

MAINTENANCE PC SECTION

Contents

1. Maintenance PC Setup.....	MPC01-10
1.1 Requirements for the Maintenance PC.....	MPC01-10
1.2 Maintenance PC Setup Workflow	MPC01-30
1.3 Settings other than those of Maintenance PC software.....	MPC01-50
1.3.1 Setting LAN Port Transfer Rate.....	MPC01-50
1.3.2 Checking Overlap of Port Number	MPC01-70
1.3.3 Setting Browser	MPC01-90
1.3.3.1 Setting the Browser Compatibility Display to OFF.....	MPC01-90
1.3.3.2 Setting Cookie and Disabling Pop-up Blocker	MPC01-110
1.3.3.3 Enabling JavaScript.....	MPC01-120
1.3.3.4 Registering the Maintenance PC as a Trusted Site (Windows Server)	MPC01-130
1.3.3.5 Setting Security Level (Windows Server 2012 or later)	MPC01-140
1.3.4 Setting of Antivirus Program.....	MPC01-150
1.3.5 Setting Java Security.....	MPC01-160
1.3.6 Enabling Adobe Flash Player (Windows Server 2012 or later)	MPC01-210
1.3.6.1 Using Flash Player in Windows Server 2012.....	MPC01-210
1.3.6.2 How to use Flash Player that is installed on Windows Server 2016 or later.....	MPC01-220
1.3.7 Settings to Register Specific IP Address in Audit Log	MPC01-230
1.3.8 IIS/FTP Server Setup	MPC01-240
1.3.9 Setting Virtual Memory	MPC01-251
1.4 Maintenance PC Software Initial Installation/Update Installation.....	MPC01-260
1.4.1 Workflow of Installation.....	MPC01-260
1.4.2 OSS That Is to Be Installed	MPC01-270
1.4.3 Installation Procedure.....	MPC01-280
2. Using Maintenance PC at Client's Site	MPC02-10
2.1 Workflow of Settings and Operations of the Maintenance PC at Client's Site	MPC02-10
2.2 Connecting Maintenance PC to Storage System.....	MPC02-30
2.3 Settings Other Than those of Maintenance PC Software at Client's Site	MPC02-60
2.3.1 IP Address Setting of Maintenance PC	MPC02-60
2.3.2 Bridge Setting of LAN Ports	MPC02-90
2.3.3 Proxy Setting of Browser.....	MPC02-100
2.3.4 Preparation for Connecting to another Storage System That Has the Same IP Address via LAN.....	MPC02-120
2.4 Registering Storage Systems to Be Maintained in Storage Device List	MPC02-130
2.5 Starting Web Console	MPC02-190
2.6 Starting the MPC Window.....	MPC02-220
2.6.1 Starting the MPC Window from Web Console.....	MPC02-220
2.6.2 Starting the MPC Window from the MPC Software Window	MPC02-250
2.7 Starting the Maintenance Utility Window	MPC02-260
2.7.1 Starting the Maintenance Utility window from the Web Console window.....	MPC02-270

2.7.2 Starting the Maintenance Utility Window from the MPC Window	MPC02-280
2.7.3 Starting the Maintenance Utility Window by Specifying IP Address of CTL	MPC02-280
2.7.4 Closing the Maintenance Utility Window	MPC02-290
2.8 Maintenance PC Operation after Maintenance Work.....	MPC02-300
2.8.1 Stopping Web Console.....	MPC02-300
2.8.2 Shutting down the Maintenance PC	MPC02-310
2.8.3 Disconnecting the Maintenance PC from the Storage System	MPC02-320
2.9 Troubleshooting of Storage Device List	MPC02-330
2.10 Troubleshooting of Web Console	MPC02-360
2.11 Troubleshooting of Maintenance Utility	MPC02-400
2.12 Troubleshooting during Operation in Connection with External Server	MPC02-450
2.13 Incorrect display errors	MPC02-460
2.14 Operating Storage Systems to Be Maintained by Using Storage Device List.....	MPC02-470
2.14.1 Checking Status of Storage System.....	MPC02-470
2.14.2 Stopping the Service of Storage System.....	MPC02-500
2.14.3 Starting the Service of Storage System	MPC02-510
2.14.4 Changing Storage System Information and Updating Software of Web Console	MPC02-520
2.14.5 Deleting Registered Storage Systems	MPC02-530
3. Storage System Maintenance Function.....	MPC03-10
3.1 Network Setting [Start Separate Action].....	MPC03-10
3.2 Firmware	MPC03-30
3.3 User Administration	MPC03-40
3.3.1 Setting up User Account.....	MPC03-40
3.3.2 Disabling User Accounts	MPC03-70
3.3.3 Changing User Account Authentication	MPC03-90
3.3.4 Removing User Accounts	MPC03-120
3.3.5 User Account Information	MPC03-140
3.3.5.1 Backup User Accounts.....	MPC03-140
3.3.5.2 Restore of User Account Information.....	MPC03-150
3.3.6 Roles to be Required for the Operation Window of Maintenance Utility	MPC03-160
3.4 Alert Notifications	MPC03-170
3.4.1 Setting up Email Notification when Storage System Failures Occur.....	MPC03-180
3.4.1.1 Prerequisites.....	MPC03-180
3.4.1.2 Procedure	MPC03-180
3.4.1.3 Example of Test Mail.....	MPC03-210
3.4.2 Setting up Syslog Notification.....	MPC03-220
3.4.2.1 Prerequisites.....	MPC03-220
3.4.2.2 Procedure	MPC03-220
3.4.3 Setting up SNMP Notification	MPC03-270
3.4.3.1 Procedure	MPC03-270
3.4.3.2 Adding SNMP Trap Notification Destinations.....	MPC03-320
3.4.3.3 Adding the Request Permission Setting that Accepts GET REQUEST and GETNEXT REQUEST	MPC03-350
3.4.3.4 Deleting the SNMP Trap Notification	MPC03-380

3.4.3.5 Deleting an IP Address and Community of the SNMP Manager which Accepts GET REQUEST and GETNEXT REQUEST	MPC03-390
3.4.3.6 Changing the Sending Trap Settings	MPC03-400
3.4.3.7 Changing the Request Permission Setting	MPC03-430
3.4.3.8 Performing the Trap Report Test.....	MPC03-470
3.5 Time Setting	MPC03-480
3.5.1 Setting Synchronization Information.....	MPC03-480
3.6 Network Setting.....	MPC03-510
3.6.1 Network Setting	MPC03-510
3.6.2 Network Permissions.....	MPC03-550
3.7 Setting up License Keys	MPC03-570
3.7.1 Types of License Keys.....	MPC03-570
3.7.1.1 Using the Permanent Key	MPC03-570
3.7.1.2 Using the Term Key	MPC03-580
3.7.1.3 Using the Temporary Key	MPC03-580
3.7.1.4 Using the Emergency Key	MPC03-580
3.7.2 Software and Licensed Capacity	MPC03-590
3.7.3 Installing Software Using a License Key Code.....	MPC03-600
3.7.4 Enabling a License	MPC03-630
3.7.5 Disabling a License	MPC03-640
3.7.6 Removing Program Product.....	MPC03-650
3.7.7 Verifying License	MPC03-660
3.7.7.1 Examples of the displayed window	MPC03-670
3.7.8 Cautions on Licensed Capacity in Non-License-Related Windows.....	MPC03-680
3.7.9 Troubleshooting related to licenses.....	MPC03-690
3.7.10 Precautions related to the pool capacity when using Dynamic Provisioning.....	MPC03-700
3.8 Audit Log Settings	MPC03-710
3.8.1 Verifying the Settings to Transfer the Syslog Server	MPC03-710
3.8.2 Transferring Audit Log to the Syslog Server	MPC03-720
3.8.2.1 Prerequisites.....	MPC03-720
3.8.2.2 Operation Procedure	MPC03-720
3.8.3 Exporting Audit Log	MPC03-760
3.8.3.1 Exporting Audit Log (Maintenance Utility).....	MPC03-760
3.8.3.2 Exporting Audit Log (Web Console).....	MPC03-780
3.8.4 Sending a Test Message to the Syslog Server.....	MPC03-790
3.9 Turn on/off Locate LEDs	MPC03-800
3.9.1 Turn on Locate LED	MPC03-800
3.9.2 Turn off Locate LED.....	MPC03-840
3.10 Power on Storage System	MPC03-860
3.11 Power off Storage System.....	MPC03-880
3.12 Edit UPS Mode	MPC03-960
3.13 Edit Login Message	MPC03-980
3.14 Select Cipher Suite	MPC03-1000
3.15 Update Certificate Files.....	MPC03-1010
3.16 Edit or Confirm System Parameters	MPC03-1030

3.17 Force Release System Lock	MPC03-1050
3.18 Reboot GUM	MPC03-1070
3.19 Change Password	MPC03-1100
3.20 Boot System Safe Mode	MPC03-1120
3.21 Alert Display	MPC03-1130
3.22 Alert Display Related to FRU (Field Replacement Unit)	MPC03-1160
3.23 Management Menu	MPC03-1220
3.24 Power Supply Management	MPC03-1230
3.25 System Management	MPC03-1240
3.26 Resetting GUM	MPC03-1250
3.27 Acquiring Dumps using Maintenance Utility	MPC03-1260
3.28 Obtaining Configuration Information Backup	MPC03-1280
3.28.1 Configuration Information Backup Function	MPC03-1280
3.28.2 Downloading Configuration Information Backup File	MPC03-1290
3.29 Checking Existence of Pinned Track and Blocked LDEV	MPC03-1300
4. Storage System Management Function	MPC04-10
4.1 Connecting to the Host	MPC04-10
4.1.1 Creating Parity Groups	MPC04-10
4.1.2 Checking the Logical Devices	MPC04-110
4.1.3 Allocating the Logical Devices of a Storage System to a Host	MPC04-120
4.1.4 Configuring a Host Group or iSCSI Target	MPC04-170
4.1.4.1 Editing Host Group	MPC04-170
4.1.4.2 Editing iSCSI Target	MPC04-200
4.2 Managing Drives	MPC04-240
4.2.1 Setting Spare Drives	MPC04-240
4.2.1.1 Guidelines When Allocating Spare Drives	MPC04-240
4.2.1.2 Checking Spare Drive	MPC04-240
4.2.1.3 Allocating/Deleting Spare Drives	MPC04-250
4.2.1.4 Assign Spare Drives (Without Safety Checks)	MPC04-261
4.2.2 Managing Parity Group	MPC04-270
4.2.2.1 Creating Parity Group	MPC04-270
4.2.2.2 Checking Parity Group	MPC04-280
4.2.2.3 Deleting Parity Group	MPC04-280
4.2.2.4 Formatting Parity Group	MPC04-300
4.2.2.5 Interrupting Parity Group Format Task	MPC04-320
4.2.2.6 Creating Parity Group (Without Safety Checks)	MPC04-321
4.2.2.7 Deleting Parity Group (Without Safety Checks)	MPC04-324
4.2.2.8 Formatting Parity Group (Without Safety Checks)	MPC04-326
4.2.3 Managing Logical Device	MPC04-330
4.2.3.1 Creating Logical Device	MPC04-330
4.2.3.2 Checking Logical Device	MPC04-330
4.2.3.3 Allocating the Logical Devices of a Storage System to a Host	MPC04-330
4.2.3.4 Formatting LDEVs	MPC04-340
4.2.3.5 Formatting a Specific LDEV	MPC04-370

4.2.3.6 Interrupting Format Task	MPC04-390
4.2.3.7 Deleting Logical Device	MPC04-410
4.2.3.8 Releasing Logical Device Assignments	MPC04-430
4.2.3.9 Formatting a Specific LDEV (Without Safety Checks)	MPC04-441
4.3 Managing Port	MPC04-450
4.3.1 Editing Fibre Channel	MPC04-450
4.3.2 Editing iSCSI	MPC04-470
4.3.3 Deleting Host Group Information	MPC04-500
4.3.4 Deleting iSCSI Target Information	MPC04-520
4.3.5 Using CHAP Authentication with iSCSI Ports	MPC04-540
4.3.5.1 Configuring One-Way CHAP	MPC04-550
4.3.5.2 Changing One-Way CHAP Settings	MPC04-580
4.3.5.3 Deleting a One-Way CHAP User	MPC04-610
4.3.6 Deleting LUN Paths from Ports	MPC04-611
4.4 Logical Device Maintenance	MPC04-620
4.4.1 Blocking LDEVs	MPC04-620
4.4.2 Restoring Blocked LDEVs	MPC04-640
4.4.3 Editing an LDEV Name	MPC04-660
4.4.4 Force Restore LDEVs	MPC04-680
4.4.5 Blocking LDEVs (Without Safety Checks)	MPC04-691
4.4.6 Restoring Blocked LDEVs (Without Safety Checks)	MPC04-693
4.4.7 Force Restore LDEVs (Without Safety Checks)	MPC04-695
4.4.8 Shredding LDEVs (Without Safety Checks)	MPC04-697
4.5 Web Console Operation	MPC04-700
4.5.1 Local Replication	MPC04-710
4.5.1.1 Initializing Local Replica Pairs	MPC04-710
4.5.2 Data Retention Utility	MPC04-720
4.5.3 Universal Volume Manager	MPC04-730
4.5.4 Remote Replication	MPC04-740
4.5.4.1 Remote Replica Function Switch	MPC04-740
4.5.4.2 Assign Remote Command Devices Window	MPC04-770
4.5.5 Dynamic Provisioning/Dynamic Tiering/active flash/Thin Image	MPC04-780
4.6 Copy Back Setting	MPC04-800
4.6.1 Setting the Copy Back	MPC04-800
4.6.2 Changing the Copy Back	MPC04-800
4.7 Verify (Parity Consistency Check)	MPC04-820
4.7.1 Executing Verify (Parity Consistency Check)	MPC04-820
4.7.2 Interrupting Verify	MPC04-850
4.7.3 Checking the Progress	MPC04-860
4.7.3.1 Checking the Progress in the "Parity Group" Window	MPC04-870
4.7.3.2 Checking the Progress in the "LDEV" Window	MPC04-880
4.7.3.3 Checking the Progress in the Task	MPC04-890
4.7.4 Executing Verify (Parity Consistency Check) (Without Safety Checks)	MPC04-901
4.8 Managing Resource Group	MPC04-910
4.8.1 Adding LDEVs to Resource Group	MPC04-910

4.8.2 Removing LDEVs from Resource Group	MPC04-940
4.9 Encryption Keys	MPC04-960
4.9.1 Force Restore Keys from File.....	MPC04-960
4.9.2 Force Restore Keys from Server.....	MPC04-980
5. Maintenance Function of Maintenance PC.....	MPC05-10
5.1 Mode	MPC05-10
5.2 Dump	MPC05-50
5.3 Log	MPC05-250
5.3.1 Log Indication	MPC05-250
5.3.2 Log Delete	MPC05-450
5.4 Online Read Margin (ORM)	MPC05-470
5.5 Management of Drive Threshold Values	MPC05-720
5.6 Setting Machine Install Data	MPC05-810
5.7 System Option	MPC05-830
5.8 Setting System Option Mode	MPC05-880
5.9 System Tuning	MPC05-930
5.10 Config Backup.....	MPC05-990
5.11 Maintenance Screen	MPC05-1000
5.11.1 Start.....	MPC05-1000
5.11.2 Terminate	MPC05-1030
5.11.3 Update	MPC05-1040
5.12 Maintenance Procedure	MPC05-1050
5.12.1 Copy Status View	MPC05-1050
5.12.2 Version of Firmware	MPC05-1060
5.12.2.1 Basic Info	MPC05-1070
5.12.2.2 MP Ver.(Curt./Running).....	MPC05-1080
5.12.2.3 MP Ver.(Curt./FM).....	MPC05-1100
5.12.2.4 CFM/GUM Ver.	MPC05-1120
5.12.2.5 HDD Ver.....	MPC05-1130
5.12.2.6 ENC Ver.	MPC05-1150
5.12.3 Pin Data Indication	MPC05-1170
5.12.4 PCB/SFP Revision Display.....	MPC05-1200
5.12.5 Inter-PCB Logical Path.....	MPC05-1210
5.12.6 Restoring Failed MP	MPC05-1240
5.12.7 Failed CTL Recovery	MPC05-1290
5.12.8 Error or Failure Status Action	MPC05-1350
6. Monitoring.....	MPC06-10
7. Installing the Maintenance PC Tool	MPC07-10
7.1 Use of OnlineDumpTool	MPC07-10
7.1.1 Installation	MPC07-10
7.1.2 Uninstallation.....	MPC07-50
7.1.3 Upload Procedure	MPC07-60

7.1.4 Reference of Uploaded Results	MPC07-130
7.1.5 Message Table	MPC07-140
8. Maintenance PC Uninstallation.....	MPC08-10
8.1 OSS Uninstallation	MPC08-10
8.2 Maintenance PC Software Uninstallation.....	MPC08-20
9. Description of Windows	MPC09-10
9.1 Names of Elements of Windows (Maintenance PC)	MPC09-10
9.2 WARNING LED Status Window	MPC09-20
9.3 Maintenance Window	MPC09-30
9.3.1 Main Window	MPC09-30
9.3.2 Operation Menu	MPC09-40
9.3.3 Dialog Bar	MPC09-50
9.3.4 Information Display View	MPC09-60
9.3.4.1 Storage System Information View	MPC09-70
9.3.4.2 DKC Information View	MPC09-80
9.3.4.3 HDD Information View	MPC09-110
9.3.4.4 Dialog	MPC09-140
10. Changing/Initializing Port Numbers Used by the Maintenance PC	MPC10-10
10.1 Changing Port Numbers Used by the Maintenance PC	MPC10-20
10.2 Initializing Port Numbers Used by the Maintenance PC	MPC10-40
10.3 Reallocating Automatically Allocated Port Numbers	MPC10-50
10.4 Initializing Automatically Allocated Port Numbers	MPC10-60
10.5 Changing Range of Port Numbers to be Allocated Automatically	MPC10-70
10.6 Initializing Range of Port Numbers to be Allocated Automatically	MPC10-80
10.7 See the Port Number to be Used in the Maintenance PC	MPC10-90
10.8 Checking the Application Using the Port Number Used by the Maintenance PC	MPC10-100
11. Appendix	MPC11-10
11.1 IP Addresses of Maintenance Ports and Internal Network	MPC11-10
11.1.1 Maintenance Port Addresses	MPC11-10
11.1.2 Internal Network Addresses	MPC11-20
11.2 Port Number Used by the Maintenance PC	MPC11-30
11.3 Maintenance Utility Window Configuration	MPC11-40
11.3.1 Basic Framework	MPC11-40
11.3.2 Header Area	MPC11-50
11.3.3 Navigation Area	MPC11-60
11.3.4 Application Area	MPC11-80
11.4 Functions List of the Windows Used for Maintenance Work	MPC11-90
11.5 Stopping/Starting the Storage Navigator Services	MPC11-140
11.5.1 Stopping the Storage Navigator Services	MPC11-140
11.5.2 Starting the Storage Navigator Services	MPC11-160
11.6 Specifications of Web Server Status List	MPC11-180

11.7 Check the Version of Third Party Software MPC11-220

11.8 Restrictions on Operations of Maintenance Utility Started by Specifying IP
 Address of CTL..... MPC11-230

11.9 Setting GUM System Options MPC11-240

NOTICE: Unless otherwise stated, “firmware version” in this section indicates DKCMAIN firmware.

1. Maintenance PC Setup

The following is the general workflow from the preparation and set up of the Maintenance PC to the connection of it to the storage system.

1. Preparing Maintenance PC hardware
Check the requirements for the Maintenance PC. (See [“1.1 Requirements for the Maintenance PC”](#).)
2. Setting up the Maintenance PC
Set up the Maintenance PC before going to a client’s site. (See [“1.2 Maintenance PC Setup Workflow”](#).)
3. Using the Maintenance PC at a client’s site
Connect the Maintenance PC to the storage system and start the maintenance work. (See [“2.1 Workflow of Settings and Operations of the Maintenance PC at Client’s Site”](#).)

1.1 Requirements for the Maintenance PC

A laptop PC that can be used as the Maintenance PC must meet specifications shown in [Table 1-1](#).

Table 1-1 Maintenance PC Specifications

	Specification	
	Necessary Specification	Recommended Specification
OS	Windows 7 Professional (32bit) Windows 8.1 Professional (64bit) Windows 10 Professional/Enterprise (64bit)	
CPU	Equivalent to or more than Celeron P4505 1.87GHz (2 Core)	Equivalent to or more than Celeron G1820 2.7GHz (2 Core)
RAM	3.0 GB or more	
HDD	50 GB (*1)	
Display	1024 × 768 (XGA) or higher-resolution	1280 × 1024 (SXGA)
DVD Drive	Need	
LAN	Ethernet 10Base-T / 100Base-TX / 1000Base-T	
Necessary Program	Adobe Reader	
Web Browser	Internet Explorer 11.0 (*2)	
Locale	English (United States), Japanese (Japan)	

- *1: This is for one Storage System to be registered.

The 50 GB in the table consists of 20 GB (fixed capacity for one Storage System) and 30 GB (minimum buffer capacity).

When registering eight Storage Systems to be used, a minimum of 190 GB is required.

The 190 GB consists of 160 GB (fixed capacity for eight Storage Systems) and 30 GB (minimum buffer capacity) is required.

NOTE: The required buffer capacity varies depending on the Storage System configuration (a maximum of 100 GB).

- *2: Perform the following Internet Explorer settings.

1. Open the Internet Explorer, and then open the [Internet Options].

2. Click the [Advanced] tab.

3. When the browser is closed, if the check box for [Empty Temporary Internet Files folder when browser is closed] is selected, clear the check mark, and then click the [OK] button.

NOTE: If the Maintenance PC is used for the maintenance work on AMS2000/HUS100 disk array system, the check box might be selected as mentioned above.

To perform the maintenance work on AMS2000/HUS100 disk array system after changing the check box setting, restore the setting.

1.2 Maintenance PC Setup Workflow

The Maintenance PC setup is required for performing maintenance work. Set up the Maintenance PC before starting maintenance work at a client's site. You can perform the setup without connecting the Maintenance PC to the storage system (before going to a client's site).

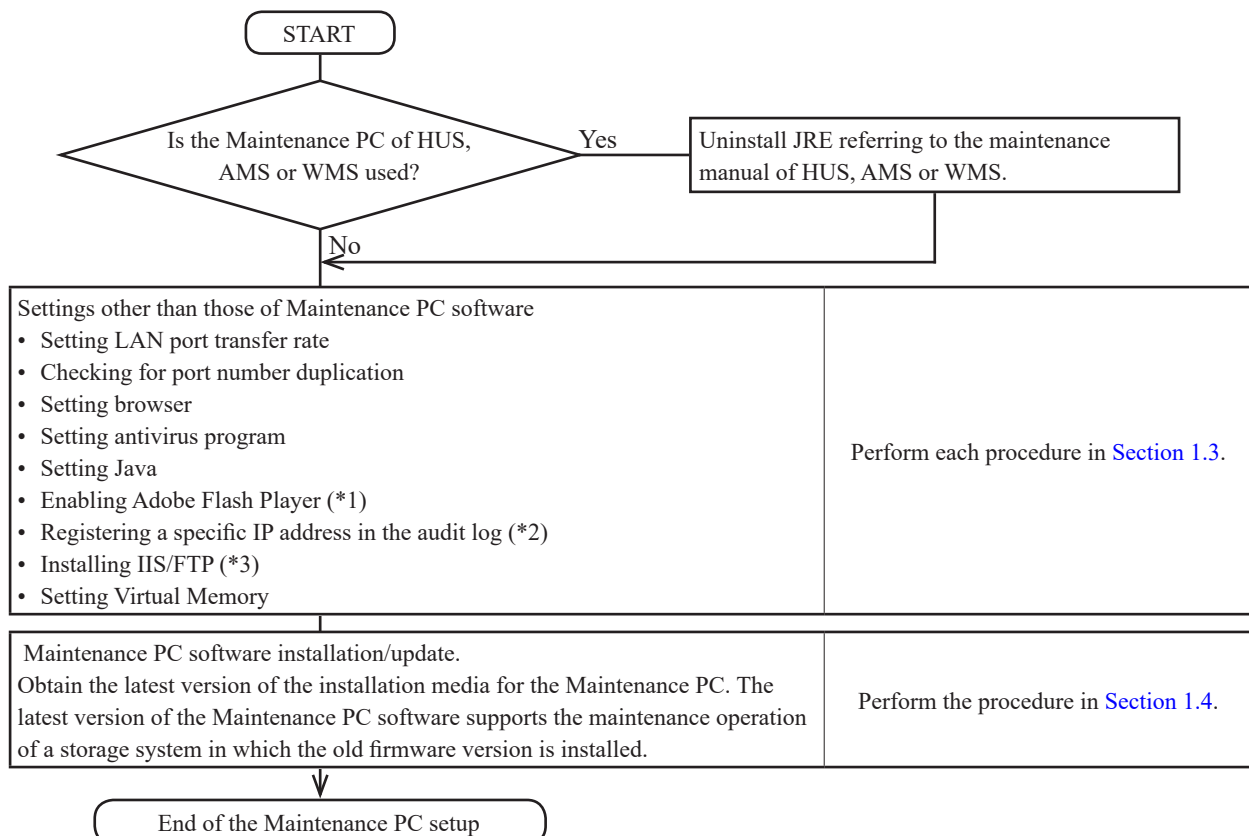
If you use the Storage Device List that is installed from the installation media of DW850 for the Maintenance PC, you can perform the maintenance work for both types of the storage systems shown below with one Maintenance PC.

Storage system type	Description
DW800 (VSP G200, G/F400, G/F600, and G/F800)	The Web Console software version 83-03-21-x0/xx or later is required. When only the DW800 storage systems are registered on Storage Device List, there are no restrictions on versions of the Web Console software.
DW850 (VSP G130, G/F350, G/F370, G/F700, and G/F900)	The Web Console software version 88-02-01-x0/xx or later is required for VSP G130. For other models, there are no restrictions on versions of the Web Console software.

Set up the Maintenance PC by following the workflow shown below. Then, register both storage system types to be maintained on Storage Device List at a client's site.

After the storage system registration is complete, perform the maintenance work as instructed in the Maintenance Manual of each storage system type.

After obtaining the new version of the Maintenance PC software from the factory, update the current Maintenance PC software according to ["1.4 Maintenance PC Software Initial Installation/Update Installation"](#).



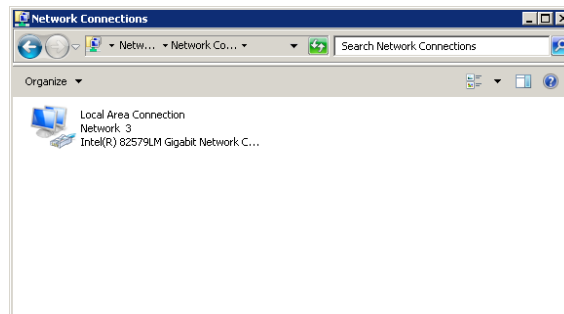
- *1: Perform this only when OS of the Maintenance PC is Windows Server 2012 or later.
- *2: An IP address of the command transmission source that is registered in the audit log might be "LOCALHOST" when maintenance work is performed on the Maintenance PC. For details, see ["1.3.7 Settings to Register Specific IP Address in Audit Log"](#).
- *3: Perform only when doing the following maintenance work.
 - INSTALLATION SECTION ["5. New Installation \(Auto Define Configuration, All Firmwares\)"](#)
 - FIRMWARE SECTION ["5.1 Procedure of New Installation \(Restore Configuration\)"](#)

1.3 Settings other than those of Maintenance PC software

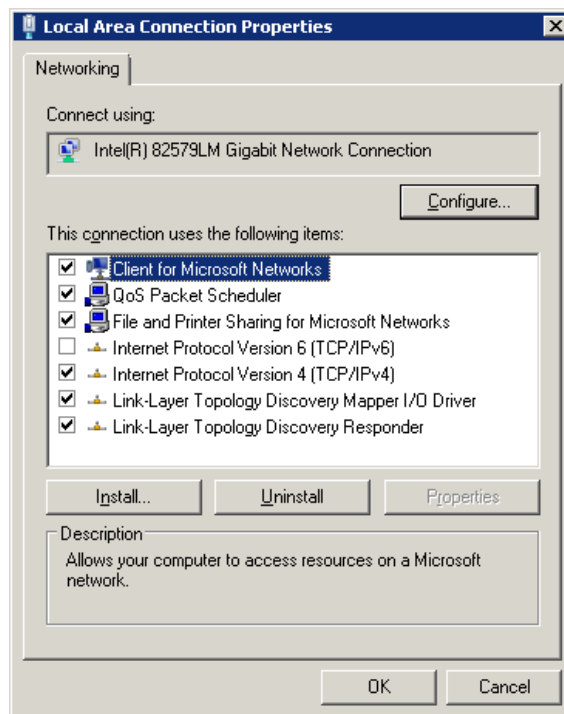
1.3.1 Setting LAN Port Transfer Rate

The procedure for setting the transfer rate of LAN ports varies depending on the OS on the Maintenance PC. The following is the procedure for Windows 7.

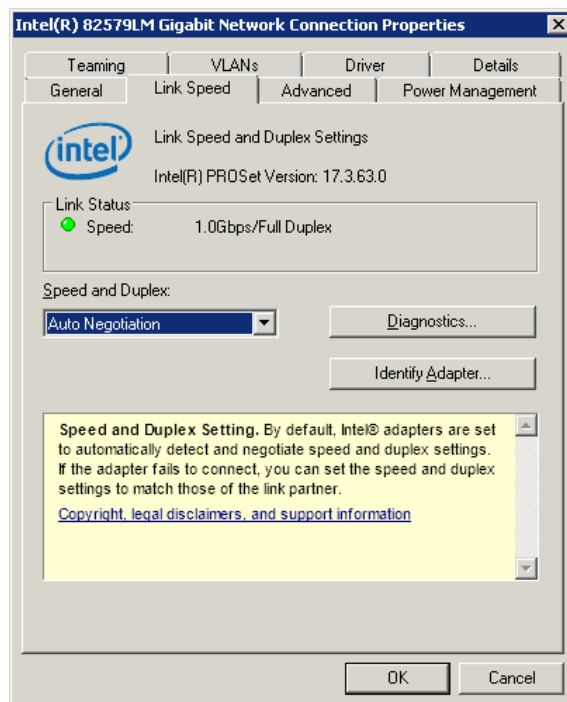
1. Open [Network and Shared Center] from [Control Panel].
2. Click [Change Adapter Settings] from the menu in the left side of the window.
3. Right-click [Local Area Connection]–[Properties].



4. The “Local Area Connection Properties” window is displayed. Click the [Configure] button.



5. Display the [Detail Settings] tab in the displayed window.
Set a property for [Link Speed and Duplex Settings] and a value for [Auto Negotiation].



6. Click the [OK] button to close the window.

1.3.2 Checking Overlap of Port Number

1. Checking overlap of port number

If the port number to be used for the Maintenance PC software is used by a different application on the Maintenance PC, the Maintenance PC software does not work correctly. If the port number is used by a different application, change the port number of the different application.

The port numbers to be used for the Maintenance PC are shown below.

Protocol	TCP/UDP	Port Number
FTP	TCP	20, 21 (*1)
HTTP	TCP	80
HTTPS	TCP	443
RMI	TCP	1099
RMI (SSL)	TCP	5443
HTTP	TCP	8080
HTTP	TCP	8210
HTTP	TCP	9080
HTTP	TCP	9210
RMI	TCP	11099
Command Control Interface (CCI)	UDP	36000-37000 (*2)
RMI	TCP	51099
HTTP	TCP	48081-48336 (*2)
HTTP	TCP	48411-48666 (*2)
RMI	TCP	51100-51355 (*2)

*1: This port number is used only when the following maintenance work is performed.

- INSTALLATION SECTION [“5. New Installation \(Auto Define Configuration, All Firmwares\)”](#)
- FIRMWARE SECTION [“5.1 Procedure of New Installation \(Restore Configuration\)”](#)

*2: An unused port number within the specified range is automatically selected. Therefore, you do not need to check the overlap of the port number.

To check a port number used by a different application, refer to the manual of the application. For the port numbers used by Hitachi Command Suite, see [“11.2 Port Number Used by the Maintenance PC”](#).

NOTE: If the Maintenance PC software is run when the port number is used by a different application, a troubleshooting code shown in [“10.8 Checking the Application Using the Port Number Used by the Maintenance PC”](#) is output in a background service log.

2. When you cannot change a port number used by a different application

Change a port number used by the Maintenance PC software. (However, port numbers 20 and 21 (FTP) cannot be changed.)

To change a port number used by the Maintenance PC software, the Maintenance PC software needs to be installed. After installing the Maintenance PC software, change a port number by referring to [“10.1 Changing Port Numbers Used by the Maintenance PC”](#).

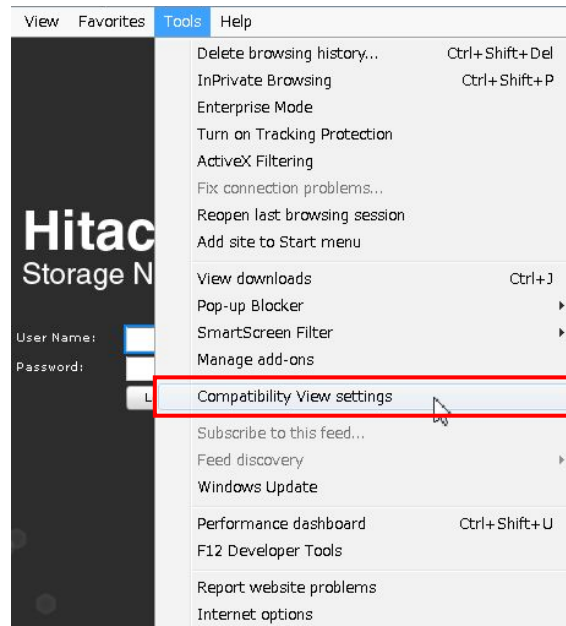
If you change the port number after installing the Maintenance PC software, you need to select an option other than that for ordinary initial installation in the window to select ending/continuing the installation. For details, see [“1.4.3 Installation Procedure”](#).

1.3.3 Setting Browser

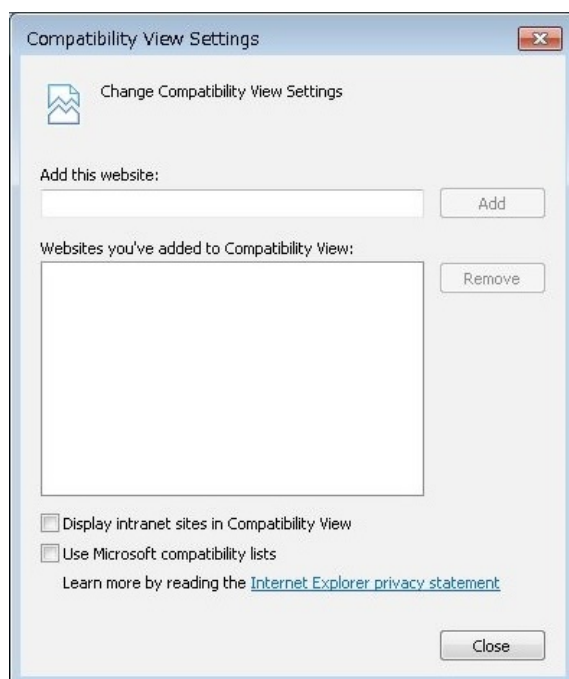
1.3.3.1 Setting the Browser Compatibility Display to OFF

1. Change the compatibility view settings.

Click [Tools] – [Compatibility View settings].



2. Uncheck [Display intranet sites in Compatibility View].



1.3.3.2 Setting Cookie and Disabling Pop-up Blocker

On the Web browser, set the cookie and disable the pop-up blocker.

For the detailed procedure of the Web browser, refer to the Help of your Web browser.

1. Settings to enable the cookie of the Web browser

From the menu bar, select [Tools]-[Internet Options] and click [Privacy]. Then, click [Advanced] and set as follows in the “Advanced Privacy Settings” window.

- Check the checkbox of [Override automatic cookie handling].
- For [First-party Cookies], select [Accept].
- For [Third-party Cookies], select [Accept].
- Check the checkbox of [Always allow session cookies].

2. Settings to allow pop-ups to open

From the Windows [Start] menu, click [Control Panel]-[Internet Options] and display the “Internet Options” window. In the “Internet Options” window, click the [Privacy] tab, uncheck the checkbox of [Turn on Pop-up Blocker], and click the [OK] button.

NOTE: When an add-on with the pop-up blocker of the third vendor is installed in the Web browser (for example, Google Toolbar), set the add-on to allow pop-ups to open, too. For the setting procedure, refer to the documentation of the add-on.

1.3.3.3 Enabling JavaScript

When using Windows 8.1 or Windows Server 2016, enable JavaScript by following the steps below.

1. On the menu bar of Internet Explorer, click [Tools]-[Internet Options]. The “Internet Options” window is displayed.

2. Click the [Security] tab. The “Security” window is displayed.

3. Click [Custom Level]. The “Security Settings” window is displayed.

4. Set [Active scripting] to [Enable].

5. Click the [OK] button.

6. If the “Warning” window is displayed, click the [YES] button.

7. Click the [OK] button to close the “Internet Options” window.

8. Restart the Web browser.

1.3.3.4 Registering the Maintenance PC as a Trusted Site (Windows Server)

When using Windows Server, the “Web Console” window might not be displayed.
Add the Maintenance PC to the [Trusted Sites] list by following the steps below.

1. On the menu bar of Internet Explorer, click [Tools]-[Internet Options]. The “Internet Options” window is displayed.

2. Click the [Security] tab. The “Security” window is displayed.

3. Select [Trusted sites].

4. Click [Sites]. The “Trusted sites” window is displayed.

5. Under [Add this website to the zone:], enter the following URL:
 - http://(IP address of Maintenance PC)
 - https://(IP address of Maintenance PC)
 - http://127.0.0.1
 - https://127.0.0.1
 - http://localhost
 - https://localhost

6. Click the [Add] button.

7. Click the [Close] button to close the “Trusted sites” window.

8. Click the [OK] button to close the “Security” window.

1.3.3.5 Setting Security Level (Windows Server 2012 or later)

Pages might not be displayed correctly depending on the security level settings of Internet Explorer.
Lower the security level of the trusted sites of Internet Explorer by following the steps below.

Prerequisites

- The URL of the Maintenance PC is registered as a trusted site according to the procedure described in [“1.3.3.4 Registering the Maintenance PC as a Trusted Site \(Windows Server\)”](#).

1. On the menu bar of Internet Explorer, click [Tools]-[Internet Options]. The “Internet Options” window is displayed.
2. Click the [Security] tab. The “Security” window is displayed.
3. Select [Trusted sites].
4. Click [Sites]. The “Trusted sites” window is displayed.
5. Set [Security level for this zone] to Medium-high.
6. Click the [OK] button to close the “Security” window.

1.3.4 Setting of Antivirus Program

1. Scan target setting

When using Web Console on the Maintenance PC in which an antivirus program is installed, the operation of Web Console might be affected.

To prevent this from happening, exclude the following directory from the real time virus scan targets of an antivirus program.

C:\Mapp\wk

“C:\Mapp” indicates a Web Console installation directory.

When other than “C:\Mapp” is specified for an installation directory, replace it with the specified installation directory.

For the excluded directories, run the virus scan periodically while Web Console is not used or services are stopped.

2. Firewall pass-through setting

When an antivirus program that supports the Firewall function is used, the Firewall pass-through setting is required. For the port numbers for which the setting is performed, see [“2.2 Connecting Maintenance PC to Storage System”](#).

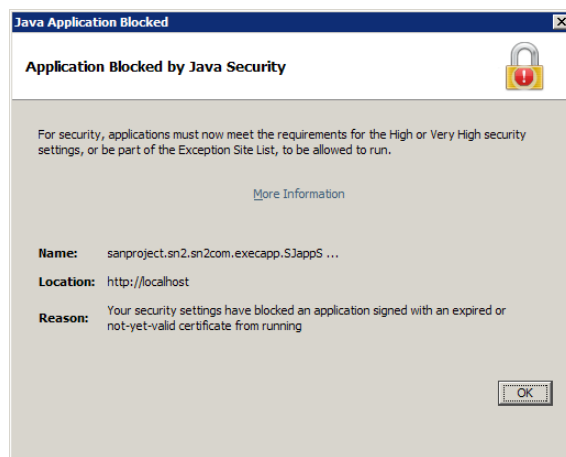
1.3.5 Setting Java Security

Change the Java security settings when an application is blocked by the Java security settings (expiration of the electronic certificate) so that the application can be used after the expiration.

NOTE: Code signing is implemented in Java programs to identify the author. When the expiration date of the electronic certificate used for code signing is reached, you cannot use the SVP or the Web Console.

Target version: Java 1.7.0_55 or later
Java 1.8.0_5 or later

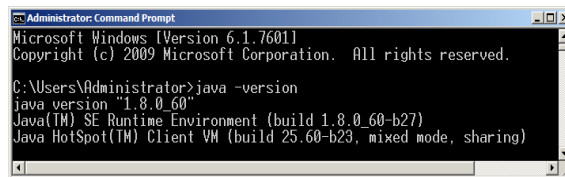
If the certificate is expired, the following window appears.
The alert window might vary depending on the Java version.



[Checking Java version]

Check the Java version in use.

1. Open the command prompt on the Maintenance PC.
2. Execute the “java -version” command to check the Java version.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>java -version
java version "1.8.0_60"
Java(TM) SE Runtime Environment (build 1.8.0_60-b27)
Java HotSpot(TM) Client VM (build 25.60-b23, mixed mode, sharing)
```

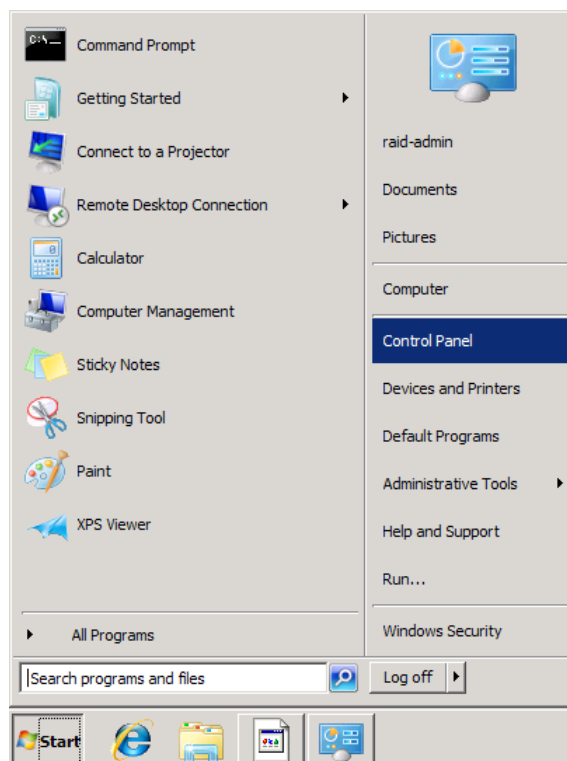
- For Java 1.7.0_55 or later, or Java 1.8.0_5 or later:
Go to [\[Changing Java security settings\]](#).
- For the other Java versions:
End the operations because the settings do not need to be changed.

[Changing Java security settings]

Change the settings following the procedure below.

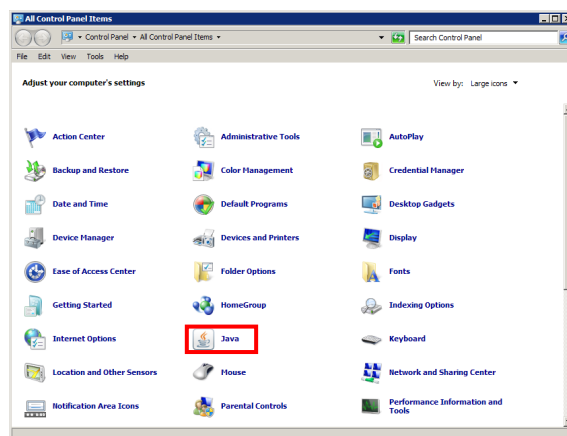
1. Open Control Panel

Select [Start]-[Control Panel].

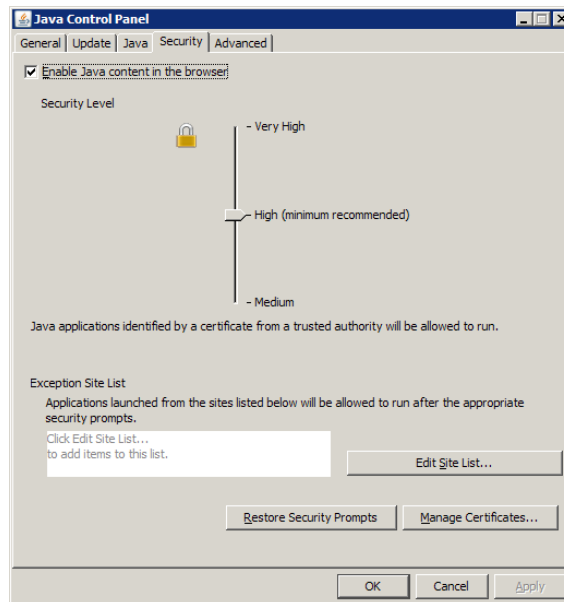


2. Open Java Control Panel

Select [Java].



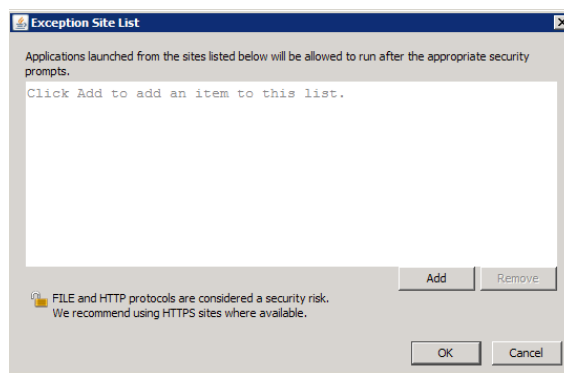
3. Open the [Security] tab in the Java Control Panel



4. Click the [Edit Site List...] button.

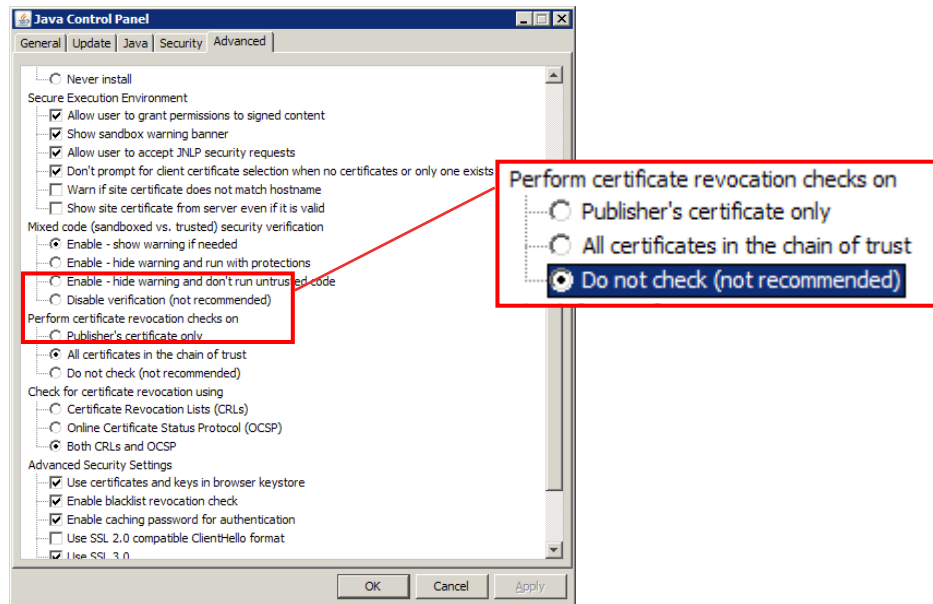
5. In the “Exception Site List” window, click the [Add] button to add the following URLs, and then click the [OK] button.

- URLs to be added:
- http://(IP address of Maintenance PC)
 - https://(IP address of Maintenance PC)
 - http://(IP address of GUM of CTL1)
 - http://(IP address of GUM of CTL2)
 - https://(IP address of GUM of CTL1)
 - https://(IP address of GUM of CTL2)
 - http://127.0.0.1
 - https://127.0.0.1
 - http://localhost
 - https://localhost



6. Open the [Advanced] tab in the Java Control Panel
Set “Perform certificate revocation checks on” to “Do not check (not recommended)” and click [OK] button.

NOTE: If “Perform certificate revocation checks on” is not displayed, set “Perform signed code certificate revocation checks on” to “Do not check (not recommended)” and click [OK] button.



7. End the procedure for changing the settings
If the alert for the expiration of the electronic certificate is displayed after the setting change, contact the Technical Support Division.

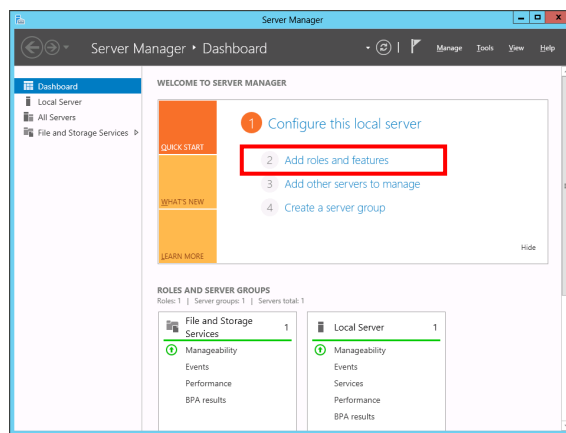
1.3.6 Enabling Adobe Flash Player (Windows Server 2012 or later)

Flash Player is included by Internet Explorer of Windows Server 2012 or later, and therefore can be used Web Console without install Flash Player. However, since Flash Player is disabled by default, set it to be enabled in the following method. (The following setting procedure is an example for Windows Server 2012.)

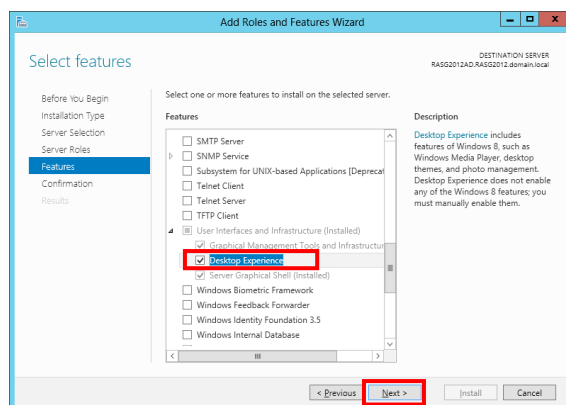
1.3.6.1 Using Flash Player in Windows Server 2012

In Windows Server 2012, installing [Desktop Experience] of [User Interface Infrastructure] enables Flash Player. The procedure for installing Desktop Experience is displayed next.

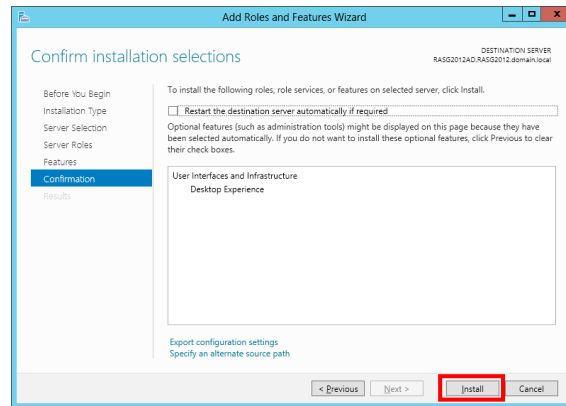
1. Click [Add roles and features] in [Server Manager > Dashboard] - [WELCOME TO SERVER MANAGER] - [QUICK START].



2. Click [Next >] for all of [Before You Begin], [Installation Type], [Server Selection] and [Server Roles] in [Add Roles and Features Wizard]. After proceeding to the [Features] items of [Add Roles and Features Wizard], click [User Interfaces and Infrastructure (Installed)], check [Desktop Experience] and click [Next>].



3. Click the [Install] button.



4. Reboot the PC.

1.3.6.2 How to use Flash Player that is installed on Windows Server 2016 or later

For Windows Server 2016, perform the following steps to use Adobe Flash Player.

1. Start the command prompt as Administrator.

2. Execute the following command:

