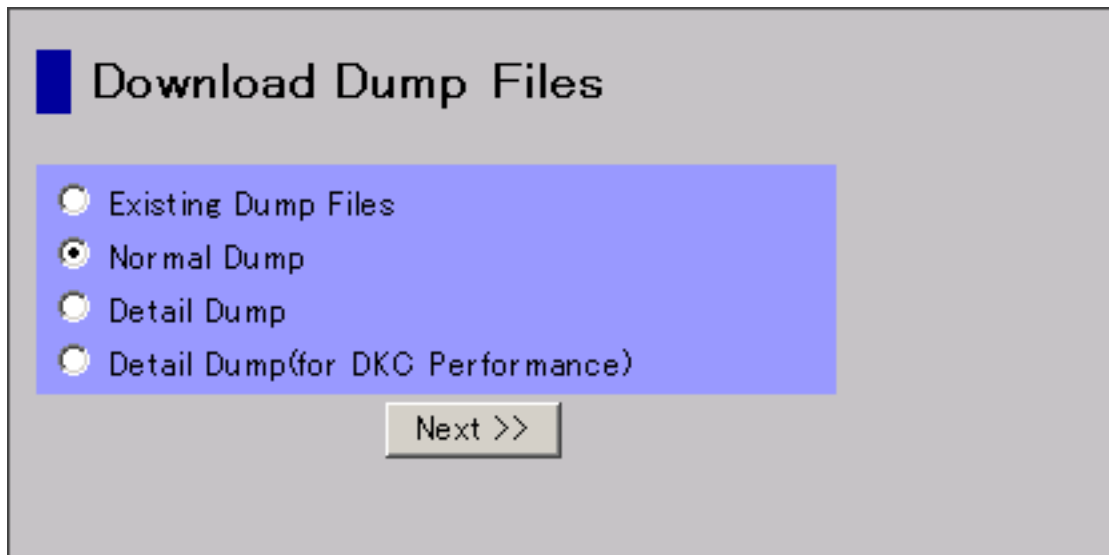
This section describes the **Restore File** window features and controls.



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.

Item	Description
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

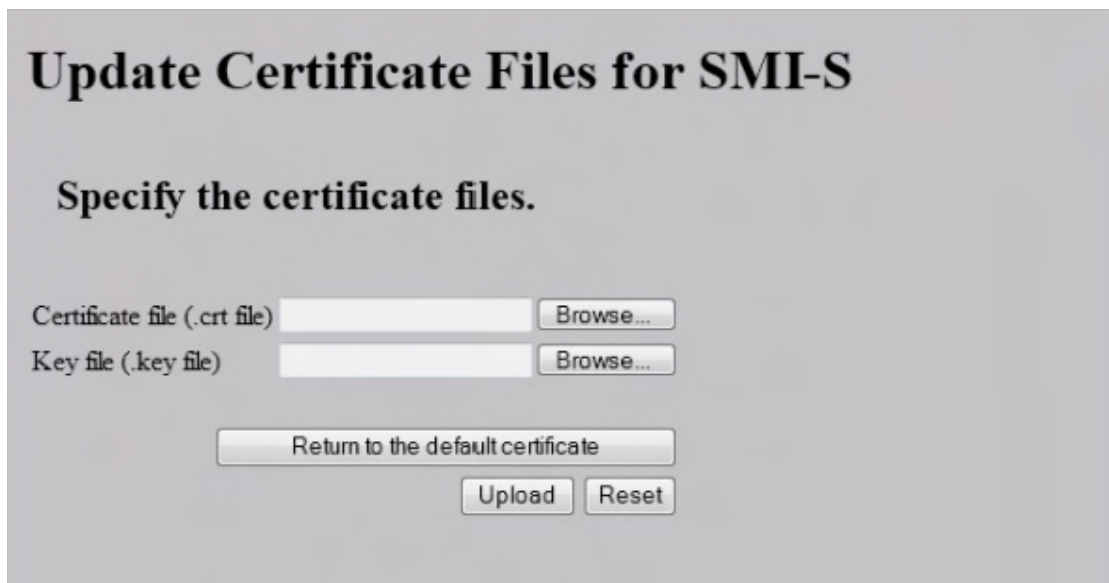
This section describes the **Update Certificate Files** window features and controls.

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).

Item	Description
I understood that I canceled HTTP blocking or TLS communication might fail.	Confirm the messages about a possible TLS communication failure and recommendations described in the dialog box, and then select the check box for this item.
Return to the default certificate	Returns the SSL certificate to default.
Upload	Uploads the SSL certificate.
Reset	Cancel 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.

