WEB CONSOLE SECTION

Contents

1. Before using Web Console

An IP address needs to be set before using Web Console on SVP.
Refer to “System Administrator Guide” for the specification of the commonness part of Web Console for the operation and conventions.

NOTE: There are cases that users copy a file from SVP to the maintenance PC via Remote Desktop in Web Console.

Blank Sheet

Blank Sheet

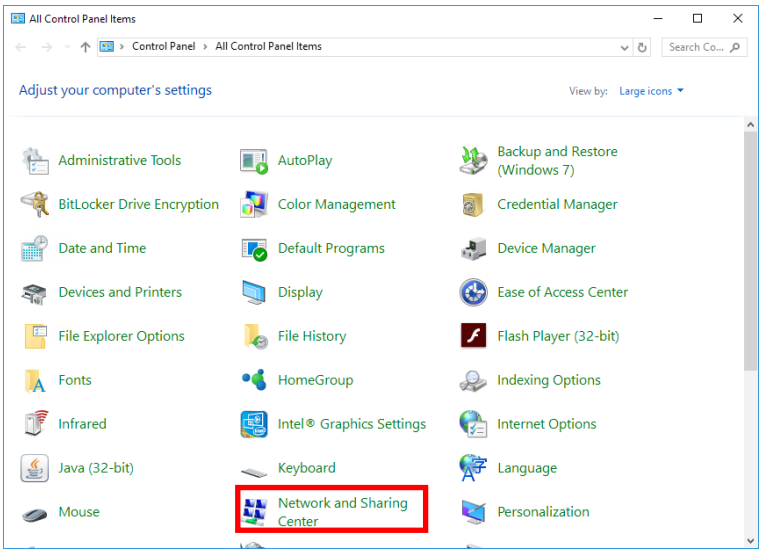
1.1 Setting IP Address and Network

When using Web Console from a remote personal computer or using the SNMP Agent function, a connection to an external LAN and a setting of a network is required (See (LOC04-50)).
To connect the external server (external authentication server, key management server, and so on) to SVP, the IP address setting needs to be performed of the DNS server.
Please setup according to the worksheet which the user's administrator indicated at the time of a new Installation.
Please setup the contents which took the duplicate from a setup on SVP before REPLACE.

NOTE: Don't change connection name. If you do so, Web Console will not work.

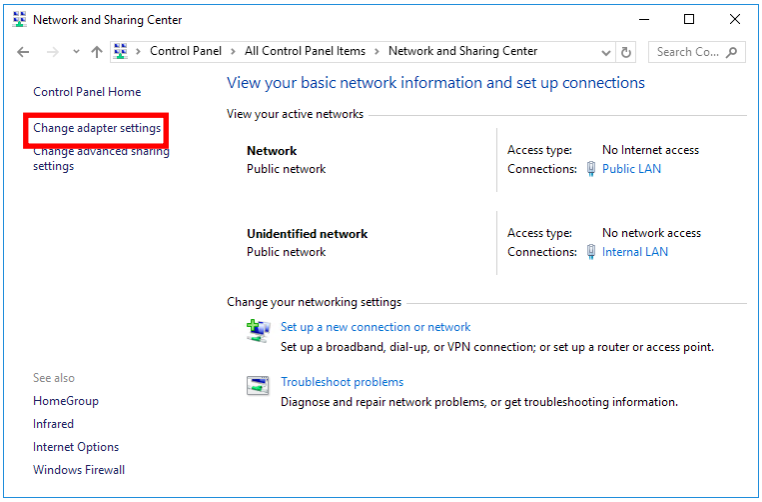
1. Setting IP address
   (1) Open the Control Panel window.
   Click [Start], and then select [Control Panel] from [Windows System].

   (2) Opening the Network and Sharing Center window
   Click [Network and Sharing Center] in the All Control Panel Items window.



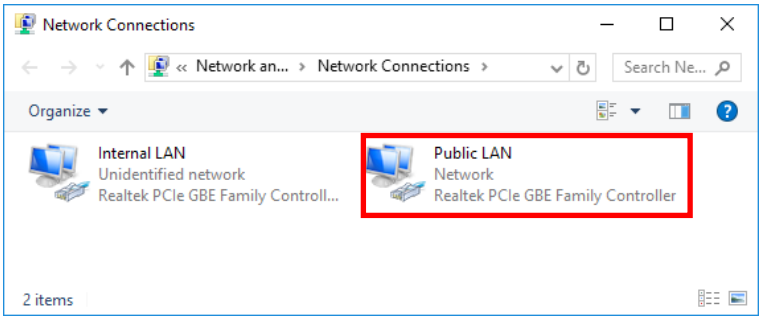
(3) Opening the Network Connections window

Select [Change adapter settings] in the left side of Network and Sharing Center window.



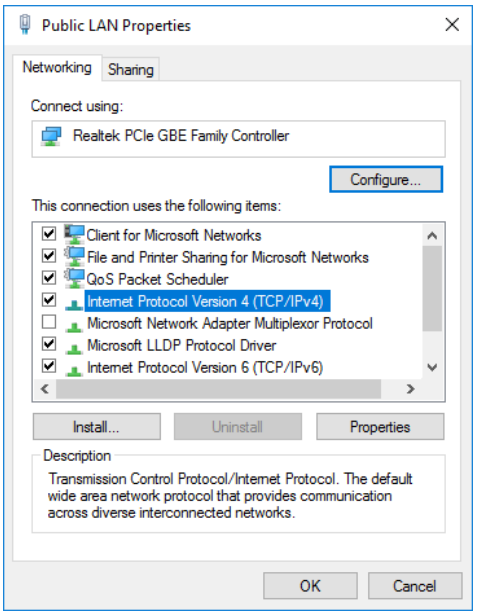
(4) Opening the Public LAN Properties window

Select [Public LAN] in the Network Connections window and click [Properties] by clicking the right mouse button.



(5) Opening the Internet Protocol Version 4 (TCP/IPv4) Properties window

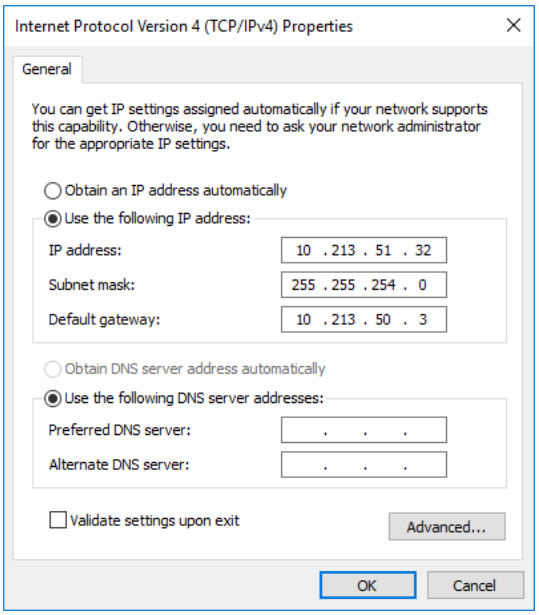
Select [Internet Protocol Version 4 (TCP/IPv4)] in the Public LAN Properties window and click [Properties].



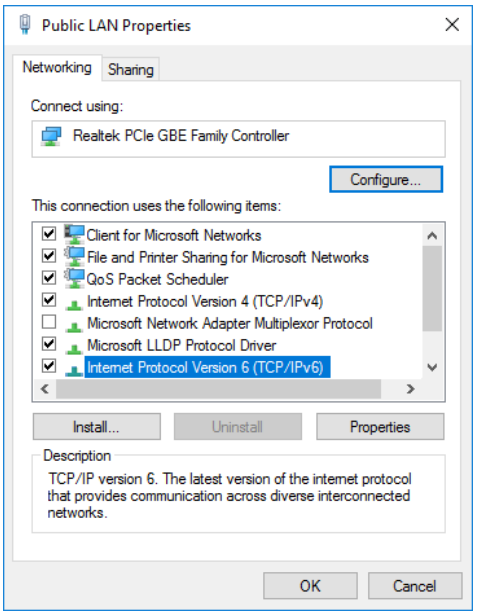
(6) Setting the external IP address

Set the “IP address”, “Subnet mask”, “Default gateway”, “Preferred DNS server” and “Alternate DNS server” and click [OK].

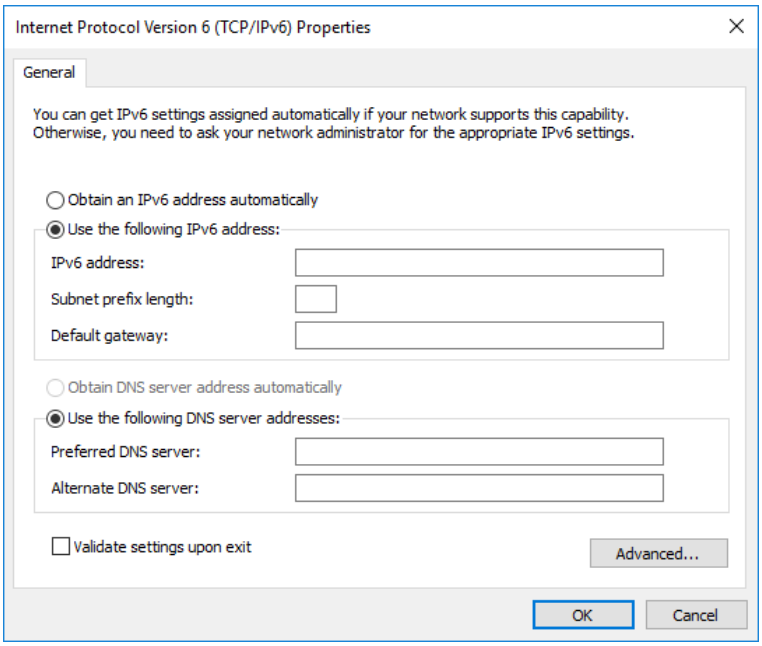
When you do not set IPv6, go to Step (9).



(7) Opening the Internet Protocol Version 6 (TCP/IPv6) Properties window
Select [Internet Protocol Version 6 (TCP/IPv6)] in the Public LAN Properties window and click [Properties].



(8) Setting the external IP address
Set the “IPv6 address”, “Subnet prefix length”, “Default gateway”, “Preferred DNS server”, “Alternate DNS server” and click [OK].



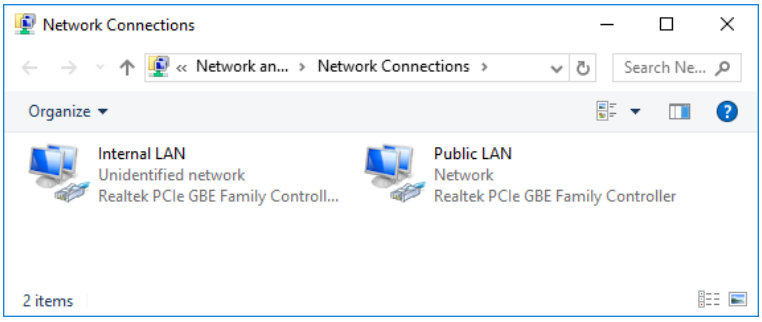
(9) Closing the window
After the setting is completed, click [OK] in the Public LAN Properties window.

2. Changing the Public LAN settings (Speed and Duplex) according to the settings on customer's switch (HUB)

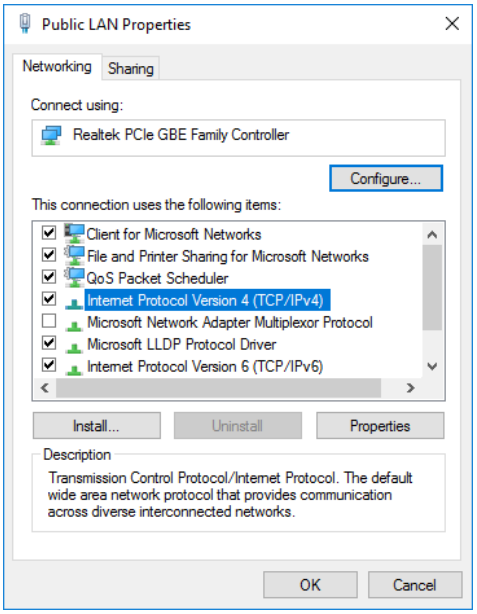
NOTICE:	Do not change the Internal LAN setting from [Auto Negotiation].

Checking the Public LAN settings (Speed and Duplex) according to the settings on customer's switch (HUB).
Ask your customer about the settings on the switch (HUB) to be connected to the SVP.
When "100M Full Duplex" is fixed against the SVP in the settings on customer's switch (HUB), this procedure is required..

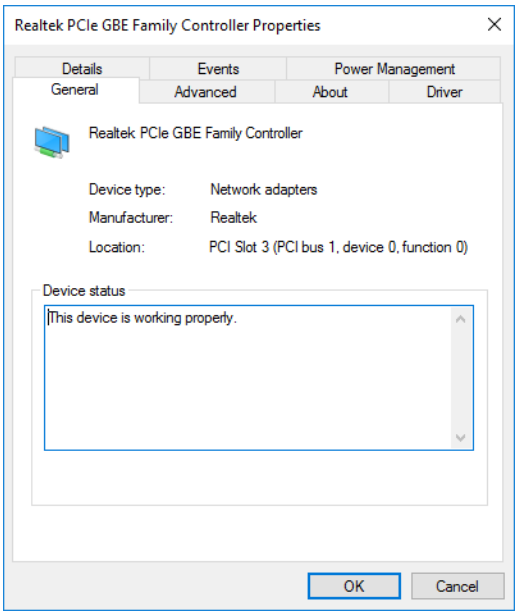
(1) Opening the Public LAN Properties window
Select [Public LAN] in the Network Connections window and select [Properties] by clicking the right mouse button.



(2) Opening the configuration windows
Click [Configure...] in the window.

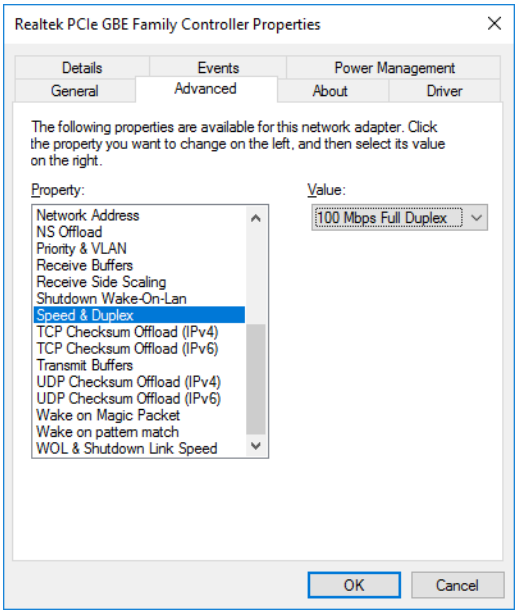


(3) Switching the tab
After [Configure...] is clicked, the window shown below opens.
Select the [Advanced] tab in the window.



(4) Setting the Connection Properties

Select the [Advanced] tab, and then select [Speed & Duplex] in the “Property” pull-down list. Change the value for “Value” from ‘Auto Negotiation’ to ‘100 Mbps Full Duplex’.



(5) Applying the settings and closing the window

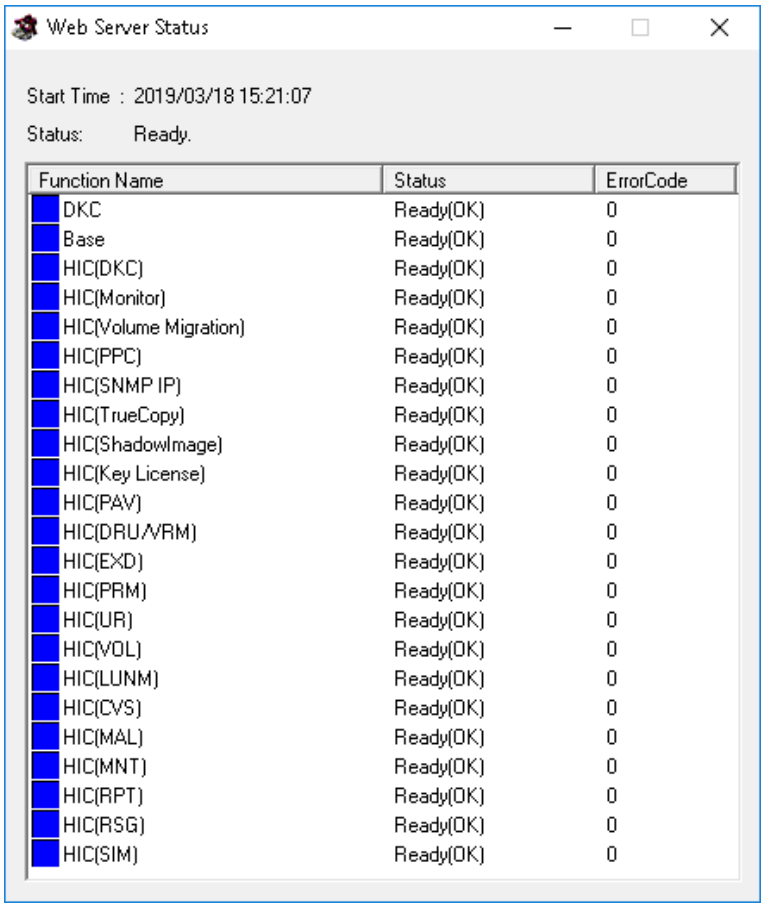
Return to the Pubic LAN Properties window by clicking [OK] and close the window by clicking [OK].

NOTE: When you use Web Console only with the IPv6 connection, set it referring to “4. IPv6 Setting”.

2. Web Console

2.1 Specifications of Web Server Status

Activate RISMAN, which is a program for accepting requests of a client and for performing high-speed processing through having structures of the RMI server and RAID in the memory, in order to make Web Console operate.
The window was always displayed as DKC460I. It does not usually displays as DKC510I/DKC610I/DKC710I/DKC810I/DKC910I. When [Web Server Status] of SVP launcher is pressed, the window as shown below displays.



Web Console cannot operate until all the statuses above become Ready(OK).

- Start Time: Time when RISMAN was activated.
- Status: Processing is displayed when RISMAN has the right of maintenance or Ready when it has not. (The mode can be changed to Modify even in the Processing status, however, a maintenance work cannot be done.)
- This window is started by pressing [Web Server Status] on the SVP window.

• Function Name

	Name	Description	Part code
1	DKC	Displays whether the DKC is ready or not.	0002
2	Base	Displays the status of the management of configuration information.	0002/0003
3	HIC (DKC)	Displays the state of initialization of the common function.	8005
4	HIC (Monitor)	Displays the state of initialization of the Performance Monitor function.	5105
5	HIC (Volume Migration)	Displays the state of initialization of the Volume Migration function.	5205
6	HIC (PPC)	Displays the state of initialization of the Server Priority Manager function.	5305
7	HIC (SNMP IP)	Displays the state of initialization of the SNMP Information function.	0305
8	HIC (TrueCopy)	Displays the state of initialization of the Remote Copy function.	6005/6105
9	HIC (ShadowImage)	Displays the state of initialization of the ShadowImage function.	7005/7105
10	HIC (Key License)	Displays the state of initialization of the Key License function.	0405
11	HIC (PAV)	Displays the state of initialization of the PAV function.	9005
12	HIC (Volume Security)	Displays the state of initialization of the Volume Security function.	9105
13	HIC (Volume Retention Manager)	Displays the state of initialization of the Volume Retention Manager z/OS® / Data Retention Utility function.	9205/9605
14	HIC (EXD)	Displays the state of initialization of Universal Volume Manager function.	0605
15	HIC (PRM)	Displays the state of initialization of Virtual Partition Manager function.	8505
16	HIC (UR)	Displays the state of initialization of the Universal Replicator function.	6505/6605
17	HIC (VOL)	Displays the state of initialization of the Quick Shadow / Dynamic Provisioning function.	3005
18	HIC(XRC)	Displays the state of initialization of the XRC function.	6805
19	HIC (LUNM)	Displays the state of initialization of the LUN Manager function.	1005
20	HIC (CVS)	Displays the state of initialization of the Volume Manager function.	3305
21	HIC (MAL)	Displays the state of initialization of the E-Mail information function.	8605
22	HIC (MNT)	Displays the state of initialization of the Maintenance function.	8705
23	HIC (RPT)	Displays the state of initialization of the Report function.	8805
24	HIC (RSG)	Displays the state of initialization of the Resource Group function.	20705
25	HIC (SIM)	Displays the state of initialization of the SIM Syslog information function.	8905

- Status

	Display	Color	Meaning
1	Not Initialize	Gray	Initialization is not started yet.
2	Initialize (Stat)	Yellow	Initialization is in progress.
3	Initialize (Retry)	Yellow	Initialization failed and it is being retried.
4	Ready (OK)	Blue	Ready for operation
5	Refresh (Start)	Green	Refreshment is in progress. The internal buffer is being initialized after a writing from the SVP / SNMP / Web Console has been completed.
6	Refresh (Retry)	Green	Refreshment failed and is being retried.
7	Initialize (Error)	Red	Initialization failed. (It is retried every other minute) (*1) (*3)
8	Refresh (Error)	Red	Refreshment failed. (It is retried every other minute) (*1)
9	Initialize (Pause)	Yellow	Initialization temporarily stops. (*2)
10	Refresh (Pause)	Yellow	Refreshment temporarily stops. (*2)

NOTE:
- When any of the statuses, Initialize (Start) / Refresh (Start) / Initialize (Retry) / Refresh(Retry) exists, no maintenance work can be done from an SVP. The message “INS2268E” is displayed on the SVP.
  However, it changes to the state of Initialize (Pause) / Refresh (Pause) in about 10 seconds and the maintenance work on the SVP may be possible.
- When an initialization or refreshment operation fails, a retrial operation is performed. When you want to do a maintenance work, do it when the Status is Ready. (Otherwise, an SVP rebooting, which is done after executing Define Information Files or All Configuration Files for alteration of the Config, may fail.)
- While an SVP maintenance work is being done, an initialization or refreshment operation fails and the status becomes Retry. When the maintenance work is completed, close the SVP window immediately.
- Operation of Web Console for a part whose status is not Ready (OK) cannot be done.
- There is a possibility the configuration is being changed from a user application (RAID Manager etc.) other than Storage Navigator if the display of Initialize (Start) / Refresh (Start) remains as is for a while. It will turn into the state of Ready (OK) a while after the configuration change is completed performed from the user application.

*1: When xxxx (Error) status is displayed for more than 2 minutes without any retry, there may be a problem just on display.
If you can reboot by pressing Web Console button and can press the each function button normally, there is no problem.
When DKC has been powered off, it is likely to turn into the state of xxxx (Error).
After DKC has been powered on for a while, it turns into the state of Ready (OK).

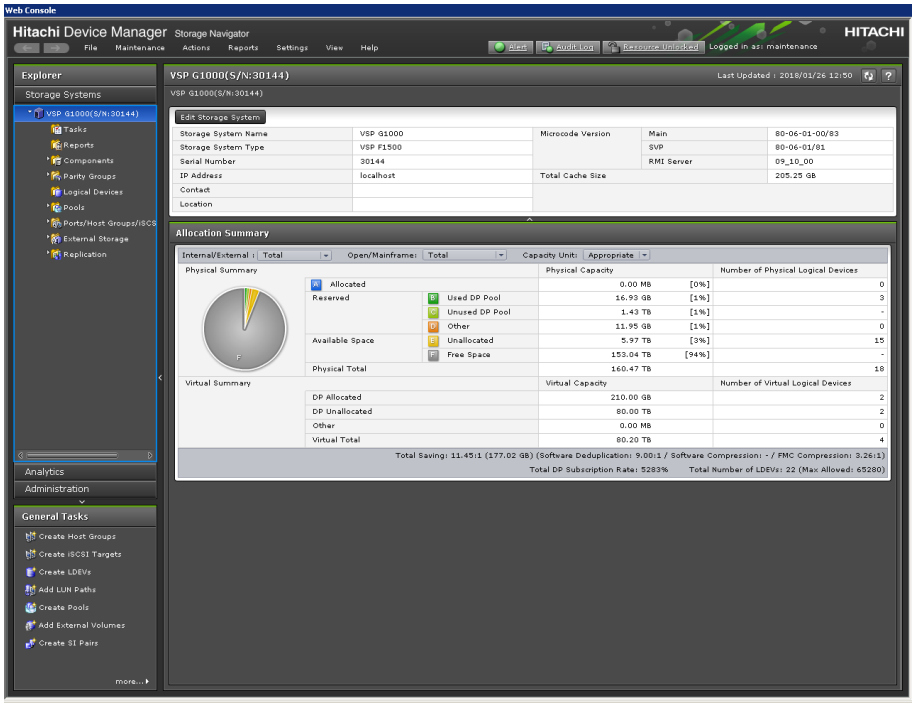
*2 Initialization/Refresh is restarted by changing the SVP to the View mode.

*3 When a storage system is ended without shutting down SVP ,“Initialize (Error)” may be displayed at the time of initialization of RISMAN, a retry recovers.

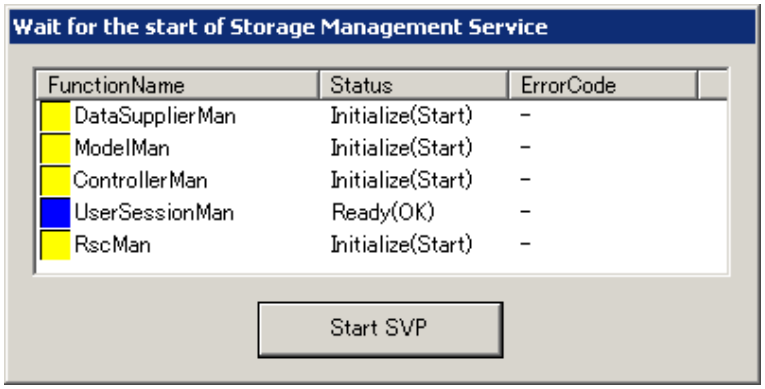
- Error Code
  When an error occurs, its error cord is displayed.
  Refer to errors which occur in each part shown in the list of Web Console messages.
  (Part codes are listed in the item of Function Name.)

2.2 Procedure for Activation Using SVP

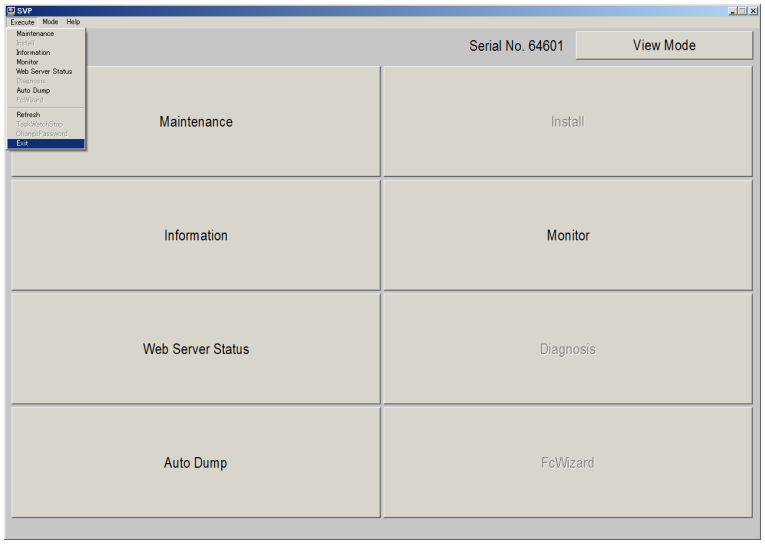
When SVP is logged in Remote Desktop, Web Console automatically starts up. Select [Maintenance]-[Maintenance Components] from the Action menu to start the maintenance screen.



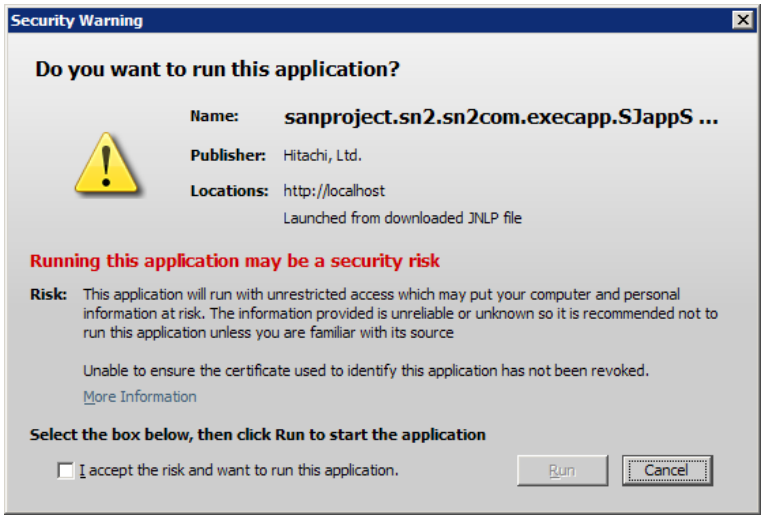
NOTE1: When Web Console is not ready, the screen below is displayed. Clicking [Start SVP] will start the maintenance screen.



NOTE2: Just after the micro-program exchanges, the maintenance screen starts without the main window of Web Console. If the maintenance screen is closed, the main window of Web Console starts automatically (If Web Console is not ready, the above screen appears until it is ready). If you click [Start SVP], the maintenance screen starts. When you close the maintenance screen, the main window of Web Console starts automatically. If you want to close the maintenance screen, change [View Mode] to [Modify Mode] and then select [Execute]-[Exit].



If the security warning as shown in the following figure is displayed, click [Run].



NOTE: Do not activate Web Console from the SVP by specifying the URL on Internet Explorer.

If the screen below is displayed, click [Allow].

2.3 Specifications Common to Functions of Web Console

Refer to “System Administrator Guide” for the specification of the commonness part of Web Console.

2.4 Before Using Web Console (You are requested to read this without fail)

The operation of Web Console is similar to the operation of Storage Navigator. Refer to Storage Navigator Conventions of “System Administrator Guide”.

2.4.1 Auto Account Lock

For the purpose of avoiding password brute force attack, the storage system has the function to lock the user account for 60 seconds if login to SVP fails three times in a row.
Two functions are available to avoid brute force attacks on user names and passwords. One of them locks the user account for a given length of time, and the other disables the user account.

- Account lock function
  When user login fails for a certain number of times in a row, the function locks the user account for a given length of time.

- Account disabling function
  When user login fails for the specified number of times in a row, the function disables the user account.

  NOTE: If all accounts registered to SVP are disabled, you cannot log into SVP (Authentication can be done in the authentication server).
  Prevent all accounts from being disabled.

This section describes the procedure for changing to the method that disables the account when login fails for the specified number of times, and the procedure for changing back to the original method.

- Procedure for switching to the account disabling function
  (1) Open the 'Run' window
  Right-click [Start], and then select [Run].

  (2) Enter the following command, and click [OK] to run the batch file.
  "setAccountLock_UnlockedByAdmin X"
  X: Specify a numerical value from 1 to 32 as the number of times login fails until the account is disabled.

  (3) After the batch file ended normally, the message "All process completed." appears.
  If it ends abnormally, the following message is output. Check the parameter.
  "Parameter is invalid.
  Confirm the execution parameter and try again."

  NOTE: If all accounts registered to SVP are disabled, you cannot log into SVP (Authentication can be done in the authentication server).
  Prevent all accounts from being disabled.

- Procedure for switching to the account lock function
  (1) Open the 'Run' window
  Right-click [Start], and then select [Run].

  (2) Enter the following command, and click [OK] to run the batch file.
  "setAccountLock_UnlockedByTimer"

  (3) After the batch file ended normally, the message "All process completed." appears.
  If it ends abnormally, the following message is output. Check the extra parameter.
  "Parameter is invalid.
  Confirm the execution parameter and try again."

2.5 Actions to Be Taken According to Result of Trouble shooting

Refer to Trouble shooting of “System Administrator Guide”.

NOTE: If the trouble is not solved in spite of it, collect a dump and restart the SVP.

	Failure	Recovery action	Remarks
1	All or part of the Web Console window is not displayed. Or it is displayed in white.	Put the mouse pointer on the part not displayed or the white part to display the Web Console window. If the problem persists, close the window and then open it again.	NOTE
2	The Web Console on the SVP cannot be started and error (10,6027) occurred.	A LAN cable may fall out. Please confirm the LAN cable. If the LAN cable falls out, connect it and reboot SVP.	
3	The Storage Navigator PC experiences an error (10,6027), when accessing the SVP from the Storage Navigator PC.	SVP (a Web server) cannot recognize the IP address of the Storage Navigator PC or the HUB. Check the following. For the connection between the equipment, refer to Figure 2-1. (1) Was the SVP restarted during the installation or maintenance work without the external LAN cable connection to the SVP? (2) Was the SVP restarted during the installation or maintenance work without turning on the power of the LAN equipment like the HUB or router connected to the SVP external LAN? Or, was the SVP restarted without turning on the power of the Storage Navigator PC when the PC is directly connected to the external LAN of the SVP? If one of the above is true, connect the external LAN cable of the SVP, turn on the power of the LAN equipment like the HUB or router, restart the SVP, and then access to the SVP (Web server) from the Storage Navigator PC.	
4	The wrong information is displayed on Storage Navigator regarding a product name, a vender name and a function name, etc.	Select [File] - [Refresh All] on Web Console, and then restart SVP.	

(To be continued)

(Continued from the preceding page)

	Failure	Recovery action	Remarks
5	Web Console doesn't start even if SVP is logged in remote desktop.	Web Console doesn't occasionally start while changing the storage system configuration until the change ends. Please wait until the change ends. Please confirm whether the storage system is operated from RAID Manager etc. when Web Console do not start for a long time. Open the Maintenance Utility (Sub Panel) window, and check whether communication error messages are displayed. If communication error messages are displayed, perform the LAN error recovery procedure (see (TRBL03-64-10)).	
6	The (20121 107024) error occurred on the main window of Storage Navigator on SVP.	Please respond to the message, and exit the Storage Navigator main window by pressing [Alt] and [F4] key.	
7	After the (20121 107024) error occurs on the main window of Storage Navigator on SVP, the (20121 107025) error is repeatedly displayed.	Please exit the Storage Navigator main window by pressing [Alt] and [F4] key.	
8	It's impossible to use maintenance PC's directory if SVP is logged in remote desktop. • Installing License Key • Downloading Audit Log • Downloading Reports • Exporting displayed information etc.	Please use SVP's directory to import or export files. If you install license key, please move license key's file to SVP's directory and use the file for installing. If you download a file, please download to SVP's directory and move the file for need.	
9	The (20121 107096) error occurs repeatedly on the main window of Storage Navigator on SVP.	Please exit the Storage Navigator main window by pressing [Alt] and [F4] keys.	
10	After a remote desktop connection to SVP is established, an error code is displayed in the 'Wait for the start of Storage Management Service' window.	See the "Storage Navigator Messages Guide" and take the necessary action.	
11	Version update notification dialog of Flash Player pops up.	Do not update Flash Player. Doing so might cause a login failure to SVP, startup failure of Storage Navigator, or other problems.	

(To be continued)

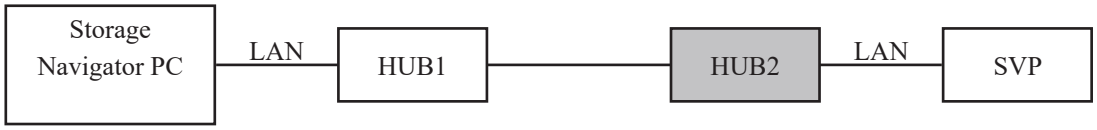
(Continued from the preceding page)

	Failure	Recovery action	Remarks
12	The (20020-108000) error occurs on the main window of Web Console on the SVP.	When the maintenance screen is starting up and the Web Console window is activated, close the maintenance screen once. Then start the maintenance screen again by following the procedure in "2.2 Procedure for Activation Using SVP". If the maintenance screen is not started, log off the SVP and log on it again. Then, before the Web Console window is opened, click [Start SVP] in the Wait for the start of Storage Management Service window to open the maintenance screen.	
13	When opening the secondary windows in the Internet Explorer, the following error message is displayed: "Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item."	Complete the following steps to set up the Internet Explorer. (1) Register the URL of the SVP to be connected to [Trusted sites] on the internet options window. (2) Click [Safety]-[SmartScreen Filter]-[Turn Off SmartScreen Filter ...] from the menu bar in the Internet Explorer. (3) Click [Turn Off SmartScreen Filter], and then click [OK]. (4) Restart the Internet Explorer, and then open the secondary window again.	
14	The following error occurred during the operation in the Web Console window. • 00002-009000	Other administrative clients might be setting Storage Navigator. Check that all the setting windows of Storage Navigator are closed, and then operate Web Console again. In the case other than the above, restart the SVP. After that, operate Web Console.	

When restart SVP by the state that LAN between SVP and Storage Navigator PC is not connected to justly, there is the case that gets impossible to start Storage Navigator ((10,6027) error occurred).

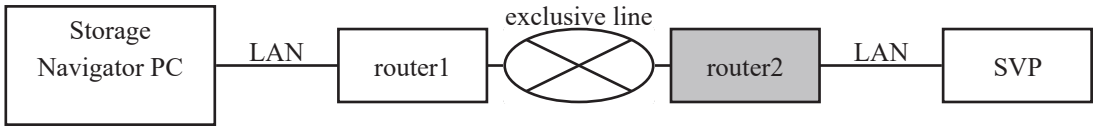
Figure 2-1 Connection Example of LAN

Case1:



Recovery Action: In this case, please restart of SVP by a state of On with a power supply of HUB2 by all means.

Case2:



Recovery Action: In this case, please restart of SVP by a state of On with a power supply of router2 by all means.

Case3:

Recovery Action: In this case, please restart of SVP by a state of On with a power supply of Storage Navigator PC by all means.

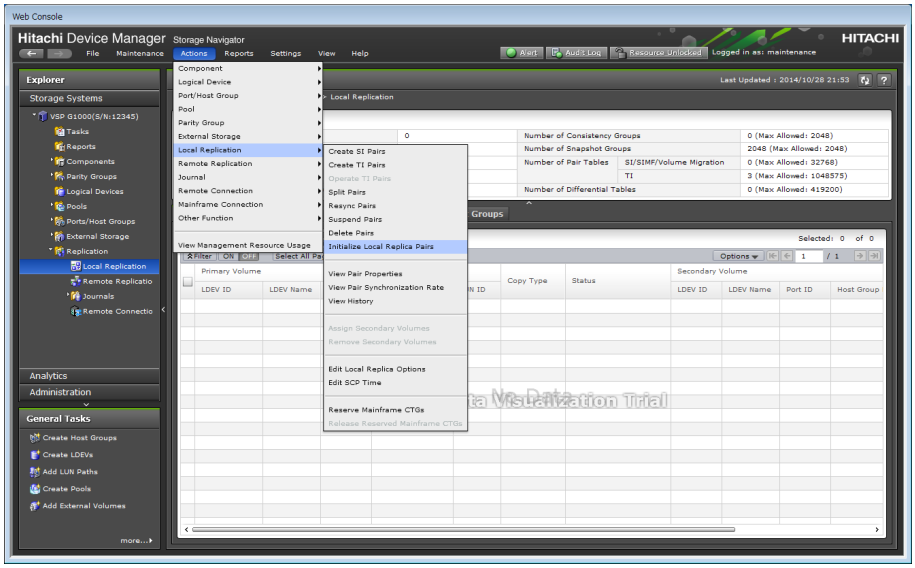
3. Storage System Management Function

> **⚠ CAUTION**
>
> - Before starting the following procedures, be sure to contact the Technical Support Division and follow the judgement as required.
> - The following procedures can be performed only by Web Console of the Maintenance PC.

3.1 Local Replication

Select [Replication]-[Local Replication] at the left of the main window to open Local Replication window.

3.1.1 Initialize Local Replica Pairs



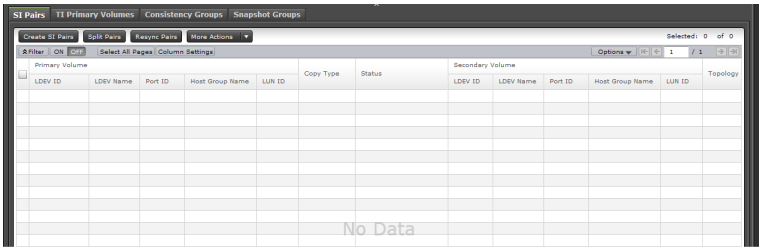
1. Select [Actions]-[Local Replication]-[Initialize Local Replica Pairs] at the top of the main window.
   - Initialize Local Replica Pairs
     It deletes all the pairs that have been formed by ShadowImage / ShadowImage for Mainframe / Volume Migration / FlashCopy (R) V2 / FlashCopy (R) SE / Thin Image and sets the pair status of the volume to Simplex (to SMPL, in the case of ShadowImage).
     Refer to the "Initialization Procedure for ShadowImage" (TRBL06-150) for the Initialize procedure and notes.
     To operate the 'Initialize Local Replica Pairs', an entry of a password is required. For the password, refer to the Technical Support Division.

     NOTE1: When the Initialize Local Replica Pairs is performed, not only pairs formed by ShadowImage for Mainframe, but also pairs formed by ShadowImage / Volume Migration / FlashCopy (R) V2 / FlashCopy (R) SE / Thin Image are deleted.

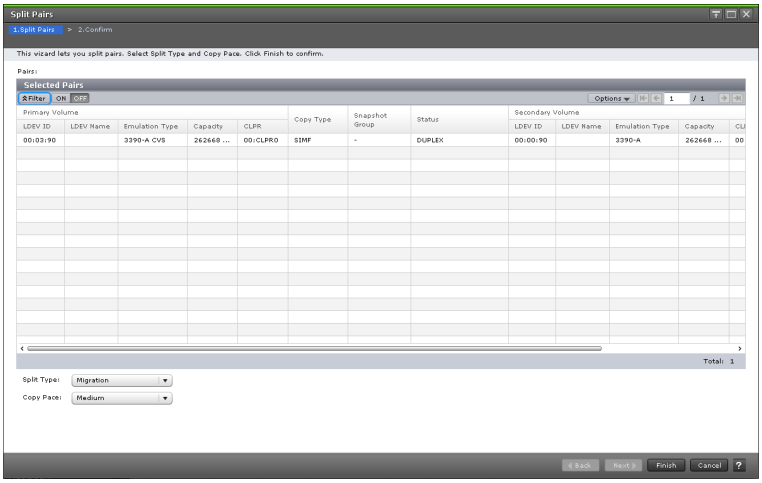
     NOTE2: Perform the operation only when it is directed by the Technical Support Division.

3.1.2 Split Pairs window

Select [SI Pairs] at the application area to activate.
Select a volume in Duplex status.
Select [Split Pairs] to activate 'Split Pairs' window.
(If selecting volumes other than a volume in Duplex status, the operation fails.)

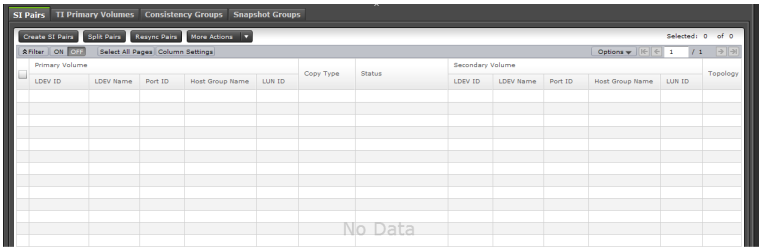


1. [Split Type] drop-down list
   Select migration VOL and open the Split Pairs window.
   The [Split Type] drop-down list is fixed in [Migration].
   - Migration (split type)
     Split pair operation by Migration is split type for exclusive use of Migration VOL.
     It execute data migration by the migration VOL.

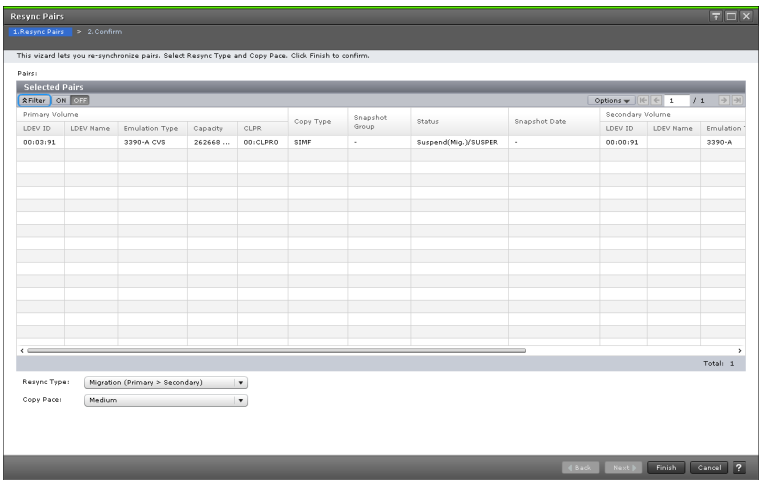


3.1.3 Resync Pairs window

Select [SI Pairs] at the application area to activate.
Select a volume in Suspend (Mig.)/SUSPER status.
Select [Resync Pairs] to activate Resync Pairs window.
(If selecting volumes other than a volume in Suspend (Mig.)/SUSPER status, the operation fails.)