```
dism /online /add-package /packagepath:"C:\Windows\servicing\Packages\Adobe-Flash-For-Windows-Package~31bf3856ad364e35~amd64~~10.0.14393.0.mum"
```

3. Reboot the PC.

1.3.7 Settings to Register Specific IP Address in Audit Log

If all the following conditions are met, an IP address of the command transmission source that is registered in the audit log might be “LOCALHOST” when maintenance operation is performed on the Maintenance PC. Apply Windows Update KB2883200 to the Maintenance PC so that a specific IP address can be registered in the audit log.

Condition

- Performing maintenance by the remote desktop connection to SVP (Supervisor PC)
- Connection source OS is a Windows 2012 Server R2 (64bit), Windows 8.1 Pro (64bit) or Windows 10 (64bit)
- Windows Update KB2883200 non-adaptation

1.3.8 IIS/FTP Server Setup

NOTE: The IIS/FTP server setup is necessary only when performing the following maintenance work.

- INSTALLATION SECTION “5. New Installation (Auto Define Configuration, All Firmwares)”
- FIRMWARE SECTION “5.1 Procedure of New Installation (Restore Configuration)”

IIS/FTP server setup is not necessary for maintenance work other than the above. However, when the IIS/FTP server is not set up, the alert message (21542-005033) saying that the IIS/FTP server is required for the above maintenance work appears.

- Unchecking the checkbox of [Not start service after addition immediately] and clicking [Apply] in the “Add System” window at the time of registering the storage system
- Starting the service of the Storage System icon of the storage system registered in the Storage Device List

The Web server functions provided by Microsoft are called IIS (Internet Information Services).

IIS include a Web server, FTP server and SMTP server.

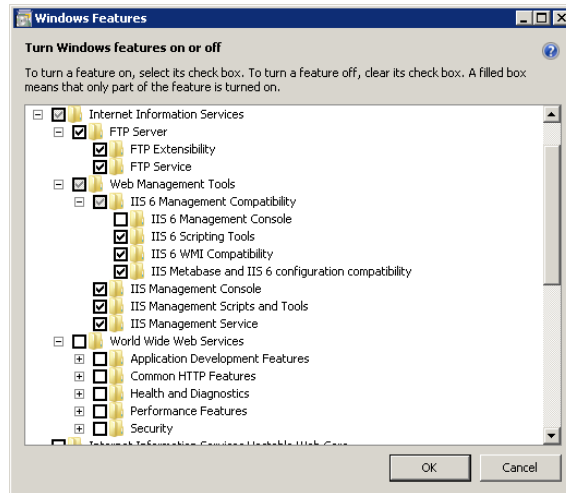
IIS of Windows 7/Windows 8.1/Windows 10 have the restrictions on the maximum number of simultaneous connections.

The procedure for Windows7 is shown below as an example.

1. Installing IIS/FTP

- (1) Click the [Control Panel] button.
- (2) Click the [Programs and Features] button.
- (3) Click [Turn Windows features on or off].
- (4) Select [Internet Information Services] and set the following items.
 - (a) Check the check boxes of the following items.
 - FTP Server
 - FTP Service
 - FTP Extensibility
 - Web Management Tools
 - IIS 6 Management Compatibility
 - IIS 6 WMI Compatibility
 - IIS 6 Scripting Tools
 - IIS Metabase and IIS 6 configuration compatibility
 - IIS Management Console
 - IIS Management Service
 - IIS Management Scripts and Tools

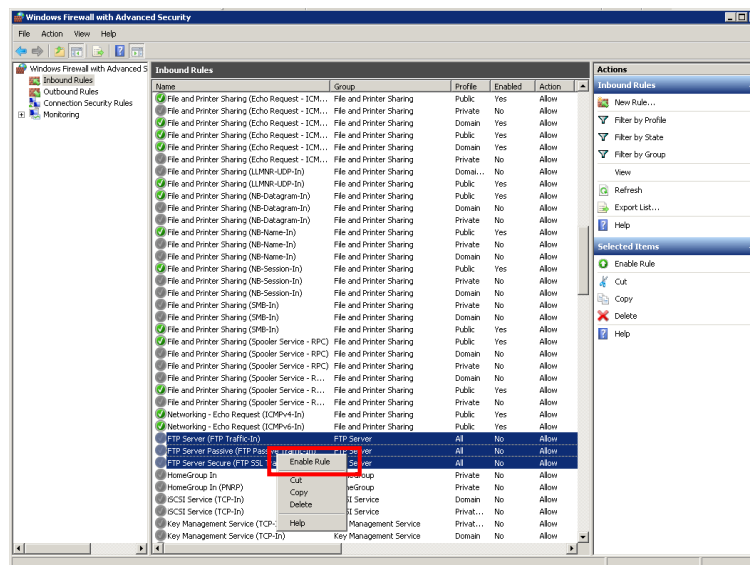
- (b) Uncheck the check boxes of the following items.
- World Wide Web Services



2. Setting the FTP firewall

Enabling the FTP firewall setting if it is not enabled

- (1) Open [Administrative Tools] from [Control Panel] to start [Windows Firewall with Advanced Security].
- (2) Click [Inbound Rules] of the left side tree to select three types of FTP Server Passive, FTP Server Secure, and FTP server. Select [Enable Rule] from the right-click menu.



1.3.9 Setting Virtual Memory

NOTICE: The status of the Web Application Server becomes [TRSTNA000007] during startup of the Web Console, and then the Web Console might not be started. In this case, even if the virtual memory of the Windows OS is already set, change the initial size and maximum size of the virtual memory by following the procedure below:

1. In the [Control Panel], select [System] - [Advanced system settings], and then open the System Properties.
2. In the System Properties, select [Advanced] - [Performance] - [Settings...], and then open the Performance Options.
3. In the Performance Options, select [Advanced] - [Virtual memory] - [Change...], and then open the Virtual Memory.
4. In the Virtual Memory, make the following settings.
 - (1) Clear the check mark for [Automatically manage paging file size for all drives].
 - (2) Select any drive in the "Drive" field. (Any drive other than drive C is recommended.)
 - (3) Select [Custom size], and then set both the [Initial size] and [Maximum size] to the value of [Recommended] displayed at the bottom of the dialog box.

After making the settings, restart the Maintenance PC to have the settings enabled.

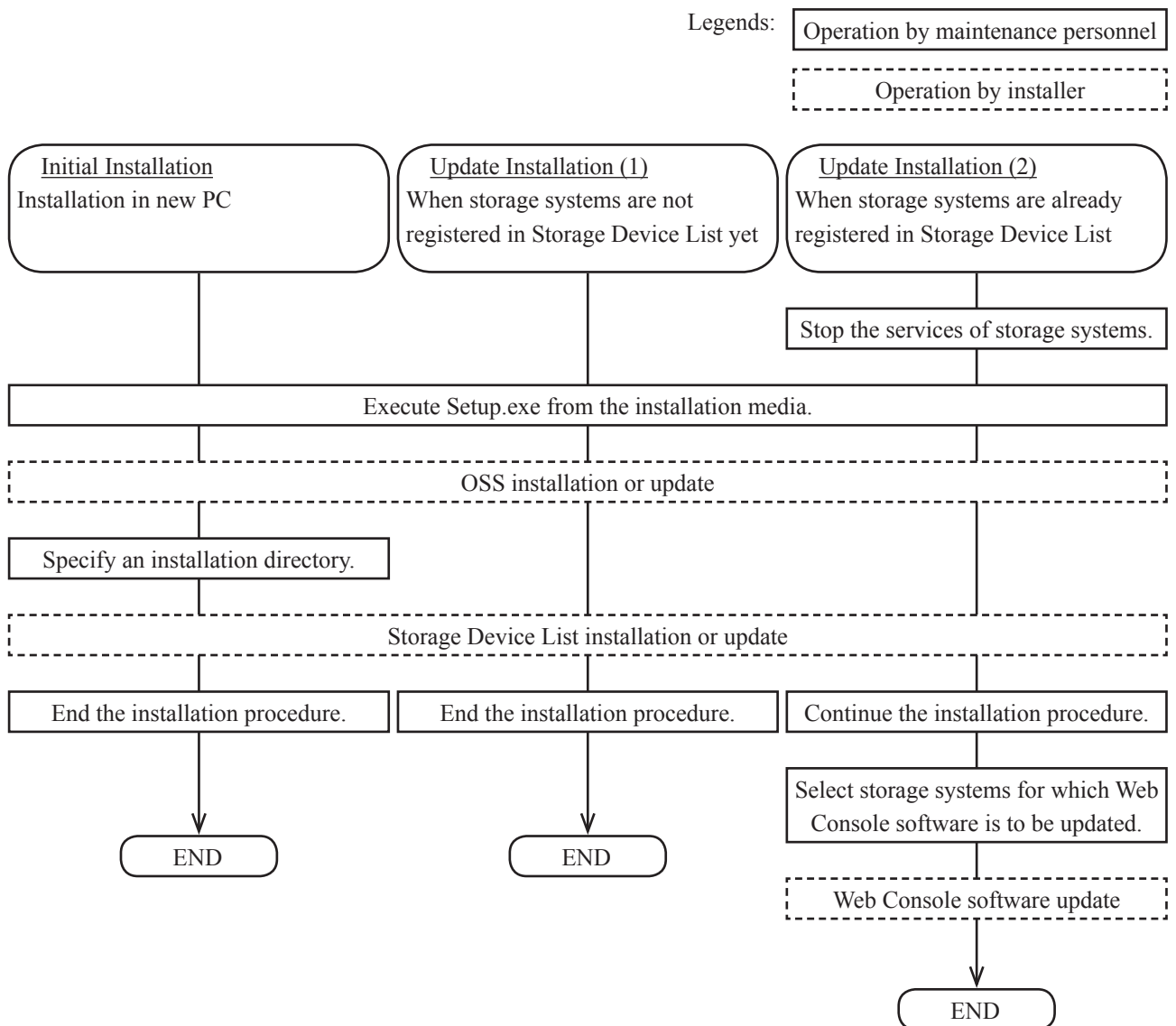
1.4 Maintenance PC Software Initial Installation/Update Installation

1.4.1 Workflow of Installation

Install the following Maintenance PC software using the installation media.

- (1) OSS (Open Source Software)
Software required for using Maintenance PC software.
- (2) Storage Device List
Software to start/stop the service for performing the storage system maintenance. You can register the storage systems to be maintained in the Storage Device List window.
- (3) Web Console software
Software to operate the storage systems registered in Storage Device List.

The general workflow of installation is shown below.



1.4.2 OSS That Is to Be Installed

The names and versions of the OSS that is to be installed in the Maintenance PC are shown below.
For the procedure for checking versions of OSS that is installed in the Maintenance PC, see [“11.6 Specifications of Web Server Status List”](#).

Installation media	Software							
	JRE	JRE (Client)	Perl	Apache	Jetty	OpenSSL	Flash	PuTTY
When the firmware version is less than 88-01-03-x0/xx	8 Update 152	8 Update 152	5.18.1.1800	2.4.16	9.2.10	1.0.2n	20.0.0.306	0.64
When the firmware version is 88-01-03-x0/xx or later	↑	↑	↑	↑	↑	↑	28.0.0.161	↑

NOTICE:

- If Storage Device List is updated using the installation media, the software of the version that is described in the table is installed.
However, for the update installation, the software other than JRE (Client) and Flash is updated to the version that is described in the table, and the version of JRE (Client) and Flash is not updated. The Maintenance PC still operates normally in this case. Furthermore, the version of JRE (Client) and Flash can be updated arbitrarily by the customer's decision within the range that is described in the above table or “Requirements for Windows-based computers” of “System Administrator Guide”.
- When the version of JRE6 or later is not installed, JRE (Client) is installed.
- When the following conditions are met, Flash is installed.
 - When OS is Windows7.
 - When Version of Flash Player 13 and over is not installed.

NOTICE: If JRE8 on the Maintenance PC starts, the JRE (Client) setting in JRE7 or earlier that is installed in the customer environment might partly return to the default setting. When this phenomenon occurs, perform the setting again.

1.4.3 Installation Procedure

CAUTION

There are the installation media for the Maintenance PC and the installation media for the SVP. Use the installation media corresponding to the PC (Maintenance PC/SVP) for the installation/update.

If incorrect installation media is used, the Maintenance PC or the SVP does not operate correctly. In that case, see ["8.2 Maintenance PC Software Uninstallation"](#) to remove it (The procedure for remove the SVP software is the same).

Then, use the correct installation media and install it again.

- NOTICE:**
- In the environment where Command Control Interface (CCI) is not installed, CCI is automatically installed when the MPC Software is installed.
 - In the environment where Command Control Interface (CCI) is already installed, install the MPC software in the drive with the same letter as assigned to the drive for CCI. If it cannot be installed in a drive with the same letter as assigned to the drive for CCI, install it in a different drive with a letter later in alphabetical order. When the MPC software is installed in a drive with a letter earlier than assigned to the drive for CCI, an error such as "raidmgr is not found." occurs if a CCI command is not run in full path.
 - In the environment where Command Control Interface (CCI) is installed, CCI update is available using CCI contained in the media with the MPC Software while the MPC Software is installed. The CCI version displayed in "Programs and Features" is not updated. To check the version of CCI installed, run the CCI command "raidqry -h".
 - For 32-bit PC, Command Control Interface (CCI) contained in the MPC Software media is not available. Install Hitachi 32-bit CCI in the drive with the same drive letter as assigned to the drive containing Maintenance PC.

1. Stopping Storage System services

In the case of update installation, stop the services of the storage systems on Storage Device List. (See [“2.14.2 Stopping the Service of Storage System”](#).)

If storage systems are not registered in Storage Device List, you do not need to stop storage system services.

2. Inserting the installation media

Insert [Installation Media for Maintenance PC] into the DVD drive of the Maintenance PC.

3. Right-click Setup.exe immediately under the drive to select [Execute as Administrator].

NOTE: • If a DVD drive is not mounted on a PC, copy all the files of installation media for the Maintenance PC to “work folder”. For a “work folder” name, do not use a double-byte character because Setup.exe might not start if a double-byte character is included in the name.

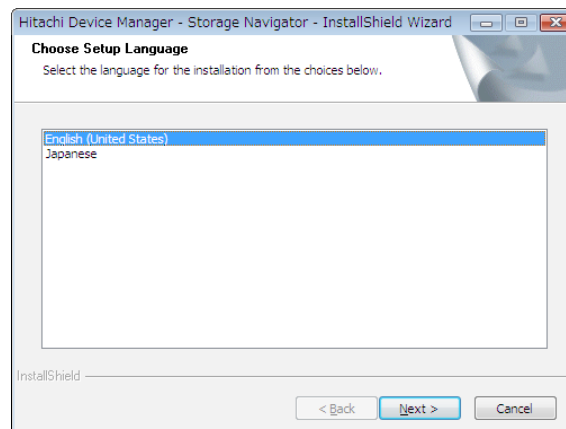
Then, use the files in “work folder”.

- If an antivirus program is installed on the Maintenance PC, too much time might be taken for the installation, or an alert message of the antivirus program might be displayed, affecting the installation operation. That is why we recommend that you suspend the antivirus program during the installation.

4. Checking languages

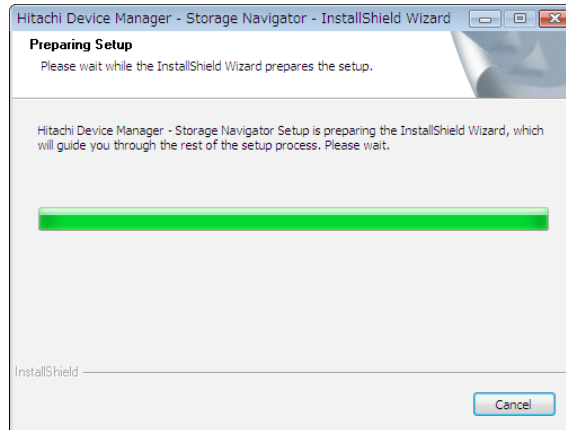
In the case of initial installation, the following window is displayed.

Select either English or Japanese.



5. Preparing for installation

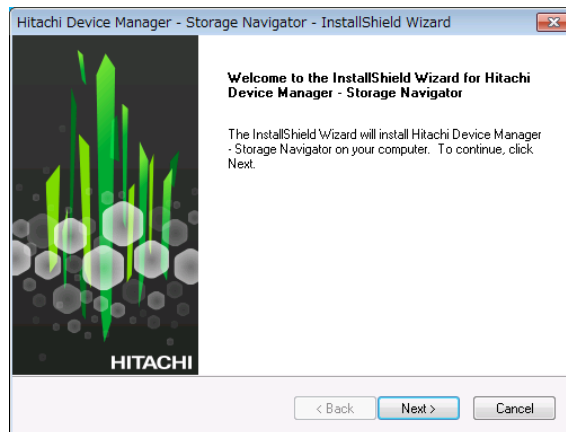
The “Preparing Setup” window is displayed. Wait until the preparation is completed.



6. Installation start

The “InstallShield” window is displayed when the preparation is completed.

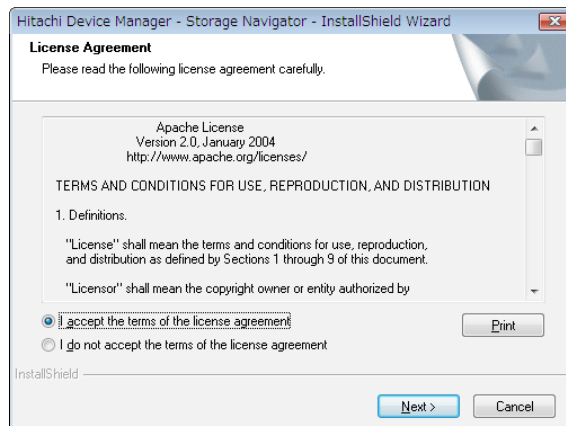
Click the [Next >] button.



7. Confirming OSS licenses

The “Confirmation” window of the OSS licenses is displayed.

Select [I accept the terms of the license agreement] and click the [Next >] button.



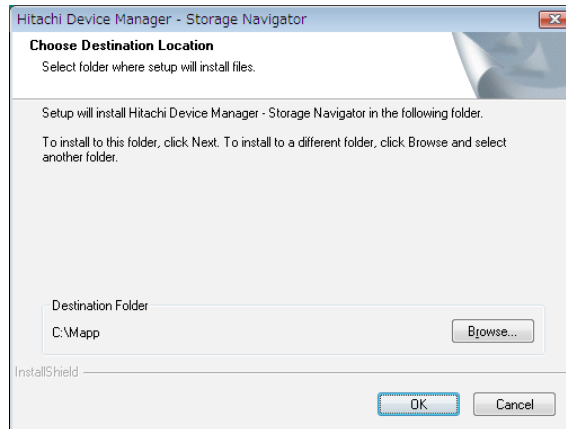
8. Selecting an installation directory

In the case of initial installation, the following window is displayed. Specify the installation directory.

- (1) The confirmation message concerning the installation drive for the storage management software is displayed. Check the content and click [OK].



- (2) Select a directory to be installed and click [OK].
The default directory is [C:\Mapp].

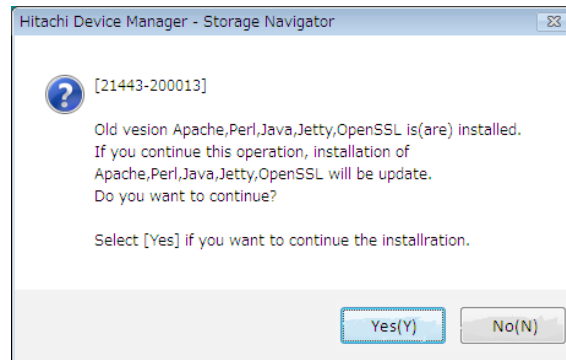


NOTE: To change the default directory to a different one, available characters for the directory are one-byte alphanumeric characters, '-' (hyphen), and '_' (underscore). The number of characters for a directory path is up to 22.

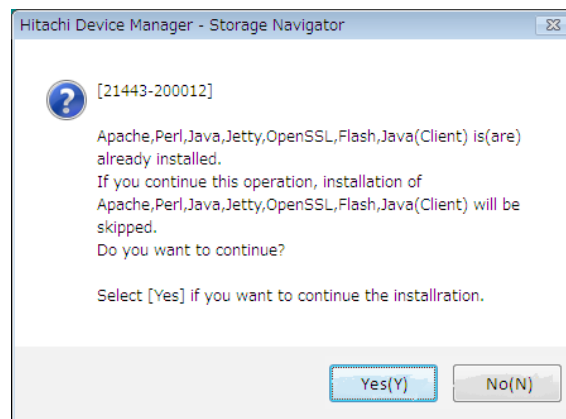
9. OSS update confirmation message

In the case of update installation, the following window is displayed. Click the [Yes] button.

(1) When a prior version of OSS is already installed



(2) When a same or later version of OSS is already installed



10. Command Control Interface (CCI) update confirmation message

When Command Control Interface (CCI) is installed separately, a message is displayed for updating the CCI using CCI contained in the media with the MPC Software. To perform update, shut down the CCI, and then click [Yes].

When [No] is clicked, the CCI version is not changed.

When multiple CCI applications are installed, the CCI in a drive with the earliest letter in alphabetical order will be updated.



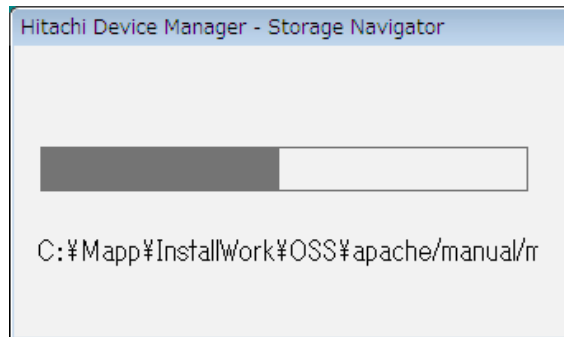
11. Decompressing and copying the Software

Decompress the files in the media and copy them to the folder selected in [Step 8](#).

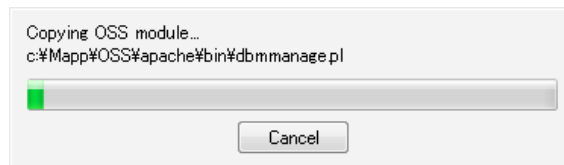
The following window is displayed during the processing.

Wait until the decompression and copy are completed.

<Decompressing Files>

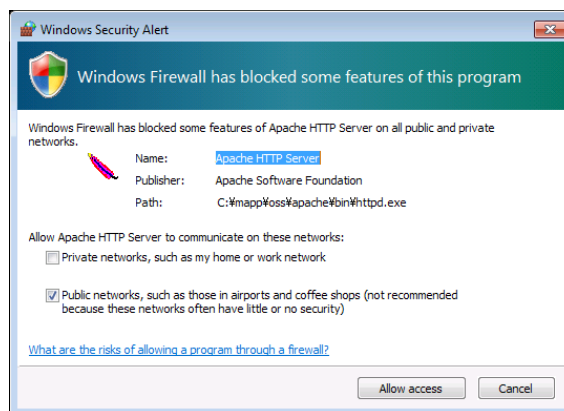


<Copying Files>



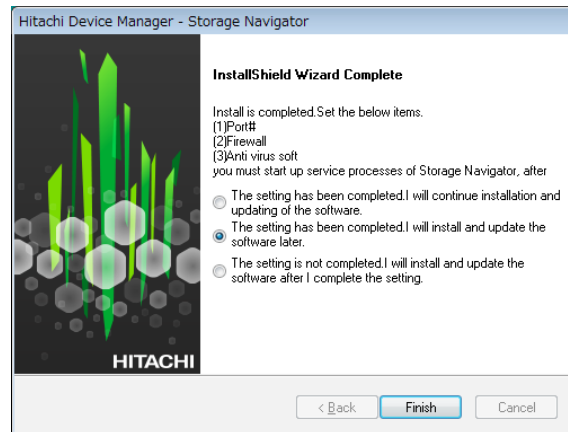
12. Windows Security Alert

When the “Windows Security Alert” window is displayed, click [Allow Access].



13. Selecting whether to end or continue the installation procedure

The following window is displayed.



<For initial installation or update installation when storage systems are not registered in Storage Device List yet>

End the installation procedure here.

Select [The setting has been completed. I will install and update the software later.] and click the [Finish] button. Remove the installation media.

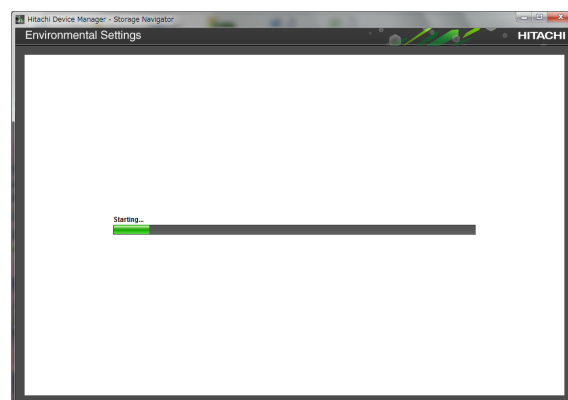
NOTE: If you change the port number used by the Maintenance PC software later (see [“1.3.2 Checking Overlap of Port Number”](#)), select [The setting is not completed. I will install and update the software after I complete the setting.] and click the [Finish] button. Remove the installation media. Then, change the port number and restart the maintenance PC.

<For update installation when storage systems are already registered in Storage Device List>

Continue the installation procedure and update the Web Console software for the storage systems registered in Storage Device List.

Select [The setting has been completed. I will install and update the software later.] and click the [Finish] button. Go to [Step 14](#).

14. The “Preparing Setup” window is displayed. Wait until the preparation is complete.

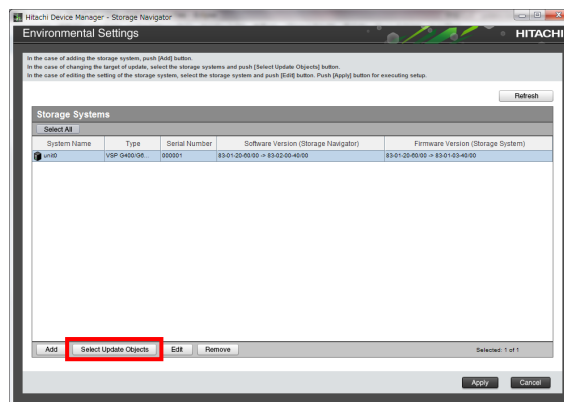


15. Selecting storage systems of the Web Console software update objects

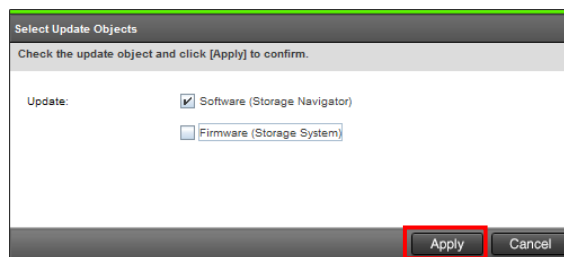
The registered storage systems are displayed on Storage Device List. Repeat Steps (1) and (2) shown below for each storage system.

- (1) Select a storage system and click the [Select Update Objects] button.

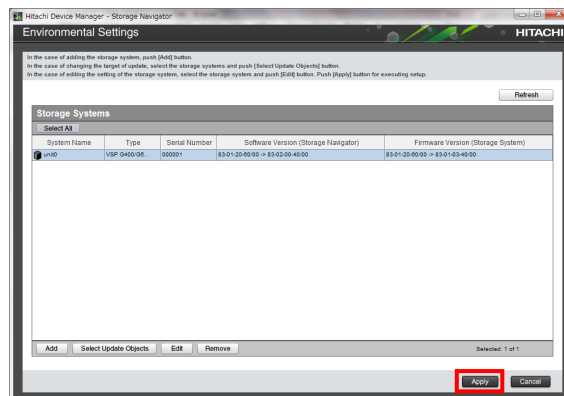
NOTE: Select only the storage systems supported by the installation media. If both types of the storage systems, DW800 and DW850, are registered on one Maintenance PC, both storage system types are displayed. The storage systems to which the Web Console software update can be applied depend on the installation media you use. To update the Web Console software on the storage systems that are not supported by the installation media, perform the update through Storage Device List after completing the installation procedure (refer to an appropriate storage system maintenance manual).



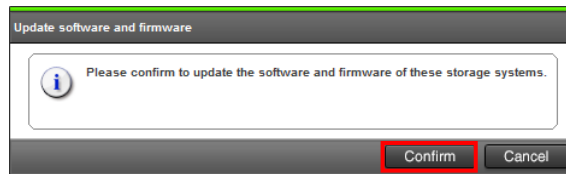
- (2) In the “Select Update Objects” window, uncheck [Firmware (Storage System)], check [Software (Storage Navigator)] only, and click the [Apply] button.



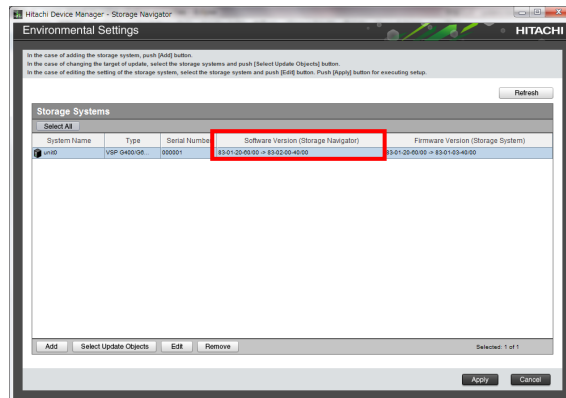
16. Click the [Apply] button.



17. The “Update software and firmware” window is displayed. Click the [Confirm] button.



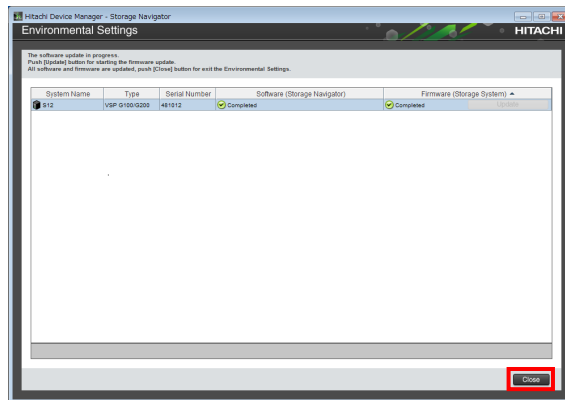
18. The Web Console software update is started.
- You can see the software update status in the Software column.



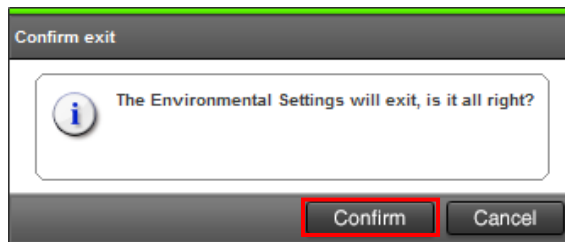
The software update status is as shown below.

Status	Description
Waiting	Software is not updated. Software is updated one by one. If the software of a storage system is already updated, the other storage systems are in this state.
In Progress	Software update is running.
Completed	Software update is complete.
Failed	Software update failed. If storage systems were added, the addition might not be complete. Click and follow the message.
(Not Update)	This is not selected as a software update target. If storage systems were added, this state does not appear.

19. After completing the update of the software, click the [Close] button.



20. Click the [Confirm] button to terminate the tool.



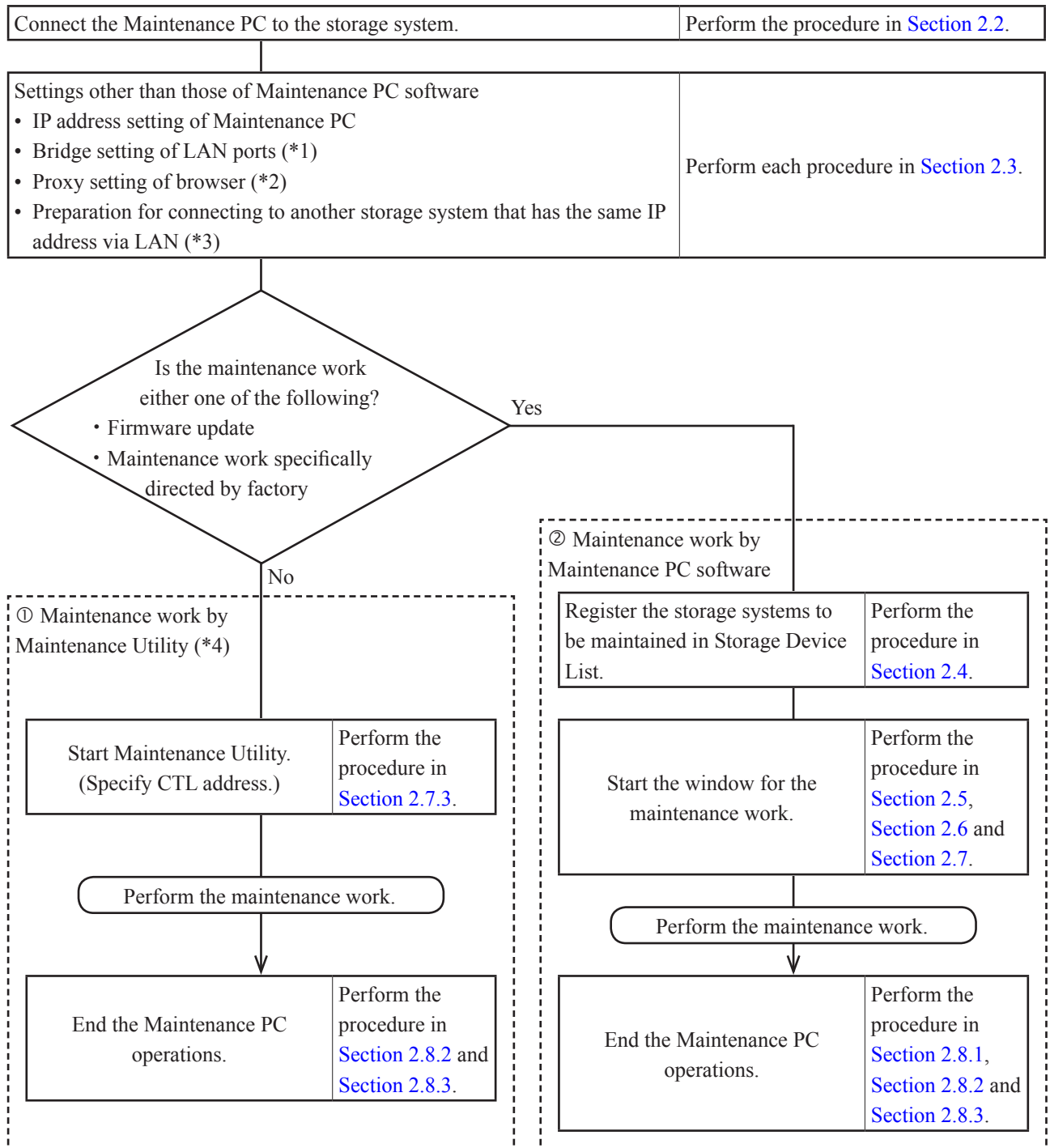
End the installation procedure of the Maintenance PC software and remove the installation media.

NOTE: If an antivirus program was suspended in [Step 3](#), run it again.

2. Using Maintenance PC at Client's Site

2.1 Workflow of Settings and Operations of the Maintenance PC at Client's Site

The Maintenance PC settings before starting the maintenance work and the Maintenance PC operations after the maintenance work are shown in the following workflow.



- *1 Perform the setting only when the Maintenance PC has two or more LAN ports and they are directly connected to the CTL1 maintenance port and CTL2 maintenance port not via HUB.
- *2 Perform the setting only when the browser is set to use a proxy server.
- *3 Perform the preparation only when connecting to another storage system that has the same IP address as that of the storage system that you have ever connected to.
- *4: When you perform the maintenance work using Maintenance Utility in procedure ① according to TROUBLESHOOTING SECTION, operations on the Web Console, operations on the MPC window, or operations that use a force execution option of Maintenance Utility might be required. In such a case, log out of Maintenance Utility once, start the window for maintenance work of the Maintenance PC software by following the procedure ②, and then resume the work. If you acquire the dumps using Maintenance Utility in procedure ①, see [“3.27 Acquiring Dumps using Maintenance Utility”](#).

2.2 Connecting Maintenance PC to Storage System

NOTICE: When configuring the maintenance LAN, avoid a large-scale network configuration in which many and unspecified devices are connected. Create a closed network configuration by connecting the necessary devices only.

When performing the monitoring, see [Notes on monitoring].

1. Connect a power cable and LAN cable to the Maintenance PC
2. Connect the LAN cable to the maintenance LAN port at the CTL1 side. (Refer to [Figure 2-2.](#))
Connect the LAN cable to the maintenance LAN port at the CTL2 side, when that at the CTL1 side cannot be used because of the device failure.

NOTE: For new installation of the Firmware, Controller Board 1 and 2 must be normal.
Connect the LAN cable to the Controller Board 1 side.

3. Connect the power cable of the Maintenance PC to a 100V AC outlet prepared by customers.
4. Turn on the Power Supply of the Maintenance PC.

[Notes on monitoring]

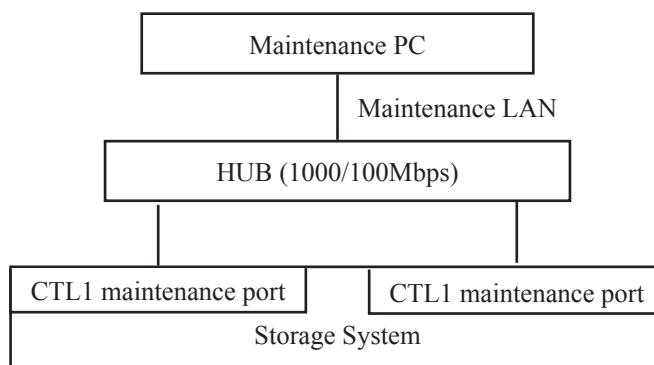
There are the following two methods for monitoring:

- Using the performance monitor function of Web Console
- Using the “System Monitor” window of Maintenance Utility

When collecting the monitor information by using the performance monitor function of Web Console, connect the Maintenance PC to CTL1 and CTL2 by using HUB to communicate with DKC.

NOTE: If CTL1 and CTL2 are not connected simultaneously, monitor data might be missed.
Connect the Maintenance PC to the Storage System with the following connection configuration diagram.

Figure 2-1 Connection Configuration Diagram



<When the Maintenance PC and the storage system are connected through a network hub equipped with the Firewall function>

Perform the pass-through setting of the Firewall for the following port numbers.

Protocol	TCP/UDP	Port Number	Transfer Direction
HTTP	TCP	80	From Maintenance PC to the storage system
HTTPS	TCP	443	From Maintenance PC to the storage system
SVP Communication Protocol (SSL)	TCP	10500	From Maintenance PC to the storage system

When you perform the following maintenance work, perform the Firewall pass-through setting for all port numbers (from the storage system to the Maintenance PC and vice versa).

- INSTALLATION SECTION “[5. New Installation \(Auto Define Configuration, All Firmwares\)](#)”
- FIRMWARE SECTION “[5.1 Procedure of New Installation \(Restore Configuration\)](#)”

<When the Maintenance PC is used as SVP and the Maintenance PC and the management terminal are connected through a network hub equipped with the Firewall function>

Perform the pass-through setting of the Firewall for the following port numbers.

Protocol	TCP/UDP	Port Number	Transfer Direction
HTTP	TCP	80 (*1)	From management terminal to Maintenance PC
HTTPS	TCP	443 (*1)	From management terminal to Maintenance PC
RMI	TCP	1099 (*1)	From management terminal to Maintenance PC
RMI (SSL)	TCP	5443 (*1)	From management terminal to Maintenance PC
RMI	TCP	51099 (*1)	From management terminal to Maintenance PC
RMI	TCP	51100-51355 (*1)	From management terminal to Maintenance PC

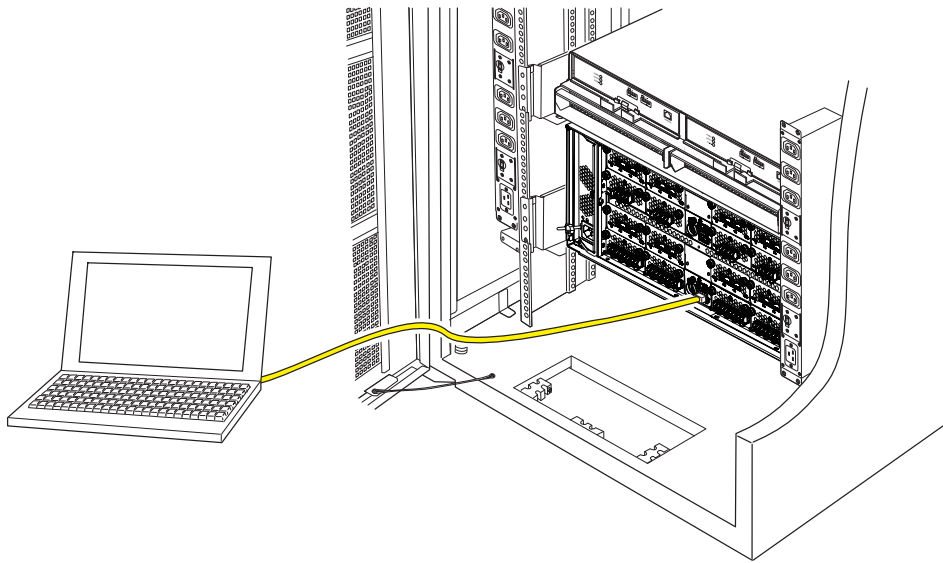
*1: The port number can be changed. (See “[10.1 Changing Port Numbers Used by the Maintenance PC](#)”.) If you change the port number, you need to perform the Firewall pass-through setting for the changed port number.

<When the management terminal and the storage system are connected through a network hub equipped with the Firewall function>

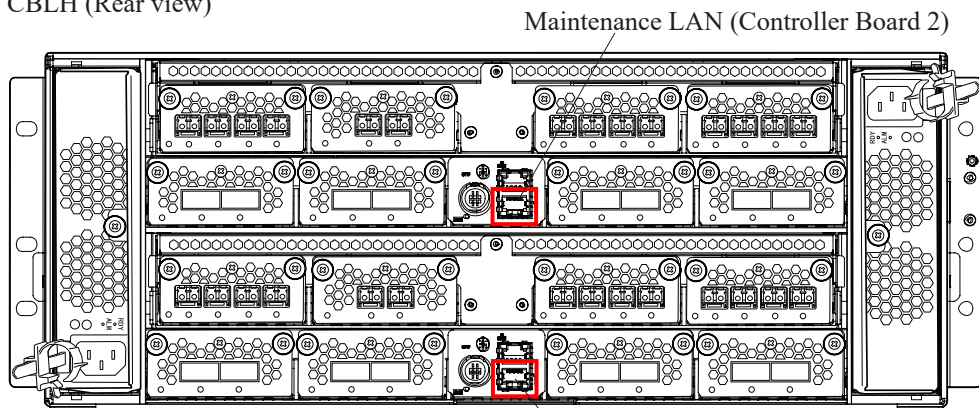
Perform the pass-through setting of the Firewall for the following port numbers.

Protocol	TCP/UDP	Port Number	Transfer Direction
HTTP	TCP	80	From management terminal to the storage system
HTTPS	TCP	443	From management terminal to the storage system

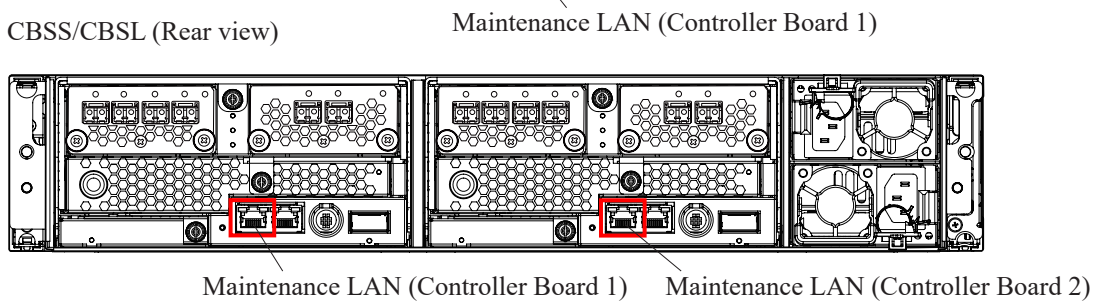
Figure 2-2 Connection of Cables



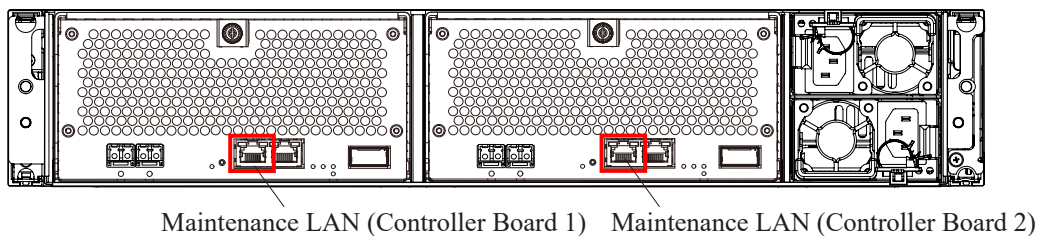
• CBLH (Rear view)



• CBSS/CBSL (Rear view)



• CBXSS/CBXSL (Rear view)



2.3 Settings Other Than those of Maintenance PC Software at Client's Site

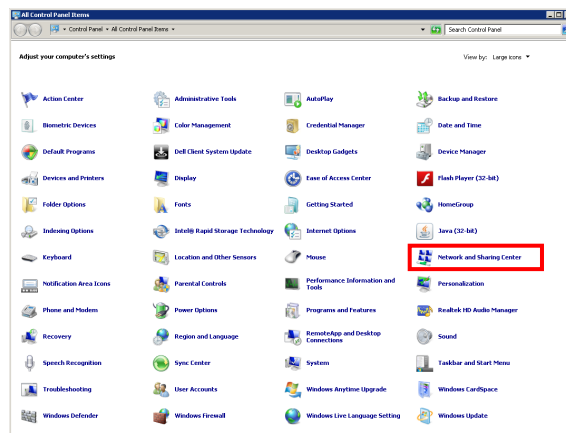
2.3.1 IP Address Setting of Maintenance PC

NOTE: When the storage systems to be maintained are already registered in Storage Device List, confirm that all the Storage System icons are in the service stop status ("Stopped" status), and then perform the following procedure. If you perform the procedure when they are in another status, a reboot of the Maintenance PC is required.

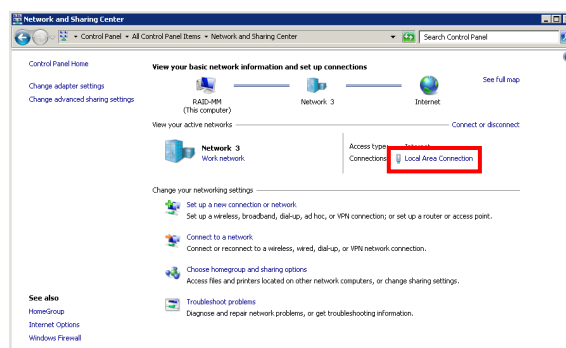
- Example of Service stop status icon



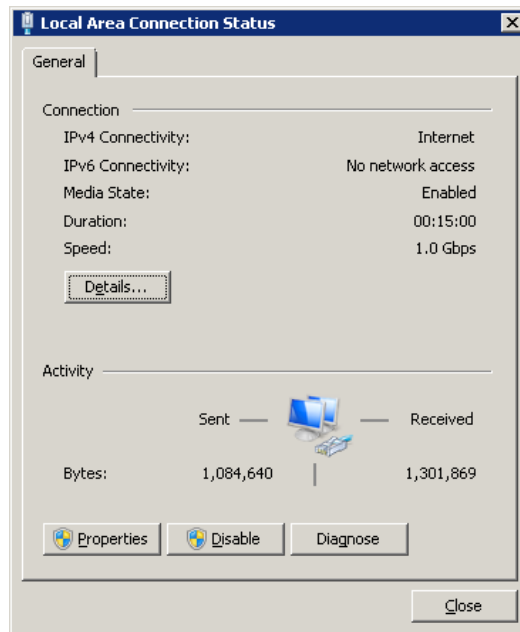
1. Open [Network and Sharing Center] from [Start] - [Control Panel].



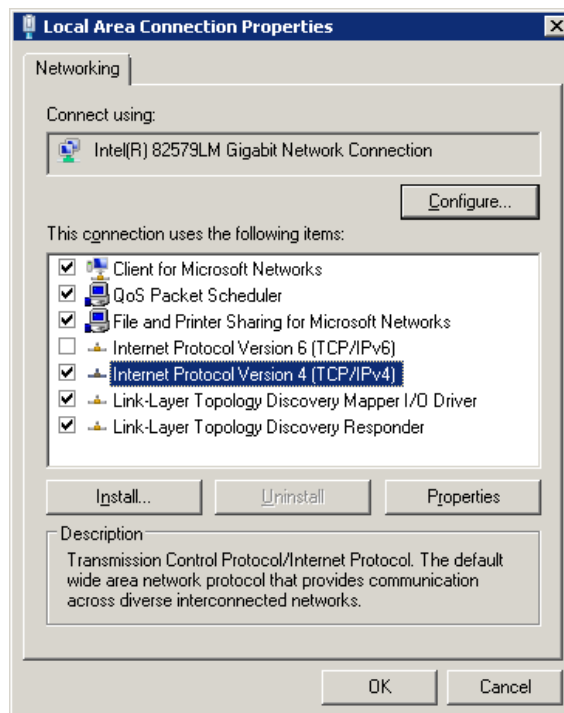
2. Click the [Local Area Connection].



- Click the [Properties] button in the “Local Area Connection Status” window.



- Select the [Internet Protocol Version 4 (TCP/IPv4)] in the “Local Area Connection Properties” window and click the [Properties] button.



5. Set an IP address in the “Internet Protocol Version 4 (TCP/IPv4) Properties” window and click the [OK] button.

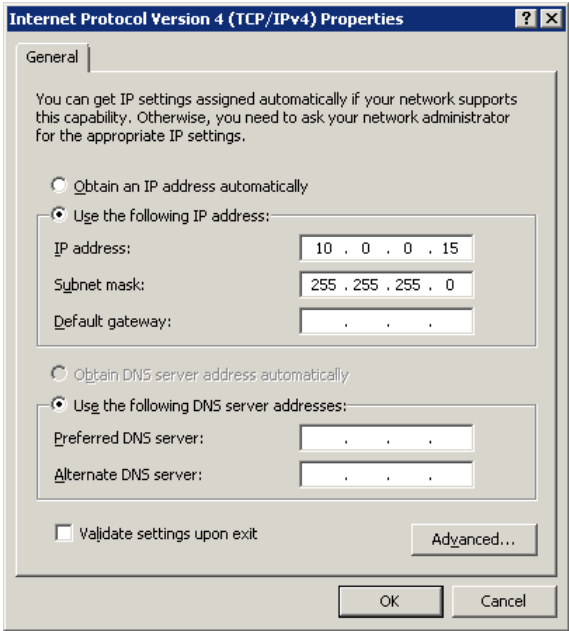


Table 2-1 Operation Environment shows two types of IP addresses of the maintenance LAN port.

- Item No. 1: Initial setting status
Item No. 2: Network already set up at factory shipment

Table 2-1 Operation Environment

Item No.	Maintenance LAN Port (CTL1)		Maintenance LAN Port (CTL2)		Maintenance PC	
	IP Address	Subnet Mask	IP Address	Subnet Mask	IP Address (*1)	Subnet Mask
1	10.0.0.16	255.255.255.0	10.0.0.17	255.255.255.0	10.0.0.15	255.255.255.0
2	aaa.aaa.aaa.aaa	255.255.255.0	aaa.aaa.aaa.aaa	255.255.255.0	aaa.aaa.aaa.15	255.255.255.0

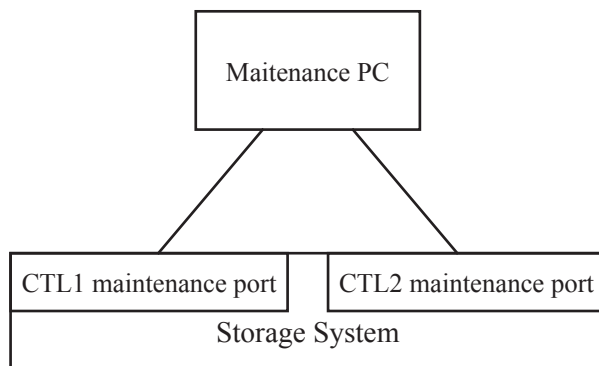
aaa: An IP address set in the “Network Setting” window of the Storage System.

*1: When “15” cannot be used as a host address (address competition and others), specify the address not to compete with the maintenance port address of CTL.

6. Click the [OK] button in the local area connection property and close the window.
7. Close the network connection window.

2.3.2 Bridge Setting of LAN Ports

When the Maintenance PC has two or more LAN ports and they are directly connected to the CTL1 maintenance port and CTL2 maintenance port of the storage system not via HUB, perform the bridge setting of the LAN ports.



<Bridge setting procedure>

1. In Control Panel, select [Network and Sharing Center] and click [Change adapter settings] in the displayed window.
2. Select two LAN connection icons with the Ctrl key pressed, right-click, and then select [Bridge Connections].
3. The Network Bridge icon is made.
4. Right-click the Network Bridge icon and select [Properties].
5. Select [Internet Protocol Version 4 (TCP/IPv4)] and select [Properties].
6. Select [Use the following IP address:] and enter a different IP address from the ones that are used for the two LAN ports.
7. After setting the IP address, click the [OK] and close the window.

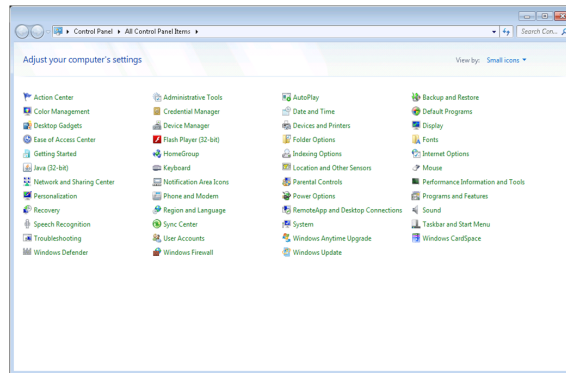
2.3.3 Proxy Setting of Browser

If the browser of Maintenance PC is set to use a proxy server, pages of Web Console or Maintenance Utility might not be found.

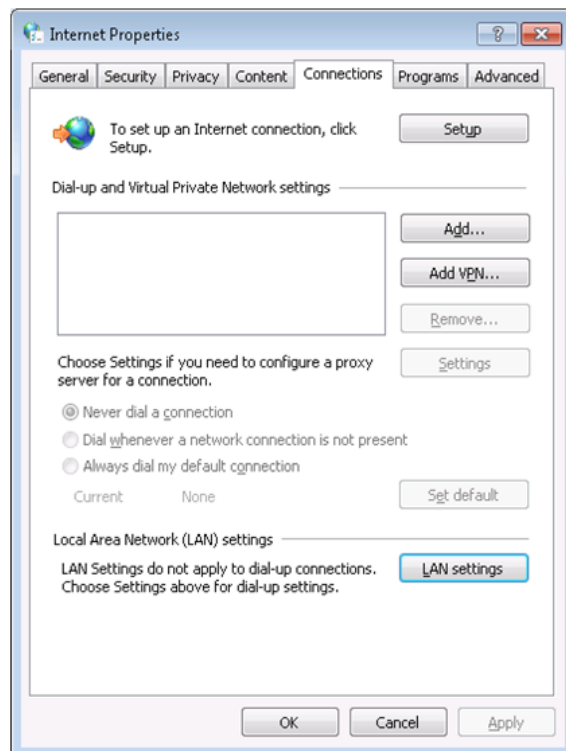
Set the IP address of CTL1 and CTL2 and the IP address of the Maintenance PC to [Exceptions] of the proxy.

- An example of the proxy setting procedure (in case of Windows 7)

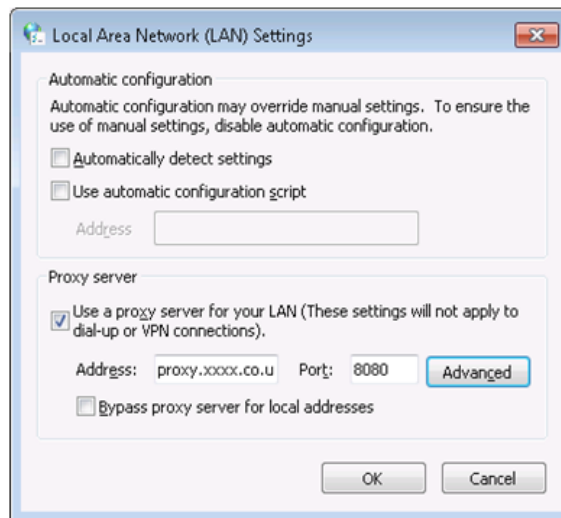
1. Open [Internet Options] from [Start] – [Control Panel].



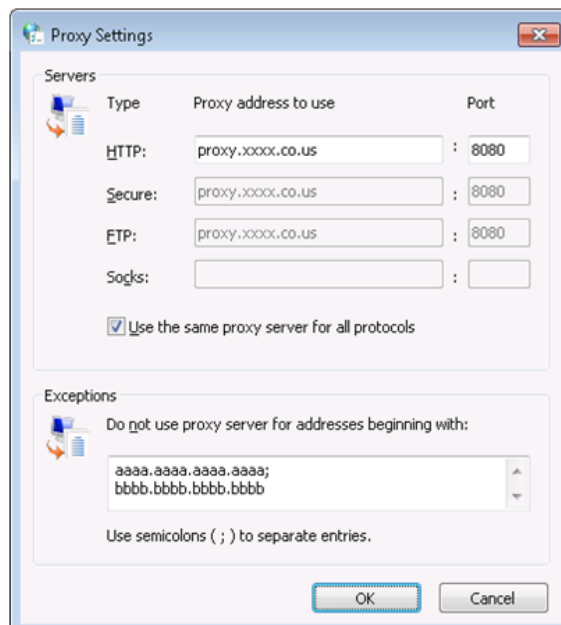
2. Select [LAN settings] of the [Connections] tab.



3. When [Use a proxy server for your LAN] is checked, select [Advanced].



4. Add the IP address of CTL1 and CTL2 and the IP address of the Maintenance PC to [Exceptions], and then select [OK].



2.3.4 Preparation for Connecting to another Storage System That Has the Same IP Address via LAN

- Procedure for preparing for connecting to another storage system that has the same IP address via LAN
Before connecting to another storage system that has the same IP address via LAN, execute the following command from the command prompt on the Maintenance PC to delete the information of the IP address stored in the arp table.

When connecting to a storage system, the IP address and the physical address of the storage system are stored in pairs in the Maintenance PC. Unless you delete the stored information, you cannot connect to another storage system that has the same IP address.

```
arp -d IP address
```

- IP address: An IP address stored in the arp table

Example) When deleting the IP address 10.0.0.16 (default value) from the arp table

```
arp -d 10.0.0.16
```

To verify that the IP address stored in the arp table is deleted, execute the following command.