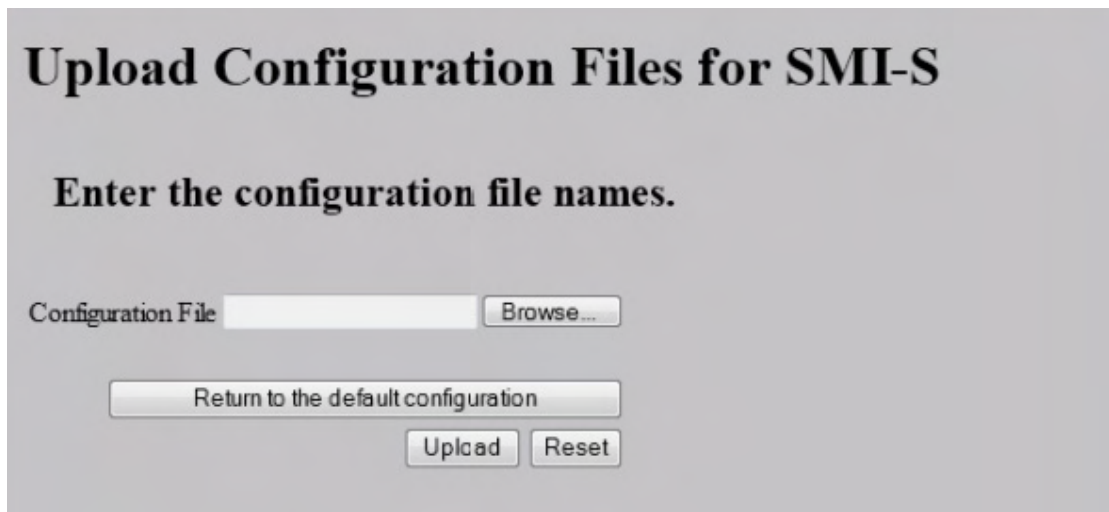


Item	Description
Certificate file (.crt file)	Click Browse... and specify the certificate file (server.crt file).
Key file (.key file)	Click Browse... and specify the key file (server.key file).
Return to the default certificate	Returns the SSL certificate to default.
Upload	Uploads the certificate to the SMI-S provider.

Item	Description
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.

SMI-S Artificial Indication

Enter the user ID and the password.

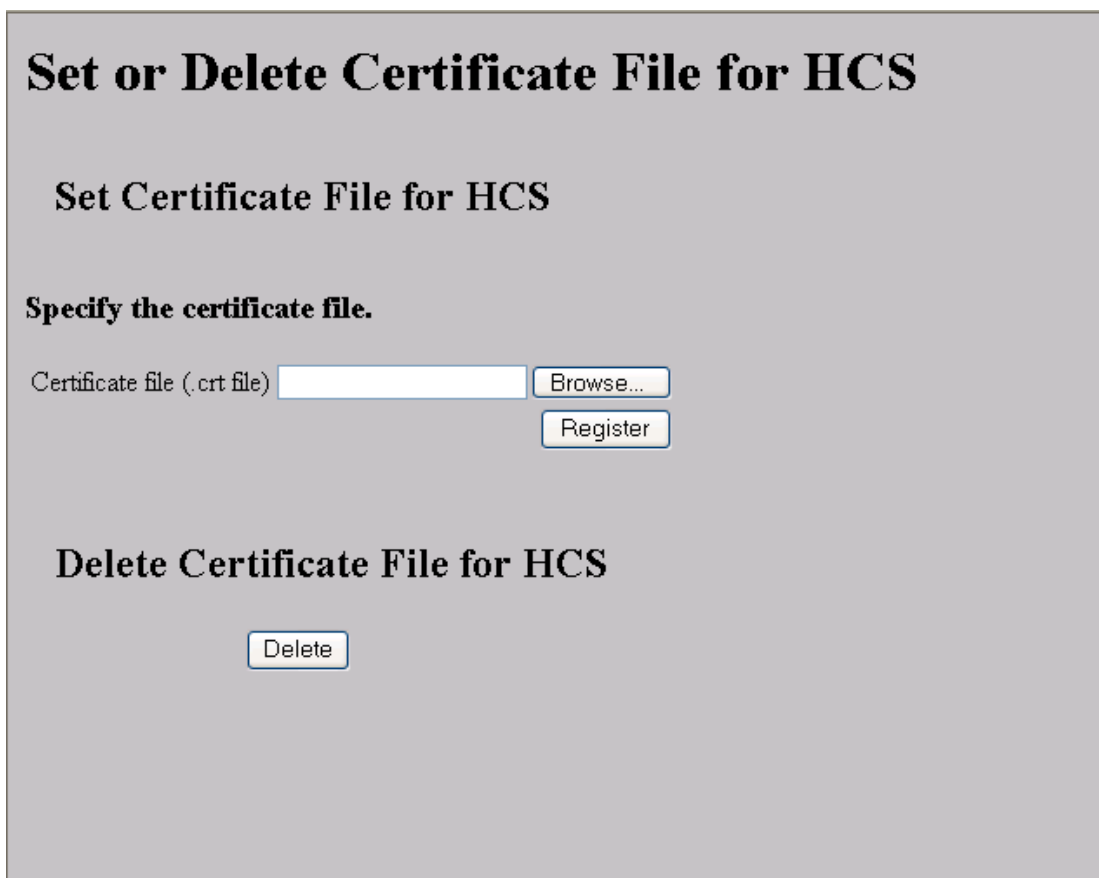
User ID:

Password:

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.



Item	Description
Certificate file (.crt file)	Click Browse... and specify the certificate file (server.crt file).
Register	Registers the certificate for HCS.
Delete	Deletes the certificate for HCS.

TLS Security Settings window

This section describes the TLS Security Settings window features and controls.

TLS Security Settings

Protocol: TLS1.2 TLS1.3

Cipher Suites:

TLS1.2

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS1.3

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384

Minimum Key Length (Key Exchange):

RSA:

DHE:

ECDHE:

Renegotiation: Yes No (Recommended)

It is recommended first to release HTTP blocking, and then perform the TLS security settings. If applying the TLS security settings without releasing HTTP blocking first, connecting to the tool panel using HTTP and HTTPS might fail. In this case, connect to the tool panel using HTTP, and then apply the appropriate TLS security settings. If the problem persists despite retrying, contact customer support.

I understood that I canceled HTTP blocking or TLS communication might fail.

Table 32

Item	Description
Protocol	<p>Protocols that is allowed to be used in the communication path. The following protocols are supported:</p> <ul style="list-style-type: none"> ▪ TLS1.2 ▪ TLS1.3

Item	Description
Cipher Suites	<p>Cipher Suites that are allowed to be used in the communication path. The following cipher suites are supported:</p> <ul style="list-style-type: none"> ▪ TLS1.2 <ul style="list-style-type: none"> • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ▪ TLS1.3 <ul style="list-style-type: none"> • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384
Minimum Key Length (Key Exchange)	<p>Sets the minimum key length allowed for key exchange during the communications.</p> <p>The minimum key length supported by the key exchange algorithm set on the TLS Security Setting dialog box in the Tool Panel dialog box is applied when a certificate with RSA public key is set during the communications between the management client and the SVP.</p>

Item	Description
	<p>When the following cipher suites are valid, and when a server certificate, root certificate, or client certificate with an RSA public key is uploaded to the SVP, the key length of the RSA public key of the certificate must be longer than the key length selected on the TLS Security Setting dialog box in the Tool Panel dialog box.</p> <ul style="list-style-type: none"> ▪ TLS_RSA_WITH_AES_128_CBC_SHA ▪ TLS_RSA_WITH_AES_128_CBC_SHA256 ▪ TLS_RSA_WITH_AES_256_CBC_SHA256 ▪ TLS_RSA_WITH_AES_256_GCM_SHA384 <p>When the SVP communicates with a Syslog server, key management server, external authentication and authorization server, or Hitachi Command Suite server, the key length of the key exchange key set on the server must satisfy the following:</p> <ul style="list-style-type: none"> ▪ RSA: 2048 bits or more ▪ DHE: 2048 bits ▪ ECDHE: secp256r1, secp384r1, or secp521r1 <p>The supported key exchange algorithms have a minimum key lengths.</p> <p>RSA</p> <ul style="list-style-type: none"> 2048 bits 3072 bits 4096 bits <p>DHE</p> <ul style="list-style-type: none"> 2048 bits <p>ECDHE</p> <ul style="list-style-type: none"> 256 bits (secp256r1) 384 bits (secp384r1) 521 bits (secp521r1)

Item	Description
Renegotiation	Sets whether to allow (Yes) or disallow (No (Recommended)) renegotiation.

TLS Security Settings Communication Test window

This section describes the TLS Security Settings Communication Test window features and controls.