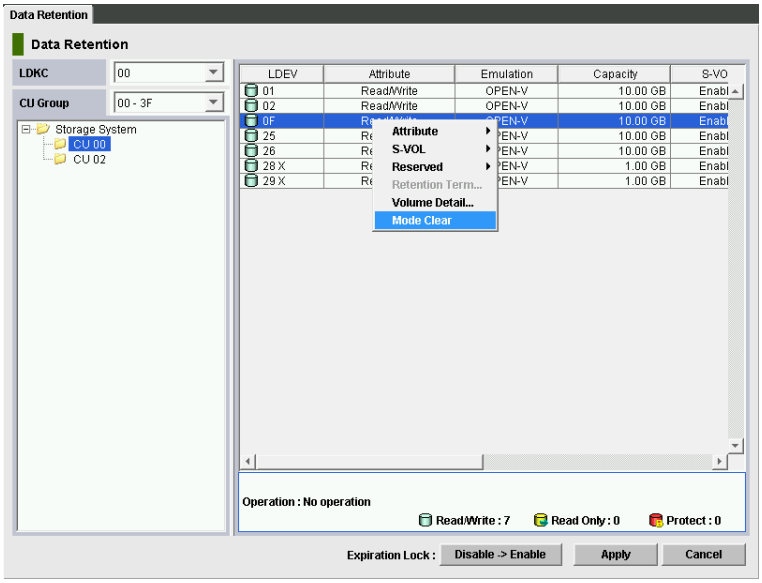


1. [Resync Type] drop-down list
   Select Migration VOL and open the Resync Pairs window.
   The [Resync Type] drop-down list is fixed in [Migration (Primary > Secondary)].
   - Migration (Primary > Secondary)
     Resynchronize pair operation by Migration is Resynchronize Type for exclusive use of Migration VOL. The copy direction for a normal resync operation is S-VOL to T-VOL, with data migration by the migration VOL.



3.2 Data Retention Utility

Select [Actions]-[Other Function]-[Data Retention...].



1. Canceling the mode attribute
   In the Data Retention window, when the operation for changing the access attribute is performed, [Mode Clear] is displayed in a pop-up menu.
   Use this menu when you want to cancel the attribute, Zer and Inv.

   NOTE: For the attributes, Zer and Inv, refer to “Provisioning Guide for Open Systems”.

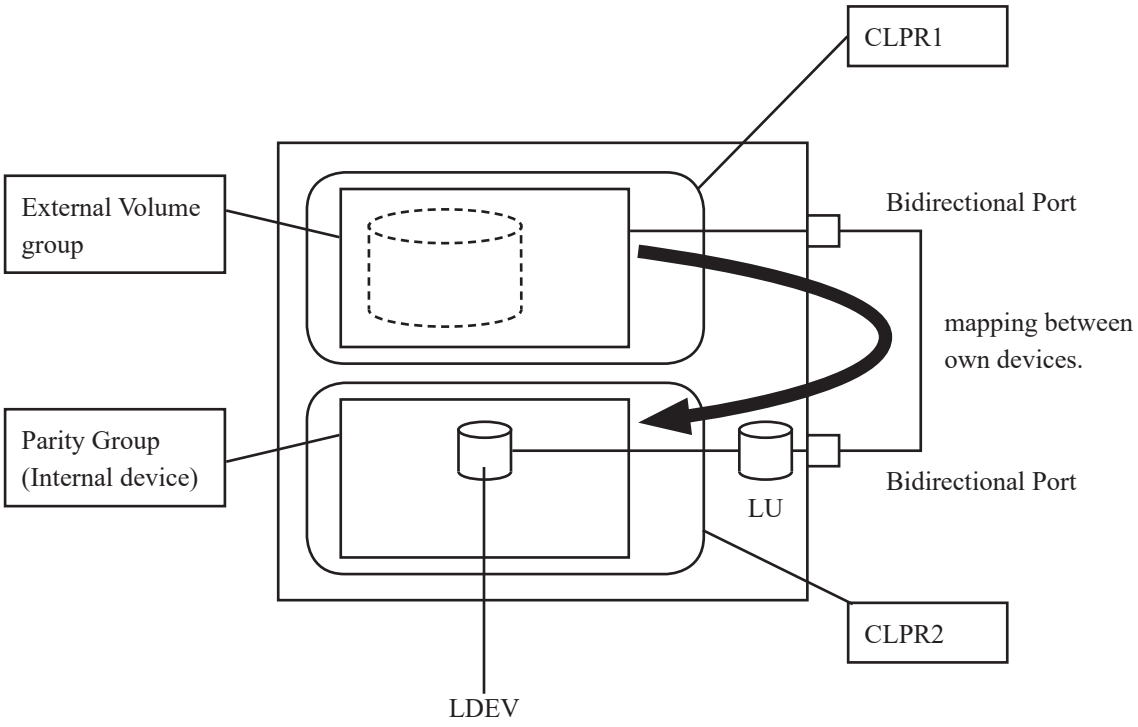
3.3 Universal Volume Manager

3.3.1 Mapping its own volumes

Provided that the External Volume is its own volume, it allows to be mapped as an external storage device. But every LDEV of the external group must be allocated to another CLPR that is different from one which is allocated to some internal LDEVs.

It is shown for example when mapping between own LU and own external group as following.

For example when mapping between own external group

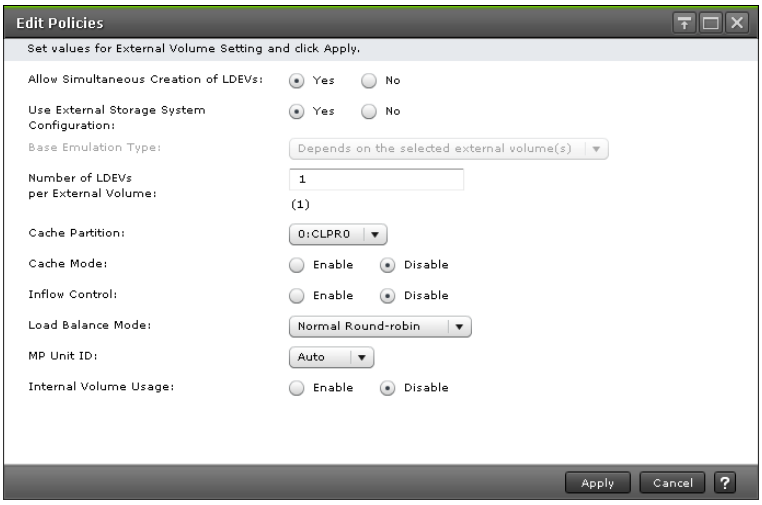


3.3.2 Previous arrangement for mapping its own volumes

The procedure for mapping its own volumes is described below:

1. Login to SVP.

2. Select [Actions]-[External Storage]-[Edit Policies] on the web console to activate Edit Policies window.



3. Select [Enable] on [Internal Volume Usage] item, then click [Apply].

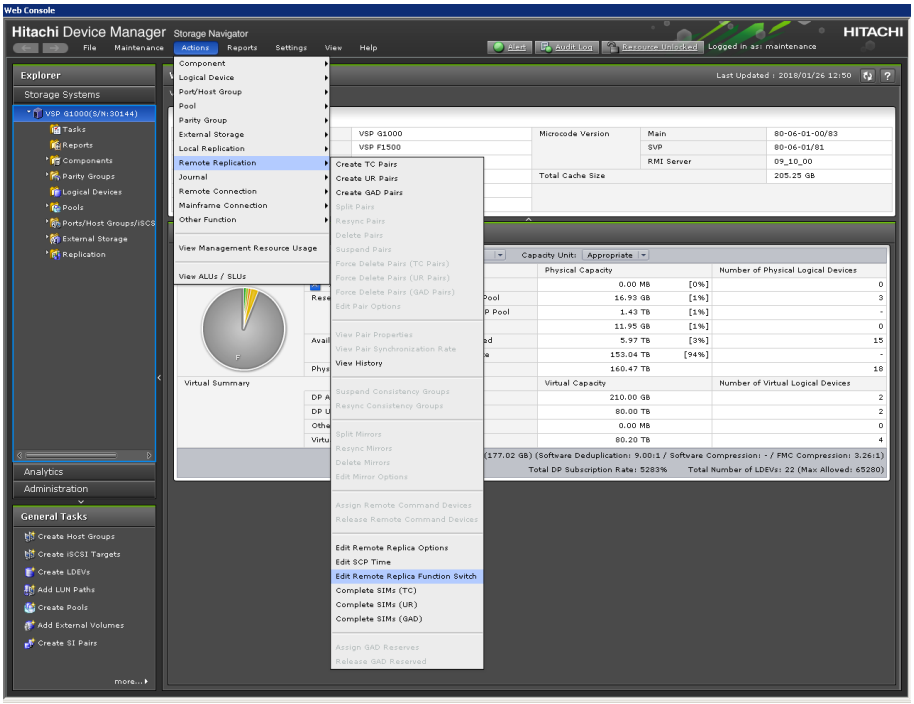
3.3.3 Note for mapping its own volumes

Mapping its own volumes could be done by SVP only.
The external volumes are available for data migration only.

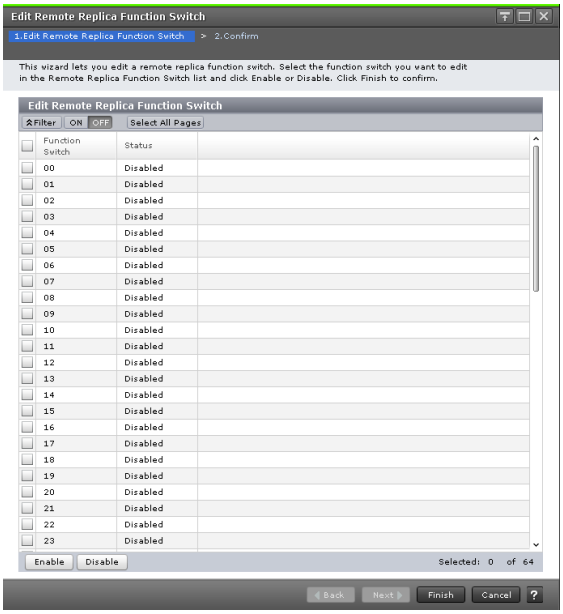
3.4 Remote Replication

3.4.1 Remote Replica Function Switch

Select [Actions]-[Remote Replication]-[Edit Remote Replica Function Switch] menu at the top of the Storage Navigator main window to activate Edit Remote Replica Function Switch window.



3.4.1.1 Edit Remote Replica Function Switch



In Edit Remote Replica Function Switch window, select function switch to be changed. Click [Enable], [Disable].
When click [Finish], confirmation window is displayed. Check the task name, and click [Apply].

NOTE: Perform the operation only when it is directed by the Technical Support Division.

NOTE: Please refer to "3.4.1.2 Remote Copy Function Switch" for the function allocated in each switch.

3.4.1.2 Remote Copy Function Switch

The function allocated in each switch is as follows.

Switch#	Contents
7	Function switch for TC-MF. Prevents the SSB of F/M = FB from being reported to the host.
11	Function switch for TC/TC-MF. Allows pair creation to operate at a copy pace of up to 32 Tracks if 15 Tracks is specified for the copy pace of the pair creation. However, for OPEN-V, the copy pace becomes 4 Tracks.
12	Function switch for TC-MF. Sets the CFW Data option to Only M-VOL when pair creation or pair resynchronization is performed from the mainframe host or RAID Manager.
15	Function switch for TC/TC-MF/GAD/UR/UR-MF. When Switch #17 is enabled, you can use Switch #15 to change the threshold value of path failure. Use Switch #15 for the storage system to which a remote connection is added (the storage system that has the port with the initiator attribute). Change the threshold value of path failure by using Switch #15 in combination with Switch #20 (see "Setting the threshold value of path failure:").
17	Function switch for TC/TC-MF/GAD/UR/UR-MF. When the occurrence count of LIP, RSCN, or TOV of the path between MCU and PCU, where temporary path failures are repeated, exceeds the threshold value, the failed logical path of the port can be blocked by Switch #17. Blocking the failed path prevents deterioration of the remote copy performance which is caused by use of the failed path. Use Switch #17 for the storage system to which a remote connection is added (the storage system that has the port with the initiator attribute). The threshold value can be changed by using Switch #15 and Switch #20 (see "Setting the threshold value of path failure:").
18	Function switch for TC/TC-MF/GAD. When Switch #17 is enabled, the occurrence count of fibre link failures is included in the count for the threshold to block a path by enabling Switch #18. Use Switch #18 for the storage system to which a remote connection is added (the storage system that has the port with the initiator attribute).
20	Function switch for TC/TC-MF/GAD/UR/UR-MF. When Switch #17 is enabled, you can use Switch #20 to change the threshold value of path failure. Use Switch #20 for the storage system to which a remote connection is added (the storage system that has the port with the initiator attribute). Change the threshold value of path failure by using Switch #20 in combination with Switch #15 (see "Setting the threshold value of path failure:").
21	Function switch for TC-MF. Sets the copy pace to 3 Tracks when pair creation or pair resynchronization is performed with the PPRC command (DKC Emulation = 2107).

(To be continued)

(Continued from preceding page)

Switch#	Contents
33	Function switch for TC/TC-MF/GAD. In the cases that the PDCM function of the McData ES3232 fibre channel switch is used on the MCU-RCU path, when the login response is late, the path status can be changed to non-normal by Switch # 33.
36	Function switch for TC-MF/UR-MF. For TC-MF pairs, use Switch #36 to set the time stamp option to Enable when performing pair creation or pair resynchronization with GDPS or RAID Manager. In the TC-MF/UR-MF cascade configuration, the consistency of UR-MF is kept by setting the time stamp option of TC-MF pairs to Enable. However, for TC-MF pairs, when pair creation or pair resynchronization is performed with GDPS or RAID Manager, the time stamp option cannot be set to Enable. In this case, use Switch #36 to enable the option.
40, 41, 42	Function switch for TC/TC-MF/GAD/UR/UR-MF. If the RIO response is delayed on a specific path between MCU and RCU, when the occurrence count of the delayed RIO response exceeds the threshold value, blocking the logical path due to excess of the threshold value prevents deterioration of the remote copy performance which is caused by use of the path on which the RIO response is delayed. Use Switch #40, Switch #41, and Switch #42 for the storage system to which a remote connection is added (the storage system that has the port with the initiator attribute). Change the time of RIO response that is counted as a delay by using Switch #40, Switch #41, and Switch #42 in combination (see “Setting the threshold value of RIO repose delay:”).
43	Function switch for TC/TC-MF/GAD/UR/UR-MF. A path can be blocked by using Switch #43 even if the number of paths falls below the minimum allowable number when Switch #17 or a combination of Switch #40, Switch #41, and Switch #42 works to block the path. If the number of normal paths falls below the minimum allowable number, remote copy pairs are suspended due to the failure. Use Switch #43 when you want to prioritize the response time to the host over keeping the pair status of the remote copy. Use Switch #43 for the storage system to which a remote connection is added (the storage system that has the port with the initiator attribute).

Setting the threshold value of path failure:

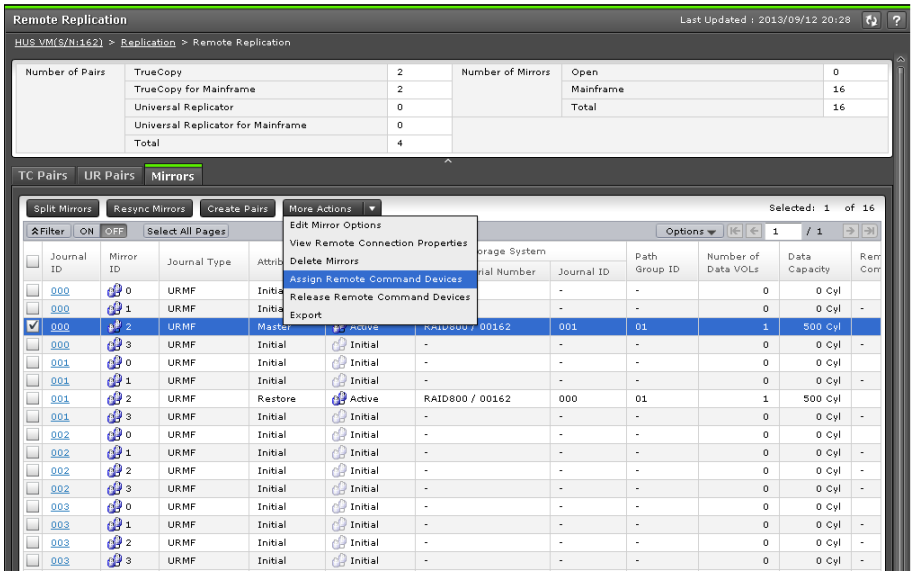
Function switch			Threshold value of path failure for blockade		
Switch #17	Switch #15	Switch #20	LIP	RSCN	TOV
Enable	Disable	Disable	15 times	15 times	5 times
	Disable	Enable	10 times	10 times	4 times
	Enable	Disable	7 times	7 times	3 times
	Enable	Enable	3 times	3 times	2 times

Setting the threshold value of RIO repose delay:

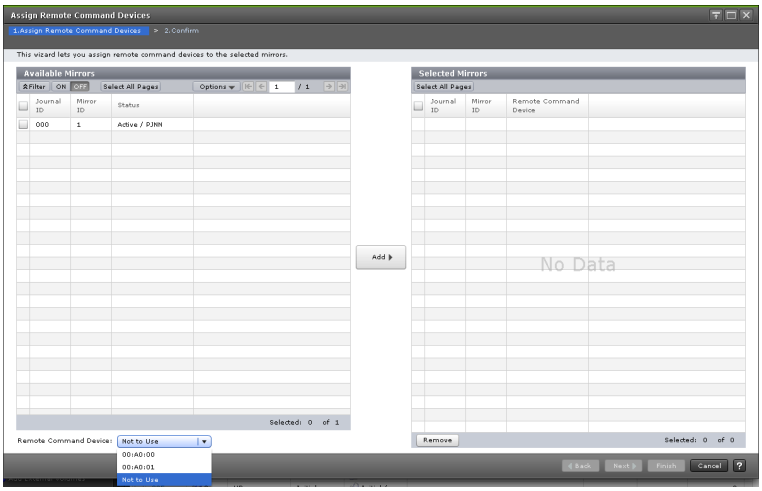
Function switch			Threshold value of RIO response delay for path blockade	
Switch #40	Switch #41	Switch #42	Time of RIO response that is counted as a delay	Threshold value for path blockade
Disable	Disable	Enable	10 sec	100 times/10 minutes
Disable	Enable	Disable	5 sec	
Disable	Enable	Enable	2.5 sec	
Enable	Disable	Disable	1 sec	
Enable	Disable	Enable	0.5 sec	
Enable	Enable	Disable	0.25 sec	
Enable	Enable	Enable	0.1 sec	

3.4.2 Assign Remote Command Devices window

Select [Mirrors] at the application area of 'Remote Replication' window.
Select mirrors in Initial, Active, Halt, Stopped, Hold, Holding, or Hold (Failure) state.
Select [More Action]-[Assign Remote Command Devices] to activate Assign Remote Command Devices window. (When mirrors other than above state are selected, the operation fails.)
Remote Command Devices can be assigned to mirror in Initial state only when mirror ID is 0.

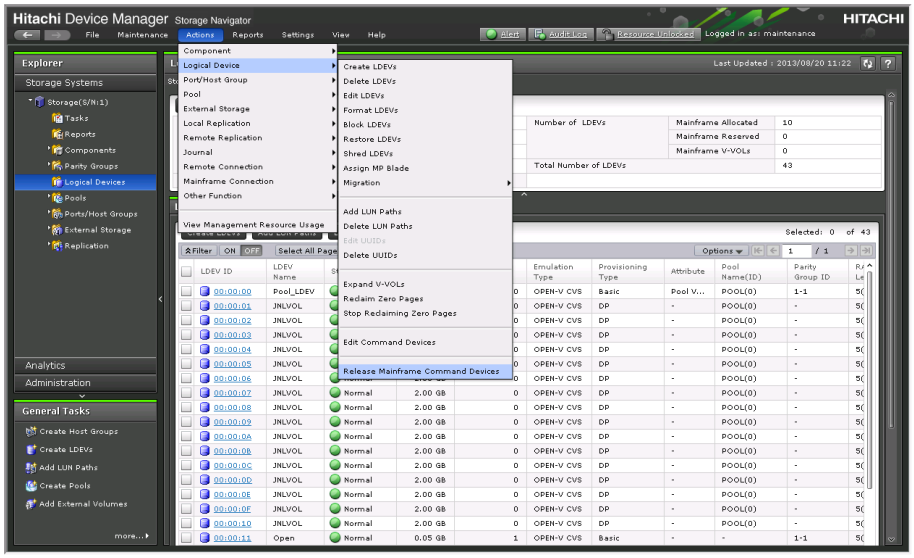


1. [Remote Command Device] drop-down list.
   When there are any LDEVs to which remote command devices can be assigned, [LEDV#] and [Not to Use] are displayed in the drop-down list.
   - [LDEV#]
     Specify LDEV# when assigning remote command devices.
   - [Not to Use]
     Select [Not to Use] when not using remote command devices.



3.5 Release Mainframe Command Devices

The command device for Business Continuity Manager is deleted in the lump.
Use this menu when you want to delete command device for Business Continuity Manager after removed the Business Continuity Manager.



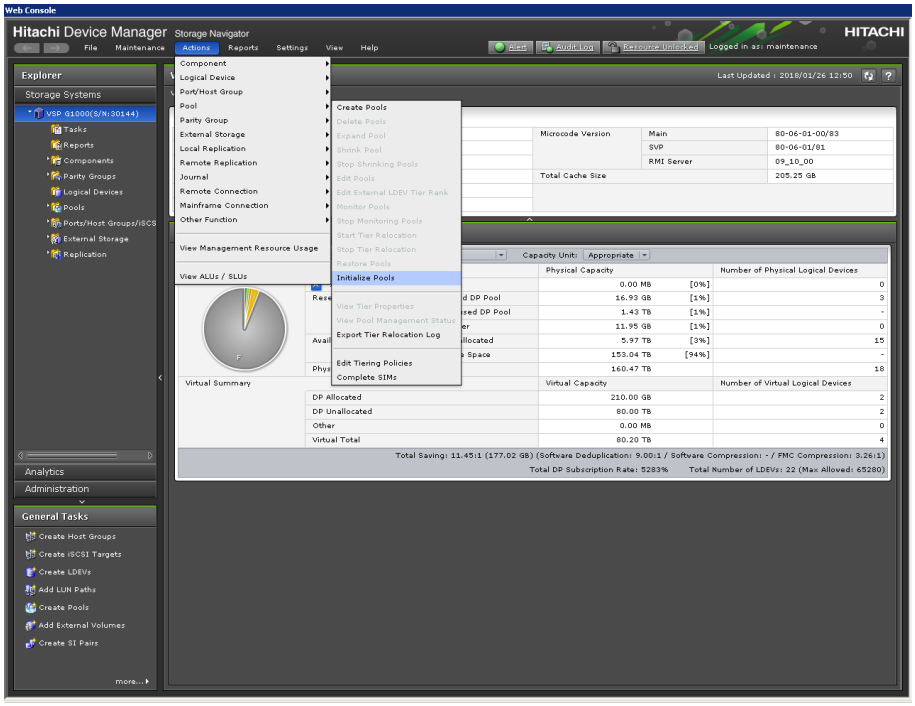
1. Select [Actions]-[Logical Device]-[Release Mainframe Command Devices] at the top of the main window.

   NOTE1: Command devices for Business Continuity Manager are deleted by this operation. But when external volumes used by Universal Volume Manager are defined as command devices, they are not deleted.

   NOTE2: To find the command device for Business Continuity Manager, use the Logical Device window. For more information about the Logical Device window, see “System Administrator Guide”.

   NOTE3: By this operation, when Command devices for Business Continuity Manager are deleted, confirm that Shared memory which is required in TrueCopy for Mainframe has been installed.

3.6 Dynamic Provisioning/Dynamic Tiering/active flash/Dynamic Provisioning for Mainframe/Dynamic Tiering for Mainframe/active flash for Mainframe



1. Initialize Pools
   Select [Actions]-[Pool]-[Initialize Pools] at the top of the main window.

   The Virtual Volumes of Dynamic Provisioning / Dynamic Tiering / active flash / Dynamic Provisioning for Mainframe / Dynamic Tiering for Mainframe /active flash for Mainframe (DP-VOL) is blockaded. And the pool of all Dynamic Provisioning / Dynamic Tiering / active flash / Dynamic Provisioning for Mainframe / Dynamic Tiering for Mainframe / active flash for Mainframe / Thin Image is blockaded. Refer to the “Initialization Procedure for Pool” (TRBL13-210) for the Initialize procedure and notes. To operate the ‘Initialize Pools’, an entry of a password is required. For the password, refer to the Technical Support Division.

NOTE1: The pool of all Dynamic Provisioning / Dynamic Tiering / active flash / Dynamic Provisioning for Mainframe / Dynamic Tiering for Mainframe / active flash for Mainframe / Thin Image is blockaded.
When the pool is blocked, the information of the volumes associated with the pool is not displayed in the Pools window. After the pool restoration is performed, the information is displayed.

NOTE2: In the case [TrueCopy / Universal Replicator / ShadowImage / Volume Migration / XRC / FlashCopy (R) V2 / FlashCopy (R) SE] use virtual volumes of Dynamic Provisioning / Dynamic Tiering / active flash / Dynamic Provisioning for Mainframe / Dynamic Tiering for Mainframe / active flash for Mainframe, delete all [TrueCopy / Universal Replicator / ShadowImage / Volume Migration / XRC / FlashCopy (R) V2 / FlashCopy (R) SE] pairs that use the virtual volumes before performing Initialize.
After Initialize completes, create [TrueCopy / Universal Replicator / ShadowImage / Volume Migration / XRC / FlashCopy (R) V2 / FlashCopy (R) SE] pairs again.
During initialize, don't create [TrueCopy / Universal Replicator / ShadowImage / Volume Migration / XRC / FlashCopy (R) V2 / FlashCopy (R) SE] pairs with virtual volumes of Dynamic Provisioning / Dynamic Tiering / active flash / Dynamic Provisioning for Mainframe / Dynamic Tiering for Mainframe / active flash for Mainframe. In the case those pairs, initialize and paircreate operation may fail.

NOTE3: Delete all Thin Image pairs before performing Initialize.
After Initialize completes, create Thin Image pairs again.
During Initialize, don't create Thin Image pairs. In the case create Thin Image pairs, initialize and paircreate operation may fail.

NOTE4: Stop the LDEV format on the LDEV on which the DP-VOL with [Compression] or [Deduplication and Compression] of capacity saving enabled exists in the Storage System before performing Initialize Pools. If Initialize Pools is performed without stopping the LDEV format, the initialization may fail.

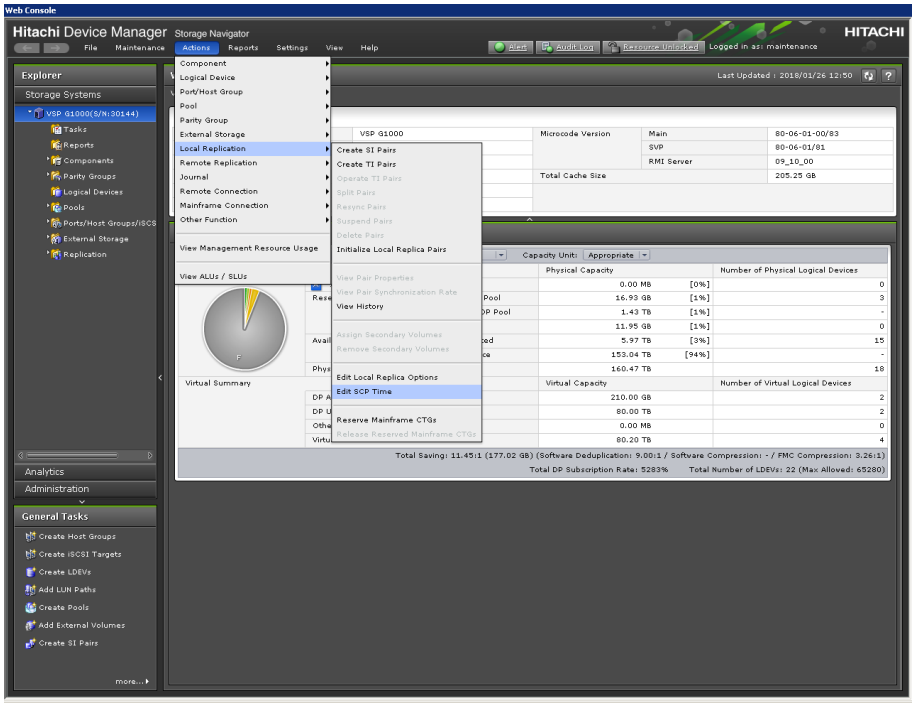
NOTE5: Do not execute the maintenance of Dynamic Provisioning until the pool restores normally after executing Initialize.

NOTE6: Procedure to recover DP-VOL:
Please recover the pool of Dynamic Provisioning / Dynamic Tiering / active flash / Dynamic Provisioning for Mainframe / Dynamic Tiering for Mainframe referring / active flash for Mainframe to "Provisioning Guide for Open Systems" or "Provisioning Guide for Mainframe Systems".
DP-VOL recovers by recovering the pool of Dynamic Provisioning / Dynamic Tiering / active flash / Dynamic Provisioning for Mainframe / Dynamic Tiering for Mainframe / active flash for Mainframe.

NOTE7: Perform the operation only when it is directed by the Technical Support Division.

3.7 Change SCP Time

Select [Actions]-[Local Replication]-[Edit SCP Time] at the top of the main window to activate Edit SCP Time window.



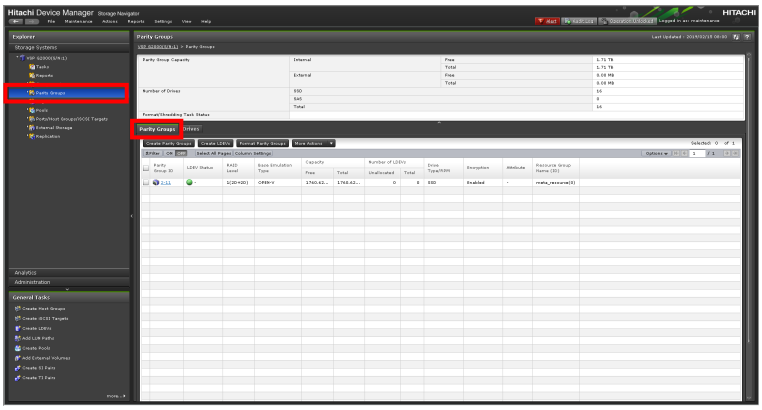
1. Changing the SCP Time
   (1) In the Edit SCP Time window, select all CUs to which the SCP Time exceeding 600 seconds is set, and select click [Change SCP Time] button.
   (2) Change SCP Time window will appear.
   (3) In the Change SCP Time window, enter 120 seconds (default value) and select click [OK].
   (4) Click [Finish] on the Edit SCP Time window.
   (5) In the Confirm window, click [Apply].

3.8 Connecting to the Host

3.8.1 Creating Parity Groups

NOTICE: When running the maintenance operation in the other window, the part status might be displayed differently from the actual status. (Example: The Drives during the addition are displayed as the [Blocked] status.).
In that case, complete the maintenance operation running in the other window, and then refresh the display information by clicking [Refresh] ( ).
While running the maintenance operation or the maintenance processing, the system lock status is displayed as [Locked].

1. Select [Storage Systems]-[Parity Groups]. Click the [Parity Groups] tab.

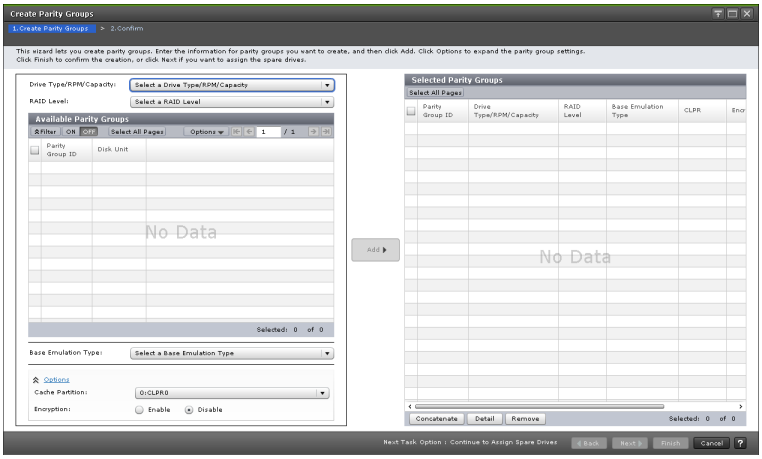


Item	Description
Parity Group ID	Number of the parity groups.
LDEV Status	A status of all the devices in the parity group.
RAID Level	RAID level specified.
Base Emulation Type	Displays the Base Emulation Type.
Capacity-Free	Available capacity of the parity group.
Capacity-Total	Entire capacity of the parity group.
Number of LDEVs-Unallocated	The number of the logical devices in the parity group that the host cannot access.
Number of LDEVs-Total	The number of the logical devices in the parity group.
Drive Type/Interface/RPM	Drive type, interface and round-per-minute (RPM) of the drive in the parity group.
Encryption	Encryption status of a parity group.
Attribute	An Attribute of the parity group.
Resource Group Name (ID)	Displays the name and ID of the resource group where the parity group is assigned.
Virtual Storage Machine	Displays the model and serial number of the virtual storage machine.

2. Click [Create Parity Groups].

3. Enter the information (Drive Type/Interface/RPM/Capacity, RAID Level, Available Parity Groups, and Base Emulation Type) of the parity group to be created and click [Add]. Click [Options] to expand the parity group settings. Click [Next].

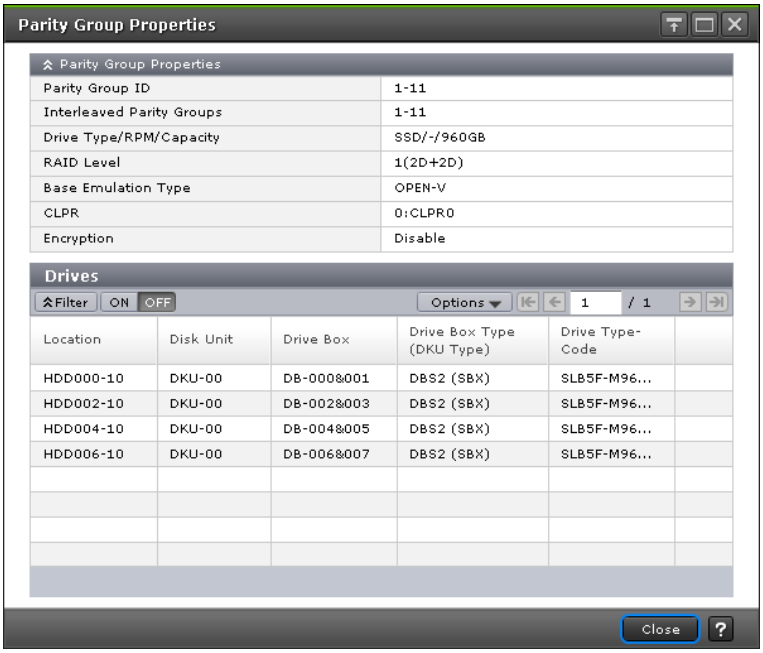
   NOTE: When you want to complete the parity group creation, click [Finish].



Item	Description
Drive Type/Interface/RPM/ Capacity	Select a Drive Type/Interface/RPM/Capacity.
RAID Level	Select a RAID Level.
Available Parity Groups	Displays the available parity group. • Parity Group ID: Displays the parity group ID. • Disk Unit: Displays the disk unit.
Base Emulation Type	Select a Base Emulation Type.
Cache Partition	Select a CLPR number which is displayed as ID:CLPR.
Encryption	Specify if encrypted parity groups are created. • Enable: Encrypted parity groups are created. • Disable: Non-encrypted parity groups are created.
[Add] button	The set content is added to the Selected Parity Groups table on the right side.
[Concatenate] button	Concatenates the parity groups selected in the Selected Parity Groups table on the right side.
[Detail] button	Opens the Parity Group Properties window (see WEBCON03-170) that displays the details of the parity group selected in the Selected Parity Groups table on the right side.
[Remove] button	Removes the parity groups selected in the Selected Parity Groups table on the right side.
[Next Task Option]	Click [Next] button to go to the task setting window, which is indicated in Task Next Option.

(To be continued)

Parity Group Properties window



[Parity Group Properties] summary

Item	Description
Parity Group ID	Display the parity group ID.
Interleaved Parity Groups	Display the interleaved parity groups.
Drive Type/Interface/RPM/ Capacity	Display the drive type/interface/RPM/capacity.
RAID Level	Display the RAID level.
Base Emulation Type	Display the base emulation type.
CLPR	Display the CLPR. It is displayed as ID:CLPR.
Encryption	Display the status of encryption.

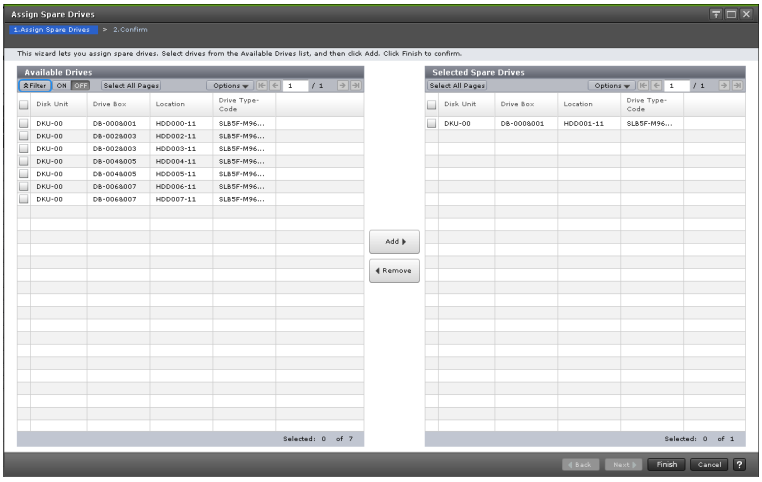
[Drives] table

Item	Description
Location	Displays the location of the drive box.
Disk Unit	Displays the disk unit.
Drive Box	Displays the drive box number.
Drive Box Type (DKU Type)	Displays the drive box type and DKU type.
Drive Type-Code	Displays the drive type code.

4. The Assign Spare Drives window appears.
   Select a spare drive from the Available Drives list, and then click [Add].
   The selected spare drive was added to the Selected Spare Drives list. Click [Finish].

   NOTE: You can also assign the spare drives in the following procedure (see "3.9.1.3 Allocating/Deleting Spare Drives").
   1. Select [Storage system]-[Parity Groups].
   2. Click [Assign Spare Drives] in the [Drives] tab.

   NOTE: If the capacity of a drive exceeds the capacity of a spare in the Storage System, an error message appears.



[Available Drives] table and [Selected Spare Drives] table

Item	Description
Disk Unit	Displays the disk unit.
Drive Box	Displays the drive box number.
Location	Displays the location of the drive box.
Drive Type-Code	Displays the drive type code.
[Add] button	Adds one or more drives selected in the Available Drives table to the Selected Spare Drives table.
[Remove] button	Removes one or more selected drives from the Selected Spare Drives table, and relocates drives to the Available Drives table.

5. Check the set contents in the Confirm window and enter a task name in [Task Name].

6. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

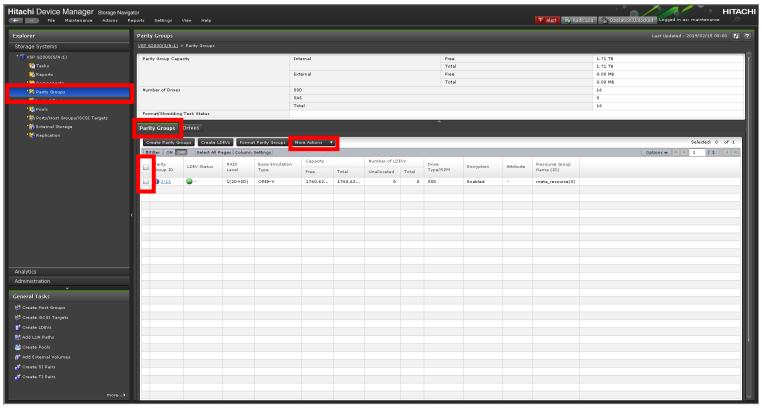
7. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.
   After the task is completed, you can perform the procedure of “3.8.2 Creating LDEVs and Adding LUN Paths”.

   NOTE: To change the accelerated compression setting, perform the procedure in “3.8.1.1 Changing the accelerated compression setting”.

3.8.1.1 Changing the accelerated compression setting

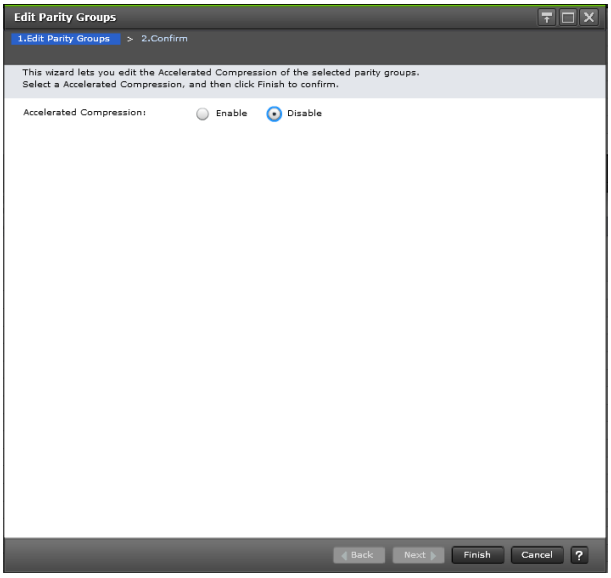
Select a target parity group and change the accelerated compression setting as follows:

1. From the [Storage Systems] tree, select [Parity Groups], and click the [Parity Groups] tab.



2. Check the checkbox for the parity group for which you want to change the accelerated compression setting, and select [More Actions]-[Edit Parity Groups].

3. Select [Enable] or [Disable] for [Accelerated Compression].
   If you want to enable the accelerated compression for the parity group, select [Enable].
   If you want to disable it, select [Disable].



4. Check the set content, and click [Finish].

5. Check the set content in the Confirm window and enter a task name in [Task Name].

6. Click [Apply] to apply the setting to the storage system. Tasks are stored in the task queue and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

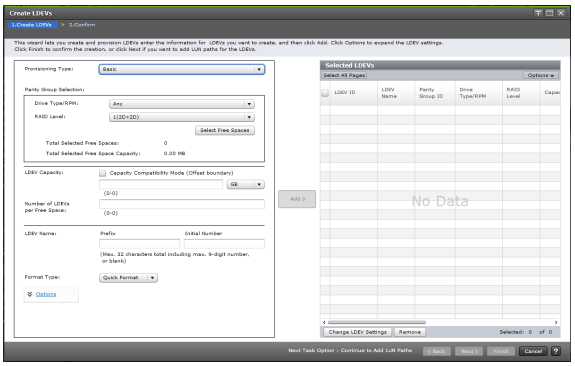
7. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.8.2 Creating LDEVs and Adding LUN Paths

1. In the Web Console window, select [Storage Systems]-[Parity Groups].

2. Click [Create LDEVs].

3. The Create LDEVs window appears. Enter the information for LDEVs you want to create, and then click [Add]. Click [Options] to expand the LDEV settings. Click [Next].



NOTE: Specify a format type other than [No Format].