```
arp -a
```

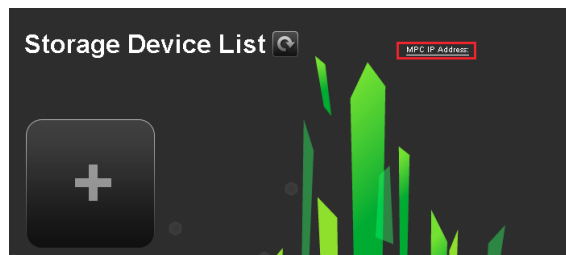
If the specified IP address does not exist or if the message “No ARP Entries Found” is returned, the IP address is deleted from the arp table.

2.4 Registering Storage Systems to Be Maintained in Storage Device List

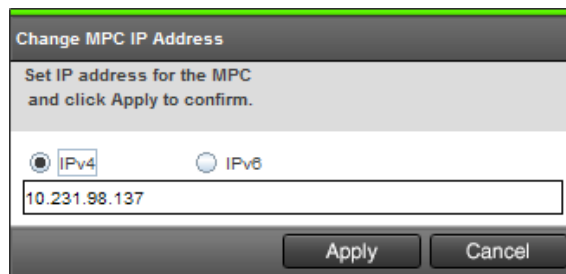
Up to 256 Storage Systems can be registered in Storage Device List. However, you can operate only one Storage System for which the service is running.

NOTE: In the following procedure, the installation media for the Maintenance PC is used.
If you register both types of the storage systems, DW800 and DW850, on one Maintenance PC, prepare the installation media of each storage system type.
For the procedure for registering the DW800 storage systems, refer to the Maintenance Manual of DW800.

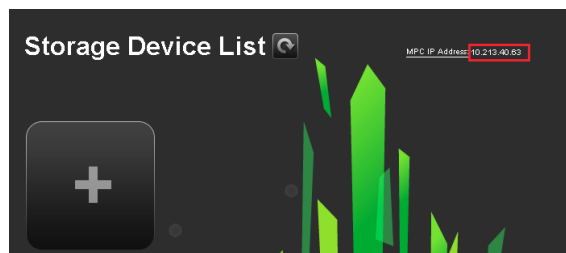
1. Right-click the connection icon “Open Storage Device List” on the desktop of the Maintenance PC and select [Run as administrator].
-
2. Set an IP Address.
 - (1) Click the [MPC IP Address] link in the “Storage Device List” window.



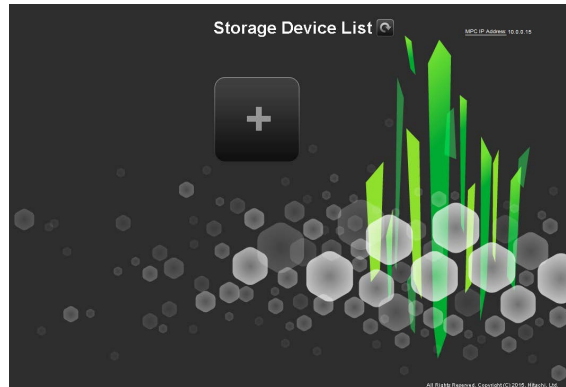
- (2) In the “Change MPC IP Address” window, enter the IP address of the Maintenance PC and click the [Apply] button.



- (3) Check that the IP address set in [Step \(2\)](#) is displayed beside the [MPC IP Address] link.



3. Create a Storage System icon.
 - (1) Click the plus button in the displayed “Storage Device List” window.



- (2) Perform the Storage System settings in the “Add System” window.
Enter all the items, and then click the [Apply] button.
See the [MPC02-160](#) to perform it [Manual].
For the new installation, select [Manual].

- When selecting [Auto Discovery]

Item	Description
Software Selection	Click the [Browse...] button and select [Software\productname.inf] in the installation media for the Maintenance PC to acquire installation information.
System Selection	<p>Select the input method of the Storage System information.</p> <ul style="list-style-type: none"> • [Auto Discovery] (default selection): Acquire the Storage System information automatically. • [Manual]: Set each of the displayed items, [System Type], [Software Version] and [Serial Number].
IP Address (CTL1)	<ul style="list-style-type: none"> • Select a type of IP address of the maintenance port of CTL1. [IPv4] (Default) [IPv6] • Enter the CTL1 IP address in a format corresponding to the selected IP address.
IP Address (CTL2)	<ul style="list-style-type: none"> • Select a type of IP address of the maintenance port of CTL2. [IPv4] (Default) [IPv6] • Enter the CTL2 IP address in a format corresponding to the selected IP address.
System Name	<p>Enter a Storage System display name.</p> <p>The number of characters you can enter is zero to 180.</p> <p>Allowed characters are one-byte alphanumeric characters, symbols (# \$ % & ' * + - . / = ? @ ^ _ ` { } ~).</p> <p>You cannot use one-byte spaces.</p>
Description	<p>Enter the description of the Storage System.</p> <p>The number of characters you can enter is zero to 180.</p>
User Name	Enter the user name and password for the maintenance account of the storage system.
Password	A password for the maintenance account of the storage system is changed by your customer after the storage system is installed. Ask your customer to let you know the password.
Not start service after addition immediately	<p>Select whether to connect the registered Storage System immediately. Check the checkbox for New Installation.</p> <p>If the checkbox is unchecked, the service starts and Web Console gets ready to start immediately. (Default is unchecked)</p>

- When selecting [Manual]

Add System

Set values for the new System and click [Apply] to confirm.

System Selection: ☐ Auto Discovery ☒ **Manual**

System Type:

Software Version:

Serial Number:
(6-digit Number)

IP Address (CTL1): ☒ IPv4 ☐ IPv6

IP Address (CTL2): ☒ IPv4 ☐ IPv6

System Name:
(Max, 180 characters)

Description:
(Max, 180 characters, or blank)

User Name:
(Max, 256 characters)

Password:
(Max, 256 characters)

☐ Not start service after addition immediately

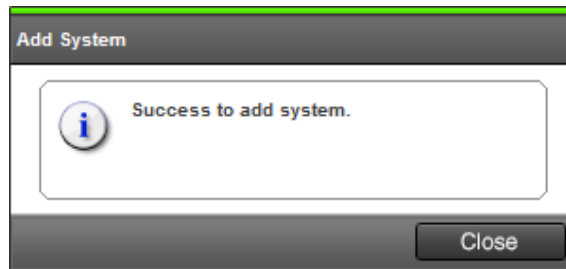
Item	Description
Software Selection	Click the [Browse...] button and select [Software\productname.inf] in the installation media for the Maintenance PC to acquire installation information.
System Selection	Select the input method of the Storage System information. <ul style="list-style-type: none"> • [Auto Discovery] (default selection): Acquire the Storage System information automatically. • [Manual]: Set each of the displayed items, [System Type], [Software Version] and [Serial Number].
System Selection - System Type	Select a Storage System type. [VSP G900 and VSP F900] [VSP G700 and VSP F700] [VSP G370 and VSP F370] [VSP G350 and VSP F350] [VSP G130]

(To be continued)

(Continued from preceding page)

Item	Description						
System Selection - Software Version	<p>Select the Software version, which is supported by the selected System Type in the setup media. The Config version is in parentheses of the Software version.</p> <p>A phrase to identify whether the software is designed for use in Japan or for global use is displayed at the end of the software version.</p> <p><Example></p> <p>xx-xx-xx-xx/xx(xx-xx-xx/60) for Japan domestic</p> <p>xx-xx-xx-xx/xx(xx-xx-xx/00) for global</p> <p>• Notes:</p> <p>When a Config version model is 60, “for Japan domestic” is displayed; when a Config version model is 00, “for global” is displayed.</p> <p>Select the corresponding model of the Config version (last two digits after “/”) from the following models depending on the model name of the Storage System.</p> <table border="1"> <thead> <tr> <th>Model name of the Storage System</th><th>Model of Config version to be selected</th></tr> </thead> <tbody> <tr> <td>HT-40SE, HT-40SF, HT-40SG</td><td>60</td></tr> <tr> <td>DW850</td><td>00</td></tr> </tbody> </table>	Model name of the Storage System	Model of Config version to be selected	HT-40SE, HT-40SF, HT-40SG	60	DW850	00
Model name of the Storage System	Model of Config version to be selected						
HT-40SE, HT-40SF, HT-40SG	60						
DW850	00						
System Selection - Serial Number	Enter the serial number. The serial number consists of a six digit number beginning with “4”. Only numbers are usable.						
IP Address (CTL1)	Enter the CTL1 IP address. Select IPv4 (Default) or IPv6, and then enter the IP address.						
IP Address (CTL2)	Enter the CTL2 IP address. Select IPv4 (Default) or IPv6, and then enter the IP address.						
System Name	<p>Set the display name of the storage system.</p> <p>The number of characters you can enter up to 180.</p> <p>Allowed characters are one-byte alphanumeric characters, symbols (# \$ % & ' * + - . / = ? @ ^ _ ` { } ~).</p> <p>You cannot use one-byte spaces.</p>						
Description	<p>Enter the description of the Storage System.</p> <p>The number of characters you can enter is zero to 180.</p>						
User Name	Enter the user name and password for the maintenance account of the storage system.						
Password	A password for the maintenance account of the storage system is changed by your customer after the storage system is installed. Ask your customer to let you know the password.						
Not start service after addition immediately	<p>Select whether to connect the registered Storage System immediately.</p> <p>If the checkbox is unchecked, the service starts and Web Console gets ready to start immediately. (Default is unchecked)</p>						

- (3) The confirmation message is displayed. Click the [Close] button.



- (4) A Storage System icon is added.



Table 2-2 Icon Display Item

Item	Displayed Description
Storage System Display Name	Display a display name of the Storage System.
Login user name	Display a login user name.
Storage System type	Display a model type of the Storage System.
Storage System serial number	Display the Storage System serial number.
CTL1 IP address	Display the set CTL1 IP address.
CTL2 IP address	Display the set CTL2 IP address.
Software version	Display the applied Software version.
Config version	Display the applied Config version.
Service start	Display whether the service starts automatically when starting the Maintenance PC.
Description	Display the descriptive text entered by a user.

4. Eject media

I will remove the media from the DVD drive.

2.5 Starting Web Console

NOTICE: After the storage system is registered, if the IP Address of the Maintenance PC is changed, click [MPC IP Address] on the top right of the Storage Device List window. Then, in the “Change MPC IP Address” window, set the IP address of the Maintenance PC. After that, ensure that the IP address is correctly set, and then click the [Apply] button to complete the address setting.

When two or more storage systems are registered, you can start Web Console of only one storage system whose service is running.

1. Click the [Start Service] button of the Storage System icon.

NOTE: When Starting Service is [Auto], the service starts automatically after starting the Maintenance PC. Go to [Step 4](#).

NOTE: If the “Web Console” window does not open, see “[2.9 Troubleshooting of Storage Device List](#)” and “[2.10 Troubleshooting of Web Console](#)”. If the solution cannot be found in these sections, contact the Technical Support Division.



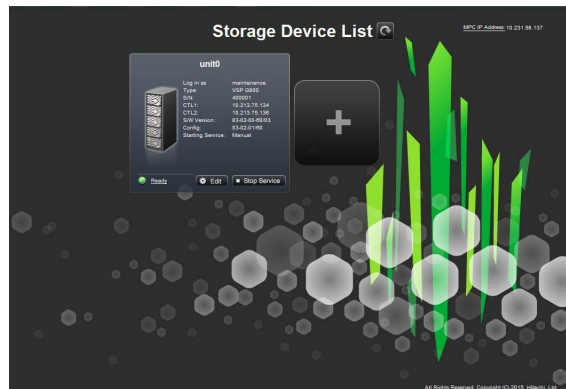
2. The message “Start the service. Is it OK?” is displayed. Click the [Confirm] button.

3. The message “The service started” is displayed. Click the [Close] button.

4. Click the refresh button beside the title of “Storage Device List” and update the Storage System icon to the enable operation status.
 - 10 to 20 minutes is needed for changing the Storage System icon to the enable operation status.
 - If the Storage System icon is not changed to the enable operation status after 10 minutes, refer to TROUBLESHOOTING SECTION [“3.29 MPC Failure Recovery”](#) and [“3.28.1.5 Background Service Log”](#).

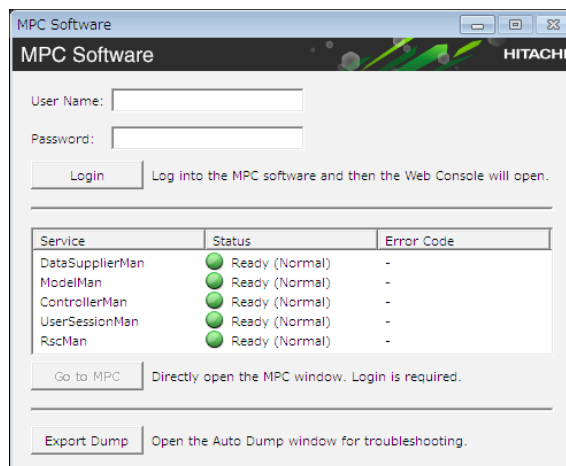


5. Click the Storage System icon.



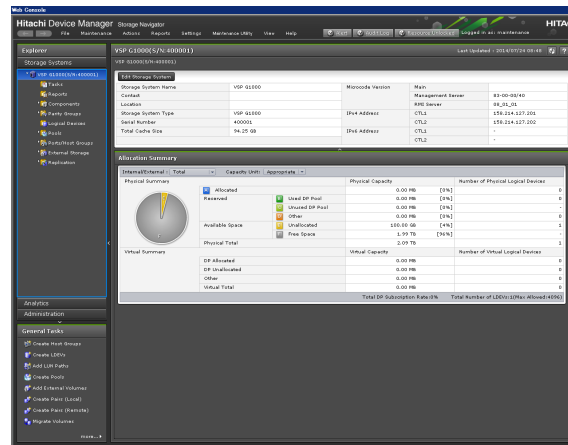
6. "MPC Software" is displayed and the service status is checked automatically.
Enter a user name and password for the maintenance account of the storage system, and then click the [Login] button. A password for the maintenance account of the storage system is changed by your customer after the storage system is installed. Ask your customer to let you know the password.
When all become [Ready (Normal)], go to [Step 7](#).

NOTE: If not logged in, the "Web Console" window is not displayed. The [Login] button becomes inactive after logging in.



7. Web Console starts.

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



2.6 Starting the MPC Window

A window for service personnel work is called an “MPC” window and only accessed by Maintenance PC.

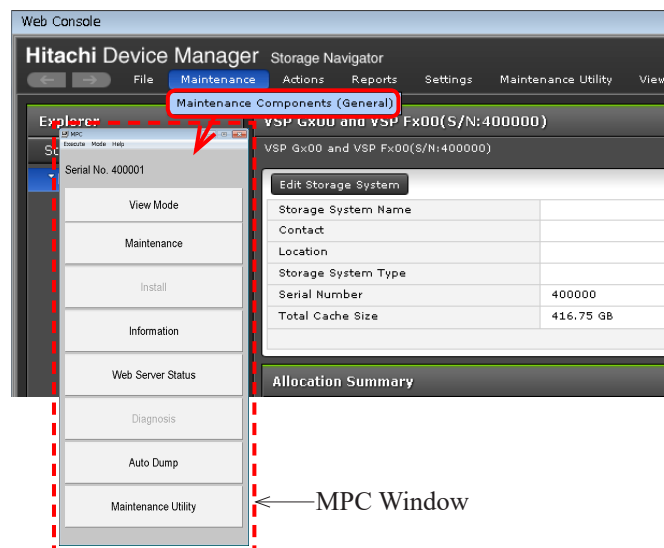
2.6.1 Starting the MPC Window from Web Console

NOTICE: If the installed Java version is Java 1.7.0_55 or later, or Java 1.8.0_5 or later, and than "Application Blocked by Java Security" window or "Application Blocked by Security Settings" is displayed, you cannot use the Web Console.
The above Java versions are installed on your machine, see [“1.3.5 Setting Java Security”](#) to register the Storage System to Java exception site.

NOTE: When the “Web Console” window is not running, refer to [“2.6.2 Starting the MPC Window from the MPC Software Window”](#).

NOTE: If the “MPC” window does not open, see [“2.10 Troubleshooting of Web Console”](#). If the solution cannot be found in this section, contact the Technical Support Division.

Select [Maintenance Components (General)] from the tool bar [Maintenance] in the “Web Console” window.

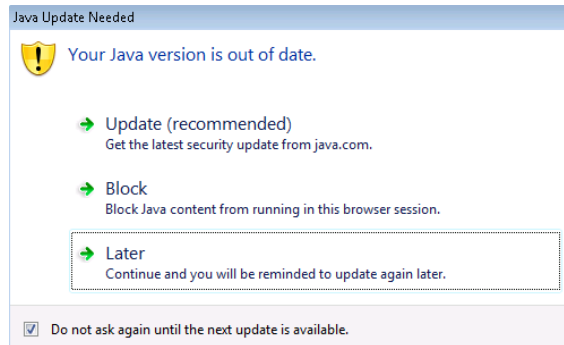


To close the MPC window, change the mode to [View Mode], and from the tool bar, select [Execute]-[Exit].

(1) Java start

The displayed windows differ according to the JRE (Java Runtime Environment) versions.

(a) The update of the Java application may be promoted.



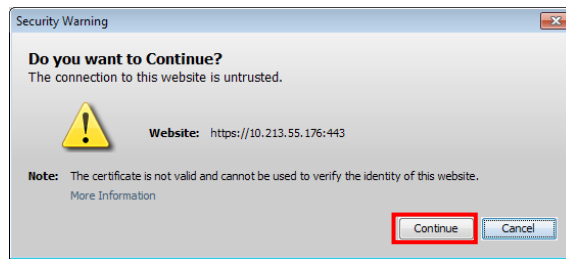
When starting the “MPC” window with the Java you are using, click [Later]. If you check the checkbox of [Do not ask again until the next update is available.] once and click [Later], this window is not displayed from now on. When clicking [Update(recommended)] or [Block], restart the “Web Console” window. When checking the checkbox of [Do not ask again until the next update is available.] and selecting [Update(recommended)] or [Block], the MPC window cannot be opened. To open the MPC window, execute the following procedures.

- (i) Click [All Programs]-[Java]-[Configure Java] from the [Start] menu of Windows and start [Java Control Panel].
- (ii) Click the [Security] tab of [Java Control Panel].
- (iii) If the checkbox of [Enable Java content in the browser] in the [Security] tab is checked, uncheck it once and click the [Apply] button.
- (iv) Check the checkbox of [Enable Java content in the browser] and click the [Apply] button.
- (v) Click the [OK] button of [Java Control Panel] to close the window.
- (vi) Restart the “Web Console” window.

NOTE: When changing the Java setting in [Java Control Panel], a message like “Java Plugin settings changed” may be displayed. If such message is displayed, click the [OK] button.

- (b) When the message “Do you want to Continue?” is displayed, click the [Continue] button.

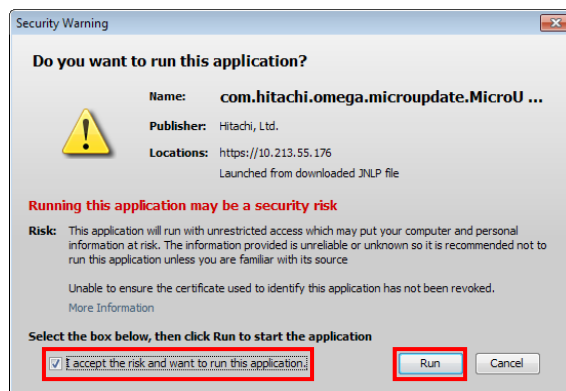
NOTE: This window may not be displayed.



NOTE: If you press the [Cancel] button in the window, the “MPC” window cannot be opened. From the tool bar of the Web Console window, select [Maintenance]-[Maintenance Components (General)] again.

- (c) When the message “Do you want to run this application?” is displayed, check [I accept the risk and want to run this application.] and click the [Run] button.

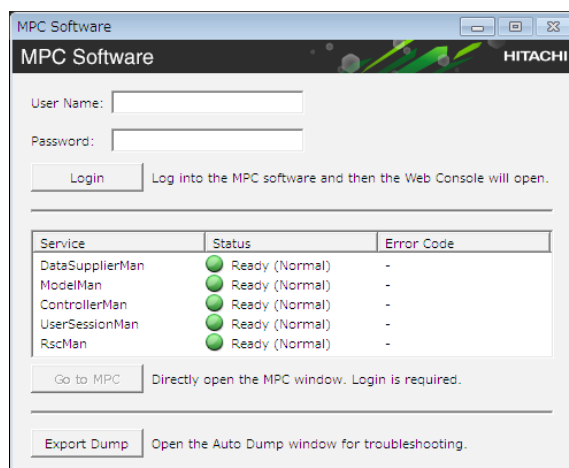
NOTE: This window may not be displayed.



NOTE: If you press the [Cancel] button in the window, the “MPC” window cannot be opened. From the tool bar of the Web Console window, select [Maintenance]-[Maintenance Components (General)] again.

2.6.2 Starting the MPC Window from the MPC Software Window

When the “Web Console” window is not running, start the “MPC” window from the “MPC Software” window.



1. Login

In the “MPC Software” window, enter the user name and password for the maintenance account of the storage system, and then click the [Login] button. A password for the maintenance account of the storage system is changed by your customer after the storage system is installed. Ask your customer to let you know the password.

- NOTE:
- Once logged in, the [Open MPC Window] button is activated.
 - If you cannot login, refer to the event log of the Maintenance PC/SVP and check that the communication with the CTL is established.
After checking that the communication with the CTL is established, click the [Login] button again.
(Refer to TROUBLESHOOTING SECTION [“3.30 Event log of MPC/SVP”](#) for how to check the event log of the Maintenance PC/SVP.)
 - If the communication with the CTL is not established even after waiting for a while (about three minutes), gather dump from the [Export Dumps] button.
Clicking the [Export Dump] button displays the “Select Dump Type” window. Refer to [“5.2 Dump”](#).
You cannot gather the DKC Memory dump and the GUM trace when the communication is not established.

NOTICE: If the installed Java version is Java 1.7.0_55 or later, or Java 1.8.0_5 or later, and than "Application Blocked by Java Security" window or "Application Blocked by Security Settings" is displayed, you cannot use the Web Console.
The above Java versions are installed on your machine, see [“1.3.5 Setting Java Security”](#) to register the Storage System to Java exception site.


2. Displaying the “MPC” window

Click the [Open MPC Window] button in the “MPC Software” window.

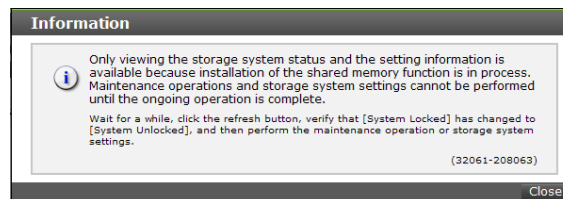
2.7 Starting the Maintenance Utility Window

A maintenance function window accessed by service personnel and users is called Maintenance Utility.

NOTICE: When running the maintenance operation in the other window, the part status might be displayed differently from the actual status. (Example: The Shared Memory function status before completing the addition is displayed as the status after the addition.).

In that case, complete the maintenance operation running in the other window, and then refresh the display information by clicking the [Refresh] button ().

While running the maintenance operation or the maintenance processing, the messages like the following examples are displayed when logging into Maintenance Utility or refreshing the window.

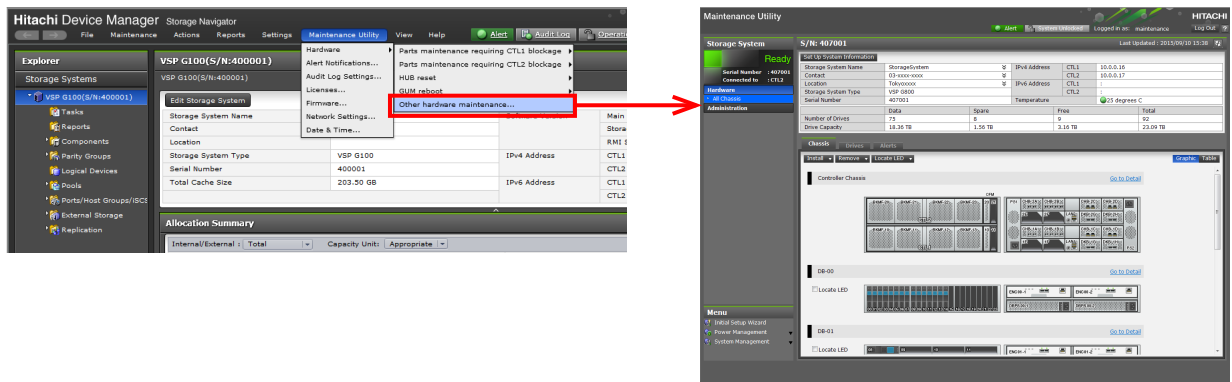


NOTICE: In the Maintenance Utility window, do not use the menus of the Web browser. If you use the browser menu ([Back], [Forward]) or shortcut keys and function keys, you are logged out of Maintenance Utility forcibly and the settings that are operated in the window are discarded. To use Maintenance Utility again, close the Web browser window, and then start Maintenance Utility again.

NOTE: If the “Maintenance Utility” window does not open, see [“2.11 Troubleshooting of Maintenance Utility”](#). If the solution cannot be found in this section, contact the Technical Support Division.

2.7.1 Starting the Maintenance Utility window from the Web Console window

Selecting a menu from the toolbar [Maintenance Utility]-[Hardware]-[Other hardware maintenance...] in the “Web Console” window displays the “Maintenance Utility” window.



NOTE: The following message might be displayed at the time of starting Maintenance Utility. This can be displayed due to monitoring by the security software or antivirus software installed on the PC.

When the message is displayed, click the [Add] button to release the monitoring.

* The window actually displayed might be different from the one below.



2.7.2 Starting the Maintenance Utility Window from the MPC Window

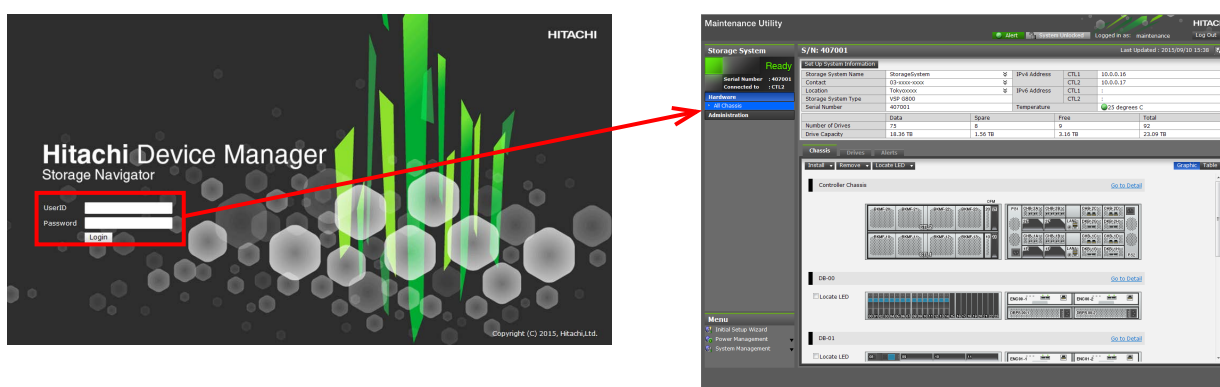
Click the [Maintenance Utility] button in the “MPC” window.

NOTE: When the “MPC” window is not running, see [“2.6 Starting the MPC Window”](#) and [“2.6.2 Starting the MPC Window from the MPC Software Window”](#).

2.7.3 Starting the Maintenance Utility Window by Specifying IP Address of CTL

Enter an IP address of CTL1 or CTL2 directly in the address bar of the browser.

Then, the login window opens. Enter the user name and password for the maintenance account of the storage system, and then click the [Login] button. A password for the maintenance account of the storage system is changed by your customer after the storage system is installed. Ask your customer to let you know the password.



The operations of Maintenance Utility started by specifying an IP address of CTL are restricted unlike Maintenance Utility started from the Web Console window or the MPC window. For details, see [“11.8 Restrictions on Operations of Maintenance Utility Started by Specifying IP Address of CTL”](#).

You can also choose the startup window by specifying an IP address of CTL with a parameter. For details, see the following table.

Connection LAN port	Startup window	Path to specify
Maintenance port	Maintenance Utility	http(s)://<CTLx IP address>/ http(s)://<CTLx IP address>/MaintenanceUtility
	Hitachi Storage Advisor Embedded	http(s)://<CTLx IP address>/StorageAdvisorEmbedded
Management port	Hitachi Storage Advisor Embedded	http(s)://<CTLx IP address>/ http(s)://<CTLx IP address>/StorageAdvisorEmbedded
	Maintenance Utility	http(s)://<CTLx IP address>/MaintenanceUtility

2.7.4 Closing the Maintenance Utility Window

1. When the work is completed, click the [Logout] button.



2. The login window or the logout completion window is displayed. Click the [X] button to close the window.

NOTE: When the Web Console window or the MPC window starts, not the login window but the logout completion window is displayed.

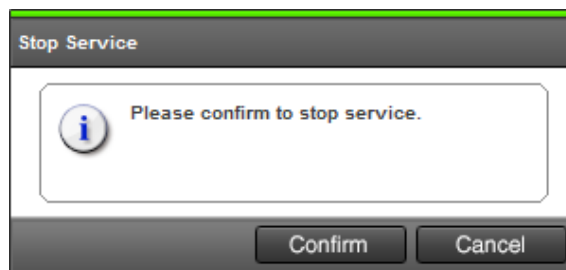
2.8 Maintenance PC Operation after Maintenance Work

2.8.1 Stopping Web Console

1. Click the [Stop Service] button of the Storage System icon which is running Web Console.



2. The confirmation message is displayed. Click the [Confirm] button.

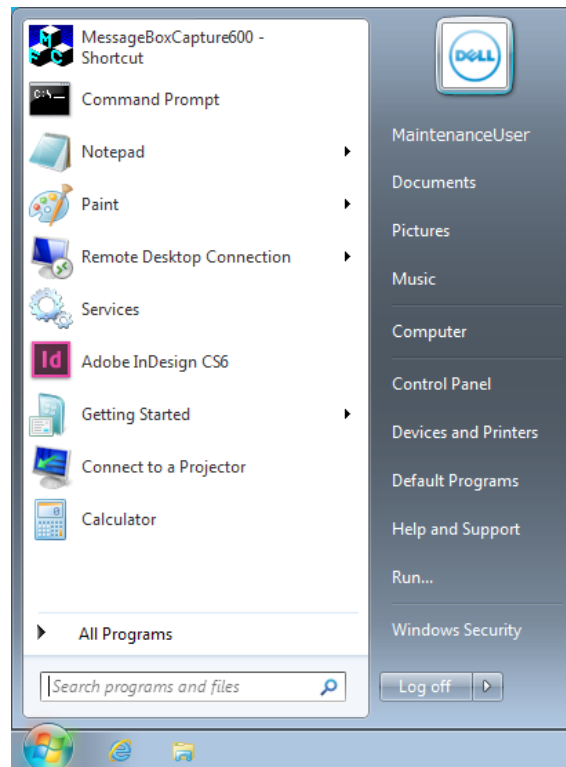


Web Console is automatically stop.

2.8.2 Shutting down the Maintenance PC

Close all the open windows.

Click the [Windows] button and then [Shut Down].



NOTE: When you power OFF the Maintenance PC in Windows 8.1 or Windows 10, open a command prompt, and execute the following command: `shutdown /s /f /t 0`
If you power OFF the Maintenance PC by other methods, the system of Maintenance PC may not start normally on the next time you power ON the Maintenance PC.
If you power OFF the Maintenance PC by methods other than executing the command, please reboot the Maintenance PC after the Maintenance PC has been booted.

If you configure the following setting, you can power OFF the Maintenance PC by methods other than executing the command. And you can start Storage Navigator normally on the next time you power ON the Maintenance PC.

- Control panel > [System and Security] > [Power Option]
 - > [Require a password on wakeup] or [Choose what the power buttons do]
 - > [System Settings]
 - > [Change settings that are currently unavailable]
 - > [Shutdown settings]
 - > Clear the check box of [Turn on fast startup (recommended)]
 - > [Save changes]

#This setting may be restored in Windows Update and all.

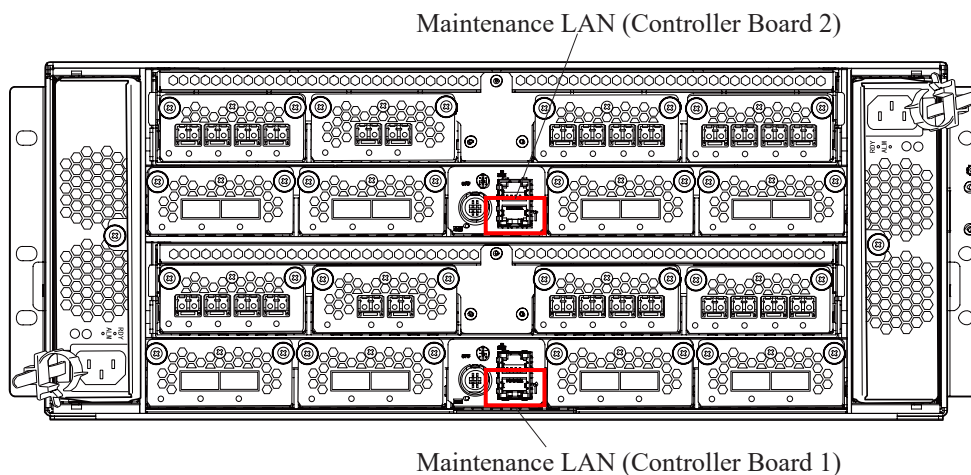
In the case of Windows except the above, you can use all methods to power OFF the Maintenance PC.

2.8.3 Disconnecting the Maintenance PC from the Storage System

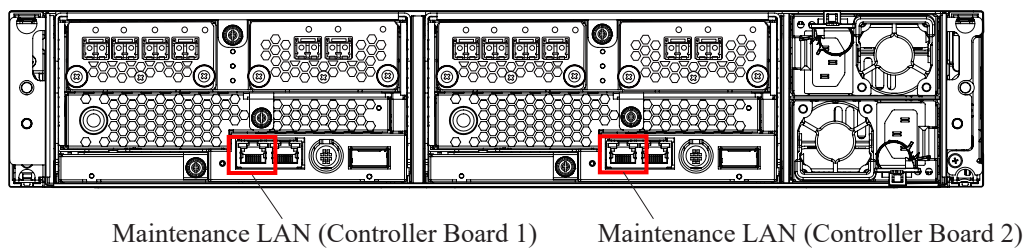
1. Power off the Maintenance PC.
2. Disconnect the power cable from the 100V AC outlet prepared by customers.
3. Disconnect the LAN cable from the maintenance LAN port at the CTL. (Refer to [Figure 2-3.](#))
4. Disconnect the power cable and LAN cable from the Maintenance PC.

Figure 2-3 Location of Maintenance LAN Port

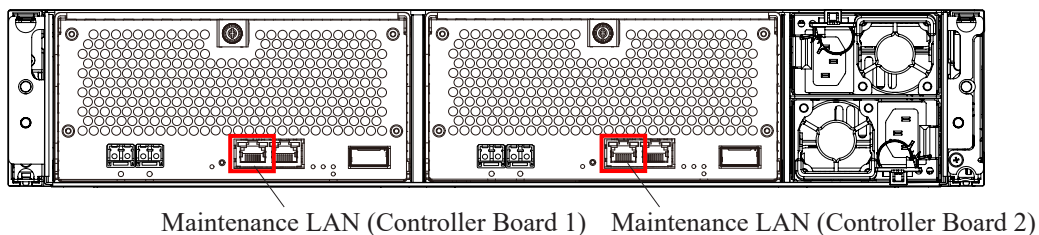
• CBLH (Rear view)



• CBSS/CBSL (Rear view)



• CBXSS/CBXSL (Rear view)



2.9 Troubleshooting of Storage Device List

No	Failure	Recovery action
1.	When [Apply] button clicked on the Add System dialog, the (21041 007006 or 21041 007008) error occurred and the icon is not created.	Failed to connect to the system when getting the system information. Please retry after confirming that enter the correct IP address, set the network between the Maintenance PC and the system, or the system is online. If add the system, that does not connect the Maintenance PC, select "Manual" and fill additional field.
2.	When [Apply] button clicked on the Add System dialog, the (21542 005019) error occurred and the icon is not created.	Free space of the storage device of the Maintenance PC is insufficient for creating service. Please create 200G or more of free space of the storage device which installed the supervisor.
3.	When [Start Service] button clicked, the (21542 005019) error occurred and the service cannot be started.	Two or more services cannot be executed simultaneously. Please stop the service started, before start the other service.
4.	When [Start Service] button clicked, the (21542 005026) error occurred and the service cannot be started.	The Maintenance PC IP Address is invalid. Please click the text of [MPC IP Address] on the top right of the screen of Storage Device List, and set the IP Address of Maintenance PC on the "Change MPC IP Address" window. And retry [Start Service] button again. After that, ensure that the IP address is correctly set, and then click the [Apply] button to complete the address setting.
5.	The status of the service changed to [Error] after reboot MPC with the service which [Starting Service] is settle as "Auto". When click status, "Error(21542 005026)" of "Status" of "BASE" is shown on the Service Status dialog.	The Maintenance PC IP Address is invalid. Please click the text of [MPC IP Address] on the top right of the screen of Storage Device List, and set the IP Address of Maintenance PC on the [Change MPC IP Address] dialog. And retry [Start Service] button again. After that, ensure that the IP address is correctly set, and then click the [Apply] button to complete the address setting.

(To be continued)

(Continued from preceding page)

No	Failure	Recovery action												
6.	<p>After starting Web Console, the following window is displayed and you cannot log in.</p> <div><p>Please wait... Storage Navigator is loading.</p><table><tr><td><Service></td><td><Status></td></tr><tr><td>DataSupplierMan</td><td>Starting</td></tr><tr><td>ModelMan</td><td>Starting</td></tr><tr><td>ControllerMan</td><td>Starting</td></tr><tr><td>UserSessionMan</td><td>Ready (Normal)</td></tr><tr><td>RscMan</td><td>Starting</td></tr></table><p>Storage Navigator start-up may take up to 30 minutes. If services do not become Ready (Normal) after 30 minutes, there may be a problem in the network connection between the SVP and the storage system. Please verify that:</p><ul style="list-style-type: none">- The environment allows accesses from the SVP to the IP address of the storage system specified at storage system registration.- The user name or password of the storage system specified at storage system registration is correct, and- GUM of the storage system specified at system registration is not rebooting.</div>	<Service>	<Status>	DataSupplierMan	Starting	ModelMan	Starting	ControllerMan	Starting	UserSessionMan	Ready (Normal)	RscMan	Starting	<p>Two or more Maintenance PCs might be connected. One Storage system can connect with one Maintenance PC at a time. If other Maintenance PCs are connected, disconnect them.</p> <p>Then, restart the Maintenance PC that you use.</p> <p>If no other Maintenance PCs are connected, reboot GUM from Maintenance Utility.</p> <p>Reboot GUM in CTL1 and CTL2 one by one. (Refer to the “3.18 Reboot GUM” for the reboot method.)</p> <p>Then, restart the Maintenance PC that you use.</p> <p>NOTE: If you reboot GUM in both CTLs at a time, the communication with the Maintenance PC might disconnect or the SIM report might fail.</p>
<Service>	<Status>													
DataSupplierMan	Starting													
ModelMan	Starting													
ControllerMan	Starting													
UserSessionMan	Ready (Normal)													
RscMan	Starting													
7.	<p>When the Storage Device List is started, the (21041 006005) error occurred and the Storage Device List cannot be started.</p>	<p>Failed to connect to the Supervisor service (DKCMan/MAPPAppServer/MAPPWebServer).</p> <p>Check the state of background services of the storage management software and cope with the trouble (See TROUBLESHOOTING SECTION “3.28.1.5 Background Service Log”). If the trouble is not solved, perform the following:</p> <p>Please select [Controlle Panel]->[Administration tool]->[Services] on the Windows, and confirm the status of DKCMan, MAPPAppServer and MAPPWebServer is [Started]. And then it is restarting Storage Device List as an Administrator.</p> <p>In the case of that the status of of DKCMan, MAPPAppServer and MAPPWebServer is not [Started], right-click on the service and select [Start], or reboot the Maintenance PC after select [Properties] and [Startup Type] is settle as [Automatic].</p>												
8	<p>When clicking the Storage System icon, the (21041 006002) error occurs and the Web Console cannot be started.</p>	<p>The default browser is not set.</p> <p>Set the default browser on the setting screen of the browser which is installed on the Maintenance PC, and try again.</p>												

(To be continued)

(Continued from preceding page)

No	Failure	Recovery action
9	When clicking the Storage System icon, entering a username and password on the MPC Software window, and clicking the Login button, a message saying that the username and password are incorrect is displayed and you cannot log in.	<p>A customer might have changed the password. Check the password, enter a correct username and password, and try to log in again.</p> <p>If the trouble is not solved, the port number to be used for the MPC might be used by another application. See the background service log to check the operation status of each application. If there is a problem, solve the problem following the procedure described in TROUBLESHOOTING SECTION “3.28.1.5 Background Service Log”.</p> <p>If the trouble is not solved when no problem is found in the status of the application, check that the communication with CTL is established by seeing the event log of MPC/SVP. (Refer to TROUBLESHOOTING SECTION “3.30 Event log of MPC/SVP”.) After confirming that the communication with CTL is established, enter a correct username and password and try to log in again.</p>

2.10 Troubleshooting of Web Console

Refer to Troubleshooting of “System Administrator Guide”.

	Failure	Recovery action	Remarks
1	When starting the subscreen on Web Console, the (10 6027) error occurs.	A LAN cable may fall out. Please confirm the LAN cable. If the LAN cable falls out, connect it and reboot Maintenance PC.	(*1)
		The Apache version might not be supported by the Maintenance PC Software. After uninstalling Apache, see “ 1.4 Maintenance PC Software Initial Installation/Update Installation ” and perform the update installation.	
		Since the Web Console program different from the Firmware version may be started, you need to clear the cache of Java. Select [Start] – [Control Panel], open the control panel, start the control panel of Java, and clear the cache file.	
2	The wrong information is displayed on Maintenance PC regarding a product name, a vender name and a function name, etc.	Select [Start] – [Control Panel] on Web Console, and then restart Maintenance PC.	
3	The (20121 107024) error occurred on the main window of “Web Console” on Maintenance PC.	Please respond to the message, and exit the “Web Console” main window.	
4	After the (20121 107024) error occurs on the main window of “Web Console” on Maintenance PC, the (20121 107025) error is repeatedly displayed.	Please exit the “Web Console” main window by pressing [Alt] and [F4] key.	
5	The (20121 107096) error occurs repeatedly on the main window of “Web Console” on Maintenance PC.	Please exit the “Web Console” main window by pressing [Alt] and [F4] keys.	

*1: If the trouble is not solved in spite of it, collect a dump and restart the Maintenance PC. Refer to “[5.2 Dump](#)”.

(To be continued)

(Continued from preceding page)

	Failure	Recovery action	Remarks
6	An error (20020-108000) occurs on the “Web Console” window after a Java error dialog appears and the “MPC” window does not open when selecting [Maintenance Components (General)] from the tool bar [Maintenance] in the “Web Console” window on the Maintenance PC.	<p>If Java application error, "Unable to launch the application" has occurred before 20020-108000 error occurs, take the recovery actions described in item Step 14.</p> <p>The port number to be used for the MPC might be used by another application. See the background service log to check the operation status of each application. If there is a problem, solve the problem following the procedure described in TROUBLESHOOTING SECTION “3.28.1.5 Background Service Log”.</p> <p>If the trouble is not solved when no problem is found in the status of the application, clear the Java cache file in accordance with the following steps and then retry the operation.</p> <ol style="list-style-type: none"> 1. Select [Start] – [Control Panel] – [Java] to open the Java control panel. 2. On the [General] tab, click [Setting...] under the [Temporary Internet Files] section. 3. Click [Delete Files...]. 4. Check [Cached Application and Applets] , and then click [OK]. <p>When it is still unsolved, press the [F4] key while pressing the [ALT] key to terminate the “Web Console” window once. Then, click the [Go to MPC] button in the “MPC Software” window.</p>	

(To be continued)

(Continued from preceding page)

	Failure	Recovery action	Remarks
7	When secondary windows or maintenance windows is started, displayed dialog window “Application Blocked by Java Security” or “Application Blocked by Security Settings”	<p>It may be that an application signed with expired certificate.</p> <p>Do the exception setting with following steps.</p> <ol style="list-style-type: none"> 1. Select [Start] – [Control Panel] – [Java] to open the [Java Control Panel]. 2. Select [Edit Site List ...] from [Security] Tab. 3. Select [Add], enter the following Addresses in Exception Site List, and click [OK] button. <ul style="list-style-type: none"> - <http://localhost> - <https://localhost> - <http://127.0.0.1> - <https://127.0.0.1> - <http://(IP address of SVP)> - <https://(IP address of SVP)> - <http://(IP address of GUM of CTL1)> - <http://(IP address of GUM of CTL2)> - <https://(IP address of GUM of CTL1)> - <https://(IP address of GUM of CTL2)> <p>If [Security Warning - HTTP Location] was displayed, Click [Continue] button.</p> <ol style="list-style-type: none"> 4. If the installed Java version is Java 1.7.0_55 or later or Java 1.8.0_5 of later, perform the following setting, too. <ul style="list-style-type: none"> • From the [Advanced] tab, select [Do not check (not recommended)] for [Perform certificate revocation checks on]. 5. Close [Java Control Panel], and restart Internet Explorer. 	
8	The following error occurred during the operation in the “Web Console” window. • 00002-009000	<p>Other administrative clients might be setting Storage Navigator.</p> <p>Check that all the setting windows of Storage Navigator are closed, and then operate Web Console again.</p> <p>In the case other than the above, restart the Maintenance PC. After that, operate Web Console.</p>	
9	The system lock status is displayed as [Locked] and the resource group status as [Unlocked] in the “Operation Lock Property” window.	Restart the Maintenance PC. After that, operate Web Console.	

(To be continued)

(Continued from preceding page)

	Failure	Recovery action	Remarks
10	When secondary windows or “MPC” windows is started, the window saving the JNLP file was displayed.	Make it possible to store the encrypted pages in the following procedure. 1. Open [Tools] – [Internet Options] of Internet Explorer and select the [Advanced] tab. 2. Uncheck [Security] – [Do not save encrypted pages to disk] in [Settings] and select [OK] to close the window.	
11	Web Console is automatically closed while operating IPv6 address settings from Storage Navigator.	The resource group remains in lock status when this failure occurs. Open the “Release Lockout” window, and release the resource group. To release the resource group, stop other tasks. Other resource groups used are also released. For details, see the “Release Lockout” window in System Administrator Guide. In addition, update Flash Player to the version 13 or later. For the update procedure, see “Installing Adobe Flash Player” in System Administrator Guide.	
12	The (20020-108000) error occurs on the main window of “Web Console” on Maintenance PC.	When the “MPC” window is starting up and the “Web Console” window is activated, close the “MPC” window once. Then start the “MPC” window again by following the procedure in “2.6.1 Starting the MPC Window from Web Console” .	
13	An error occurred during the operation in the “Web Console” window. • 20121-107022	The locale of the Maintenance PC might be set to other than English (United States) or Japanese (Japan). A setting procedure of the locale is shown as follows (an example for Windows 7). 1. Open the “Region and Language” window of [Control Panel]. 2. Set [Format] of the [Formats] tab to [English (United States)] or [Japanese (Japan)] and click the [Apply] button. 3. Select the [Administrative] tab. 4. Click the [Copy settings ...] button. 5. Check [Welcome screen and system accounts] and click the [OK] button.	

(To be continued)

(Continued from preceding page)


	Failure	Recovery action	Remarks
14	<p>On the Web Console, the sub screen or the "MPC" window displays a Java application error "Unable to launch the application." and does not open.</p> <p>When clicking the [Details] button, "Could not load file/URL specified" is displayed.</p>	<p>If the "MPC" window does not open, perform the following procedure:</p> <p>In the "Web Console" window, press the [F4] key while pressing the [Alt] key to close the "Web Console" window once.</p> <p>Then, to open the "MPC" window, click the [Go to MPC] button in the "MPC Software" window, which opens automatically after closing the "Web Console" window.</p> <p>If the sub screen does not open, or if the "MPC" window does not open even after completing the above procedure, perform the following procedure:</p> <ol style="list-style-type: none"> 1. Open the Internet Explorer, and then open the [Internet Options]. 2. Click the [General] tab. 3. When the check box for [Delete browsing history on exit] is selected, click the [Delete] button, and then open the "Delete Browsing History" window. 4. When the check box for [Temporary internet files and website files] is selected, clear the check box, and then click the [Delete] button. 5. Click the [Advanced] tab. 6. When the browser is closed, if the check box for [Empty Temporary Internet Files folder when browser is closed] is selected, clear the check mark, and then click the [OK] button. 7. Close the browser. 8. Perform the operations again using the "Web Console". <p>NOTE: If the Maintenance PC is used for the maintenance work on AMS2000/HUS100 disk array system, the check box might be selected as mentioned above.</p> <p>To perform the maintenance work on AMS2000/HUS100 disk array system after changing the check box setting, restore the setting.</p>	

(To be continued)

(Continued from preceding page)

	Failure	Recovery action	Remarks
14		<p>If the failure still occurs, perform the following steps:</p> <ol style="list-style-type: none"> 1. Open the Internet Explorer, and then open the [Internet Options]. 2. Click [Settings] on the [General] tab, open [Website Data Settings] window, and then click the [Caches and databases] tab. 3. Clear the check mark for the [Allow website caches and databases], and then click the [OK] button. 4. Close the browser. 5. Repeat Steps 1 and 2, select the check box for [Allow website caches and databases], and then click the [OK] button to close the window. 6. Close the browser. 7. Perform the operations again using the "Web Console". 	
15	In the "Operation Lock Property" window, the system lock status is displayed as [Unlocked], but the message "Another user is working" is displayed and the operation involving system configuration changes fails.	<p>There might be an inconsistency in the system lock status due to a communication error between the storage system and the Maintenance PC and so on.</p> <ol style="list-style-type: none"> 1. Setting operations of Storage Navigator might be being performed on another management client. Make sure that all windows of Storage Navigator are closed, and then retry the operation. 2. If the problem is not solved, restart the Maintenance PC. <p>If the problem persists, perform "2.2.12 Recovery Procedure for the System Lock during a Setting Change" in TROUBLESHOOTING SECTION.</p>	

2.11 Troubleshooting of Maintenance Utility

Description	Failure	Recovery Action
Network failures Login failures	<ul style="list-style-type: none"> The network cannot connect to Maintenance Utility. The 32061-204002 error occurs while operating Maintenance Utility. The network cannot log into the Maintenance Utility. 	<p>Check that the LAN cable is not removed. If it is removed, connect the cable, and then restart the operation.</p> <p>If it cannot recover, perform the following.</p> <ol style="list-style-type: none"> When logging in, log out once and operate it again after closing the browser. If it cannot recovered yet, enter the IP address (*1) of CTL1/CTL2 in the address bar of the browser directly to log in to Maintenance Utility and check the status of the Storage System. If it cannot be recovered yet, see “3.41 Recovery Procedure when a GUM Failure Occurs (SIM = afflxx)” in the TROUBLESHOOTING SECTION to recover.