TLS Security Settings

Protocol: TLS1.2 TLS1.3

Cipher Suites:

TLS1.2

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS1.3

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384

Minimum Key Length (Key Exchange):

RSA:

DHE:






ECDHE:

Renegotiation: Yes No (Recommended)

It is recommended first to release HTTP blocking, and then perform the TLS security settings. If applying the TLS security settings without releasing HTTP blocking first, connecting to the tool panel using HTTP and HTTPS might fail. In this case, connect to the tool panel using HTTP, and then apply the appropriate TLS security settings. If the problem persists despite retrying, contact customer support.

I understood that I canceled HTTP blocking or TLS communication might fail.

Table 33

Communication Test	<p>Tests whether TLS communication is enabled for the following communication paths:</p> <ul style="list-style-type: none"> ▪ SVP – Syslog Server ▪ SVP – Key Management Server ▪ SVP – LDAP Server ▪ SVP – HCS server <p>The following icons and status indicate the status of each communication path during the Communication Test:</p> <ul style="list-style-type: none"> ▪ : Processing ▪ : Normal ▪ : Skipped ▪ : Error <p>If a problem occurs during the Communication Test, an error message appears in the field on the dialog box.</p> <ul style="list-style-type: none"> ▪ : Waiting
--------------------	---

Create CSR and Self-Signed Certificate window

This section describes the Create CSR and Self-Signed Certificate window features and controls.

Create CSR and Self-Signed Certificate

CSR Settings:

Country Name:
(2 Characters)

State or Province Name:
(Max. 128 Characters)

Locality Name:
(Max. 128 Characters)

Organization Name:
(Max. 64 Characters)

Organization Unit Name:
(Max. 64 Characters)

Common Name:
(Max. 64 Characters)

E-mail Address:
(Max. 128 Characters, or blank)

Optional Company Name:
(Max. 64 Characters, or blank)

Private Key Settings:

Key Type:

Key Length:

Password:
(4-20 characters, or blank)

Re-enter Password:

Create Self-Signed Certificate

Profile (.cfg file): Default Custom

Item	Description
CSR Settings	

Item	Description
Country Name	Enter the country name in 2 half-width alphabetic letters. (Example: US)
State or Province Name	Enter the state or province name. (Example: California)
Locality Name	Enter the city or region name. (Example: San Jose)
Organization Name	Enter the organization name. (Example: Hitachi)
Organization Unit Name	Enter the organization unit name. (Example: ITPro)
Common Name	Enter the IP address or the host name.
E-mail Address	(Optional) Enter your email address.
Optional Company Name	(Optional) Enter an additional organization name.
Private Key settings	
Key Type	Select RSA or ECDSA from the pull-down menu.
Key Length	<p>Select the key length from the pull-down menu.</p> <p>The key lengths that you can select depend on the key type:</p> <ul style="list-style-type: none"> ▪ RSA: 2048 bits, 3072 bits, 4096 bits ▪ ECDSA: 256 bits (secp256r1), 384 bits (secp384r1), 521 bits (secp521r1)
Password	Enter the password of the private key. No entry is required if you set no password
Re-entry Password	If you set a password, you must enter it. Re-enter the password that you set in Password.
Create CSR File and Key File	Open File Chooser, and then proceed to Download dialog box . The button is not activated unless you enter or select all required items for CSR settings and private key settings.
Create Self-Signed Certificate	To create a self-signed certificate, select the check box. The default is off.

Item		Description
Profile (.cfg file)	Default	By default, the system will automatically apply the default settings, and then no file selection is required.
	Custom	Select the profile reference location. Click Browse to select the profile you want to browse. For more information about the Profile (.cfg file) settings, see the table in the following section.
Create Self-Signed Certificate File		<p>Create a self-signed certificate file. The button is not activated unless you enter or select all of the following required fields:</p> <ul style="list-style-type: none"> ▪ CSR settings ▪ Private key settings ▪ Profile (Select Default or Custom. For Custom, select a file.)
Close		Close the file setting window.

Profile (.cfg file)

Profile (.cfg file) is a file that defines the parameters to be set with the self-signed certificate. The following describes the profile formats, settings, and parameters to be defined.