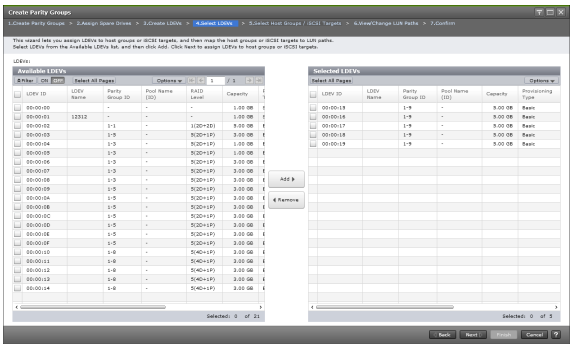
NOTE: When clicking [Options], you can set up the detailed LDEV information.

NOTE: You can also create the LDEV in the following procedure (see "3.9.3 Managing Logical Device").
1. Select [Storage Systems]-[Logical Device].
2. Click [Create LDEVs in the LDEVs] tab.

Item	Description
Provisioning Type	Select the type of LDEV. Basic: Internal volume. Dynamic Provisioning: DP-VOL. External: External volume. Snapshot: Thin Image volume. ALU: LDEV of the ALU attribution.
Drive Type/Interface/RPM	Select the drive type, interface and RPM.
RAID Level	Select the RAID level. External Storage is selected from the Drive Type/Interface/RPM field, a hyphen (-) appears.
Select Free Spaces	Displays the Select Free Spaces window.
Total Selected Free Spaces	Displays the number of the selected free spaces.
Total Selected Free Space Capacity	Displays the total capacity of the free spaces.

Item	Description
LDEV Capacity	• Capacity Compatibility Mode (Offset boundary): If you want to offset the specified LDEV capacity by boundary, set the Capacity Compatibility Mode (Offset boundary) to ON. • Input area: Specify the LDEV capacity to create in a free space, a pool, or an external volume. Detailed calculation of the LDEV capacity differs depending on the specification of the unit. For details, see “Provisioning Guide for Open Systems”.
Number of LDEVs per Free Space, Number of LDEVs, or Number of LDEVs per External Volume	Specify the number of LDEVs to create in a free space, pool, or the external volume.
LDEV Name	LDEV name. Specify the prefix characters and the initial number. • Prefix: A fixed character string. • Initial Number: The initial number of the LDEV name. Specify the initial number according to the examples below. You can specify up to 32 characters total. Example: • 1: Up to 9 numbers are added (1, 2, 3... 9). • 08: Up to 92 numbers are added (08, 09, 10...99). • 23: Up to 77 numbers are added (23, 24, 25...99). • 098: Up to 902 numbers are added (098, 099,100... 999).
Format Type	Specify the format type. This appears when an internal or external volume is used. Quick Format: Quick formatting is the default format type. You cannot select this when the provisioning type is something other than the internal volume. Normal Format: Normal formatting. Parity Group Format: Format the parity group. You can select this when no LDEV exists in the parity group. No Format: Volumes are not formatted.
Initial LDEV ID	Specify the LDEV ID. LDKC is fixed to 00. Default of CU and DEV is 00:00. For creating multiple LDEVs, select the interval of the assigned LDEV ID from the Interval list.
View LDEV IDs	Displays the View LDEV IDs windows.
MP Unit ID	Specify the MP unit you want to assign to the LDEV. Select Auto or an arbitrary ID. The default is Auto. You can select an ID of MPU-10 or MPU-20. If automatic assignment is enabled for one or more MPs, you can also select Auto. If Auto is enabled, the default is Auto. If Auto is disabled, the default is the lowest number of the MP unit.
T10 PI	Sets the T10 PI attribute of the LDEV. [Enabled]: Enables the T10 PI attribute of the LDEV. [Disabled]: Disables the T10 PI attribute of the LDEV. This function can be set when any of [Basic], [DP], and [Snapshot] is selected in [Provisioning Type].

4. The Select LDEVs window appears.
   Select a LDEV from the [Available LDEVs] list, and then click [Add].
   The selected LDEV was added to the [Selected LDEVs] list. Click [Next].



[Available LDEVs] table and [Selected LDEVs] table

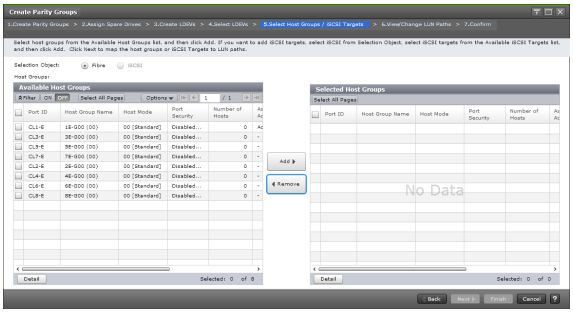
Item	Description
LDEV ID	LDEV identifiers. LDEV IDs may be appear for undefined LDEVs. A hyphen appearing in columns to the right of the LDEV ID and LDEV name (for example, Parity Group ID, Pool Name ID, Capacity, and so on) indicates the LDEV is undefined.
LDEV Name	LDEV names.
Parity Group ID	Parity group identifier where the LDEV belongs.
Pool Name (ID)	Pool name and pool identifier.
RAID level	RAID level specified.
Capacity	Capacity of each LDEV.
Provisioning Type	Provisioning type of each volume. Basic: Internal volume DP: V-VOLs of Dynamic Provisioning External: External volume Snapshot: Thin Image volume ALU: LDEV of the ALU attribution.
Attribute	Attribute of the volume indicating how the LDEV is used. Command Device: Command device Remote Command Device: Remote command device JNL VOL: Journal volume Pool VOL: Pool volume. The number in parentheses shows the pool ID. ALU: LDEV of the ALU attribution. SLU: LDEV of the SLU attribution. Hyphen (-): Volume in which the attribute is not defined
T10 PI	Displays the information on the T10 PI attribute of the LDEV. [Enabled]: The T10 PI attribute of the LDEV is enabled. [Disabled]: The T10 PI attribute of the LDEV is disabled.
Number of Paths	Number of paths set for the LDEV.
Resource Group Name (ID)	Resource group name and identifier of the LDEV.

(To be continued)

(Continued from the preceding page)

Item	Description
Virtual Storage Machine	Model name and serial number of the virtual storage machine that has the LDEV.
[Add] button	Adds one or more LDEVs selected in the Available LDEVs table to the Selected LDEVs table.
[Remove] button	Removes one or more selected LDEVs from the Selected LDEVs table and relocates the LDEVs to the Available LDEVs table.

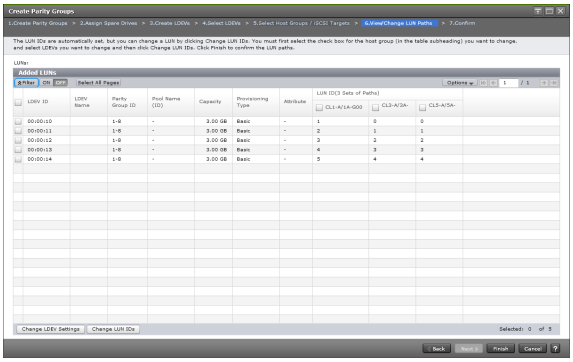
5. The Select Host Groups window appears.
   Select a host group from the [Available Host Groups] list, and then click [Add].
   The selected LDEV was added to the [Selected Host Groups] list. Click [Next].



[Available Host Groups] table and [Selected Host Groups] table

Item	Description
Port ID	Port identifiers.
Host Group Name	Name and identifier of each host group that uses a port. Some undefined host groups may appear. If a host group is not defined, the host name is blank.
Host Mode	The host mode of the host group.
Port Security	LUN security setting (Enabled or Disabled) on the port.
Number of Hosts	Number of hosts registered in the host group.
T10 PI mode	Displays the T10 PI mode setting of the port ([Enabled] or [Disabled]).
Resource Group Name (ID)	Resource group name and identifier of the host group.
[Add] button	Adds one or more host groups selected in the Available Host Groups table to the Selected Host Groups table.
[Remove] button	Removes one or more selected host groups from the Selected Host Groups table and relocates the host groups to the Available Host Groups table.

6. The “View/Change LUN Paths” window appears. Confirm the settings, and then click [Finish].



[Added LUNs] table

Item	Description
LDEV ID	LDEV identifier, which is the combination of LDKC, CU, and LDEV.
LDEV Name	Name of the LDEV.
Parity Group ID	Identifier of the parity group.
Pool Name (ID)	Pool names and pool identifiers. If the LDEV is not used as a pool-VOL, a hyphen (-) appears.
Capacity	Size of each logical volume.
Provisioning Type	Provisioning types for each logical volume. Basic: Internal volume. External: External volume. DP: V-VOL of Dynamic Provisioning. Snapshot: Thin Image volume. ALU: LDEV of the ALU attribution.
Attribute	Displays the attribute of the LDEV. Command Device: Command device. Remote Command Device: Remote command device. ALU: LDEV of the ALU attribution. SLU: LDEV of the SLU attribution. Hyphen (-): Volume in which the attribute is not defined.
T10 PI	Displays the information on the T10 PI attribute of the LDEV. [Enabled]: The T10 PI attribute of the LDEV is enabled. [Disabled]: The T10 PI attribute of the LDEV is disabled.
LUN ID ((number of LUNs) Sets of Paths)	Number of assigned LUNs.
port ID/ host group name	Name of the port and the host group of assigned LUNs. This item appears according to the number of assigned LUNs.
Change LDEV Settings	To change the LDEV name setting, select an LDEV then click this button.
Change LUN IDs	To change the LUN setting, select the checkbox in the table column of port ID/host group name, select the target LDEV, then click this button.

7. Check the set contents in the Confirm window and enter a task name in [Task Name].

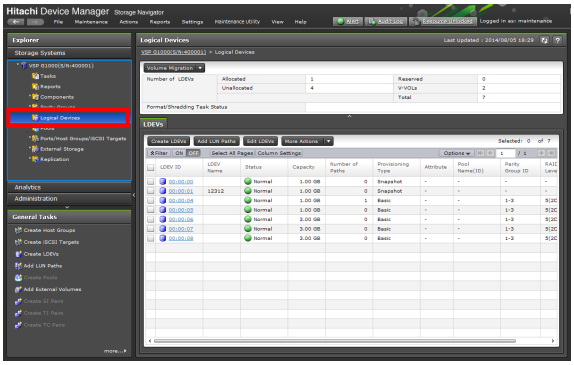
8. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

9. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.8.3 Checking the Logical Devices

1. Select [Storage Systems]-[Logical Devices].



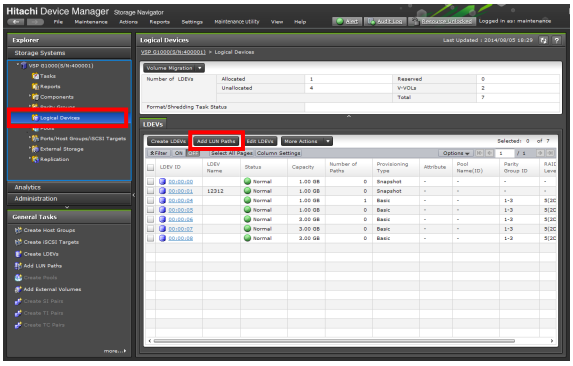
Item	Description
LDEV ID	Number of the logical device
LDEV Name	LDEV name
Status	A status of the logical device
Capacity	Available capacity of the parity group
Number of Paths	The number of the logical devices path
Provisioning Type	A type of the logical device
Attribute	An Attribute of the logical device.
Pool Name (ID)	Pool Name (ID)
Parity Group ID	Number of the parity groups
RAID Level	RAID level specified

3.8.4 Allocating the Logical Devices of a Storage System to a Host

Set mappings of the Port ID, and host group/iSCSI Target for a logical device so that they are used in the configuration set by a host. The setting of the mapping can be modified while an I/O is being executed using the existing mapping setting.

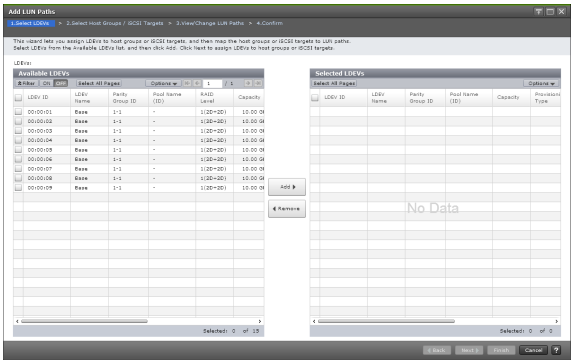
NOTICE:	When the Storage System and the host are connected with the Fibre Channel interface, the logical device of the Storage System cannot be recognized unless the logical device 0 is not created in the Storage System depending on the host. When using this host, create the logical device 0 or map the logical device to host group 0.

1. Select [Storage Systems]-[Logical Devices].



2. Click [Add LUN Paths].

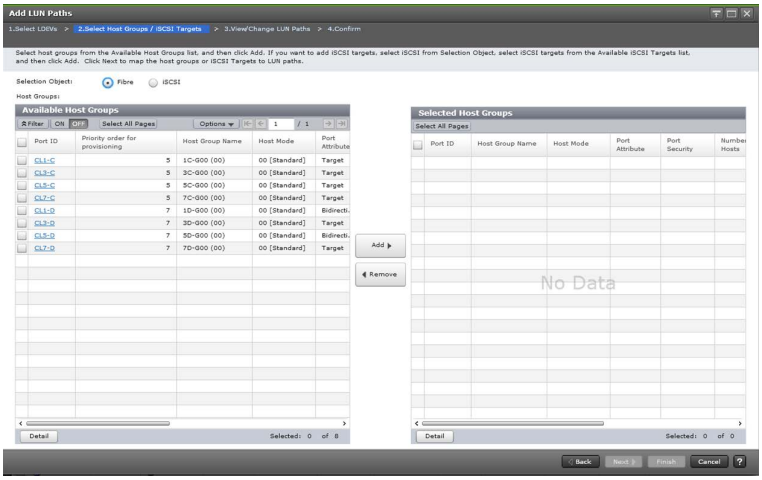
3. The Select LDEVs window appears.
   Select a spare drive from the [Available LDEVs] list, and then click [Add].
   The selected LDEV was added to the [Selected LDEVs] list. Click [Next].



[Available LDEVs] table and [Selected LDEVs] table

Item	Description
LDEV ID	LDEV identifier, which is the combination of LDKC, CU, and LDEV.
LDEV Name	Name of the LDEV.
Parity Group ID	Identifier of the parity group.
Pool Name (ID)	Pool name and pool identifier. If the LDEV is not used as a pool-VOL, a hyphen (-) appears.
RAID Level	Displays the RAID level. If multiple RAID levels exist in a pool, Mixed appears in this field.
Capacity	Size of each logical volume.
Provisioning Type	Provisioning type for each logical volume. Basic: Internal volume. External: External volume. DP: V-VOL of Dynamic Provisioning. Snapshot: Thin Image volume. ALU: LDEV of the ALU attribution.
Attribute	Displays the attribute of the LDEV. Command Device: Command device. Remote Command Device: Remote command device. ALU: LDEV of the ALU attribution. SLU: LDEV of the SLU attribution. Hyphen (-): Volume in which the attribute is not defined.
T10 PI	Displays the information on the T10 PI attribute of the LDEV. [Enabled]: The T10 PI attribute of the LDEV is enabled. [Disabled]: The T10 PI attribute of the LDEV is disabled.
Number of Paths	Number of paths set for the LDEV.
Resource Group Name (ID)	Resource group name and identifier of the LDEV.
Virtual Storage Machine	Model name and serial number of the virtual storage machine that has the LDEV.
[Add] button	Adds logical volumes selected from the Available LDEVs table to the Selected LDEVs table.
[Remove] button	Removes logical volumes from the Selected LDEVs table.

4. The Add LUN Paths window appears.
   Select a Fibre, iSCSI from the [Available Host Groups] list or the [Available iSCSI Targets] list, and then click [Add].
   The selected LDEV was added to the [Selected Host Groups] list or the [Select iSCSI Targets] list. Click [Next].



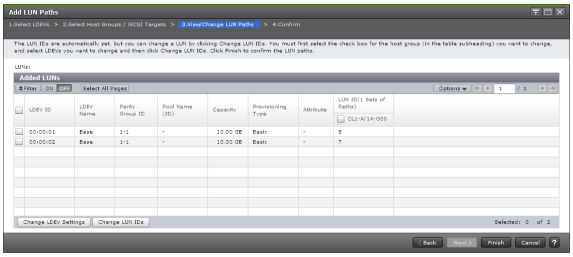
[Available Host Groups] table

Item	Description
Port ID	Identifier of the port. Clicking the link displays the Port Redundancy Level window.
Priority order for provisioning	Ports to be used are displayed in order from higher priority.
Host Group Name	Name of the host group.
Host Mode	The host mode of the host group.
Port Attribute	Attribute of the port indicating I/O flow. • Target: Receives I/O commands from a host. • Bidirectional
Port Security	LUN security setting (Enabled or Disabled) on the port.
Number of Hosts	Number of hosts registered in the host group.
Resource Group Name (ID)	Resource group name and identifier of the host group.
T10 PI mode	Displays the T10 PI mode setting of the port ([Enabled] or [Disabled]).
Virtual Storage Machine	Model name and serial number of the virtual storage machine that has the LDEV.
[Detail] button	Details about the selected host group.
[Add] button	Adds host groups selected from the Available Host Groups table to the Selected Host Groups table.
[Remove] button	Removes the selected host groups from the Selected Host Groups table.

[Selected Host Groups] table

Item	Description
Port ID	Identifier of the port.
Host Group Name	Name of the host group.
Host Mode	The host mode of the host group.
Port Attribute	Attribute of the port indicating I/O flow. • Target: Receives I/O commands from a host. • Bidirectional
Port Security	LUN security setting (Enabled or Disabled) on the port.
Number of Hosts	Number of hosts registered in the host group.
Resource Group Name (ID)	Resource group name and identifier of the host group.
T10 PI mode	Displays the T10 PI mode setting of the port ([Enabled] or [Disabled]).
Virtual Storage Machine	Model name and serial number of the virtual storage machine that has the LDEV.
[Detail] button	Details about the selected host group.

5. The View/Change LUN Paths window appears. Check the settings and click [Finish].



[Added LUNs] table

Item	Description
LDEV ID	LDEV identifier, which is the combination of LDKC, CU, and LDEV.
LDEV Name	Name of the LDEV.
Parity Group ID	Identifier of the parity group.
Pool Name (ID)	Pool names and pool identifiers. If the LDEV is not used as a pool-VOL, a hyphen (-) appears.
Capacity	Size of each logical volume.
Provisioning Type	Provisioning types for each logical volume. Basic: Internal volume. External: External volume. DP: V-VOL of Dynamic Provisioning. Snapshot: Thin Image volume. ALU: LDEV of the ALU attribution.
Attribute	Displays the attribute of the LDEV. Command Device: Command device. Remote Command Device: Remote command device. ALU: LDEV of the ALU attribution. SLU: LDEV of the SLU attribution. Hyphen (-): Volume in which the attribute is not defined.
T10 PI	Displays the information on the T10 PI attribute of the LDEV. [Enabled]: The T10 PI attribute of the LDEV is enabled. [Disabled]: The T10 PI attribute of the LDEV is disabled.
LUN ID ((number of LUNs) Sets of Paths)	Number of assigned LUNs.
port ID/ host group name	Name of the port and the host group of assigned LUNs. This item appears according to the number of assigned LUNs.
Change LDEV Settings	To change the LDEV name setting, select an LDEV then click this button.
Change LUN IDs	To change the LUN setting, select the checkbox in the table column of port ID/host group name, select the target LDEV, then click this button. The Change LUN IDs window is displayed. Enter the changed ID in the head LUN ID and click [OK].

6. Check the set contents in the Confirm window and enter a task name in [Task Name].

7. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

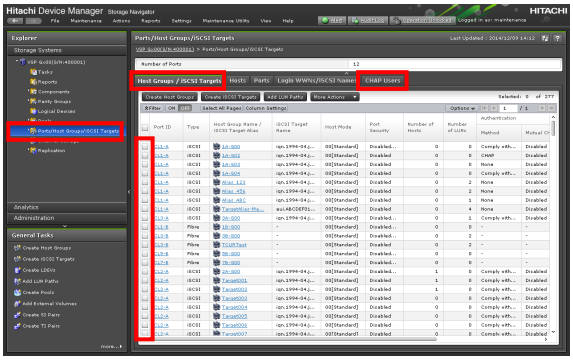
8. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.8.5 Configuring a Host Group or iSCSI Target

A host group is a logical entity of two or more hosts that share access to specific disks on the Storage System. The hosts in a host group can run the same or different operating systems.

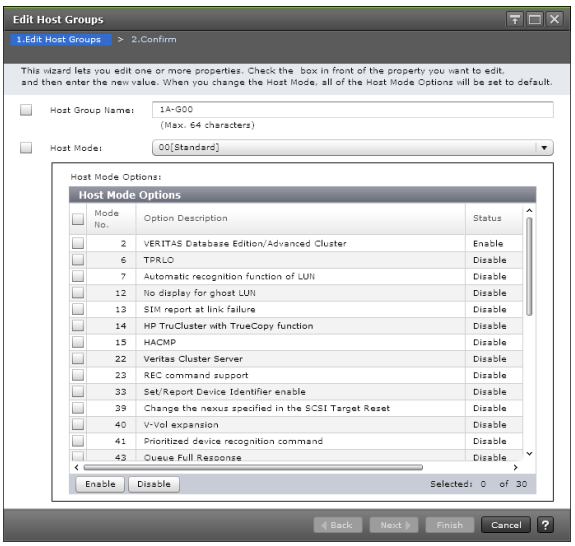
3.8.5.1 Editing Host Group

1. Select [Storage Systems]-[Ports/Host Groups/iSCSI Targets]. Click the [Host Groups/iSCSI Targets] tab.



2. Check [Type] is specified [Fibre], and then check the check box of the port that you want to edit. Click [More Actions]-[Edit Host Groups].

3. The Edit Host Groups window appears. Enter the setting information and click [Finish].



Item		Description
Host Group Name		Specify the name of the host group. Host group name can be up to 64 single-byte ASCII characters (alpha-numerals and symbols). You cannot use the following symbols: \ / : , ; * ? " < > | You cannot use blanks at the beginning or end of the host group name. If a host group assigned to an initiator port is included in the specified host groups, this item is unavailable.
Host Mode		Select the host mode from the list. If a host group assigned to an initiator port is included in the specified host groups, this item is unavailable.
Host Mode Options		To set the host mode option, select a host mode option, then click [Enable]. If you do not need a host mode option, select an unnecessary host mode option, then click [Disable].
	Mode No.	Number identifier of the host mode option.
	Option Description	Description of the host mode option.
	Status	Indicates the current status setting (Enabled or Disabled) of the host mode option on this host group.
	[Enable] button	Enables the host mode option.
	[Disable] button	Disables the host mode option.

4. Check the set contents in the Confirm window and enter a task name in [Task Name].

5. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

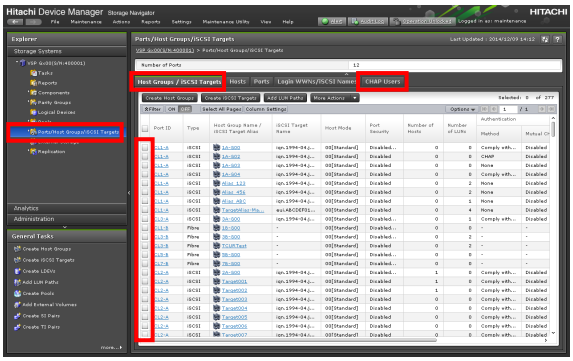
   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

6. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

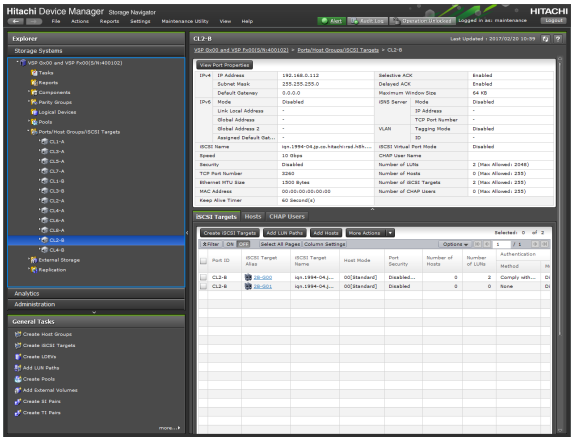
3.8.5.2 Editing iSCSI Target

With iSCSI, the host connection mode, mapping of logical devices, and LUN security information are set to targets, not to ports. In this way, you can select the host to which the Storage System is connected based on each target.

1. Select [Storage Systems]-[Ports/Host Groups/iSCSI Targets]. Click the [Host Groups/iSCSI Targets] tab.

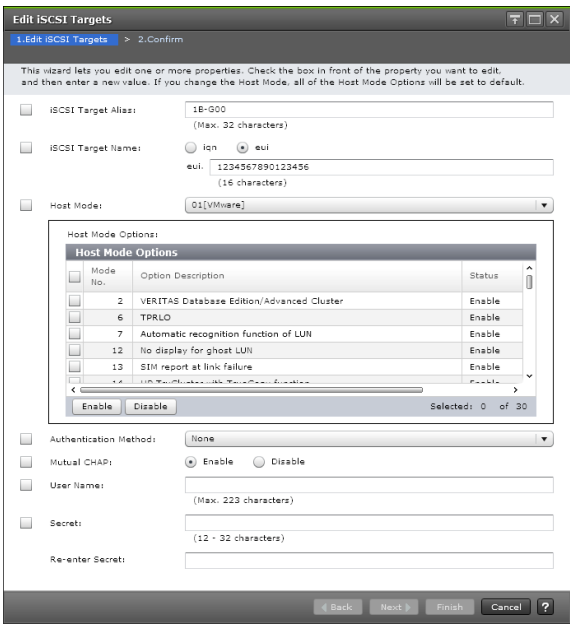


2. Check [Type] is specified [iSCSI], and then check the check box of the port that you want to edit.



3. Display the iSCSI Targets tab.
   Click the iSCSI port you want to set. Click [More Actions]-[Edit iSCSI Target].

4. The Edit iSCSI Targets window appears. Enter the setting information and click [Finish].



Item	Description
iSCSI Target Alias	Display an iSCSI target alias. Up to 32 alphanumeric characters and symbols (! # $ % & ' + - . = @ ^ _ { } ~ ( ) [ ] space)
iSCSI Target Name	[ign] or [eui]: Select either format.
	Text box: Enter an iSCSI target name. • The following describes the iqn format. Format: iqn.1994-04.jp.co.hitachi:rsd. Model name.t. Serial number. Port name iSCSI target ID Display example: iqn.1994-04.jp.co.hitachi:rsd.h8s.t.62507. (Port ID) (iSCSI target ID) You can use up to 219 ASCII characters (alphanumeric characters and symbols). However, you cannot use the following symbols. \ / , ; * ? " < > | • The eui format is described. Format: eui. (OUI6 digits) (Storage System fixed value) (Serial number) (Port name) (iSCSI target ID) Display example: eui.02004567A425678D You can use 16-digit hexadecimal numbers.
Host Mode	Select a host mode from the list.

(To be continued)

(Continued from preceding page)

Item		Description
Host Mode Option		When setting a host mode option, select the host mode option to be set and click [Enable]. When a host mode option is unnecessary, select the unnecessary host mode option and click [Disable].
	Mode No.	Display a host mode option number.
	Option Description	Display the description of the host mode option.
	Status	Display the setting of the host mode option (Enable/Disable).
	[Enable] button	Enable a host mode option.
	[Disable] button	Disable a host mode option.
Authentication Method		Select a CHAP authentication setting ([CHAP], [None] or [Comply with Host Setting]). Selecting [CHAP] can set the following options.
Mutual CHAP		Select the two-way authentication mode ([Enable] or [Disable]). When selecting [Enable], the mode becomes the two-way authentication. When selecting [Disable], the mode becomes the one-way authentication.
User Name		Set a user name. When selecting [Disable] for [Mutual CHAP], the setting is arbitrary. When selecting [Enable] for [Mutual CHAP], the setting is indispensable. You can set one to 223 characters. One-byte alphanumeric numbers (case-sensitive), one-byte spaces and the following one-byte symbols are available. . - + @ _ = : / [ ] ~
Secret		Set secret used for host authentication. When selecting [Disable] for [Mutual CHAP], the setting is arbitrary. When selecting [Enable] for [Mutual CHAP], the setting is indispensable. You can set 12 to 32 characters. One-byte alphanumeric numbers, one-byte spaces and the following one-byte symbols are available. . - + @ _ = : / [ ] ~
Re-enter Secret		Re-enter the same characters for confirming the secret entry. When selecting [Disable] for [Mutual CHAP], the setting is arbitrary. When selecting [Enable] for [Mutual CHAP], the setting is indispensable.

⚠ CAUTION

If an iSCSI target set for the port is included when selecting multiple iSCSI targets to which different host modes are set, you cannot complete the [Edit iSCSI Targets] operation.

⚠ CAUTION

When changing the secret twice or more for the same iSCSI target successively, wait for the completion of the applied task, and then execute the next change.
If you change the secret without waiting for the completion of the applied task, the user name may not be the expected change.

5. Check the set contents in the Confirm window and enter a task name in [Task Name].

6. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

7. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.9 Managing Drives

3.9.1 Setting Spare Drives

3.9.1.1 Guidelines When Allocating Spare Drives

The spare drives of VSP 5500, 5500H can be used in RAID1, RAID5, or RAID6. One CBX pair can have up to 64 spare drives, and one storage system can have 192 spare drives installed as the maximum. Drives in one CBX pair can be used as spare drives for a different CBX pair.

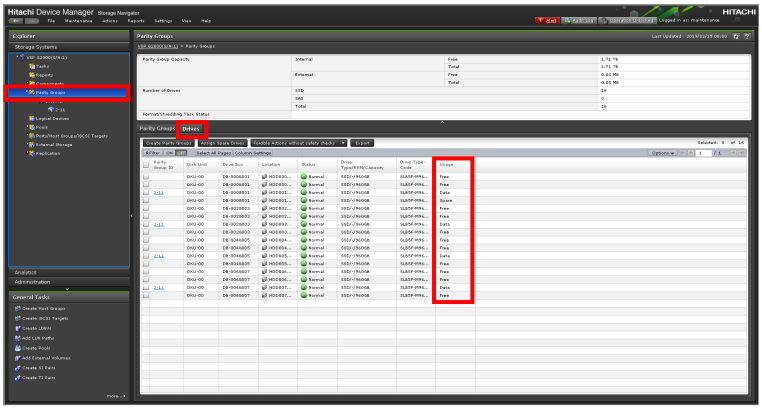
Table 3-1 Maximum number of spare drives

Number of DKC	Maximum number of spare disks		
	1CBX pair	2CBX pair	3CBX pair
2DKC	64	—	—
4DKC	64	128	—
6DKC	64	128	192

3.9.1.2 Checking Spare Drive

1. In the Web Console window, select [Storage Systems]-[Parity Groups].

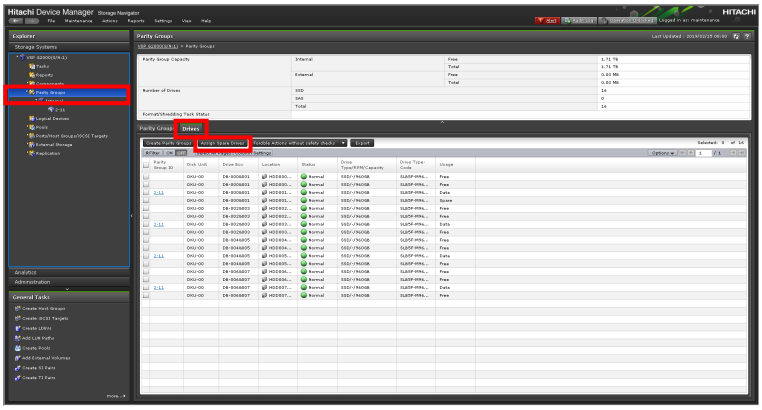
2. Click the [Drives] tab. Check the Usage is specified “Spare”.



Item	Description
Parity Group ID	Number of the parity groups.
Disk Unit	Displays the disk unit.
Drive Box	Displays the drive box number.
Location	Displays the location of the drive box.
Status	A status of the drive.
Drive Type/Interface/RPM/ Capacity	Displays the drive type, interface, round-per-minute (RPM), and capacity.
Drive type code	Display the drive type code.
Usage	Usage of the drive.

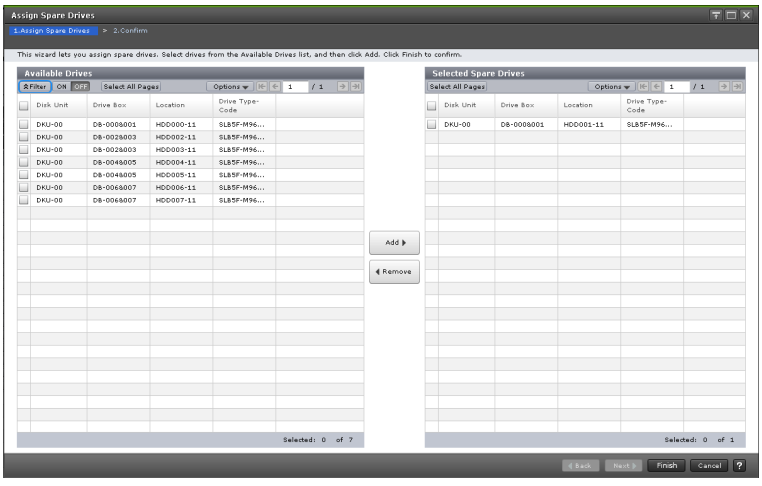
3.9.1.3 Allocating/Deleting Spare Drives

1. Select [Storage Systems]-[Parity Groups]. Click the [Drives] tab.



2. Click [Assign Spare Drives].

3. The Assign Spare Drives window appears.
When assigning spare drives, select a spare drive from the [Available Drives] list, and then click [Add] .
The selected drive is added to the [Selected Spare Drives] list.
When deleting spare drives, select a spare drive from the [Selected Spare Drives] list and click [Remove].
The selected spare drive is added to the [Available Drives] list.
A removed spare becomes available free space for the storage system to use.



[Available Drives] table and [Selected Spare Drives] table

Item	Description
Disk Unit	Displays the disk unit.
Drive Box	Displays the drive box number.
Location	Displays the location of the drive box.
Drive Type-Code	Displays the drive type code.

(To be continued)

(Continued from preceding page)

Item	Description
[Add] button	Adds one or more drives selected in the Available Drives table to the Selected Spare Drives table.
[Remove] button	Removes one or more selected drives from the Selected Spare Drives table, and relocates drives to the Available Drives table.

4. Confirm the settings. Click [Finish].

5. Check the set contents in the Confirm window and enter a task name in [Task Name].

6. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

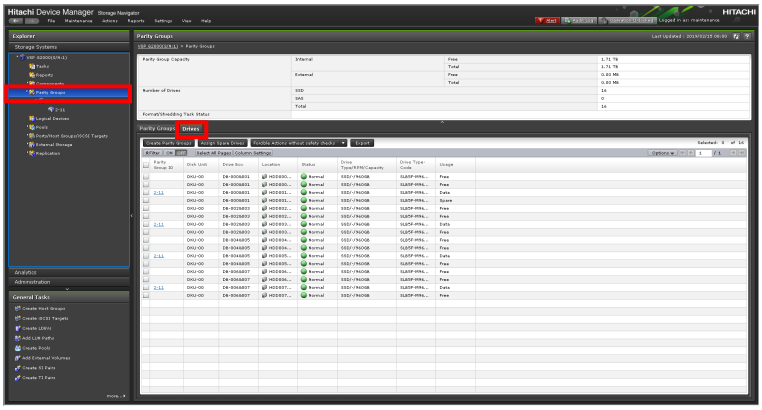
7. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.9.1.4 Assign Spare Drives (Without Safety Checks)

⚠ CAUTION

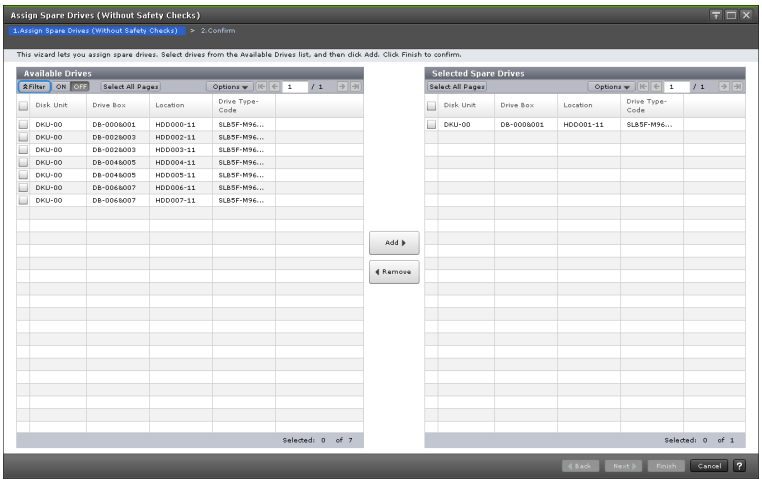
- Be sure to contact the Technical Support Division and follow the judgement before assigning spare drives with the procedure.
- The procedure is able to operate only by Web Console of the Maintenance PC.

1. Select [Storage Systems]-[Parity Groups]. Click the [Drives] tab.



2. Click [Forcible Actions without safety checks]-[Assign Spare Drives (Without Safety Checks)].

3. The Assign Spare Drives window appears.
   When assigning spare drives, select a spare drive from the [Available Drives] list, and then click [Add] .
   The selected drive is added to the [Selected Spare Drives] list.
   When deleting spare drives, select a spare drive from the [Selected Spare Drives] list and click [Remove].
   The selected spare drive is added to the [Available Drives] list.
   A removed spare becomes available free space for the storage system to use.



[Available Drives] table and [Selected Spare Drives] table

Item	Description
Disk Unit	Displays the disk unit.
Drive Box	Displays the drive box number.
Location	Displays the location of the drive box.
Drive Type-Code	Displays the drive type code.
[Add] button	Adds one of more drives selected in the Available Drives table to the Selected Spare Drives table.
[Remove] button	Removes one or more selected drives from the Selected Spare Drives table, and relocates drives to the Available Drives table.

4. Confirm the settings. Click [Finish].

5. Check the set contents in the Confirm window and enter a task name in [Task Name].

6. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

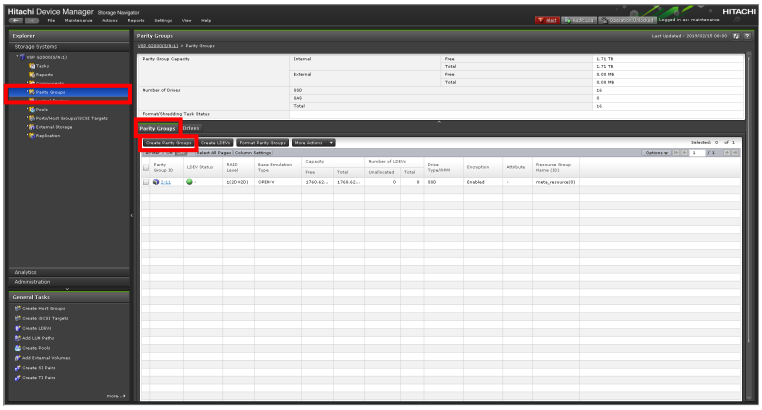
   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

7. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.9.2 Managing Parity Group

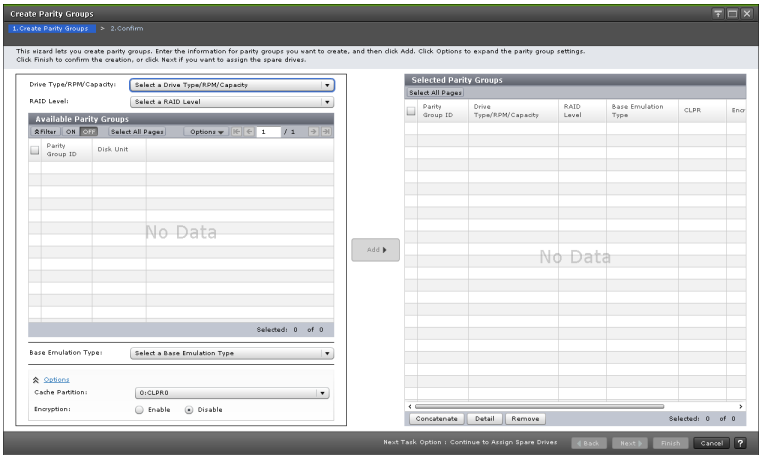
3.9.2.1 Creating Parity Group

1. Select [Storage Systems]-[Parity Groups]. Click the [Parity Groups] tab.



2. Click [Create Parity Groups].

3. Enter the information for parity groups you want to create, and then click [Add]. Click [Finish] .



Item	Description
Drive Type/Interface/RPM/ Capacity	Select a Drive Type/Interface/RPM/Capacity.
RAID Level	Select a RAID Level.
Available Parity Groups	Displays the available parity group. • Parity Group ID: Displays the parity group ID. • Disk Unit: Displays the disk unit.
Base Emulation Type	Select a Base Emulation Type.
Cache Partition	Select a CLPR number which is displayed as ID:CLPR.
Encryption	Specify if encrypted parity groups are created. • Enable: Encrypted parity groups are created. • Disable: Non-encrypted parity groups are created.
[Add] button	The set content is added to the Selected Parity Groups table on the right side.
[Concatenate] button	Concatenates the parity groups selected in the Selected Parity Groups table on the right side.
[Detail] button	Opens the Parity Group Properties window (see WEBCON03-170) that displays the details of the parity group selected in the Selected Parity Groups table on the right side.
[Remove] button	Removes the parity groups selected in the Selected Parity Groups table on the right side.

4. Click [Apply] to apply the settings to the Storage System.

5. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

6. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

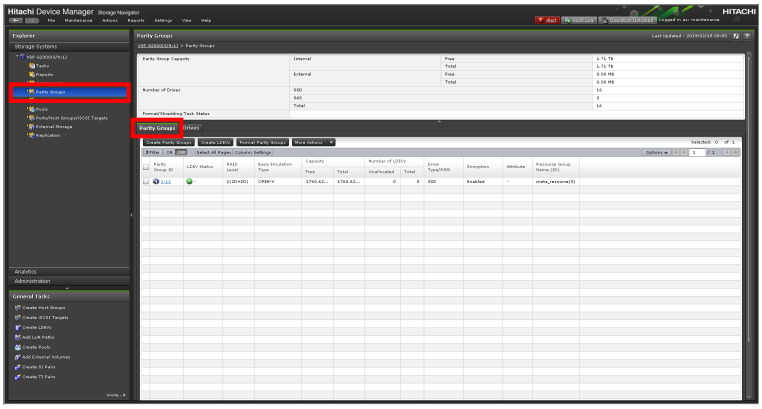
   NOTE: To change the accelerated compression setting, perform the procedure in “3.8.1.1 Changing the accelerated compression setting”.

3.9.2.2 Checking Parity Group

1. In the Web Console window, select [Storage Systems]-[Parity Groups].

2. Click the [Parity Groups] tab.

3. You can verify the parity group that has been set.



Item	Description
Parity Group ID	Parity group ID of the parity group in the storage system
LDEV Status	LDEV status. A variety of icons are used to indicate the LDEV status. For details, see “Provisioning Guide for Open Systems” or “Provisioning Guide for Mainframe Systems”.
RAID Level	RAID level [* (asterisk)]: Interleaved parity group. Either of the concatenated parity groups is displayed. [- (hyphen)]: The RAID level is not defined.
Base Emulation Type	Emulation type
Capacity	Information about the capacity [Free]: The free space capacity is displayed. The capacity of the control information used by the storage system such as control cylinders is not included in the displayed capacity. [Total]: The total capacity of LDEVs and the free space is displayed.
Number of LDEVs	Information about the number of LDEVs [Unallocated]: Number of unallocated LDEVs [Total]: Total number of LDEVs

(To be continued)

(Continued from the preceding page)

Item	Description
Drive Type/Interface/RPM	Drive type/interface/RPM (revolutions per minute) [- (hyphen)]: The drive type/interface/RPM is not defined.
Encryption	Encryption information [Enable]: Encrypted parity group [Disable]: Non-encrypted parity group [- (hyphen)]: The encryption setting is not defined for the parity group.
Accelerated Compression (*1)	Information on the accelerated compression setting for the parity group (*2) [Enable]: The accelerated compression is enabled for the parity group. [Disable]: The accelerated compression is disabled for the parity group. [- (hyphen)]: The accelerated compression is not supported for the parity group.
Expanded Space Used (*1)	Whether the LDEV is allocated to the physical area or the extension area [Enable]: The LDEV is using the extension area. [Disable]: The LDEV is using the physical area.
Attribute	Attribute of the parity group [- (hyphen)]: The attribute is not defined for the parity group.
Resource Group Name (ID)	Resource group name and ID of the parity group. ID is shown in the parentheses.
Virtual Storage Machine (*1)	Model type and serial number of the virtual storage machine to which the parity group belongs

*1: Does not appear by default. To display this item, change the settings in the [Column Settings] window. For details of the [Column Settings] window, see “System Administrator Guide”.