	<ul style="list-style-type: none"> The network cannot connect to Maintenance Utility when starting it on Web Console. 	<p>The following message might be displayed at the time of starting Maintenance Utility. This can be displayed due to monitoring by the security software or antivirus software installed on the PC. When the message is displayed, click the [Add] button to release the monitoring.</p> <p>* The window actually displayed might be different from the one below.</p> 
	<ul style="list-style-type: none"> Login for Maintenance Utility is not available even if 30 minutes elapse after the progress reaches 99%. 	<p>See TROUBLESHOOTING SECTION “3.41 Recovery Procedure when a GUM Failure Occurs (SIM = afflxx)” and restore the failure.</p>

(To be continued)


(Continued from preceding page)

Description	Failure	Recovery Action
Network failures Login failures	<ul style="list-style-type: none"> The network cannot connect to Maintenance Utility. The actual IP address and the IP address displayed in the Maintenance Utility window do not match. 	<p>If CTL1 and CTL2 are removed, and then inserted CTL1 into the slot for CTL2 and CTL2 into the slot for CTL1 when the power is off, the actual IP addresses and the IP addresses displayed in the Maintenance Utility window do not match.</p> <ol style="list-style-type: none"> Enter the IP address (*1) directly to the address bar in your browser: Enter the IP address of CTL1 for CTL2 or vice versa. When you can log into the Maintenance Utility, confirm that the system is in the READY state, and then click the Apply button in the Network Setting window to reflect the settings by following the procedure in “3.6 Network Setting”. If it cannot be recovered yet, see “3.41 Recovery Procedure when a GUM Failure Occurs (SIM = afflxx)” in the TROUBLESHOOTING SECTION to recover.
JavaScript security troubleshooting	<ul style="list-style-type: none"> The “Maintenance Utility” window opens, but it is still blank even after one minute or more elapse. An operational problem occurs in the window such as the input value of a text box is not reflected correctly. 	<p>Add Maintenance Utility to the reliable site in the following procedure and open Maintenance Utility again. Set the security level of the trusted sites to “Medium” or less.</p> <ol style="list-style-type: none"> Open [Tool] – [Internet Options] in the Internet Explorer and select the [Security] tab. Select [Reliable Site], and then select [Site (S)]. Uncheck [All Sites in This Zone Require Confirmation (https:) by Servers (S)]. Enter the IP address of CTL1 into [Add This Web Site to Zone (D)] and click [Add] and select [Close]. Add the IP address of CTL2 in the same way. When returning to the “Internet Option” window, select [OK] to close the window.
Compatibility display	<ul style="list-style-type: none"> Contents displayed in the “Maintenance Utility” window are corrupted. A specific window is not displayed. Clicking the button has no response. 	<p>Exclude Maintenance Utility from the compatibility display target. See “1.3.3.1 Setting the Browser Compatibility Display to OFF” for the setting method.</p>

*1: The IP address of CTL1/CTL2 is displayed by the icon of the “Storage Device List” window or the Storage System information of “Storage Navigator”.

(To be continued)

(Continued from preceding page)

Description	Failure	Recovery Action
Browser Cache clearing	<ul style="list-style-type: none"> • Login to Maintenance Utility fails. • The “Maintenance Utility” window opens, but it is still blank even after one minute or more elapse. 	Clear the browser Cache and open Maintenance Utility again.
Correspondence in case the status displays of device status and Maintenance Utility differ.	The status displays of device status and Maintenance Utility differ.	GUM is rebooted. Refer to the “ 3.18 Reboot GUM ” for the reboot method.
SmartScreen filter	Multiple same windows are displayed after clicking a button.	Turn off the SmartScreen filter function in the following procedure, and then open Maintenance Utility again. <ol style="list-style-type: none"> 1. Click the gear icon () in Internet Explorer, and then click [Safety] – [Disable SmartScreen Filter Function]. 2. Make sure that [turn off SmartScreen filter] is selected, and then click [OK] to close the window.
File download is impossible or File downloading is required	Clicking the [Refresh] button in the “Firmware” window displayed the error “XXX cannot be downloaded. You cannot open this Internet site. …”. Or the message about the preservation of the JNLP file is displayed.	Make it possible to store the encrypted pages in the following procedure. <ol style="list-style-type: none"> 1. Open [Tools] - [Internet Options] of Internet Explorer and select the [Advanced] tab. 2. Uncheck [Security] - [Do not save encrypted pages to disk] in [Settings] and select [OK] to close the window.

(To be continued)

(Continued from preceding page)

Description	Failure	Recovery Action
The screen of [Update] cannot start.	When secondary windows or Maintenance Utility windows is started, displayed dialog window “Application Blocked by Java Security” or “Application Blocked by Security Settings”	<p>It may be that an application signed with expired certificate. Do the exception setting with following steps.</p> <ol style="list-style-type: none"> 1. Select [Start] – [Control Panel] – [Java] to open the [Java Control Panel]. 2. Select [Edit Site List ...] from [Security] Tab. 3. Select [Add], enter the following Addresses in Exception Site List, and click [OK] button. <ul style="list-style-type: none"> - <http://(CTL1 address)> - <http://(CTL2 address)> - <https://(CTL1 address)> - <https://(CTL2 address)> - <http://(IP address of SVP)> - <https://(IP address of SVP)> <p>If [Security Warning - HTTP Location] was displayed, Click [Continue] button.</p> <ol style="list-style-type: none"> 4. If the installed Java version is Java 1.7.0_55 or later or Java 1.8.0_5 of later, perform the following setting, too. <ul style="list-style-type: none"> • From the [Advanced] tab, select [Do not check (not recommended)] for [Perform certificate revocation checks on]. 5. Close [Java Control Panel], and restart Internet Explorer.
	The “Update Firmware” window is not displayed after the Java logo appears and then disappears.	<p>Occurs when the total amount of free space of the Maintenance PC memory is less than 512 MB. Terminate unnecessary applications to create 512 MB or more free space (1 GB is recommended) in the memory.</p> <p>Open the Windows Task Manager and see “Commit” of “System” in the Performance tab to check the free space of the memory.</p>
	When the “Update” window is opened in Maintenance Utility, the message “Unable to launch the application.” is displayed.	<ol style="list-style-type: none"> (1) If the version of JRE (Client) on the Maintenance PC is JRE7, install JRE8 or later. (2) Check that the “Use TLSv1.2” setting for Java is enabled. If the “Use TLSv1.2” setting is disabled, perform the TLS settings as shown in the following procedure. <ol style="list-style-type: none"> 1. Click the Windows Start button and open [Control Panel]. 2. Click the [Java] icon. 3. In the “Java Control Panel” window, open the [Advanced] tab. 4. Click [Advanced Security Settings] to confirm that [Use TLS1.2] is checked, and then click [OK].
GUM internal failure	When logging into the Maintenance Utility, the storage system state was Ready but the hardware state was not displayed. The error message (60863-200030) was displayed.	<p>GUM is rebooted.</p> <p>See “3.18 Reboot GUM” for the reboot method.</p>

(To be continued)

(Continued from preceding page)

Description	Failure	Recovery Action
The download failed in the backup of the audit log export or the user account information.	<p>The following error occurs when backing up the audit log export or the user account information.</p> <ul style="list-style-type: none"> The error window "Maintenance Utility cannot be started." is displayed in the Web browser. 	<p>This phenomenon might occur when an unsupported browser is used.</p> <p>See "1.1 Requirements for the Maintenance PC" and use a browser of the supported version.</p>
The displayed description in the Maintenance Utility window is distorted.	<ul style="list-style-type: none"> A specific window is not displayed. Clicking the button has no response. 	<p>Exclude the Maintenance Utility window from the compatibility display target.</p> <p>In the Internet Explorer, check the [Compatibility View] on the address bar, and turn OFF the compatibility view.</p> <p>[Compatibility View] is not appeared (less than IE11):</p> <ol style="list-style-type: none"> Select [Tools] – [Compatibility View Settings]. Clear the "Display intranet sites in Compatibility View" and the "Display all websites in Compatibility View" check box. Click [Close] button.
Correspondence when the status of the Storage System with the Maintenance Utility is stuck at "Power-on in progress"	READY LED lights solid green and the status of the storage system with the Maintenance Utility is stuck at "Power-on in progress".	<ol style="list-style-type: none"> If the internal network is changed from the default value and also "5.2 Automatic Configuration Definition Mode (System Configuration Initialization)" in FIRMWARE SECTION has been performed, set the default value (10.251.0.15/4.15) referring to "3.6 Network Setting". If the conditions 1 are not satisfied, perform the following procedure. <ul style="list-style-type: none"> Connect to Maintenance Utility to check if a SIM is reported for the other CTL than the CTL whose status is stuck at "Power-on in progress". If no SIM is reported, perform the dummy replacement of the CTL whose status is stuck at "Power-on in progress". For the replacement procedure, see REPLACEMENT SECTION "2.4 Replacing a Controller Board". If a SIM is reported, follow the procedure according to the SIM.
The maintenance operation cannot be continued.	The system lock status is displayed as [Unlocked], but the message "The operation cannot be performed because another user is working on it ." is displayed and the maintenance operation cannot be continued.	<p>There might be an inconsistency in the system lock status due to a communication error between the storage system and the Maintenance PC and so on.</p> <ol style="list-style-type: none"> Setting operations of Storage Navigator might be being performed on another management client. Make sure that all windows of Storage Navigator are closed, and then retry the operation. If the problem is not solved, restart the Maintenance PC. If the problem persists, perform "2.2.12 Recovery Procedure for the System Lock during a Setting Change" in TROUBLESHOOTING SECTION.

2.12 Troubleshooting during Operation in Connection with External Server

External server	Failure	Recovery Action
HCS (Hitachi Command Suite) server	The login to the storage system from the HCS (Hitachi Command Suite) is failed.	When the password of the storage system is changed, the information registered on HCS also needs to be changed. Change the information following the procedure described in “Changing storage system information” in Hitachi Command Suite User Guide.

2.13 Incorrect display errors

The following table lists incorrect display errors:

Error condition	Probable cause / Recommended action
A question mark (?) displays in a table or other area of the window.	<ul style="list-style-type: none"> • When the question mark appears in the “View Tier Properties” window, see the topic describing this window in the Provisioning Guide for Open Systems. If the problem still persists, contact Hitachi Data Systems Support Center. • When the question mark appears in the “Add External Volumes” window, see the topic describing this window in the Hitachi Universal Volume Manager User Guide. If the problem still persists, contact Hitachi Data Systems Support Center. • If the question mark appears in another window, refresh the window. Contact Hitachi Data Systems Support Center if the question mark remains after you refresh the window.
The image is not displayed correctly.	<p>Log out. Then, press the [Ctrl] key and the [F5] key at the same time to read it again forcibly.</p> <p>After that, if the phenomenon is still not resolved even logged in again, contact the Technical Support Division.</p>
The window is stuck during the window operation.	<p>Check the network between the Maintenance PC and the Storage System. After that, log in again. When “System is locked” is displayed, refer to “3.17 Force Release System Lock” and release the locked status. If the phenomenon is not resolved, contact the Technical Support Division.</p>
The image display is unclear after completing the input setting in the window.	<p>The window becomes unclear when entering slashes sequentially. There is no problem if you use it as is.</p>
After changing the registered user account without stopping the services of the registered storage system, the “20122-208003” error occurred during the Storage Navigator operation.	<p>Perform Stop Service of the storage system in Storage Device List. After that, click Edit to register the enabled user account information again, and then perform Start Service.</p>

2.14 Operating Storage Systems to Be Maintained by Using Storage Device List

2.14.1 Checking Status of Storage System

The Storage System icon shows the status of the Storage System.

Table 2-3 Storage System Icon Type

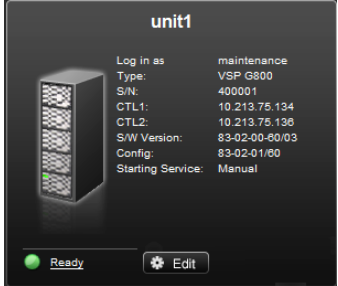
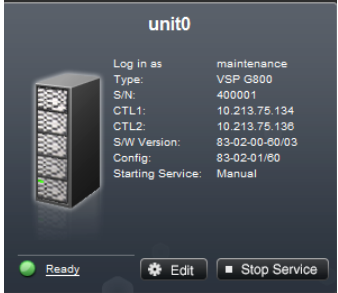

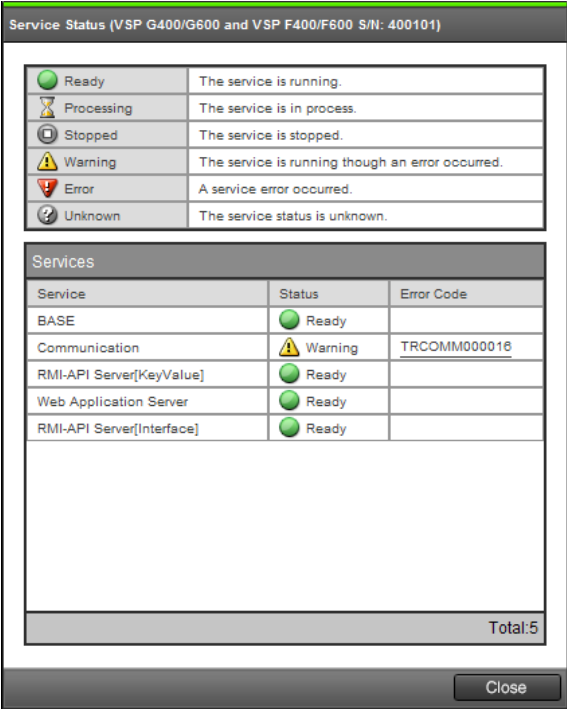
Status Name	Overview	Icon
Default	Display the Storage System information.	 <p>The icon for 'unit1' displays a server rack icon on the left. To the right, the following information is listed: Log in as: maintenance, Type: VSP G800, S/N: 400001, CTL1: 10.213.75.134, CTL2: 10.213.75.136, S/W Version: 83-02-00-60/03, Config: 83-02-01/60, Starting Service: Manual. At the bottom, there is a green 'Ready' indicator and an 'Edit' button.</p>
Operation enabled status	The operation button display is enabled. The mouseover changes the status.	 <p>The icon for 'unit0' displays a server rack icon on the left. To the right, the following information is listed: Log in as: maintenance, Type: VSP G800, S/N: 400001, CTL1: 10.213.75.134, CTL2: 10.213.75.136, S/W Version: 83-02-00-60/03, Config: 83-02-01/60, Starting Service: Manual. At the bottom, there is a green 'Ready' indicator, an 'Edit' button, and a 'Stop Service' button.</p>
Service stop status	The service is stopped.	 <p>The icon for 'StorageSystem' displays a server rack icon on the left. To the right, the following information is listed: Log in as: maintenance, Type: VSP G400/G600, S/N: 400001, CTL1: 127.0.0.1, CTL2: 127.0.0.2, S/W Version: 83-00-00-60/00, Config: 83-00-00/60, Starting Service: Manual. At the bottom, there is a red 'Stopped' indicator, an 'Edit' button, and a 'Start Service' button.</p>

Table 2-4 Operation Button

Item	Button	Description
Status icon	[Stopped]	“Service Status” window is displayed. Check the service list. (*1) Ready : The service is running. Processing : The service is in process. Warning : The service is running though an error occurred. Stopped : The service is stopped. Error : A service error occurred. Fatal Error : A service error occurred. Re-setup required. Unknown : The service status is unknown.
	[Ready]	
Edit button	[Edit]	“Edit System” window is displayed. Refer to “2.14.4 Changing Storage System Information and Updating Software of Web Console” .
Start service	[Start Service]	The service starts and the Storage System icon changes to the default display.
Stop Service	[Stop Service]	The service stops and the Storage System icon changes to the Service stop status display.

*1: Clicking the status button/status icon displays the service status dialog.
 Check the displayed status list and statuses. For details about the status list and statuses, see [MPC02-490](#).



Item	Description
A list of service statuses	Displays a list of statuses that each service module can take.
Services	Displays a list of statuses for each service module. Displays a status error code if the status is Warning or Error. When clicking Error Code, an error message is displayed. Follow its troubleshooting.

NOTE: If the error message instructs to see a manual, see TROUBLESHOOTING SECTION [“3.28.1.3 Storage Device List Troubleshooting”](#).

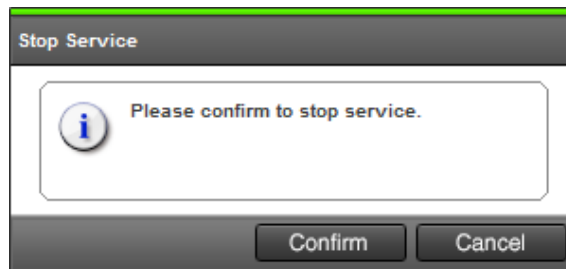
2.14.2 Stopping the Service of Storage System

The following shows the procedure for stopping the service of the Storage System.

1. Right-click the [Open Storage Device List] icon on the desktop of the Maintenance PC, select [Run as administrator] to start the Storage System, and then click the [Stop Service] button of the registered Storage System in the “Storage Device List” window.

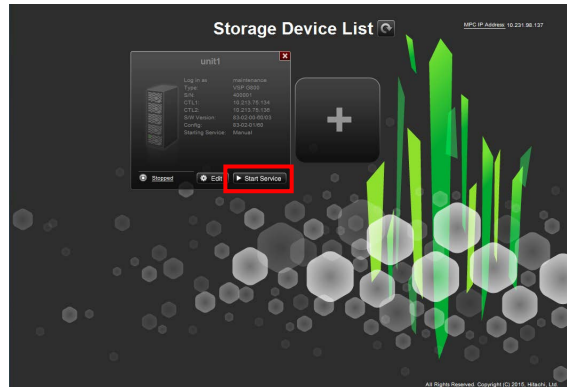


2. The confirmation message is displayed. Click the [Confirm] button.

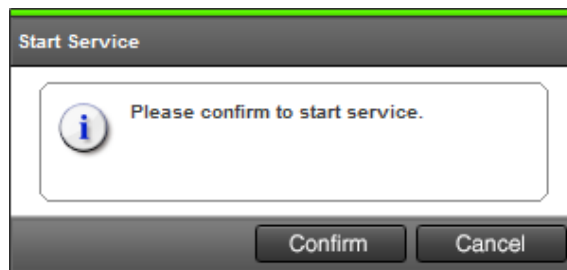


2.14.3 Starting the Service of Storage System

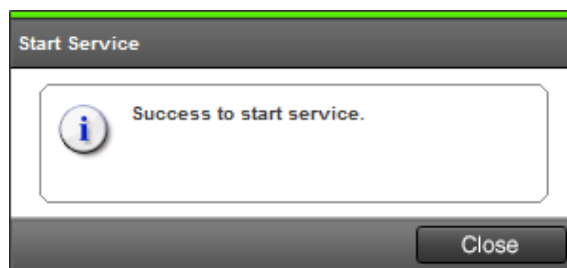
1. Click the [Start Service] button of the registered Storage System on the “Storage Device List” window.



2. The “Start Service” window is displayed. Click the [Confirm] button.



3. The “Starting Service Completed” window is displayed. Click the [Close] button.
The status of the registered Storage System in the “Storage Device List” window becomes “Ready”.



2.14.4 Changing Storage System Information and Updating Software of Web Console

NOTICE: Make sure to perform the update installation of the Maintenance PC Software in accordance with ["1.4 Maintenance PC Software Initial Installation/Update Installation"](#) before performing the following procedure.

NOTE: When updating the Web Console software, the installation media for the Maintenance PC is used. If both types of the storage systems, DW800 and DW850, are registered on one Maintenance PC, prepare the installation media that supports the storage systems on which the Web Console software update is performed.

For the procedure for updating the Web Console software of DW800, refer to the Maintenance Manual of DW800.

1. Stop the Storage System service by the storage device list (Refer to ["2.14.2 Stopping the Service of Storage System"](#)).
2. Click the [Edit] button of the registered Storage System on the storage device list.
3. Check the check box of [Software].
4. Specify "Software\productname.inf" in the setup media by the [Browse...] button of Software Selection in [Software].

5. Select System Selection: [Auto Discovery]/[Manual] in [Software] and click the [Apply] button.

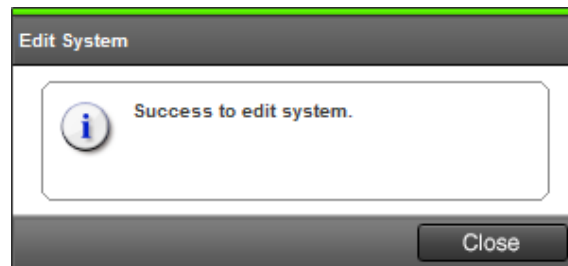
When selecting [Auto Discovery]

The 'Edit System' dialog box is shown with the 'Software' checkbox checked. Under 'Software Selection', there is a text field and a 'Browse...' button. The 'System Selection' section has two radio buttons: 'Auto Discovery' (selected) and 'Manual'. Below this, the 'Connect Information' section has two IP address fields (CTL1 and CTL2), each with 'IPv4' and 'IPv6' radio buttons. The 'System Information' section has a 'System Name' field (with 'unit0' entered) and a 'Description' field. The 'User Information' section has a 'User Name' field (with 'maintenance' entered) and a 'Password' field. At the bottom, there is a checkbox for 'Start service automatically, when the MPC is rebooted.' and 'Apply' and 'Cancel' buttons.

When selecting [Manual]

The 'Edit System' dialog box is shown with the 'Software' checkbox checked. Under 'Software Selection', there is a text field containing 'C:\Media(MApp)\software\productname.inf' and a 'Browse...' button. The 'System Selection' section has two radio buttons: 'Auto Discovery' and 'Manual' (selected). Below this, the 'System Type' field contains 'VSP G800' and the 'Software Version' field contains '83-02-00-00/03/83-02-01/00'. The 'Connect Information' section has two IP address fields (CTL1 and CTL2), each with 'IPv4' and 'IPv6' radio buttons. The 'System Information' section has a 'System Name' field (with 'unit0' entered) and a 'Description' field. The 'User Information' section has a 'User Name' field (with 'maintenance' entered) and a 'Password' field. At the bottom, there is a checkbox for 'Start service automatically, when the MPC is rebooted.' and 'Apply' and 'Cancel' buttons.

6. The confirmation message is displayed. Click the [Close] button.

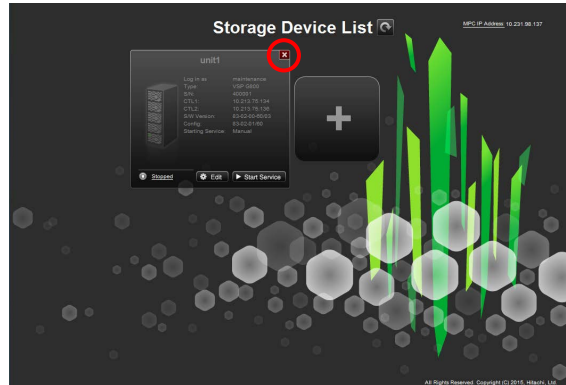


2.14.5 Deleting Registered Storage Systems

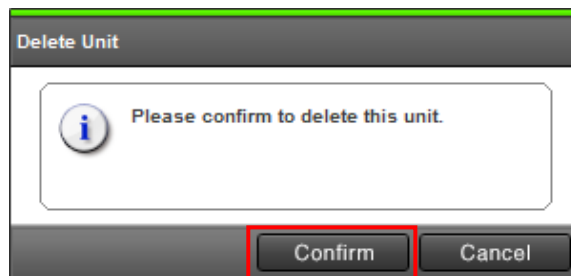
NOTICE: Before deleting the Storage System icon, close the Event Viewer of Windows.

Stop the service of a Storage System, and then perform the following procedure.

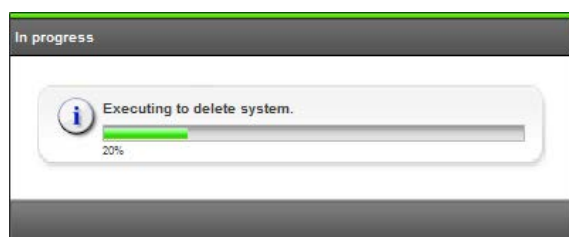
1. Click the [×] button in the upper right of the registered Storage System in the “Storage Device List” window.



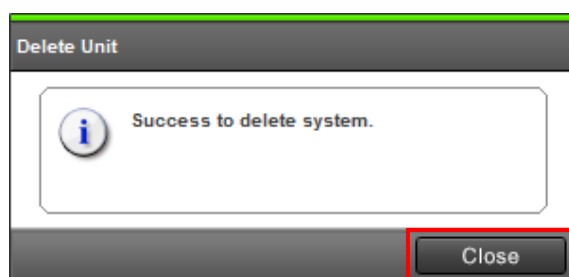
2. The “Delete Unit” window is displayed. Click the [Confirm] button.



3. The “In progress” window is displayed. Wait until the deletion is complete.



4. The confirmation message is displayed. Click the [Close] button.

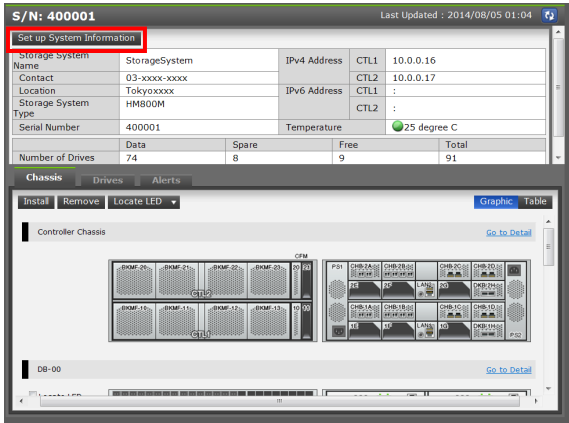


3. Storage System Maintenance Function

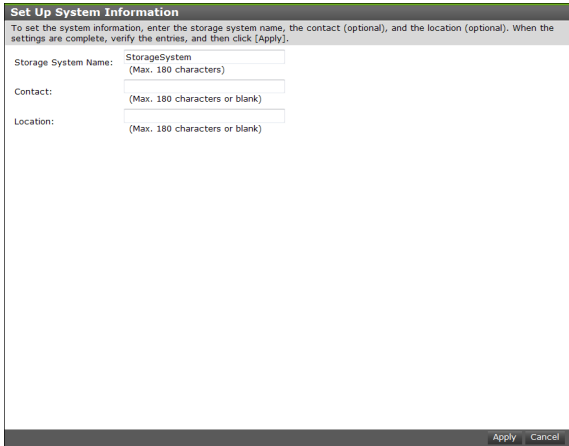
3.1 Network Setting [Start Separate Action]

This is a window to register the system information (system name/address/installation position). Such information is used when using the alert notice function by SNMP.

- 1. Start Maintenance Utility form the Maintenance PC.
- 2. Click the [Set Up System Information] button in the “Maintenance Utility” window.



- 3. The [Set Up System Information] window is displayed. Set up.



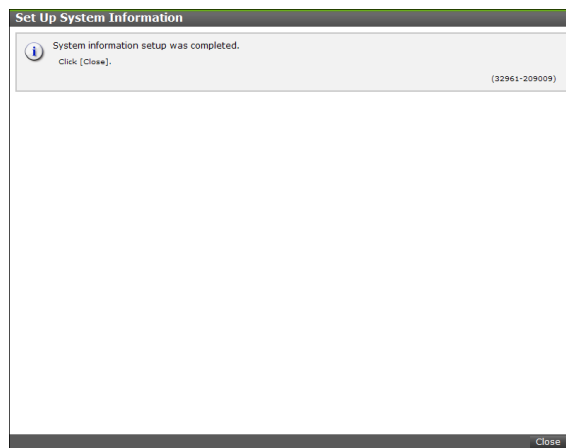
Item	Input Description
Storage System Name	Set a name of the Storage System. You can enter a maximum of 180 alphanumeric characters except for some symbols (\\, /, ;, *, ? " < > & % ^). Do not enter a blank for the first or last character. If you change this item, the Storage System name of [SNMP] Tab in the “Alert Notifications” window and the Storage System name in the “Storage System” window on Web Console are also changed.

(To be continued)

(Continued from preceding page)

Item	Input Description
Contact	Set an administrator and contact information. 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 of [SNMP] Tab in the “Alert Notifications” window and the contact in the “Storage System” window on Web Console are also changed.
Location	Set an installation location 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. If you change this item, the place of [SNMP] Tab in the “Alert Notifications” window and the place in the “Storage System” window on Web Console are also changed.

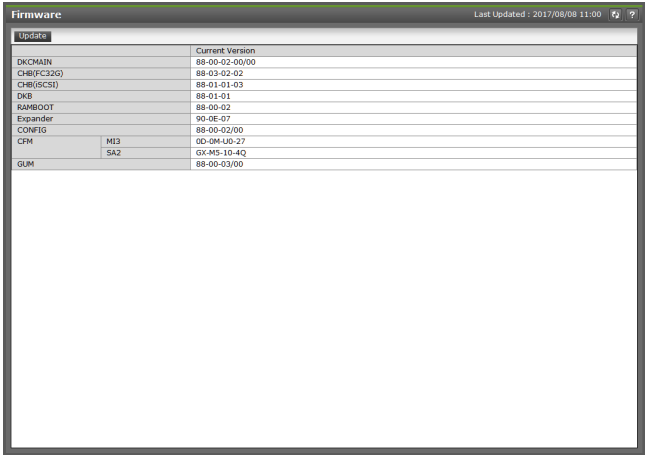
4. A completion message is displayed. Click the [Close] button.



3.2 Firmware

This is a window to display the currently installed firmware version and update various firmware of the Storage System.

- To display the installed firmware versions, select [Administration] - [Firmware] in the Maintenance Utility main window.



For the procedure of the online firmware update, see FIRMWARE SECTION [“3.3 Operating Procedure”](#).

3.3 User Administration

This window is displayed only when logged into Maintenance Utility by specifying the CTL IP address directly by the browser. Use Device Manager or Web Console usually.

To change the availability of using each operation window of Maintenance Utility, register the user in the user group which has an appropriate role (authority).

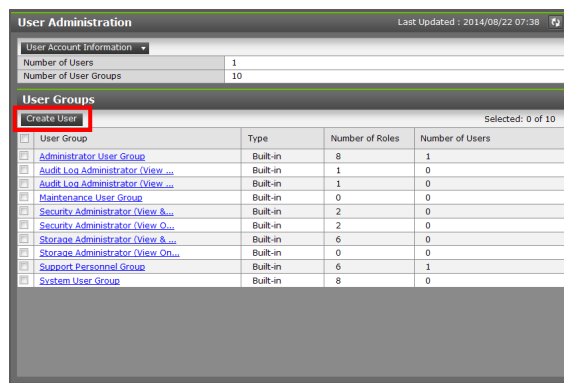
You can control the availability of using each operation window of Maintenance Utility in accordance with the role given to the user group. For the role required for each operation window, see [“3.3.6 Roles to be Required for the Operation Window of Maintenance Utility”](#).

NOTE: The Support Personnel group and Maintenance (vendor only) role contain the authorities for vendor maintenance. Do not grant the authorities to the accounts other than those used by vendor maintenance personnel.

3.3.1 Setting up User Account

How to create a user and register it in the user group is described. You can create up to 20 users including the built-in user.

1. In the “Maintenance Utility” window, select [Administration] - [User Administration].
2. Click the [Create User] button of the “User Groups” window.



3. Create a new user account. Specify the User name, Account Status, Authentication and User Group. Click the [Finish] button.

Item	Description
User Name	<p>Enter the user name to be created.</p> <p>You can use up to 256 one-byte alphanumeric characters and the following symbols.</p> <p>(! # \$ % & ' * + - . / = ? @ ^ _ ` { } ~)</p>
Account Status	<p>Select whether to enable or disable the account. If the account is disabled, you will not be able to log into Web Console.</p>
Authentication	<ul style="list-style-type: none"> Select [Local] to authenticate the user by Web Console only without using the authentication server. <p>[Local]: Does not use authentication server. Uses a dedicated password for Web Console.</p> <p>You can enter 6 to 256 one-byte alphanumeric characters and symbols for the password.</p> <p>The character length and valid characters for the password depend on management applications of storage systems. When creating a user who uses all management applications, set the password by following the conditions below.</p> <ul style="list-style-type: none"> - Password: 6 to 63 characters - Valid characters: One-byte alphanumeric characters and symbols (- , . : @ _) <ul style="list-style-type: none"> [External]: Uses authentication server. See “System Administrator Guide” for the details of the user management using the authentication server.
User Group	<p>Select a user group to which the user is made to belong.</p>

4. Confirm the settings. Click the [Apply] button.

Create User

Verify the settings, and then click [Apply].

Added User

User Name	maintenance
Account Status	Enable
Authentication	Local
Password	*****
Number of User Groups	1

Selected User Groups

User Group Name	Type	Number of Roles
Administrator User Group	Built-in	8

Total: 1


< Back

Apply

Cancel

5. A completion message is displayed. Click the [Close] button.

Create User



Create User was completed.
Click [Close].

(32461-209013)

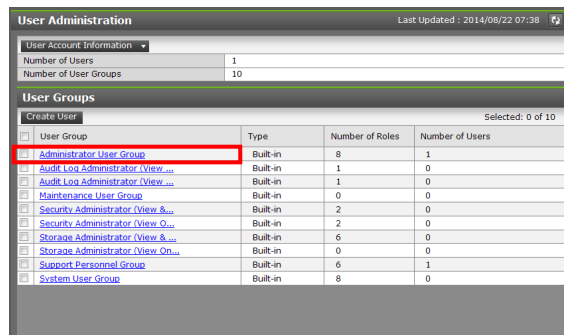
Close

3.3.2 Disabling User Accounts

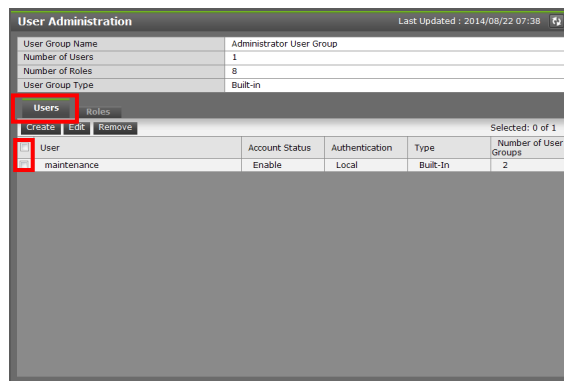
NOTICE:

- Log into an account that is different from the user whose account that you want to disable (you cannot disable the current login user account).
- To disable the user account specified by the registered storage system in the Storage Device List window, click Stop Service of the registered storage system. After disabling the user account, click Edit to set an enable user account. When the user account was disabled without performing Stop Service, Refer to [“2.13 Incorrect display errors”](#).

1. In the “Maintenance Utility” window, select [Administration] - [User Administration].
2. In the “User Groups” window, click the user group which the user belongs to.



3. Click the [Users] tab. Select the user that you want to disable.



4. Click the [Edit] button.

5. Select [Disable] from [Account Status] and click the [Finish] button.

Edit User

To update the user account information, edit the settings, and then click [Finish].

User Name: maintenance

Account Status: ☒ Enable ☐ Disable

Authentication: ☒ Local:

Current Password:

New Password:

Re-enter Password:

(6 - 256 characters)

☐ External:

User Groups

<input type="checkbox"/>	User Group Name	Type	Number of Roles
<input checked="" type="checkbox"/>	Administrator User Group	Built-in	8
<input type="checkbox"/>	Audit Log Administrator (View ...	Built-in	2
<input type="checkbox"/>	Audit Log Administrator (View ...	Built-in	2
<input type="checkbox"/>	Maintenance User Group	Built-in	2
<input type="checkbox"/>	Security Administrator (View &...	Built-in	3

Selected: 2 of 10

Finish

Cancel

6. Confirm the settings. Click the [Apply] button.

Edit User

Verify the edited settings, and then click [Apply].

Edited User

User Name	maintenance
Account Status	Disable
Authentication	Local
Password	
Number of User Groups	4

Selected User Groups

User Group Name	Type	Number of Roles
Administrator User Group	Built-in	16
Support Personnel	Built-in	16

Total: 4

< Back

Apply

Cancel

7. A completion message is displayed. Click the [Close] button.

Edit User

Edit User was completed.

Click [Close].

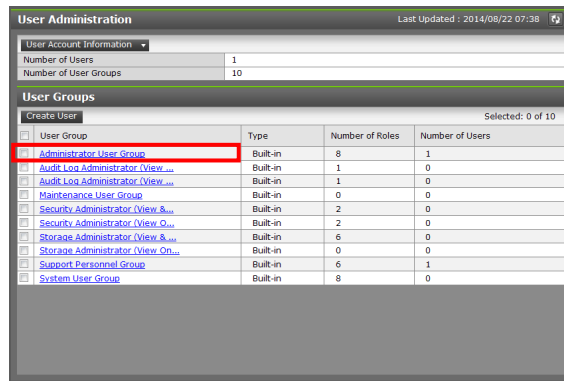
(32461-209015)

Close

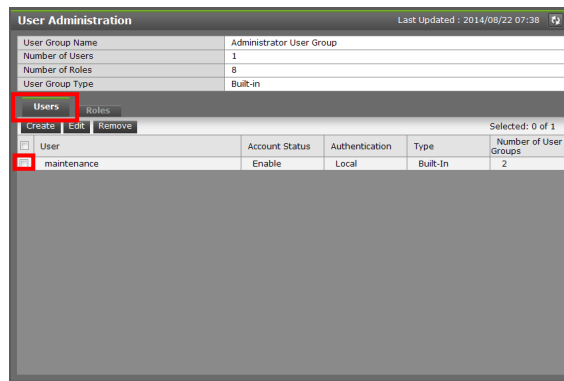
3.3.3 Changing User Account Authentication

How to change the user account authentication and the password is described.

1. In the “Maintenance Utility” window, select [Administration] - [User Administration].
2. In the “User Groups” window, click the user group which the user belongs to.



3. Click the [Users] tab. Select a user to be edited.



4. Click the [Edit] button.

5. Enter a change of [Local] and [External] of [Authentication] or a password.

NOTICE:

- When changing the password, enter a new password. If no password is entered, the current password is maintained.
- To change the user account specified by the registered storage system in the Storage Device List window, click Stop Service of the registered storage system. After changing the user account, click Edit to set the changed password. When the password was changed without performing Stop Service, Refer to [“2.13 Incorrect display errors”](#).

Edit User
To update the user account information, edit the settings, and then click [Finish].

User Name: maintenance

Account Status: ☒ Enable ☐ Disable

Authentication: ☒ Local: Current Password:
 New Password:
 (6 - 256 characters)
 Re-enter Password:

☐ External:

User Group Name	Type	Number of Roles
<input checked="" type="checkbox"/> Administrator User Group	Built-in	8
<input type="checkbox"/> Audit Log Administrator (View ...)	Built-in	2
<input type="checkbox"/> Audit Log Administrator (View ...)	Built-in	2
<input type="checkbox"/> Maintenance User Group	Built-in	2
<input type="checkbox"/> Security Administrator (View &...)	Built-in	3

Selected: 2 of 10

Finish Cancel

6. Confirm the settings. Click the [Apply] button.

Edit User
Verify the edited settings, and then click [Apply].

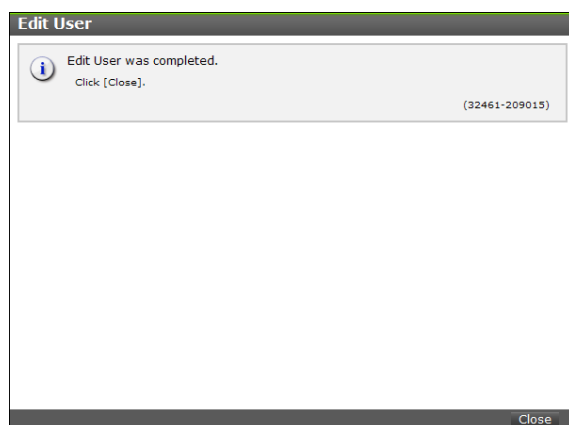
Edited User	
User Name	maintenance
Account Status	Disable
Authentication	Local
Password	
Number of User Groups	4

Selected User Groups		
User Group Name	Type	Number of Roles
Administrator User Group	Built-in	16
Support Personnel	Built-in	16

Total: 4

< Back Apply Cancel

7. A completion message is displayed. Click the [Close] button.

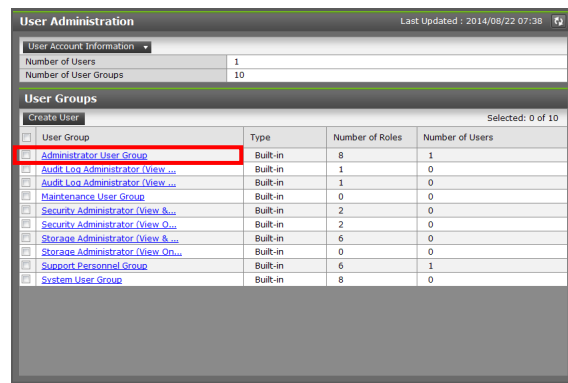


3.3.4 Removing User Accounts

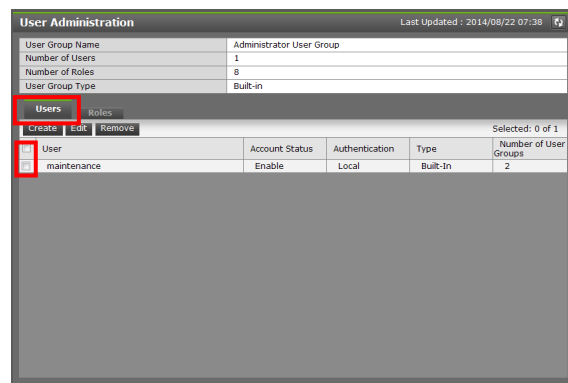
Security Administrators can remove a user account when the account is no longer in use. Built-in user accounts cannot be deleted. If deleting the current user account in If deleting the current login user account, you can continue the Web Console operation until you log out.

NOTICE: To delete the user account specified by the registered storage system in the Storage Device List window, click Stop Service of the registered storage system. After deletion, click Edit to set an enabled user account. When the user account was disabled without performing Stop Service, Refer to [“2.13 Incorrect display errors”](#).

1. In the “Maintenance Utility” window, select [Administration] - [User Administration].
2. In the “User Groups” window, click the user group which the user belongs to.

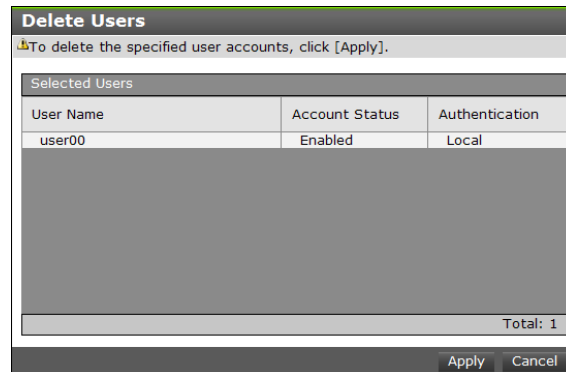


3. Click the [Users] tab. Select the user that you want to remove.

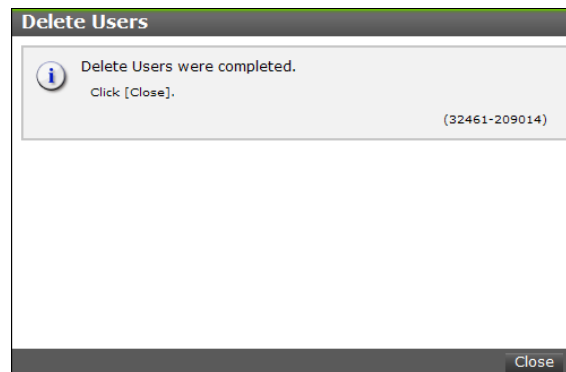


4. Click the [Remove] button.

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



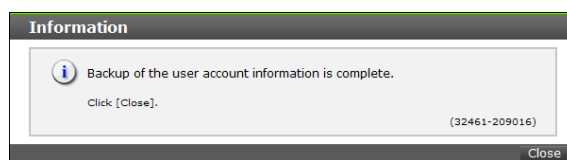
6. A completion message is displayed. Click the [Close] button.



3.3.5 User Account Information

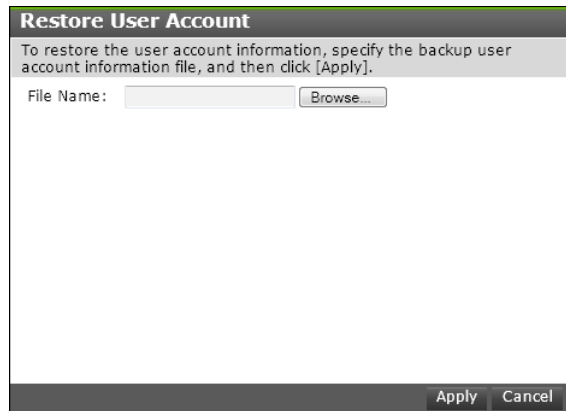
3.3.5.1 Backup User Accounts

1. In the “Maintenance Utility” window, select [Administration] - [User Administration].
2. Select [User Account Information]-[Backup].
3. Specify a storage destination and a file name in the displayed window and download a file.
4. The message appears asking whether you want to remove the selected item. Click the [Close] button.

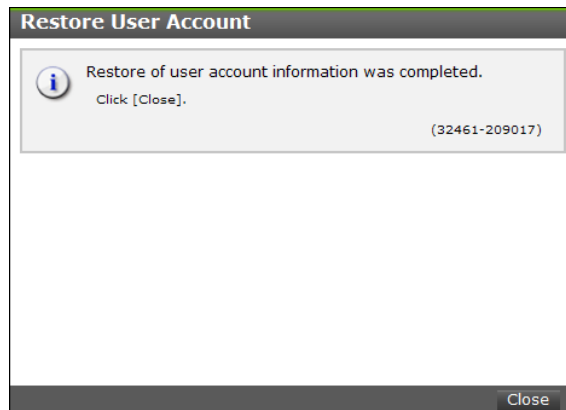


3.3.5.2 Restore of User Account Information

1. In the “Maintenance Utility” window, select [Administration] - [User Administration].
2. Select [User Account Information]-[Restore]. The “Restore User Account” window is displayed.
3. Specify file names to be restored and click the [Apply] button.



4. A completion message is displayed. Click the [Close] button.



3.3.6 Roles to be Required for the Operation Window of Maintenance Utility

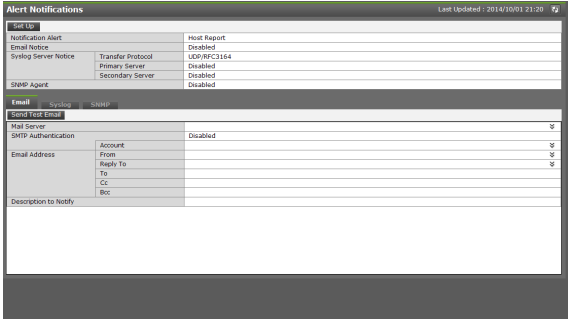
The following shows the roles required to use each operation window of Maintenance Utility. For the details of the roles, see “System Administrator Guide”.

Maintenance Utility operation item	Required role name
Initial Setup Wizard	Storage Administrator (Initial Configuration)
Set Up System Information	Storage Administrator (Initial Configuration)
Firmware	Support Personnel or User Maintenance
User Administration	Security Administrator (View & Modify)
Alert Notifications	Storage Administrator (Initial Configuration)
Set Up Date & Time	Storage Administrator (Initial Configuration)
Set Up Network Settings	Storage Administrator (Initial Configuration)
Licenses	Storage Administrator (Initial Configuration)
Audit Log Settings	Audit Log Administrator (View & Modify)
Turn on/off Locate LEDs	Support Personnel or User Maintenance
Power on Storage System	Support Personnel or User Maintenance
Power off Storage System	Support Personnel or User Maintenance
Edit UPS Mode	Support Personnel or User Maintenance
Edit Login Message	Storage Administrator (Initial Configuration)
Select Cipher Suite	Security Administrator (View & Modify)
Update Certificate Files	Security Administrator (View & Modify)
Force Release System Lock	Storage Administrator (Initial Configuration)
Reboot GUM	Support Personnel or User Maintenance
Change Password	No role is required.
Boot System Safe Mode	Support Personnel
Alert Display	Support Personnel or User Maintenance
Alert Display Related to FRU	Support Personnel or User Maintenance
Select Login Window	Storage Administrator (Initial Configuration)
Download System Dump	No role is required.
Download Small System Dump	No role is required.
Download Configuration Backup	Support Personnel or User Maintenance
View Volume Status	Support Personnel or User Maintenance
Administration Menu	–
Power Management	–
System Management	–
Resetting GUM	–

3.4 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.

- 1. Starting “Alert Notifications” window
In the “Maintenance Utility” window, select [Administration] - [Alert Notifications].
- 2. The “Alert Notifications” window is displayed.



3.4.1 Setting up Email Notification when Storage System Failures Occur

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

3.4.1.1 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.

3.4.1.2 Procedure

1. Starting “Alert Notifications” window.

In the “Maintenance Utility” window, select [Administration] - [Alert Notifications].

2. In the “Alert Notifications” window, click [Set Up].

The screenshot shows the 'Alert Notifications' configuration window. At the top, there is a 'Set Up' button highlighted with a red rectangle. Below it, there are several sections for configuring notifications. The 'Email' section is expanded, showing fields for 'Mail Server', 'SMTP Authentication', 'Email Address', 'Reply To', 'To', 'Cc', 'Bcc', and 'Description to notify'. The 'Email Address' field is currently empty. The 'SMTP Authentication' section shows 'Account' as 'Disabled'. The 'Reply To' field is also empty. The 'To' field is empty. The 'Cc' field is empty. The 'Bcc' field is empty. The 'Description to notify' field is empty.

3. In the “Set Up Alert Notifications” 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.

Set Up Alert Notifications

To edit the alert notification settings of Email, Syslog, and SNMP, set the required information for alert notification settings for the information types. When the settings are complete, verify the settings, and then click [Apply].

Notification Alert: ☒ Host Report ☐ All

Email Syslog SNMP

Email Notice: ☒ Enable ☐ Disable

Email Address (To):

Registered Address	
To	test002@email.co.jp
Cc	test003@email.co.jp

Add Delete Selected: 0 / 2

Email Address (From): test001@email.co.jp (Max. 255 characters)

Email Address (Reply To): test032@email.co.jp (Max. 255 characters)

Description to Notify: (Max. 511 characters or blank)

Mail Server Settings:

Mail Server: ☐ Identifier ☒ IPv4 ☐ IPv6

SMTP Authentication: ☐ Enable ☒ Disable

Account: (Max. 255 characters) Password: (Max. 255 characters)

Apply Cancel

Item	Description
Notification Alert	<p>Selects a target SIM for notifying alerts.</p> <ul style="list-style-type: none"> • [Host Report]: Reports the alert to only the SIMs that report to the host. • [All]: Reports the alert to all SIMs. <p>The target SIM for notifying alerts is common for Email, Syslog, and SNMP.</p>
Email Notice	<p>Selects whether to notify the service information message (SIM)</p> <ul style="list-style-type: none"> • [Enable]: Notifies the service information message (SIM) by email. • [Disable]: Does not notify the service information message (SIM) by email.
Email Address (To)	<p>The attribute to transmit the failure information (SIM) and the mail address are displayed on the [Registration Address] table. If selected [Enable] at [Email Notice], you must set up this item.</p> <ul style="list-style-type: none"> • [Email Address]: Displays the mail address.
Email Address (From)	<p>Specifies an email address of the sender to notify the service information message (SIM). Enter up to 255 alphanumeric characters (ASCII codes) and symbols: (! # \$ % & ` + - * / ^ { } _ . @ ~ = ?).</p> <p>If selected [Enable] at [Email Notice], you must set up this item.</p>
Email Address (Reply to)	<p>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).</p> <p>Enter up to 255 alphanumeric characters (ASCII codes) and symbols: (! # \$ % & ` + - * / ^ { } _ . @ ~ = ?).</p>

(To be continued)

(Continued from preceding page)

Item	Description
Description to Notify	Displays the content that is described at the head of the E-mail text for failure information alert. This is not an indispensable input item. The number of characters is limited up to 511 one-byte characters. A line feed also allowed. A line feed counts as two characters. Allowed characters are one-byte alphanumeric characters, symbols (! " # \$ % & ' () * + - . / : ; < = > ? @ [\] ^ _ ` { } ~), one-byte spaces and line feeds.
Mail Server Settings-Mail Server	Specifies a mail server information. You cannot set all 0 (zero) to the IP address. <ul style="list-style-type: none"> • [Identifier]: To specify a host name, select Identifier and enter up to 255 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. <ul style="list-style-type: none"> • [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: (! \$ % - . @ _ ` ~).

4. Select [Enable] at [Email Notice].

5. At [Email Address (To)], specify the attributes (TO, CC, or BCC) of the destination mail addresses.

6. Specify [Email Address (From)] (required) and [Email Address (Reply to)] (arbitrary)

7. Enter the content to describe in the beginning of the e-mail text into [Description to Notify].

8. Specify [Mail Server] information.

9. 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.

10. Click [Apply]

3.4.1.3 Example of Test Mail

An example of a test email follows:

```
Mail title: VSP Gx00 Report

// HM800 //VSP //////////////////////////////////////
// Ver 1.1 e-Mail Report
////////////////////////////////////
Date : 04/03/2015
Time : 00:19:11
Machine : VSP Gx00 (Serial# 400001)
RefCode : 7ffffff
Detail : This is Test Report.
```

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)
Description to Notify	This is the content entered in the "Set Up Alert Notifications" window. Nothing is displayed when it is not entered.
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.
Action Code	This is the estimated failed part information indicated for the maintenance. It is not described in the test mail. The information on a failure part is displayed by the items of [Action Code], [Possible Failure Parts] and [Location]. Up to eight pieces of information on the failure parts are displayed.

See the SIM RC SECTION ["2. Reference Codes"](#) for reference codes and failure details.

3.4.2 Setting up Syslog Notification

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

3.4.2.1 Prerequisites

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

3.4.2.2 Procedure

1. Starting “Alert Notifications” window.

In the “Maintenance Utility” window, select [Administration] - [Alert Notifications...].

2. In the “Alert Notifications” window, click [Set Up].

The screenshot shows the 'Alert Notifications' configuration window. At the top, there is a 'Set Up' button highlighted in red. Below it, there are sections for 'Email', 'Syslog', and 'SNMP Agent'. The 'Email' section is expanded, showing fields for 'Mail Server', 'SMTP Authentication', 'Email Address', 'Reply To', 'To', 'Cc', 'Bcc', and 'Description to notify'. The 'Syslog' section shows 'Transfer Protocol' set to 'UDP/162' and 'Primary Server' set to '100.100.100.104'. The 'SNMP Agent' section shows 'Primary Server' and 'Secondary Server' both set to 'Disabled'. At the bottom, there is a 'Send Test Email' button.

3. In the “Set Up Alert Notifications” window, Click the [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	<p>Selects a target SIM for notifying alerts.</p> <ul style="list-style-type: none"> • [Host Report]: Reports the alert to only the SIMs that report to the host. • [All]: Reports the alert to all SIMs. <p>The target SIM for notifying alerts is common for Email, Syslog, and SNMP.</p>
Transfer Protocol	<p>Selects the Syslog transfer protocol.</p> <ul style="list-style-type: none"> • [New Syslog Protocol (TLS1.2/RFC5424)] • [Old Syslog Protocol (UDP/RFC3164)]
Primary Server	<p>Selects whether to use the Syslog server.</p> <ul style="list-style-type: none"> • [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-Syslog Server	<p>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.</p> <ul style="list-style-type: none"> • 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). <p>Specifies this item only when [Enable] is selected at [Primary Server].</p>
Primary Server- Port Number	<p>Specifies a port number to be used at the Syslog server.</p> <p>Specifies this item only when [Enable] is selected at [Primary Server].</p>

(To be continued)

(Continued from preceding page)

Item	Description
Primary Server-Client Certificate File Name	<p>Specifies a certificate file. Click [Browse], and then specify a certificate file.</p> <p>You must set this item only when [New Syslog Protocol (TLS1.2/ RFC55424)] is selected at [Transfer Protocol] and when [Enable] is selected at [Primary Server].</p> <ul style="list-style-type: none"> • 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	<p>Enters a password for the client certificate. Up to 128 characters can be entered for the password.</p> <p>Allowed characters are alphanumeric characters and symbols: ! # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~.</p> <p>Specifies this item only when [Client Certificate File Name] is specified.</p>
Primary Server- Root Certificate File Name	<p>Specifies a certificate file. Click [Browse], and then specify a certificate file.</p> <p>You must set this item only when [New Syslog Protocol (TLS1.2/ RFC55424)] is selected at [Transfer Protocol] and when [Enable] is selected at [Primary Server].</p> <ul style="list-style-type: none"> • 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	<p>Selects whether to use an alternative server (secondary server) to the Syslog server.</p> <ul style="list-style-type: none"> • [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- Syslog Server	<p>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].</p>
Secondary Server-Port Number	<p>Specifies a port number to be used on the secondary server.</p> <p>Specifies this item only when [Enable] is selected at [Secondary Server].</p>
Secondary Server-Client Certificate FileName	<p>Specifies a certificate file. Click [Browse], and then specify a certificate file.</p> <p>This item is settable only when [New Syslog Protocol (TLS1.2/ RFC55424)] is selected at [Transfer Protocol] and when [Enable] is selected at [Primary Server].</p> <ul style="list-style-type: none"> • 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.

(To be continued)

(Continued from preceding page)

Item	Description
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].
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]. <ul style="list-style-type: none"> • 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].
Retry	Displays the Retry setting. <ul style="list-style-type: none"> • [Enable]: Retry when the connection to the Syslog server fails. • [Disable]: Does not retry when the connection to the Syslog server fails.
Retry Interval	Specifies the retry interval when the communication with the Syslog server fails in the range of 1 to 60 seconds. Specifies this item only when [New Syslog Protocol (TLS1.2/ RFC5424)] is selected at [Transfer Protocol].

-
4. Select the Syslog transfer protocol at [Transfer Protocol] in the [Syslog] tab.
-
5. If you want to transfer the Syslog to the primary server, select [Enable] at [Primary Server], go to [Step 6](#).
If you do not transfer the Syslog to the primary server, go to [Step 8](#).
-
6. Specify the IP address and port number.
-
7. 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].
-
8. If you want to transfer the Syslog to the secondary server, select [Enable] at [Secondary Server], go to [Step 9](#).
If you do not transfer the Syslog to the secondary server, go to [Step 11](#).
-
9. Specify the IP address and port number.
-

10. 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].

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

12. Specify [Retry] and [Retry Interval] when [New Syslog Protocol (TLS1.2/ RFC5424)] is selected at [Transfer Protocol].

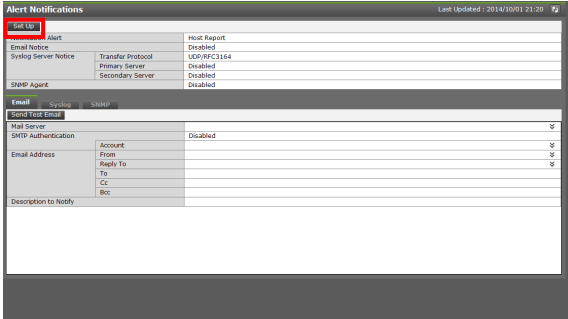
13. Click [Apply].

3.4.3 Setting up SNMP Notification

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

3.4.3.1 Procedure

- 1. Starting “Alert Notifications” window.
In the “Maintenance Utility” window, select [Administration] - [Alert Notifications].
- 2. In the “Alert Notifications” window, click [Set Up].



- The “Set Up Alert Notifications” window appears. Click the [SNMP] tab.
Set the transmission information of the SNMP which notifies storage system failures.
[When selecting v1 or v2c for the SNMP version]

Set Up Alert Notifications

To edit the alert notification settings of Email, Syslog, and SNMP, set the required information for alert notification settings for the information types. When the settings are complete, verify the settings, and then click (Apply).

Notification Alert: ☐ Host Report ☒ All

Email ☐ Syslog ☒ **SNMP**

SNMP Agent: ☒ Enable ☐ Disable

SNMP Version: **v1**

Sending Trap Setting:

Registered Sending Trap Settings	
<input type="checkbox"/> Community	Send Trap to
<input type="checkbox"/> public	10.10.10.10, 10.10.10.20, 10.10.10.30
<input type="checkbox"/> publicpublicpublic	10.10.10.10

Add Change Remove Selected: 0 of 2

Request Authentication Setting:

Registered Request Authentication Settings	
<input type="checkbox"/> Community	Requests Permitted
<input type="checkbox"/> public	10.10.10.10, 10.10.20.10, 10.10.10.30

Add Change Remove Selected: 0 of 1

System Group Information:

Storage System Name: (Max. 180 characters)

Contact: (Max. 180 characters or blank)

Location: (Max. 180 characters or blank)

SNMP Engine ID: 0x80000074043938346264353061

Apply Cancel

[When selecting v3 for the SNMP version]

Set Up Alert Notifications

To edit the alert notification settings of Email, Syslog, and SNMP, set the required information for alert notification settings for the information types. When the settings are complete, verify the settings, and then click (Apply).

Notification Alert: ☐ Host Report ☒ All

Email ☐ Syslog ☒ **SNMP**

SNMP Agent: ☒ Enable ☐ Disable

SNMP Version: **v3**

Sending Trap Setting:

Send Trap to	User Name	Authentication Mode	Authentication Protocol	Encryption Mode	Encryption Protocol
<input type="checkbox"/> 10.10.10.10	public	Enable	SHA	Enable	AES

Add Change Remove Selected: 0 of 1

Request Authentication Setting:

User Name	Authentication Mode	Authentication Protocol	Encryption Mode	Encryption Protocol
<input type="checkbox"/> public	Enable	SHA	Enable	AES

Add Change Remove Selected: 0 of 1

System Group Information:

Storage System Name: (Max. 180 characters)

Contact: (Max. 180 characters or blank)

Location: (Max. 180 characters or blank)

SNMP Engine ID: 0x80000074043938346264353061

Apply Cancel

Item	Description
Notification Alert	<p>Selects a target SIM for notifying alerts.</p> <ul style="list-style-type: none"> • [Host Report]: Reports the alert to only the SIMs that report to the host. • [All]: Reports the alert to all SIMs. <p>The target SIM for notifying alerts is common for Email, Syslog, and SNMP.</p>
SNMP Agent	<p>Selects whether to use the SNMP agent.</p> <ul style="list-style-type: none"> • [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	<p>[Community](*2) Displays the community name accepting the SNMP trap report</p> <p>[Send Trap to] Displays the IP address that reports the SNMP trap.</p> <p>[User Name](*3) Displays the user name used for the SNMP trap report.</p> <p>[Authentication] - [Mode](*3) Displays whether the authentication by the password is enabled.</p> <p>[Authentication] - [Protocol](*3) When the authentication by the password is enabled, displays the authentication method.</p> <p>[Encryption] - [Mode](*3) Displays whether the encryption is enabled.</p> <p>[Encryption] - [Protocol](*3) When the encryption is enabled, displays the encryption method.</p> <p>For the settings, see “3.4.3.2 Adding SNMP Trap Notification Destinations”.</p>

(To be continued)

(Continued from preceding page)

Item	Description
Request Authentication Setting	<p>[Community](*)2 Displays the community name that accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST (*1).</p> <p>[Requests Permitted](*)2 Displays the IP address that accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST (*1).</p> <p>[User Name](*)3 Displays the user name that accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST.</p> <p>[Authentication] - [Mode] (*)3 Displays whether the authentication by the password is enabled.</p> <p>[Authentication] - [Protocol] (*)3 When the authentication by the password is enabled, displays the authentication method.</p> <p>[Encryption] - [Mode] (*)3 Displays whether the encryption is enabled.</p> <p>[Encryption] - [Protocol] (*)3 When the encryption is enabled, displays the encryption method.</p> <p>For the settings, see “3.4.3.3 Adding the Request Permission Setting that Accepts GET REQUEST and GETNEXT REQUEST”.</p>
System Group Information-Storage System Name	<p>Specifies the name of the storage system.</p> <p>Enter up to 180 alphanumeric characters (ASCII codes), except for some symbols (\, / ; : * ? " < > & % ^). Do not enter a blank for the first or last character.</p> <p>This is an indispensable input item.</p> <p>If you change this item, the storage system name in the “Storage System” window of Web Console and Maintenance Utility is also changed.</p>
System Group Information-Contact	<p>Specifies the contact information such as administrator’s name and telephone number.</p> <p>Enter up to 180 alphanumeric characters (ASCII codes), except for some symbols (\, / ; : * ? " < > & % ^). Do not enter a blank for the first or last character.</p> <p>If you change this item, the contact in the “Storage System” window of Web Console and Maintenance Utility is also changed.</p>
System Group Information-Location	<p>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.</p> <p>If you change this item, the location in the “Storage System” window of Web Console and Maintenance Utility is also changed.</p>

*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.

4. Confirm the settings. Click [Apply].

3.4.3.2 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 “Set Up Alert Notifications” window, click the [SNMP] tab. Under the [Sending Trap Setting], click the [Add] button.

The screenshot shows the 'Set Up Alert Notifications' window. At the top, there are tabs for 'Email', 'Syslog', and 'SNMP'. The 'SNMP' tab is selected and highlighted with a red box. Below the tabs, there are sections for 'SNMP Agent', 'SNMP Version', 'Sending Trap Setting', 'Request Authentication Setting', and 'System Group Information'. The 'Sending Trap Setting' section contains a table with columns for 'Send Trap to', 'User Name', 'Authentication Mode', 'Authentication Protocol', 'Encryption Mode', and 'Encryption Protocol'. The first row shows '10.10.10.10', 'public', 'Enable', 'SHA', 'Enable', and 'AES'. Below the table, there are buttons for 'Add', 'Change', and 'Remove', with 'Add' highlighted by a red box. The 'System Group Information' section has input fields for 'Storage System Name', 'Contact', and 'Location'. At the bottom, there is an 'SNMP Engine ID' field with the value '0x80000074043938346264333061'.

Set Up Alert Notifications

To edit the alert notification settings of Email, Syslog, and SNMP, set the required information for alert notification settings for the information types. When the settings are complete, verify the settings, and then click [Apply].

Notification Alert: ☐ Host Report ☒ All

Email Syslog **SNMP**

SNMP Agent: ☒ Enable ☐ Disable

SNMP Version: v3

Sending Trap Setting:

Send Trap to	User Name	Authentication Mode	Authentication Protocol	Encryption Mode	Encryption Protocol	
<input type="checkbox"/>						
<input checked="" type="checkbox"/>	10.10.10.10	public	Enable	SHA	Enable	AES

Add Change Remove Selected: 0 of 1

Request Authentication Setting:

User Name	Authentication Mode	Authentication Protocol	Encryption Mode	Encryption Protocol	
<input type="checkbox"/>					
<input checked="" type="checkbox"/>	public	Enable	SHA	Enable	AES

Add Change Remove Selected: 0 of 1

System Group Information:

Storage System Name: storageSystemName (Max. 180 characters)

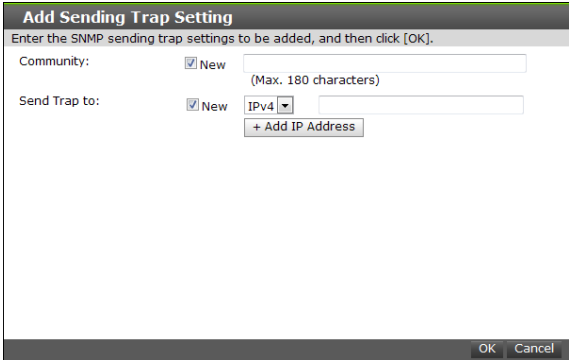
Contact: contact (Max. 180 characters or blank)

Location: location (Max. 180 characters or blank)

SNMP Engine ID: 0x80000074043938346264333061

Apply Cancel

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. <ul style="list-style-type: none">• [+ 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	<p>Enter the IP address that reports the SNMP trap.</p> <ul style="list-style-type: none"> • [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: YYYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY (YYYYY is a hexadecimal number.)
User Name (*1)	<p>Enter the user name used for the SNMP trap report.</p> <p>Enter up to 32 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? " < > & % ^). Do not enter a blank for the first or last character.</p>
Authentication	<p>Select whether to enable or disable the authentication by the password.</p> <ul style="list-style-type: none"> • [Enabled]: Enable the authentication by the password. • [Disabled]: Disable the authentication by the password.
Authentication - Protocol	<p>When enabling the authentication by the password, select the authentication method (SHA or MD5).</p>
Authentication - Password	<p>When enabling the authentication by the password, enter the password. The password should be between eight and 64 characters.</p> <p>Enter alphanumeric characters except for some symbols (\ , / ; : * ? " < > & % ^).</p>
Encryption	<p>Select whether to enable or disable the encryption.</p> <ul style="list-style-type: none"> • [Enabled]: Enable the encryption. • [Disabled]: Disable the encryption.
Encryption - Protocol	<p>When enabling the encryption, select the encryption method (AES or DES).</p>
Encryption - Key	<p>When enabling the encryption, enter the key. The key should be between eight and 64 characters.</p> <p>Enter alphanumeric characters except for some symbols (\ , / ; : * ? " < > & % ^).</p>
Encryption - Re-enter Key	<p>Re-enter the key entered by [Key].</p>

*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 the [OK] button. The entered information is added to [Sending Trap Settings] in the “Set Up Alert Notifications” window.

4. Confirm the settings. Click the [Apply] button.

3.4.3.3 Adding the Request Permission Setting that Accepts GET REQUEST and GETNEXT REQUEST

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

1. In the “Set Up Alert Notifications” window, click the [SNMP] tab. Under the [Request Authentication Setting], click the [Add] button.

Set Up Alert Notifications
To edit the alert notification settings of Email, Syslog, and SNMP, set the required information for alert notification settings for the information types. When the settings are complete, verify the settings, and then click [Apply].

Notification Alert: ☐ Host Report ☒ All

Email Syslog **SNMP**

SNMP Agent: ☒ Enable ☐ Disable

SNMP Version: v3

Sending Trap Settings:

Send Trap to	User Name	Authentication Mode	Protocol	Encryption Mode	Protocol
<input type="checkbox"/> 10.10.10.10	public	<input checked="" type="checkbox"/> Enable	SHA	<input checked="" type="checkbox"/> Enable	AES

[Add] [Change] [Remove] Selected: 0 of 1

Request Authentication Setting:

User Name	Authentication Mode	Protocol	Encryption Mode	Protocol
<input type="checkbox"/> public	<input checked="" type="checkbox"/> Enable	SHA	<input checked="" type="checkbox"/> Enable	AES

[Add] [Change] [Remove] Selected: 0 of 1

System Group Information:

Storage System Name: (Max. 180 characters)

Contact: (Max. 180 characters or blank)

Location: (Max. 180 characters or blank)

SNMP Engine ID: 0x80000074043938346264333061

[Apply] [Cancel]

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

Add Request Authentication Setting
Enter the SNMP request authentication settings to be added, and then click [OK].

Community: ☒ New (Max. 180 characters)

Requests Permitted: ☐ All ☒ New [IPv4] [Add IP Address]

[OK] [Cancel]

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 64 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 64 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 the [OK] button.
The entered information is added to [Request Authentication Setting] in the “Set Up Alert Notifications” window.
-
4. Confirm the settings. Click the [Apply] button.

3.4.3.4 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 “Set Up Alert Notifications” window, Click the [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]

Set Up Alert Notifications

To edit the alert notification settings of Email, Syslog, and SNMP, set the required information for alert notification settings for the information types. When the settings are complete, verify the settings, and then click [Apply].

Notification Alert: ☐ Host Report ☒ All

Email ☐ Syslog ☒ **SNMP**

SNMP Agent: ☒ Enable ☐ Disable

SNMP Version: v1

Sending Trap Setting:

Registered Sending Trap Settings	
Community	Send Trap to
public	10.10.10.10, 10.10.10.20, 10.10.10.30
publicpublic	10.10.10.10

Add Change Remove Selected: 0 of 2

Request Authentication Setting:

Registered Request Authentication Settings	
Community	Requests Permitted
public	10.10.10.10, 10.10.10.20, 10.10.10.30

Add Change Remove Selected: 0 of 1

System Group Information:

Storage System Name:

Contact:

Location:

SNMP Engine ID: 0x80000074043938346264353061

Apply Cancel

[When selecting v3 for the SNMP version]

Set Up Alert Notifications

To edit the alert notification settings of Email, Syslog, and SNMP, set the required information for alert notification settings for the information types. When the settings are complete, verify the settings, and then click [Apply].

Notification Alert: ☐ Host Report ☒ All

Email ☐ Syslog ☒ **SNMP**

SNMP Agent: ☒ Enable ☐ Disable

SNMP Version: v3

Sending Trap Setting:

Send Trap to	User Name	Authentication Mode	Authentication Protocol	Encryption Mode	Encryption Protocol
10.10.10.10	public	Enable	SHA	Enable	AES

Add Change Remove Selected: 0 of 1

Request Authentication Setting:

User Name	Authentication Mode	Authentication Protocol	Encryption Mode	Encryption Protocol
public	Enable	SHA	Enable	AES

Add Change Remove Selected: 0 of 1

System Group Information:

Storage System Name:

Contact:

Location:

SNMP Engine ID: 0x80000074043938346264353061

Apply Cancel

2. Confirm the settings. Click [Apply].

3.4.3.5 Deleting an IP Address and Community of the SNMP Manager which Accepts GET REQUEST and GETNEXT REQUEST

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

1. In the “Set Up Alert Notifications” window, Click the [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]

Set Up Alert Notifications

To edit the alert notification settings of Email, Syslog, and SNMP, set the required information for alert notification settings for the information types. When the settings are complete, verify the settings, and then click [Apply].

Notification Alert: ☐ Host Report ☒ All

Email ☐ Syslog ☒ **SNMP**

SNMP Agent: ☒ Enable ☐ Disable

SNMP Version: v1

Sending Trap Setting:

Registered Sending Trap Settings	
Community	Send Trap to
public	10.10.10.10, 10.10.10.20, 10.10.10.30
publicpublic	10.10.10.10

Add | Change | Remove Selected: 0 of 2

Request Authentication Setting:

Registered Request Authentication Settings	
Community	Requests Permitted
public	10.10.10.10, 10.10.20.10, 10.10.10.30

Add | Change | Remove Selected: 0 of 1

System Group Information:

Storage System Name: storageSystemName (Max. 180 characters)

Contact: contact (Max. 180 characters or blank)

Location: location (Max. 180 characters or blank)

SNMP Engine ID: 0x80000074043938346264333061

Apply Cancel

[When selecting v3 for the SNMP version]

Set Up Alert Notifications

To edit the alert notification settings of Email, Syslog, and SNMP, set the required information for alert notification settings for the information types. When the settings are complete, verify the settings, and then click [Apply].

Notification Alert: ☐ Host Report ☒ All

Email ☐ Syslog ☒ **SNMP**

SNMP Agent: ☒ Enable ☐ Disable

SNMP Version: v3

Sending Trap Setting:

Send Trap to	User Name	Authentication Mode	Protocol	Encryption Mode	Protocol
10.10.10.10	public	Enable	SHA	Enable	AES

Add | Change | Remove Selected: 0 of 1

Request Authentication Setting:

User Name	Authentication Mode	Protocol	Encryption Mode	Protocol
public	Enable	SHA	Enable	AES

Add | Change | Remove Selected: 0 of 1

System Group Information:

Storage System Name: storageSystemName (Max. 180 characters)

Contact: contact (Max. 180 characters or blank)

Location: location (Max. 180 characters or blank)

SNMP Engine ID: 0x80000074043938346264333061

Apply Cancel

2. Confirm the settings. Click [Apply].

3.4.3.6 Changing the Sending Trap Settings

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

1. In the “Set Up Alert Notifications” window, click the [SNMP] tab.
Select targets to be changed in [Sending Trap Setting] and click the [Change] button.

Set Up Alert Notifications
To edit the alert notification settings of Email, Syslog, and SNMP, set the required information for alert notification settings for the information types. When the settings are complete, verify the settings, and then click [Apply].

Notification Alert: ☐ Host Report ☒ All

Email ☐ Syslog ☒ **SNMP**

SNMP Agent: ☒ Enable ☐ Disable

SNMP Version: v3

Sending Trap Settings:

Send Trap to	User Name	Authentication Mode	Authentication Protocol	Encryption Mode	Encryption Protocol
<input checked="" type="checkbox"/> 10.10.10.10	public	<input checked="" type="checkbox"/> Enable	SHA	<input checked="" type="checkbox"/> Enable	AES

Selected: 0 of 1

Request Authentication Setting:

User Name	Authentication Mode	Authentication Protocol	Encryption Mode	Encryption Protocol
<input checked="" type="checkbox"/> public	<input checked="" type="checkbox"/> Enable	SHA	<input checked="" type="checkbox"/> Enable	AES

Selected: 0 of 1

System Group Information:

Storage System Name:

Contact:

Location:

SNMP Engine ID: 0x80000074043938346264353061

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

Change Sending Trap Setting
Change the SNMP sending trap settings, and then click [OK].

Community: publicpublicpublicpublicpublicpublicpublicpublic (Max. 180 characters)

Send Trap to: 10.10.10.10

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. <ul style="list-style-type: none">• [+ 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	<p>Enter the IP address that reports the SNMP trap.</p> <ul style="list-style-type: none"> • [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)	<p>Enter the user name used for the SNMP trap report.</p> <p>Enter up to 32 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? " < > & % ^). Do not enter a blank for the first or last character.</p>
Authentication	<p>Select whether to enable or disable the authentication by the password.</p> <ul style="list-style-type: none"> • [Enabled]: Enable the authentication by the password. • [Disabled]: Disable the authentication by the password. <p>The columns of [Authentication] and [Encryption] are displayed only when selecting [Enabled].</p>
Authentication - Protocol	<p>When enabling the authentication by the password, select the authentication method (SHA or MD5).</p>
Authentication - Change Password	<p>The column of [Password] is displayed only when checking the checkbox of [Change Password].</p>
Authentication - Password	<p>When enabling the authentication by the password, enter the password. The password should be between eight and 64 characters.</p> <p>Enter alphanumeric characters except for some symbols (\ , / ; : * ? " < > & % ^).</p>
Encryption	<p>Select whether to enable or disable the encryption.</p> <ul style="list-style-type: none"> • [Enabled]: Enable the encryption. • [Disabled]: Disable the encryption. <p>The column of [Encryption] is displayed only when selecting [Enabled].</p>
Encryption - Protocol	<p>When enabling the encryption, select the encryption method (AES or DES).</p>

(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 64 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 the [OK] button.

The entered information is changed in [Sending Trap Settings] in the “Set Up Alert Notifications” window.

4. Confirm the settings. Click the [Apply] button.

3.4.3.7 Changing the Request Permission Setting

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

1. In the “Set Up Alert Notifications” window, click the [SNMP] tab. Select targets to be changed in [Request Authentication Setting] and click the [Change] button.

Set Up Alert Notifications

To edit the alert notification settings of Email, Syslog, and SNMP, set the required information for alert notification settings for the information types. When the settings are complete, verify the settings, and then click [Apply].

Notification Alert: ☐ Host Report ☒ All

Email ☐ Syslog ☒ **SNMP**

SNMP Agent: ☒ Enable ☐ Disable

SNMP Version: v3

Sending Trap Setting:

Send Trap to	User Name	Authentication		Encryption	
		Mode	Protocol	Mode	Protocol
<input checked="" type="checkbox"/> 10.10.10.10	public	<input checked="" type="checkbox"/> Enable	SHA	<input checked="" type="checkbox"/> Enable	AES

Add Change Remove Selected: 0 of 1

Request Authentication Settings:

User Name	Authentication		Encryption	
	Mode	Protocol	Mode	Protocol
<input checked="" type="checkbox"/> public	<input checked="" type="checkbox"/> Enable	SHA	<input checked="" type="checkbox"/> Enable	AES

Add Change Remove Selected: 0 of 1

System Group Information:

Storage System Name: (Max. 180 characters)

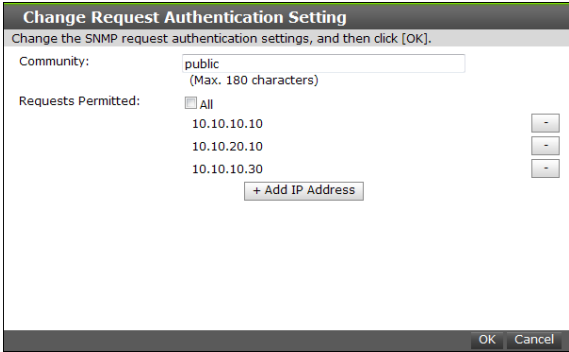
Contact: (Max. 180 characters or blank)

Location: (Max. 180 characters or blank)

SNMP Engine ID: 0x80000074043938346264333061

Apply Cancel

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



Item	Description
Community	<p>Newly enter or select the community name that accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST.</p> <p>Enter up to 180 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? " < > & % ^ '). Do not enter a blank for the first or last character.</p>
Request Permitted	<p>When accepting GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST of all users, check the checkbox of [All].</p> <p>When specifying the user who accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST, newly enter or select the IP address.</p> <ul style="list-style-type: none">• [+ 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. <p>Clicking “-” on the right of the IP address deletes the IP address.</p>

[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. <ul style="list-style-type: none"> • [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 64 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. <ul style="list-style-type: none"> • [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 64 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 the [OK] button.

The entered information is changed in [Request Authentication Setting] in the “Set Up Alert Notifications” window.

4. Confirm the settings. Click the [Apply] button.

3.4.3.8 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 “Set Up Alert Notifications” window.

Procedure

1. Starting “Alert Notifications” window.

In the “Maintenance Utility” window, select [Administration] - [Alert Notifications].

2. In the “Alert Notification” window, click the [SNMP] tab. Click [Send Test SNMP Trap].

The screenshot shows the 'Alert Notifications' window with the 'SNMP' tab selected. The 'Send Test SNMP Trap' button is highlighted with a red box. The window contains several sections: 'Set Up' with a table of notification settings, 'Email' and 'Syslog' tabs, and 'SNMP' settings including 'Storage System Name', 'Location', 'SNMP Trap', and 'SNMP Manager'.

Set Up	
Notification Alert	Host Report
Email Notice	Disabled
Syslog Server Notice	Transfer Protocol: UDP/RFC3164
	Primary Server: Disabled
	Secondary Server: Disabled
SNMP Agent	Disabled

SNMP Settings:

Storage System Name	Location	SNMP Trap
	IP Address	Community

SNMP Manager	IP Address

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

3.5 Time Setting

This is a window to set the system time.

3.5.1 Setting Synchronization Information

This function sets the Storage System's time automatically using the NTP protocol. To use this function, it is required that an NTP server exists in the same LAN in which the Storage System exists. After the setting is made, the Storage System resets the time by referring to the specified NTP server for the current time once a day at the specified time. When the setting is not made, the Storage System does not make the reference.

NOTE: To use this function, it is required that an NTP server exists in the same LAN in which the Storage System exists.

The Storage System's Time Zone is the G.M.T. (Greenwich mean time). If the other Time Zone is used, the Storage System's time may not be set correctly.

This function does not work when the Storage System is being maintained or the setting is being made through Web Console. In such a case, the setting is postponed until the next day.

In case time set goes wrong, check a setup of a NTP server's IP address, and a use port, and give the mode as View mode after a setup again. Moreover, the cause by the side of a NTP server can be considered as other factors.

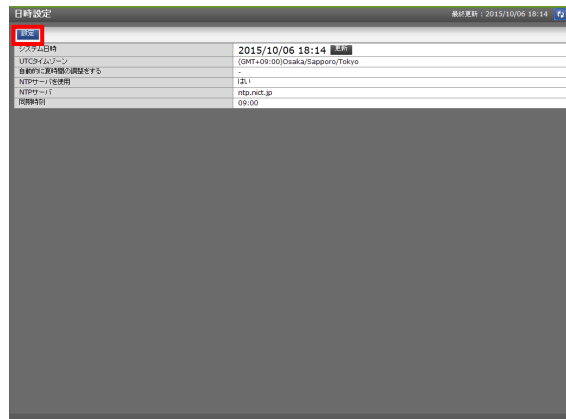
NOTE:

- Please do not execute the PS ON procedure at the synchronization check time.
- Please do not execute collecting the Port Dump at the synchronization check time.

1. Starting "Date & Time" window

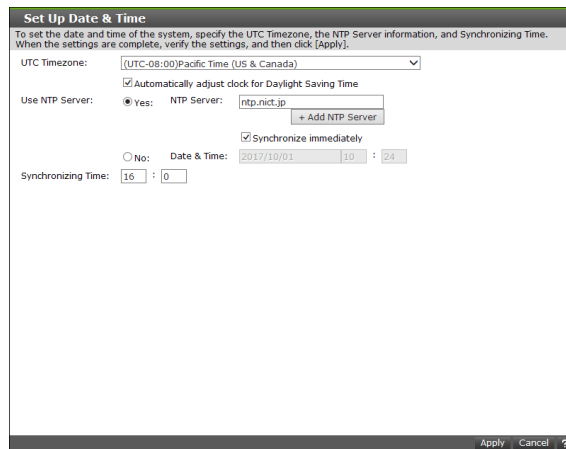
In the "Maintenance Utility" window, select [Administration] - [Date & Time].

2. The “Date & Time” window is displayed. Click the [Set Up] button.



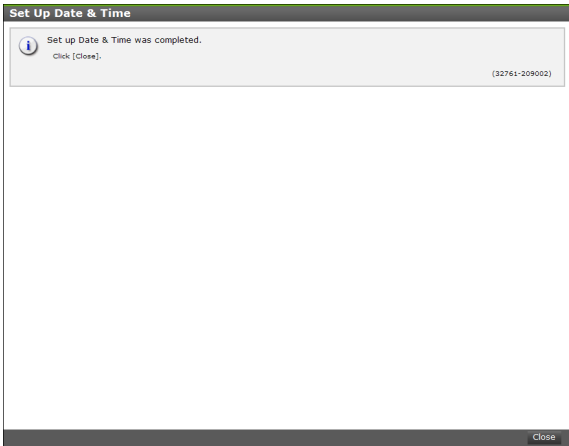
3. Time setting

The “Set Up Date & Time” window is displayed. Set up.

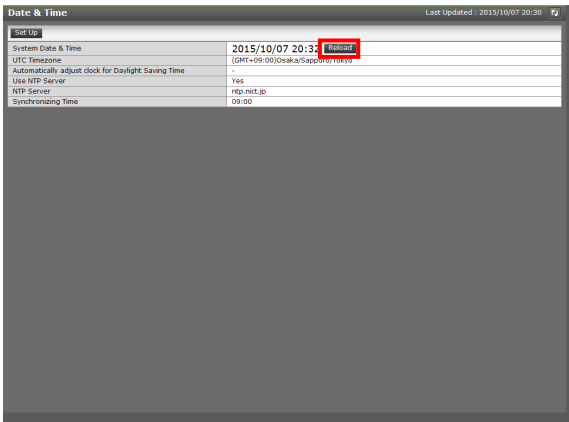


Item	Input Description
UTC Timezone	Select an area of the Universal Time Coordinated
Automatically adjust clock for Daylight Saving Time	Select whether to adjust the daylight-saving time automatically. Displayed only when the UTC time zone applies the daylight-saving time.
Use NTP Server	Check the use of the NTP server
Yes: NTP Server	Enter an IP address or a server name. <ul style="list-style-type: none"> Clicking [Add +NTP Server] can enter up to five NTP servers. Enter the IP address in either the IPv4 format or the IPv6 format. Enter the server name within 255 one-byte alphanumeric characters. The following symbols cannot be used for the server name. !"#\$%&'()*+,-./:;<=>?@[\\]^_`{ }~ Spaces can be used. By checking the checkbox of [Synchronize immediately], the time information is obtained from the NTP server and reflected to the storage system when the [Apply] button is clicked.
No: Date & Time	Set a time manually. Set the following items. Enter Month/Day/Year Hour/Minute. (No Second) Clicking the [Apply and Next] button in this window reflects the set time.
Synchronizing Time	Synchronize with NTP server a time with the specified.

4. A completion message is displayed. Click the [Close] button.



5. Updating display
Clicking the [Reload] button updates the display.



3.6 Network Setting

This is a window to perform the network setting (such as IP address setting) for management (for user) and maintenance (for service personnel). This window can set HTTP (port 80) disconnection.

3.6.1 Network Setting

1. Starting “Network setting” window

In the “Maintenance Utility” window, select [Administration] - [Network setting].

When Maintenance Utility is started by specifying the IP address of the CTL from the browser, the Network Settings item is not displayed in the environment where the GUM and the DKC cannot communicate with each other. Start Maintenance Utility from the Web Console window.

If Maintenance Utility is started from the “Web Console” window or the “MPC” window so as to take recovery actions against the internal IP address inconsistency, the menu is displayed even when GUM and DKC cannot communicate with each other.

2. Network setting

- Click the [Set Up Network Settings] button for setting the network detail. Go to [Step 3](#).
- Click the [Set Up Network Permissions] button for setting the network permission. Go to [“3.6.2 Network Permissions” Step 3](#).

The screenshot shows the 'Network Settings' window with two tabs: 'Set Up Network Settings' (active) and 'Set Up Network Permissions'. The 'Set Up Network Settings' tab contains the following configuration details:

		CTL1	CTL2
IPv4 Configuration	IPv4 Address	10.213.74.111	10.213.74.112
	Subnet Mask	255.255.255.0	255.255.255.0
	Default Gateway	10.213.1.1	10.213.1.1
	DNS Server 1	10.213.1.2	10.213.1.2
	DNS Server 2	10.213.1.3	10.213.1.3
IPv6 Configuration	IPv6 Address	-	-
	Link Local Address	-	-
	Subnet Prefix Length	-	-
	Default Gateway	-	-
	DNS Server 1	-	-
MAC Address	MAC Address	88-88-88-88-88-88-88-88	88-88-88-88-88-88-88-88
	Network Connection Mode	Storage System	Storage System
Maintenance Port	Maintenance Port	192.168.233.116	192.168.233.117
	DNS Search Order	g	
Network Permissions	Internal Network	10.1.0.10/4.15	
	HTTP Port	Enabled	
	Command Control Interface Communication Port and Configuration Manager REST API Non-encrypted Communication Port	Disabled	
	Configuration Manager REST API Encrypted Communication Port	Disabled	
	Configuration Manager REST API Encrypted Communication Port	Disabled	

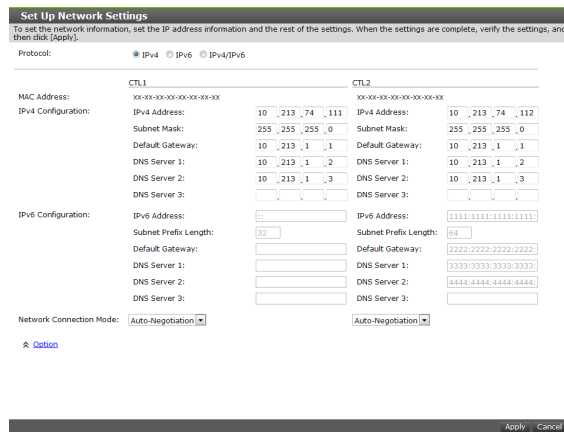
3. Advanced setting of network

CAUTION

About “Forcibly run without safety checks”:

If you check this checkbox and execute the maintenance, the system may go down. Do not check it unless instructed by the message, the manual or the contact described in the manual. This checkbox is displayed only when Maintenance Utility is started from the “Web Console” window or the “MPC” window.

The [Set Up Network Settings] window is displayed. Set up. After the setup, select the [Apply] button.



Set Up Network Settings
To set the network information, set the IP address information and the rest of the settings. When the settings are complete, verify the settings, and then click [Apply].

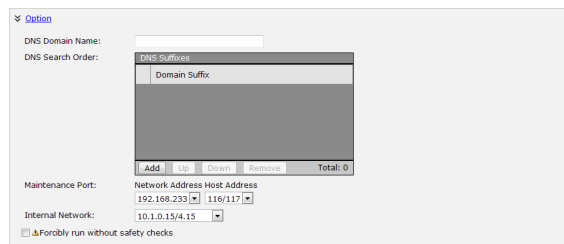
Protocol: ☒ IPv4 ☐ IPv6 ☐ IPv4/IPv6

	CTL1	CTL2
MAC Address:	xx-xx-xx-xx-xx-xx-xx-xx	xx-xx-xx-xx-xx-xx-xx-xx
IPv4 Configuration:	IPv4 Address: 10 . 213 . 74 . 111 Subnet Mask: 255 . 255 . 255 . 0 Default Gateway: 10 . 213 . 1 . 1 DNS Server 1: 10 . 213 . 1 . 2 DNS Server 2: 10 . 213 . 1 . 3 DNS Server 3:	IPv4 Address: 10 . 213 . 74 . 112 Subnet Mask: 255 . 255 . 255 . 0 Default Gateway: 10 . 213 . 1 . 1 DNS Server 1: 10 . 213 . 1 . 2 DNS Server 2: 10 . 213 . 1 . 3 DNS Server 3:
IPv6 Configuration:	IPv6 Address: :: Subnet Prefix Length: 32 Default Gateway: DNS Server 1: DNS Server 2: DNS Server 3:	IPv6 Address: 1111:1111:1111:1111 Subnet Prefix Length: 64 Default Gateway: 2222:2222:2222:2222 DNS Server 1: 3333:3333:3333:3333 DNS Server 2: 4444:4444:4444:4444 DNS Server 3:
Network Connection Mode:	Auto-Negotiation	Auto-Negotiation

[Option](#)

Apply Cancel

Clicking Option displays the following window.



Option

DNS Domain Name:

DNS Search Order:

DNS Suffixes
Domain Suffix

Add Up Down Remove Total: 0

Maintenance Port:

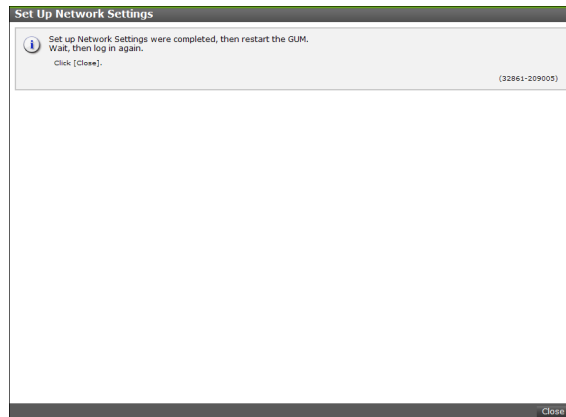
Network Address Host Address: 192.168.233 . 116/117

Internal Network: 10.1.0.15/4.15

☐ Forcibly run without safety checks

Item		Input Description
Protocol		Selects the network protocol. <ul style="list-style-type: none"> • [IPv4]: IPv4 is a setting target. • [IPv6]: IPv6 is a setting target. • [IPv4/IPv6]: IPv4 and IPv6 are setting targets.
MAC Address		Displays the MAC address of CTL1 or CTL2.
IPv4 configuration	IPv4 Address	Specifies the IPv4 address of CTL1 or CTL2.
	Subnet Mask	Specifies the subnet mask of CTL1 or CTL2 in the IPv4 format.
	Default Gateway	Specifies the default gateway of CTL1 or CTL2 in the IPv4 format.
	DNS Server 1	Specifies the DNS server 1 of CTL1 or CTL2 in the IPv4 format.
	DNS Server 2	Specifies the DNS server 2 of CTL1 or CTL2 in the IPv4 format.
	DNS Server 3	Specifies the DNS server 3 of CTL1 or CTL2 in the IPv4 format.
IPv6 configuration	IPv6 configuration	Selects whether to set the IPv6. <ul style="list-style-type: none"> • Enable: Sets the IPv6 settings. • Disable: Does not set the IPv6.
	IPv6 Address	Specifies the IPv6 address of CTL1 or CTL2.
	Subnet PreFix Length	Specifies the subnet prefix length of CTL1 or CTL2.
	Default Gateway	Specifies the default gateway of CTL1 or CTL2 in the IPv6 format.
	DNS Server 1	Specifies the DNS server 1 of CTL1 or CTL2 in the IPv6 format.
	DNS Server 2	Specifies the DNS server 2 of CTL1 or CTL2 in the IPv6 format.
	DNS Server 3	Specifies the DNS server 3 of CTL1 or CTL2 in the IPv6 format.
Network Connection Mode		Selects for CTL1 and CTL2 respectively.
Option		
	DNS Domain Name	Enters a domain name. <ul style="list-style-type: none"> • Enter the domain name with three and more and 255 or less one-byte alphanumeric characters including periods (.). • Enter a label (delimited by a period (.)) of the domain name within 63 one-byte alphanumeric characters. • The following symbols cannot be used for the domain name. !"#\$%&'()*+,-./:;<=>?@[\\]^`{ }~ Spaces cannot be used.
	DNS Search Order	Enters a domain name. <ul style="list-style-type: none"> • You can enter up to six domain names. • Enter the domain name with three and more and 255 or less one-byte alphanumeric characters including periods (.). • Enter domain names within 256 characters in total. • Enter a label (delimited by a period (.)) of the domain name within 63 one-byte alphanumeric characters. • The following symbols cannot be used for the domain name. !"#\$%&'()*+,-./:;<=>?@[\\]^`{ }~ Spaces cannot be used.