- File format
 - Format: Text
 - Extension: .cfg
 - Character code: ISO-8859-1
 - Line terminator: CRLF
- File settings
 - Parameter 1 = Parameter 1 setting value
 - Parameter 2 = Parameter 2 setting value

Examples of profile (.cfg) descriptions

```
days=3650
```

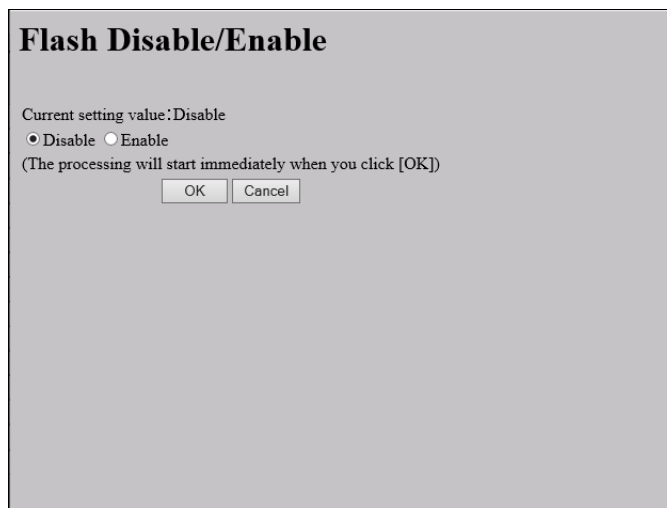
```
hashAlgorithm=SHA384
```

Table 34 Parameters to be defined by profile

Item	Description
days	Specifies the number of days that the certificate is valid from the time of self-signed certificate creation. An integer value from 1 to 3650 can be specified. It is recommended that the effective period be less than 825 days (27 months). If this parameter is not specified, 365 is set.
hashAlgorithm	Specifies the hash algorithm to be used with the self-signed certificate. SHA256 or SHA384 can be specified. If SHA256 is specified, SHA-256 is set as the hash algorithm for the self-signed certificate. If SHA384 is specified, SHA-384 is set as the hash algorithm for the self-signed certificate. If this parameter is not specified, SHA-256 is set as the hash algorithm for the self-signed certificate.

Flash Enable/Disable window

This section describes the Flash Disable/Enable dialog box features and controls.

**Table 35**

Item	Description
Current setting value	Setting status of the function of displaying HDvM - SN by using Adobe Flash Player.
Disable	Disables the function of displaying HDvM - SN by using Adobe Flash Player. This disallows the use of HDvM - SN running on a web browser.

Item	Description
Enable	Enables the function of displaying HDvM - SN by using Adobe Flash Player. This allows the use of HDvM - SN running on a web browser.

CaptiveBundleUpload window

This section describes the CaptiveBundleUpload dialog box features and controls.



Table 36

Item	Description
Specify a file to be uploaded	Selects Captive Bundle Application (CBA) file to be uploaded to the SVP. Click Browse to open the file selection window.
Upload	Uploads the selected CBA file to the SVP.

WSUS Settings

This section describes the Windows Server Update Services (WSUS) Settings dialog box features and controls

WSUS Settings

WSUS:
 WSUS: Disable Enable

Server URL:
 (Max. 511 Characters)

Active hours (6-18 hours):
 Start Hour:
 End Hour:

Item	Description
Disable	Disables the WSUS function.
Enable	Enables the WSUS function.
Server URL	<p>Enter the WSUS server URL to download Security Updates.</p> <p>Example of URL: <code>http://wsus.example.com</code>, <code>http://192.0.2.0</code></p> <ul style="list-style-type: none"> ▪ Add <code>http://</code> or <code>https://</code> at the beginning of the URL. ▪ The URL can be specified by using a host name or an IP address. ▪ Specify the URL with up to 511 characters using alphanumeric characters and the following symbols: <code>! \$ % - . @ _ ` ~ / :</code>
Active hours	Specify the start and end time so that the active hours range is set between 6 and 18 hours. The automatic restart of the SVP for applying Security Updates is disabled during the specified active hours.
Next	Opens the dialog box to confirm the WSUS settings updates.
Cancel	Cancels the WSUS settings updates.

Appendix G: 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.

Supported TLS versions

The following table shows the TLS versions supported by the SMI-S function.

DKCMAIN program version	TLS versions		
	Earlier than TLS1.2	TLS1.2	TLS1.3
Earlier than 90-02-00-xx	No	Yes	No
90-02-00-xx or later	No	Yes	Yes

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 VVolForSnapshot parameter (on page 545) .
PoolIDForSnapshot	Specifies pools that can be used by the SMI-S provider. For parameter details, see PoolIDForSnapshot parameter (on page 546) .
ResourceGroup	Specifies the resource groups that the SMI-S provider can use. For parameter details, see ResourceGroup parameter (on page 547) .

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` ignored.

VVolForSnapshot parameter

Use the `VVolForSnapshot` parameter to specify virtual volumes, which are usable as S-VOLs, 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

Hitachi Vantara



Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
HitachiVantara.com | community.HitachiVantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
HitachiVantara.com/contact