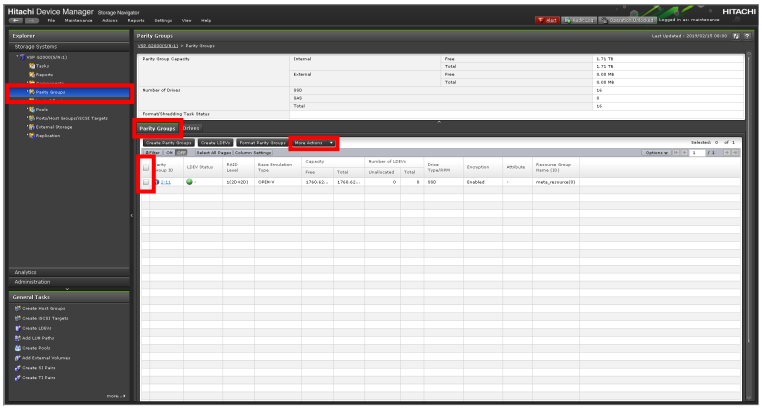
*2: Existing parity groups can have accelerated compression enabled non-destructively with data-in-place. For the detailed procedure, see “Provisioning Guide for Open Systems”.

3.9.2.3 Deleting Parity Group

> **⚠ CAUTION**
>
> All user data is lost by deleting the parity group and its associated logical device. Backup user data before deleting the parity group.

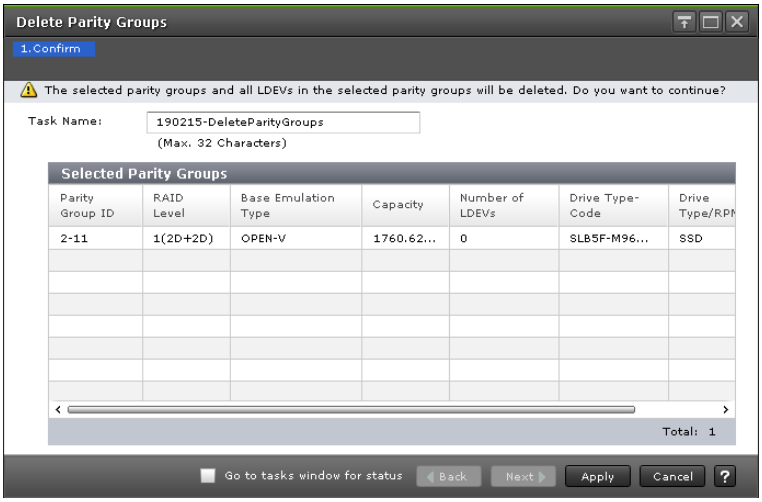
The parity group can be deleted even when logical devices are defined in the specified parity group.

1. Select [Storage Systems]-[Parity Groups]. Click the [Parity Groups] tab.



2. Check a parity group to be deleted and click [More Actions]-[Delete Parity Groups].

3. Check the set contents in the Confirm windows and enter a task name to [Task Name].



[Selected Parity Groups] table

Item	Description
Parity Group ID	Displays the parity group ID.
RAID Level	Displays the RAID level.
Base Emulation Type	Displays the Base Emulation Type.
Capacity	Displays the capacity of the parity group.
Number of LDEVs	Displays the number of LDEVs in the parity group.
Drive Type-Code	Displays the drive type code.
Drive Type/Interface/RPM	Displays the drive type, interface and RPM.

4. Click [Apply] to apply the settings to the Storage System.

5. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

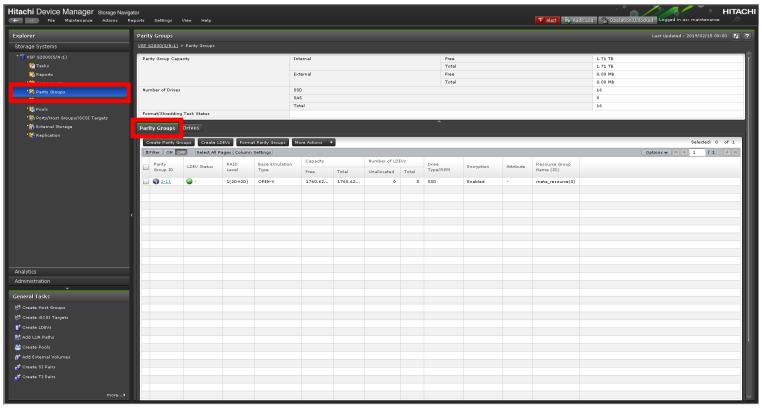
   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

6. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.9.2.4 Formatting Parity Group

For the parity group, execute the physical format by SCSI command.

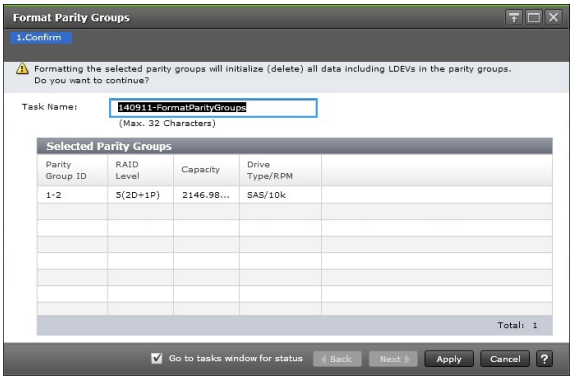
1. To format all LDEVs in [Parity Groups], select the [Parity Groups] tab.



2. Select the target LDEVs and block them.
   For information about how to block the LDEV, please refer to the “3.11.1 Blocking LDEVs”.

3. Check the parity group to be formatted and click [Parity Group Format].

4. Check the set contents in the Confirm windows and enter a task name to [Task Name].



Item	Description
Parity Group ID	Parity group identifier of the parity group in the storage system.
RAID Level	RAID level. An asterisk “*” indicates that the parity group to which the LDEV belongs is interleaved (concatenated). Either RAID level of the parity group appears.
Capacity	Capacity of the selected LDEV.
Drive Type/Interface/RPM	Drive type, interface and rpm in use on this LDEV.

5. Click [Apply] to apply the settings to the Storage System.

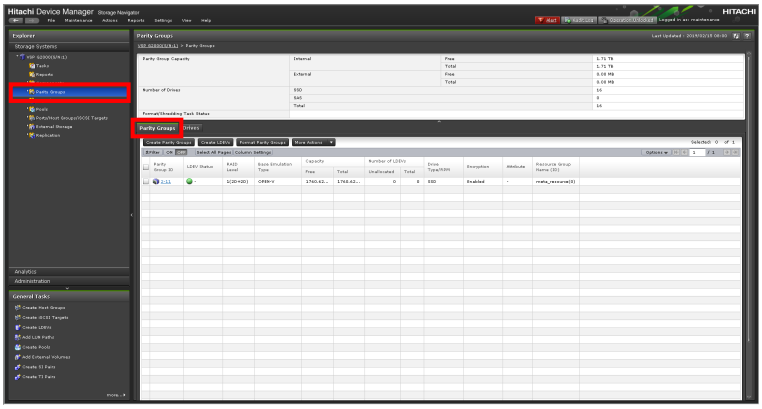
6. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

7. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

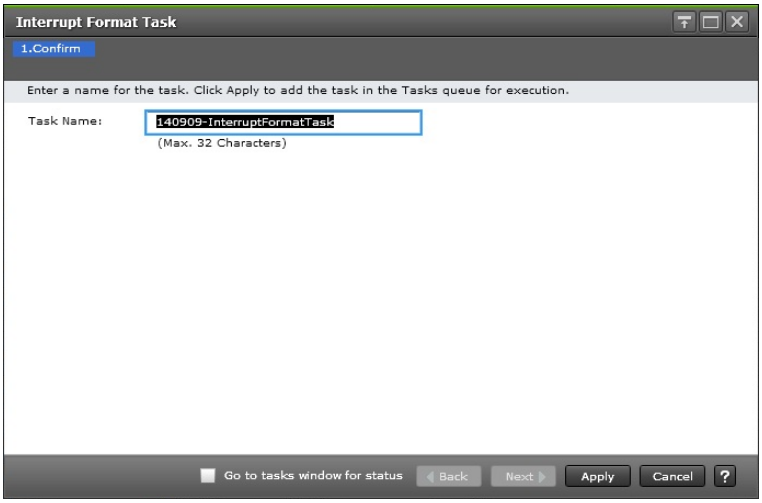
3.9.2.5 Interrupting Parity Group Format Task

1. To format all LDEVs in [Parity Groups], select [Parity Groups].



2. Click [More Actions]-[Interrupt Format Task].

3. Check the set contents in the Confirm window and enter a task name to [Task Name].



4. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

5. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

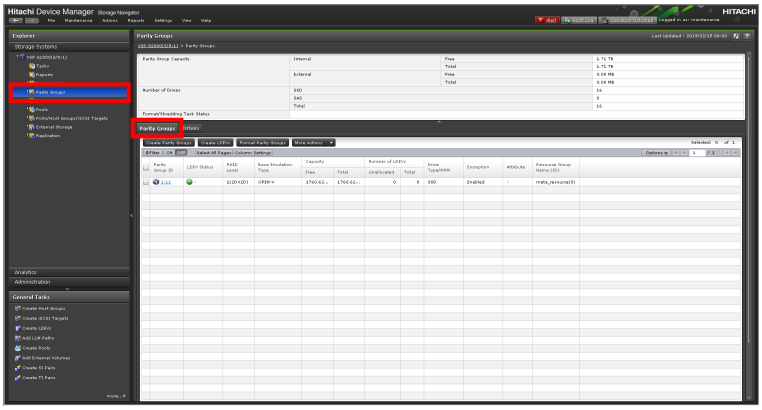
   NOTE: If you execute [Interrupt Format Task], the end time of the formatting task and the interruption task may differ by one to ten minutes on the Task window. Confirm the completion of the interruption by the completion of the formatting task.

3.9.2.6 Creating Parity Group (Without Safety Checks)

⚠ CAUTION

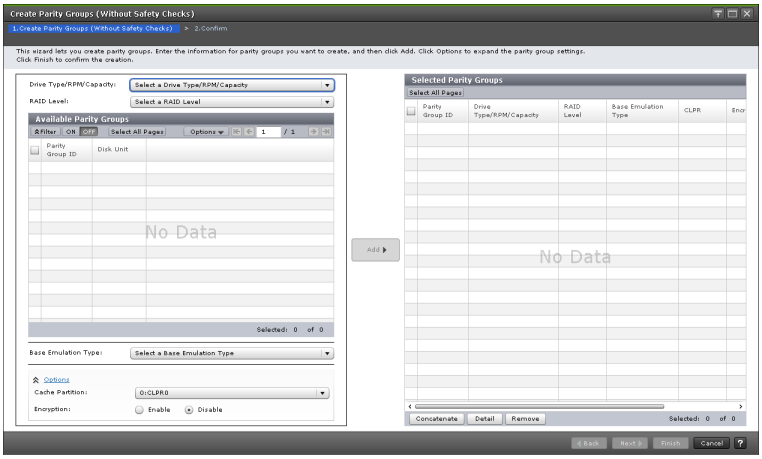
- Be sure to contact the Technical Support Division and follow the judgement before creating parity group with the procedure.
- The procedure is able to operate only by Web Console of the Maintenance PC.

1. Select [Storage Systems]-[Parity Groups]. Click the [Parity Groups] tab.



2. Click [More Actions]-[Forcible Actions without safety checks]-[Create Parity Groups (Without Safety Checks)].

3. Enter the information for parity groups you want to create, and then click [Add]. Click [Finish].



Item	Description
Drive Type/Interface/RPM/ Capacity	Select a Drive Type/Interface/RPM/Capacity.
RAID Level	Select a RAID Level.
Available Parity Groups	Displays the available parity group. • Parity Group ID: Displays the parity group ID. • Disk Unit: Displays the disk unit.
Base Emulation Type	Select a Base Emulation Type.
Cache Partition	Select a CLPR number which is displayed as ID:CLPR.
Encryption	Specify if encrypted parity groups are created. • Enable: Encrypted parity groups are created. • Disable: Non-encrypted parity groups are created.
[Add] button	The set content is added to the Selected Parity Groups table on the right side.
[Concatenate] button	Concatenates the parity groups selected in the Selected Parity Groups table on the right side.
[Detail] button	Opens the Parity Group Properties window (see WEBCON03-170) that displays the details of the parity group selected in the Selected Parity Groups table on the right side.
[Remove] button	Removes the parity groups selected in the Selected Parity Groups table on the right side.

4. Check the settings in the Confirm window and enter a task name to [Task Name]. Click [Apply] to apply the settings to the Storage System.

5. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

6. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

   NOTE: To change the accelerated compression setting, perform the procedure in “3.8.1.1 Changing the accelerated compression setting”.

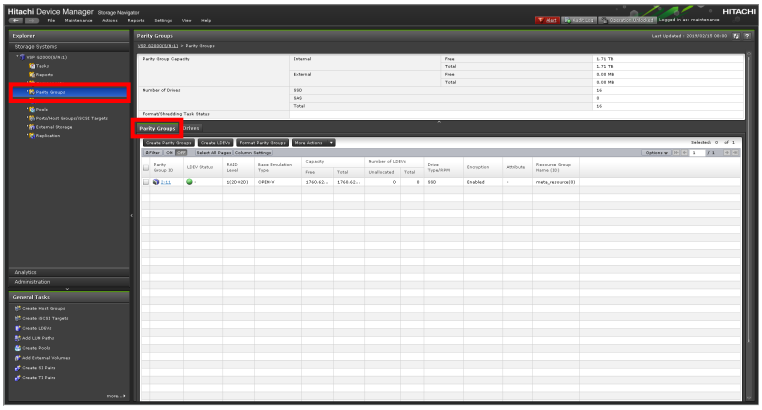
3.9.2.7 Deleting Parity Group (Without Safety Checks)

⚠ CAUTION

- Be sure to contact the Technical Support Division and follow the judgement before deleting parity group with the procedure.
- The procedure is able to operate only by Web Console of the Maintenance PC.
- All user data is lost by deleting the parity group and its associated logical device. Backup user data before deleting the parity group.

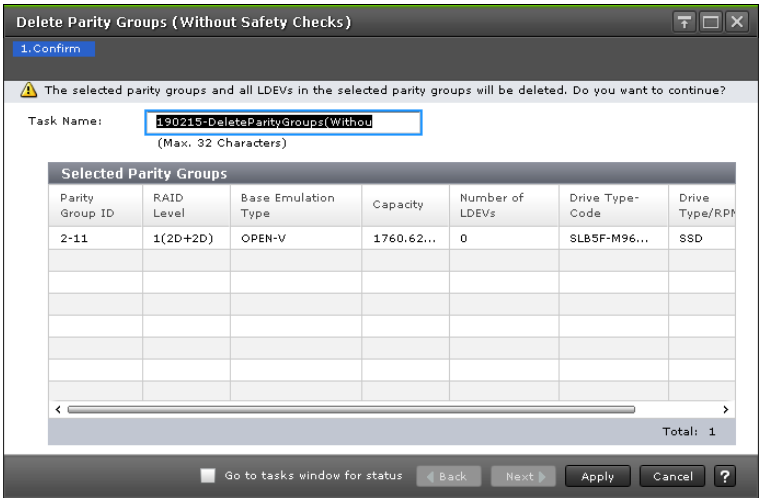
The parity group can be deleted even when logical devices are defined in the specified parity group.

1. Select [Storage Systems]-[Parity Groups]. Click the [Parity Groups] tab.



2. Check a parity group to be deleted and click [More Actions]-[Forcible Actions without safety checks]-[Delete Parity Groups (Without Safety Checks)].

3. Check the set contents in the Confirm window and enter a task name to [Task Name].



[Selected Parity Groups] table

Item	Description
Parity Group ID	Displays the parity group ID.
RAID Level	Displays the RAID level.
Base Emulation Type	Displays the Base Emulation Type.
Capacity	Displays the capacity of the parity group.
Number of LDEVs	Displays the number of LDEVs in the parity group.
Drive Type-Code	Displays the drive type code.
Drive Type/Interface/RPM	Displays the drive type, interface and RPM.

4. Click [Apply] to apply the settings to the Storage System.

5. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

6. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

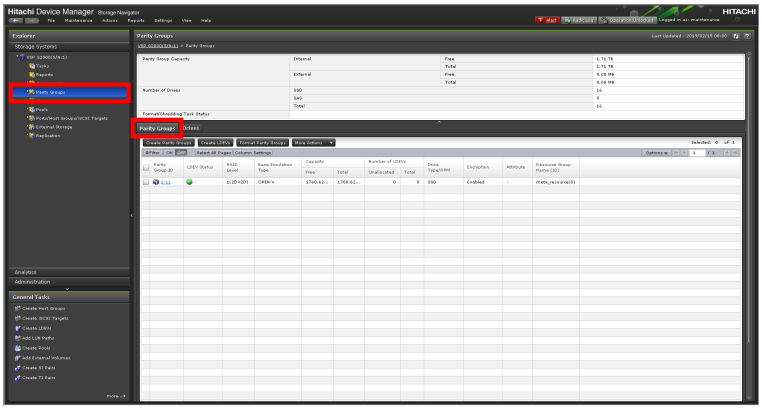
3.9.2.8 Formatting Parity Group (Without Safety Checks)

⚠ CAUTION

- Be sure to contact the Technical Support Division and follow the judgement before formatting parity group with the procedure.
- The procedure is able to operate only by Web Console of the Maintenance PC.

For the parity group, execute the physical format by SCSI command.

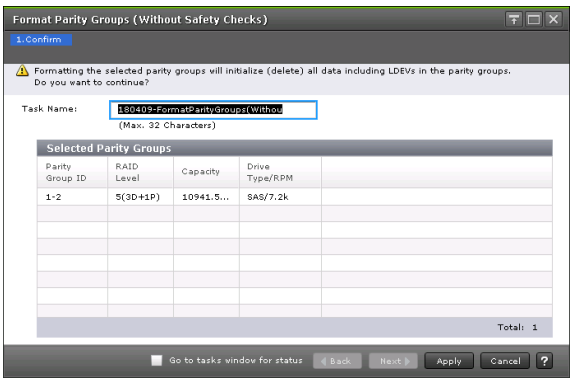
1. To format all LDEVs in [Parity Groups], select the [Parity Groups] tab.



2. Select the target parity group and block LDEVs associated with the parity group.
   For information about how to block the LDEV, refer to the "3.11.1 Blocking LDEVs".

3. Check the parity group to be formatted and click [More Actions]-[Forcible Actions without safety checks]-[Format Parity Groups (Without Safety Checks)].

4. Check the settings in the Confirm window and enter a task name to [Task Name].



[Selected Parity Groups] table

Item	Description
Parity Group ID	Displays the parity group identifier in the storage system.
RAID Level	Displays the RAID level. An asterisk "*" indicates that the parity group to which the LDEV belongs is interleaved (concatenated). Either RAID level of the parity group appears.
Capacity	Displays the capacity of the parity group.
Drive Type/Interface/RPM	Displays the drive type, interface and RPM.

5. Click [Apply] to apply the settings to the Storage System.

6. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking "Apply"] in the wizard and click [Apply].

7. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.9.3 Managing Logical Device

3.9.3.1 Creating Logical Device

1. In the Web Console window, select [Storage Systems]-[Logical Devices].

2. In the [LDEVs] tab, click [Create LDEVs].

3. The Create LDEVs window appears.
   Enter the information for LDEV you want to create, and then click [Add].
   The LDEV was added to the [Selected LDEVs] list. Click [Finish].

   NOTE: When clicking [Options], you can set up the detailed LDEV information.

4. The Confirm window appears.
   In the Confirm window, confirm the settings and specify the task name, and then click [Apply].

3.9.3.2 Checking Logical Device

1. In the Web Console window, select [Storage Systems]-[Logical Devices].

2. Check the set contents.

3.9.3.3 Allocating the Logical Devices of a Storage System to a Host

Set mappings of the Port and host group/iSCSI Target for a logical device.
Refer to “3.8.4 Allocating the Logical Devices of a Storage System to a Host”.

3.9.3.4 Formatting LDEVs

If you initialize LDEVs that are being used, you will need to format the LDEVs. Read the following topics before formatting LDEVs.

About formatting LDEVs

The LDEV Format function, which includes Normal Format, and Quick Format. These functions format volumes, including external volumes.
Before formatting volumes, ensure that the volumes are in blocked status.
The following table lists which formatting functions can be used on which LDEV types.

Formatting function	Corresponding volume
Normal Format	Internal volume Virtual volume External volume
Quick Format	Internal volume

The Quick Format function formats internal volumes in the background.
While Quick Format is running in the background, you can configure your system before the formatting is completed.
Before using Quick Format to format internal volumes, ensure that the internal volumes are in blocked status.

I/O operation from a host during Quick Format are allowed. Formatting in the background might affect performance.

Quick Format cannot be performed on the following volumes:
- Any volumes other than internal volumes
- Volumes assigned an access attribute other than read/write
- Pool volumes
- Journal volumes

The following table shows the Quick Format specifications.

Table 3-2 Quick Format Specifications

Item	Description
Preparation for executing the Quick Format feature	The internal volume must be in blocked status.
The number of parity groups that can undergo Quick Format	Quick Format can be performed on multiple parity groups simultaneously. The number of those parity groups depends on the total of parity group entries. The number of entries is an indicator for controlling the number of parity groups on which Quick Format can be performed. The number of parity group entries depends on the drive capacity configuring each parity group. The number of entries for parity groups is as follows. • Parity group configured with drives of 32 TB or less: 1 entry • Parity group configured with drives of more than 32 TB: 2 entries The maximum number of entries on which Quick Format can be performed is as follows. • VSP 5100, VSP 5100H, VSP 5500, VSP 5500H: 72 entries The number of volumes on which Quick Format can be performed is not limited.
Concurrent Quick Format operations	Additional Quick Format can be executed during Quick Format execution. In this case, the total number of entries during Quick Format and those to be added is limited to the maximum number of entries per model.
Preliminary processing	At the beginning of the Quick Format operation, Web Console performs preliminary processing to generate management information. If a volume is undergoing preliminary processing, the Web Console main window shows the status of the volume as Preparing Quick Format. While preliminary processing is in progress, hosts cannot perform I/O access to the volume.

(To be continued)

(Continued from the preceding page)

Item	Description
Blocking and restoring of volumes	If a volume undergoing Quick Format is blocked, the Storage System recognizes that the volume is undergoing Quick Format. After the volume is restored, the status of the volume changes to Normal (Quick Format). Therefore, parity groups in which all volumes during Quick Format are blocked are included in the number of entries during Quick Format. The number of entries for additional Quick Format can be calculated with the following calculating formula: The maximum number of entries - X - Y (Legend) X: The number of entries for parity groups during Quick Format. Y: The number of entries for parity groups in which all volumes during Quick Format are blocked.
Storage System is powered off and back on	The Quick Format operation resumes when power is turned back on.
Restrictions	• Quick Format cannot be executed on external volumes, virtual volumes, the journal volumes of Universal Replicator. • The volume migration feature or the QuickRestore feature cannot be applied to volumes undergoing Quick Format. When you use Command Control Interface to execute the volume migration operation or the QuickRestore operation on volumes undergoing Quick Format, EX_CMDRJE will be reported to Command Control Interface. In this case, check the volume status with Web Console.

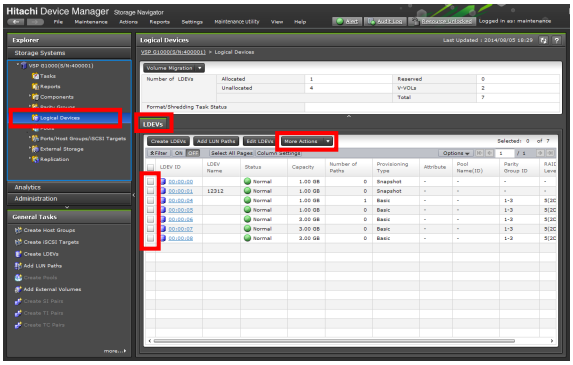
3.9.3.5 Formatting a Specific LDEV

This procedure performs Normal formatting on the volume.

> **⚠ CAUTION**
>
> When a specified logical device is formatted, the user data within the specified logical device is lost. When incorrectly specifying a logical device, click [Cancel] and redo processing by selecting a logical device to be reformatted.

> **NOTICE:** When you perform the LDEV maintenance operation using RAID Manager, the LDEV status displayed on the Web Console might be different from the actual status.
> (For example, the status of the LDEV that is being formatted by RAID Manager is displayed as "Blocked" instead of "Formatting".)
> In such a case, click [Update] to update the displayed information after the maintenance operation performed by RAID Manager is complete.
> You can check the LDEV status using RAID Manager.

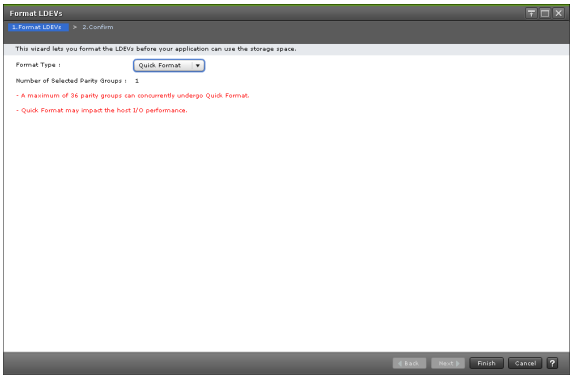
1. Select [Storage Systems]-[Logical Devices]. Click the [LDEVs] tab.



2. Select and block the LDEV to be formatted.
   See Blocking LDEV on "3.11.1 Blocking LDEVs" for blocking an internal volume. See the Hitachi Universal Volume Manager User Guide for blocking an external volume.

3. Click [Format LDEVs].
   When you select one of the following tabs, click [More Actions]-[Format LDEVs].
   - LDEVs tab, which appears when Logical Devices is selected from the Storage System tree.
   - Virtual Volumes tab, which appears when a pool from Pools in the Storage System tree is selected.

4. In the Format LDEVs window, select the format type from the [Format Type] list, and then click [Finish].



Item	Description
Format type	Set the type of formats. [Quick Format]: This is a quick format. The quick format is the initial value of the format type. When selecting an external volume, you cannot select the quick format. [Normal Format]: This is a normal format.
Number of parity group selections	Display the number of selected target parity groups.

5. In the Confirm window, click [Apply].
   If “Go to tasks window for status” is checked, the Tasks window opens.

6. Click [Apply] to apply the settings to the Storage System.

7. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

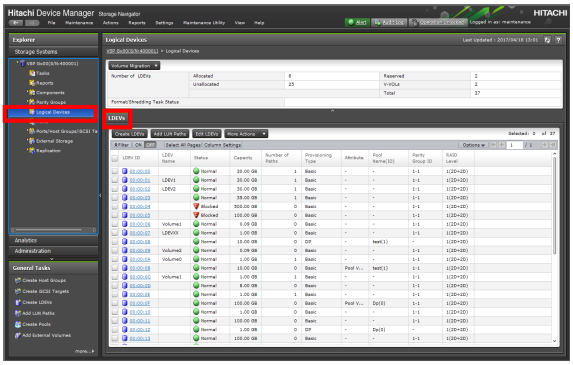
   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

8. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

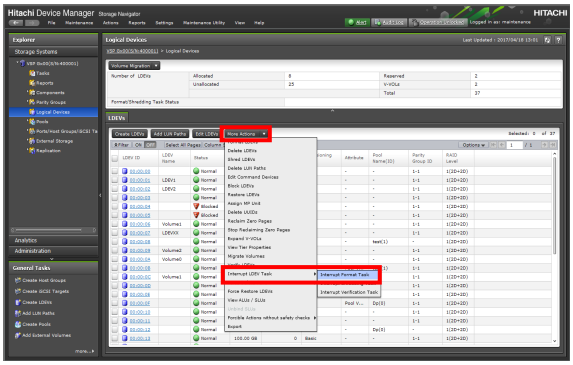
3.9.3.6 Interrupting Format Task

Suspend the formatting task. You can suspend the formatting task during Normal Format.
You cannot suspend the formatting task during the Quick Format.

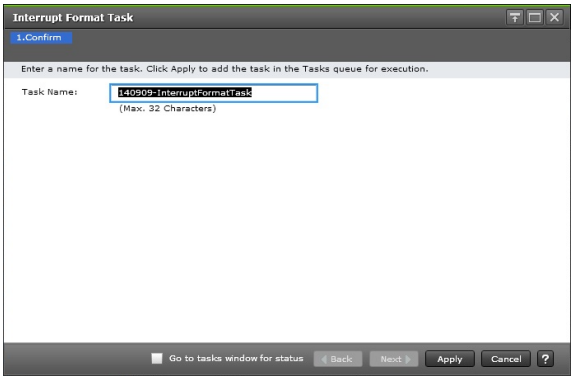
1. Select [Storage Systems]-[Logical Devices]. Click the [LDEVs] tab.



2. Select [More Actions]-[Interrupt LDEV Task]-[Interrupt Format Task].



3. Check the set contents in the Confirm window and enter a task name to [Task Name].



Item	Description
Task name	Enter a task name. You can use up to 32 alphanumeric characters and symbols (excluding / \ : , ; * ? " < > |). Characters are case-sensitive.

4. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

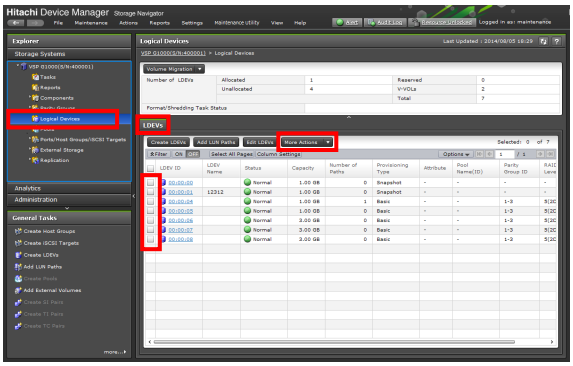
5. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

   NOTE: If you execute [Interrupt Format Task], the end time of the formatting task and the interruption task may differ by one to ten minutes on the Task window. Confirm the completion of the interruption by the completion of the formatting task.

3.9.3.7 Deleting Logical Device

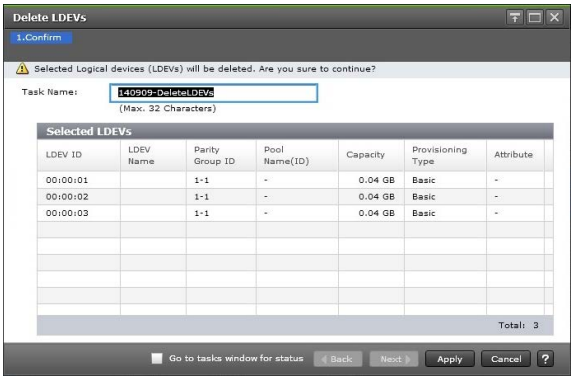
> **⚠ CAUTION**
>
> Deleting logical devices deletes all the data associated with them. Therefore, back up the data associated with logical devices before deleting them..

1. Select [Storage Systems]-[Logical Devices]. Click the [LDEVs] tab.



2. Check a logical device to be deleted. Click [More Actions]-[Delete LDEVs].

3. Check the set contents in the Confirm window and enter a task name in [Task Name].



Item	Description
LDEV ID	LDEV identifier, which is the combination of LDKC, CU, and LDEV.
LDEV Name	LDEV name.
Parity Group ID	Parity group identifier.
Pool Name (ID)	Pool name and pool identifier.
Capacity	LDEV capacity.

(To be continued)

(Continued from the preceding page)

Item	Description
Provisioning Type	Provisioning type assigned to the LDEV. Basic: Internal volume. DP: DP-VOL. External: External volume. Snapshot: Thin Image volume. ALU: LDEV of the ALU attribution.
Attribute	Displays the attribute of the LDEV. Command Device: Command device. ALU: LDEV of the ALU attribution. SLU: LDEV of the SLU attribution. Hyphen (-): Volume in which the attribute is not defined.

4. Click [Apply] to apply the settings to the Storage System.

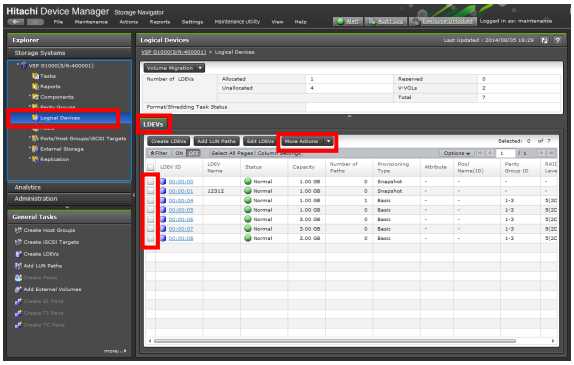
5. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

6. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

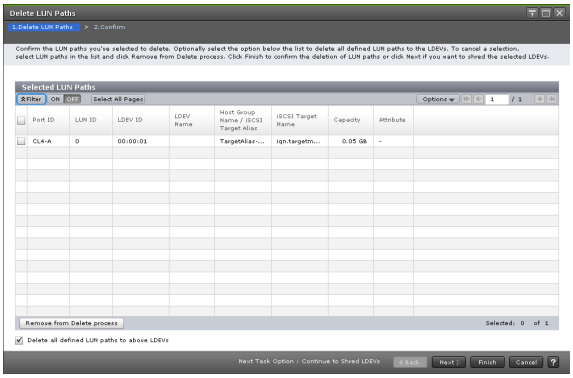
3.9.3.8 Releasing Logical Device Assignments

1. Select [Storage Systems]-[Logical Devices]. Click the [LDEVs] tab.



2. Check a logical device to be delete the LUN path. Click [More Actions]-[Delete LUN Paths].

3. Check the logical devices you want to release in [Selected LUN Paths]. Click [Finish].



[Selected LUN Paths] table

Item	Description
Port ID	Identifier of the port.
LUN ID	Identifier of the selected LUN paths.
LDEV ID	LDEV identifier, which is the combination of LDKC, CU, and LDEV.
LDEV Name	Name of the LDEV.
Host Group Name	Name of the host group.
Capacity	Size of each logical volume.
Attribute	Displays the attribute of the LDEV. Command Device: Command device. Remote Command Device: Remote command device. Hyphen (-): Volume in which the attribute is not defined.
T10 PI	Displays the information on the T10 PI attribute of the LDEV. [Enabled]: The T10 PI attribute of the LDEV is enabled. [Disabled]: The T10 PI attribute of the LDEV is disabled.

(To be continued)

(Continued from preceding page)

Item	Description
Remove from Delete process	Removes LUN paths from the Selected LUN Paths table.
Delete all defined LUN paths to above LDEVs	Removes LUN paths from the Selected LUN Paths table. When this checkbox is selected, the host groups of all the alternate paths in the LDEV displayed in the Selected LUNs table must be assigned to the Storage Administrator group permitted to manage them.
Next Task Option	Click [Next] to go to the task setting window, which is indicated in Task Next Option.

4. Check the set contents in the Confirm window and enter a task name in [Task Name].

5. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

6. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

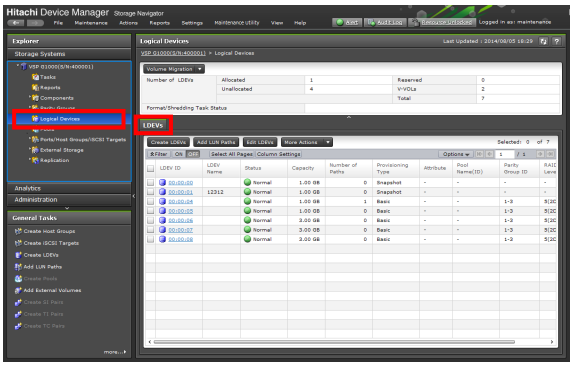
3.9.3.9 Formatting a Specific LDEV (Without Safety Checks)

⚠ CAUTION

- Be sure to contact the Technical Support Division and follow the judgement before formatting a specific LDEV with the procedure.
- The procedure is able to operate only by Web Console of the Maintenance PC.
- When a specified logical device is formatted, the user data within the specified logical device is lost. When incorrectly specifying a logical device, click [Cancel] and redo processing by selecting a logical device to be formatted.

NOTICE: When you perform the LDEV maintenance operation using RAID Manager, the LDEV status displayed on the Web Console might be different from the actual status. (For example, the status of the LDEV that is being formatted by RAID Manager is displayed as "Blocked" instead of "Formatting".)
In such a case, click [Update] to update the displayed information after the maintenance operation performed by RAID Manager is complete.
You can check the LDEV status using RAID Manager.

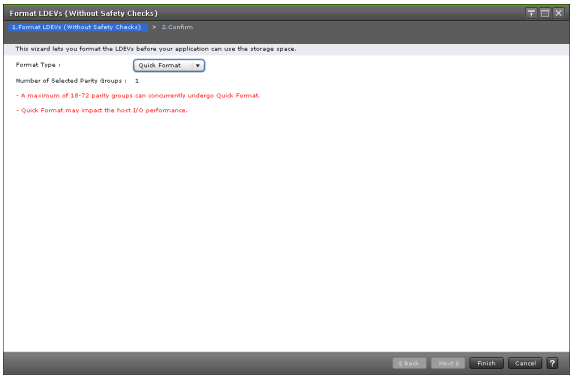
1. Select [Storage Systems]-[Logical Devices]. Click the [LDEVs] tab.



2. Select and block the LDEV to be formatted.
See Blocking LDEV on "3.11.1 Blocking LDEVs" for blocking an internal volume. See the Hitachi Universal Volume Manager User Guide for blocking an external volume.

3. Click [More Actions]-[Forcible Actions without safety checks]-[Format LDEVs (Without Safety Checks)].

4. In the Format LDEVs (Without Safety Checks) window, select the format type from the [Format Type] list, and then click [Finish].



Item	Description
Format type	Set the type of formats. [Quick Format]: This is a quick format. This type is the initial value of the format type. When selecting an external volume, you cannot select the quick format. [Normal Format]: This is a normal format.
Number of Selected Parity Groups	Display the number of selected parity groups.

5. Check the set contents in the Confirm window and enter a task name in [Task Name].

6. Click [Apply] to apply the settings to the Storage System.

7. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

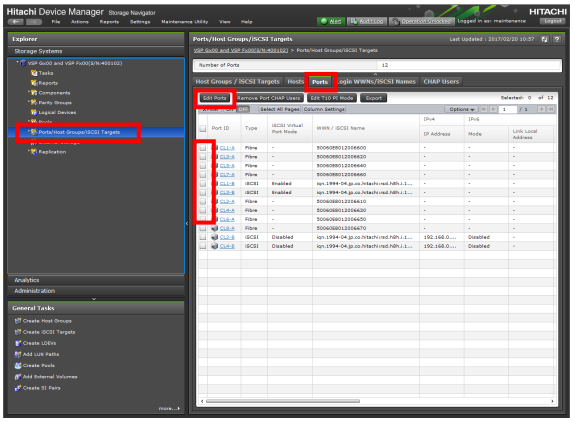
   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

8. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.10 Managing Port

3.10.1 Editing Fibre Channel

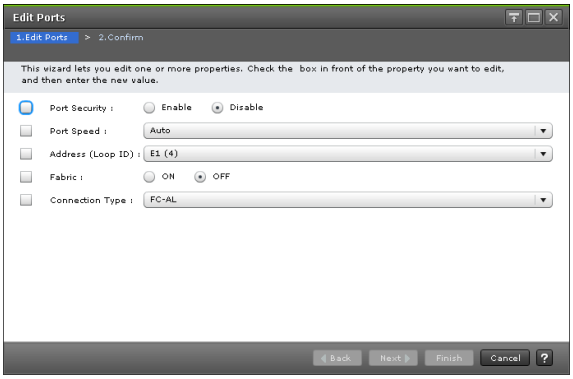
1. Select [Storage Systems]-[Ports/Host Groups/iSCSI Targets]. Click the [Ports] tab.



2. Check [Type] is specified [Fibre], and then check the check box of the port that you want to edit.

3. Click [Edit Ports].

4. The Edit Ports window appears. Enter the setting information and click [Finish].



Item	Description
Port Security	Select whether LUN security is Enabled or Disabled.
Port Speed	Select the data transfer speed, in Gbps, for the selected Fibre Channel port. If Auto is selected, the storage system automatically sets the data transfer speed to 4, 8, 16 or 32 Gbps. NOTE: If you are using 4-Gbps HBA and switch, set the transfer speed of the CHB (FC) port as 4 Gbps. If you are using 8-Gbps HBA and switch, set the transfer speed of the CHB (FC) port as 8 Gbps. If you are using 16-Gbps HBA and switch, set the transfer speed of the CHB (FC) port as 16-Gbps. If the Auto Negotiation setting is required, the linkup may become improper at server restart. Check a channel lamp, and if it is blinking, remove and re-insert the cable to perform the signal synchronization and linkup. If you are using 32-Gbps HBA and switch, set the transfer speed of the CHB (FC) port as 32 Gbps. When the transfer speed of the CHB (FC) port is set to Auto, the data might not be transferred at the maximum speed depending on the connected device. Confirm the transfer speed appearing in Speed in the Ports list when you start up the storage system, HBA, or switch. When the transfer speed is not the maximum speed, select the maximum speed from the list on the right or remove and reinsert the cable.
Address (Loop ID)	Select the address of the selected port.
Fabric	Select whether a fabric switch is set to ON or OFF.
Connection Type	Select the topology. • FC-AL: Fibre Channel arbitrated loop • P-to-P (point-to-point). NOTE: Some fabric switches require that you specify point-to-point topology. If you enable a fabric switch, check the documentation for the fabric switch to determine whether your switch requires point-to-point topology.

5. Check the set contents in the Confirm window and enter a task name in [Task Name].

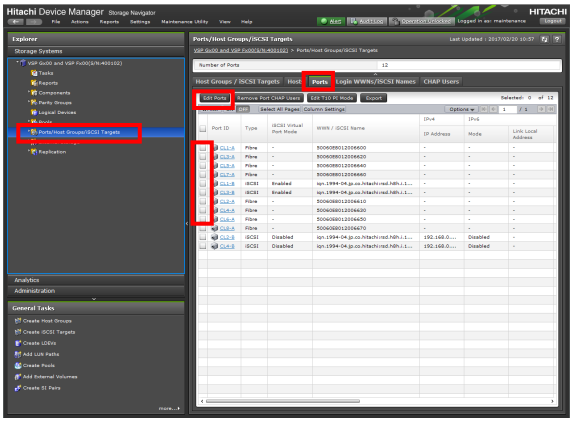
6. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

7. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.10.2 Editing iSCSI

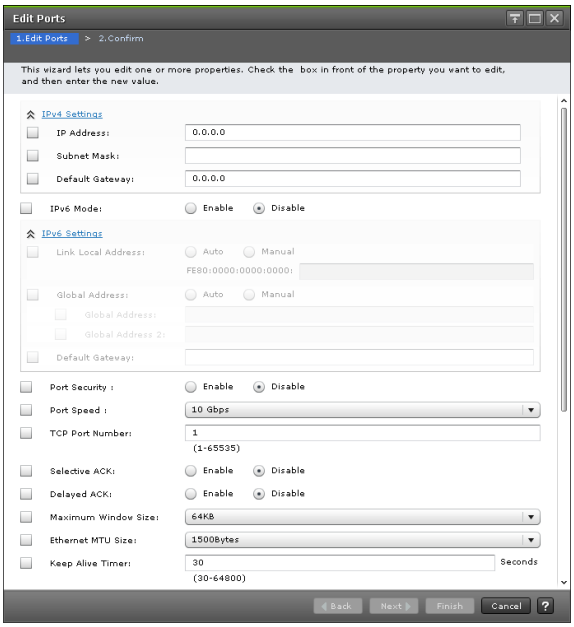
1. Select [Storage Systems]-[Ports/Host Groups/iSCSI Targets]. Click the [Ports] tab.