	Maintenance Port	Selects the network address and the host address of the maintenance. Do not change the port.
	Internal Network	Specifies the internal network IP address. Do not change the network.

4. A completion message is displayed. Click the [Close] button.



-
5. The logout window is displayed. Click the [X] button to close the window.

NOTE:

- When logged in from the browser, return to the “Login” window.
- When changing only the network connection mode, you do not log in again.

-
6. When changing the IP address, change the IP address of the Storage Device List.
Refer to [“2.14.4 Changing Storage System Information and Updating Software of Web Console”](#) for the detail.

NOTE: If you change the IP address of the Maintenance PC before changing the IP address of Storage Device List, you cannot edit the setting of Storage Device List.

-
7. When changing the IP address of the maintenance port, change the IP address of the Maintenance PC.
Refer to [“2.3.1 IP Address Setting of Maintenance PC”](#) for the detail.

3.6.2 Network Permissions

1. Starting “Network setting” window

In the “Maintenance Utility” window, select [Administration] - [Network setting].

When Maintenance Utility is started by specifying the IP address of the CTL from the browser, the Network Settings item is not displayed in the environment where the GUM and the DKC cannot communicate with each other. Start Maintenance Utility from the Web Console window.

If Maintenance Utility is started from the “Web Console” window or the “MPC” window so as to take recovery actions against the internal IP address inconsistency, the menu is displayed even when GUM and DKC cannot communicate with each other.

2. Network setting

- Click the [Set Up Network Settings] button for setting the network detail. Go to [“3.6.1 Network Setting” Step 3](#).
- Click the [Set Up Network Permissions] button for setting the network permission. Go to [Step 3](#).

The screenshot shows the 'Network Settings' window with a 'Last Updated' timestamp of 2018/03/27 09:34. The window has two tabs: 'Set Up Network Settings' (active) and 'Set Up Network Permissions'. The configuration is organized into several sections:

IPv4 Configuration		CTL	DKC
IPv4 Address	10.213.74.111	10.213.74.112	
Subnet Mask	255.255.255.0	255.255.255.0	
Default Gateway	10.213.1.1	10.213.1.1	
DNS Server 1	10.213.1.2	10.213.1.2	
DNS Server 2	10.213.1.3	10.213.1.3	
DNS Server 3			

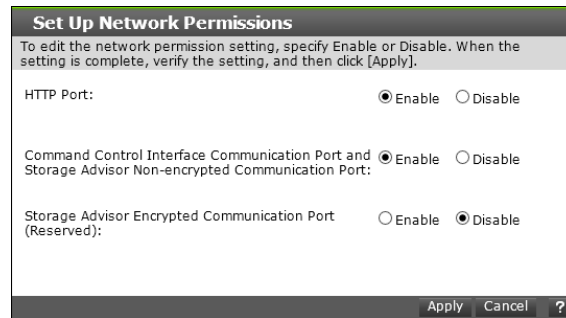
IPv6 Configuration	
IPv6 Address	-
Link Local Address	-
Subnet Prefix Length	-
Default Gateway	-
DNS Server 1	-
DNS Server 2	-
DNS Server 3	-

MAC Address	A4:5B:9C:00:00:00:00:00	00:00:00:00:00:00:00:00
Network Connection Mode	10Mbps 10G	10Mbps 10G
Maintenance Port	Storage System	
DNS Domain Name	192.168.233.116	192.168.233.117
DNS Search Order	0	
Internal Network	10.1.0.10/4.15	

Network Permissions	
HTTP Port	Enabled
Command Control Interface Communication Port and Configuration Manager REST API Non-encrypted Communication Port	Disabled
Configuration Manager REST API Encrypted Communication Port	Disabled

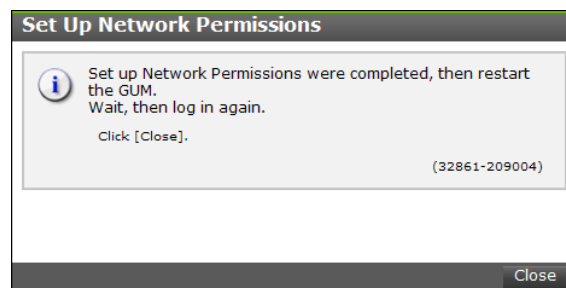
3. Network permission

The [Set Up Network Permissions] window is displayed. After the setup, select the [Apply] button.



Item		Input Description
HTTP Port	Enable	Enable the HTTP Port.
	Disable	Disable the HTTP Port.
Command Control Interface Communication Port and Storage Advisor Non-encrypted Communication Port	Enable	Enable the Command Control Interface Communication Port and Storage Advisor Non-encrypted Communication Port.
	Disable	Disable the Command Control Interface Communication Port and Storage Advisor Non-encrypted Communication Port.
Storage Advisor Encrypted Communication Port (Reserved)	Enable	Enable the Storage Advisor Encrypted Communication Port (Reserved).
	Disable	Disable the Storage Advisor Encrypted Communication Port (Reserved).

4. A completion message is displayed. Click the [Close] button.



5. The GUM reboots automatically.

The logout window is displayed. Click the [X] button to close the window.

NOTE: When logged in from the browser, return to the “Login” window.

3.7 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.

3.7.1 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.

3.7.1.1 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.

3.7.1.2 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.

3.7.1.3 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.

3.7.1.4 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.

3.7.2 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	<p>The licensed capacity is estimated by using one of the following capacities, which depends on the software product.</p> <ul style="list-style-type: none">• Normal volumes (LDEV)• External volumes mapped to the storage system• Pools <p>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.</p>
Implementation capacity/ usable capacity	<p>The license capacity is estimated using the capacity of all the LDEVs in the storage system. Virtual volumes are not included.</p> <p>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 the Accelerated Compression setting.)</p>
Unlimited capacity	You can use the software regardless of the volume capacity.

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

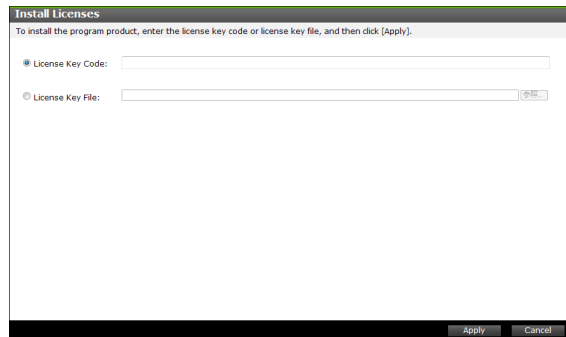
2. The “Licenses” window is displayed. Click the [Install] button.

[illegible]

Item	Description
Program Product Name	Displays the program product name.
Status	<p>Displays the installation status of a program product :</p> <ul style="list-style-type: none">  [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	<p>The license type:</p> <ul style="list-style-type: none"> • Permanent • Term • Temporary • Emergency • Blank (if no license key is installed)
License Capacity	<ul style="list-style-type: none"> • [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)	<p>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.</p> <p>If the expiration is unlimited, a hyphen (-) is displayed.</p> <p>If no license key is installed, blank is displayed.</p>

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

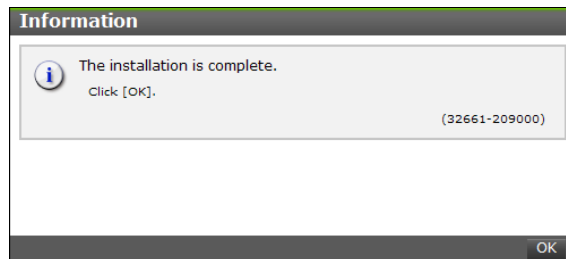
4. Click the [Apply] button.



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 the [OK] button.

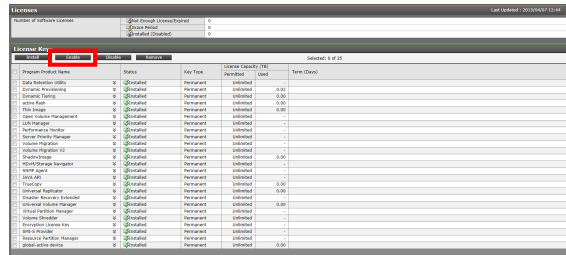


6. Remove the license media.

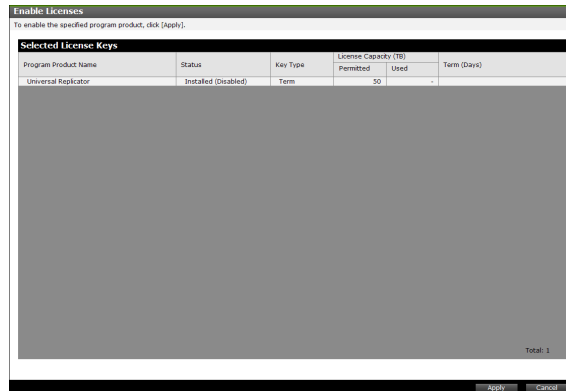
3.7.4 Enabling a License

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

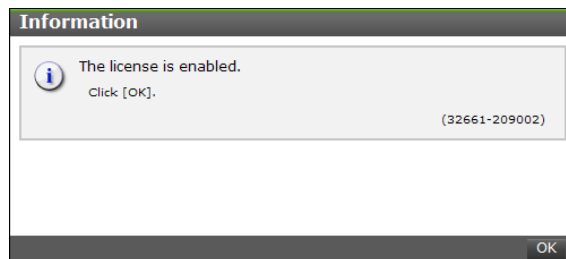
1. Select the license that you want to disable. You can select multiple licenses.
2. Click the [Enable] button in the “License Keys” window.



3. Confirm the settings. Click the [Apply] button.



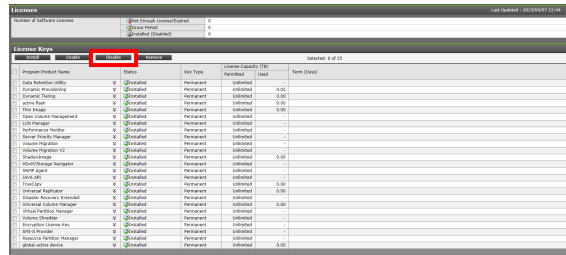
4. A completion message is displayed. Click the [OK] button.



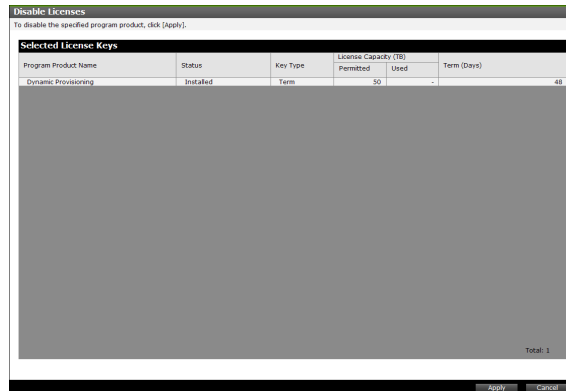
3.7.5 Disabling a License

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

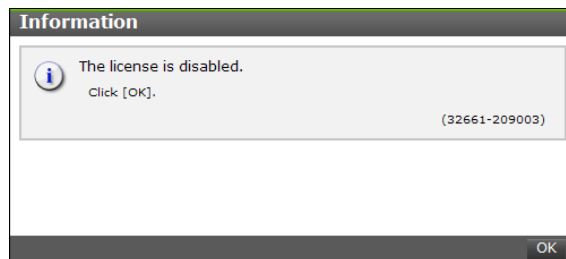
1. Select the license that you want to disable. You can select multiple licenses.
2. Click the [Disable] button in the “License Keys” window.



3. Confirm the settings. Click the [Apply] button.



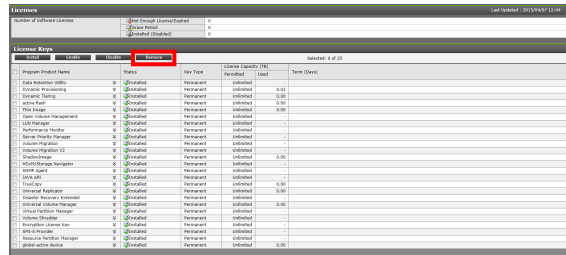
4. A completion message is displayed. Click the [OK] button.



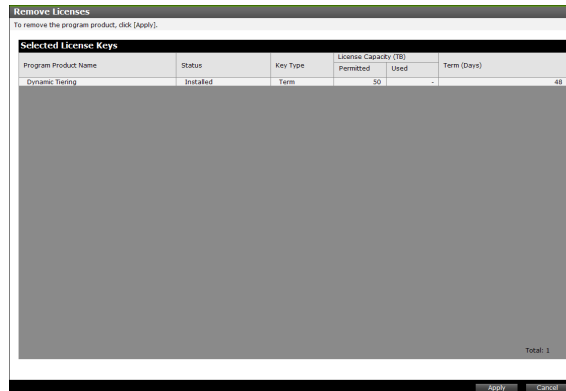
3.7.6 Removing Program Product

The following procedure describes to remove the program product.

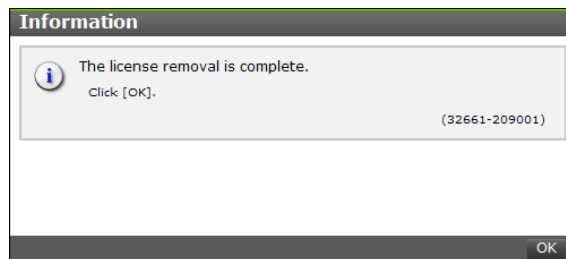
1. Select the license that you want to remove. You can select multiple licenses.
2. Click the [Remove] button in the “License Keys” window.



3. Confirm the settings. Click the [Apply] button.



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



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

[illegible]

See OPTION & FIRMWARE VERSION SECTION “1.2 Software Package and Program Product” for the list of program product.

3.7.7.1 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 key or 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 key or 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

3.7.8 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.

3.7.9 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.

3.7.10 Precautions related to the pool capacity when using Dynamic Provisioning

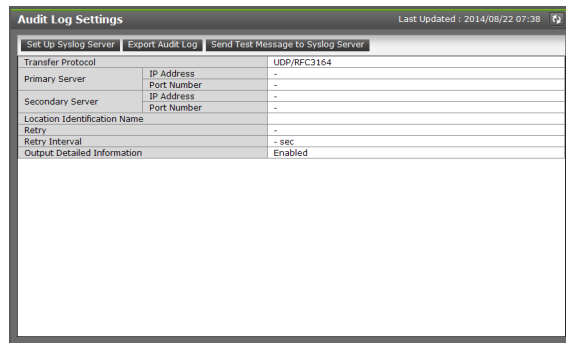
Types of errors	Cause and Actions to be taken
The license capacity is insufficient without adding LDEVs.	When using Dynamic Provisioning, the used capacity of the pool may increase depending on the stored capacity of the data in the LDEV without adding LDEVs. Purchase the insufficient licenses within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

3.8 Audit Log Settings

This is a window to download audit logs and set the transfer destination. The audit log transfer method supports Syslog server transfer.

3.8.1 Verifying the Settings to Transfer the Syslog Server

In the “Maintenance Utility” window, select [Administration] - [Audit Log Settings]. Confirm the settings of the information required to transfer the Syslog server in the “Audit Log Settings” window.



Item	Description
Transfer Protocol	Selects the Syslog transfer protocol. <ul style="list-style-type: none"> • New Syslog Protocol (TLS1.2/RFC5424) • Old Syslog Protocol (UDP/RFC3164)
Primary Server	IP address: Displays the IP address of the primary Syslog server of the audit log transfer destination. Port number: Displays the port number of the primary Syslog server of the audit log transfer destination.
Secondary Server	IP address: Displays the IP address of the secondary Syslog server of the audit log transfer destination. Port number: Displays the port number of the secondary Syslog server of the audit log transfer destination.
Location Identification Name	Displays the location identification name, so that you can identify the storage system.
Retry	Displays the Retry setting. <ul style="list-style-type: none"> • [Enable] : Retry when the connection to the Syslog server fails. • [Disable] : Does not retry when the connection to the Syslog server fails. Displays this item only when New Syslog Protocol (TLS1.2/ RFC5424) is selected at Transfer Protocol.
Retry Interval	Displays the Retry interval. Displays this item only when New Syslog Protocol (TLS1.2/RFC5424) is selected at Transfer Protocol and Retry is Enabled.
Output Detailed Information	Displays the output detailed information setting. <ul style="list-style-type: none"> • [Enabled] : Transfer the detailed information of audit log to the Syslog server. • [Disabled] : Does not transfer the detailed information of audit log to the Syslogserver.

3.8.2 Transferring Audit Log to the Syslog Server

If you configure Syslog server settings, the audit log will always be transferred to the Syslog server and stored as the Syslog files.

You can select either of the following protocols to transfer the audit log to the Syslog server. The output file format is different by the selected protocol.

- TLS1.2/RFC5424
- UDP/RFC3164

NOTICE: When you use UDP/RFC3164, consider the characteristics of UDP (User Datagram Protocol) when designing a network. See RFC3164 (Request for Comments) issued by IETF (Internet Engineering Task Force) for more details.

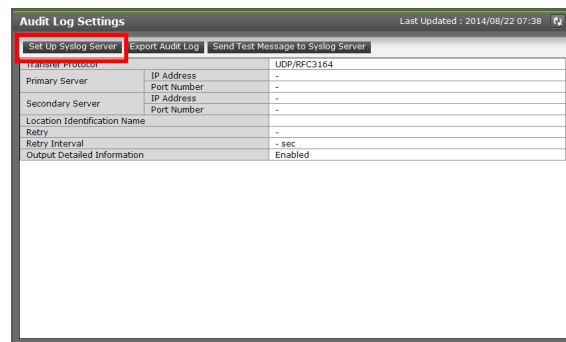
3.8.2.1 Prerequisites

- You must have Audit Log Administrator (View & Modify) role to configure Syslog server settings.
- Make sure the storage system is connected to Syslog servers on a LAN.
- Make sure the Syslog servers are configured so as to transfer audit logs to the Syslog servers.
- The Syslog server certificate and the client certificate is required to use TLS1.2/RFC5424. See “System Administrator Guide” for details.

NOTICE: If audit logs are transferred before configuring the setting of a Syslog server to which the audit logs are transferred, the logs are not saved on the Syslog server and lost. See the user manual of the Syslog server for the details of the Syslog server setting.

3.8.2.2 Operation Procedure

1. In the “Maintenance Utility” window, select [Administration] - [Audit Log Settings].
2. Click [Set Up Syslog Server] in the “Audit Log Settings” window.



3. Set up the Syslog server settings.

Item	Description
Transfer Protocol	<p>Selects a protocol to transfer the audit log.</p> <ul style="list-style-type: none"> • New Syslog Protocol (TLS1.2/RFC5424) • Old Syslog Protocol (UDP/RFC3164)
Primary Server	<p>Selects whether to use the Syslog server.</p> <ul style="list-style-type: none"> • [Enable] : Transfers the audit log to the Syslog server. • [Disable] : Do not transfer the audit log to the Syslog server.
Primary Server-Syslog Server	<p>Specifies an IP address of a server you want to set as a Syslog server.</p> <ul style="list-style-type: none"> • 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).
Primary Server-Port Number	<p>Enters a port number to be used at the Syslog server.</p>
Primary Server-Client Certificate File Name	<p>Specifies a certificate file. Click Browse, and then specify a certificate file.</p> <p>This item is settable only when [TLS1.2/RFC5424] is selected at [Transfer Protocol].</p> <ul style="list-style-type: none"> • 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	<p>Specifies a password for the client certificate. Up to 128 characters can be entered for the password.</p> <p>Allowed characters are alphanumeric characters and symbols: ! # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~.</p> <p>Specifies this item only when Client Certificate File Name is specified.</p>

Item	Description
Primary Server- Root Certificate File Name	<p>Specifies a certificate file. Click Browse, and then specify a certificate file.</p> <p>This item is settable only when [TLS1.2/RFC5424] is selected at [Transfer Protocol].</p> <ul style="list-style-type: none"> • 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	<p>Selects whether to use an alternative server (secondary server) to the Syslog server.</p> <ul style="list-style-type: none"> • [Enable] : Transfers the audit log to the secondary server. • [Disable] : Does not transfer the audit log to the secondary server.
Secondary Server- Syslog Server	<p>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- Server Setting.</p>
Secondary Server-Port Number	<p>Specifies a port number to be used on the secondary server.</p>
Secondary Server- Client Certificate File Name	<p>Specifies a certificate file. Click Browse, and then specify a certificate file.</p> <p>This item is settable only when [TLS1.2/RFC5424] is selected at [Transfer Protocol].</p> <ul style="list-style-type: none"> • 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	<p>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- Server Setting.</p>
Secondary Server-Root Certificate File Name	<p>Specifies a certificate file. Click Browse, and then specify a certificate file.</p> <p>This item is settable only when [TLS1.2/RFC5424] is selected at [Transfer Protocol].</p> <ul style="list-style-type: none"> • 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	<p>Specifies an arbitrary name for the storage system that transfers the audit log 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 (,) and a space cannot be used. Be sure to set it only when [Primary Server] or [Secondary Server] is [Enabled].</p>
Retry	<p>Selects whether to retry when the connection to the Syslog server fails.</p> <ul style="list-style-type: none"> • [Enable] : Retry when the connection to the Syslog server fails. • [Disable] : Does not retry when the connection to the Syslog server fails. <p>Specifies this item only when New Syslog Protocol (TLS1.2/ RFC5424) is selected at Transfer Protocol.</p>
Retry Interval	<p>Specifies the retry interval when the communication with the Syslog server fails in the range of 1 to 60 seconds. The default is 1 second.</p> <p>Specifies this item only when New Syslog Protocol (TLS1.2/ RFC5424) is selected at Transfer Protocol.</p>
Output Detailed Information	<p>Selects whether to transfer the detailed information of the audit log to the Syslog server.</p> <ul style="list-style-type: none"> • [Enable] : Transfer the detailed information of audit log to the Syslog server. • [Disable] : Does not transfer the detailed information of audit log to the Syslog server.

4. Select a protocol to transfer the audit log at [Transfer Protocol].

5. Select [Enable] at [Primary Server]. Set up the following items.
 - IP address and port number.
 - Client certificate file name, password, and root certificate file name
(Specify this item only when New Syslog Protocol (TLS1.2/ RFC5424) is selected at [Transfer Protocol]).

6. If you want to transfer the audit log information to the secondary server, select Enable at Secondary Server. Set up the following items.
 - IP address and port number.
 - Client certificate file name, password, and root certificate file name
(Specify this item only when New Syslog Protocol (TLS1.2/ RFC5424) is selected at [Transfer Protocol]).

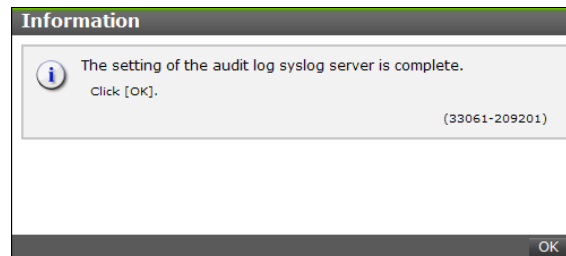
7. Specify an arbitrary name for the storage system in [Location Identification Name], so that you can identify the Storage System.

8. When the connection to the Syslog server fails, if you want to retry, select [Enable] at [Retry] and set up at [Retry interval] (Specify this item only when New Syslog Protocol (TLS1.2/ RFC5424) is selected at [Transfer Protocol]).

9. If you want to transfer the detailed information of audit log to the Syslog server, select [Enable] at [Output Detailed Information].

10. Click the [Apply] button.

11. A completion message is displayed. Click the [OK] button.

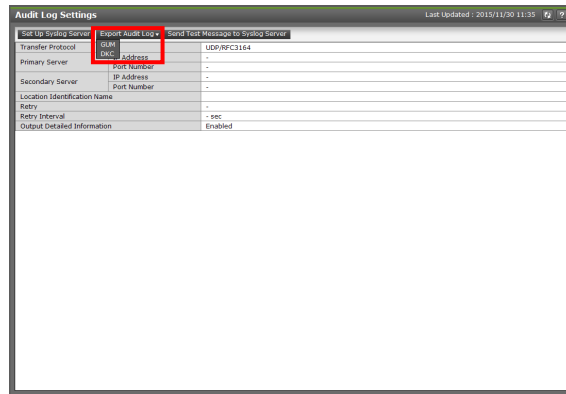


3.8.3 Exporting Audit Log

3.8.3.1 Exporting Audit Log (Maintenance Utility)

There are two types of audit logs for the Storage System: the audit log of the GUM and the audit log of the DKC. For the export of the audit log of the GUM, export the audit log for each controller because each controller is equipped with one GUM. When you log in to Maintenance Utility implemented in the GUM of the connection destination from the computer that outputs the audit log, you can export only the audit log of the GUM of the connection destination. To export the audit log of the other GUM, connect to the other GUM by specifying its IP address. For the export of the audit log of the DKC, you can export the audit log, whichever GUM is connected. Storage Navigator does not have a function to specify a connection destination. For that reason, log in to Maintenance Utility to perform the export.

1. In the “Maintenance Utility” window, select [Administration] - [Audit Log Settings].
2. Click [Export Audit Log] in the “Audit Log Settings” window to select GUM or DKC.



3. The confirmation window is displayed. Click the [OK] button.
4. The white window or the security confirmation window is displayed.
If the certificate is invalid at the time of the https connection, the security confirmation window is displayed, select “Continue to this website (not recommended)”.

NOTICE: Do not close the white window or the security confirmation window until the export is completed. The export may fail.

5. The file download window is displayed. Export is actualized by downloading the files. If [DKC] is selected, it takes two to three minutes to display the file download window.

NOTICE:

- The file download window is displayed in the Maintenance Utility window. If the Maintenance Utility window is hidden in the while window or the security confirmation window, click the Maintenance Utility window to check the download window.
- The form of the file download window varies depending on the browser.
- Depending on the browser setting, the file download might be started without displaying the file download window.

6. Click [Save as] in the file download window.

7. Enter a download destination and a file name, and then click [Save] button.

8. Confirm the download progress.

NOTICE:

- Because files to be downloaded are generated dynamically, the file size in the estimated file transfer completion time are unknown or hidden.
- The time of downloading files depends on the network speed.

9. Confirm the completion of the download.

NOTICE: Close the white window or the security confirmation window manually when the window remains.

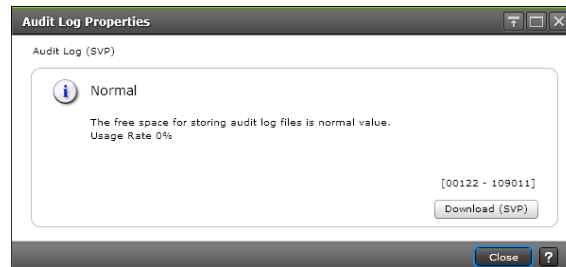
NOTICE: Note the following precautions related to the records in the audit log of DKC.

1. Location identification name
If you select [Administration] - [Audit Log Settings] - [Set Up Syslog Server] - [Location Identification Name] in the Maintenance Utility and there change the location identification name, depending on timing, the location identification name in the event records generated before the change might be updated to the location identification name after the change.
2. Time lag length in the date and time information
If you select [Administration] - [Date & Time] - [Set Up] - [UTC Timezone] in the Maintenance Utility and there change the UTC time zone involving a change in the time lag length, depending on timing, the time lag length in the event records generated before the change might be updated to the time lag length after the change.

3.8.3.2 Exporting Audit Log (Web Console)

1. In the “Web Console” window, click [Audit Log] button on the menu bar.
The icons displayed on the menu bar show the accumulated status of the audit log files.

2. “Audit Log Properties” window is displayed.

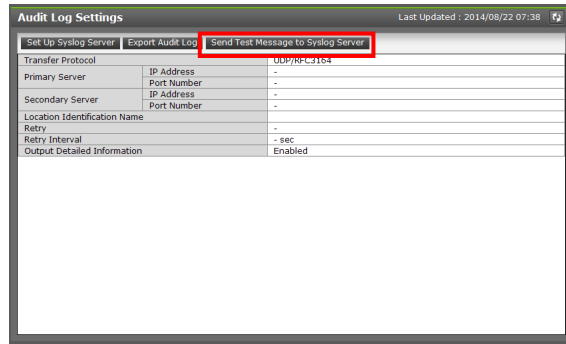


Item	Description
Usage Rate	This indicates how much the storage capacity of the non-transfer audit logs is to the maximum storage capacity.
Download (SVP)	Audit logs of the following contents/type are exported: <ul style="list-style-type: none">• Operation set by the Maintenance PC

3. Click the [Download (SVP)] button.
Select [Download (SVP)] to export logs operated by the Web Console.
The message of preparation completion appears.
4. Click OK, and the window to specify the export destination is opened.
5. Specify the export destination and the file name, and click the [Save] button.
6. Click the [Close] button.

3.8.4 Sending a Test Message to the Syslog Server

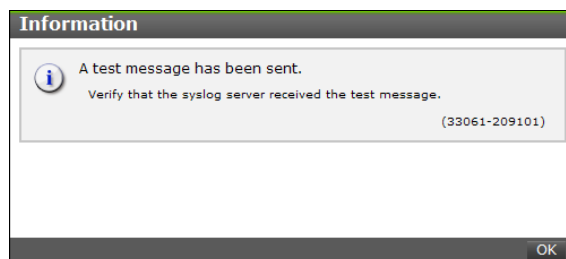
1. In the “Maintenance Utility” window, select [Administration] - [Audit Log Settings].
2. Click [Send Test Message to Syslog Server] in the “Audit Log Settings” window.



3. Confirm that the Syslog server is receiving the log of Syslog server setting. The function name of the log is “AuditLog” and the operation name is “Send Test Message”.

NOTICE: If the audit log is not received by the Syslog server, check whether the set IP address and port number matches the IP address and port number of the Syslog server, and make sure that the Client Certificate File Name, password, and the Root Certificate File Name are correct. If the settings are correct, check the Syslog server setting. See the user manual of the Syslog server for the details of the Syslog server setting.

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



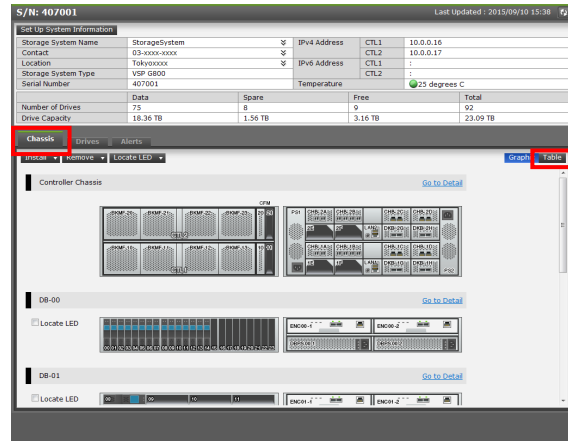
3.9 Turn on/off Locate LEDs

This is a window to turn on/off the LEDs located on the front and rear of the Drive Box.

3.9.1 Turn on Locate LED

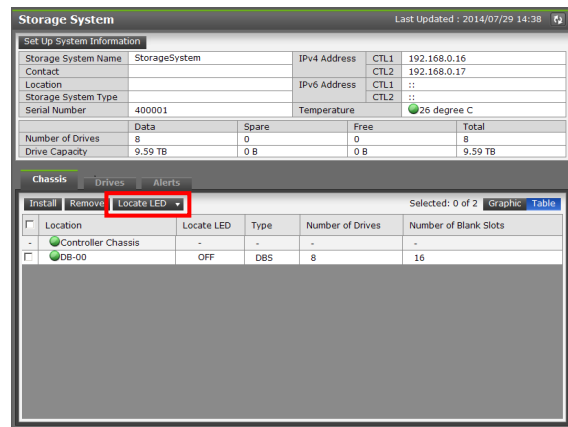
1. Table display of Drive Box

Select the [Table] switch from the [Chassis] tab in the main window.




2. Select (multiple) DBs from the list

Select a DB to change and select [Turn on] from the [Locate LED] menu. (Multiple selection possible)



3. Check the lighting-up target DB on the list and click the [Apply] button.

Turn On Locate LEDs

 To turn the Locate LED ON, verify the selected drive boxes, and click [Apply].

Selected Drive Boxes

Location	Status	Type	Result
DB-01	Normal	DBL	


Total: 1

Apply

Cancel

4. A message is displayed. Click the [Close] button.

Turn On Locate LEDs

 Turn on Locate LEDs were completed.
Click [Close].
(32961-209006)

Selected Drive Boxes

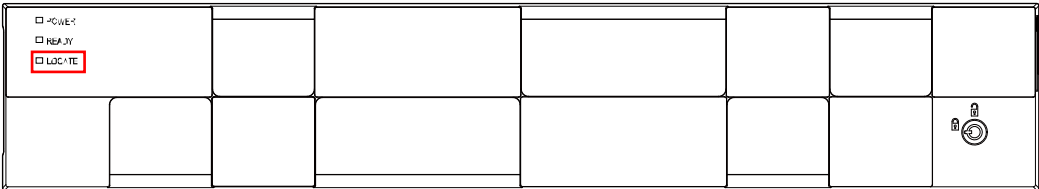
Location	Status	Type	Result
DB-01	Normal	DBL	NG

Total: 1

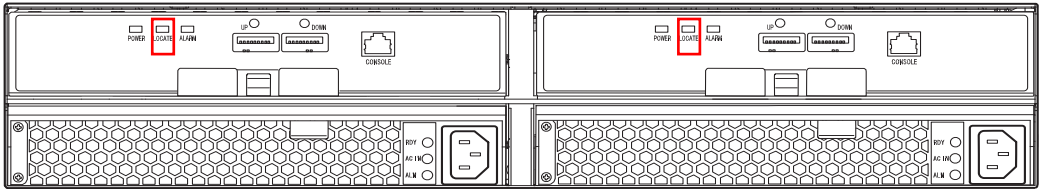
Close

5. The Locate LED on the Drive Box and both LOCATE LEDs on two ENC's light up.

DBS/DBL

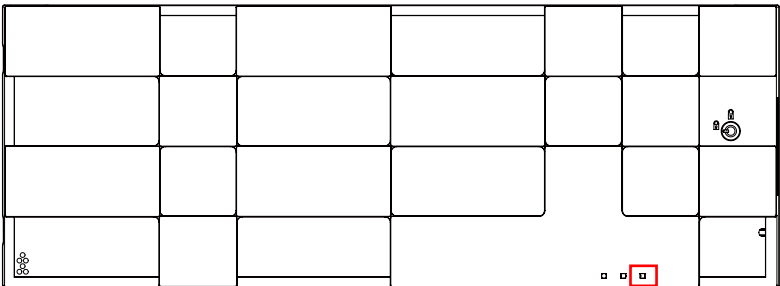


DBL/DBS Front Bezel

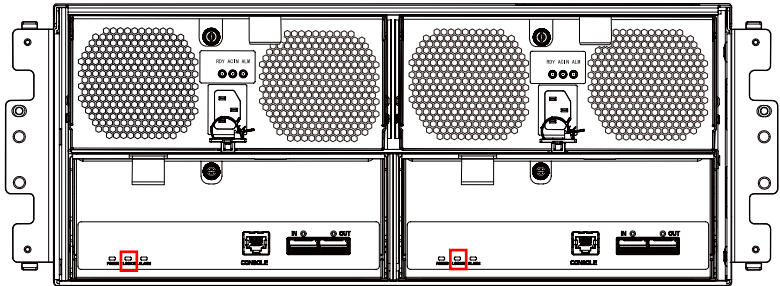


Rear view of DBS/DBL

DB60

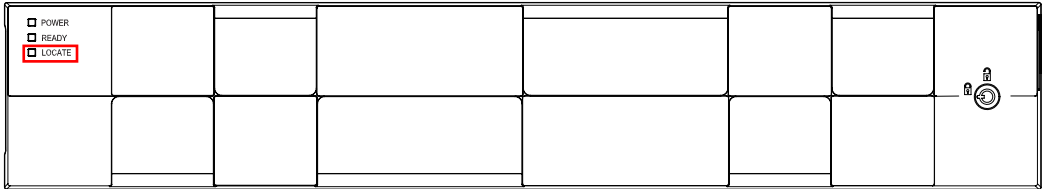


Front view of DB60

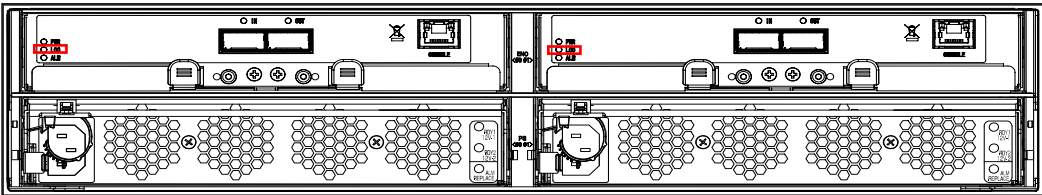


Rear view of DB60

DBF



DBF Front Bezel

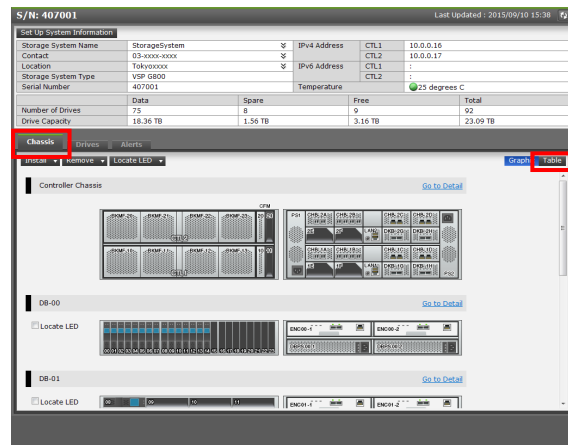


Rear view of DBF

3.9.2 Turn off Locate LED

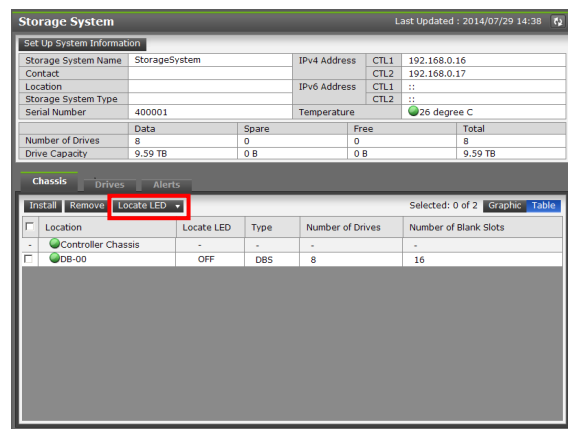
1. Table display of Drive Box

Select the [Table] switch from the [Chassis] tab in the main window.




2. Select (multiple) DBs from the list

Select a DB to change and select [Turn off] from the [Locate LED] menu. (Multiple selection possible)



3. Check the lighting-up target DB on the list and click the [Apply] button.

Turn Off Locate LEDs

 To turn the Locate LED OFF, verify the selected drive boxes, and click [Apply].

Selected Drive Boxes

Location	Status	Type	Result
DB-00	Normal	DBS	


Total: 1

Apply

Cancel

4. A message is displayed. Click the [Close] button.

Turn Off Locate LEDs

 Turn off Locate LEDs were completed.
Click [Close].
(32961-209007)

Selected Drive Boxes

Location	Status	Type	Result
DB-00	Normal	DBS	OK

Total: 1

Close

5. A completion message is displayed. Click the [Close] button.

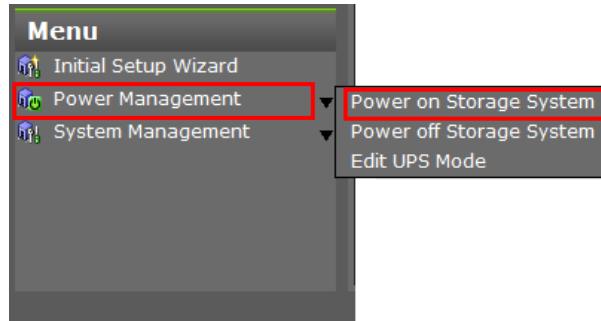
3.10 Power on Storage System

This is a window to power on the Storage System (DKC).

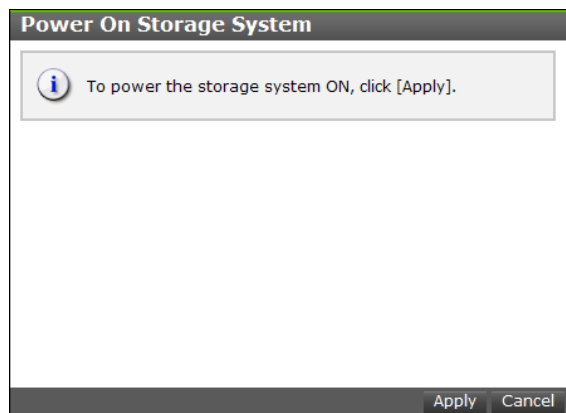
NOTE: If you turn off the Storage System by the main switch, you cannot turn on the Storage System from the power management menu.

1. Operation menu panel

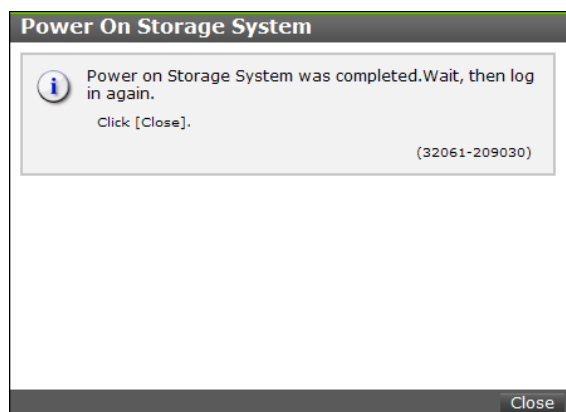
Select [Power on Storage System] from [Power Management].



2. Click the [Apply] button.



3. A completion message is displayed. Click the [Close] button.



4. The GUM reboots automatically.

The logout window is displayed. Click the [X] button to close the window.

NOTE: When logged in from the browser, return to the “Login” window.

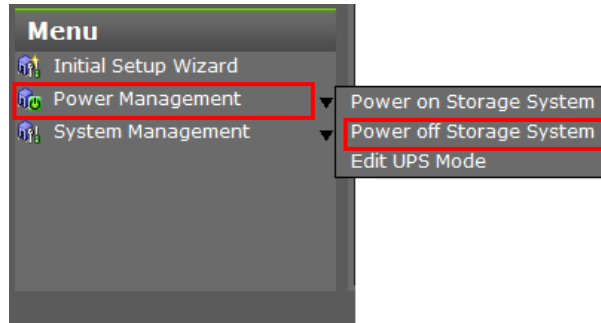
3.11 Power off Storage System

This is a window to power off (planned shutdown) the Storage System (DKC).

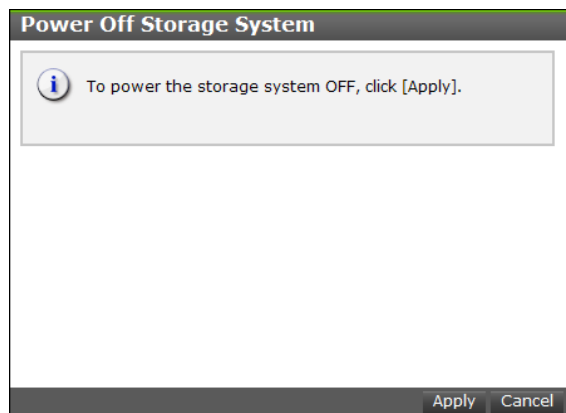
NOTE: If you turn off the Storage System by the main switch, you cannot turn on the Storage System from the power management menu.

1. Operation menu panel

Select [Power off Storage System] from [Power Management].



2. Click the [Apply] button.



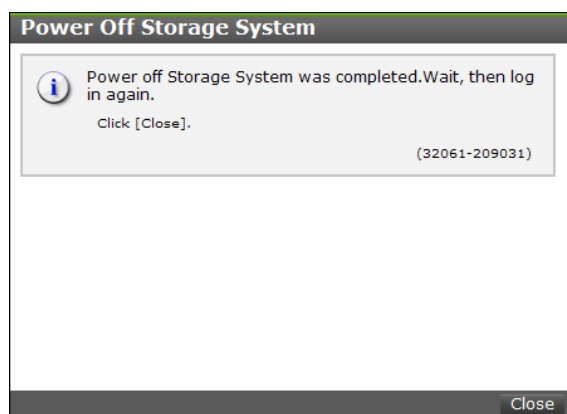
3. Displaying the Password entry window.

⚠ CAUTION

This operation may cause a serious error such as a system down or a data loss. Confirm the appropriateness of the operation, and then input of the password.

Enter the login password for the maintenance account of the storage system, and then click the [OK] button.

4. A completion message is displayed. Click the [Close] button.
When powering on and using the Storage System, log in again.

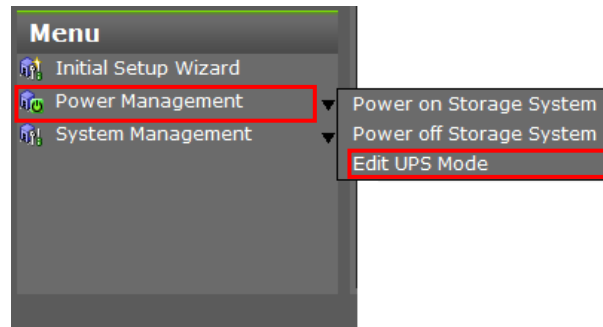


3.12 Edit UPS Mode

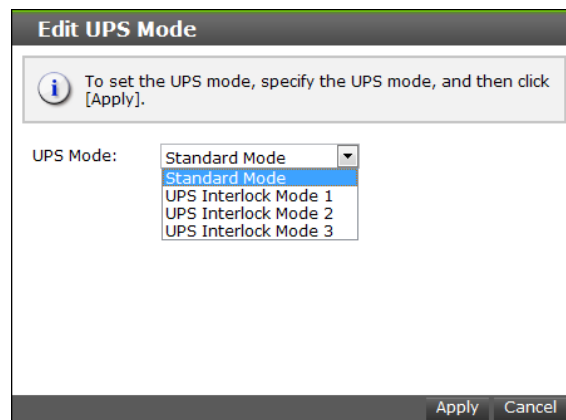
This is a window to change the UPS mode (UPS connection setting).

1. Operation menu panel

Select [Edit UPS Mode] from [Power Management].



2. Select [UPS Interlock Mode] from the [UPS Mode] pull-down menu and click the [Apply] button.



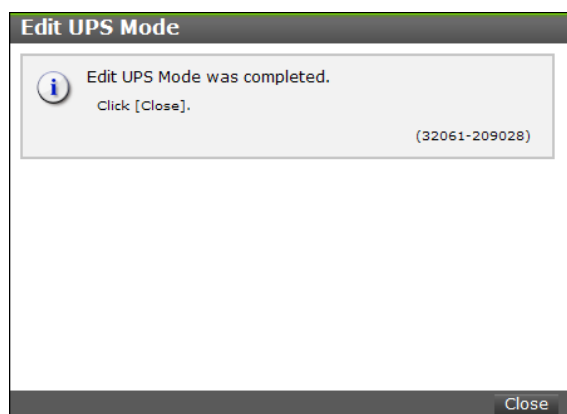
Normal Mode : Do not use UPS interlock.

UPS Interlock Mode 1 : Use this mode by connecting the UPS and the interlock cable only for the 1 system.

UPS Interlock Mode 2 : This mode is unusable.

UPS Interlock Mode 3 : Use this mode by connecting the UPS and the interlock cable to both 1 system and 2 system.

3. A message is displayed and click the [Close] button.



NOTE: You need to turn off the Storage System to reflect the mode change. turn off the Storage System in the following procedure.

(The mode is reflected when restarting the system.)

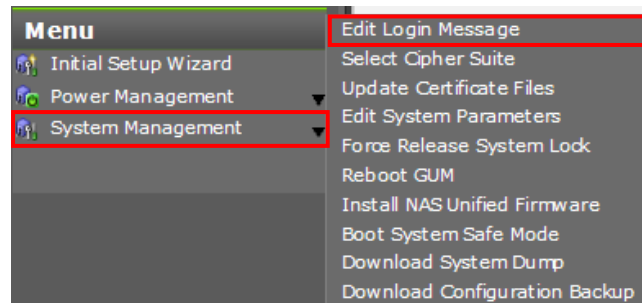
- (1) Turn off the main switch.
Check that the READY LED (green) goes out.
- (2) Remove two power cables from the Controller Chassis.
- (3) After waiting for about 30 seconds, install two power cables in the Controller Chassis.
- (4) When interlocking with the UPS, turn on the output of the UPS.
- (5) Turn on the main switch.

3.13 Edit Login Message

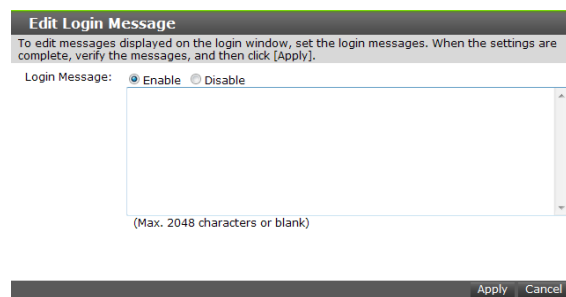
This is a window to edit the messages displayed in the login window (a window displayed when the CTL IP address is directly entered into the browser) of the “Maintenance Utility” window.

1. Operation menu panel

Select [Edit Login Message] from [System Management].

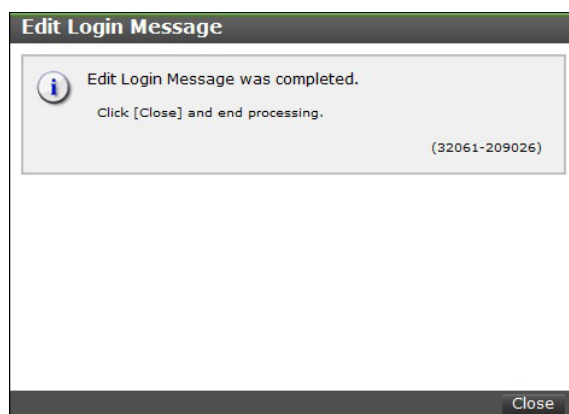


2. Enter a message to be displayed at a login time and click the [Apply] button.



Item	Description
Selecting login message display	Select whether to enable or disable the login message display. <ul style="list-style-type: none"> • [Enabled]: Enables the display of login messages. • [Disabled]: Disables the display of login messages.
Login Message	Enter a message to be displayed at the time of login. <ul style="list-style-type: none"> • A line feed is counted as two characters. • Character decoration is not allowed. Enter simple text information. • You can enter up to 2048 characters. A blank is also allowed.

3. A completion message is displayed. Click the [Close] button.

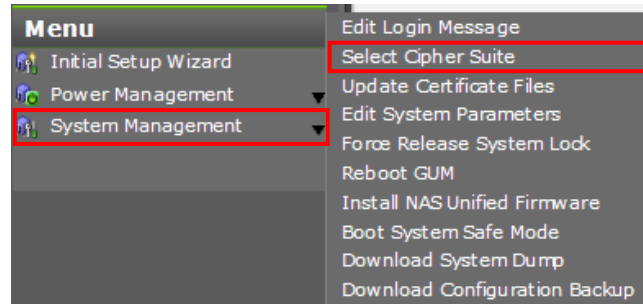


3.14 Select Cipher Suite

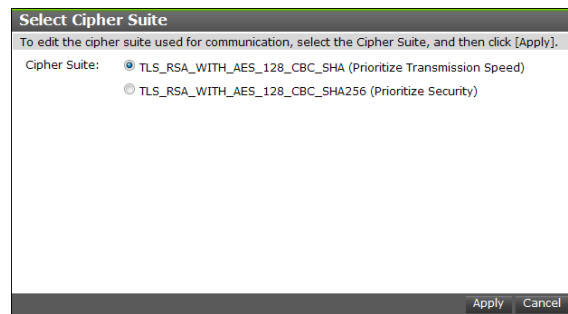
This is a window to change the encryption intensity of the communication between the SVP and the CTL.

1. Operation menu panel

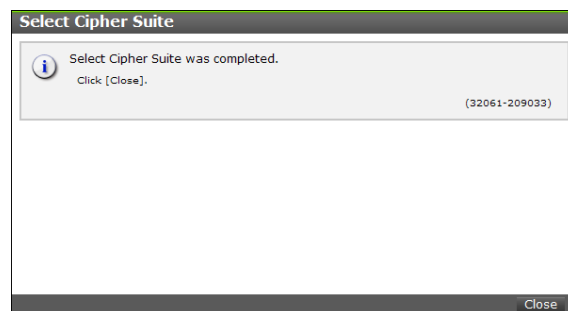
Select [Select Cipher Suite] from [System Management].



2. Select Cipher Suite and click the [Apply] button.



3. A completion message is displayed. Click the [Close] button.



3.15 Update Certificate Files

Update the certificate files used for the communications shown below.

Type of communication	Item used for updating certificate file
HTTPS communication between client and CTL	[Web Server]
Communication for management between SVP and CTL	[Connect to SVP]

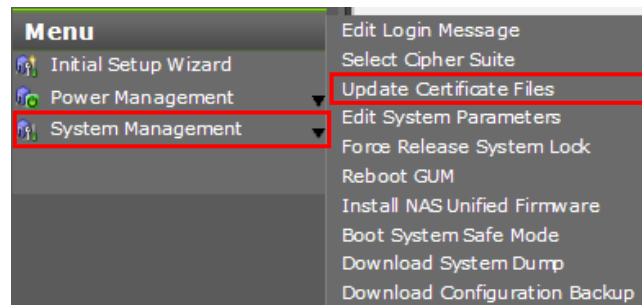
Use the PKCS#12 format.

If you have a server certificate file and a secret key file in the PEM format, you need to convert the files to the PKCS#12 format.

Furthermore, you need to register the server certificate file before converting to the PKCS#12 format in the SVP and the Maintenance PC.

1. Operation menu panel

Select [Update Certificate Files] from [System Management].

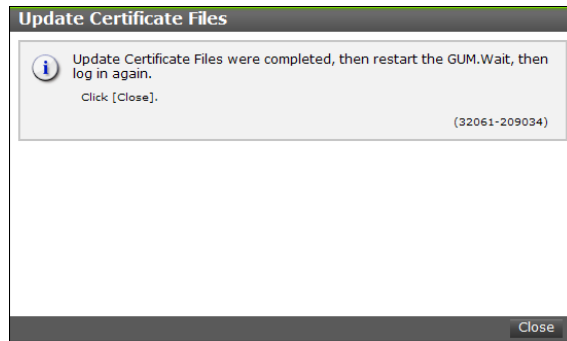


2. Set Update Certificate Files and click the [Apply] button.

 A screenshot of a dialog box titled 'Update Certificate Files'. It contains instructions: 'To update the server certificate, select the certificate file, and enter the password. When the settings are complete, verify the entries, and then click [Apply].'. There are two sections: 'Web Server:' and 'Connect to SVP:'. Each section has a 'Browse...' button, a 'Password:' field, and a 'Re-enter Password:' field. A note '(Max. 128 characters or blank)' is present below each password field. At the bottom right are 'Apply' and 'Cancel' buttons.

Item		Description
Web Server		Select a file from the [Browse] button.
	Password	Enter a password. A maximum of 128 letters or a blank is possible.
	Re-enter Password	Re-enter the password.
Connection to SVP		Select a file from the [Browse] button.
	Password	Enter a password. A maximum of 128 letters or a blank is possible.
	Re-enter Password	Re-enter the password.

3. A completion message is displayed. Click the [Close] button.



4. The GUM reboots automatically.
The logout window is displayed. Click the [X] button to close the window.
NOTE: When logged in from the browser, return to the "Login" window.

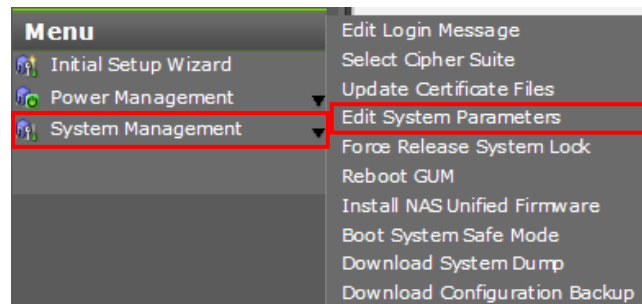
3.16 Edit or Confirm System Parameters

This is a window used for initial installation of the Storage System and volatilization start. This window is displayed only when starting the “Maintenance Utility” window in the following procedures.

- Selecting a menu from the toolbar [Maintenance Utility]-[Hardware]-[Other hardware maintenance...] in the “Web Console” window
- Click the [Maintenance Utility] button in the “MPC” window

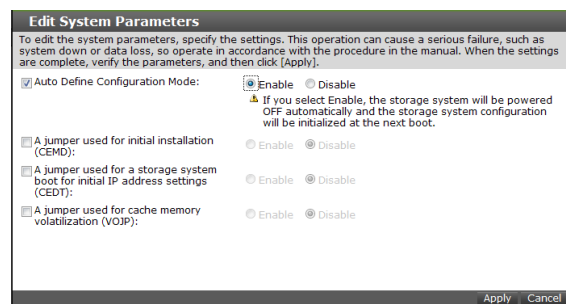
1. Operation menu panel

Select [Edit System Parameters] from [System Management].



2. Set the [Edit System Parameters] and click the [Apply] button.

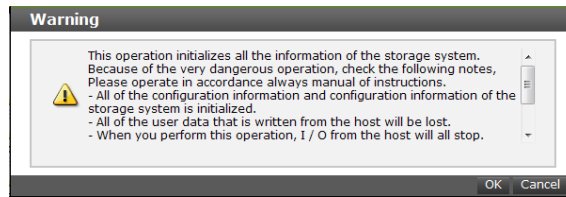
If you do not change system parameters (you just confirm system parameters), click the [Cancel] button.



Menu	Description
Auto Define Configuration Mode	Auto Define Configuration Mode Selecting Enable powers off the Storage System automatically and initializes the system configuration at the next start.
A jumper used for initial installation (CEMD)	A jumper used for initial installation
A jumper used for a storage system boot for initial IP address settings (CEDT)	A jumper used for a storage system boot for initial IP address settings
A jumper used for cache memory volatilization (VOJP)	A jumper used for cache memory volatilization

- NOTE:
- The Auto Define Configuration Mode, CEMD, CEDT and VOJP can be set by either Maintenance Utility of CTL1/CTL2. (The setting is not required in both CTLs)
 - Set CEMD, CEDT and VOJP only when instructed in the manual.

3. Enabling the Auto Define Configuration Mode displays the Confirm window. Click the [OK] button.



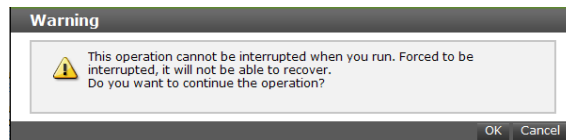
4. Displaying the Password entry window

CAUTION

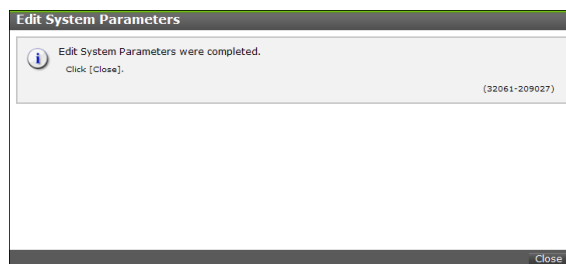
This operation may cause a serious error such as a system down or a data loss. Confirm the appropriateness of the operation, and then input of the password.

Enter the login password for the maintenance account of the storage system, and then click the [OK] button.

5. Enabling the Auto Define Configuration Mode displays the final confirmation message when clicking the [OK] button in the Password entry window.
Check the contents of the message and click the [OK] button if no problem is found.



6. A completion message is displayed. Click the [Close] button.
Check that the system configuration is initialized after completing the operation.

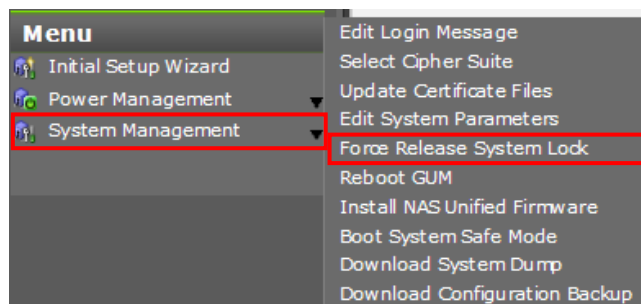


3.17 Force Release System Lock

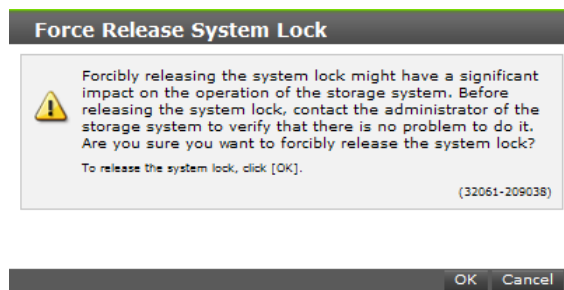
NOTICE: While the other user is changing the setting by Storage Navigator or Maintenance Utility, the system lock status is displayed. If the other user cannot change the setting completely due to errors or others, the system lock status might not be released. This is a function to release the system lock forcibly in such case. To perform Force Release System Lock, check that the other user is not changing the setting. If Force Release System Lock is performed while the other user is changing the setting, multiple users can change the setting at the same time and the Storage System might not be set as the user intends.

1. Operation menu panel

Select [Force Release System Lock] from [System Management].



2. Click the [OK] button.



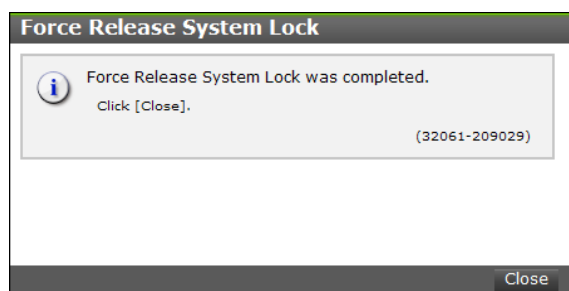
3. Displaying the Password entry window

CAUTION

This operation may cause a serious error such as a system down or a data loss. Confirm the appropriateness of the operation, and then input of the password.

Enter the login password for the maintenance account of the storage system, and then click the [OK] button.

4. A completion message is displayed. Click the [Close] button.



3.18 Reboot GUM

This is a window to restart the connected GUM.

This function is operated by service personnel.

- NOTE:
- To reboot GUM of the both controllers, perform the following procedure.
 1. Log into the Maintenance Utility of CTL1 and reboot GUM.
 2. Wait for about five minutes.
 3. Confirm that you can log into the Maintenance Utility of CTL1.
(If you cannot login, wait for one to two minutes and login again. Note that it might take up to 20 minutes until you can login)
 4. Log into the Maintenance Utility of CTL2 and reboot GUM.
 5. Wait for about five minutes.
 6. Confirm that you can log into the Maintenance Utility of CTL2.
(If you cannot login, wait for one to two minutes and login again. Note that it might take up to 20 minutes until you can login)
 - If the login window of the Maintenance Utility is not displayed, you cannot log into the Maintenance Utility or an error occurs when you try to reboot GUM, perform [“3.26 Resetting GUM”](#).
 - For influence of rebooting the GUM, see the NOTE in [“3.26 Resetting GUM”](#). (The influence of rebooting the GUM and the influence of resetting the GUM are the same.)

1. Connecting a maintenance PC

Connect the maintenance PC and the Storage System.

To reboot GUM (GUM1) of CTL1, connect the service PC and the Controller Board 1.

To reboot GUM (GUM2) of CTL2, connect the service PC and the Controller Board 2.

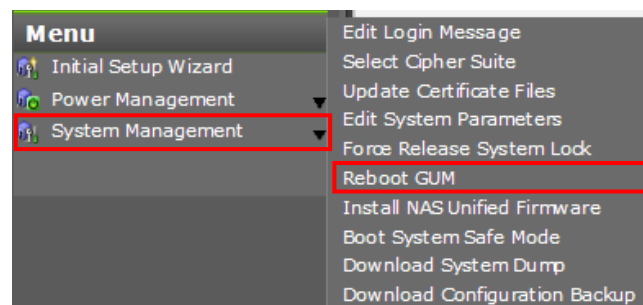
- Connect the maintenance PC and the Controller Board via LAN cable referring to [“2.2 Connecting Maintenance PC to Storage System”](#).

2. Starting Maintenance Utility

Start Maintenance Utility form the Maintenance PC.

3. Operation menu panel

Select [Reboot GUM] from [System Management].

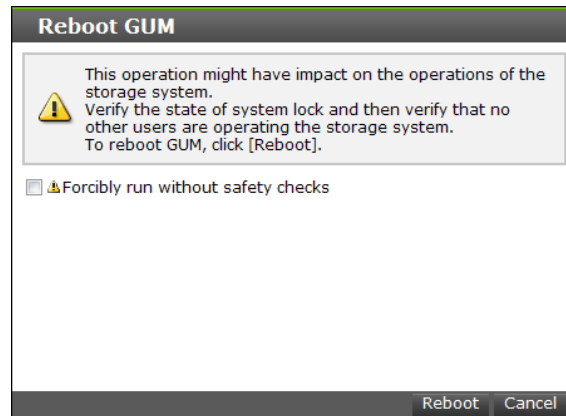


- Click the [Reboot] button.

CAUTION

About “Forcibly run without safety checks”:

If you check this checkbox and execute the maintenance, the system may go down. Do not check it unless instructed by the message, the manual or the contact described in the manual. This checkbox is displayed only when Maintenance Utility is started from the “Web Console” window or the “MPC” window.



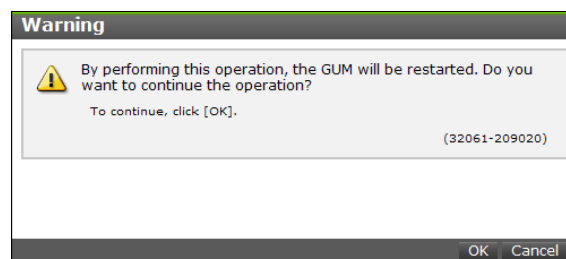
- Displaying the Password entry window

CAUTION

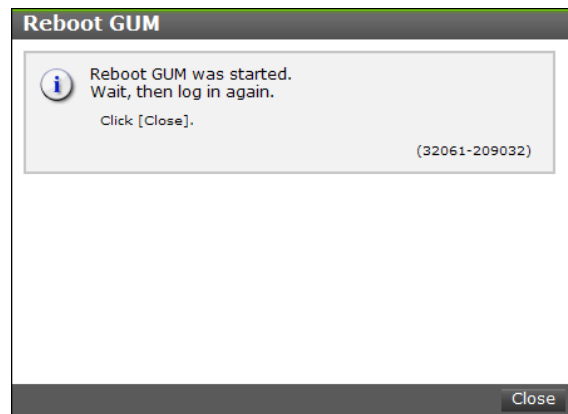
The Storage System operation might be affected. Confirm the appropriateness of the operation, and then input of the password.

Enter the login password for the maintenance account of the storage system, and then click the [OK] button.

- A confirmation message is displayed. Click the [OK] button.
Clicking the [Cancel] button returns to [Step 4](#).



7. A completion message is displayed. Click the [Close] button.



8. The GUM reboots automatically.
The logout window is displayed. Click the [X] button to close the window.

3.19 Change Password

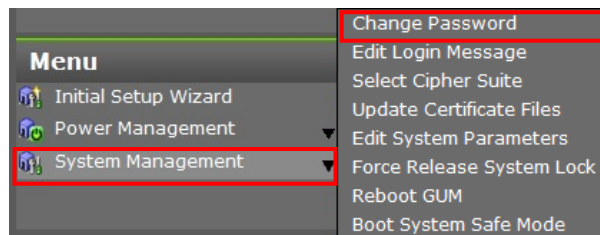
This is the window to change the password of the logged in user account.

This window is displayed only when specifying the IP address of the CTL on the browser (see [“2.7.3 Starting the Maintenance Utility Window by Specifying IP Address of CTL”](#)) and logging into the Maintenance Utility.

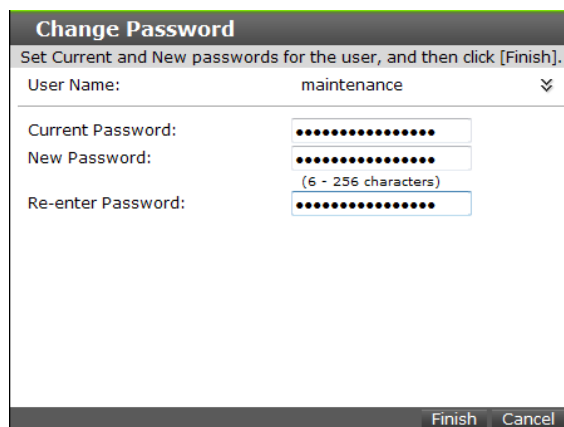
NOTICE: To change the user account specified by the registered storage system in the Storage Device List window, click Stop Service of the registered storage system. After changing the user account, click Edit to set the changed password. When the password was changed without performing Stop Service, Refer to [“2.13 Incorrect display errors”](#). When HCS (Hitachi Command Suite) is used, the information registered on HCS also needs to be changed. Change the information following the procedure described in “Changing storage system information” in Hitachi Command Suite User Guide.

1. Operation menu panel

Select [Change Password] from [System Management].



2. Enter the current password and a new password, and then click the [Finish] button.



3. A confirmation message is displayed. Click the [Apply] button.

Change Password

Verify the edited settings, and then click [Apply].

Edited User

User Name	maintenance	⌵
Password	*****	⌵


Back

Apply

Cancel

4. A completion message is displayed. Click the [Close] button.

Edit User

 Edit User was completed.
Click [Close].

(32461-209015)

Close

3.20 Boot System Safe Mode

This work is special (exceptional). If you perform this work without permission, the Storage System may go down.

When performing this work, contact the Technical Support Division for its validity and procedure.

3.21 Alert Display

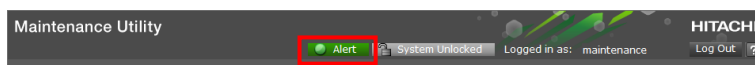
You can check “Alert” described in this section by referring to “[2] SIM Log ” of “5.3.1 Log Indication” and “Internal Alert” by “[1] SSB Log”.

When a storage system state is Alarm, Warning, Information, there may be an alert of non-reference. Of the main screen choose the [DKC] button, [GUM(CTL1)] button and [GUM(CTL2)] button among the [Alert] tab, and, please confirm whether there is not an alert of non-reference.

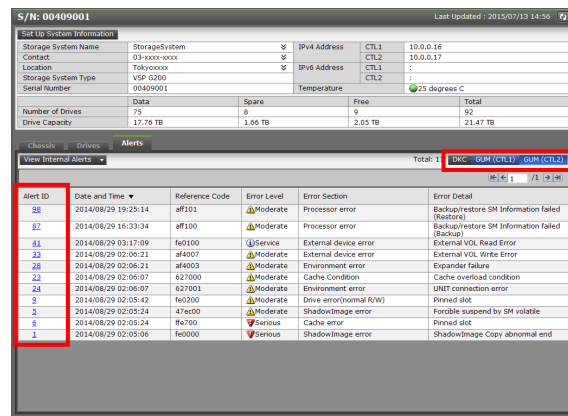
The warning information of the Storage System is displayed in the [Alerts] tab in the Maintenance Utility main window.

Refer to [Table 11-7](#) for the Storage System status.

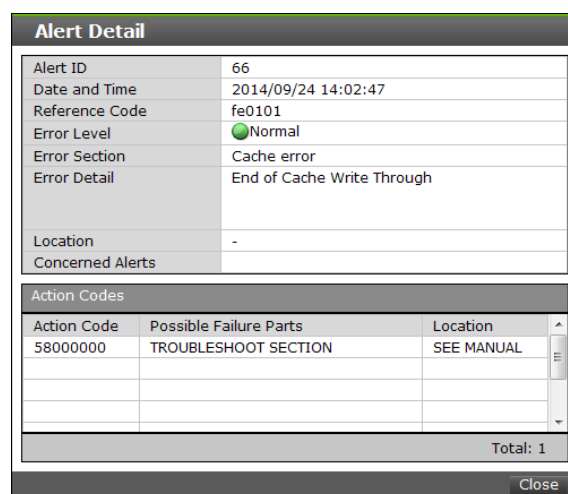
1. Clicking the [Alert] button displays the [Alerts] tab.



2. You can check the each DKC/GUM alert by clicking the [DKC] button, [GUM(CTL1)] button and [GUM(CTL2)] button. To check the internal alerts, go to [Step 4](#).



3. Clicking the link text of the alert ID displays the “Alert Detail” window. Check the alert contents. See SIM RC SECTION ([SIMRC00-00](#)) for the details of the displayed content.



4. <Check of Internal Alerts>

Select [Internal Alerts (DKC)] and [Internal Alerts (GUM)] from the [Refer to Internal Alert] pull-down menu of the [Alert] tab. See SSBLOG SECTION ([SSBLOG00-00](#)) for the details of the displayed content.

[Internal Alerts (DKC)]

[SSB] tab

Internal Alerts (DKC)

SSB
SSBS

Alert ID	Date and Time ▼	F/M	Error Code
23456	2014/01/02 12:59:59	x7	6789
23463	2014/01/02 10:59:59	x4	0156
23452	2014/01/01 23:59:59	x3	2345
23459	2014/01/01 23:59:59	x0	9012
23460	2014/01/01 22:59:59	x1	9023
23461	2014/01/01 21:59:59	x2	9034
23462	2014/01/01 20:59:59	x3	9045
23457	2014/01/01 15:59:59	x8	7890
			Total: 30

Close

[SSBS] tab

Internal Alerts (DKC)

SSB

SSBS

⏪

⏴

1

/4

⏵

⏩

Alert ID	Date and Time ▼	F/M	Error Code
23456	2014/01/02 12:59:59	x7	6789
23463	2014/01/02 10:59:59	x4	0156
23452	2014/01/01 23:59:59	x3	2345
23459	2014/01/01 23:59:59	x0	9012
23460	2014/01/01 22:59:59	x1	9023
23461	2014/01/01 21:59:59	x2	9034
23462	2014/01/01 20:59:59	x3	9045
23457	2014/01/01 15:59:59	x8	7890

Total: 30

Close

[Internal Alerts (GUM)]

[SSB(CTL1)] tab

Internal Alerts (GUM)

SSB (CTL1)

SSB (CTL2)

⏪ ⏩ 1 / 1138 ⏪ ⏩

Alert ID	Date and Time ▼	F/M	Error Code
123456	2014/01/02 12:59:59	x7	6789
123463	2014/01/02 10:59:59	x4	0156
123452	2014/01/01 23:59:59	x3	2345
123459	2014/01/01 23:59:59	x0	9012
123460	2014/01/01 22:59:59	x1	9023
123461	2014/01/01 21:59:59	x2	9034
123462	2014/01/01 20:59:59	x3	9045
123457	2014/01/01 15:59:59	x8	7890

Total: 10240

Close

[SSB(CTL2)] tab

Internal Alerts (GUM)

SSB (CTL1)

SSB (CTL2)

⏪
⏴
1
/1138
⏵
⏩

Alert ID	Date and Time ▼	F/M	Error Code
123456	2014/01/02 12:59:59	x7	6789
123463	2014/01/02 10:59:59	x4	0156
123452	2014/01/01 23:59:59	x3	2345
123459	2014/01/01 23:59:59	x0	9012
123460	2014/01/01 22:59:59	x1	9023
123461	2014/01/01 21:59:59	x2	9034
123462	2014/01/01 20:59:59	x3	9045
123457	2014/01/01 15:59:59	x8	7890

Total: 10240

5. <Check of Internal Alert Detail>

In the [Internal Alerts (DKC)] window or the [Internal Alerts (GUM)] window, click a link text of Alert ID. Then, the [Internal Alert Detail] window appears.

The internal alert data (448 bytes) is displayed in the Error Data field.

The 145th and later bytes in the internal alert data contain up to eight action codes of 4 bytes.

Internal Alert Detail	
Alert ID	613
Date and Time	2017/02/10 01:02:56
F/M	9f
Error Code	00f2
Concerned Alerts	
Error Data	<pre> 7503090E 341C8C00 34330000 00802000 00000000 000001F9 00000000 00000000 10000000 0000018C 00FF0000 00000080 00340000 0000FF8C 00000080 00000000 00000000 00000000 2E5C4473 766D6D61 696E2E63 00000000 00000000 00000000 F5110000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 5F000000 FFFFFFFF 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 </pre>

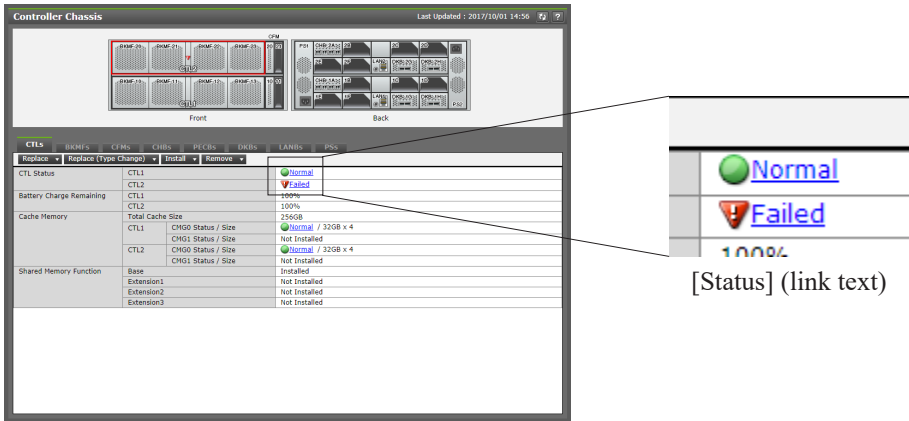
When 0xFFFFFFFF or 0x00000000 is displayed, no action code is contained.

See ACC (ACTION CODE) SECTION ([ACC00-00](#)) for the details of the displayed content.

3.22 Alert Display Related to FRU (Field Replacement Unit)

Among the alerts displayed in “3.21 Alert Display” in the “Maintenance Utility” window, the alerts possible to replace the specified hardware are displayed in the “Related Alerts” window.

- 1. Click [Status] (link text) of the hardware from the hardware menu in the “Maintenance Utility” window.
 - Display example of [Status] for the Controller Chassis (VSP G900).



For the [Status] (link text) field of each hardware, see the table below.

[In case of CBXS]

Part	Main window	Tab	Status
Controller Chassis	Controller Chassis window	[Drives] tab	[Status]
		[CTLs] tab	[CTL Status]
			[Battery Status]
			[Cache Memory] - [CTL1 Status], [CTL2 Status]
			[CFM Status]
			[Fan Status]
			[SFP Status] (*1)
Drive Box	Drive Box window	[PSs] tab	[Status]
		[Drives] tab	[Status]
		[ENCs] tab	[Status]
		[PSs] tab	[Status]

*1: When you click [SFP Status], the “Port Status” window is displayed, and then you can check the status of the port.
Clicking the [View Port Status] button of the CTL tab also displays the “Port Status” window.
When you click [SFP Status] on the “Port Status” window, the “Related Alerts” window is displayed.

[In case of CBSS/CBSL]

Part	Main window	Tab	Status
Controller Chassis	Controller Chassis window	[Drives] tab	[Status]
		[CTLs] tab	[CTL Status]
			[Fan Status]
			[CTL1 Status], [CTL2 Status]
		[CHBs] tab	[Status]
			[SFP Status] (*1)
		[BKMs] tab	[BKM Status]
			[Battery]-[Status]
Drive Box	Drive Box window	[CFMs] tab	[Status]
		[PSs] tab	[Status]
		[Drives] tab	[Status]
		[ENCs] tab	[Status]
		[PSs] tab	[Status]

*1: When you click [SFP Status], the “Port Status” window is displayed, and then you can check the status of the port.

To check the status of all ports, click the [View Port Status] button on the [CHBs] tab.

When you click [SFP Status] on the “Port Status” window, the “Related Alerts” window is displayed.

[In case of CBLH1]

Part	Main window	Tab	Status
Controller Chassis	Controller Chassis window	[CTLs] tab	[CTL Status]
			[CMG0 Status], [CMG1 Status]
			[BKMfS Status]
		[BKfMs] tab	[Battery]-[Status]
			[Status]
		[CFMs] tab	[Status]
		[CHBs] tab	[Status]
			[SFP Status] (*1)
Drive Box	Drive Box window	[DKBs] tab	[Status]
		[LANBs] tab	[Status]
		[PSs] tab	[Status]
		[Drives] tab	[Status]
		[ENCs] tab	[Status]

*1: When you click [SFP Status], the “Port Status” window is displayed, and then you can check the status of the port.

To check the status of all ports, click the [View Port Status] button on the [CHBs] tab.

When you click [SFP Status] on the “Port Status” window, the “Related Alerts” window is displayed.

[In case of CBLH2]








Part	Main window	Tab	Status
Controller Chassis	Controller Chassis window	[CTLs] tab	[CTL Status]
			[CMG0 Status], [CMG1 Status]
		[BKFM]s tab	[BKMFs Status]
			[Battery]-[Status]
		[CFMs] tab	[Status]
		[CHBs] tab	[Status]
			[SFP Status] (*1)
		[PECBs] tab	[Status]
		[DKBs] tab	[Status]
Drive Box	Drive Box window	[LANBs] tab	[Status]
		[PSs] tab	[Status]
		[Drives] tab	[Status]
		[ENCs] tab	[Status]
Channel Board Box	Channel Board Box window	[PSs] tab	[Status]
			[Status]
		[CHBs] tab	[Status]
		[SWPKs] tab	[SFP Status] (*1)
			[Status]
		[FANs] tab	[Status]
		[PCPs] tab	[Status]
		[PSs] tab	[Status]

*1: When you click [SFP Status], the “Port Status” window is displayed, and then you can check the status of the port.

To check the status of all ports, click the [View Port Status] button on the [CHBs] tab.








When you click [SFP Status] on the “Port Status” window, the “Related Alerts” window is displayed.

- The followings are displayed in [Status].

[Status]	Description	Parts frame color	Status icon
Normal	<p>This indicates normal status.</p> <p>But the latest status might not be reflected due to failures of other related parts.</p> <p>If failures in other related parts are notified, the latest status is reflected by replacing the failed parts.</p>	None	
Warning	<ul style="list-style-type: none"> Parts failures are suspected. This might be displayed due to failures of other related parts. If this is caused by the failures of other related parts, the latest status is reflected by replacing the failed parts. In the case of Warning of BKM and BKMF, “?” is displayed in the Battery Lifespan Remaining column. After the warning is resolved, “?” returns to a numerical value. 	Amber	
Failed	<p>The parts are broken.</p> <p>[Drive Status-limited]</p> <ul style="list-style-type: none"> Parts failures are suspected. This might be displayed due to failures of other related parts. If this is caused by the failures of other related parts, the latest status is reflected by replacing the failed parts. 	Red	
Blocked	Only parts needed the blockage instruction by using Maintenance Utility are displayed, and the parts are in an exchangeable status.	Red	
Not fix	<p>[SFP Status-limited]</p> <p>The classification is in an undetermined status.</p>	None	
Warning (Port n failed)	<p>[Drive Status-limited]</p> <p>The drive port is in a failure status.</p> <p>n: Failure drive port number</p>	Amber	
Copying n % (TYPE to DRIVE)	<p>[Drive Status-limited]</p> <p>Copying is in progress.</p> <p>When multiple copy statuses exist, a line break is added to every copy status line, and then the information is displayed.</p> <p>n: Copy progress rate</p> <p>TYPE: “Correction copy” “Copy back” “Dynamic sparing” “Drive copy”</p> <p>DRIVE: Copy destination drive location (If the drive is a copy destination drive in “Correction copy”, DRIVE is displayed as “this Drive”.)</p>	Amber	

(To be continued)

(Continued from preceding page)

[Status]	Description	Parts frame color	Status icon
Copying n % (TYPE from DRIVE)	[Drive Status-limited] Copying is in progress. When multiple copy statuses exist, a line break is added to every copy status line, and then the information is displayed. n: Copy progress rate TYPE: "Copy back" "Dynamic sparing" "Drive copy" DRIVE: Copy source drive location	Amber	
Pending (TYPE to DRIVE)	[Drive Status-limited] Copying is in a suspended status. When multiple copy statuses exist, a line break is added to every copy status line, and then the information is displayed. TYPE: "Correction copy" "Copy back" "Dynamic sparing" "Drive copy" DRIVE: Copy destination drive location (If the drive is a copy destination drive in "Correction copy", DRIVE is displayed as "this Drive".)	Amber	
Pending (TYPE from DRIVE)	[Drive Status-limited] Copying is in a suspended status. When multiple copy statuses exist, a line break is added to every copy status line, and then the information is displayed. TYPE: "Copy back" "Dynamic sparing" "Drive copy" DRIVE: Copy source drive location	Amber	
Copy incomplete	[Drive Status-limited] Copying is in an incomplete status.	Amber	
Reserved	[Drive Status-limited] The spare disk is in an unusable status.	Amber	
Available (Connected)	This port is implemented and in use.	None	
Available (Not Connected)	This port is implemented and enabled.	None	
Not Available	This port is either not implemented or disabled.	None	None

- The “Related Alerts” window is displayed. Among the alerts detected by the Storage System, the alerts possible to replace the selected hardware are displayed on the list.

Related Alerts				
Alerts Related to : CTL1				
Related Alerts				
Alert ID	Date and Time ▼	Reference Code	Error Level	Error Section
244	2014/9/5 21:00:33	180100	Critical	Audit Log
243	2014/9/5 21:00:32	180000	Critical	Audit Log
242	2014/9/5 21:00:31	af0080	Critical	Environmental error
241	2014/9/5 21:00:30	af8060	Critical	Environmental error
240	2014/9/5 21:00:29	af6040	Critical	Environmental error
239	2014/9/5 21:00:28	af5020	Critical	Environmental error
238	2014/9/5 21:00:27	af2000	Critical	Environmental error
237	2014/9/5 21:00:26	39a000	Critical	Environmental error
236	2014/9/5 21:00:25	610002	Critical	Processor error
235	2014/9/5 21:00:24	610001	Critical	Processor error
				Total: 39
Close				


The conditions to be displayed in the “Related Alerts” window are as shown below. If the alerts do not meet the following conditions, they are not displayed in the “Related Alerts” window. Therefore, refer to the “Alerts” window (refer to [“3.21 Alert Display”](#)) to check them.

[Conditions to be displayed in the “Related Alerts” window]

- Only the alerts including the specified parts and the internal parts in the action codes are displayed. (You can check the actions codes in the “Alert Detail” window in [Step 3.](#))
For example, the alerts of which the action codes are only manual reference are not displayed in the “Related Alerts” window.
- The 257th alert and older from the most recent alert are not displayed.
- Among the alerts displayed in the “Related Alerts” window, the alerts detected one hour or more before the most recent alert are not displayed.

When the alerts are not displayed in the “Related Alerts” window or the failures are not recovered even if handled in accordance with the displayed alerts, refer to the “Alerts” window (refer to [“3.21 Alert Display”](#)) and identify the cause of the failures.

- Clicking the link text of the alert ID displays the “Alert Detail” window.

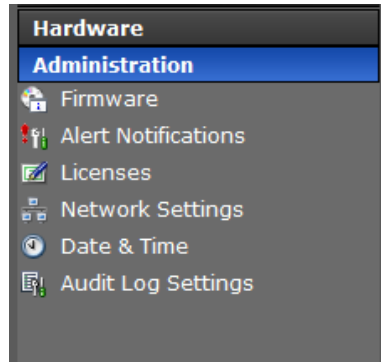
Alert Detail	
Alert ID	235
Date and Time	2014/01/01 10:59:59
Reference Code	473040
Error Level	 Acute
Error Section	Pair volume status error
Error Detail	HRC pair status change(MCU command), COPY -> PAIR
Location	BKMF-14
Concerned Alerts	

Action Codes		
Action Code	Possible Failure Parts	Location
41800100	CTL	CTL2
		Total: 1

Close

3.23 Management Menu

The items in the Administration menu of Maintenance Utility are shown below.



Item	Menu	Description
User Administration	(User Administration)	Set registration/change of the user. (See “3.3 User Administration” .)
Alert Notifications	Alert Notifications	Set an alert notice. (See “3.4 Alert Notifications” .)
Audit Log Settings	Audit Log Settings	Set an audit log. (See “3.8 Audit Log Settings” .)
Licenses	Licenses	Set license management. (See “3.7 Setting up License Keys” .)
Firmware	Firmware	Check the version of each firmware, and set the version management of each firmware. (See “3.2 Firmware” .)
Network Settings	Network Settings	Set a network. (See “3.6 Network Setting” .)
Date & Time	Date & Time	Set a date. (See “3.5 Time Setting” .)

3.24 Power Supply Management

1. Clicking the [Menu] item opens menus.

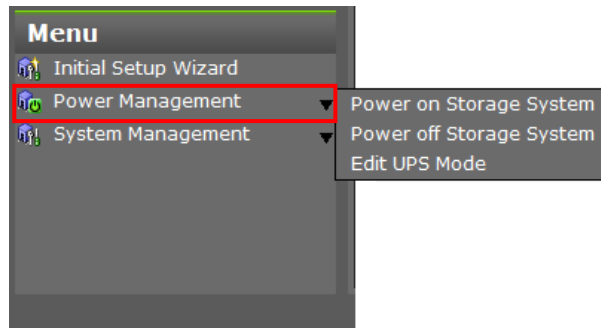


Table 3-1 List of Power Management Menus

Operation Panel	Menu	Description
Power Management	Power on Storage System (*1)	Power ON of the Storage System. (See “3.10 Power on Storage System” .)
	Power off Storage System	Power OFF of the Storage System. (See “3.11 Power off Storage System” .)
	Edit UPS Mode	Edit the UPS mode. (See “3.12 Edit UPS Mode” .)

*1: When turning off the Storage System power by the main switch, you cannot perform [Power on Storage System] from the [Power Management] menu.

3.25 System Management

Clicking the [Menu] item opens menus.

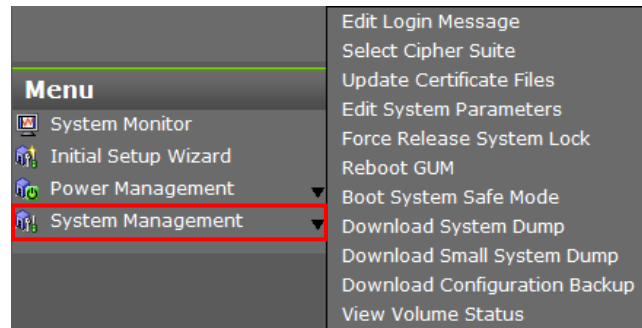


Table 3-2 List of System Management Menus

Operation Panel	Menu	Description
System Management	Edit Login Message	Edit login messages
	Select Cipher Suite	Select Cipher Suite
	Update Certificate Files	Update certificates
	Edit System Parameters	Edit system parameters
	Force Release System Lock	Release the system lock
	Reboot GUM	Reboot GUM
	Change Password	Change password
	Boot System Safe Mode	Switch to System Safe Mode
	Download System Dump	Download the dump files. For details on system dump and small system dump, refer to “5.2 Dump” .
	Download Small System Dump	
	Download Configuration Backup	Collect Configuration backup
	View Volume Status	Check whether pinned track (failed track) and blocked LDEV exist

3.26 Resetting GUM

This is the procedure to reset GUM by force.

This function is operated by service personnel.

- NOTE:
- Do not perform this procedure except the cases when [“3.18 Reboot GUM”](#) cannot be performed, or instructions in the troubleshooting and from the Technical Support Division.
 - When GUM is reset, the connection to the network is disconnected. Consult with the customer, and then perform this procedure.
 - If you perform this procedure while updating the GUM firmware, the controller failure might occur. Do not perform this procedure while updating the firmware. To confirm whether the firmware is updating, you can check whether the message that indicates the firmware is updating is displayed in the Maintenance Utility of the Controller 1 or the Controller 2 when the login button or the update button is pressed.
 - Resetting the GUM disconnects the connection to the network. Then, the communication with Storage Navigator is temporarily stopped and automatically started again.

1. See the LOCATION SECTION [“3.2 Other Switches and LEDs”](#) and confirm the location of the LAN-RST switch.
2. Press the controller LAN-RST switch that resets GUM for around one second (any sharp object such as a pen tip is necessary).
3. Wait for around five minutes.
4. Confirm that you can log into the Maintenance Utility of the reset controller (If you cannot login, retry after waiting for one to two minutes. Note that it might take up to 20 minutes until you can login.)
5. If you cannot login even after waiting for 20 minutes, press the LAN-RST switch again for one second and perform the [Step 4](#). If you cannot still login, contact the Technical Support Division.

NOTE: If GUM of the both controllers need to reset, perform the above resetting GUM procedure from the [Step 1](#) to [Step 5](#) for the other controller as well.

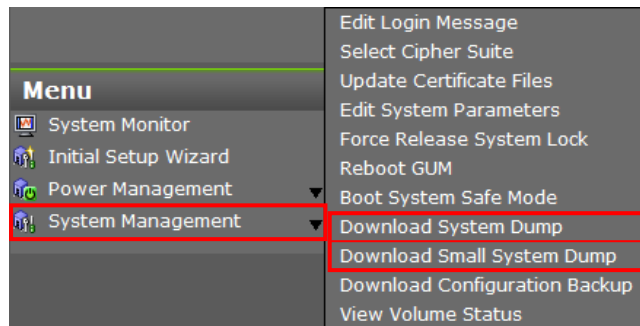
3.27 Acquiring Dumps using Maintenance Utility

The following procedure describes how to acquire system dumps and small system dumps from Maintenance Utility. For details, refer to “5.2 Dump”.

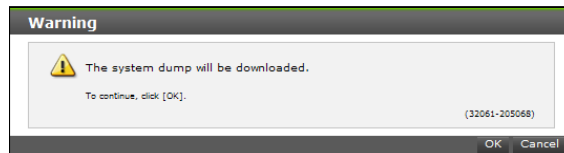
NOTICE: Confirm with the service personnel that AutoDump is not performed on the Maintenance PC. If this function is used in the status that AutoDump is performed on the Maintenance PC, the acquired dump data might be lost.

1. Operation menu panel

Select [Download System Dump] or [Download Small System Dump] from [System Management].



2. A warning message is displayed. Click the [OK] button.



3. The white window or the security confirmation window is displayed.

If the certificate is invalid at the time of the https connection, the security confirmation window is displayed, select “Continue to this website (not recommended)”.

NOTICE: Do not close the white window or the security confirmation window until the dump download is completed. The dump download may fail.

4. Wait for two or three minutes, and then the file download window is displayed.

NOTICE:

- The file download window is displayed in the Maintenance Utility window. If the Maintenance Utility window is hidden in the while window or the security confirmation window, click the Maintenance Utility window to check the download window.
- The form of the file download window varies depending on the browser.
- Depending on the browser setting, the file download might be started without displaying the file download window.

5. Click [Save as] in the file download window.

6. Enter a download destination and a file name, and then click [Save] button.

NOTE: Giving the serial number to the file name is recommended. (Example: When the serial number is 832000400001, the file name is hdcp_dump_832000400001.dmp.)
To collect dumps continuously, change the dump file name not to be overwritten.

7. Confirm the download progress.

NOTICE:

- Because files to be downloaded are generated dynamically, the file size in the estimated file transfer completion time are unknown or hidden.
- File downloading might not be transferred for about a few minutes, but no problem with this because it takes time to switch the CTL in the dump file source.
- The time of downloading files depends on the network speed.

8. Confirm the completion of the download.

NOTICE: Close the white window or the security confirmation window manually when the window remains.

9. Check that the dump file is stored in the following [Storage Destination].

[Storage Destination]: The dump file with the specified file name is stored in the storage destination specified in [Step 6](#).

3.28 Obtaining Configuration Information Backup

3.28.1 Configuration Information Backup Function

The configuration information is automatically backed up at the timing shown below.

Backup execution timing	Description
(1) Backup at the timing of change	Executed every time the configuration information is changed by setting operations.
(2) Periodic backup	Automatically executed once a day. The execution time is the synchronizing time with the NTP server which is set in the "Set Up Date & Time" window. If the NTP server is not used, the backup is executed at 0:00.

The backup file is stored in DKC. When the backup (2) is executed, the backup file stored in DKC is copied to GUM. Four-generation backup files are stored in GUM.

Therefore, immediately after the execution of the backup (2), the latest backup files exist in both DKC and GUM. When the backup (1) is executed, only the backup file stored in DKC is updated.

Storage location	Number of generations for storage
DKC	One generation (the latest one)
GUM	Four generations

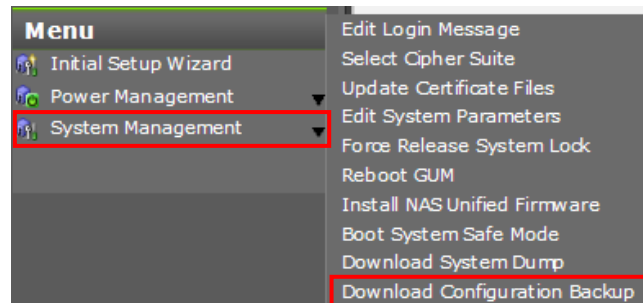
The backup files stored in DKC or GUM can be downloaded using Maintenance Utility. (See ["3.28.2 Downloading Configuration Information Backup File"](#)).

3.28.2 Downloading Configuration Information Backup File

The configuration information backup files stored in DKC or GUM can be downloaded using Maintenance Utility.

1. Operation menu panel

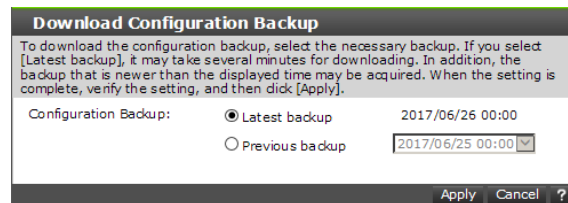
Select [Download Configuration Backup] from [System Management].



2. Download Configuration Backup

Download the configuration information backup.

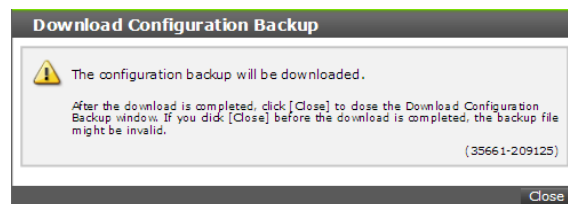
Select a necessary backup on the window shown below.



NOTE: The latest backup can be selected only when the Storage System is in the Ready status.

3. Check the download of the configuration information backup.

NOTE: Clicking the [Close] button before the download is complete (before the file is saved) might cause the backup file to be in an abnormal state.



3.29 Checking Existence of Pinned Track and Blocked LDEV

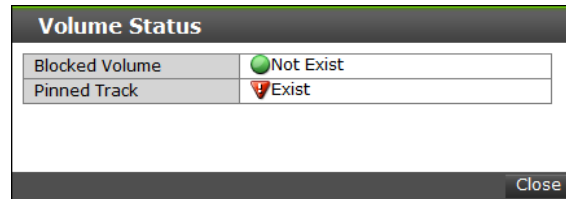
Check whether the pinned track (failed track) and the blocked LDEV exist.

1. Operation menu panel

Select [View Volume Status] from [System Management] in the Maintenance Utility window.

2. Results display

The following window is displayed.




Item	Description
Blocked volume	<ul style="list-style-type: none">• Not Exist No LDEVs are in blocked status.• Exist The LDEVs in blocked status exist. To identify the blocked LDEV, use the “Logical Devices” window selected from the [Storage Systems] tree in the Web Console window. The [Status] column for the blocked LDEV displays “Blocked”. To filter the [Status] column, specify [Status] in the filtering condition. For details about how to perform the filtering, refer to “System Administrator Guide”.
Pinned track	<ul style="list-style-type: none">• Not Exist No pinned tracks exist.• Exist The pinned tracks exist. To check the detailed information about the pinned tracks, refer to “5.12.3 Pin Data Indication”.

4. Storage System Management Function

4.1 Connecting to the Host

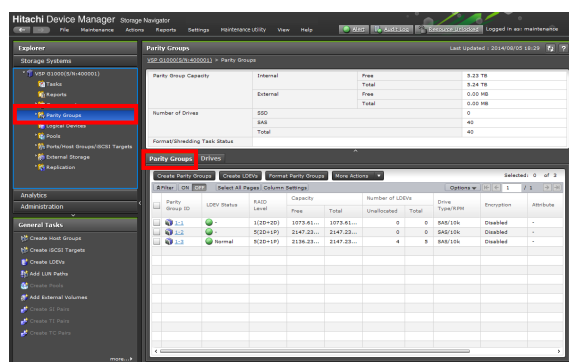
4.1.1 Creating Parity Groups

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 the [Refresh] button ().

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.

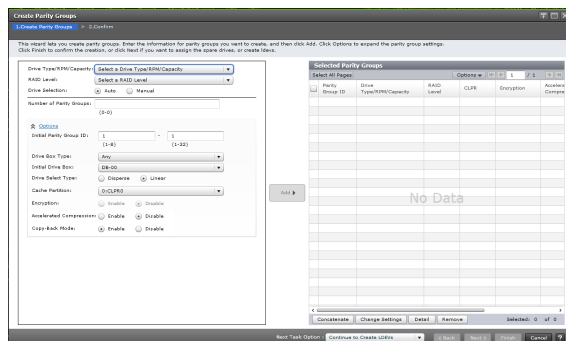


Item	Description
Parity Group ID	Number of the parity groups
LDEV Status	A status of all the devices in the parity group
RAID Level	RAID level specified.
Capacity-Free	Available capacity of the parity group
Capacity-Total	Entire capacity of the parity group
Number of LDEVs-Unallocated	The number of the 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/RPM	Drive type 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.
Copy-Back Mode	Copy-Back Mode
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 the [Create Parity Groups] button.

- Enter the information (drive type/PRM/capacity, RAID level, drive selection, and number of parity groups) of the parity group to be created and click the [Add] button. Click Options to expand the parity group settings. Click the [Next] button.

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



Item	Description
Drive Type/RPM/Capacity	Select the type of the drive box.
RAID level	Select the RAID level.
Drive Selection	Select the mode of the drive selection from Auto or Manual.
Number of Parity Groups	Enter the number of parity groups. This item appears when selected Auto as your drive selection.
Available Drives	This item appears when selected Manual as your drive selection. For drives to be incorporated to a parity group, set the checkbox of a row to ON. <ul style="list-style-type: none"> • Location: Displays the location of the drive box. • Drive Box: Displays the name of the drive box. • Drive Box Type: Displays the type of the drive box. • Drive Type-Code: Displays the type code of the drive box.
The number you have to select	Displays the number of drives that you must select. This item appears when selected Manual as your drive selection.
Initial Parity Group ID	Enter the parity group ID. Text box on the left side: Enter the numeric characters, which are the fixed characters that are placed at the beginning of the parity group ID. Text box on the right side: Enter the initial number following the prefix name.
Drive Box Type	Select the type of drive box. This item appears when selected Auto as your drive selection.
Initial Drive Box	This item appears when selected Auto as your drive selection. The smallest available number is entered in the text box as a default. No number appears in the text box if no available parity group ID exists. If you specify the parity group ID which is already used, the minimum parity group ID after that the specified parity group ID is automatically set.

(To be continued)

(Continued from preceding page)

Item	Description
Drive Select Type	<p>This item appears when selected Auto as your drive selection. Select the method for the selecting of drives in a parity group.</p> <ul style="list-style-type: none"> • Disperse: Selected drives where are located dispersedly. • Linear: Selected drives where are located linearly. <p>This item is not available with VSP G130, G350, G370 and VSP F350, F370. In VSP G130, G350, G370 and VSP F350, F370, [Linear] is set by default.</p>
Cache Partition	Select a CLPR number which is displayed as ID:CLPR.
Encryption	<p>Specify if encrypted parity groups are created.</p> <ul style="list-style-type: none"> • Enable: Encrypted parity groups are created. • Disable: Non-encrypted parity groups are created.
Accelerated Compression	<p>Specify if the Accelerated Compression is set to parity groups. (*1)</p> <ul style="list-style-type: none"> • Enable: The Accelerated Compression is set to parity groups. • Disable: The Accelerated Compression is not set to parity groups.
Copy-Back Mode	<p>Specify if the Copy-Back Mode is set to parity groups.</p> <ul style="list-style-type: none"> • Enable: The Copy-Back Mode is set to parity groups. • Disable: The Copy-Back Mode is not set to parity groups.
[Add] button	When you click Add, the configured information is added to the right side of the Selected Parity Groups table.
[Next Task Option] bull-down	Click [Next] button to go to the task setting window, which is indicated in Task Next Option.

*1: Existing parity groups can have Accelerated Compression enabled non-destructively with data-in-place. For the detailed procedure, see "Provisioning Guide".

4. The Assign Spare Drives window appears.

Select a spare drive from the Available Drives list, and then click Add.

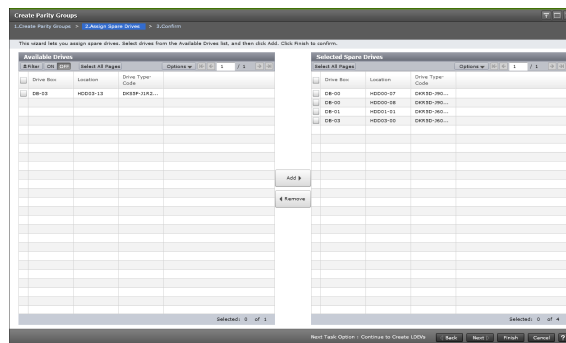
The selected spare drive was added to the Selected Spare Drives list. Click the [Next] button.

NOTE: When you want to complete the spare drive creation, click the [Finish] button.

NOTE: You can also assign the spare drives in the following procedure (see [“4.2.1.3 Allocating/Deleting Spare Drives”](#)).

1. Select [Storage system]-[Parity Groups].
2. Click [Assign Spare Drives in the Drives] tab.

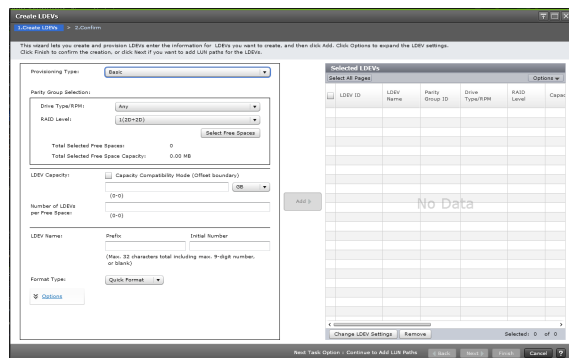
NOTE: If the capacity of a drive exceeds the capacity of a spare in the Storage System, an error message appears.



[Available Drives] table and [Selected Spare Drives]

Item	Description
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. 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 the [Next] button.



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 “4.2.3 Managing Logical Device”).

1. Select [Storage Systems]-[Logical Device].
2. Click [Create LDEVs] in the LDEVs] tab.

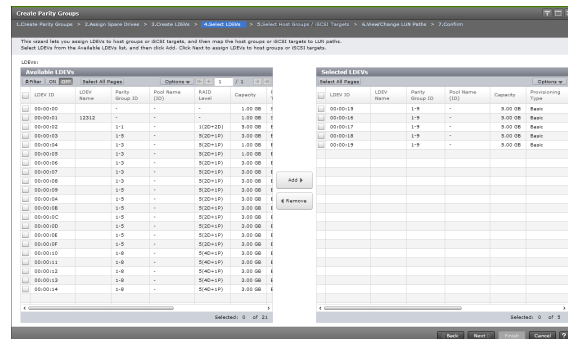
Item	Description
Provisioning Type	Select the type of LDEV. Basic: Internal volume. Dynamic Provisioning: DP-VOL. External: External volume. Snapshot: Thin Image volume. ALU: LDEV of the ALU attribution.
Drive Type/RPM	Select the data drive type and RPM. Any: All types of disk drives and RPMs that can be contained in the system. SSD: Includes SLC/MLC for SSD, and FMD. SAS/RPM: SAS drive and RPM. External Storage: External storage system. Mixed: Mixes the data drive type.
RAID Level	Select the RAID level. External Storage is selected from the Drive Type/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	<ul style="list-style-type: none"> 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. <p>Detailed calculation of the LDEV capacity differs depending on the specification of the unit. For details, see "Provisioning Guide".</p>
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	<p>LDEV name. Specify the prefix characters and the initial number.</p> <ul style="list-style-type: none"> Prefix: A fixed character string. Initial Number: The initial number of the LDEV name. <p>Specify the initial number according to the examples below. You can specify up to 32 characters total.</p> <p>Example:</p> <ul style="list-style-type: none"> 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	<p>Specify the format type. This appears when an internal or external volume is used.</p> <p>Quick Format: Quick formatting is the default format type. You cannot select this when the provisioning type is something other than the internal volume.</p> <p>Normal Format: Normal formatting.</p> <p>Parity Group Format: Format the parity group. You can select this when no LDEV exists in the parity group.</p> <p>No Format: Volumes are not formatted.</p>
Initial LDEV ID	<p>Specify the LDEV ID. LDKC is fixed to 00. Default of CU and DEV is 00:00.</p> <p>For creating multiple LDEVs, select the interval of the assigned LDEV ID from the Interval list.</p>
View LDEV IDs	Displays the View LDEV IDs windows.
MP Unit ID	<p>Specify the MP unit you want to assign to the LDEV. Select Auto or an arbitrary ID. The default is Auto.</p> <p>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.</p> <p>If Auto is enabled, the default is Auto. If Auto is disabled, the default is the lowest number of the MP unit.</p>
T10 PI	<p>Sets the T10 PI attribute of the LDEV.</p> <p>[Enabled]: Enables the T10 PI attribute of the LDEV.</p> <p>[Disabled]: Disables the T10 PI attribute of the LDEV.</p> <p>This function is [Provisioning Type] and it can be set when any of [Basic], [DP], and [Snapshot] is selected.</p>

6. The “Select LDEVs” window appears.

Select a LDEV from the [Available LDEVs] list, and then click [Add] button.

The selected LDEV was added to the [Selected LDEVs] list. Click [Next] button.



[Available LDEVs] table and [Selected LDEVs] table

Item	Description
LDEV ID	LDEV identifiers. LDEV IDs may 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)

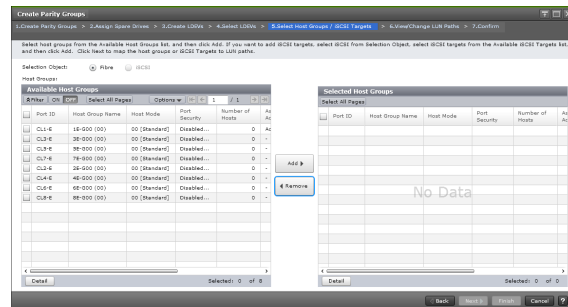
(Continued from the preceding page)

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.

7. The “Select Host Groups” window appears.

Select a host group from the [Available Host Groups] list, and then click the [Add] button.

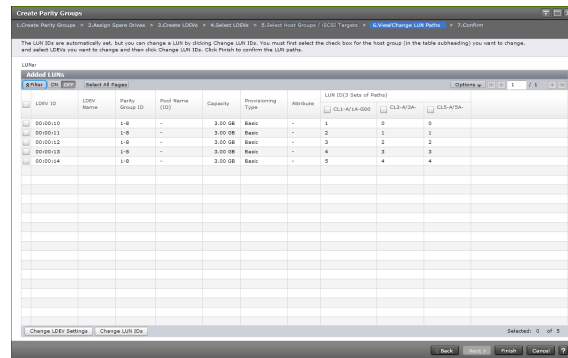
The selected LDEV was added to the [Selected Host Groups] list. Click the [Next] button.



[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.

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



[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. -: 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.

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

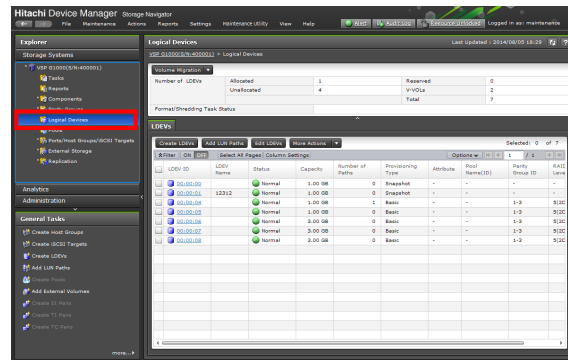
10. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

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

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

4.1.2 Checking the Logical Devices

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



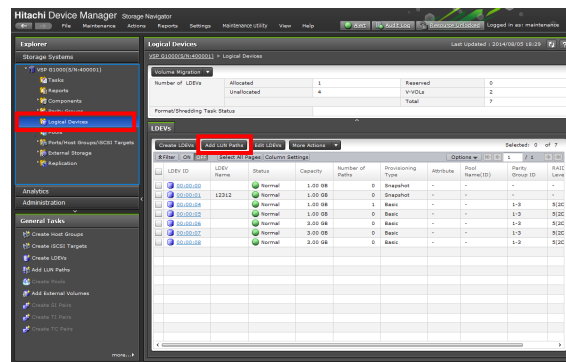
Item	Description
LDEV ID	Number of the logical device
LDEV Name	LDEV name
Status	A status of the logical device
Capacity	Available capacity of the parity group
Number of Paths	The number of the logical devices path
Provisioning Type	A type of the logical device
Attribute	An Attribute of the logical device.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

4.1.3 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.

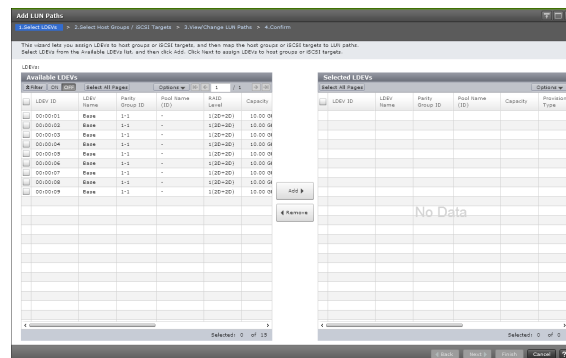
1. Select [Storage Systems]-[Logical Devices].



2. Click the [Add LUN Paths] button.

3. The “Select LDEVs” window appears.

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



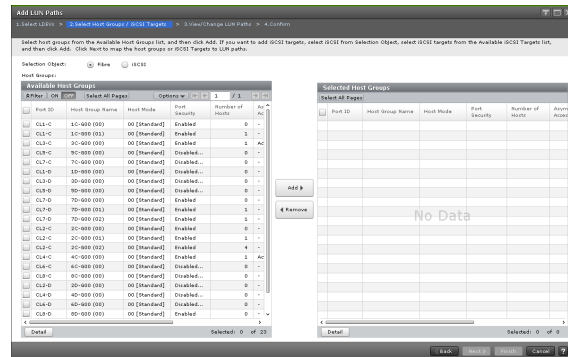
[Available LDEVs] table and [Selected LDEVs] table

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. -: 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 the [Add] button.

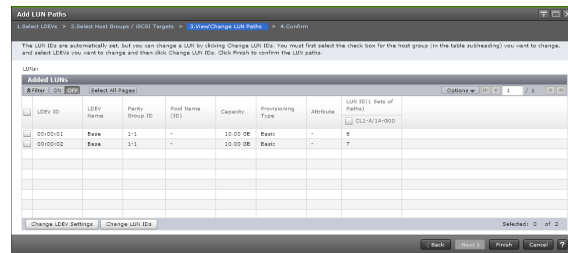
The selected LDEV was added to the [Selected Host Groups] list or the [Select iSCSI Targets] list. Click the [Next] button.



[Available Host Groups] table and [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 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.
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.

5. The “Add LUN Path” window is displayed. Check the settings and click the [Finish] button.
6. The “View/Change LUN Paths” window appears. Confirm the settings, and then click the [Next] button.



[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. -: 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 the [OK] 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].

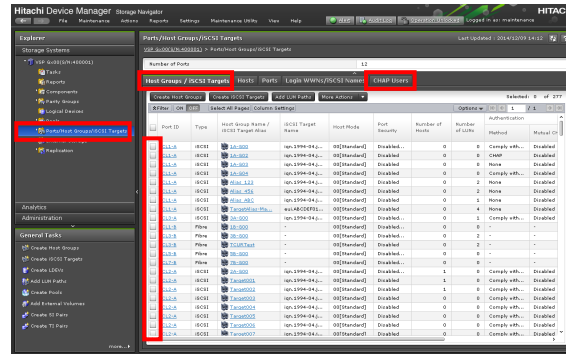
9. Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

4.1.4 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.

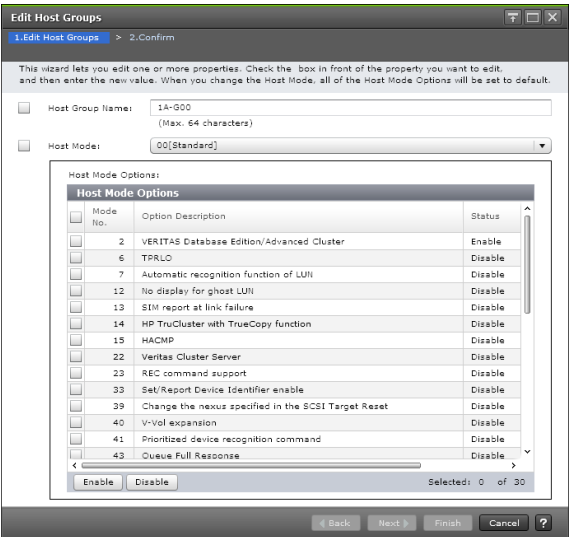
4.1.4.1 Editing Host Group

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



2. Check the [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 the [Finish] button.



Item	Description
Host Group Name	<p>Specify the name of the host group.</p> <p>Host group name can be up to 64 single-byte ASCII characters (alpha-numerals and symbols).</p> <p>You cannot use the following symbols: \ / : , ; * ? " < > </p> <p>You cannot use blanks at the beginning or end of the host group name.</p> <p>If a host group assigned to an initiator port is included in the specified host groups, this item is unavailable.</p>
Host Mode	<p>Select the host mode from the list.</p> <p>If a host group assigned to an initiator port is included in the specified host groups, this item is unavailable.</p>
Host Mode Options	<p>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.</p>
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.

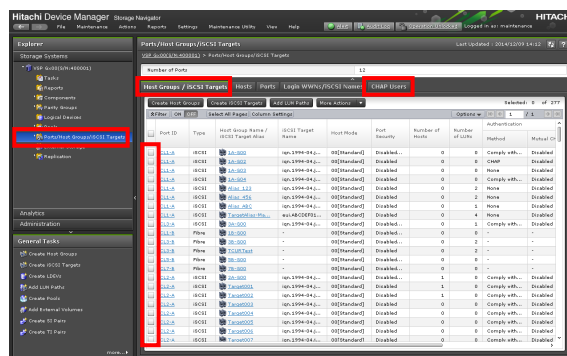
NOTE: To display the “Task” window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

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

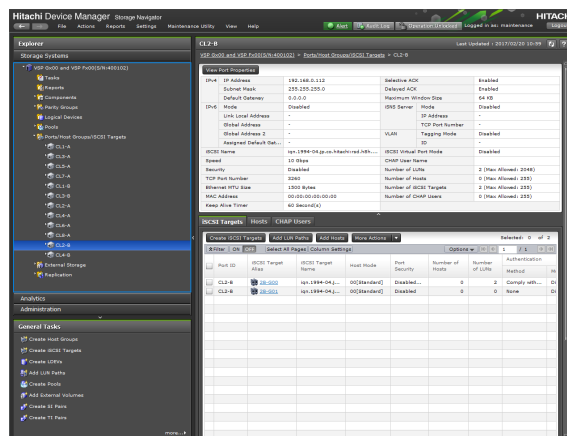
4.1.4.2 Editing iSCSI Target

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 the [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 the [Finish] button.

This wizard lets you edit one or more properties. Check the box in front of the property you want to edit, and then enter a new value. If you change the Host Mode, all of the Host Mode Options will be set to default.

☐ iSCSI Target Alias: 1B-G00 (Max: 32 characters)

☐ iSCSI Target Name: ☐ iqn ☒ eui eui: 1234567890123456 (16 characters)

☐ Host Mode: 01[VMware]

Host Mode Options:

Mode No.	Option Description	Status
2	VERITAS Database Edition/Advanced Cluster	Enable
6	TPRLO	Enable
7	Automatic recognition function of LUN	Enable
12	No display for ghost LUN	Enable
13	SIH report at link failure	Enable
14	IBM WebStorage Manager Extension	Enable

Enable Disable Selected: 0 of 30

☐ Authentication Method: None

☐ Mutual CHAP: ☒ Enable ☐ Disable

☐ User Name: (Max: 223 characters)

☐ Secret: (12 ~ 32 characters)

Re-enter Secret:

Back Next Finish Cancel ?

Item	Description
iSCSI Target Alias	Display an iSCSI target alias. Up to 32 alphanumeric characters and symbols (! # \$ % & ' + - . = @ ^ _ { } ~ () [] space)
iSCSI Target Name	[iqn] or [eui]: Select either format. Text box: Enter an iSCSI target name. <ul style="list-style-type: none"> 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.

4.2 Managing Drives

4.2.1 Setting Spare Drives

This setting is used to set, delete and reference a spare drive.

The drive that can be set as the spare drive is a data drive.

4.2.1.1 Guidelines When Allocating Spare Drives

- If it is operated in the Copy backless setting, the drive positions which configure the parity groups are replaced due to the drive failure recovery
- The following shows the maximum installation number of spare drives per Storage System.

CBXSS/CBXSL/CBSS1/CBSL1: 16 spare disks

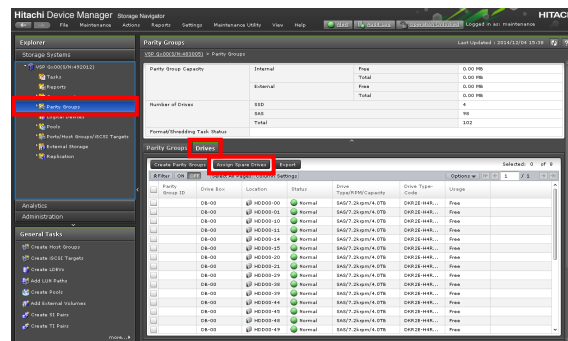
CBSS2/CBSL2: 24 spare disks

CBLH1: 48 spare disks

CBLH2: 64 spare disks

4.2.1.2 Checking Spare Drive

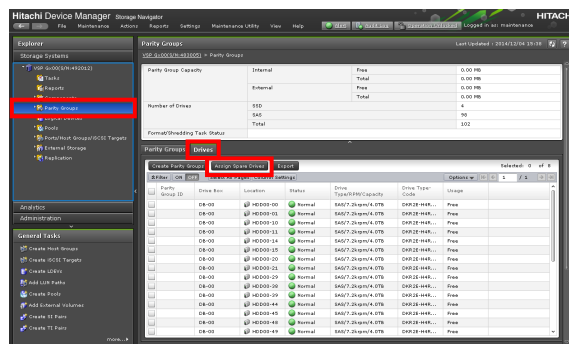
1. In the Web Console window, select [Storage Systems]-[Parity Groups].
2. Click the [Drives] tab. Check the Usage is specified “Spare”.



Item	Description
Parity Group ID	Number of the parity groups
Drive Box	Drive Box
Location	Location of the spare drive
Status	A status of the drive
Drive Type/RPM/ Capacity	Displays the drive type, round-per-minute (RPM), and capacity.
Drive type code	Display a drive type code
Usage	Usage of the drive

4.2.1.3 Allocating/Deleting Spare Drives

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



2. Click the [Allocate Spare Drives] button.

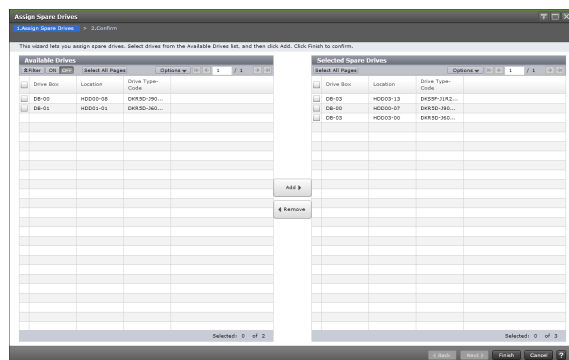
3. The "Assign Spare Drives" window appears.

When assigning spare drives, select a spare drive from the [Available Drives] list, and then click the [Add] button.

The selected spare drive was added to the [Selected Spare Drives] list.

When deleting spare drives, select a spare drive from the [Selected Spare Drives] list and click the [Remove] button. 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
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.

4. Confirm the settings. Click the [Finish] button.

-
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].

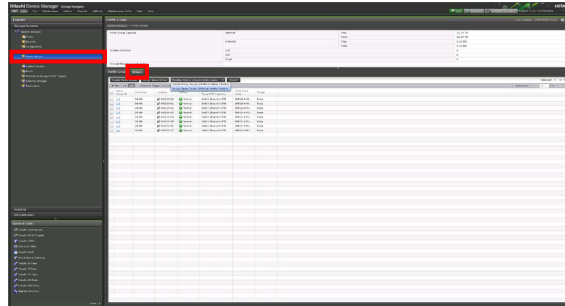
7. Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

4.2.1.4 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)].

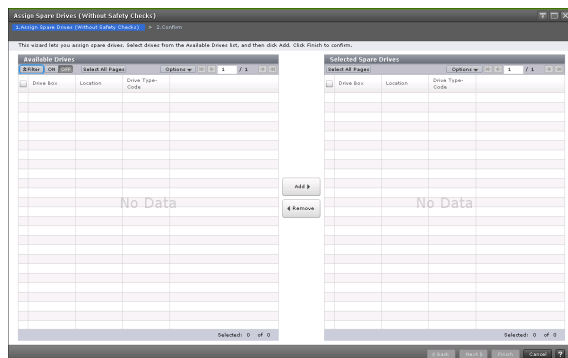
3. The “Assign Spare Drives” window appears.

When assigning spare drives, select a spare drive from the [Available Drives] list, and then click the [Add] button.

The selected spare drive was added to the [Selected Spare Drives] list.

When deleting spare drives, select a spare drive from the [Selected Spare Drives] list and click the [Remove] button. 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
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.

4. Confirm the settings. Click the [Finish] button.

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.

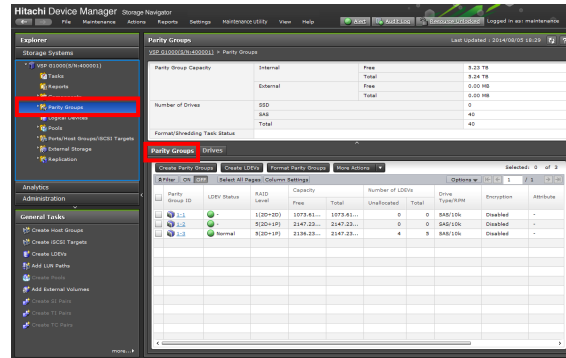
NOTE: To display the “Task” window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

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

4.2.2 Managing Parity Group

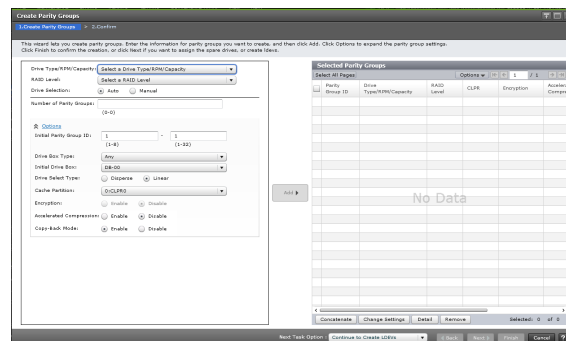
4.2.2.1 Creating Parity Group

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



2. Click the [Create Parity Groups] button.

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



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

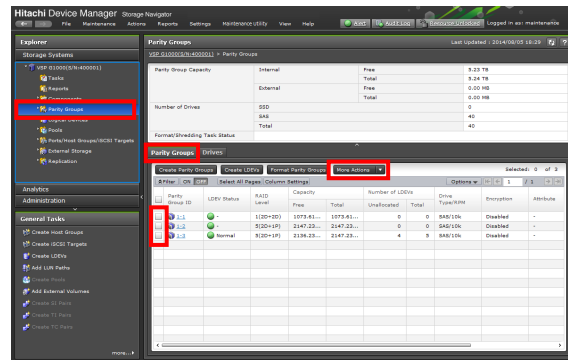
5. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

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.