2. Check [Type] is specified [iSCSI], and then check the check box of the port that you want to edit.

3. Click [Edit Ports].

4. The Edit Ports window appears. Check the checkboxes of the items to be edited, enter the setting information, and then click [Finish].



Information Setting Area (When Selecting iSCSI)

Item	Description
IPv4 settings (*1)	Set the information corresponding to IPv4. • [IP Address]: Enter an IP address. Note that, when selecting multiple ports, you cannot enter the IP address. • [Subnet Mask]: Enter a subnet mask. • [Default Gateway]: Enter a default gateway.
IPv6 mode (*1)	Set this to enable IPv6. • [Enable]: Enable the IPv6 mode. In this case, you can set each item of [IPv6 settings]. • [Disable]: Disable the IPv6 mode.

IPv6 settings (*1)	Set the information corresponding to IPv6.
	• [Link Local Address]: Set a link local address.
	  • [Auto]: Set a link local address automatically.
	  • [Manual]: Set a link local address manually. Enter the address into the text box.
	• [Global Address]: Select the setting method of a global address from Auto or Manual.
	  • [Auto]: Set a global address automatically.
	  • [Manual]: Set a global address manually.
	  • [Global Address]: When [Manual] is selected, enter an address into the global address 1. This item is a must for [Manual].
	  • [Global Address 2]: When [Manual] is selected, enter an address into the global address 2. This item is optional.
	• [Default Gateway]: Enter an address into the default gateway.

Port Security	Set the LUN security of the port. • [Enable]: Enable the LUN security of the port. • [Disable]: Disable the LUN security of the port.
Port Speed	Select the data transfer speed of the port. The unit is Gbps (Gigabit per second). Auto, 10 Gbps and 1 Gbps are selectable for Copper. Optic is fixed to 10 Gbps. When selecting [Auto], the transfer speed is set to 1 Gbps or 10 Gbps automatically by the Storage System. (*2)
TCP Port Number (*1)	Set a TCP port number.
Selective ACK (*1)	Set a selective ACK • [Enable]: Enable the selective ACK • [Disable]: Disable the selective ACK
Delayed ACK (*1)	Set a delayed ACK • [Enable]: Enable the delayed ACK. • [Disable]: Disable the delayed ACK.
Maximum Window Size (*1)	Set a maximum window size. The settable value is 64 KB, 128 KB, 256 KB, 512 KB or 1024 KB.
Ethernet MTU Size (*1)	Set an Ethernet MTU size. The settable value is 1500 bytes, 4500 bytes or 9000 bytes.

(To be continued)

(Continued from preceding page)

Item	Description
Keep Alive Timer (*1)	Set a time interval when executing the Keep Alive option.
VLAN Tagging Mode (*1)	Set a VLAN tagging mode. • [Enable]: Enable the VLAN tagging mode. Set an item of [VLAN ID]. • [Disable]: Disable the VLAN tagging mode.
iSNS Server (*1)	Set this to enable the iSNS server. • [Enable]: Enable the iSNS server. When this is enabled, set an IP address and a TCP port number. • [Disable]: Disable the iSNS server.
IP Address	Set an IP address in the IPv4 or IPv6 format.
TCP Port Number	Set a TCP port number.
CHAP User Name	Set the CHAP user name.
Secret	Set the secret used for host authentication.
Re-enter Secret	Re-enter the same characters for confirming the secret entry.

*1: The items cannot be set when the port is an iSCSI virtual port (the port whose iSCSI virtual port mode is [Enable]). Use Command Control Interface (CCI) when editing iSCSI virtual ports.

*2: If CNA or the switch supports 1 Gbps, fix the port transfer speed of the CHB (iSCSI Channel Board) to 1 Gbps and use it. If CNA or the switch supports 10 Gbps, fix the port transfer speed of the CHB to 10 Gbps and use it.

⚠ CAUTION

If you want to change multiple parameters for a port twice or more, wait until the currently applied task finishes, and perform the next setting change.

If you perform the next setting change (the next task) before the currently applied task finishes, only the setting done by the next task will be applied, so the result might be different from what you expected.

5. Check the set contents in the Confirm window and enter a task name in [Task Name].

6. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

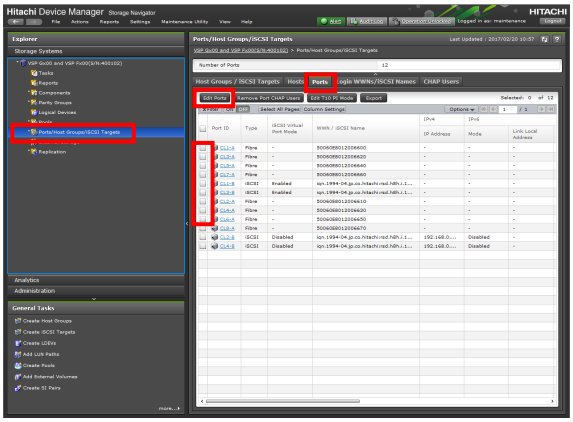
   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

7. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.10.3 Deleting Host Group Information

After you define host group information for the Fibre Channel ports on your storage system, use the following procedure to initialize the host group information.

1. In the Web Console window, select [Storage Systems]-[Ports/Host Groups/iSCSI Targets]. Click the [Ports] tab.

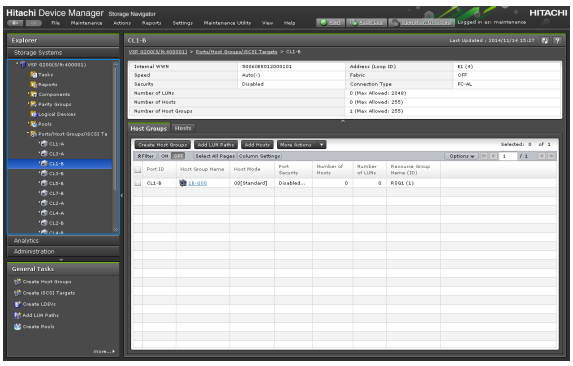


2. Check that any of [Fibre]/[iSCSI] is specified for [Type], and then click the port name that you want to edit.

3. The selected port window opens.

4. Click the [Host Groups] tab.

5. Check the check box of the host group that you want to initialize, and then click [More Actions] and select [Delete Host Groups].



6. Check the set contents in the Confirm windows and enter a task name in [Task Name].

7. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

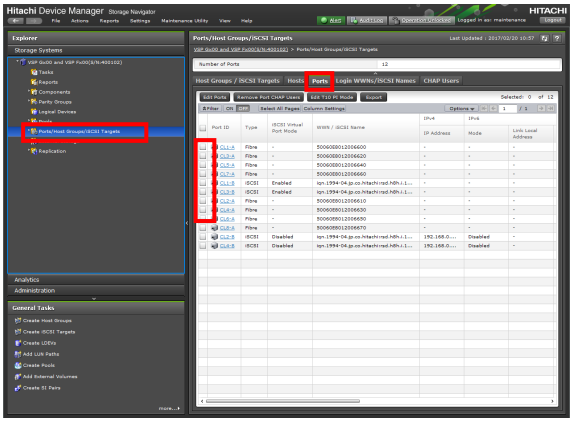
8. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.10.4 Deleting iSCSI Target Information

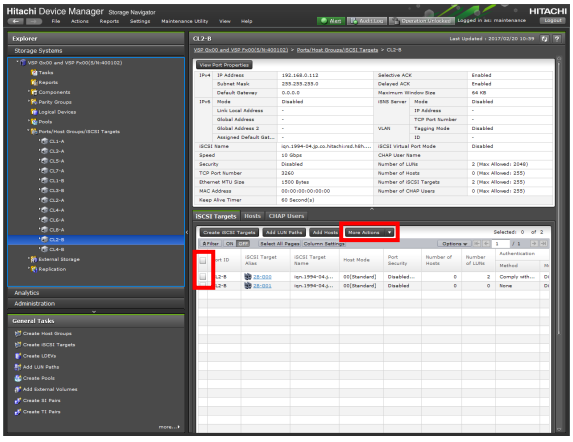
After you define target information for the iSCSI ports on your Storage System, use the following procedure to initialize the target information.

1. Select [Storage Systems]-[Ports/Host Groups/iSCSI Targets]. Click the [Ports] tab. Click the port in which the iSCSI target to be deleted is set.

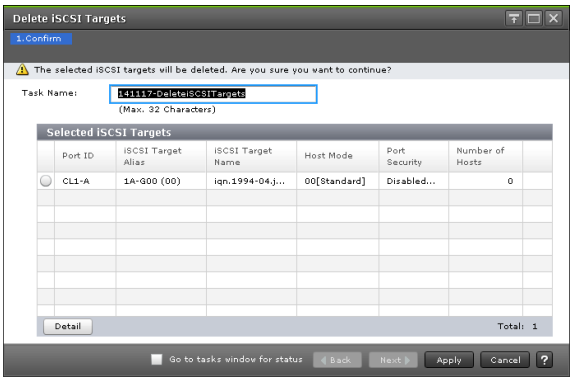
   NOTE: Check [Type] is specified “iSCSI”.



2. The [iSCSI Targets] tab is displayed. Check the check box of the iSCSI target to be deleted, and then click [More Actions]-[Delete iSCSI Targets].



3. The Confirm window appears. In the Confirm window, confirm the settings and specify the task name, and then click [Apply].
   Check the set contents in the Confirm window and enter a task name in [Task Name].



[Selected iSCSI Target] table

Item	Description
Port ID	Display a port name.
iSCSI Target Alias	Display an iSCSI target alias and ID.
iSCSI Target Name	Display an iSCSI target name.
Host Mode	Display a host mode.
Port Security	Display a LUN security setting of the port (Enable/Disable).
Number of Hosts	Display the number of hosts.
[Detail] button	Selecting rows and clicking the button display the iSCSI Target Property window.

4. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

5. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.10.5 Using CHAP Authentication with iSCSI Ports

Challenge Handshake Authentication Protocol (CHAP) is an optional iSCSI authentication method where the Storage System (target) authenticates iSCSI initiators on the host server.

The Storage System uses two types of CHAP authentication:
- One-way CHAP
- Mutual CHAP

With one-way CHAP, the Storage System authenticates all requests for access issued by the iSCSI initiator(s) on the host server via a CHAP secret.

To set up one-way CHAP authentication, you enter a CHAP secret on the Storage System and then configure each iSCSI initiator on the host server to send that secret each time it tries to access the Storage System.

With mutual CHAP, both the Storage System and the iSCSI initiator authenticate each other. To set up mutual CHAP, you configure the iSCSI initiator with a CHAP secret that the Storage System must send to the host sever to establish a connection. In this 2-way authentication process, both the host server and the Storage System are sending information that the other must validate before a connection is allowed.

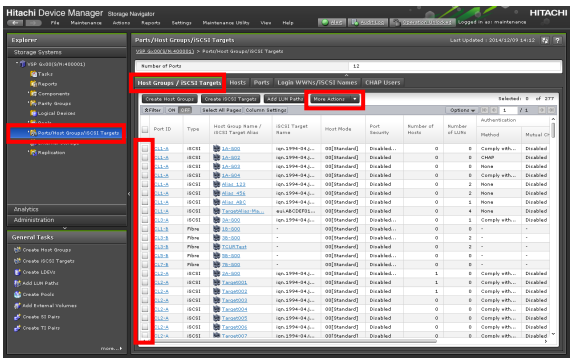
CHAP is an optional feature and is not required to use iSCSI. However, if you do not configure CHAP authentication, any host server connected to the same IP network as the Storage System can read from and write to the Storage System.

NOTICE: If you enable CHAP authentication on the Storage System, configure it on the host server as well using the iSCSI initiator. If you replace an HBA in an attached host, change the iSCSI Name setting in CHAP. If changing the MTU size, make the change in the Storage System and at the switch/host set.

3.10.5.1 Configuring One-Way CHAP

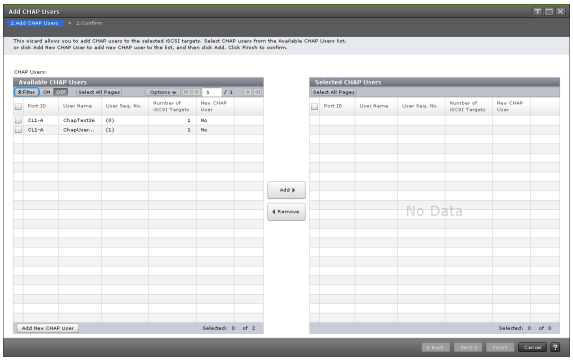
To set up one-way CHAP on the Storage System:

1. Select [Storage Systems]-[Ports/Host Groups/iSCSI Targets]. Click the [Host Groups/iSCSI Targets] tab.



2. Check a line to be added and click [More Actions]–[Add CHAP Users].

3. Select a CHAP user from the [Available CHAP Users] list and click [Add] to add it to the [Selected CHAP Users] list.
   In case of new addition, go to Step (1).
   After completing the addition of the necessary CHAP users, click [OK].

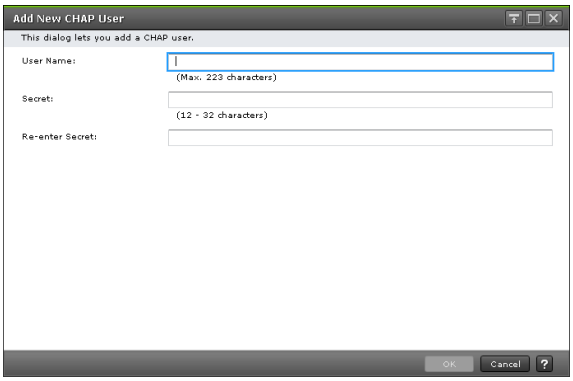


4. Click [Finish].

[Available CHAP Users] table and [Selected CHAP Users] table

Item	Description
Port name	Display a port name.
User name	Display a user name.
User Seq. No.	Display the user sequence ID in decimal notation in parentheses.
Number of iSCSI Targets	Display the number of iSCSI targets.
New CHAP User	Display whether the CHAP user is newly added. Display [Applied] if it is not connected to the port of the Storage System or it is a newly added CHAP user. Display [Not Applied] if it is a CHAP user already connected to the other port via a cable.
Add New CHAP User	When adding a new CHAP user, click [Add New CHAP User]. Note that, when adding a new CHAP user, the port name and iSCSI target name are blank.
[Add] button	Add the CHAP user selected from the [Available CHAP Users] table to the [Selected CHAP Users] table.
[Remove] button	Delete the CHAP user selected from the [Selected CHAP Users] table from the [Selected CHAP Users] table.

(1) When creating the new CHAP user, click [Add New CHAP User]. Enter the CHAP user information, and then click [OK].
Return to Step 3.



[Added CHAP Users] table

Item	Description
User Name	Set a user name. You can set one to 223 characters. One-byte alphanumeric characters (case-sensitive), one-byte spaces and the following one-byte symbols are available. . - + @ _ = : / [ ] ~
Secret	Set secret. One-byte alphanumeric characters, one-byte spaces and the following one-byte symbols are available. . - + @ _ = : / [ ] ~
Re-enter Secret	Re-enter the same characters for confirming the secret entry. If the same characters are not entered, an error occurs.

5. Check the set contents in the Confirm window and enter a task name in [Task Name].

6. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

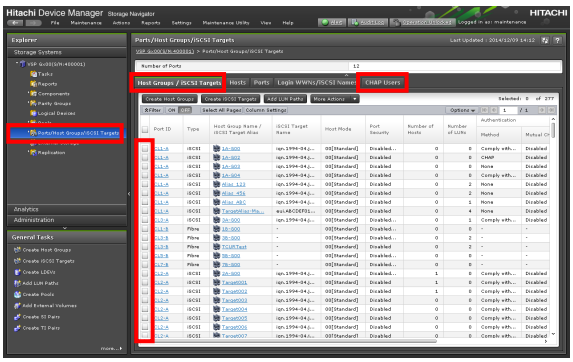
   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

7. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.10.5.2 Changing One-Way CHAP Settings

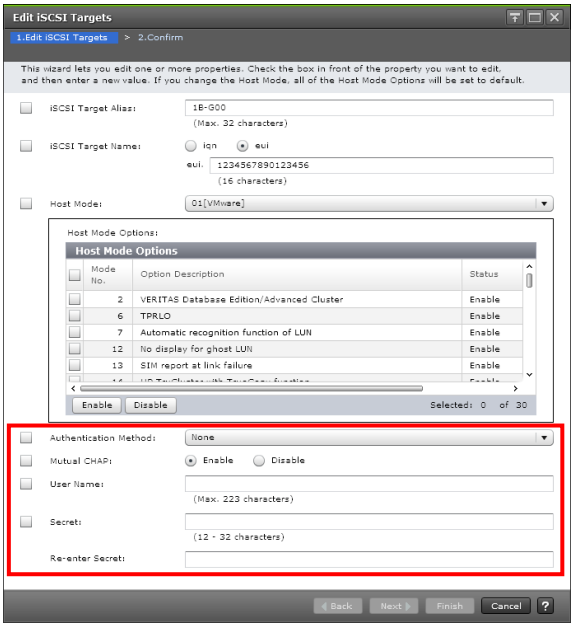
You can set the authentication mode in the Edit iSCSI Targets window.

1. Select [Storage Systems]-[Ports/Host Groups/iSCSI Targets]. Click the [Host Groups/iSCSI Targets] tab.



2. Check the check box of the iSCSI target that you want to edit. Click [More Actions] – [Edit iSCSI Target].

3. The Edit iSCSI Targets window appears. Enter the setting information and click [Finish].



Item		Description
iSCSI Target Alias		Display an iSCSI target alias. Up to 32 alphanumeric characters and symbols (! # $ % & ' + - . = @ ^ _ { } ~ ( ) [ ] space)
iSCSI Target Name		[ign] or [eui]: Select either format.
		Text box: Enter an iSCSI target name. • The following describes the iqn format. Format: iqn.1994-04.jp.co.hitachi:rsd. Model name.t. Serial number. Port name iSCSI target ID Display example: iqn.1994-04.jp.co.hitachi:rsd.h8s.t.62507. (Port ID) (iSCSI target ID) You can use up to 219 ASCII characters (alphanumeric characters and symbols). However, you cannot use the following symbols. \ / , ; * ? " < > | • The eui format is described. Format: eui. (OUI6 digits) (Storage System fixed value) (Serial number) (Port name) (iSCSI target ID) Display example: eui.02004567A425678D You can use 16-digit hexadecimal numbers.
Host Mode		Select a host mode from the list.
Host Mode Option		When setting a host mode option, select the host mode option to be set and click [Enable]. When a host mode option is unnecessary, select the unnecessary host mode option and click [Disable].
	Mode No.	Display a host mode option number.
	Option Description	Display the description of the host mode option.
	Status	Display the setting of the host mode option (Enable/Disable).
	[Enable] button	Enable a host mode option.
	[Disable] button	Disable a host mode option.
Authentication Method		Select a CHAP authentication setting ([CHAP], [None] or [Comply with Host Setting]). Selecting [CHAP] can set the following options.
Mutual CHAP		Select the two-way authentication mode ([Enable] or [Disable]). When selecting [Enable], the mode becomes the two-way authentication. When selecting [Disable], the mode becomes the one-way authentication.
User Name		Set a user name. When selecting [Disable] for [Mutual CHAP], the setting is arbitrary. When selecting [Enable] for [Mutual CHAP], the setting is indispensable. You can set one to 223 characters. One-byte alphanumeric numbers (case-sensitive), one-byte spaces and the following one-byte symbols are available. . - + @ _ = : / [ ] ~

(To be continued)

(Continued from preceding page)

Item	Description
Secret	Set secret used for host authentication. When selecting [Disable] for [Mutual CHAP], the setting is arbitrary. When selecting [Enable] for [Mutual CHAP], the setting is indispensable. You can set 12 to 32 characters. One-byte alphanumeric numbers, one-byte spaces and the following one-byte symbols are available. . - + @ _ = : / [ ] ~
Re-enter Secret	Re-enter the same characters for confirming the secret entry. When selecting [Disable] for [Mutual CHAP], the setting is arbitrary. When selecting [Enable] for [Mutual CHAP], the setting is indispensable.

4. Edit the setting, and then click [Finish].

5. Check the set contents in the Confirm window and enter a task name in [Task Name].

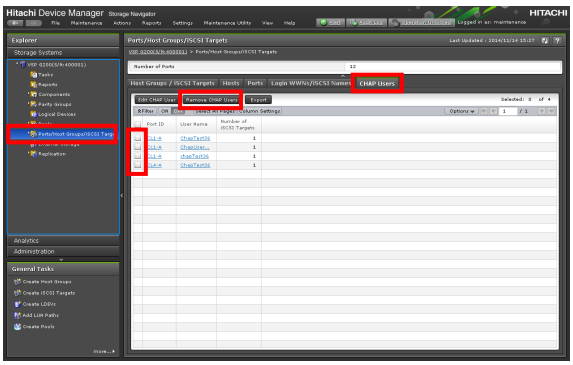
6. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

7. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

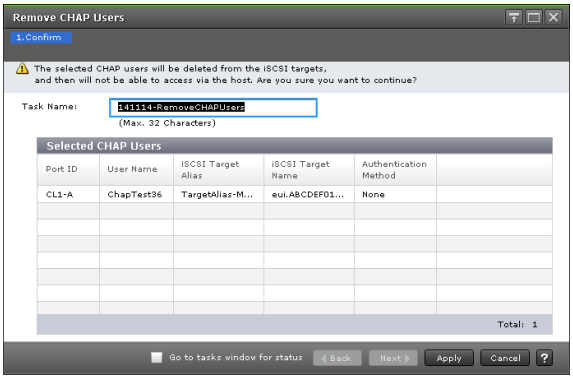
3.10.5.3 Deleting a One-Way CHAP User

1. Select [Storage Systems]-[Ports/Host Groups/iSCSI Targets]. Click the [CHAP Users] tab.



2. Check the check box of the port name that you want to remove and then click [Remove CHAP Users].

3. Check the set contents in the confirm windows and enter a task name in [Task Name].



[Selected CHAP Users] table

Item	Description
Port ID	Display a port name.
User Name	Display a user name.
iSCSI Target Alias	Display an iSCSI target alias name and ID.
iSCSI Target Name	Display an iSCSI target name.
Authentication Method	Display a CHAP authentication setting (CHAP, None, Comply with Host Setting).

4. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

5. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.10.6 Deleting LUN Paths from Ports

Delete LUN paths defined for host groups/iSCSI targets allocated to ports.

1. From the [Storage Systems] tree in the Web Console window, select [Ports/Host Groups/iSCSI Targets].
2. Select host groups or iSCSI targets of the ports to be operated and select the [LUNs] tab.
3. Select the check box for the LDEV ID from which LUN paths are deleted.
4. Click [More Actions]-[Delete LUN Paths] to display the [Delete LUN Paths] window.
5. Confirm that the LU paths you want to delete are displayed in the [Selected LUN Paths] table.
6. Check the setting contents in the Confirm window and enter a task name in [Task Name].
7. Click [Apply] to apply the settings to the storage system. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

8. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

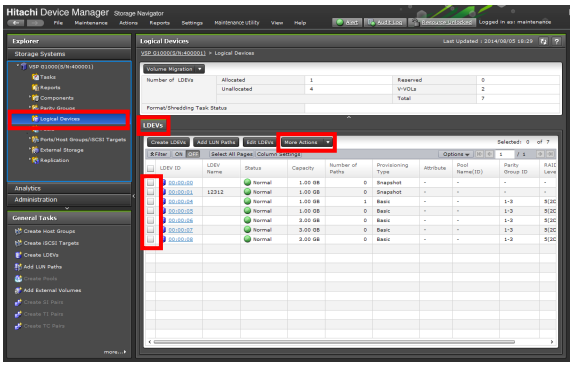
Blank Sheet

3.11 Logical Device Maintenance

When formatting or shredding the registered LEDVs, it is necessary to block the LDEVs in advance. When blocking LDEVs, you can select a parity group unit or LDEV unit as an operation unit. When releasing the LDEV blockade, you can select a parity group or LDEV group as an operation unit.

3.11.1 Blocking LDEVs

1. Select [Storage Systems]-[Logical Devices]. Click the [LDEVs] tab.

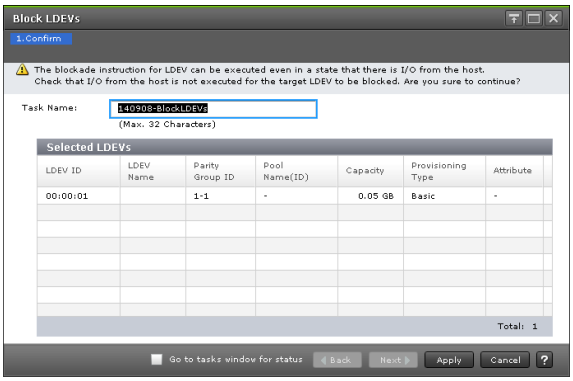


2. If [Blocked] does not appear in the [Status] column, you can use the following steps to block the LDEV. If [Blocked] does appear in the column, you can skip the remaining steps.

3. Select the LDEV.
   You can select multiple LDEVs that are listed together or separately.

4. Click [More Actions]-[Block LDEVs].

5. Note the settings in the Confirm window and enter a unique [Task Name] or accept the default and click [Apply].
   If “Go to tasks window for status” is checked, the Tasks window opens.



[Selected LDEVs] table

Item	Description
LDEV ID	LDEV identifier, which is the combination of LDKC, CU, and LDEV.
LDEV Name	LDEV name.
Parity Group ID	Parity group identifier.
Pool Name (ID)	Pool name and pool identifier.
Capacity	LDEV capacity.
Provisioning Type	Provisioning type assigned to the LDEV. Basic: Internal volume. DP: DP-VOL. External: External volume. Snapshot: Thin Image volume. ALU: LDEV of the ALU attribution.
Attribute	Displays the attribute of the LDEV. Command Device: Command device. Remote Command Device: Remote command device. ALU: LDEV of the ALU attribution. SLU: LDEV of the SLU attribution. Hyphen (-): Volume in which the attribute is not defined.

6. Click [Apply] to apply the settings to the Storage System.

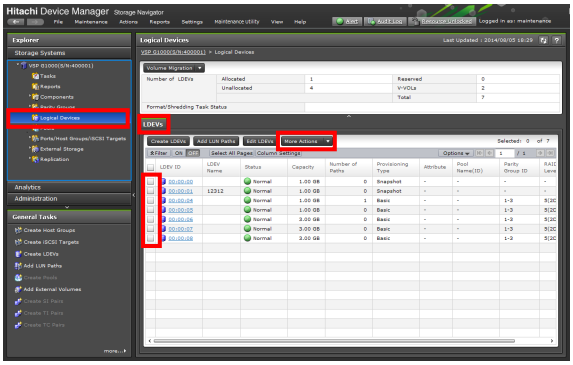
7. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

8. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.11.2 Restoring Blocked LDEVs

1. Select [Storage Systems]-[Logical Devices]. Click the [LDEVs] tab.

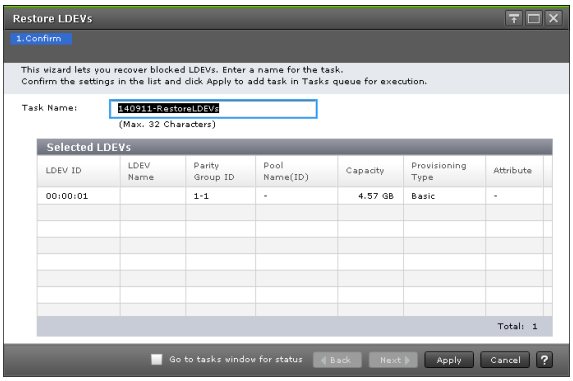


2. If [Blocked] appears in the [Status] column, you can use the following steps to restore the LDEV.
   If [Blocked] does not appear in the column, you can skip the remaining steps.

3. Select the LDEV.
   You can select multiple LDEVs that are listed together or separately.

4. Click [More Actions]-[Restore LDEVs].

5. Note the settings in the Confirm window and enter a unique [Task Name] or accept the default and click [Apply].
   If “Go to tasks window for status” is checked, the Tasks window opens.



Item	Description
LDEV ID	LDEV identifier, which is the combination of LDKC, CU, and LDEV.
LDEV Name	LDEV name.
Parity Group ID	Parity group identifier.
Pool Name (ID)	Pool name and pool identifier.
Capacity	LDEV capacity.
Provisioning Type	Provisioning type assigned to the LDEV. Basic: Internal volume. DP: DP-VOL. External: External volume. Snapshot: Thin Image volume. ALU: LDEV of the ALU attribution.
Attribute	Displays the attribute of the LDEV. Command Device: Command device. Remote Command Device: Remote command device. JNL VOL: Journal volume. ALU: LDEV of the ALU attribution. SLU: LDEV of the SLU attribution. Hyphen (-): Volume in which the attribute is not defined.

6. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

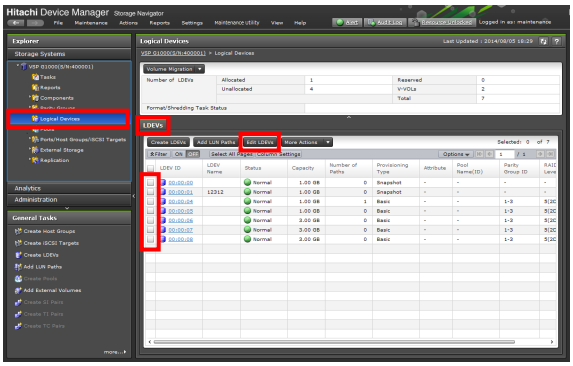
   NOTE:
   - When [Provisioning Type] of the target LDEV is [Basic], the task processing time for each [Parity Group ID] in which the target LDEV belongs increases by about five seconds.
   - To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

7. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.11.3 Editing an LDEV Name

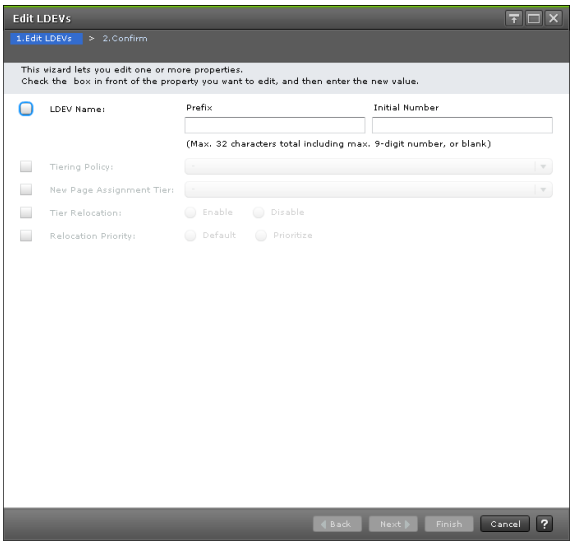
You can edit the name of a registered internal volume.
For information about editing a registered external volume, see Hitachi Universal Volume Manager User Guide.

1. Select [Storage Systems]-[Logical Devices]. Click the [LDEVs] tab.



2. Select the target LDEV. Click [Edit LDEVs].

3. In the Edit LDEVs window, edit the LDEV Name.



Item	Description
LDEV Name	Specify the LDEV name, using up to 32 characters. • Prefix: Fixed character string. • Initial Number: Initial number. Specify the initial number according to these examples. Example: - 1: Up to 9 numbers are added (1, 2, 3 ... 9) - 08: Up to 92 numbers are added (08, 09, 10 ...99) - 23: Up to 77 numbers are added (23, 24, 25 ...99) - 098: Up to 902 numbers are added (098, 099, 100 ... 999)
Tiering Policy	Specify the tiering policy for the LDEV. For details about the setting. You can specify this function only when the V-VOLs using Dynamic Tiering/active flash are available. See “Provisioning Guide for Open Systems”.
New Page Assignment Tier	Specify the new page assignment tier you want to assign to the LDEV. Middle is set by default. You can select from High, Middle, or Low. See “Provisioning Guide for Open Systems”. You can specify this function only when the V-VOLs that use Dynamic Tiering/active flash are available.
Tier Relocation	Specify Enable or Disable for the performing of the tier relocation. You can specify this function only when the V-VOLs using Dynamic Tiering/active flash are available.
Relocation Priority	Specify the relocation priority assigned to the LDEV. You can set this function under the following conditions: • When there are V-VOLs where Dynamic Tiering/active flash is enabled. • When the tier relocation is enabled.

4. Click [Finish].

5. In the Confirm window, confirm the settings, in Task Name type a unique name for this task or accept the default, and then click [Apply].
   If “Go to tasks window for status” is checked, the Tasks window opens.

6. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

7. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.11.4 Force Restore LDEVs

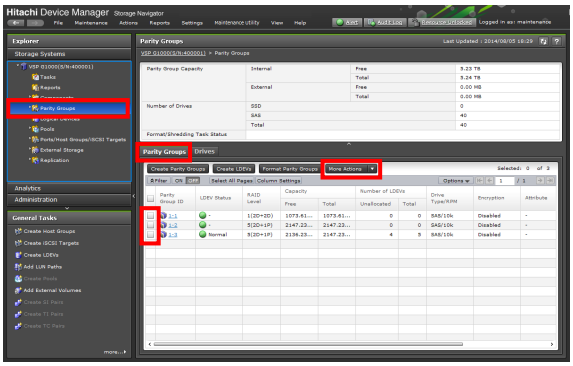
Prerequisites

LDEVs to be restored forcibly should be blocked.

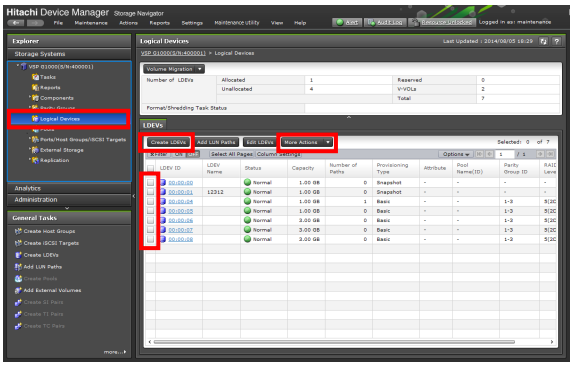
NOTE: When specifying a parity group, all the LDEVs belonging to the parity group should be blocked.

Procedure

1. Specify LDEVs to be restored forcibly.
   (1) When forcibly restoring all the LDEVs belonging to the parity group.
   Select [Parity Group] from the [Storage System] tree and display the [Parity Groups] tab. Check the check box of the parity group.

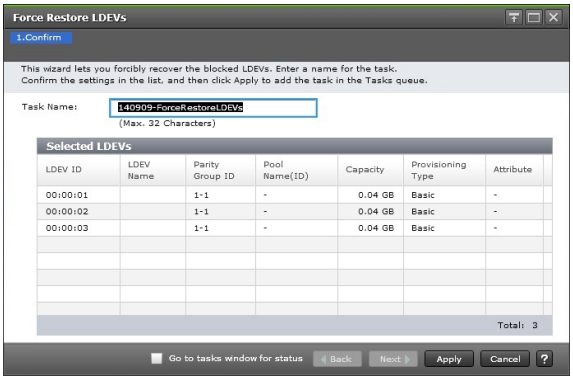


   (2) When forcibly restoring each LDEV.
   Select [Logical Device] from the [Storage System] tree and display the [LDEVs] tab. Select the check box of the LDEV.



2. Click [More Actions]-[Force Restore LDEVs].

3. Check the set contents in the Confirm window and enter a task name in [Task Name].



[Selected LDEVs]

Item	Description
LDEV ID	LDEV identifier, which is the combination of LDKC, CU, and LDEV.
LDEV Name	Displays the LDEV name.
Parity Group ID	Displays the parity group ID.
Pool Name (ID)	Pool name (Pool identifier)
Capacity	LDEV capacity
Provisioning Type	Provisioning type to be assigned to the LDEV. [Basic]: Internal volume. [DP]: DP-VOL. [External]: External volume. Snapshot: Thin Image volume. ALU: LDEV of the ALU attribution.
Attribute	Displays the attribute of the parity group. [Command Device]: Command device. ALU: LDEV of the ALU attribution. SLU: LDEV of the SLU attribution. [Hyphen(-)]: The parity group in which the attribute is not defined.

4. Click [Apply] to apply the settings to the Storage System.

5. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

NOTE:
- To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].
- Please call Technical Support Division for asking the password.

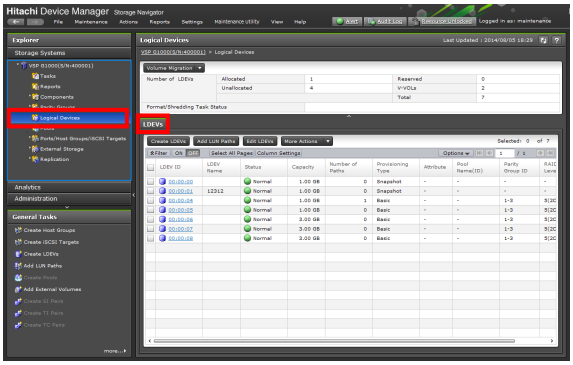
6. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.11.5 Blocking LDEVs (Without Safety Checks)

⚠ CAUTION

- Be sure to contact the Technical Support Division and follow the judgement before blocking LDEVs with the procedure.
- The procedure is able to operate only by Web Console of the Maintenance PC.

1. Select [Storage Systems]-[Logical Devices]. Click the [LDEVs] tab.

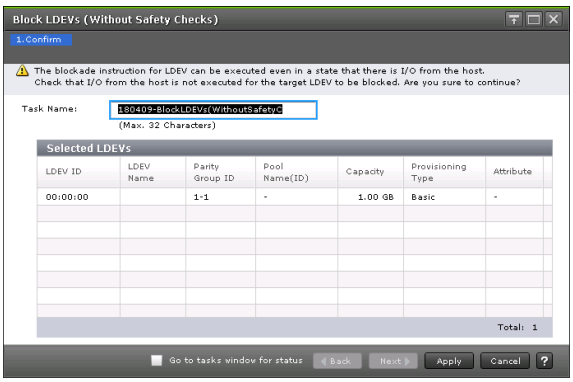


2. If [Blocked] does not appear in the [Status] column, you can use the following steps to block the LDEV. If [Blocked] appear in the [Status] column, you can skip the remaining steps.

3. Select the LDEV.
   You can select multiple LDEVs that are listed together or separately.

4. Click [More Actions]-[Forcible Actions without safety checks]-[Block LDEVs (Without Safety Checks)].

5. Check the set contents in the Confirm window and enter a task name in [Task Name].



[Selected LDEVs] table

Item	Description
LDEV ID	LDEV identifier, which is the combination of LDKC, CU, and LDEV.
LDEV Name	LDEV name.
Parity Group ID	Parity group identifier.
Pool Name (ID)	Pool name and pool identifier.
Capacity	LDEV capacity.
Provisioning Type	Provisioning type assigned to the LDEV. Basic: Internal volume DP: Dynamic Provisioning volume External: External volume Snapshot: Thin Image volume ALU: LDEV of the ALU attribute
Attribute	Displays the attribute of the LDEV. Command Device: Command device Remote Command Device: Remote command device ALU: LDEV of the ALU attribute SLU: LDEV of the SLU attribute Hyphen (-): Volume in which the attribute is not defined.

6. Click [Apply] to apply the settings to the Storage System.

7. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

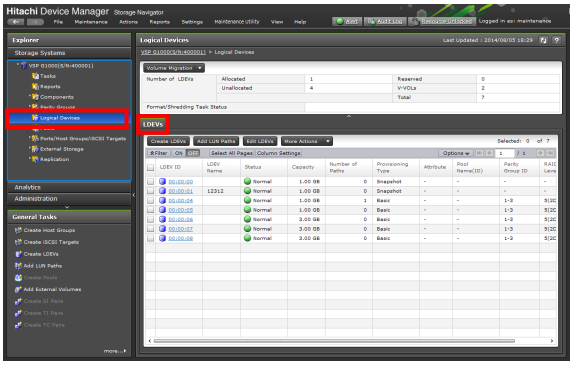
8. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.11.6 Restoring Blocked LDEVs (Without Safety Checks)

⚠ CAUTION

- Be sure to contact the Technical Support Division and follow the judgement before restoring blocked LDEVs with the procedure.
- The procedure is able to operate only by Web Console of the Maintenance PC.

1. Select [Storage Systems]-[Logical Devices]. Click the [LDEVs] tab.

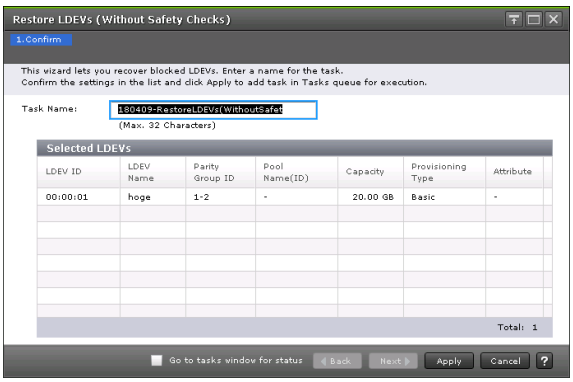


2. If [Blocked] appear in the [Status] column, you can use the following steps to restore the LDEV.
   If [Blocked] does not appear int the [Status] column, you can skip the remaining steps.

3. Select the LDEV.
   You can select multiple LDEVs that are listed together or separately.

4. Click [More Actions]-[Forcible Actions without safety checks]-[Restore LDEVs (Without Safety Checks)].

5. Check the set contents in the Confirm window and enter a task name in [Task Name].



[Selected LDEVs] table

Item	Description
LDEV ID	LDEV identifier, which is the combination of LDKC, CU, and LDEV.
LDEV Name	LDEV name.
Parity Group ID	Parity group identifier.
Pool Name (ID)	Pool name and pool identifier.
Capacity	LDEV capacity.
Provisioning Type	Provisioning type assigned to the LDEV. Basic: Internal volume DP: Dynamic Provisioning volume External: External volume Snapshot: Thin Image volume ALU: LDEV of the ALU attribute
Attribute	Displays the attribute of the LDEV. Command Device: Command device Remote Command Device: Remote command device JNL VOL: Journal volume ALU: LDEV of the ALU attribute SLU: LDEV of the SLU attribute Hyphen (-): Volume in which the attribute is not defined.

6. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

NOTE:
- When [Provisioning Type] of the target LDEV is [Basic], the task processing time for each [Parity Group ID] in which the target LDEV belongs increases by about five seconds.
- To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

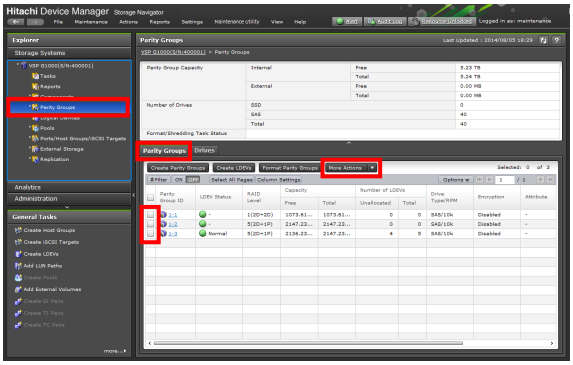
7. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.11.7 Force Restore LDEVs (Without Safety Checks)

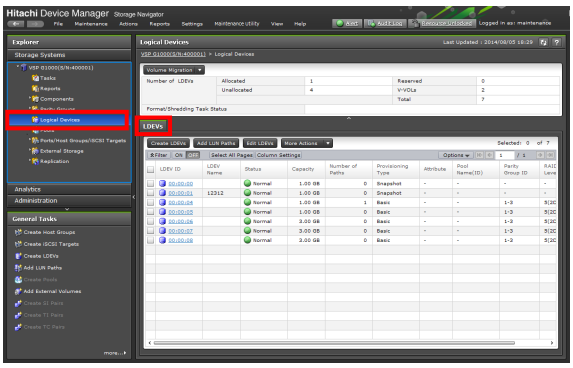
⚠ CAUTION

- Be sure to contact the Technical Support Division and follow the judgement before force restoring blocked LDEVs with the procedure.
- The procedure is able to operate only by Web Console of the Maintenance PC.
- Be sure to contact the Technical Support Division and ask them to release password for the operation.

1. Specify LDEVs to be restored forcibly.
   (1) When forcibly restoring all the LDEVs belonging to the parity group.
   Select [Parity Groups] from the [Storage Systems] tree and display the [Parity Groups] tab.
   Check the check box of the parity group.

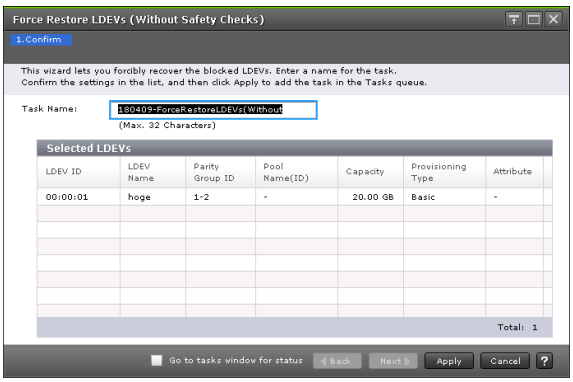


   (2) When forcibly restoring each LDEV.
   Select [Logical Devices] from the [Storage Systems] tree and display the [LDEVs] tab.
   Check the check box of the LDEV.



2. Click [More Actions]-[Forcible Actions without safety checks]-[Force Restore LDEVs (Without Safety Checks)].

3. Check the set contents in the Confirm window and enter a task name in [Task Name].



[Selected LDEVs] table

Item	Description
LDEV ID	LDEV identifier, which is the combination of LDKC, CU, and LDEV.
LDEV Name	LDEV name.
Parity Group ID	Parity group identifier.
Pool Name (ID)	Pool name and pool identifier.
Capacity	LDEV capacity.
Provisioning Type	Provisioning type assigned to the LDEV. Basic: Internal volume DP: Dynamic Provisioning volume External: External volume Snapshot: Thin Image volume ALU: LDEV of the ALU attribute
Attribute	Displays the attribute of the LDEV. Command Device: Command device Remote Command Device: Remote command device JNL VOL: Journal volume ALU: LDEV of the ALU attribute SLU: LDEV of the SLU attribute Hyphen (-): Volume in which the attribute is not defined.

4. Click [Apply] to apply the settings to the Storage System.

5. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

NOTE: • To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].
• Please contact Technical Support Division for asking the password.

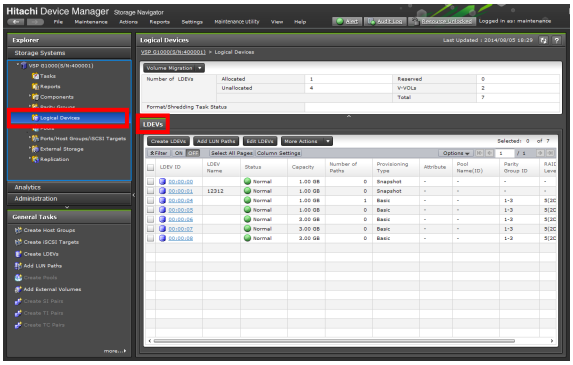
6. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.11.8 Shredding LDEVs (Without Safety Checks)

⚠ CAUTION

- Be sure to contact the Technical Support Division and follow the judgement before shredding LDEVs with the procedure.
- The procedure is able to operate only by Web Console of the Maintenance PC.

1. Select [Storage Systems]-[Logical Devices]. Click the [LDEVs] tab.

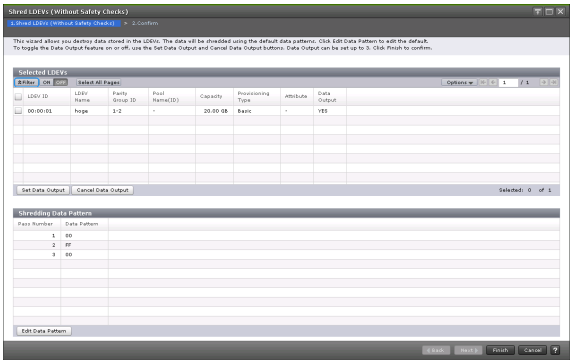


2. If [Blocked] appear in the [Status] column, you can use the following steps to shred the LDEV.

3. Select the LDEV.

4. Click [More Actions]-[Forcible Actions without safety checks]-[Shred LDEVs (Without Safety Checks)].

5. To save the shredding result to a file, click [Set Data Output]. You can output the shredding results of up to three volumes. If you don't want to save the results to a file, click [Cancel Data Output].



[Selected LDEVs] table

Item	Description
LDEV ID	LDEV identifier, which is the combination of LDKC, CU, and LDEV.
LDEV Name	LDEV name.
Parity Group ID	Parity group identifier.
Pool Name (ID)	Pool name and pool identifier.
Capacity	LDEV capacity.
Provisioning Type	Provisioning type assigned to the LDEV. Basic: Internal volume DP: Dynamic Provisioning volume External: External volume Snapshot: Thin Image volume ALU: LDEV of the ALU attribute
Attribute	Displays the attribute of the LDEV. Command Device: Command device Remote Command Device: Remote command device JNL VOL: Journal volume ALU: LDEV of the ALU attribute SLU: LDEV of the SLU attribute Hyphen (-): Volume in which the attribute is not defined.
Data Output	YES: The results of the shredding operation will be saved in a file. NO: The results of the shredding operation will be not saved in a file.

- Button

Item	Description
Set Data Output	If this button is selected, Yes appears in the Data Output column. If the data output setting is enabled, the results of the shredding operation will be saved in a file. Results can be saved for up to three volumes.
Cancel Data Output	If this button is selected, No appears in the Data Output column. If the data output setting is disabled, the results of the shredding operation will be not saved in a file.

[Shredding Data Pattern] table

Item	Description
Pass Number	Order of the overwrite pass.
Data Pattern	Dummy data pattern for the overwrite pass.

• Button

Item	Description
Edit Data Pattern	Click to open the Edit Shredding Data Pattern dialog box, which allows you to change the data pattern setting.

6. Click [Finish].

7. Verify the settings in the Shred LDEVs window.
   When the settings are correct, enter a unique task name or accept the default name.

8. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

9. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.12 Web Console Operation

Web Console and Storage Navigator have the common window display and operation. Refer to the “System Administrator Guide” for the details.

3.13 (Blank)

Blank Sheet

3.14 Verify (Parity Consistency Check)

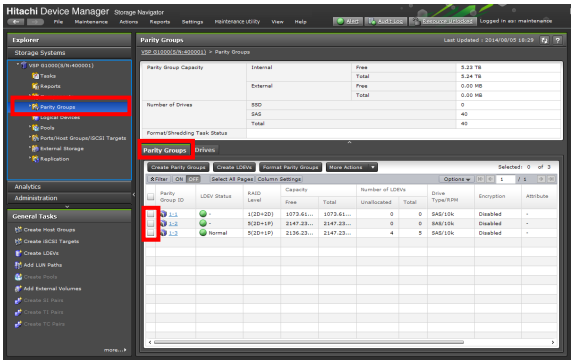
3.14.1 Executing Verify (Parity Consistency Check)

1. Select [Storage Systems]-[Parity Groups]. Click the [Parity Groups] tab.

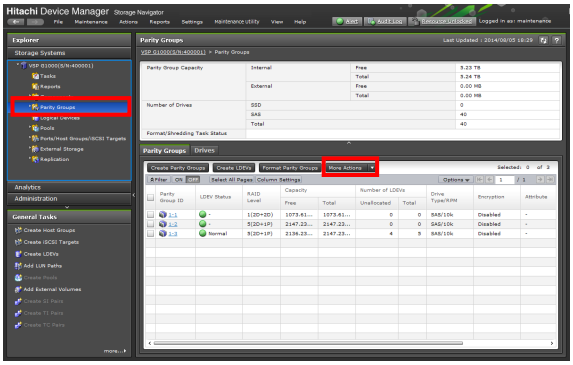
2. Set Verify from the [Parity Group] tab.
   - Select a parity group whose LDEV status is [Normal] or [Quick Format].
   - You can specify two or more parity groups. The number of parity groups you can specify is up to 16.
   - When specifying 17 or more parity groups, a message is displayed. Change the number of the specified parity groups up to 16.

   Go to Step 3.

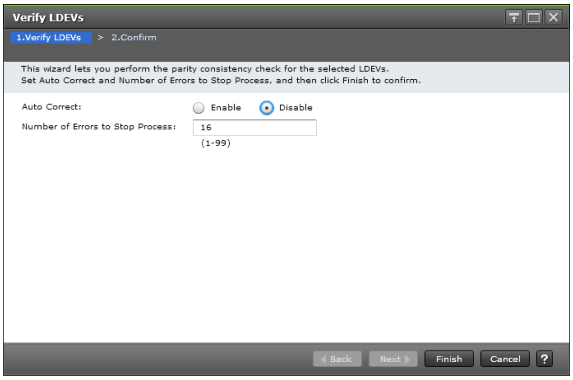
   NOTE: For a simple LDEV, set it from the [LDEVs] tab. Selectable LDEVs should have the LDEV status of [Normal] or [In Quick Format].



3. Click [More Actions]-[Verify LDEVs].



4. Set the items of “Auto Correct” and “Number of Errors to Stop Process” in the Verify LDEVs window.



Item	Description
Auto Correct	Set whether to correct the errors detected by Verify automatically. The initial value is set to [Disabled]. • Enable: Corrects the detected errors automatically. • Disable: Disables the automatic correction function.
Number of Errors to Stop Process	Count the number of errors detected by Verify in a parity group. When it reaches the set number, stop Verify. When it reaches the set number, stop Verify. Set the number of errors to stop Verify. The initial value is 16.

5. Click [Finish].

6. Check the set contents in the Confirm window and enter a task name in [Task Name].
   Selecting a row and clicking [Details] display the Resource Group Property window.

7. Click [Apply] to apply the settings to the Storage System.

8. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

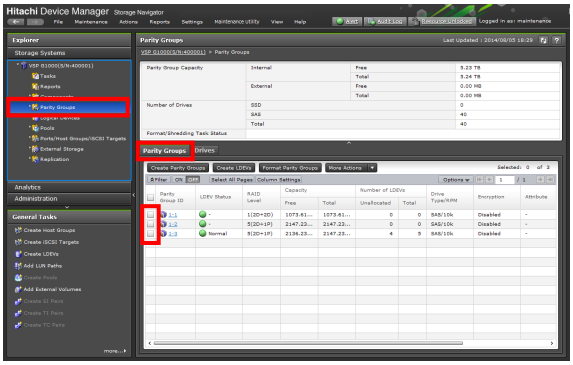
   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking "Apply"] in the wizard and click [Apply].

9. Check the task status in the Tasks window.
   When the task is completed, check the execution result of Verify according to the description in the table below.

Task status	Description
Completed	"Completed" indicates that Verify is completed for all specified parity groups. It just indicates the completion of Verify, and there might be parity inconsistency. Check the execution result of Verify by clicking the link on [Verification Result: yyyy/mm/dd hh:mm:ss] displayed in [Format/Shredding task status] in the Parity Groups window (WEBCON03-1140).
Failed	"Failed" is displayed when any of the following is met. • Verify is interrupted. • The number of detected errors reaches the number specified for [Number of Errors to Stop Process]. • Verify ended abnormally.
In progress	"In progress" indicates that Verify is in progress. You can check the progress of Verify by looking at [Verifying n% (x / y parity groups)] displayed in [Format/Shredding task status] in the Parity Groups window (WEBCON03-1140).

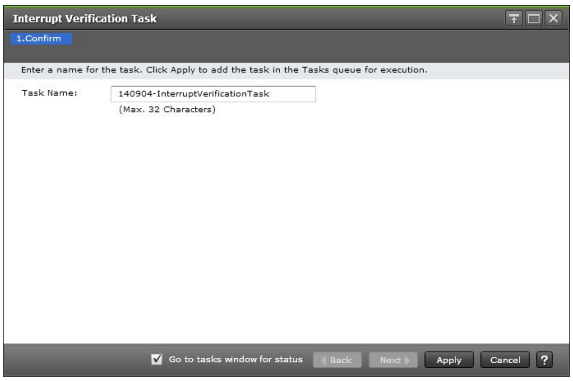
3.14.2 Interrupting Verify

1. Select [Storage Systems]-[Parity Groups]. Click the [Parity Groups] tab.



2. Click [More Actions]-[Interrupt Verification Task].

3. Check the set contents in the Confirm window and enter a task name in [Task Name].



Item	Description
Task Name	Confirm the settings, type a unique task name or accept the default, then click [Apply]. A task name is case-sensitive and can be up to 32 ASCII letters, numbers, and symbols. The default is <date>-<window name>.

4. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

5. Check the operation result in the Task window. Before execution, you can suspend or cancel the task in the Task window.

   NOTE: If you execute [Interrupt Verification Task], the end time of the verification task and the interruption task may differ by one to ten minutes on the Task window. Confirm the completion of the interruption by the completion of the verification task.

3.14.3 Checking the Progress

You can check the progress of the following items.

- Reference of format progress information
- Shredding
- Reference of Verify (parity consistency check) execution result

The three types of confirmation methods are available and you can check any of them.

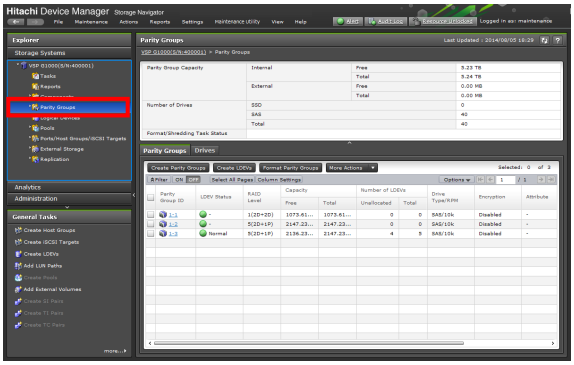
Check the progress in the Parity Group window : Refer to “3.14.3.1 Checking the Progress in the Parity Group Window”.

Check the progress in the “LDEV” window : Refer to “3.14.3.2 Checking the Progress in the “LDEV” Window”.

Check the progress with the task : Refer to “3.14.3.3 Checking the Progress in the Task”.

3.14.3.1 Checking the Progress in the Parity Group Window

1. Select [Storage Systems]-[Parity Groups]. Click the [Parity Groups] tab.



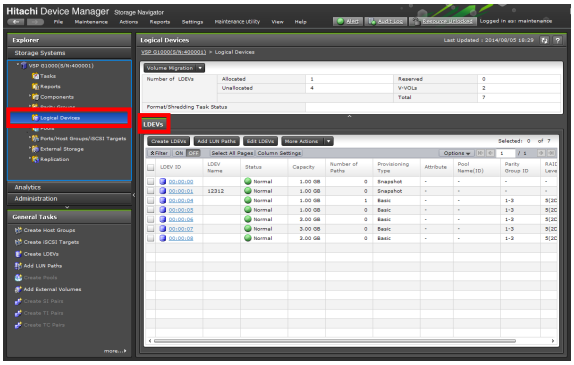
Item	Description
Parity group capacity	Displays the information on the parity group capacity. • Internal：Displays the information on the capacity of the internal volume. [Free] (*1) : Displays the capacity of free spaces of the internal volume. [Total] (*2) : Displays the capacity of all the internal volumes. • External：Displays the information on the capacity of the external volume [Free] (*1): Displays the capacity of free spaces of the external volume. [Total] (*2): Displays the capacity of all the external volumes.
Number of drives	• SSD : Displays the number of SSDs. • HDD : Displays the number of HDD Drives. • Total : Displays the total number of Drives.
Format/Shredding task status	[Formatting n%] : Displays the progress of formatting. [Preparing Quick Format n%] : Displays the progress of the preparing Quick Format. [Shredding n%] : Displays the progress of shredding. [Verifying n% (x / y parity groups)] : Displays the progress of Verify. The letters “n”, “x” and “y” indicate the Verification progress rate, the number of parity groups whose Verification is completed and the number of all parity groups which are Verification targets, respectively. [Verification Result: yyyy/mm/dd hh:mm:ss] : Display the previous Verification execution date and time. Display nothing if Verification is not executed or in execution. This display is linked. Clicking the link displays the Verification execution result in another window. Blank : When formatting or shredding is not executed, the display is a blank. Furthermore, if the storage configuration is changed and the information cannot be gathered, the display is also a blank.

*1: [Free] does not include the capacity of the control information (e.g. control cylinder) used on the Storage System.

*2: [Total] displays the capacity adding the LDEV capacity and the [Free] capacity.

3.14.3.2 Checking the Progress in the “LDEV” Window

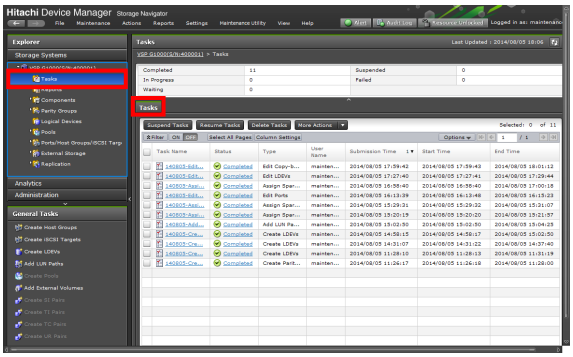
1. Select [Storage Systems]-[Logical Devices]. Click the [LDEVs] tab.



Item	Description
[Number of LDEVs]	Displays the information on the number of LDEVs. • [Defined]: Displays the number of LDEVs of the allocated open systems (excluding virtual VOLs). • [Undefined]: Displays the number of LDEVs of the unallocated open systems (excluding virtual VOLs). • [Reservation]: Displays the number of LDEVs of the reserved open systems. • [V-VOL]: Displays the number of virtual VOLs of the allocated open systems.
Number of total LDEVs	Displays the number of total LDEVs.
Format/Shredding task status	[Formatting n%]: Displays the progress of formatting. [Preparing Quick Format n%]: Displays the progress of the preparing Quick Format. [Shredding n%]: Displays the progress of shredding. [Verifying n% (x / y parity groups)] : Displays the progress of Verify. The letters “n”, “x” and “y” indicate the Verification progress rate, the number of parity groups whose Verification is completed and the number of all parity groups which are Verification targets, respectively. [Verification Result: yyyy/mm/dd hh:mm:ss] : Display the previous Verification execution date and time. Display nothing if Verification is not executed or in execution. This display is linked. Clicking the link displays the Verification execution result in another window. Blank : When formatting or shredding is not executed, the display is a blank. Furthermore, if the storage configuration is changed and the information cannot be gathered, the display is also a blank.

3.14.3.3 Checking the Progress in the Task

1. Select [Storage Systems]-[Tasks]. Click the [Tasks] tab.



This window displays a list of tasks performed on the storage system. Up to 384 tasks can display, including 256 that are Completed and/or Failed. Up to 128 tasks whose statuses are In Progress, Waiting, and Suspended can also display.

Summary

Item	Description
Completed	Number of completed tasks.
In Progress	Number of tasks in progress.
Waiting	Number of tasks waiting.
Suspended	Number of suspended tasks.
Failed	Number of tasks in which an error occurred.

[Tasks] tab

Item	Description
Task Name	Task name specified by a user when the user performed the task. Click to view the detail of the task.
Status	Task status. Click to view more details about status or errors. • : Completed or Completed(Request) : the task completed normally. NOTE: It just indicates the completion of Verify, and there might be parity inconsistency. Check the execution result of Verify by clicking the link on [Verification Result: yyyy/mm/dd hh:mm:ss] displayed in [Format/Shredding task status] in the Parity Groups window (WEBCON03-1140). • : In progress: the task is being processed by the system. • : Waiting: the task is not yet started. • : Suspended: the task has been suspended. • : Failed: the task ended abnormally.
Type	General name of the task.
User Name	User name who performed the task.
Submission Time	Date and time when the task was submitted.
Start Time	Date and time when the task was started. Blank indicates the task has not started yet.
End time	Date and time when the task completed. Blank indicates the task has not completed yet.

Item	Description
Auto Delete	Enabled: A task is automatically deleted when the following two events occur: • The task is completed • The number of tasks in the Task list reaches the maximum number the window can display (384) Disabled: Tasks will remain displayed until users delete them. Tasks whose status is Failed are automatically Disabled by the system.
[Suspend Tasks] 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	Deletes the selected tasks from the window. • The waiting or suspended tasks will be cancelled. • The failed or aborted tasks can be deleted from the window. • Tasks in progress cannot be deleted. • 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](*1)	When disabled, the selected task remains in the task list after the task is completed.
[Enable Auto Delete](*1)	When enabled, the selected task is deleted from the Task list when the following two events occur: • The task is completed • The number of tasks in the Task list reaches the maximum number the window can display (384)
[Export](*1)	Window for saving table information to a file.

*1: Appears when you click [More Actions].

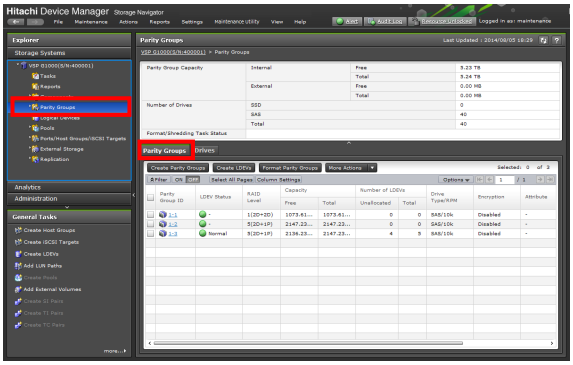
2. Check the information on the concerned task.
   You can check the detailed information by clicking the link of the task name.

3.14.4 Executing Verify (Parity Consistency Check) (Without Safety Checks)

CAUTION

- Be sure to contact the Technical Support Division and follow the judgement before verifying with the procedure.
- The procedure is able to operate only by Web Console of the Maintenance PC.

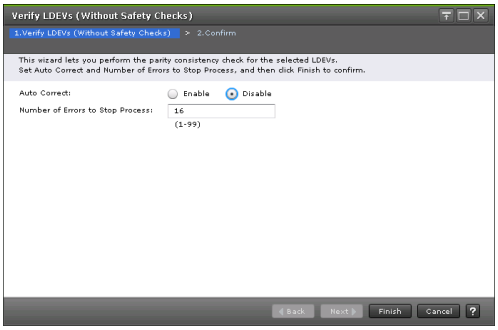
1. Select [Storage Systems]-[Parity Groups]. Click the [Parity Groups] tab.



2. Check the target parity group.

3. Click [More Actions]-[Forcible Actions without safety checks]-[Verify LDEVs (Without Safety Checks)].

4. Set the items of “Auto Correct” and “Number of Errors to Stop Process” in the “Verify LDEVs (Without Safety Checks)” window.



Item	Description
Auto Correct	Set whether to correct the errors detected by Verify automatically. The initial value is set to [Disable]. • Enable: Corrects the detected errors automatically. • Disable: Disables the automatic correction function.
Number of Errors to Stop Process	Count the number of errors detected by Verify in a parity group. When it reaches the set number, stop Verify. Set the number of errors to stop Verify. The default value is 16.

5. Click [Finish].

6. Check the set contents in the Confirm window and enter a task name in [Task Name].

7. Click [Apply] to apply the settings to the Storage System.

8. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

9. Check the task status in the Tasks window.
   When the task is completed, check the execution result of Verify according to the description in the table below.

Task status	Description
Completed	“Completed” indicates that Verify is completed for all specified parity groups. It just indicates the completion of Verify, and there might be parity inconsistency. Check the execution result of Verify by clicking the link on [Verification Result: yyyy/mm/dd hh:mm:ss] displayed in [Format/Shredding task status] in the Parity Groups window (WEBCON03-1140).
Failed	“Failed” is displayed when any of the following is met. • Verify is interrupted. • The number of detected errors reaches the number specified for [Number of Errors to Stop Process]. • Verify ended abnormally.
In progress	“In progress” indicates that Verify is in progress. You can check the progress of Verify by looking at [Verifying n% (x / y parity groups)] displayed in [Format/Shredding task status] in the Parity Groups window (WEBCON03-1140).

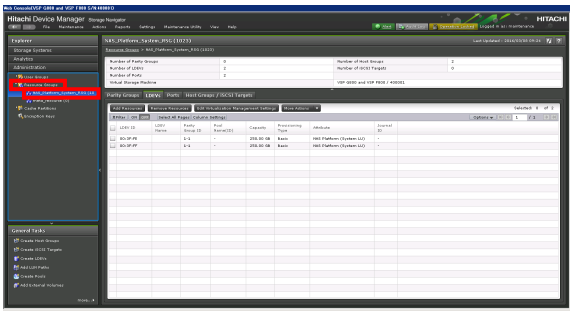
3.15 Managing Resource Group

3.15.1 Adding LDEVs to Resource Group

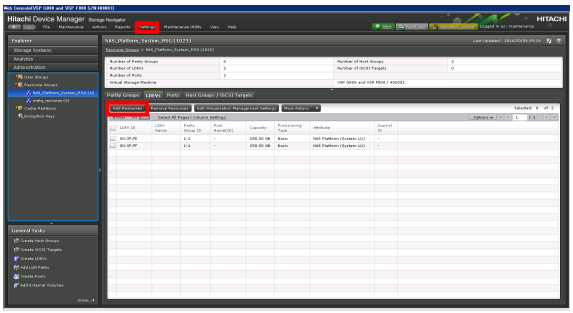
Add arbitrary LDEVs to an arbitrary resource group.

1. Select [Resource Groups] from the [Administration] tree in the Web Console window.

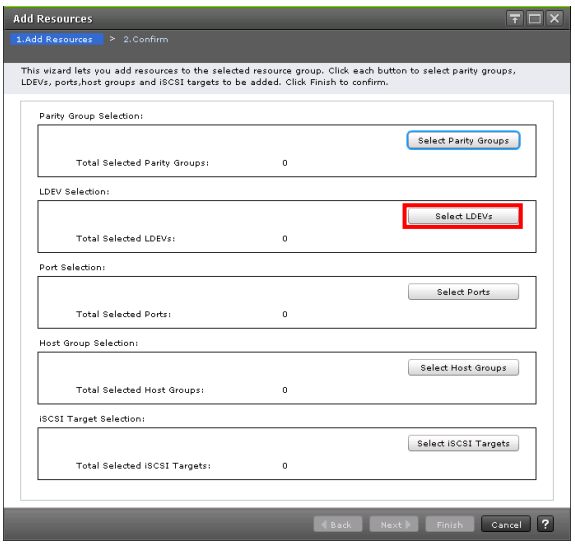
2. Click the resource group name to add LDEVs under [Resource Groups].
   The individual Resource Groups window is displayed.



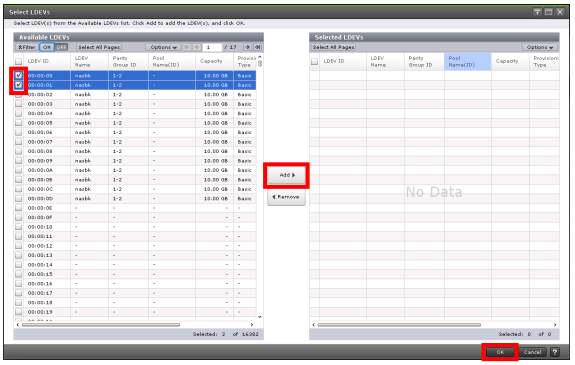
3. Display the Add Resources window in either of the following ways.
   - Click [Add Resources].
   - Select [Resource Administration] – [Add Resources] from the [Settings] menu.



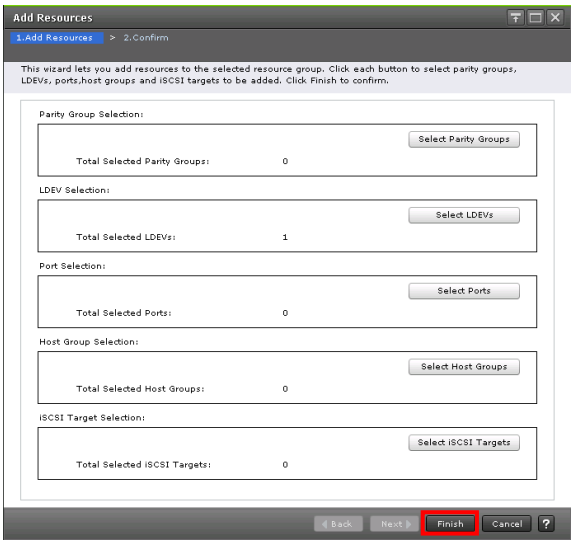
4. The Add Resources window is displayed. Click [Select LDEVs].



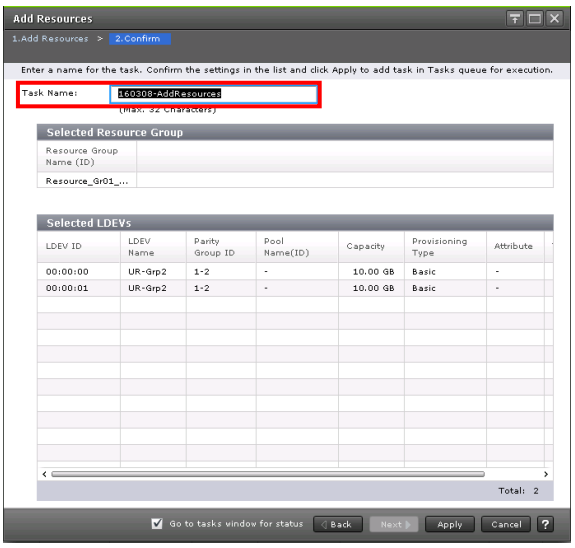
5. The Select LDEVs window is displayed. Select LDEVs to be added and click [Add]. If the addition of the selected LDEVs is confirmed, click [OK].



6. The Add Resources window is displayed again. Click [Finish].



7. Confirm the set contents in the confirmation window and enter the task name in [Task Name].



8. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

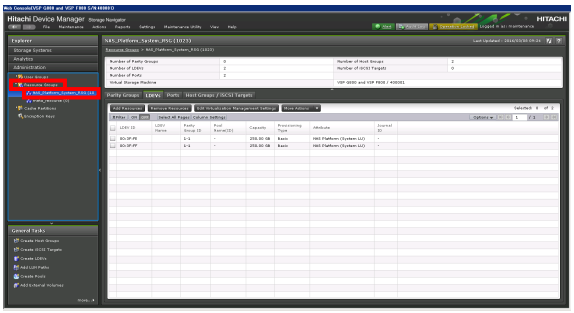
9. Check the operation result the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.15.2 Removing LDEVs from Resource Group

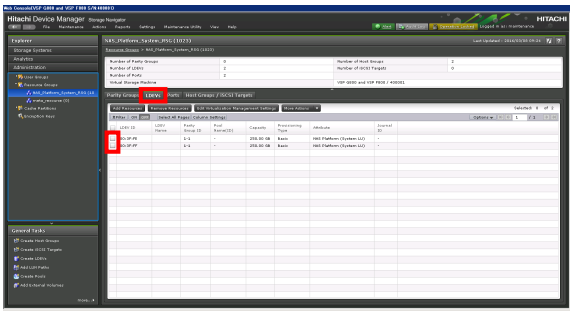
Remove arbitrary LDEVs belonging to an arbitrary resource group.

1. Select [Resource Groups] from the [Administration] tree in the Web Console window.

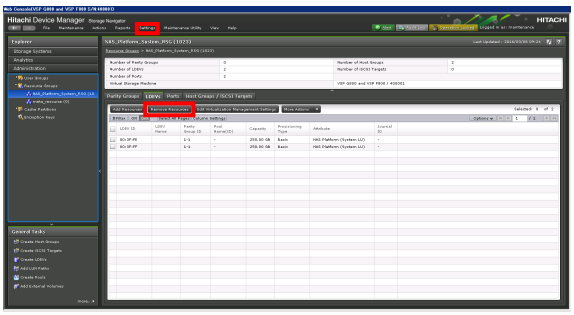
2. Click the resource group name to remove LDEVs under [Resource Groups].
   The individual Resource Groups window is displayed.



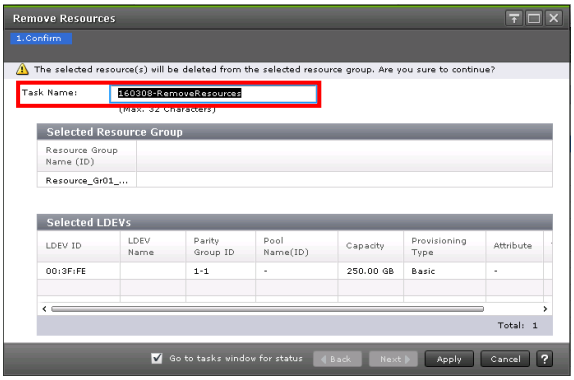
3. Select the [LDEVs] tab. Select LDEVs to be removed.



4. Display the Remove Resources window in either of the following ways.
   - Click [Remove Resources].
   - Select [Resource Administration] – [Remove Resources] from the [Settings] menu.



5. Confirm the set contents in the Remove Resources window and enter the task name in [Task Name].



6. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

   NOTE: To display the Task window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

7. Check the operation result the Task window. Before execution, you can suspend or cancel the task in the Task window.

3.16 Encryption Keys

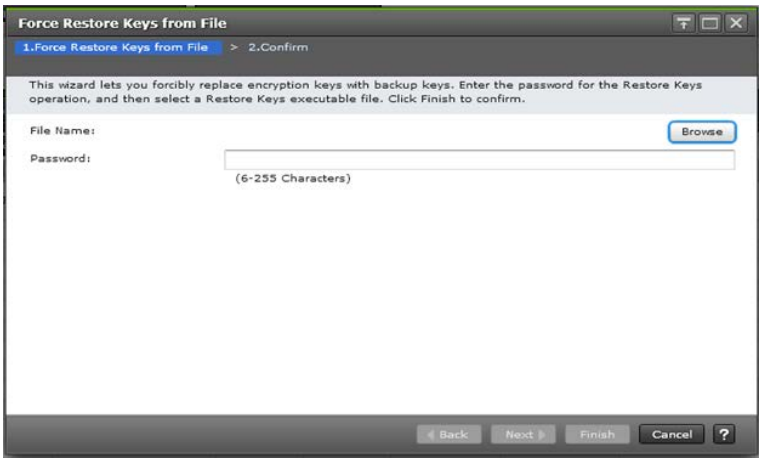
From the [Administration] tree menu in the navigation area in the left part of the Storage Navigator main window, click [Encryption Keys] to display the Encryption Keys window.

3.16.1 Force Restore Keys from File

This function restores encryption keys from the files backed up in the PC on which Storage Navigator operates. Even the encryption key files to which the Restore Keys from File function cannot be applied can be restored with the Force Restore Keys from File function.
For the Restore Keys from File function, refer to “Encryption License Key User Guide”.

1. In the Encryption Keys window, select [Restore Keys]-[From File(Force)]. The Force Restore Keys from File window is displayed.

2. In the Force Restore Keys from File window, select an encryption key file and enter the password.



3. Click [Finish].

4. In the Confirm window, confirm the settings, and enter the task name in [Task Name].

5. Click [Apply] to apply the settings to the storage system.
   The settings are queued as tasks and the tasks are executed sequentially.

   NOTE: To display the Task window automatically after the wizard is closed, select [Go to tasks window for status] and click [Apply] in the wizard.

6. In the Task window, check the operation result.
   When a task is not executed yet, you can suspend or cancel the task in the Task window.

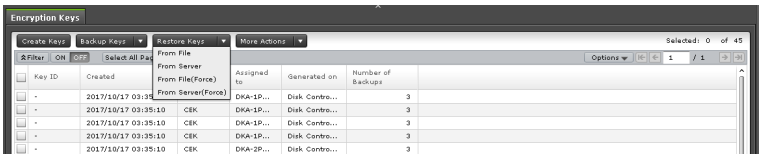
   NOTE: Restore the latest encryption key. If the encryption key that is not the latest one is restored for the reason that the encryption key is changed after the secondary backup and for other reasons, the drives and the disk boards (DKB) might be blocked and might not be able to read data.

   NOTE: To restore the encryption key, all the volumes belonging to the parity group for which the encryption key is set must be blocked.
   In addition, after the restoration of the encryption key, all the volumes belonging to the parity group for which the encryption key is set must be restored.

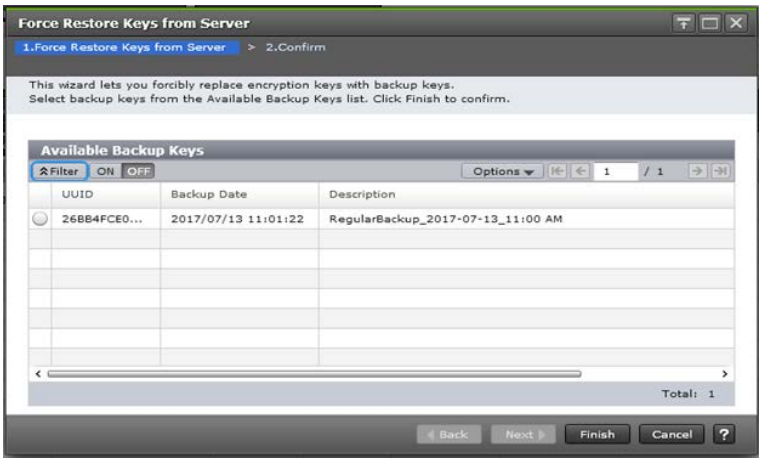
3.16.2 Force Restore Keys from Server

This function restores encryption keys by connecting to the key management server.
Even the encryption keys to which the Restore Keys from Server function cannot be applied can be restored with the Force Restore Keys from Server function.
For the Restore Keys from Server function, refer to “Encryption License Key User Guide”.

1. In the Encryption Keys window, select [Restore Keys]-[From Server(Force)]. The Force Restore Keys from Server window is displayed.



2. In the Force Restore Keys from Server window, click the radio button of the encryption key to be forcibly restored.



3. Click [Finish].

4. In the Confirm window, confirm the settings, and enter the task name in [Task Name].

5. Click [Apply] to apply the settings to the storage system.
   The settings are queued as tasks and the tasks are executed sequentially.

   NOTE: To display the Task window automatically after the wizard is closed, select [Go to tasks window for status] and click [Apply] in the wizard.

6. In the Task window, check the operation result.
   When a task is not executed yet, you can suspend or cancel the task in the Task window.

   NOTE: Restore the latest encryption key. If the encryption key that is not the latest one is restored for the reason that the encryption key is changed after the secondary backup and for other reasons, the drives and the disk boards (DKB) might be blocked and might not be able to read data.

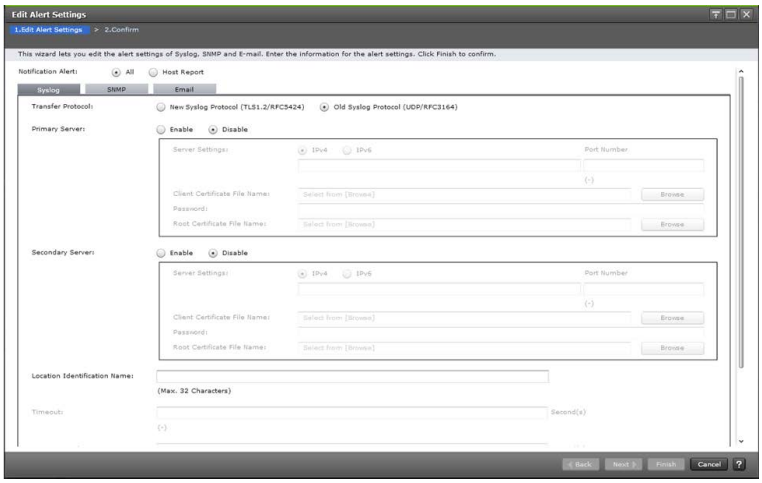
   NOTE: To restore the encryption key, all the volumes belonging to the parity group for which the encryption key is set must be blocked.
   In addition, after the restoration of the encryption key, all the volumes belonging to the parity group for which the encryption key is set must be restored.

3.17 Alert Notifications

This is a window to set the alert (SIM: Service Information Message) notice destination. The alert notice method supports E-mail transmission, SNMP trap transmission and Syslog server transfer.
For details of the windows of alert notifications, see “System Administrator Guide”.

1. Starting Edit Alert Settings window
   From the [Settings] menu of the Web Console window, select [Environmental Settings]-[Edit Alert Settings].

2. The Edit Alert Settings window is displayed.



3.17.1 Setting up Email Notification when Storage System Failures Occur

You can set the required information to notify the service information message (SIM) by email.

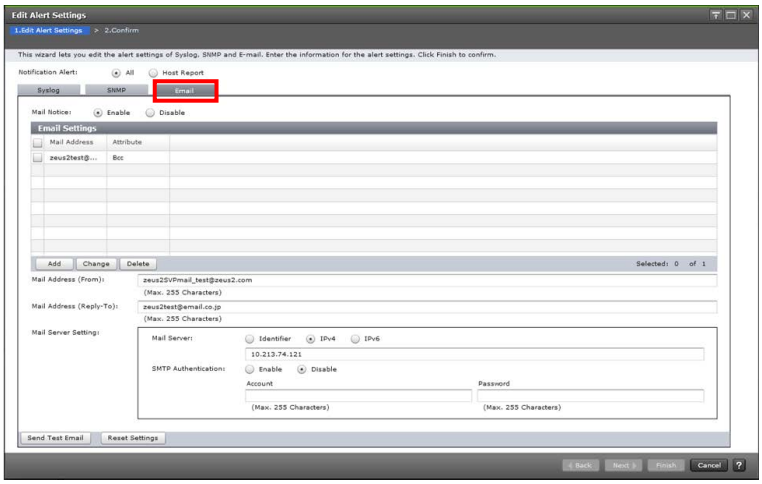
3.17.1.1 Prerequisites

- You must have a mail server that supports the Simple Mail Transfer Protocol (SMTP).
- If a firewall is used, port 25 must be used.

3.17.1.2 Procedure

1. Starting Edit Alert Settings window.
   From the [Settings] menu of the Web Console window, select [Environmental Settings]-[Edit Alert Settings].

2. In the Edit Alert Settings window, click the [Email] tab.
   Select a target SIM for notifying alerts at [Notification Alert].
   The target SIM for notifying alerts is common for Email, Syslog, and SNMP.



Item	Description
Notification Alert	Selects a target SIM for notifying alerts. • [Host Report]: Reports the alert to only the SIMs that report to the host. • [All]: Reports the alert to all SIMs. The target SIM for notifying alerts is common for Email, Syslog, and SNMP.
Mail Notice	Selects whether to notify the service information message (SIM) • [Enable]: Notifies the service information message (SIM) by mail. • [Disable]: Does not notify the service information message (SIM) by mail.
Email Settings	The attribute to transmit the failure information (SIM) and the mail address are displayed on the [Email Settings] table. If selected [Enable] at [Mail Notice], you must set up this item. • [Mail Address]: Displays the mail address. • [Attribute]: It displays a mail attribute (To/Cc/Bcc). • [Add]: It adds a mail address. The Add Address window opens. • [Change]: It changes the selected mail address and its attribute. The Change Settings window opens. You can select more than one mail address. When you select more than one mail address, you can change only attributes. • [Delete]: It deletes the selected mail address. You can select more than one mail address.

(To be continued)

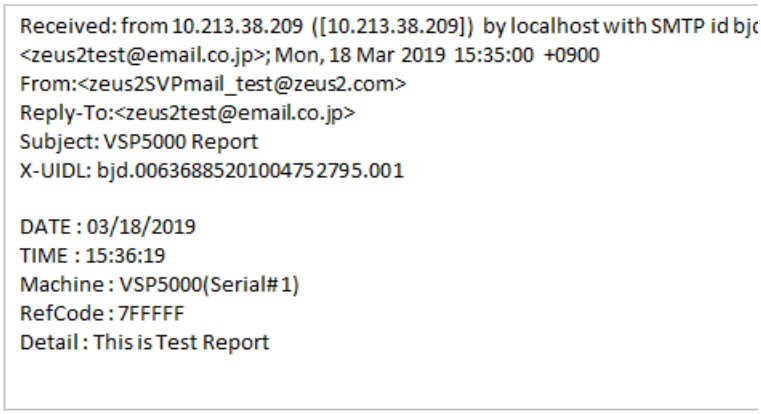
(Continued from preceding page)

Item	Description
Mail Address (From)	Specifies an email address of the sender to notify the service information message (SIM). Enter up to 255 alphanumeric characters (ASCII codes) and symbols: (! # $ % & ` + - * / ‘ ^ { } _ . @ ~ = ?). If selected [Enable] at [Email Notice], you must set up this item.
Mail Address (Reply-To)	Specifies a Reply-To address of email. If you specify this address, replies from the email receivers will be sent to this address. If you omit this address, replies from the email receivers will be sent to Mail Address (From). Enter up to 255 alphanumeric characters (ASCII codes) and symbols: (! # $ % & ` + - * / ‘ ^ { } _ . @ ~ = ?).
Mail Server Settings - Mail Server	Specifies a mail server information. You cannot set all 0 (zero) to the IP address. • [Identifier]: To specify a host name, select Identifier and enter up to 63 alphanumeric characters (ASCII codes) and symbols: (! $ % - . @ _ ` ~). • [IPv4]: To set an IPv4 address, select IPv4 and enter four integers in the range of 0 to 255 (for example, XXX.XXX.XXX.XXX, where X is a number). • [IPv6]:To set an IPv6 address, select IPv6 and enter eight hexadecimal alphanumeric in the range of 0 to FFFF. An abbreviated style of IPv6 address can also be specified. (for example, YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY, where Y is a hexadecimal digit). If selected [Enable] at [Email Notice], you must set up this item.
Mail Server Settings - SMTP Authentication	Select whether to use the SMTP authentication. • [Enable]: Uses the SMTP authentication. • [Disable]: Does not use the SMTP authentication. If selected [Enable], you must enter [Account] and [Password]. Enter up to 255 alphanumeric characters (ASCII codes) and symbols: (! $ % - . @ _ ` ~).

3. Select [Enable] at [Mail Notice].
4. At [Email Settings], specify the attributes (To, Cc, or Bcc) of the destination mail addresses.
5. Specify [Mail Address (From)] (required) and [Mail Address (Reply-To)] (arbitrary).
6. Specify [Mail Server] information.
7. At [SMTP Authentication], if you use the SMTP authentication, select [Enable]. If you do not use the SMTP authentication, select [Disable]. If selected [Enable], enter [Account] and [Password] to use the SMTP authentication.
8. Click [Send Test Email] to check whether a test mail is sent.
9. Click [Finish].
10. In the Edit Alert Settings confirmation window, check the settings and enter a task name in [Task Name].
11. Click [Apply].
    The task is registered. If the [Go to tasks window for status] check box is checked, the Tasks window opens.

3.17.1.3 Example of Test Mail

An example of a test email follows:



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

NOTE: When using the E-mail software having a function to delete line feed codes automatically, cancel the Auto Delete function of the line feed codes. If the Auto Delete function of the line feed codes is not cancelled, a non-breaking E-mail text is displayed.

Item	Description
Mail title	email title (name of storage system) + (Report)
Date	Date when a system failure occurred.
Time	Time when a system failure occurred.
Machine	Name and serial number of the storage system.
RefCode	Reference code. The same code as the one reported by SNMP traps.
Detail	Failure details. The same information as the one reported by SNMP traps.

See the SIM RC SECTION (SIMRC00-00) for reference codes and failure details.

3.17.2 Setting up Syslog Notification

You can set the required information to notify in Syslog format when storage system failures occur.

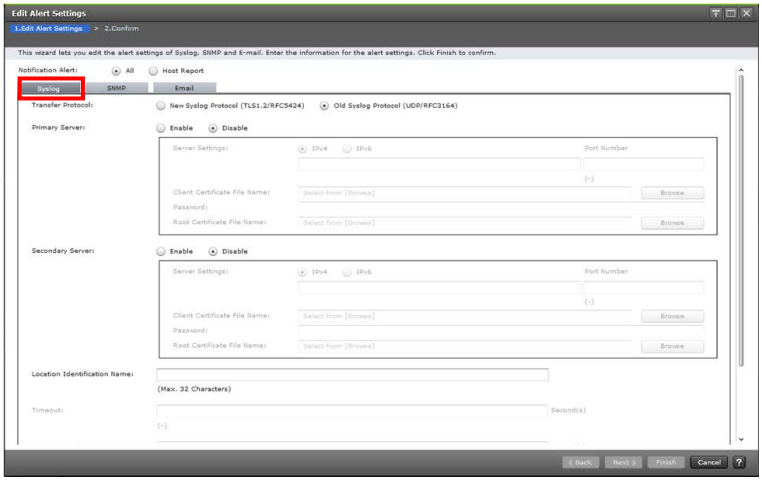
3.17.2.1 Prerequisites

- You must have a server that supports Syslogs.
- If a firewall is used, a port must be opened to transfer Syslogs.

3.17.2.2 Procedure

1. Starting Edit Alert Settings window.
   From the [Settings] menu of the Web Console window, select [Environmental Settings]-[Edit Alert Settings].

2. In the Edit Alert Settings window, click [Syslog] tab.
   Select a target SIM for notifying alerts at [Notification Alert].
   The target SIM for notifying alerts is common for Email, Syslog, and SNMP.



Item	Description
Notification Alert	Selects a target SIM for notifying alerts. • [Host Report]: Reports the alert to only the SIMs that report to the host. • [All]: Reports the alert to all SIMs. The target SIM for notifying alerts is common for Email, Syslog, and SNMP.
Transfer Protocol	Selects the Syslog transfer protocol. • [New Syslog Protocol (TLS1.2/RFC5424)] • [Old Syslog Protocol (UDP/RFC3164)]
Primary Server	Selects whether to use the Syslog server. • [Enable]: Notifies the service information message (SIM) to the Syslog server in Syslog format . • [Disable]: Does not notify the service information message (SIM) to the Syslog server in Syslog format.
Primary Server - Server Settings	Specifies an IP address of a server you want to set as a Syslog server. You cannot set all 0 (zero) to the IP address. • To set an IPv4 address, select [IPv4] and enter four integers in the range of 0 to 255 (for example, XXX.XXX.XXX.XXX, where X is a number). • To set an IPv6 address, select [IPv6] and enter eight hexadecimal alphanumeric in the range of 0 to FFFF. An abbreviated style of IPv6 address can also be specified. (for example, YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY, where Y is a hexadecimal digit). Specifies this item only when [Enable] is selected at [Primary Server].
Primary Server - Port Number	Specifies a port number to be used at the Syslog server. Specifies this item only when [Enable] is selected at [Primary Server].

(To be continued)

(Continued from preceding page)

Item	Description
Primary Server - Client Certificate File Name	Specifies a certificate file. Click [Browse], and then specify a certificate file. You must set this item only when [New Syslog Protocol (TLS1.2/ RFC5424)] is selected at [Transfer Protocol] and when [Enable] is selected at [Primary Server]. • Be sure to set it when changing the items of the certificate from inactive to active. • After applying the setting, if the certificate is not set (blank) when applying the setting again, the previously updated certificate is used.
Primary Server - Password	Enters a password for the client certificate. Up to 128 characters can be entered for the password. Allowed characters are alphanumeric characters and symbols: ! # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~. Specifies this item only when [Client Certificate File Name] is specified.
Primary Server - Root Certificate File Name	Specifies a certificate file. Click [Browse], and then specify a certificate file. You must set this item only when [New Syslog Protocol (TLS1.2/ RFC5424)] is selected at [Transfer Protocol] and when [Enable] is selected at [Primary Server]. • Be sure to set it when changing the items of the certificate from inactive to active. • After applying the setting, if the certificate is not set (blank) when applying the setting again, the previously updated certificate is used.
Secondary Server	Selects whether to use an alternative server (secondary server) to the Syslog server. • [Enable]: Notifies the service information message (SIM) to the secondary server in Syslog format . • [Disable]: Does not notify the service information message (SIM) to the secondary server in Syslog format.
Secondary Server - Server Settings	Specifies an IP address of a server you want to set as a secondary server. The restriction for the available values is the same as that of [Primary Server-Syslog Server].
Secondary Server - Port Number	Specifies a port number to be used on the secondary server. Specifies this item only when [Enable] is selected at [Secondary Server].
Secondary Server - Client Certificate File Name	Specifies a certificate file. Click [Browse], and then specify a certificate file. This item is settable only when [New Syslog Protocol (TLS1.2/ RFC5424)] is selected at [Transfer Protocol] and when [Enable] is selected at [Primary Server]. • Be sure to set it when changing the items of the certificate from inactive to active. • After applying the setting, if the certificate is not set (blank) when applying the setting again, the previously updated certificate is used.
Secondary Server - Password	Specifies a password for the client certificate. Up to 128 characters password can be entered. The restriction for the available values is the same as that of [Primary Server-Password].

(To be continued)

(Continued from preceding page)

Item	Description
Secondary Server-Root Certificate File Name	Specifies a certificate file. Click [Browse], and then specify a certificate file. This item is settable only when [New Syslog Protocol (TLS1.2/ RFC5424)]) is selected at [Transfer Protocol] and when [Enable] is selected at [Primary Server]. • Be sure to set it when changing the items of the certificate from inactive to active. • After applying the setting, if the certificate is not set (blank) when applying the setting again, the previously updated certificate is used.
Location Identification Name	Specifies an arbitrary name for the storage system that transfers the service information message (SIM) to the Syslog servers, so that you can identify the storage system. Enter 32 characters at the maximum. Allowed characters are alphanumeric characters and symbols: ! " # $ % & ' ( ) * + - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~. A comma (,). Be sure to set it only when [Primary Server] or [Secondary Server] is [Enable].
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	Specifies the retry interval when the communication with the Syslog server fails in the range of 1 to 60 seconds. The default is 1. Specifies this item only when [New Syslog Protocol (TLS1.2/ RFC5424)] is selected at [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].

3. Select the Syslog transfer protocol at [Transfer Protocol] in the [Syslog] tab.

4. If you want to transfer the Syslog to the primary server, select [Enable] at [Primary Server], go to Step 5.
   If you do not transfer the Syslog to the primary server, go to Step 7.

5. Specify the IP address and port number.

6. Specify the client certificate file, password, and root certificate file name. Specify this item only when [New Syslog Protocol (TLS1.2/ RFC5424)] is selected at [Transfer Protocol].

7. If you want to transfer the Syslog to the secondary server, select [Enable] at [Secondary Server], go to Step 8.
   If you do not transfer the Syslog to the secondary server, go to Step 10.

8. Specify the IP address and port number.

9. Specify the client certificate file, password, and root certificate file name. Specify this item only when [New Syslog Protocol (TLS1.2/ RFC5424)] is selected at [Transfer Protocol].

10. Specify an arbitrary name for the storage system in [Location Identification Name], so that you can identify the storage system.

11. Specify [Timeout], [Retry Interval] and [Number of Retries] when [New Syslog Protocol (TLS1.2/ RFC5424)] is selected at [Transfer Protocol].

12. If necessary, click [Send Test Message to Syslog Server] to test the settings.

13. Confirm that a log (detailed data: "RefCode: 7fffff, This is Test Report.") is received in the Syslog Server.

14. Click [Finish].

15. In the Edit Alert Settings confirmation window, check the settings and enter the task name in [Task Name].

16. Click [Apply].
    The task is registered. If the [Go to tasks window for status] check box is checked, the Tasks window opens.

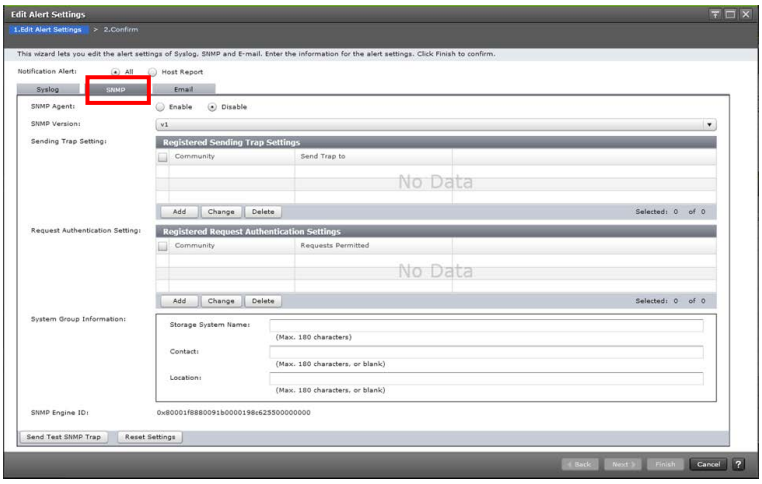
3.17.3 Setting up SNMP Notification

You can set the required information to notify in SNMP trap when storage system failures occur.

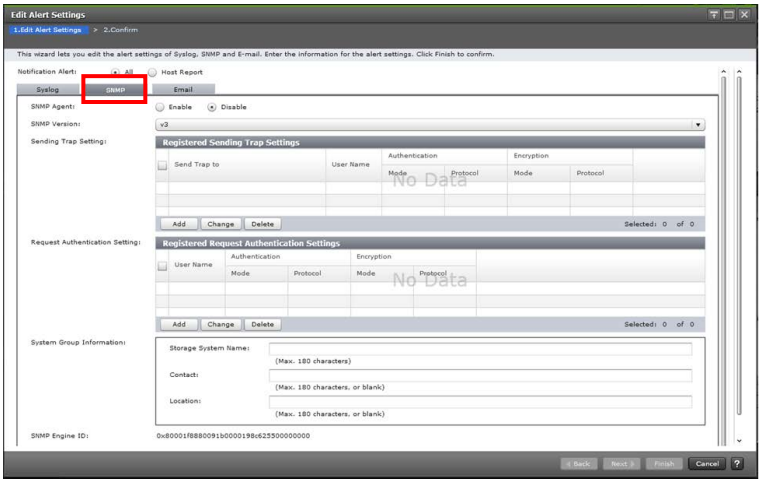
3.17.3.1 Procedure

1. Starting Edit Alert Settings window.
   From the [Settings] menu of the Web Console window, select [Environmental Settings]-[Edit Alert Settings].

2. The Edit Alert Settings window appears. Click [SNMP] tab.
   Set the transmission information of the SNMP which notifies storage system failures.
   [When selecting v1 or v2c for the SNMP version]



   [When selecting v3 for the SNMP version]



Item	Description
Notification Alert	Selects a target SIM for notifying alerts. • [Host Report]: Reports the alert to only the SIMs that report to the host. • [All]: Reports the alert to all SIMs. The target SIM for notifying alerts is common for Email, Syslog, and SNMP.
SNMP Agent	Selects whether to use the SNMP agent. • [Enable]: Notifies the service information message (SIM) by SNMP trap and accept GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST (*1). • [Disable]: Does not notify the service information message (SIM) by SNMP trap and does not accept GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST (*1).
SNMP Version	Selecting the SNMP Protocol version.
Sending Trap Setting	[Community](*2) Displays the community name accepting the SNMP trap report [Send Trap to] Displays the IP address that reports the SNMP trap. [User Name](*3) Displays the user name used for the SNMP trap report. [Authentication] - [Mode](*3) Displays whether the authentication by the password is enabled. [Authentication] - [Protocol](*3) When the authentication by the password is enabled, displays the authentication method. [Encryption] - [Mode](*3) Displays whether the encryption is enabled. [Encryption] - [Protocol](*3) When the encryption is enabled, displays the encryption method. For the settings, see “3.17.3.2 Adding SNMP Trap Notification Destinations” .

(To be continued)

(Continued from preceding page)

Item	Description
Request Authentication Setting	[Community](*2) Displays the community name that accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST (*1). [Requests Permitted](*2) Displays the IP address that accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST (*1). [User Name](*3) Displays the user name that accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST. [Authentication] - [Mode] (*3) Displays whether the authentication by the password is enabled. [Authentication] - [Protocol] (*3) When the authentication by the password is enabled, displays the authentication method. [Encryption] - [Mode] (*3) Displays whether the encryption is enabled. [Encryption] - [Protocol] (*3) When the encryption is enabled, displays the encryption method. For the settings, see "3.17.3.3 Adding the Request Permission Setting that Accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST".
System Group Information-Storage System Name	Specifies the name of the storage system. Enter up to 180 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? " < > | & % ^). Do not enter a blank for the first or last character. This is an indispensable input item. If you change this item, the storage system name in the Storage System window of Web Console is also changed.
System Group Information-Contact	Specifies the contact information such as administrator's name and telephone number. Enter up to 180 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? " < > | & % ^). Do not enter a blank for the first or last character. If you change this item, the contact in the Storage System window of Web Console is also changed.
System Group Information-Location	Specifies the installation location of the connected storage system. Enter up to 180 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? " < > | & % ^). Do not enter a blank for the first or last character. If you change this item, the location in the Storage System window of Web Console is also changed.

*1: GETBULK REQUEST is supported only when SNMP version is v2c or v3.
*2: This item is displayed when selecting v1 or v2c for the SNMP version.
*3: This item is displayed when selecting v3 for the SNMP version.

3. Click [Finish].

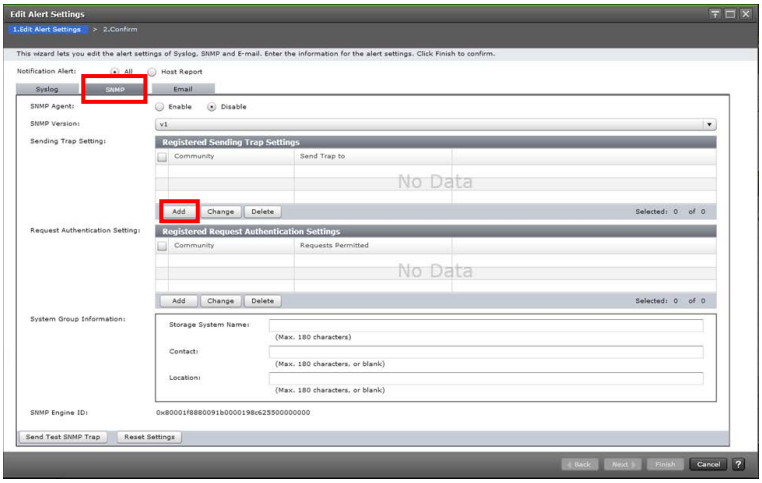
4. In the Edit Alert Settings confirmation window, check the settings and enter the task name in [Task Name].

5. Click [Apply].
   The task is registered. If the [Go to tasks window for status] check box is checked, the Tasks window opens.

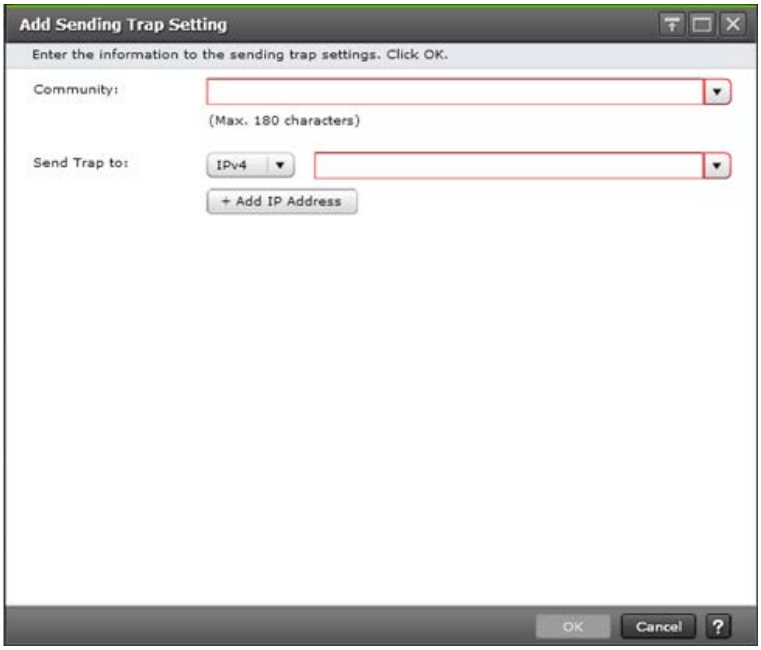
3.17.3.2 Adding SNMP Trap Notification Destinations

The following procedure describes how to add information of SNMP trap notification destinations used for trap transmission.

1. In the Edit Alert Settings window, click [SNMP] tab.Under [Sending Trap Setting], click [Add].

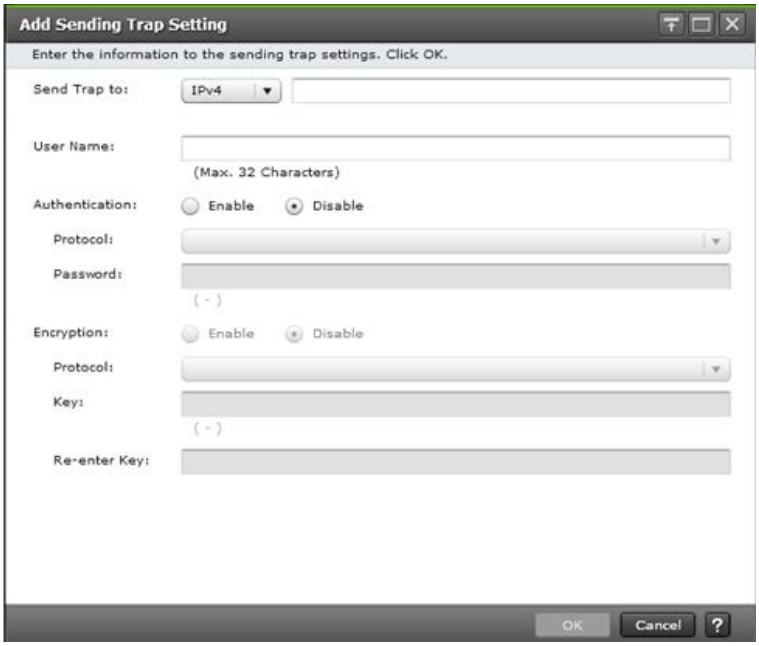


2. The Add Sending Trap Setting window appears.
[When selecting v1 or v2c as the SNMP version]



Item	Description
Community	The community name used for the SNMP trap report is displayed. Enter up to 180 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? " < > | & % ^). Do not enter a blank for the first or last character.
Send Trap to	Newly enter or select the IP address that reports the SNMP trap. • [+ Add IP Address] Add IP addresses. You can add up to 32 IP addresses. • [IPv4]: To set an IPv4 address, select [IPv4] and enter four numbers between 0 and 255. Example: XXX.XXX.XXX.XXX (XXX is a decimal number.) • [IPv6]: To set an IPv6 address, select [IPv6] and enter eight hexadecimal numbers between 0 and FFFF. Zeros can be omitted in an IPv6 address. Example: YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY (YYYY is a hexadecimal number.)

[When selecting v3 as the SNMP version]



Item	Description
Send Trap to	Enter the IP address that reports the SNMP trap. • [IPv4]: To set an IPv4 address, select [IPv4] and enter four numbers between 0 and 255. Example: XXX.XXX.XXX.XXX (XXX is a decimal number.) • [IPv6]: To set an IPv6 address, select [IPv6] and enter eight hexadecimal numbers between 0 and FFFF. Zeros can be omitted in an IPv6 address. Example: YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY (YYYY is a hexadecimal number.)
User Name (*1)	Enter the user name used for the SNMP trap report. Enter up to 32 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? ” < > | & % ^). Do not enter a blank for the first or last character.
Authentication	Select whether to enable or disable the authentication by the password. • [Enabled]: Enable the authentication by the password. • [Disabled]: Disable the authentication by the password.
Authentication - Protocol	When enabling the authentication by the password, select the authentication method (SHA or MD5).
Authentication - Password	When enabling the authentication by the password, enter the password. The password should be between eight and 180 characters. Enter alphanumeric characters except for some symbols (\ , / ; : * ? " < > | & % ^).
Encryption	Select whether to enable or disable the encryption. • [Enabled]: Enable the encryption. • [Disabled]: Disable the encryption.
Encryption - Protocol	When enabling the encryption, select the encryption method (AES or DES).

(To be continued)

(Continued from preceding page)

Item	Description
Encryption - Key	When enabling the encryption, enter the key. The key should be between eight and 180 characters. Enter alphanumeric characters except for some symbols (\ , / ; : * ? " < > | & % ^).
Encryption - Re-enter Key	Re-enter the key entered by [Key].

*1: When using the set user name for [Sending Trap Settings] or [Request Authentication Settings], enter the same details as those set by the user in the following items. If you enter different details, the trap might not be sent correctly.
- Authentication
- Authentication - Protocol
- Authentication - Password
- Encryption
- Encryption - Protocol
- Encryption - Key

3. Click [OK]. The entered information is added to [Sending Trap Settings] in the Edit Alert Settings window.

4. Click [Finish].

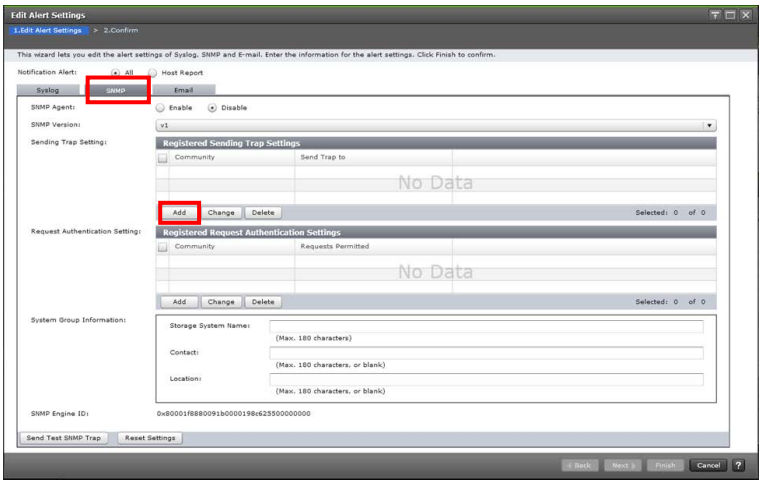
5. In the Edit Alert Settings confirmation window, check the settings and enter the task name in [Task Name].

6. Click [Apply].
The task is registered. If the [Go to tasks window for status] check box is checked, the Tasks window opens.

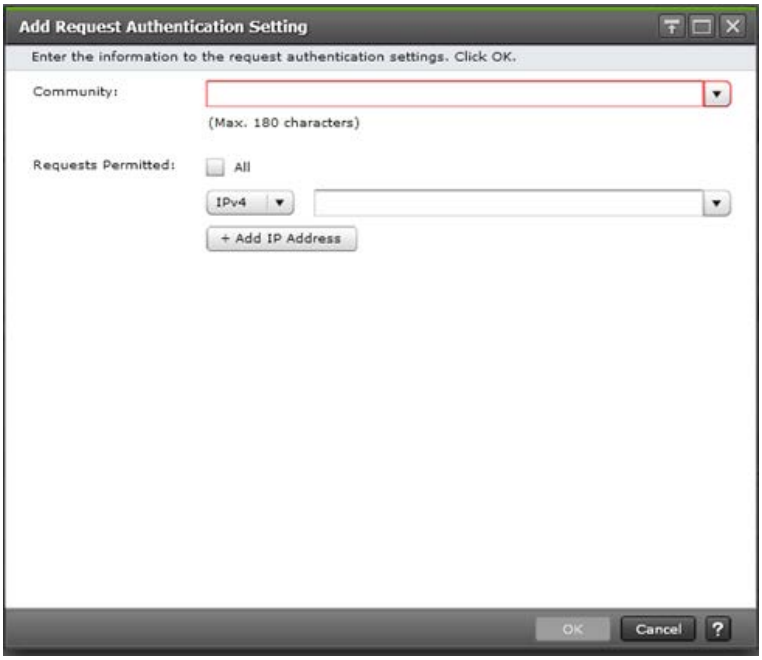
3.17.3.3 Adding the Request Permission Setting that Accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST

The following procedure describes how to add the request permission setting that accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST.

1. In the Edit Alert Settings window, click [SNMP] tab.Under [Request Authentication Setting], click [Add].

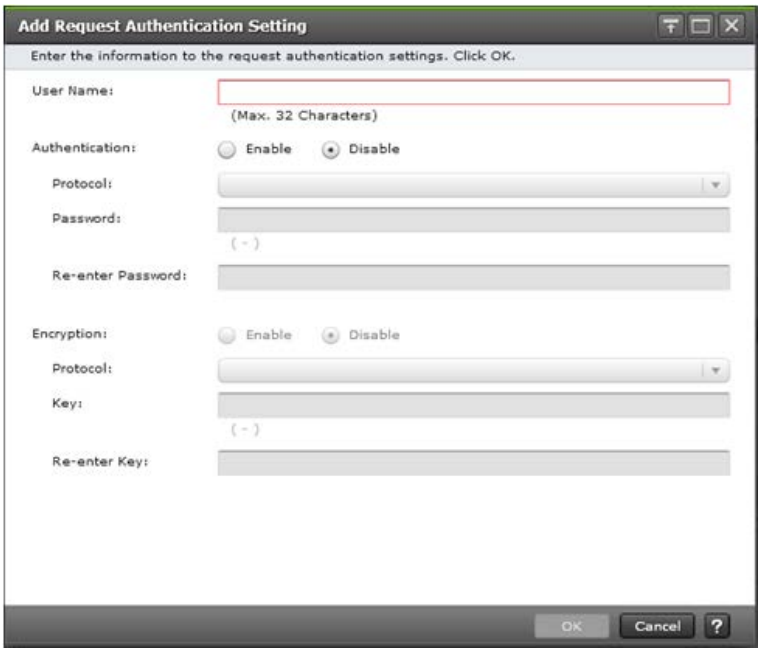


2. The Add Request Authentication Setting window appears.
[When selecting v1 or v2c as the SNMP version]



Item	Description
Community	Newly enter or select the community name that accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST. Enter up to 180 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? " < > | & % ^). Do not enter a blank for the first or last character.
Request Permitted	When accepting GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST of all users, check the checkbox of [All]. When specifying the user who accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST, newly enter or select the IP address.

[When selecting v3 as the SNMP version]



Item	Description
User Name (*1)	Enter the user name who accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST. Enter up to 32 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? ” < > | & % ^). Do not enter a blank for the first or last character.
Authentication	Select whether to enable or disable the authentication by the password. • [Enabled]: Enable the authentication by the password. • [Disabled]: Disable the authentication by the password.
Authentication - Protocol	When enabling the authentication by the password, select the authentication method (SHA or MD5).
Authentication - Password	When enabling the authentication by the password, enter the password. The password should be between eight and 180 characters. Enter alphanumeric characters except for some symbols (\ , / ; : * ? " < > | & % ^).
Authentication - Re-enter Password	Re-enter the password entered in [Password].
Encryption	Select whether to enable or disable the encryption. • [Enabled]: Enable the encryption. • [Disabled]: Disable the encryption.
Encryption - Protocol	When enabling the encryption, select the encryption method (AES or DES).
Encryption - Key	When enabling the encryption, enter the key. The key should be between eight and 180 characters. Enter alphanumeric characters except for some symbols (\ , / ; : * ? " < > | & % ^).
Encryption - Re-enter Key	Re-enter the key entered by [Key].

*1: When using the set user name for [Sending Trap Settings] , enter the same details as those set by the user in the following items. If you enter different details, the trap is not sent correctly.
- Authentication
- Authentication - Protocol
- Authentication - Password
- Encryption
- Encryption - Protocol
- Encryption - Key

3. Click [OK].
   The entered information is added to [Request Authentication Setting] in the Edit Alert Settings window.

4. Click [Finish].

5. In the Edit Alert Settings confirmation window, check the settings and enter the task name in [Task Name].

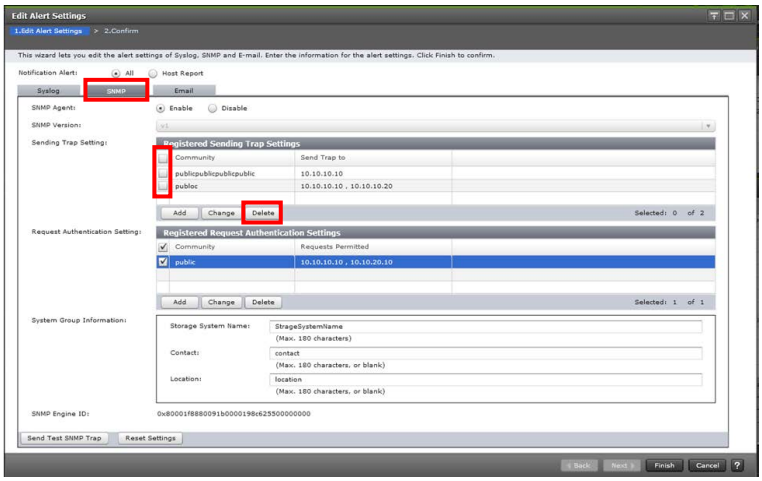
6. Click [Apply].
   The task is registered. If the [Go to tasks window for status] check box is checked, the Tasks window opens.

3.17.3.4 Deleting the SNMP Trap Notification

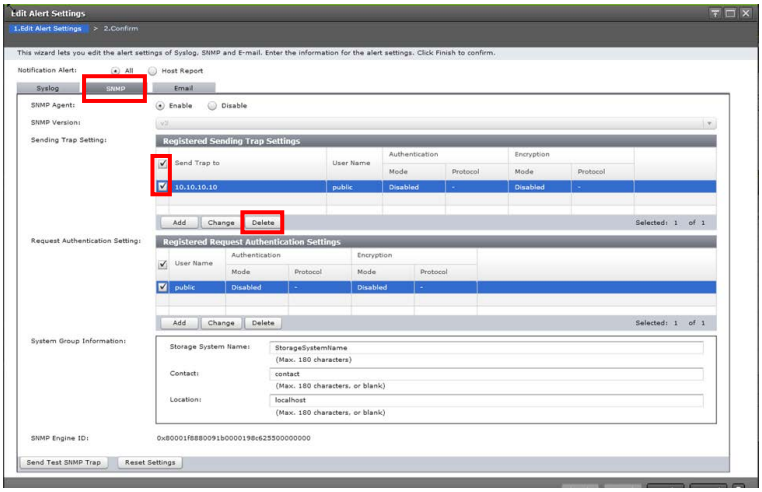
The following procedure describes how to delete an IP address and community of the SNMP trap notification destination used for trap transmission.

1. In the Edit Alert Settings window, Click [SNMP] tab.
   Select one or more community/user names to be deleted in [Sending Trap Setting] and click [Delete].
   The selected community/user names are deleted.

   [When selecting v1 or v2c for the SNMP version]



   [When selecting v3 for the SNMP version]



2. Click [Finish].

3. In the Edit Alert Settings confirmation window, check the settings and enter the task name in [Task Name].

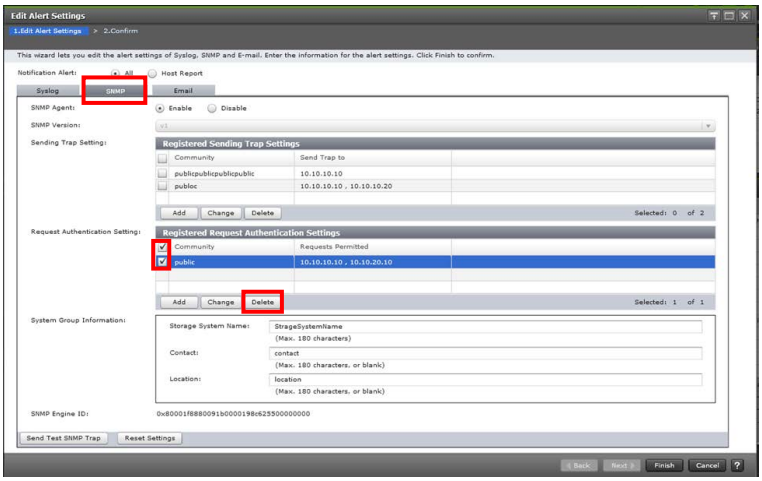
4. Click [Apply].
   The task is registered. If the [Go to tasks window for status] check box is checked, the Tasks window opens.

3.17.3.5 Deleting an IP Address and Community of the SNMP Manager which Accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST

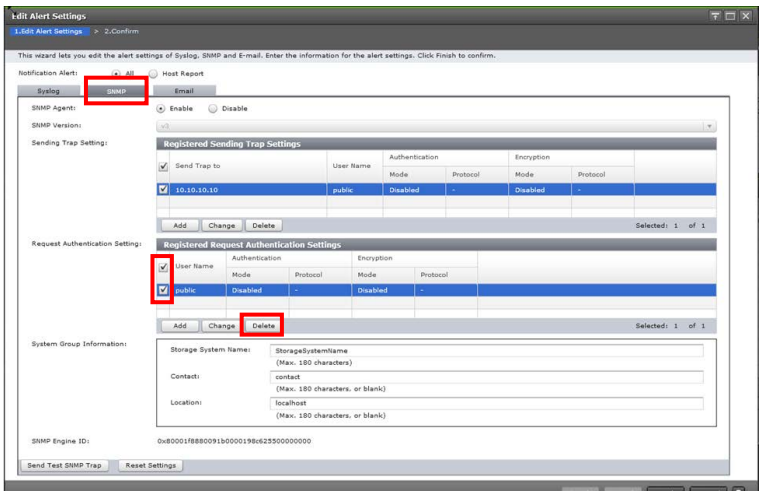
The following procedure describes how to delete an IP address and community of the SNMP manager which accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST is described.

1. In the Edit Alert Settings window, Click [SNMP] tab.
   Select one or more rows to be deleted in [Request Authentication Setting] and click [Delete].
   The selected rows are deleted.

   [When selecting v1 or v2c for the SNMP version]



   [When selecting v3 for the SNMP version]



2. Click [Finish].

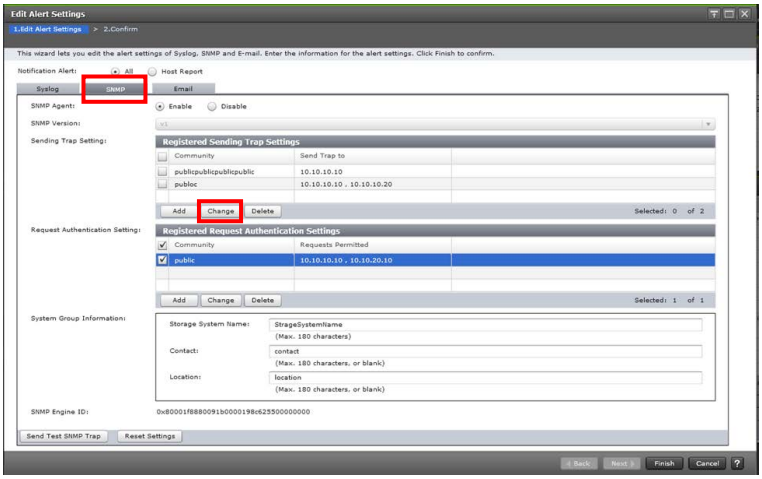
3. In the Edit Alert Settings confirmation window, check the settings and enter the task name in [Task Name].

4. Click [Apply].
   The task is registered. If the [Go to tasks window for status] check box is checked, the Tasks window opens.

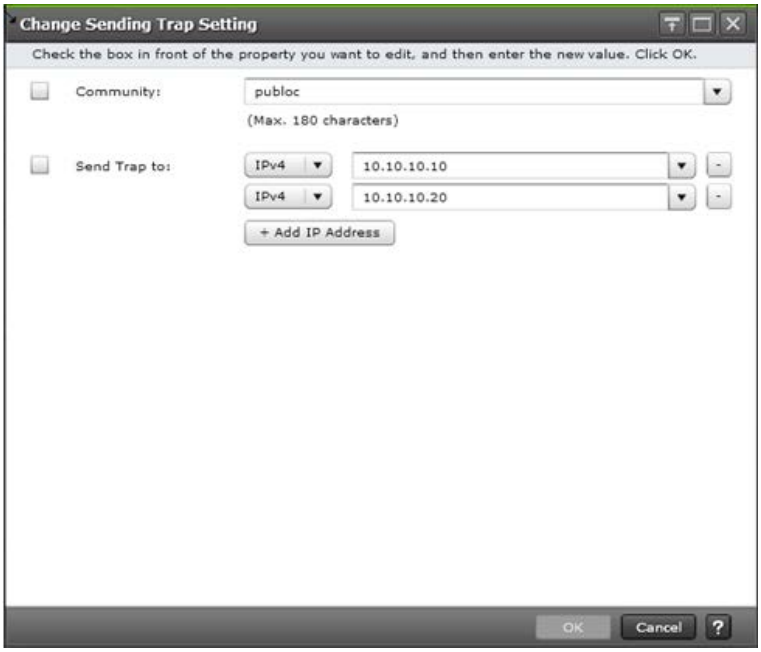
3.17.3.6 Changing the Sending Trap Settings

The following procedure describes how to change the SNMP sending trap settings used for trap transmission.

1. In the Edit Alert Settings window, click [SNMP] tab.
   Select targets to be changed in [Sending Trap Setting] and click [Change].

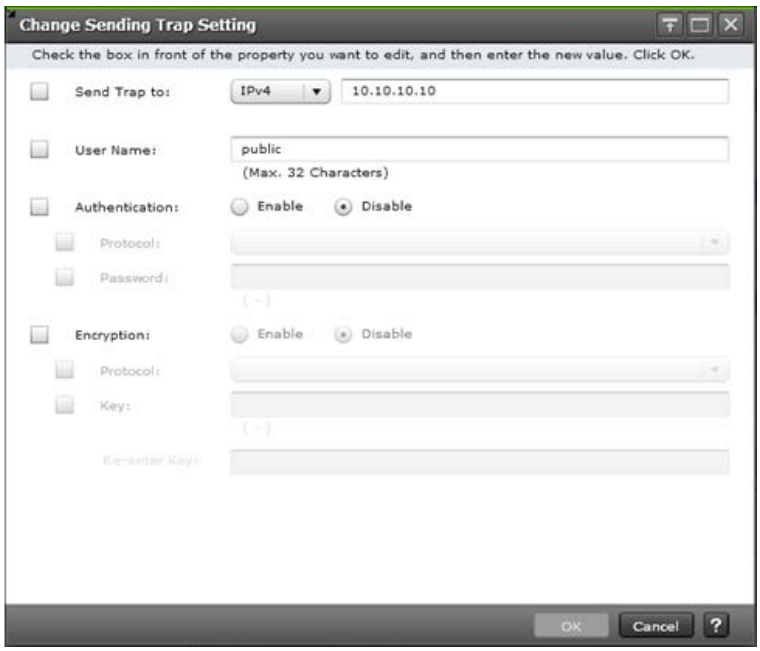


2. The Change Sending Trap Setting window appears.
[When selecting v1 or v2c as the SNMP version]



Item	Description
Community	Enter the community name used for the SNMP trap report. Enter up to 180 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? ” < > | & % ^ ’). Do not enter a blank for the first or last character.
Send Trap to	Newly enter or select the IP address that reports the SNMP trap. • [+ Add IP Address] Add IP addresses. You can add up to 32 IP addresses. • If you uncheck the [New] checkbox, you can select the existing IP address from the pull-down menu. Clicking “-“ on the right of the IP address deletes the IP address.

[When selecting v3 as the SNMP version]



Item	Description
Send Trap to	Enter the IP address that reports the SNMP trap. • [IPv4]: To set an IPv4 address, select [IPv4] and enter four numbers between 0 and 255. Example: XXX.XXX.XXX.XXX (XXX is a decimal number.) • [IPv6]: To set an IPv6 address, select [IPv6] and enter eight hexadecimal numbers between 0 and FFFF. Zeros can be omitted in an IPv6 address. Example: YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY (YYYY is a hexadecimal number.)
User Name (*1)	Enter the user name used for the SNMP trap report. Enter up to 32 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? ” < > | & % ^). Do not enter a blank for the first or last character.
Authentication	Select whether to enable or disable the authentication by the password. • [Enabled]: Enable the authentication by the password. • [Disabled]: Disable the authentication by the password. The columns of [Authentication] and [Encryption] are displayed only when selecting [Enabled].
Authentication - Protocol	When enabling the authentication by the password, select the authentication method (SHA or MD5).
Authentication - Change Password	The column of [Password] is displayed only when checking the checkbox of [Change Password].
Authentication - Password	When enabling the authentication by the password, enter the password. The password should be between eight and 180 characters. Enter alphanumeric characters except for some symbols (\ , / ; : * ? " < > | & % ^).

(To be continued)

(Continued from preceding page)

Item	Description
Encryption	Select whether to enable or disable the encryption. • [Enabled]: Enable the encryption. • [Disabled]: Disable the encryption. The column of [Encryption] is displayed only when selecting [Enabled].
Encryption - Protocol	When enabling the encryption, select the encryption method (AES or DES).
Encryption - change Key	The columns of [Key] and [Re-enter Key] are displayed only when checking the checkbox of [Change Key].
Encryption - Key	When enabling the encryption, enter the key. The key should be between eight and 180 characters. Enter alphanumeric characters except for some symbols (\ , / ; : * ? " < > | & % ^).
Encryption - Re-enter Key	Re-enter the key entered by [Key].

*1: When using the set user name for [Sending Trap Settings] or [Request Authentication Settings], enter the same details as those set by the user in the following items. If you enter different details, the trap might not be sent correctly.
- Authentication
- Authentication - Protocol
- Authentication - Password
- Encryption
- Encryption - Protocol
- Encryption - Key

3. Click [OK].
   The entered information is changed in [Sending Trap Settings] in the Edit Alert Settings window.

4. Click [Finish].

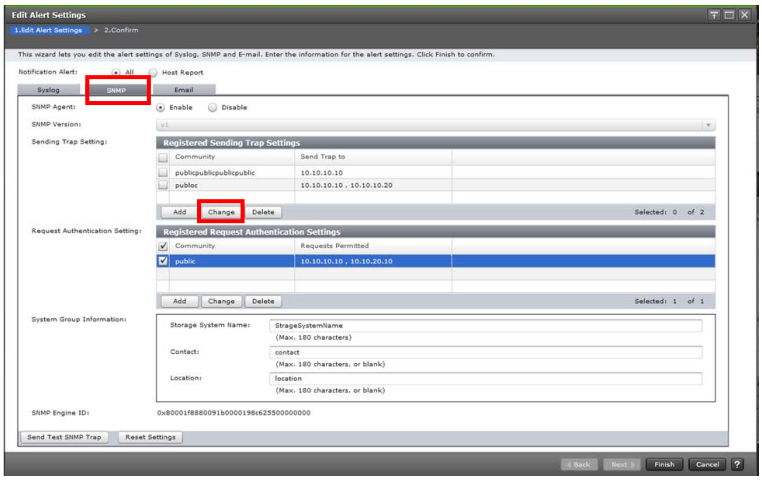
5. In the Edit Alert Settings confirmation window, check the settings and enter the task name in [Task Name].

6. Click [Apply].
   The task is registered. If the [Go to tasks window for status] check box is checked, the Tasks window opens.

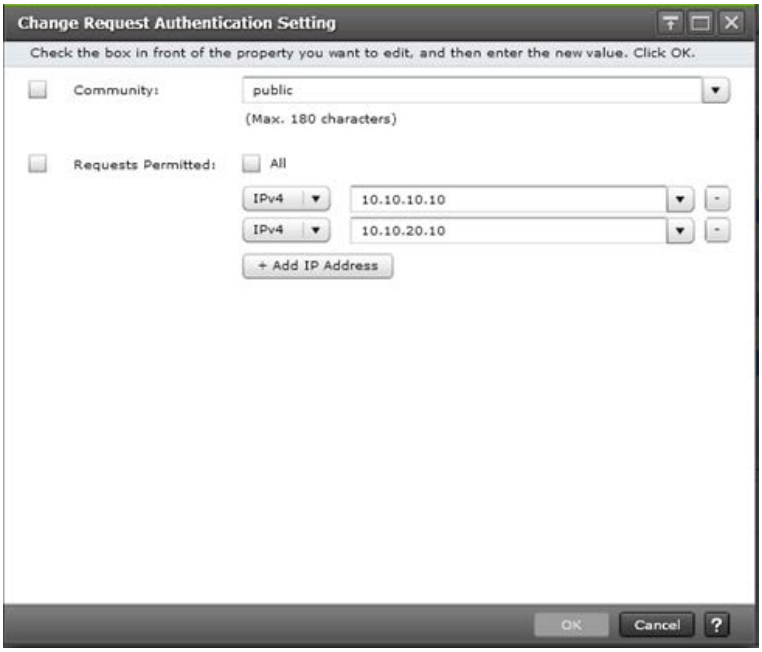
3.17.3.7 Changing the Request Permission Setting

The following describes how to change the request permission setting that accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST.

1. In the Edit Alert Settings window, click [SNMP] tab. Select targets to be changed in [Request Authentication Setting] and click [Change].

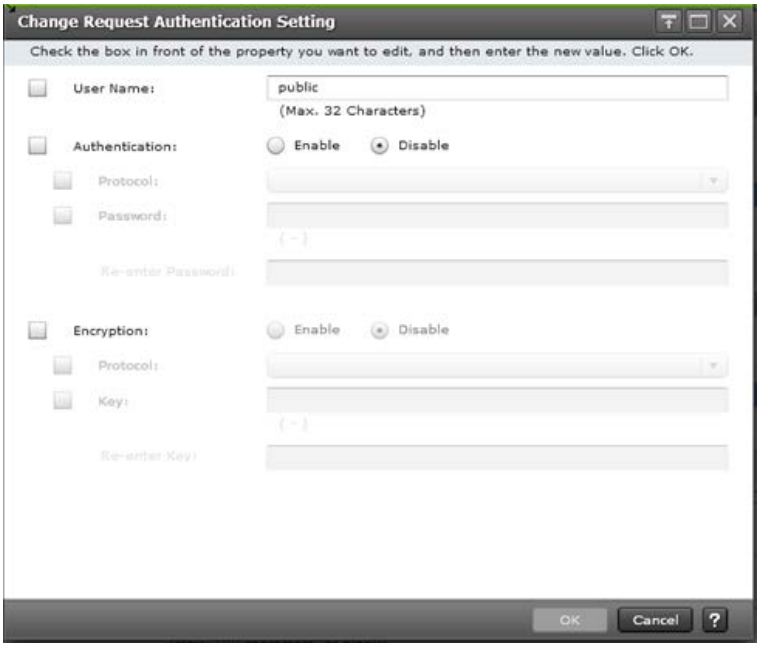


2. The Change Request Authentication Setting window appears.
[When selecting v1 or v2c as the SNMP version]



Item	Description
Community	Newly enter or select the community name that accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST. Enter up to 180 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? ” < > | & % ^ ’). Do not enter a blank for the first or last character.
Request Permitted	When accepting GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST of all users, check the checkbox of [All]. When specifying the user who accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST, newly enter or select the IP address. • [+ Add IP Address] Add IP addresses. You can add up to 32 IP addresses. • If you uncheck the [New] checkbox, you can select the existing IP address from the pull-down menu. Clicking “-“ on the right of the IP address deletes the IP address.

[When selecting v3 as the SNMP version]



Item	Description
User Name (*1)	Enter the user name who accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST. Enter up to 32 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? " < > | & % ^). Do not enter a blank for the first or last character.
Authentication	Select whether to enable or disable the authentication by the password. • [Enabled]: Enable the authentication by the password. • [Disabled]: Disable the authentication by the password. The columns of [Authentication] and [Encryption] are displayed only when selecting [Enabled].
Authentication - Protocol	When enabling the authentication by the password, select the authentication method (SHA or MD5).
Authentication - Change Password	The column of [Password] is displayed only when checking the checkbox of [Change Password].
Authentication - Password	When enabling the authentication by the password, enter the password. The password should be between eight and 180 characters. Enter alphanumeric characters except for some symbols (\ , / ; : * ? " < > | & % ^).
Authentication - Re-enter Password	Re-enter the password entered in [Password].
Encryption	Select whether to enable or disable the encryption. • [Enabled]: Enable the encryption. • [Disabled]: Disable the encryption. The column of [Encryption] is displayed only when selecting [Enabled].
Encryption - Protocol	When enabling the encryption, select the encryption method (AES or DES).

(To be continued)

(Continued from preceding page)

Item	Description
Encryption - change Key	The columns of [Key] and [Re-enter Key] are displayed only when checking the checkbox of [Change Key].
Encryption - Key	When enabling the encryption, enter the key. The key should be between eight and 180 characters. Enter alphanumeric characters except for some symbols (\ , / ; : * ? " < > | & % ^).
Encryption - Re-enter Key	Re-enter the key entered by [Key].

*1: When using the set user name for [Sending Trap Settings] , enter the same details as those set by the user in the following items. If you enter different details, the trap is not sent correctly.
- Authentication
- Authentication - Protocol
- Authentication - Password
- Encryption
- Encryption - Protocol
- Encryption - Key

3. Click [OK].
   The entered information is changed in [Request Authentication Setting] in the Edit Alert Settings window.

4. Click [Finish].

5. In the Edit Alert Settings confirmation window, check the settings and enter the task name in [Task Name].

6. Click [Apply].
   The task is registered. If the [Go to tasks window for status] check box is checked, the Tasks window opens.

3.17.3.8 Performing the Trap Report Test

Performing this operation issues the SNMP trap for test (reference code: 7fffff) to the trap sending destination.

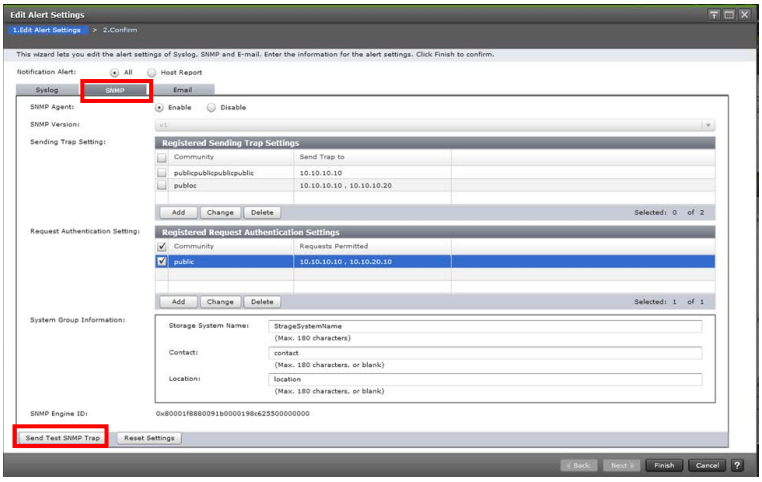
Prerequisites

- The trap sending destination should be set completely in the Edit Alert Settings window.

Procedure

1. Starting Edit Alert Settings window.
   From the [Settings] menu of the Web Console window, select [Environmental Settings]-[Edit Alert Settings].

2. In the Edit Alert Settings window, click [SNMP] tab. Click [Send Test SNMP Trap].



3. Check whether the SNMP trap (reference code: 7fffff) is received in the trap sending destination.

3.18 Setting up License Keys

The license key registration is required for using the program product. This section describes types of license keys and instructions for calculating and registering licensed capacity.

3.18.1 Types of License Keys

Install a dedicated license key for the program product in the GUM from the License window of Maintenance Utility to use the program product.

NOTE: The program product can be used in the Term key license capacity during the Term key valid period by overwriting the Term key to the Permanent key and installing it. If the Term key expires while the system is running, the operation that can be executed is restricted when the capacity required for operating the program product is insufficient.
In this case, the SIM (reference code: 7ff7xx) that informs the Term key expiration is output to the [Alert] tab in the Storage System window.

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

*1: When you log in to Storage Navigator, a warning message is displayed if 45 days or less remain before the expiration.

3.18.1.1 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] is displayed 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, an LDEV was additionally installed, [Grace Period] is displayed in the status field of the License Keys window. You can continue to perform the same operations, but the deficient amount of license must be purchased within 30 days.
- When insufficient licenses are not installed, [Not Enough License] is displayed and the program product is disabled.

3.18.1.2 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.

- [Not Enough License] or [Grace Period] is displayed in the status field of the License Keys window if there is insufficient licensed capacity.
- 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 date of installation.
- 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 at the time of installation and the term key is disabled for 100 days and a total of 250 days have elapsed since the installation, the number of remaining effective days of the term key is 215 days. This is determined by subtracting 150 days from 365 days.
  By disabling the term key on the days when the software application is not used, you can prevent the unnecessary decrease of the period in which the term key can be used.
- If the term key is expired, [Not Installed] is displayed in the status field of the License Keys window, and the software application is disabled.

3.18.1.3 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 key type field, Not Installed is displayed in the status field, and 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.

3.18.1.4 Using the Emergency Key

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

NOTE: If the emergency key is installed in the software application in which the permanent key, or the 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.

3.18.2 Software and Licensed Capacity

The licensed capacity is volume capacity that you are licensed to use with the software application. You need to estimate the amount of capacity which you want to use with the software application before you purchase the permanent key or the term key.
What is based for calculating the licensed capacity differs depending on software products.
(Refer to System Administrator Guide)

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

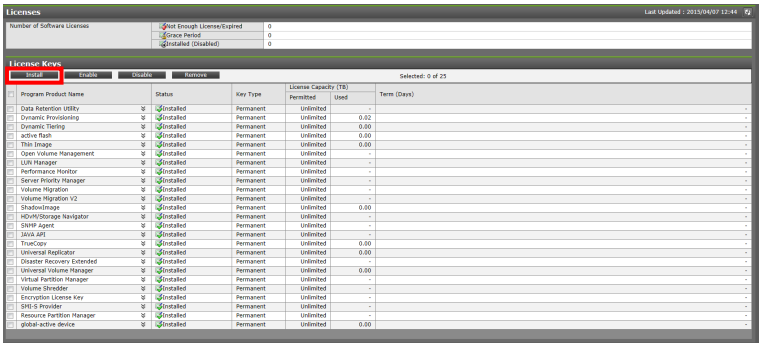
Type	Description
Used capacity	The licensed capacity is estimated by using one of the following capacities, which depends on the software product. • Normal volumes (LDEV) • External volumes mapped to the storage system • Pools When a pool contains the pool volume that belongs to the parity group whose accelerated compression setting is enabled, the license capacity to be purchased becomes the pool usable basic capacity.
Implementation capacity/ usable capacity	The license capacity is estimated using the capacity of all the LDEVs in the storage system. Virtual volumes are not included. When estimating the implementation capacity for the parity group whose accelerated compression setting is enabled, even if the internal volume exceeding the physical capacity is created in the parity group whose accelerated compression setting is enabled, estimate also for the physical capacity. (See “Provisioning Guide for Open Systems” for the accelerated compression setting.)
Unlimited capacity	You can use the software regardless of the volume capacity.

3.18.3 Installing Software Using a License Key Code

You must install a license key for each software application before you use it.

1. Starting Licenses window
   In the Maintenance Utility window, select [Administration] - [Licenses].

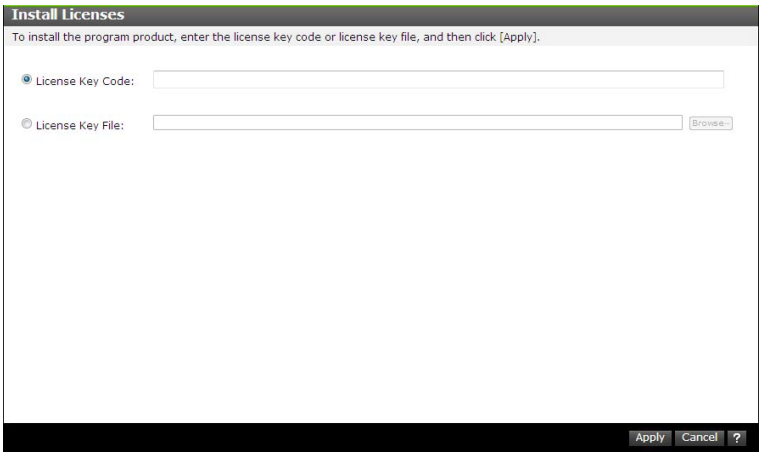
2. The Licenses window is displayed. Click [Install].



Item	Description
Program Product Name	Displays the program product name.
Status	Displays the installation status of a program product : •  [Installed] : The program product is installed. •  [Installed (Disabled)] : Installation is complete, but the license is set to disabled. This status might appear if an error occurs after you install the program product. Resolve the error and enable the license. This status also appears when the license key of this program product is installed but the license key of the prerequisite program product is expired. •  [Not Installed] : The program product is not installed. •  [Not Enough License] : Installation is complete, but the license capacity is insufficient. •  [Grace Period] : The licensed capacity is insufficient because LDEVs are added, pairs have been created pool, or volumes are added. The license expires in 30 days. Please purchase the licenses before the license key expires. •  [Expired] : The term has already expired for the Temporary key. When the status is Expired, you cannot re-install the Temporary key.
Key Type	The license type: • Permanent • Term • Temporary • Emergency • Blank (if no license key is installed)
License Capacity	• [Permitted (TB)] Displays the permitted licence capacity that is installed in an integer. If no upper limit value is set for the capacity, "Unlimited" is displayed. If no license key is installed, Blank is displayed. • [Used (TB)] Displays the volume capacity used by the program product. The capacity is displayed up to two places of decimals. The capacity is rounded up to three decimal places. If the type of licence capacity is the used capacity, a hyphen (-) is displayed. If no license key is installed, Blank is displayed. Licensed capacities are calculated assuming that 1 KB = 1,024 bytes, 1 MB = 1,024 KB, 1 GB = 1,024 MB, and 1 TB = 1,024 GB.
Term (Days)	The number of days remaining before the expiration of a Term key, a Temporary key, or an Emergency key. After the Temporary key has expired, the column shows the number of days that remain before you can reinstall the Temporary key. If the expiration is unlimited, a hyphen (-) is displayed. If no license key is installed, blank is displayed.

3. Insert “License Media” into the DVD drive and specify the license key file.

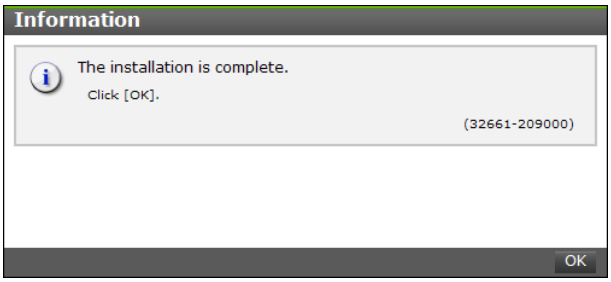
4. Click [Apply].



Item	Description
License Key	[License Key File] Install the program product with specifying the license key file. Click [Browse] to specify the name of the license key file. The file extension is “plk”

NOTICE:
- If installation fails, an error message window appears. Display error details by selecting the program product in the err message window and clicking [Detail].
- You can enter the license key code.

5. A completion message is displayed. Click [OK].



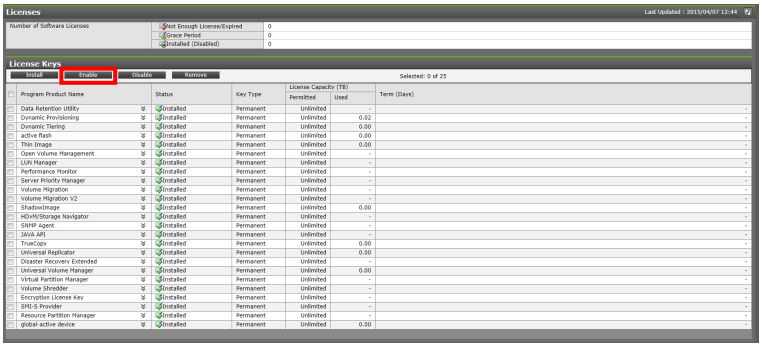
6. Remove the license media.

3.18.4 Enabling a License

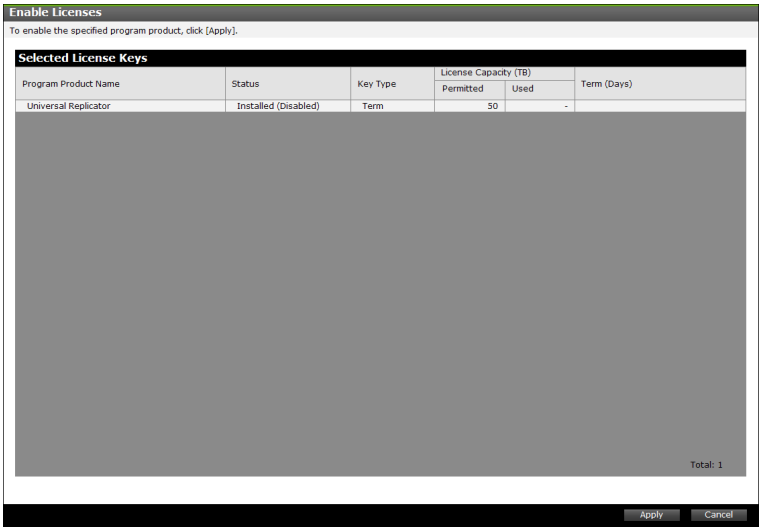
You can enable a license that is in the disabled status.

1. Select the license that you want to disable. You can select multiple licenses.

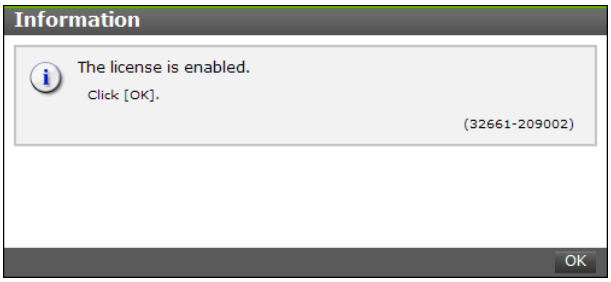
2. Click [Enable] in the License Keys window.



3. Confirm the settings. Click [Apply].



4. A completion message is displayed. Click [OK].

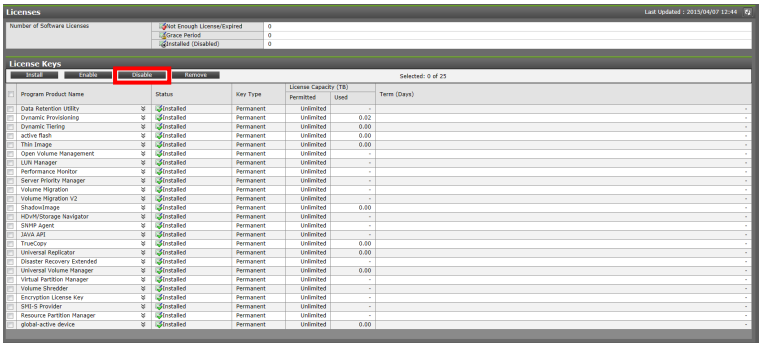


3.18.5 Disabling a License

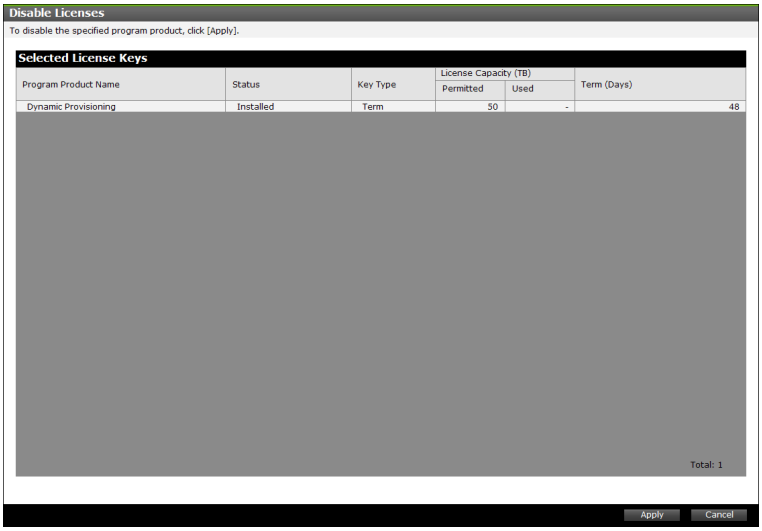
You can disable a license that is in the enabled status.

1. Select the license that you want to disable. You can select multiple licenses.

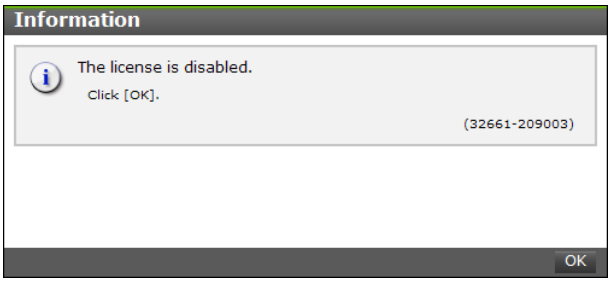
2. Click the [Disable] in the License Keys window.



3. Confirm the settings. Click [Apply].



4. A completion message is displayed. Click [OK].

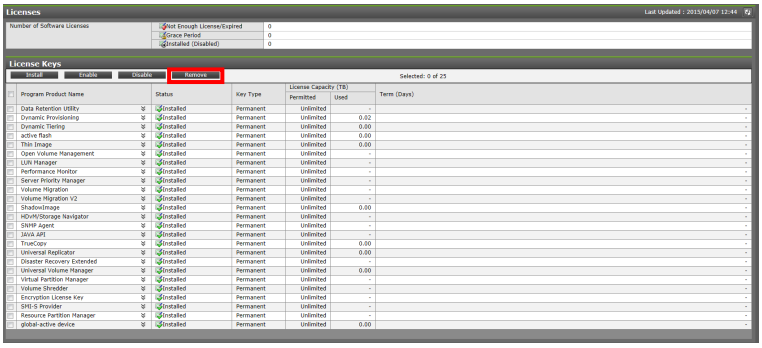


3.18.6 Removing Program Product

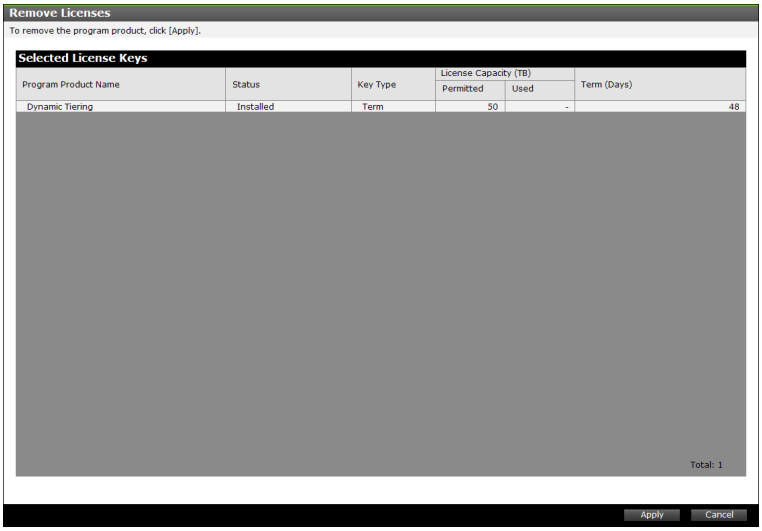
The following procedure describes to remove the program product.

1. Select the license that you want to remove. You can select multiple licenses.

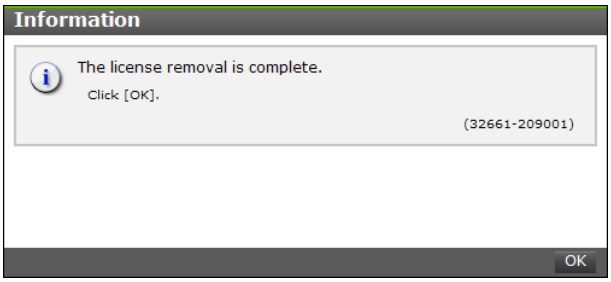
2. Click [Remove] in the License Keys window.



3. Confirm the settings. Click [Apply].

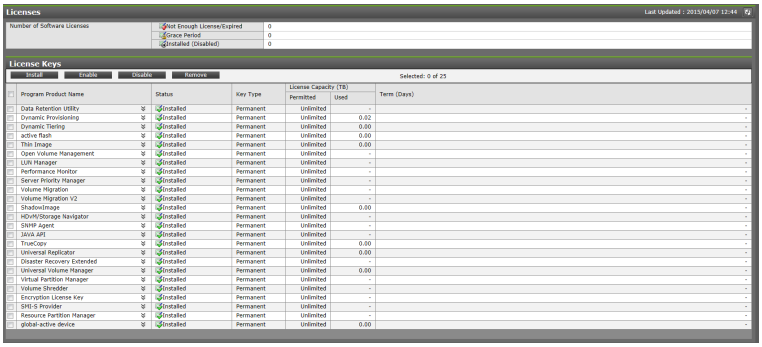


4. A completion message is displayed. Click [OK].



3.18.7 Verifying License

You can verify the license of each program product in the License Keys window.



3.18.7.1 Examples of the displayed window

The following table lists the display examples of the window by the license key status.

License key status (example)	Status	Key type	Licensed capacity	Term (Days)
Not installed.	Not Installed	Blank	Blank	Blank
Newly installed with the Permanent key.	Installed	Permanent	Permitted capacity	-
Newly installed d with the Term key and set to enable.	Installed	Term	Permitted capacity	Remaining days
Newly installed with the Term key and set to disable.	Installed (Disabled)	Term	Permitted capacity	Blank
Newly installed with the Temporary key.	Installed	Temporary	-	Remaining days
Newly installed with the Emergency key.	Installed	Emergency	-	Remaining days
A Temporary key was installed, but has expired.	Expired	Temporary	-	Remaining days
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 keyor Term	Permitted capacity and used capacity	-
Installed with the Permanent key or the Term key and then the capacity insufficiency caused by adding LDEVs.	Grace Period	Permanent keyor Term	Permitted capacity and used capacity	Remaining days
Installed with the Temporary key, and then reinstalled with the Permanent key, but the license capacity was insufficient.	Installed	Temporary	Permitted capacity and used capacity	Remaining days
Installed with the Permanent key, then reinstalled with the Emergency key.	Installed	Emergency	Permitted capacity and used capacity	Remaining days

3.18.8 Cautions on Licensed Capacity in Non-License-Related Windows

Licensed capacity is displayed not only in license-related windows but also in the Pools window and the Replication window of the Storage Navigator.

When you overwrite and install the temporary key or emergency key for an installed software application, the licensed 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 or Replication window.

For example, if you install TrueCopy with a license capacity of 5 TB by the term key and when the term has expired and you use the emergency key, ”5TB” (capacity of the term key) is displayed in [Permitted (TB)] on licenserelated windows, but ”Unlimited” (capacity for the emergency key) is displayed in Licensed Capacity on the Replication window.

3.18.9 Troubleshooting related to licenses

- After entering a license key, the installation status of the license may be [Installed (Disabled)].
  The following shows the cause and actions to be taken.

Cause	Actions to be taken
The program product was installed without installing the necessary program product.	Install the necessary program product.

- When the license key expires and becomes invalid, purchase the necessary license key.
  If a certain program product (A) expires, a program product (B) which needs the expired program product (A) is also disabled. In this case, [Installed (Disabled)] is displayed in [Status] of the program product (B) in the License Keys window.
  After that, if the program product (A) is enabled, the program product (B) is also enabled. When [Installed(Disabled)] is kept displayed in [Status] of the program product (B), enable the license status in the Enable Licenses window.
  If a license key becomes invalid, you cannot perform new setting operations. Furthermore, you cannot use Performance Monitor for monitoring. However, the configuration information set within the expiration date is enabled. Whether you can cancel the configuration information set within the expiration date differs depending on program products.

3.18.10 Precautions related to the pool capacity when using Dynamic Provisioning

Types of errors	Cause and Actions to be taken
The license capacity is insufficient without adding LDEVs.	When using Dynamic Provisioning, the used capacity of the pool may increase depending on the stored capacity of the data in the LDEV without adding LDEVs. Purchase the insufficient licenses within 30 days. For the calculation method of the pool capacity of Dynamic Provisioning, refer to “Provisioning Guide for Open Systems”.

4. IPv6 Setting

You can use Web Console and Storage Navigator (Remote Web Console in case of HPE version) with IPv6.

Internet Protocol Version used for the connection of Storage Navigator switches depending on the network setting of the PC which operates the SVP and Storage Navigator. A list of the setting of the PC which operates the SVP and Storage Navigator and Internet Protocol Version used for the connection is shown below.

Table 4-1 List of Internet Protocol Version used for the Connection

Client \ SVP			Network Setting					
			IPv4	IPv6	IPv4	IPv6	IPv4	IPv6
			Enabled	Enabled	Enabled	Disabled	Disabled	Enabled
Network Setting	IPv4	Enabled	Connected by IPv4		Connected by IPv4		Connected by IPv6	
	IPv6	Enabled						
	IPv4	Enabled	Connected by IPv4		Connected by IPv4		Connection disabled	
	IPv6	Disabled						
	IPv4	Disabled	Connection disabled (*1)		Connection disabled		Connected by IPv6	
	IPv6	Enabled						

IPv4: Internet Protocol Version 4 (TCP/IPv4)

IPv6: Internet Protocol Version 6 (TCP/IPv6)

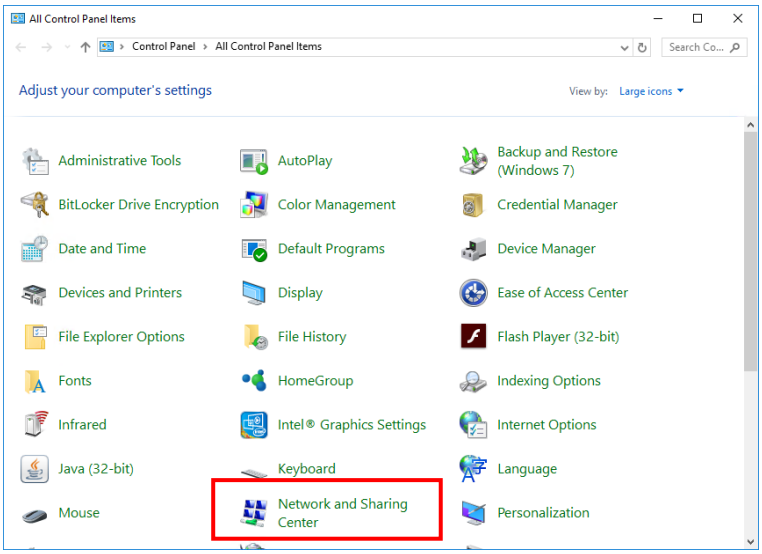
Client: PC which operates Storage Navigator (Remote Web Console in case of HPE version)

*1: If you make only IPv6 enabled for the setting of the PC which operates Storage Navigator while keeping both IPv6 and IPv4 enabled for the setting of the SVP, you cannot use Storage Navigator. When communicating only with IPv6, set both PCs which operate the SVP and Storage Navigator as IPv6.

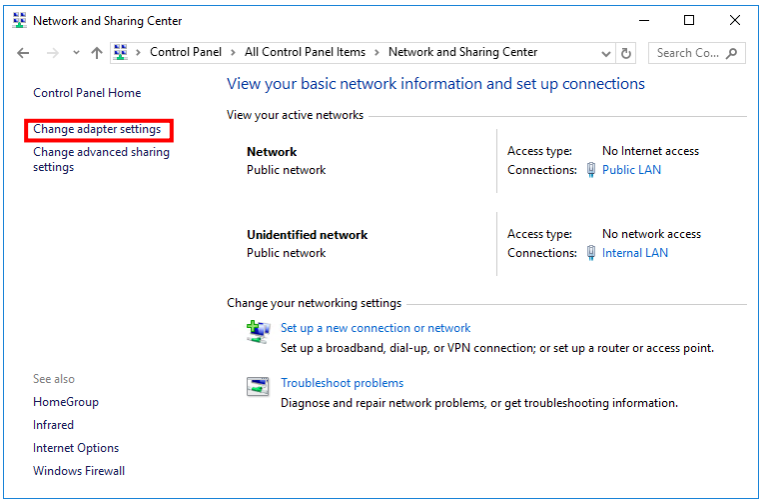
Perform the following when using Web Console only with IPv6.

1. Open the Control Panel window
   Click [Start], and then select [Control Panel] from [Windows System].

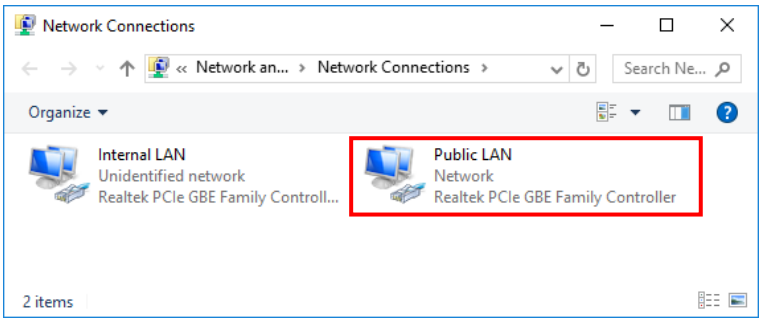
2. Launch the Network and Sharing Center
   Click [Network and Sharing Center] in the All Control Panel Items window.



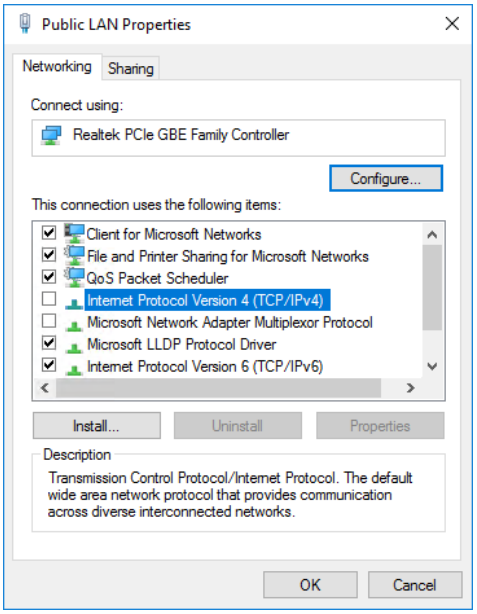
3. Launch the Network Connections
   Select [Change adapter settings] in the left side of Network and Sharing Center window.



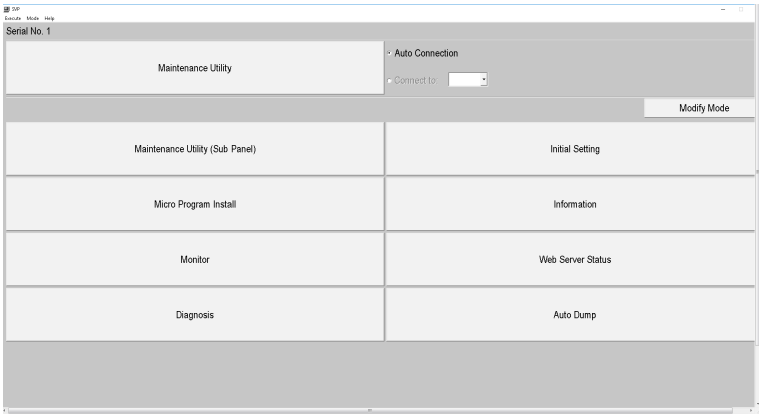
4. Open the Connection Properties window
   Right-click on the icon of [Public LAN] and click [Properties] from the displayed popup menu. Click "Continue" when the confirmation window is displayed.



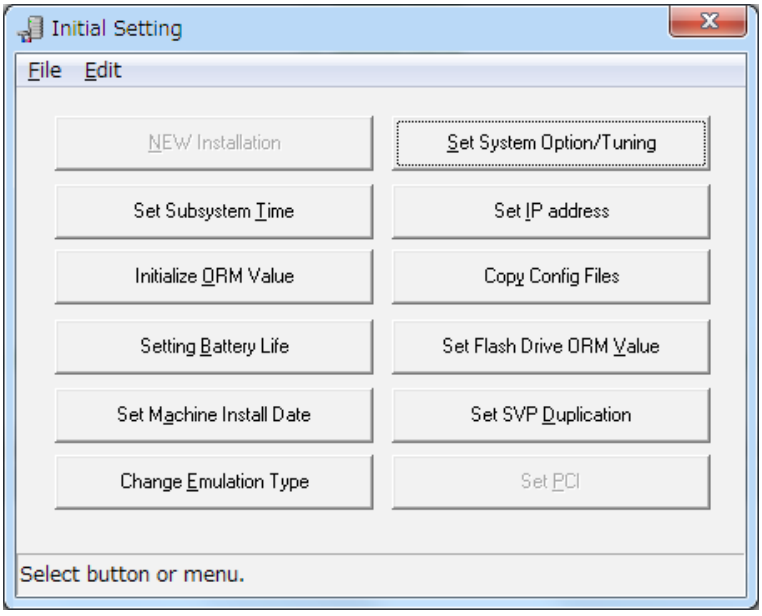
5. Set properties
   When the property is displayed, uncheck the checkbox of "Internet Protocol Version 4 (TCP/IPv4)" in the list. Click [OK] and close the window.



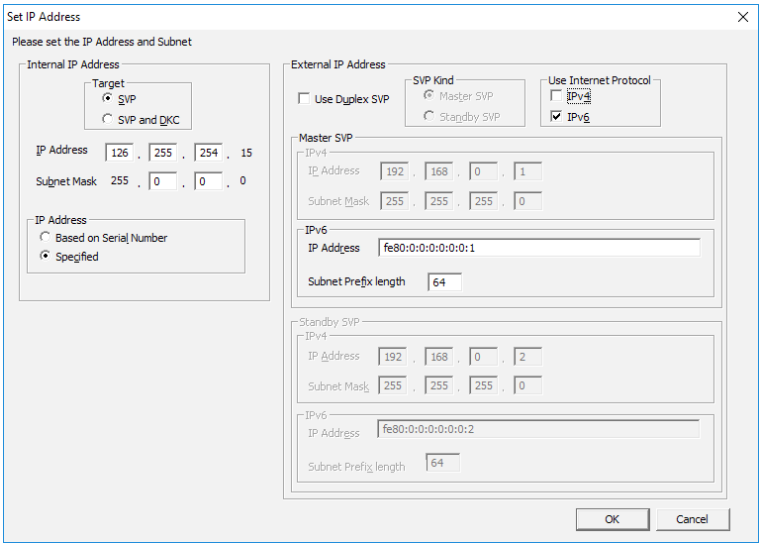
6. Operate SVP window
   Change to [Modify Mode].



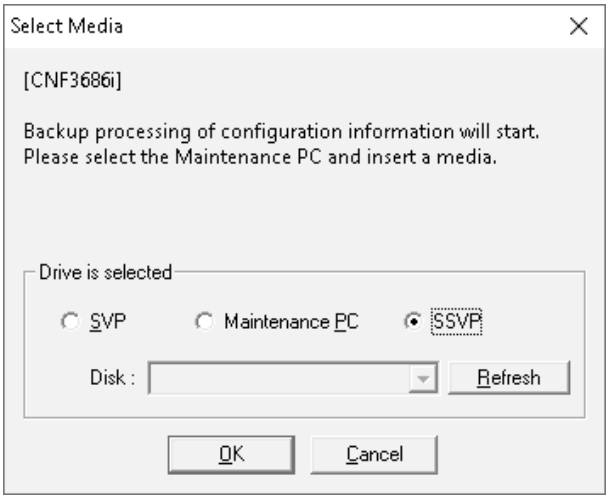
7. Open Initial Setting window
   Click [Initial Setting] from [SVP].



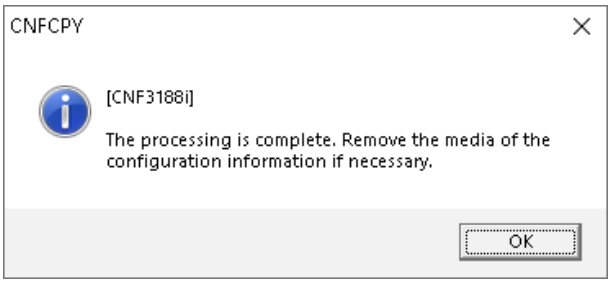
8. Set SVP properties
   Click [Set IP address] from the Initial Setting window.
   Uncheck the checkbox of IPv4 of “Use Internet Protocol” and click [OK].



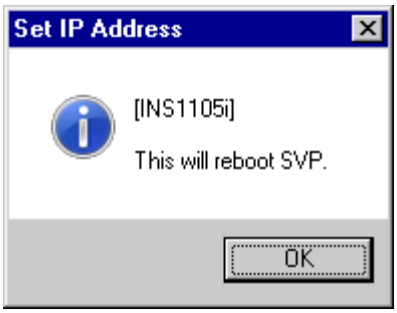
9. Insert the Config media
   Select SSVP as the location to back up the configuration information.
   Then, click [OK].



10. Take out the Config media
    When the configuration information backup is complete, the message “The processing is complete. Remove the media of the configuration information if necessary.” is displayed. Click [OK].



11. Make sure of the restart of the SVP
    Click [OK].
    The SVP is disconnected from the maintenance PC.
    After waiting for about five minutes, reconnect the SVP that has been replaced to the maintenance PC.



5. Before using the Alert setting/FTP transfer function

The setting of the Syslog/FTP server is required to use the Alert setting/FTP transfer function. Ask the customer to set the address of the Syslog/FTP server.
For details, refer to the chapter on the setting of the audit log in “Hitachi Audit Log User Guide”.