4.2.2.2 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.



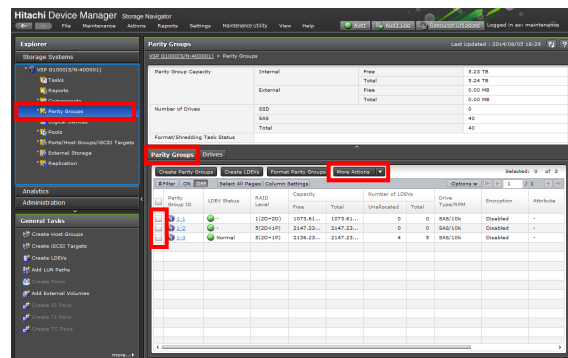
4.2.2.3 Deleting Parity Group



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

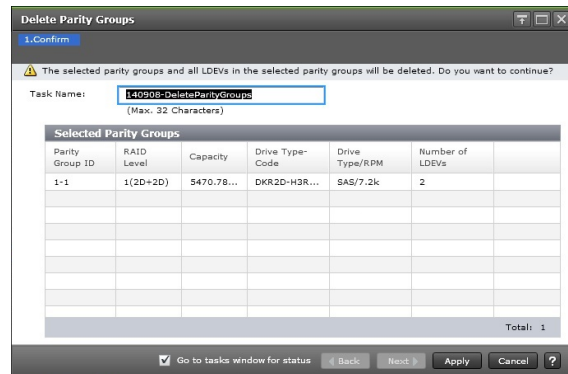
The parity group can be deleted even when logical devices are defined in the specified parity group.

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.
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/RPM	Displays the drive type 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.

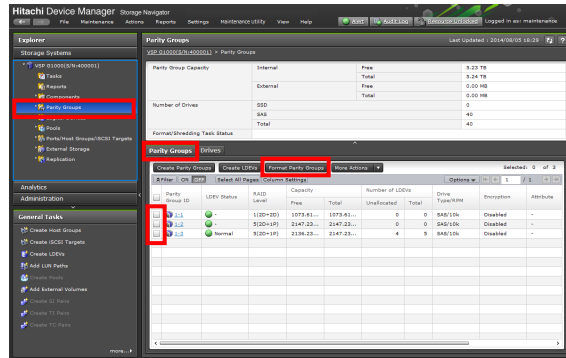
NOTE: To display the “Task” window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

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

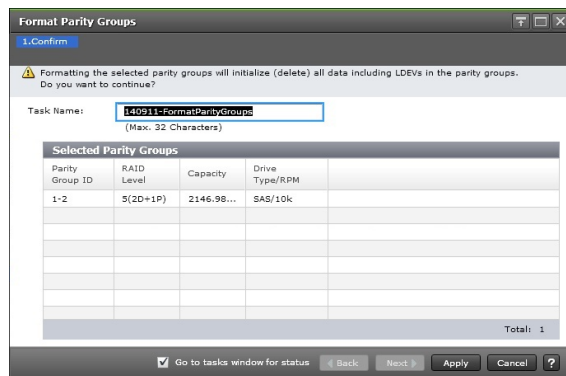
4.2.2.4 Formatting Parity Group

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

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



2. The blocked Select the target LDEV.
For information about how to block the LDEV, please refer to the [“4.4.1 Blocking LDEVs”](#).
3. Check the parity group to be formatted and click the [Parity Group Format] button.
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/RPM	Drive type and rpm in use on this LDEV.

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

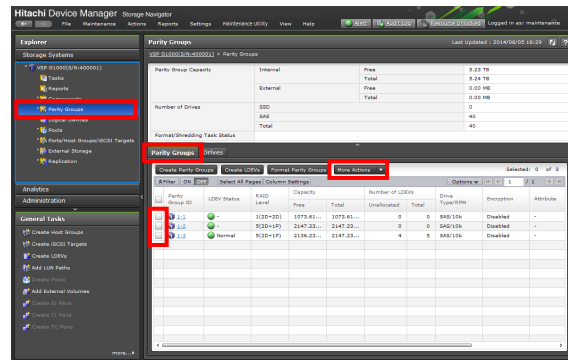
-
6. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

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.

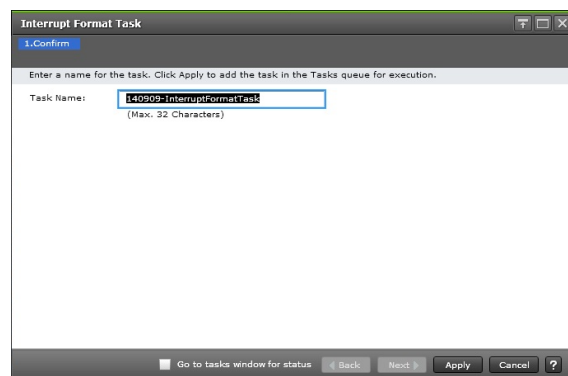
4.2.2.5 Interrupting Parity Group Format Task

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.

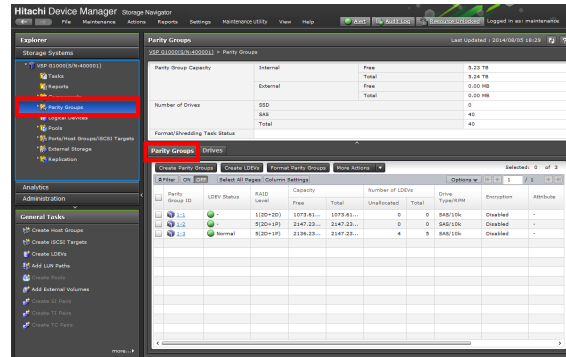
NOTE: If you execute [Interrupt Format Task], the end time of the formatting task and the interruption task may differ by one to ten minutes on the “Task” window. Confirm the completion of the interruption by the completion of the formatting task.

4.2.2.6 Creating Parity Group (Without Safety Checks)

⚠ CAUTION

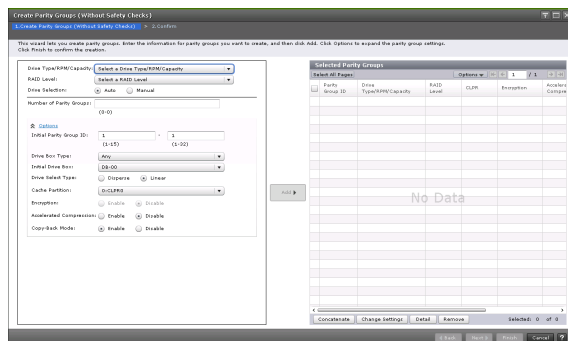
- Be sure to contact the Technical Support Division and follow the judgement before creating parity group with the procedure.
- The procedure is able to operate only by Web Console of the Maintenance PC.

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] button. Click the [Finish] button.



Item	Description
Drive Type/RPM/Capacity	Select the type of the drive box.
RAID level	Select the RAID level.
Drive Selection	Select the mode of the drive selection from Auto or Manual.
Number of Parity Groups	Enter the number of parity groups. This item appears when selected Auto as your drive selection.
Available Drives	This item appears when selected Manual as your drive selection. For drives to be incorporated to a parity group, set the checkbox of a row to ON. <ul style="list-style-type: none"> • Location: Displays the location of the drive box. • Drive Box: Displays the name of the drive box. • Drive Box Type: Displays the type of the drive box. • Drive Type-Code: Displays the type code of the drive box.
The number you have to select	Displays the number of drives that you must select. This item appears when selected Manual as your drive selection.
Initial Parity Group ID	Enter the parity group ID. Text box on the left side: Enter the numeric characters, which are the fixed characters that are placed at the beginning of the parity group ID. Text box on the right side: Enter the initial number following the prefix name.
Drive Box Type	Select the type of drive box. This item appears when selected Auto as your drive selection.
Initial Drive Box	This item appears when selected Auto as your drive selection. The smallest available number is entered in the text box as a default. No number appears in the text box if no available parity group ID exists. If you specify the parity group ID which is already used, the minimum parity group ID after that the specified parity group ID is automatically set.

(To be continued)

(Continued from preceding page)

Item	Description
Drive Select Type	<p>This item appears when selected Auto as your drive selection. Select the method for the selecting of drives in a parity group.</p> <ul style="list-style-type: none"> • Disperse: Selected drives where are located dispersedly. • Linear: Selected drives where are located linearly. <p>This item is not available with VSP G130, G350, G370 and VSP F350, F370. In VSP G130, G350, G370 and VSP F350, F370, [Linear] is set by default.</p>
Cache Partition	Select a CLPR number which is displayed as ID:CLPR.
Encryption	<p>Specify if encrypted parity groups are created.</p> <ul style="list-style-type: none"> • Enable: Encrypted parity groups are created. • Disable: Non-encrypted parity groups are created.
Accelerated Compression	<p>Specify if the Accelerated Compression is set to parity groups. (*1)</p> <ul style="list-style-type: none"> • Enable: The Accelerated Compression is set to parity groups. • Disable: The Accelerated Compression is not set to parity groups.
Copy-Back Mode	<p>Specify if the Copy-Back Mode is set to parity groups.</p> <ul style="list-style-type: none"> • Enable: The Copy-Back Mode is set to parity groups. • Disable: The Copy-Back Mode is not set to parity groups.
[Add] button	When you click Add, the configured information is added to the right side of the Selected Parity Groups table.
[Next Task Option] bull-down	Click [Next] button to go to the task setting window, which is indicated in Task Next Option.

*1: Existing parity groups can have Accelerated Compression enabled non-destructively with data-in-place. For the detailed procedure, see “Provisioning Guide”.

-
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.

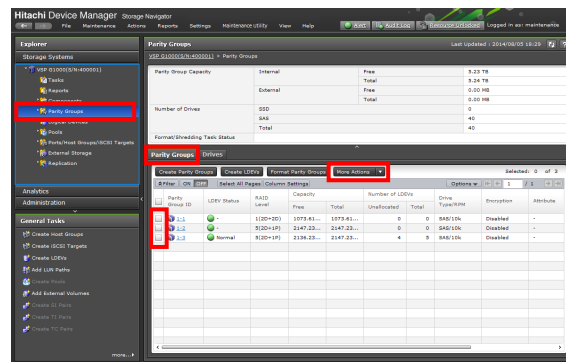
4.2.2.7 Deleting Parity Group (Without Safety Checks)

⚠ 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.

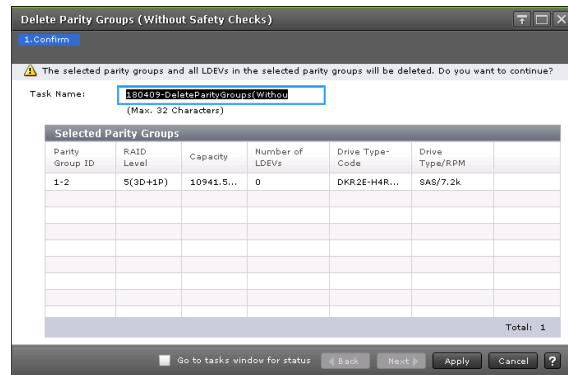
The parity group can be deleted even when logical devices are defined in the specified parity group.

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.
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/RPM	Displays the drive type 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.

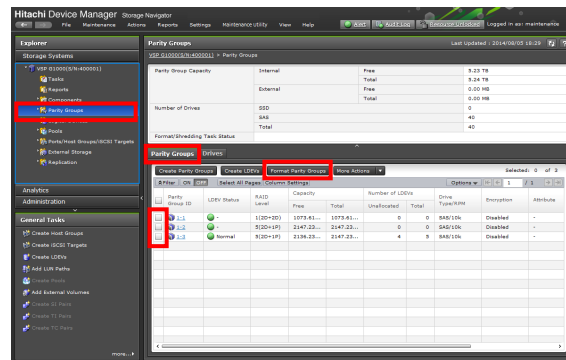
4.2.2.8 Formatting Parity Group (Without Safety Checks)

⚠ 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.

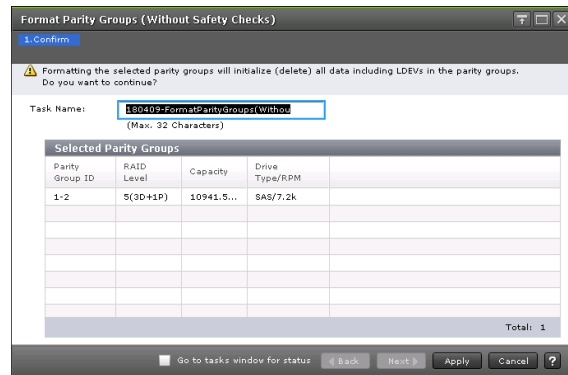
For the parity group, execute the physical format by SCSI command.

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



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 [“4.4.1 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/RPM	Displays the drive type 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.

4.2.3 Managing Logical Device

4.2.3.1 Creating Logical Device

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

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

-
3. The “Create LDEVs” window appears.

Enter the information for LDEV you want to create, and then click [Add] button.

The LDEV was added to the [Selected LDEVs] list. Click [Finish] button.

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] button.

4.2.3.2 Checking Logical Device

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

-
2. Check the set contents.

4.2.3.3 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 [“4.1.3 Allocating the Logical Devices of a Storage System to a Host”](#).

4.2.3.4 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 on page 3-19
- Storage System operation when LDEVs are formatted on page 3-19
- Quick Format function on page 3-19

Formatting LDEVs includes the following tasks:

- Formatting a specific LDEV on page 3-21
- Formatting all LDEVs in a parity group on page 3-21

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 4-1 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	<p>Quick Format can be performed on multiple parity groups simultaneously. The number of those parity groups depends on the total of parity group entries.</p> <p>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.</p> <p>The number of entries for parity groups is as follows.</p> <ul style="list-style-type: none"> • Parity group configured with drives of 32 TB or less: 1 entry • Parity group configured with drives of more than 32 TB: 2 entries <p>The maximum number of entries on which Quick Format can be performed is as follows.</p> <ul style="list-style-type: none"> • VSP G130/G350/G370, VSP F350/F370: 18 entries • VSP G700, VSP F700: 36 entries • VSP G900, VSP F900: 72 entries <p>The number of volumes on which Quick Format can be performed is not limited.</p>
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	<p>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.</p> <p>While preliminary processing is in progress, hosts cannot perform I/O access to the volume.</p>

(To be continued)

(Continued from the preceding page)

Item	Description
Blocking and restoring of volumes	<p>If a volume undergoing Quick Format is blocked, the Storage System recognizes that the volume is undergoing Quick Format.</p> <p>After the volume is restored, the status of the volume changes to Normal (Quick Format).</p> <p>Therefore, parity groups in which all volumes during Quick Format are blocked are included in the number of entries during Quick Format.</p> <p>The number of entries for additional Quick Format can be calculated with the following calculating formula: The maximum number of entries - X - Y</p> <p>(Legend)</p> <p>X: The number of entries for parity groups during Quick Format.</p> <p>Y: The number of entries for parity groups in which all volumes during Quick Format are blocked.</p>
Storage System is powered off and back on	The Quick Format operation resumes when power is turned back on.
Restrictions	<ul style="list-style-type: none"> 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. <p>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.</p> <ul style="list-style-type: none"> The prestaging feature of Cache Residency Manager cannot be applied to volumes undergoing Quick Format.

4.2.3.5 Formatting a Specific LDEV

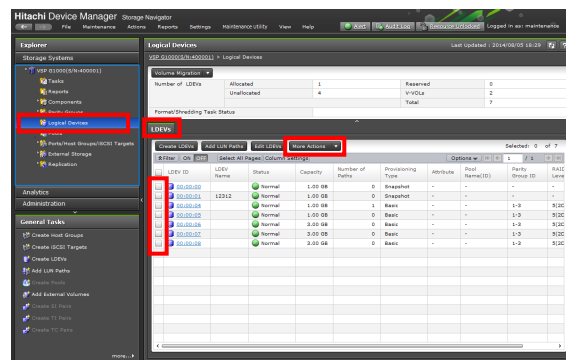
This procedure performs Normal formatting on the volume.

⚠ 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.

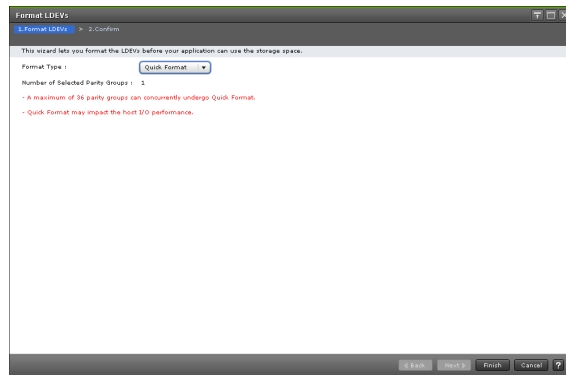
NOTICE: When you perform the LDEV maintenance operation using RAID Manager, the LDEV status displayed on the MPC might be different from the actual status.
(For example, the status of the LDEV that is being formatted by RAID Manager is displayed as “Blocked” instead of “Formatting”.)
In such a case, click the [Update] button 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 “[4.4.1 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 the [Finish] button.



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.

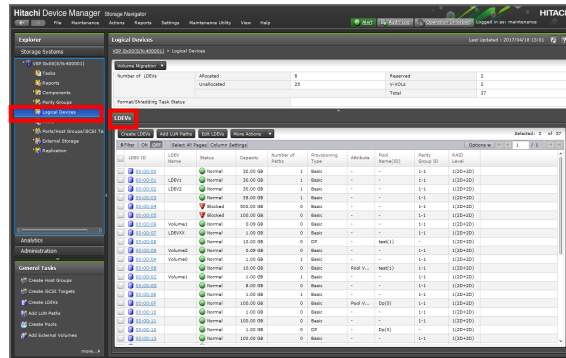
5. In the Confirm window, click the [Apply] button.
If “Go to tasks window for status” is checked, the “Tasks” window opens.
6. Click [Apply] to apply the settings to the Storage System.
7. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

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.

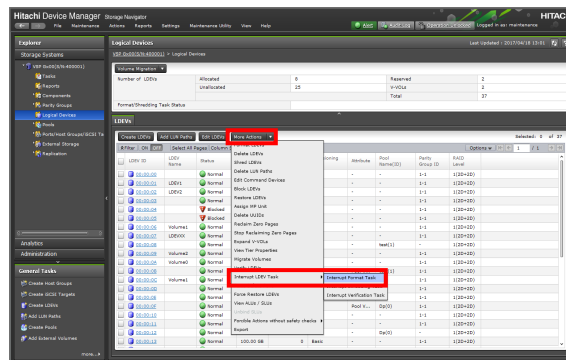
4.2.3.6 Interrupting Format Task

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

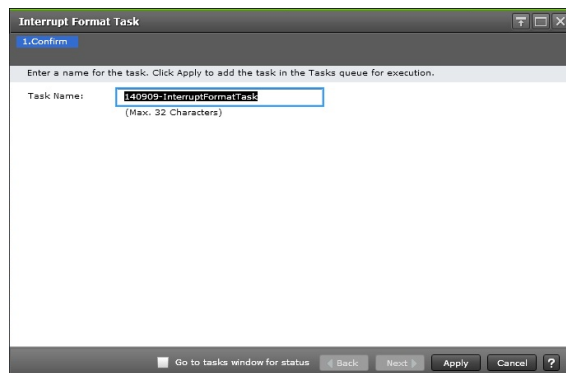
1. Select [Storage Systems]-[Logical Devices]. Click the [LDEVs] tab.



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.

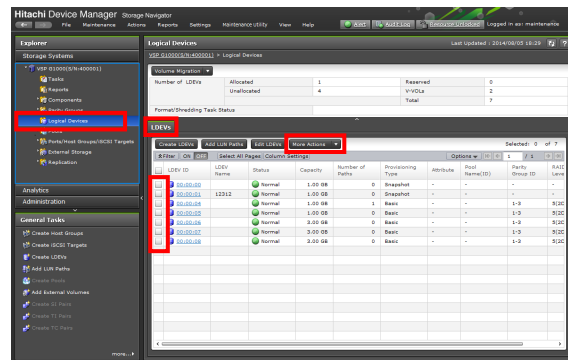
NOTE: If you execute [Interrupt Format Task], the end time of the formatting task and the interruption task may differ by one to ten minutes on the “Task” window. Confirm the completion of the interruption by the completion of the formatting task.

4.2.3.7 Deleting Logical Device

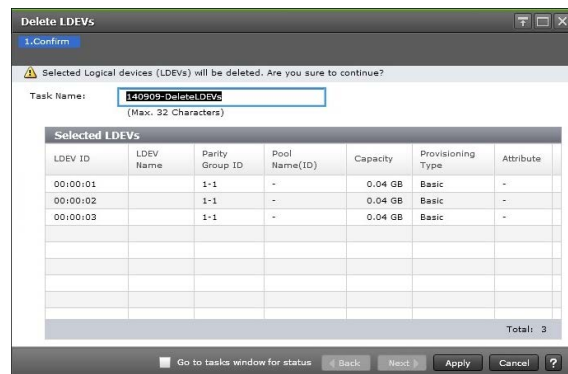


Deleting logical devices deletes all the data associated with them. Therefore, back up the data associated with logical devices before deleting them..

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.
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.

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

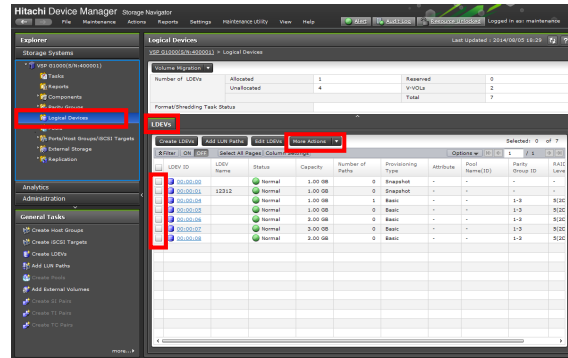
5. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

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

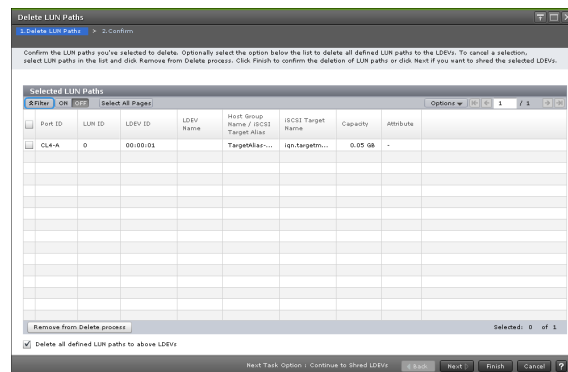
6. Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

4.2.3.8 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 the [Finish] button.



[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. -: Volume in which the attribute is not defined.

(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.

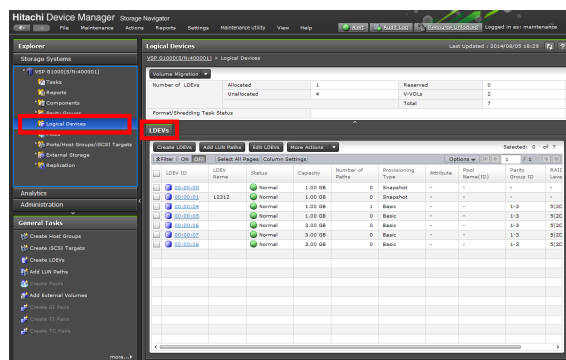
4.2.3.9 Formatting a Specific LDEV (Without Safety Checks)

⚠ 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.

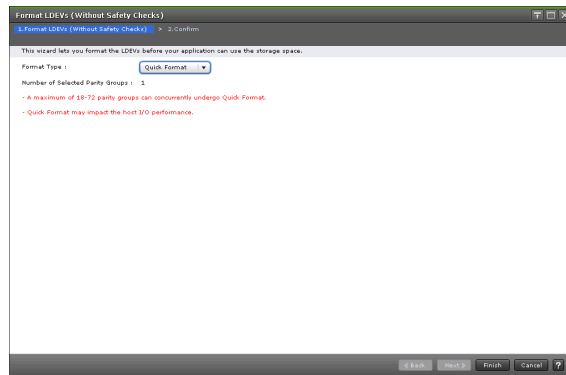
NOTICE: When you perform the LDEV maintenance operation using RAID Manager, the LDEV status displayed on the MPC might be different from the actual status.
(For example, the status of the LDEV that is being formatted by RAID Manager is displayed as “Blocked” instead of “Formatting”.)
In such a case, click the [Update] button 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 “[4.4.1 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 the [Finish] button.



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.

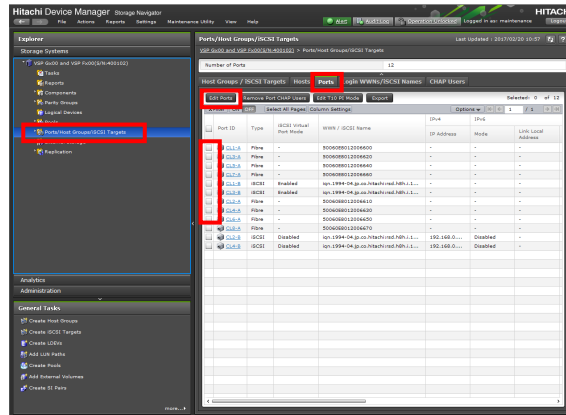
NOTE: To display the “Task” window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

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

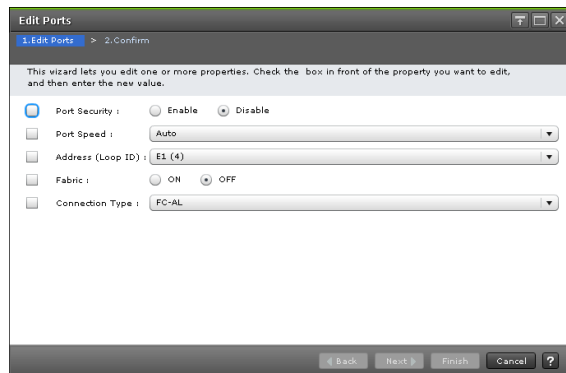
4.3 Managing Port

4.3.1 Editing Fibre Channel

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



2. Check the [Type] is specified [Fibre], and then check the check box of the port that you want to edit.
3. Click the [Edit Ports] button.
4. The “Edit Ports” window appears. Enter the setting information and click the [Finish] button.



Item	Description
Port Security	Select whether LUN security is Enabled or Disabled.
Port Speed	<p>Select the data transfer speed, in Gbps, for the selected Fibre Channel port.</p> <p>If Auto is selected, the storage system automatically sets the data transfer speed to 4, 8, 16 or 32 Gbps.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
Address (Loop ID)	Select the address of the selected port.
Fabric	Select whether a fabric switch is set to ON or OFF.
Connection Type	<p>Select the topology.</p> <ul style="list-style-type: none"> • FC-AL: Fibre Channel arbitrated loop • P-to-P (point-to-point). <p>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.</p>

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

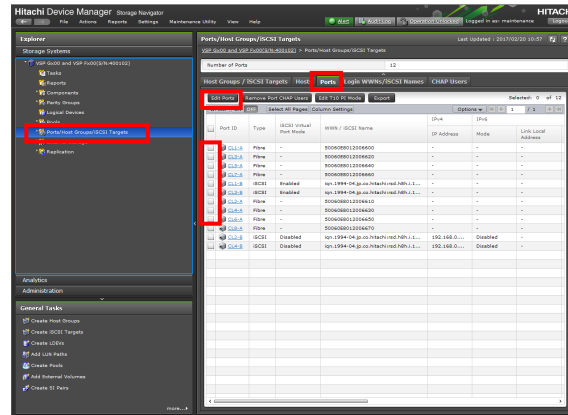
6. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

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

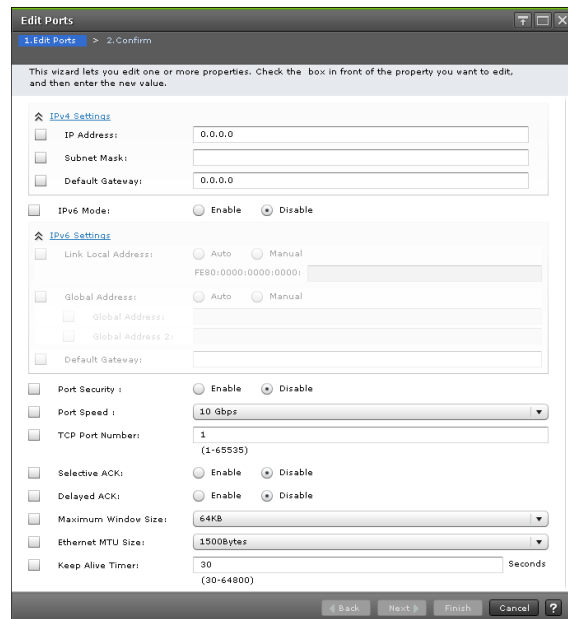
7. Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

4.3.2 Editing iSCSI

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



2. Check the [Type] button is specified [iSCSI], and then check the check box of the port that you want to edit.
3. Click the [Edit Ports] button.
4. The “Edit Ports” window appears. Check the checkboxes of the items to be edited, enter the setting information, and then click the [Finish] button.



Information Setting Area (When Selecting iSCSI)

Item	Description
IPv4 settings (*1)	Set the information corresponding to IPv4. <ul style="list-style-type: none"> • [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. <ul style="list-style-type: none"> • [Enable]: Enable the IPv6 mode. In this case, you can set each item of [Set IPv6]. • [Disable]: Disable the IPv6 mode.
IPv6 settings (*1)	Set the information corresponding to IPv6. <ul style="list-style-type: none"> • [Link Local Address]: Set a link local address. <ul style="list-style-type: none"> • [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. <ul style="list-style-type: none"> • [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. <ul style="list-style-type: none"> • [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 <ul style="list-style-type: none"> • [Enable]: Enable the selective ACK • [Disable]: Disable the selective ACK
Delayed ACK (*1)	Set a delayed ACK <ul style="list-style-type: none"> • [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.

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].

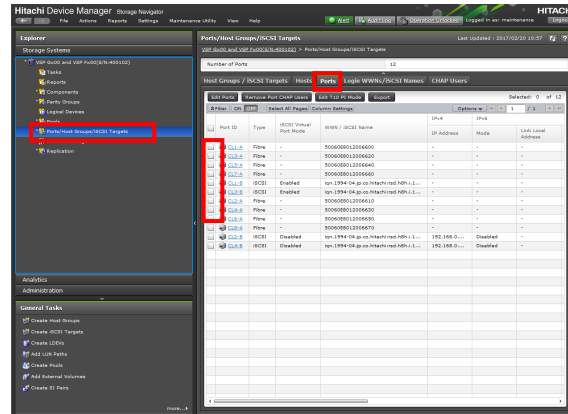
-
8. Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

4.3.4 Deleting iSCSI Target Information

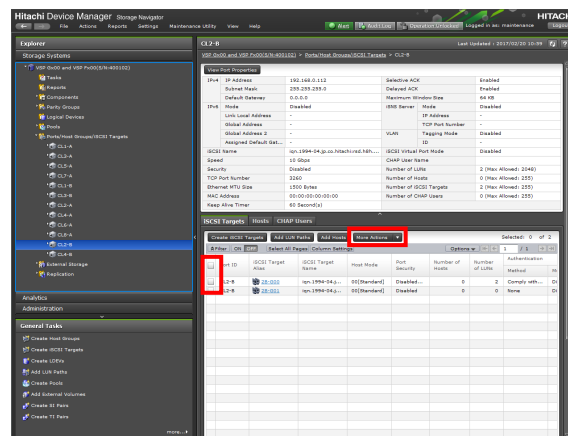
After you define target information for the iSCSI ports on your Storage System, use the following procedure to initialize the target information.

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 the [Type] is specified “iSCSI”.

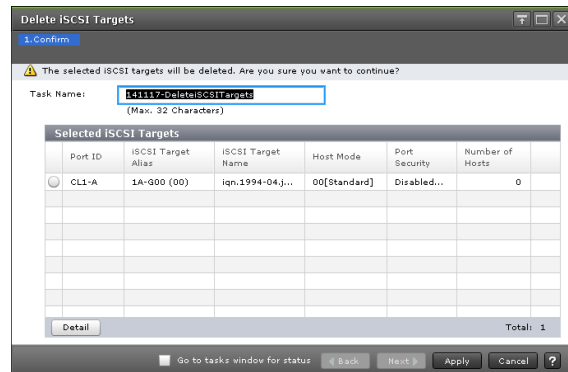


2. The [iSCSI Targets] tab is displayed. Check the check box of the iSCSI target to be deleted, and then click [More Actions]-[Delete iSCSI Targets].



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

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.

- 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].

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

4.3.5 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.

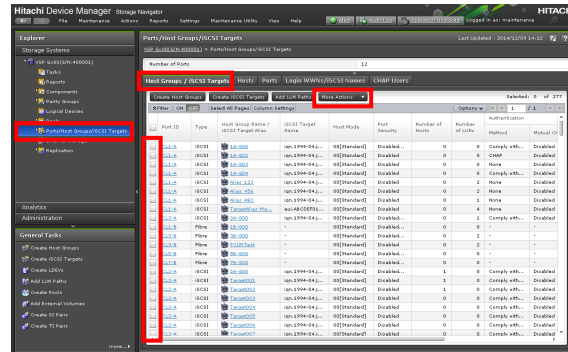
CHAP is an optional feature and is not required to use iSCSI. However, if you do not configure CHAP authentication, any host server connected to the same IP network as the Storage System can read from and write to the Storage System.

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.

4.3.5.1 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.

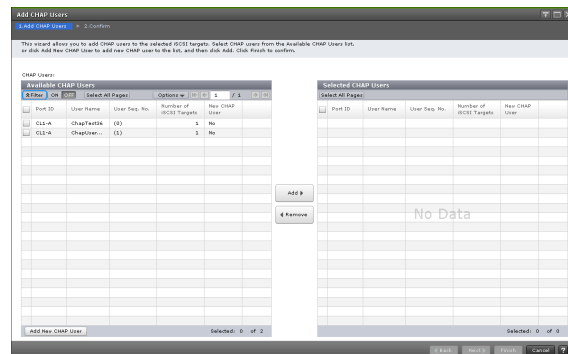


2. Check a line to be added and click [More Actions]-[Add CHAP Users].

3. Select a CHAP user from the [Available CHAP Users] list and click the [Add] button 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 the [OK] button.



4. Click the [Finish] button.

[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 the [OK] button.

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.

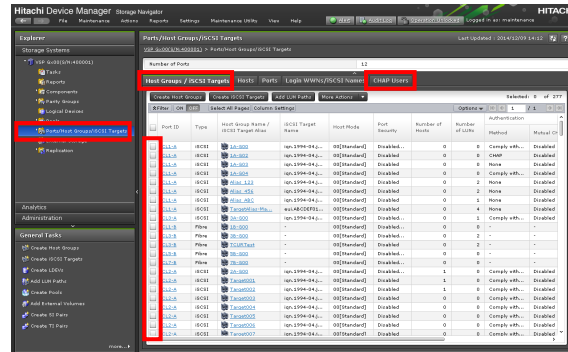
NOTE: To display the “Task” window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

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

4.3.5.2 Changing One-Way CHAP Settings

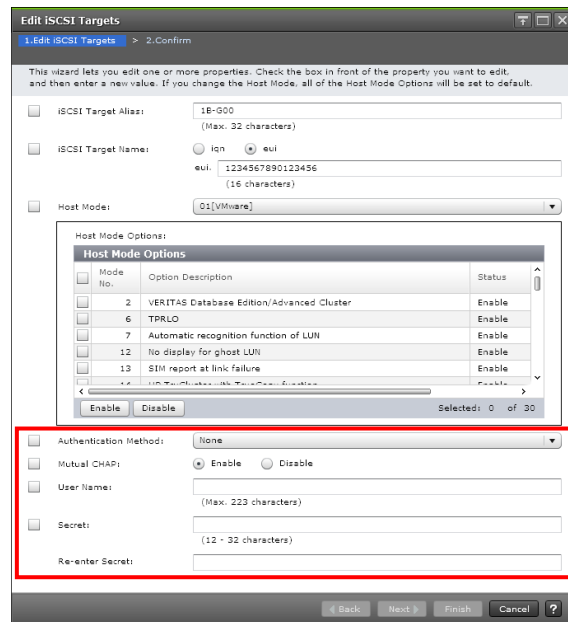
You can set the authentication mode in the “Edit iSCSI Targets” window.

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 the [Finish] button.



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. <ul style="list-style-type: none"> 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] button.

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

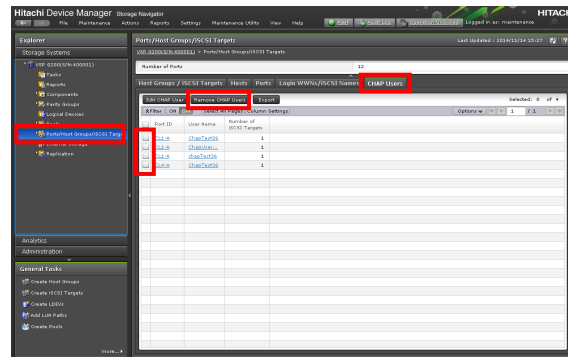
6. Click [Apply] to apply the settings to the Storage System. The set contents are queued as tasks and executed sequentially.

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.

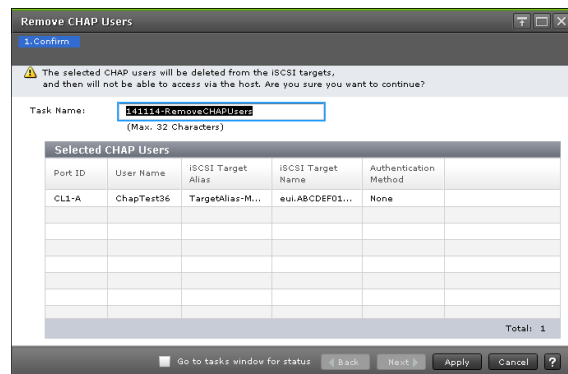
4.3.5.3 Deleting a One-Way CHAP User

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.

4.3.6 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].

NOTE: If the firmware version is earlier than 88-02-01-x0/xx and LUN paths are defined for host groups/iSCSI targets created automatically through Hitachi Storage Advisor Embedded (HSAE) (Host Group Name/iSCSI Target Alias starting with “[AutoConfig]”), perform the procedure described in [“Deleting LUN paths from ports \(for host groups/iSCSI targets created automatically through HSAE\)”](#) instead of the following procedure.

-
2. Select host groups or iSCSI targets of the ports to be operated and select the [LUN] 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 the [Apply] button 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 the [Apply] button.

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

Deleting LUN paths from ports (for host groups/iSCSI targets created automatically through HSAE)

1. Identifying servers that use host groups/iSCSI targets

- (1) In the [Ports/Host Groups/iSCSI Targets] window on Web Console, click the [Hosts] tab.
- (2) Write down WWN/iSCSI names registered in target ports.
- (3) Start HSAE by specifying the URL in the Web browser (see [“2.7.3 Starting the Maintenance Utility Window by Specifying IP Address of CTL”](#)). To perform the following procedure, use HSAE.
- (4) Click [Servers] on the dashboard or in the navigation bar.
- (5) Click any server.
- (6) In [Port Connections], check if there are paths between the target ports and the WWN/iSCSI names written down in Step (2).
If there are paths, the server is the server that uses the host groups/iSCSI targets.
- (7) Perform Steps (5) and (6) for all servers.

2. Cancelling allocation of paths to servers

Cancel the allocation of the paths to all the ports to be operated on the servers identified in Procedure 1 by following the procedure described in Hitachi Storage Advisor Embedded Guide “Setting port connections for server”.

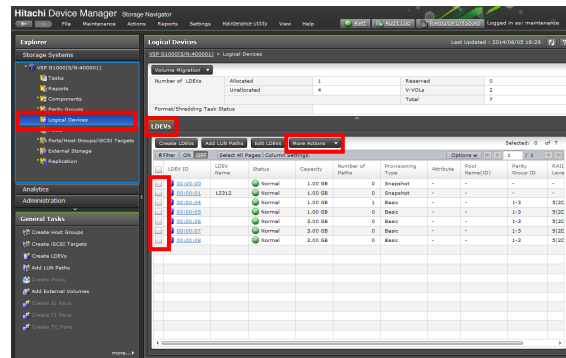
NOTE: If there are volumes attached to the servers, errors occur because the paths cannot be deleted. When errors occur, detach the volumes from the servers by following the procedure described in Hitachi Storage Advisor Embedded Guide “Detaching volumes from a server”, and then cancel the allocation of paths to the servers.

4.4 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.

4.4.1 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].

- Note the settings in the Confirm window and enter a unique [Task Name] or accept the default and click the [Apply] button.

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.

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

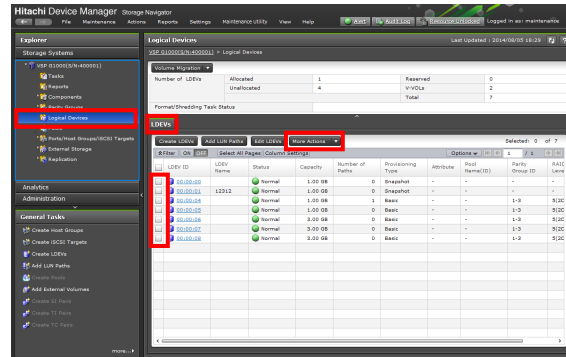
- Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

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

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

4.4.2 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].

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

[illegible]

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.

- 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].

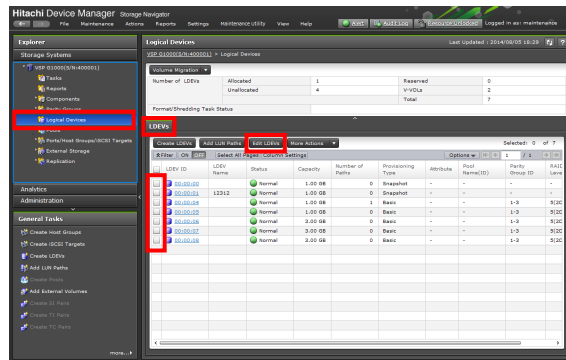
7. Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

4.4.3 Editing an LDEV Name

You can edit the name of a registered internal volume.

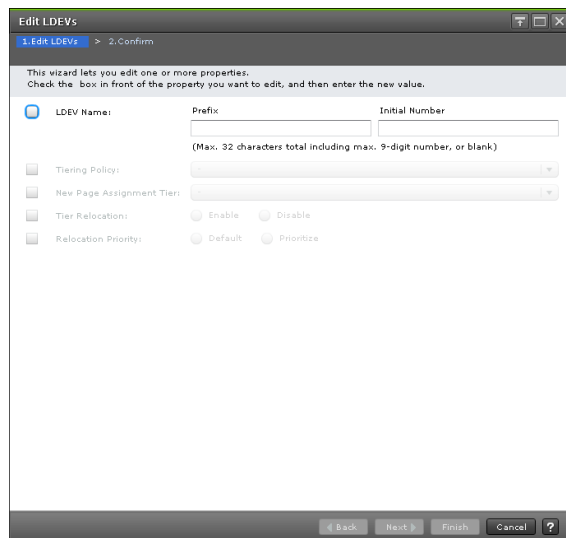
For information about editing a registered external volume, see Hitachi Universal Volume Manager User Guide.

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



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

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



Item	Description
LDEV Name	Specify the LDEV name, using up to 32 characters. <ul style="list-style-type: none"> • Prefix: Fixed character string. • Initial Number: Initial number. Specify the initial number according to these examples. Example: <ul style="list-style-type: none"> - 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".
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". 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: <ul style="list-style-type: none"> • When there are V-VOLs where Dynamic Tiering/active flash is enabled. • When the tier relocation is enabled.

4. Click the [Finish] button.

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 the [Apply] button.
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.

4.4.4 Force Restore LDEVs

Prerequisites

LDEVs to be restored forcibly should be blocked.

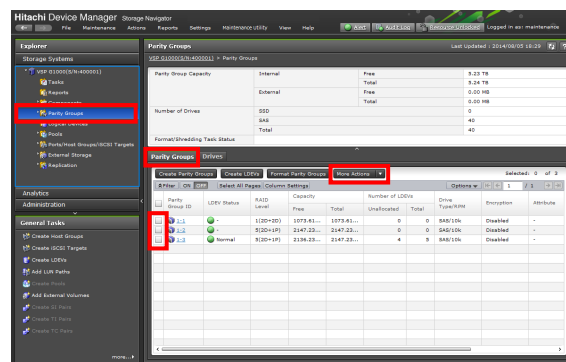
NOTE: When specifying a parity group, all the LDEVs belonging to the parity group should be blocked.

Procedure

1. Specify LDEVs to be restored forcibly.

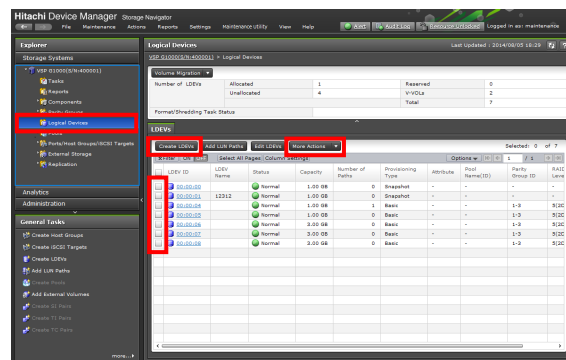
- (1) When forcibly restoring all the LDEVs belonging to the parity group.

Select [Parity Group] from the [Storage System] tree and display the [Parity Group] 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 [LDEV] 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].

Force Restore LDEVs

1. Confirm

This wizard lets you forcibly recover the blocked LDEVs. Enter a name for the task. Confirm the settings in the list, and then click Apply to add the task in the Tasks queue.

Task Name: (Max: 32 Characters)

LDEV ID	LDEV Name	Parity Group ID	Pool Name(ID)	Capacity	Provisioning Type	Attribute
00:00:01		1-1	-	0.04 GB	Basic	-
00:00:02		1-1	-	0.04 GB	Basic	-
00:00:03		1-1	-	0.04 GB	Basic	-
Total: 3						

Go to tasks window for status Back Next Apply Cancel ?

[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:

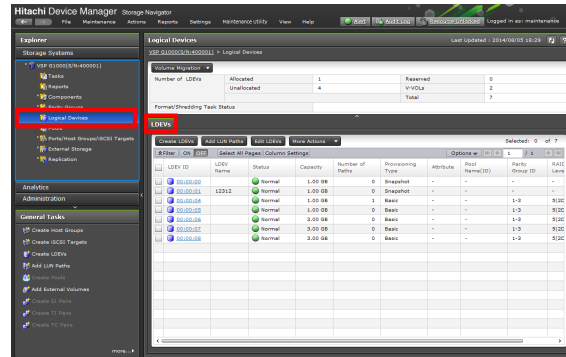
 - To display the “Task” window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].
 - Please call Technical Support Division for asking the password.
6. Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

4.4.5 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.

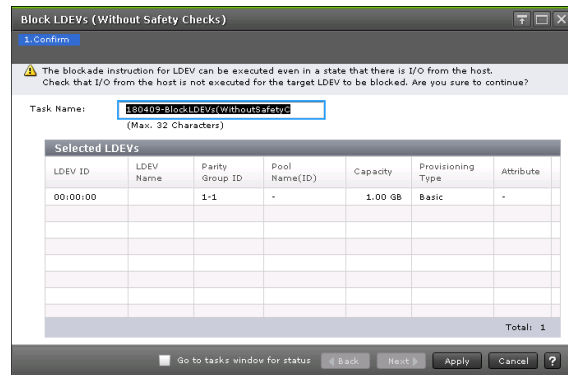


2. If [Blocked] does not appear in the [Status] column, you can use the following steps to block the LDEV.
If [Blocked] appear in the [Status] column, you can skip the remaining steps.

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.

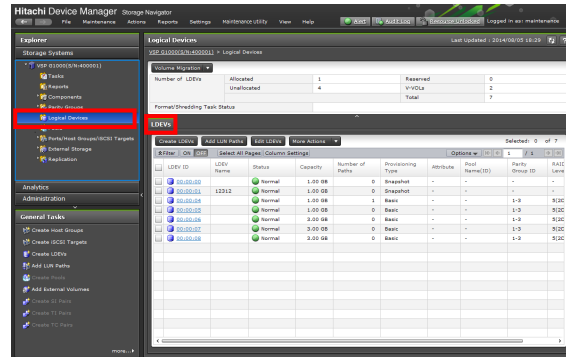
6. Click [Apply] to apply the settings to the Storage System.
7. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.
- NOTE: To display the “Task” window automatically after closing the wizard, select [Display Task Window after Clicking “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.

4.4.6 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 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]-[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.

4.4.7 Force Restore LDEVs (Without Safety Checks)

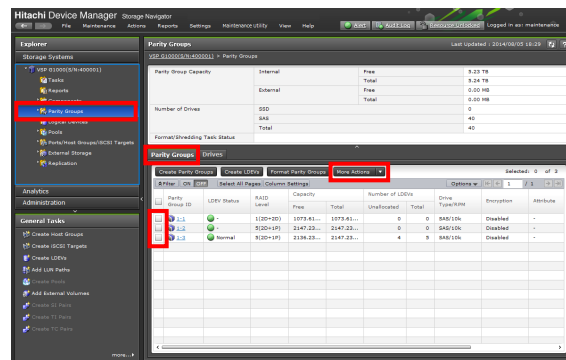
⚠ CAUTION

- 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.

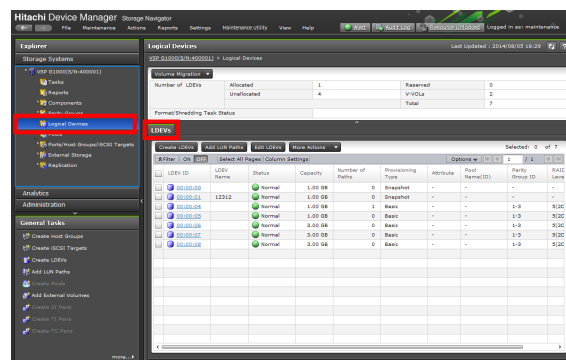
- (1) When forcibly restoring all the LDEVs belonging to the parity group.

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.

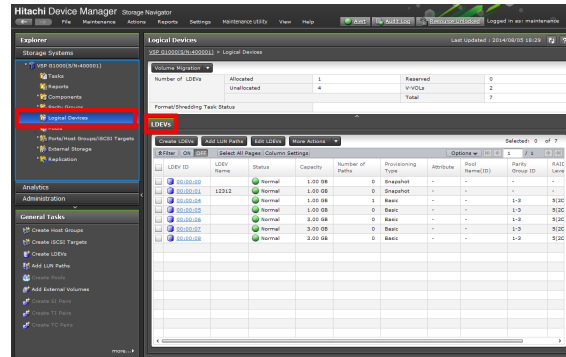
6. Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

4.4.8 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.

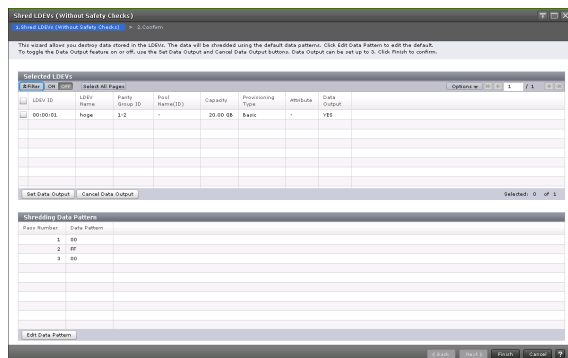


2. If [Blocked] appear in the [Status] column, you can use the following steps to shred the LDEV.

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.

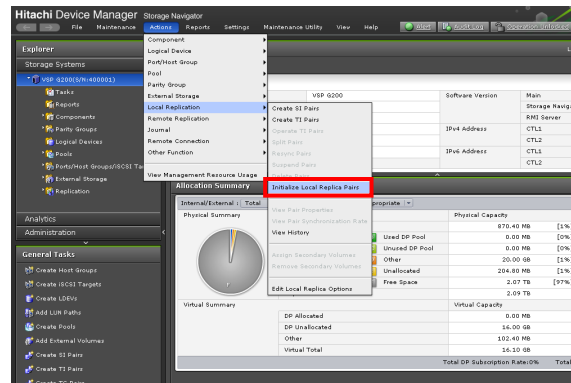
4.5 Web Console Operation

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

4.5.1 Local Replication

Clicking [Replication] - [Local Replication] from the [Storage System] tree menu in the navigation area on the left of the “Web Console” window displays the “Local Replication” window.

4.5.1.1 Initializing Local Replica Pairs



1. Click [Action] - [Local Replication] - [Initialize Local Replica Pairs] of the task bar.

- Initializing local replica pairs

Cancel all the created pairs of ShadowImage, Volume Migration and Thin Image, and change the volume pair status (Status) to SMPL. Refer to TROUBLESHOOTING SECTION “[5.2 ShadowImage Initialize procedure](#)” for the Initialize procedure and precautions. Initializing local replica pairs requires the password entry. Contact the Technical Support Division for the password.

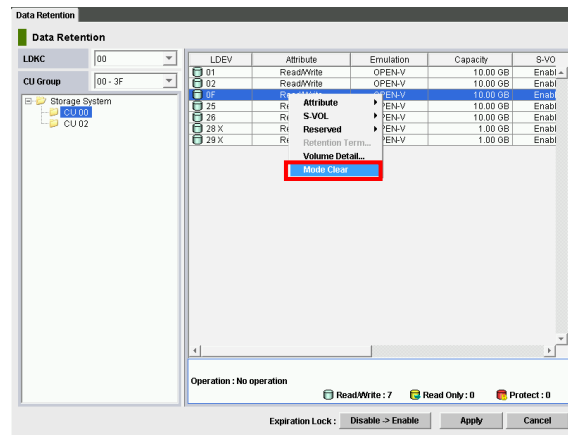
NOTE 1: Initializing local replica pairs cancels not only the pairs created by ShadowImage but the pairs created by Volume Migration and Thin Image.

NOTE 2: Perform the operation only when the Technical Support Division issues instructions.

4.5.2 Data Retention Utility

Click the [Actions] button at the top of the “Web Console” window.

Select [Other Function]-[Data Retention] to open the “Data Retention” window.



1. Canceling the mode attribute

When the “Data Retention” window from [Actions]-[Other Function]-[Data Retention] menu of Web Console is opened and the operation for changing the access attribute is performed, [Mode Clear] is displayed in a pop-up menu.

Use the menu when you want to cancel the attribute, Zer and Inv.

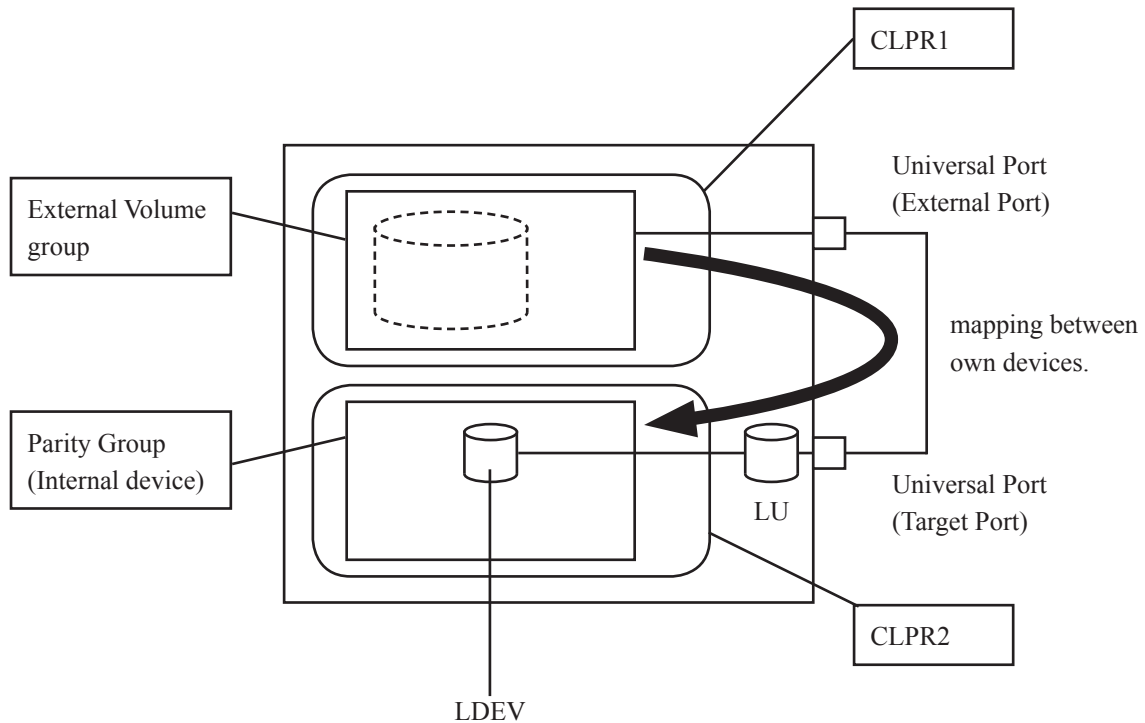
NOTE: For the attributes, Zer and Inv, refer to “Provisioning Guide”.

4.5.3 Universal Volume Manager

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.

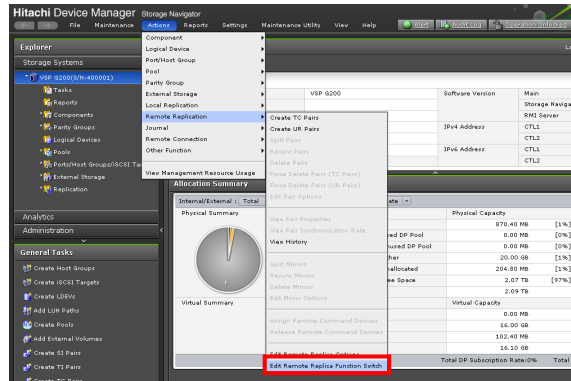
For example when mapping between own external group



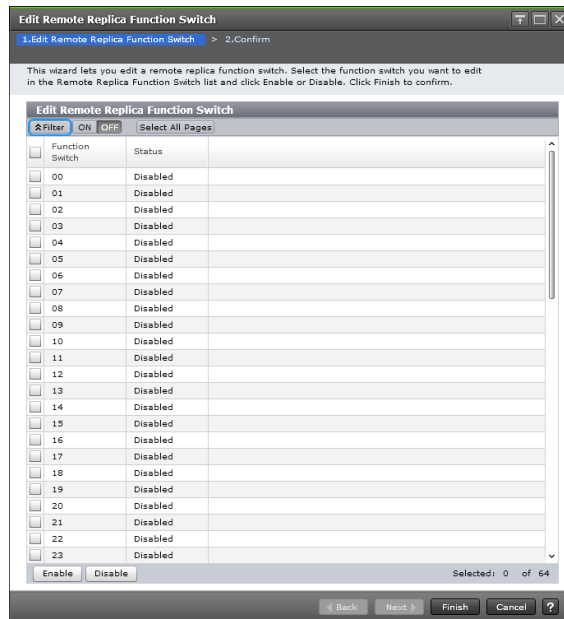
4.5.4 Remote Replication

4.5.4.1 Remote Replica Function Switch

Select [Actions]-[Remote Replication]-[Edit Remote Replica Function Switch] menu at the top of the “Web Console” window to activate the “Edit Remote Replica Function Switch” window.



1. Edit Remote Replica Function Switch



In the “Edit Remote Replica Function Switch” window, select function switch to be changed.

Click the [Enable], [Disable] button.

When click the [Finish] button, the confirmation window is displayed. Check the task name, and click the [Apply] button.

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

NOTE: Please refer to [Step 2](#) Remote Copy Function Switch for the function allocated in each switch.

2. Remote Replica Function Switch

The function allocated in each switch is as follows.

Switch#	Contents
11	A copy pace is made a maximum 4 Tracks, when “15 Tracks” is selected in the Remote Copy option parameter and “Track” is selected in the Difference Management.
15	The path failure threshold values of function switch #17 are changed. By the combination of function switch #15 and #20 the path failure threshold values are changed.
17	The path is blocked when the number of path failures reaches the threshold within a certain period.
18	The path is blocked when the number of link failures reaches the threshold within a certain period.
20	The path failure threshold values of function switch #17 are changed. By the combination of function switch #15 and #20 the path failure threshold values are changed.
30	The following functions are supported. <ul style="list-style-type: none"> • When the pair from Web Console is formed, the pair is formed with SyncCTG#7F. • When all the connections from MCU-RCU PATH cut, S-VOL that belongs to SyncCTG#7F is suspended.
33	In the cases that a PDCM function of McData ES3232 is being used on MCU-RCU path, when response of LOGIN response is late, path status of MCU is changed to non-normal.
40 to 42	The path is blocked when the number of RIO response time that exceeds the decided time reaches the threshold within a certain period. The decided time is changed by combination of function switch #40, #41 and #42.
43	In the function of switch #17 or switch #40, #41 and #42, the path is blocked even if the number of path is less than that is set by minimum path.

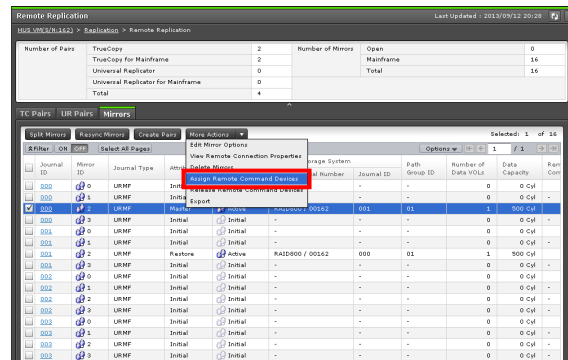
4.5.4.2 Assign Remote Command Devices Window

Click [Mirrors] at the application area of “Remote Replication” window.

Click mirrors in Initial, Active, Halt or Stopped state.

Click [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.

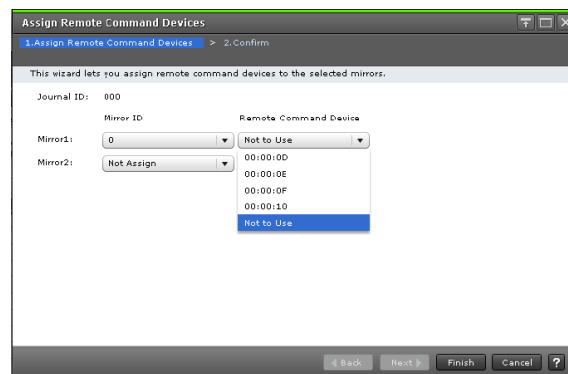


1. [Remote Command Device] drop-down list.

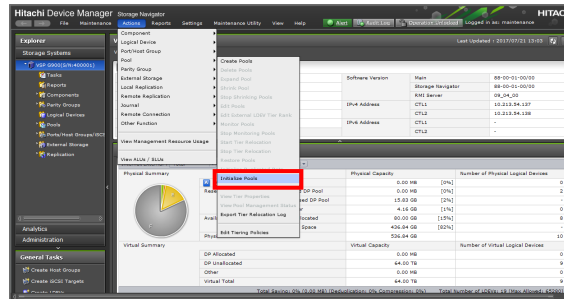
[Not to Use] is displayed at the [Remote Command Device] drop-down list.

- Not to Use

[Not to Use] is selected when not using [Remote Command Devices].



4.5.5 Dynamic Provisioning/Dynamic Tiering/active flash/Thin Image



1. Initialize Pools

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

The Virtual Volumes of Dynamic Provisioning/Dynamic Tiering/active flash is blockaded. And the pool of all Dynamic Provisioning/Dynamic Tiering/active flash/Thin Image is blockaded.

Refer to the TROUBLESHOOTING SECTION [“10.8 Initialization Procedure for Pool”](#) 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 and Thin Image is blockaded.

NOTE2: In the case [TrueCopy/Universal Replicator/ShadowImage/Volume Migration] use virtual volumes of Dynamic Provisioning, delete all [TrueCopy/Universal Replicator/ShadowImage/Volume Migration] pairs that use the virtual volumes before performing Initialize.

After Initialize completes, create [TrueCopy/Universal Replicator/ShadowImage/Volume Migration] pairs again.

During Initialize, don't create [TrueCopy/Universal Replicator/ShadowImage/Volume Migration] pairs with virtual volumes of Dynamic Provisioning. In the case create 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 the [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 operation of Dynamic Provisioning/Dynamic Tiering/active flash/Thin Image until the pool restores normally after executing Initialize.

NOTE6: Procedure to recover DP-VOL:

Please recover the pool of Dynamic Provisioning referring to "Provisioning Guide". DP-VOL recovers by recovering the pool of Dynamic Provisioning.

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

4.6 Copy Back Setting

If the copy back mode is set to enable, when a failed drive recovered, data which has been copied to the spare drive returns to the recovered drive. If the copy back mode is set to disable, when a failed drive recovered, data which has been copied to the spare drive still exist in the spare drive. This mode can be set to a parity group basis.

4.6.1 Setting the Copy Back

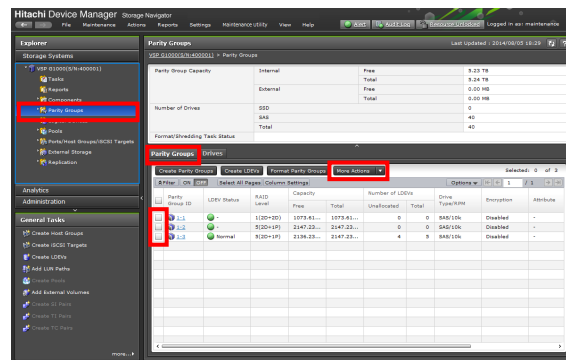
Set the copy back when creating a parity group.

Refer to “4.1.1 Creating Parity Groups” for the procedure of parity group creation.

4.6.2 Changing the Copy Back

You can change Enable/Disable of the copy back by parity group unit.

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

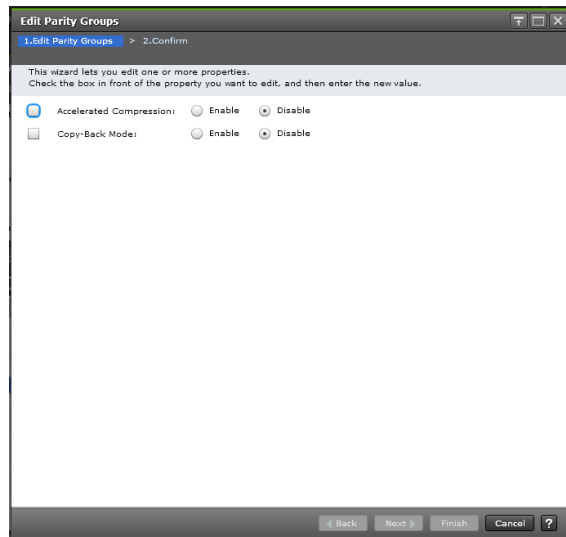


Item	Description
Copy-Back Mode	<p>[Enable] : Perform the copy back when the failed drive recovered.</p> <p>[Disable] : Do not perform the copy back when the failed drive recovered.</p> <p>*: This item is displayed in the right part of the window. Check this item by scrolling to the right.</p>

2. Select a target parity group.

3. Click [More Actions] - [Edit Parity Groups].

4. Select whether to execute the copy back or not in the “Edit Parity Groups” window.



Item		Description
Copy-Back Mode	Enable	Perform the copy back when the failed drive recovered.
	Disable	Do not perform the copy back when the failed drive recovered.

5. Click the [Finish] button.
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.

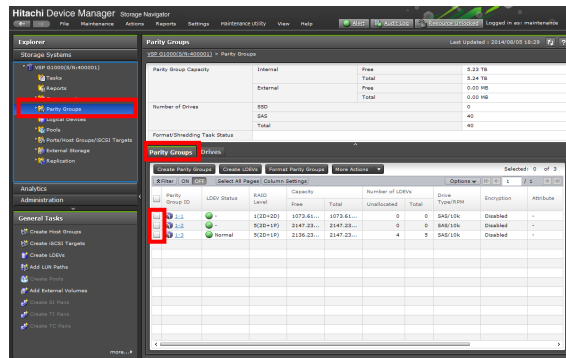
NOTE: To display the “Task” window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].
8. Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

4.7 Verify (Parity Consistency Check)

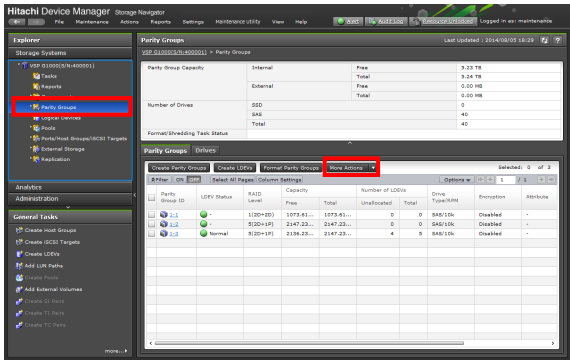
4.7.1 Executing Verify (Parity Consistency Check)

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](#).

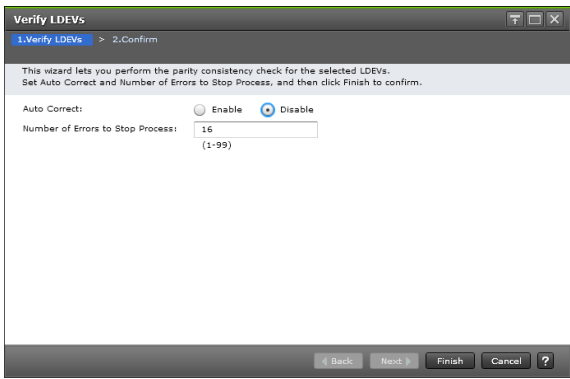
NOTE: For a simple LDEV, set it from the [LDEVs] tab. Selectable LDEVs should have the LDEV status of [Normal] or [In Quick Format].



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]. <ul style="list-style-type: none">• 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 the [Finish] button.

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.

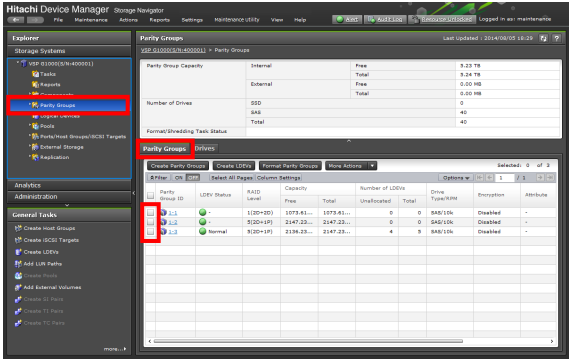
-
8. Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

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

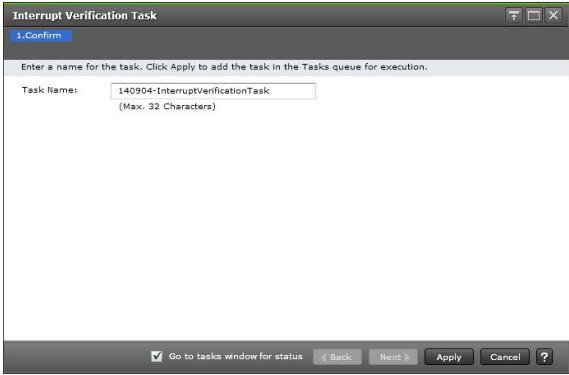
4.7.2 Interrupting Verify

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.

4.7.3 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.

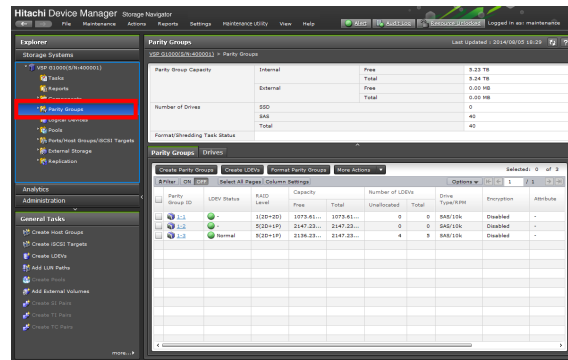
Check the progress in the “Parity Group” window : Refer to [“4.7.3.1 Checking the Progress in the “Parity Group” Window”](#).

Check the progress in the “LDEV” window : Refer to [“4.7.3.2 Checking the Progress in the “LDEV” Window”](#).

Check the progress with the task : Refer to [“4.7.3.3 Checking the Progress in the Task”](#).

4.7.3.1 Checking the Progress in the “Parity Group” Window

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



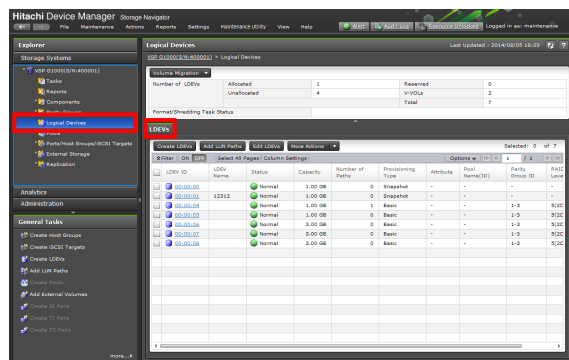
Item	Description
Parity group capacity	<p>Displays the information on the parity group capacity.</p> <ul style="list-style-type: none"> • Internal : Displays the information on the capacity of the internal volume. [Free] (*1) : Displays the capacity of free spaces of the internal volume. [Total] (*2) : 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	<ul style="list-style-type: none"> • SSD : Displays the number of SSDs. • SAS : Displays the number of SAS Drives. • Total : Displays the total number of Drives.
Format/Shredding task status	<p>[Formatting n%] : Displays the progress of formatting.</p> <p>[Preparing Quick Format n%] : Displays the progress of the preparing Quick Format.</p> <p>[Shredding n%] : Displays the progress of shredding.</p> <p>[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.</p> <p>[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.</p> <p>Blank : When formatting or shredding is not executed, the display is a blank.</p> <p>Furthermore, if the storage configuration is changed and the information cannot be gathered, the display is also a blank.</p>

*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.

4.7.3.2 Checking the Progress in the “LDEV” Window

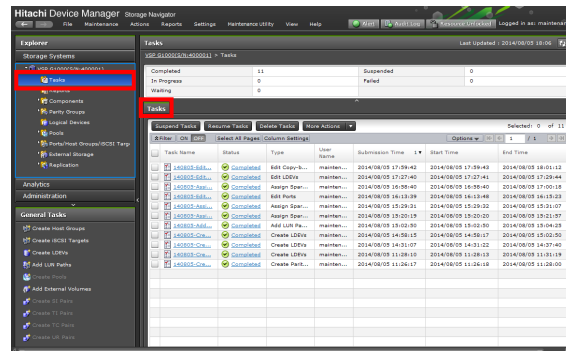
1. Select [Storage Systems]-[Parity Groups]. Click the [Drives] tab.



Item	Description
[Number of LDEVs]	<p>Displays the information on the number of LDEVs.</p> <ul style="list-style-type: none"> • [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	<p>[Formatting n%]: Displays the progress of formatting.</p> <p>[Preparing Quick Format n%]: Displays the progress of the preparing Quick Format.</p> <p>[Shredding n%]: Displays the progress of shredding.</p> <p>[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.</p> <p>[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.</p> <p>Blank : When formatting or shredding is not executed, the display is a blank.</p> <p>Furthermore, if the storage configuration is changed and the information cannot be gathered, the display is also a blank.</p>

4.7.3.3 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. <ul style="list-style-type: none"> • : Completed or Completed(Request) : the task completed normally. • : In progress: the task is being processed by the system. • : Waiting: the task is not yet started. • : 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	<p>Enabled: A task is automatically deleted when the following two events occur:</p> <ul style="list-style-type: none"> • The task is completed • The number of tasks in the Task list reaches the maximum number the window can display (384) <p>Disabled: Tasks will remain displayed until users delete them. Tasks whose status is Failed are automatically Disabled by the system.</p>
[Suspend Tasks] button	Suspends the selected tasks. They will not be started even if the storage system is ready. Only waiting tasks can be suspended.
[Resume Tasks] button	Resume the selected tasks. The status goes back to waiting.
[Delete Tasks] button	<p>Deletes the selected tasks from the window.</p> <ul style="list-style-type: none"> • The waiting or suspended tasks will be cancelled. • The failed or aborted tasks can be deleted from the window. • Tasks in progress cannot be deleted. • If the maximum number of tasks displayed on the window is reached when Auto Delete is enabled, execution of a new task will result in automatic deletion of a task starting with the oldest one.
[Disable Auto Delete](^{*1})	When disabled, the selected task remains in the task list after the task is completed.
[Enable Auto Delete](^{*1})	<p>When enabled, the selected task is deleted from the Task list when the following two events occur:</p> <ul style="list-style-type: none"> • 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].

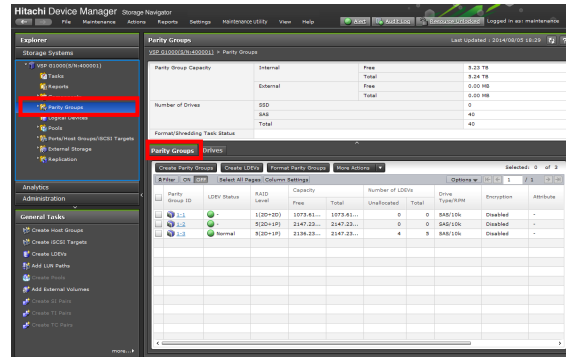
2. Check the information on the concerned task.
You can check the detailed information by clicking the link of the task name.

4.7.4 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.

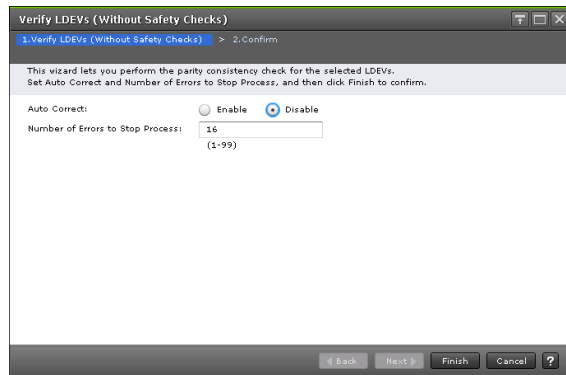
1. Select [Storage Systems]-[Parity Groups]. Click the [Parity Group] tab.



2. Check the target parity group.

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

- 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]. <ul style="list-style-type: none"> • 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.

- Click the [Finish] button.
- Check the set contents in the Confirm window and enter a task name in [Task Name].
- Click [Apply] to apply the settings to the Storage System.
- Enter the password and click [OK] in password window. The set contents are queued as tasks and executed sequentially.

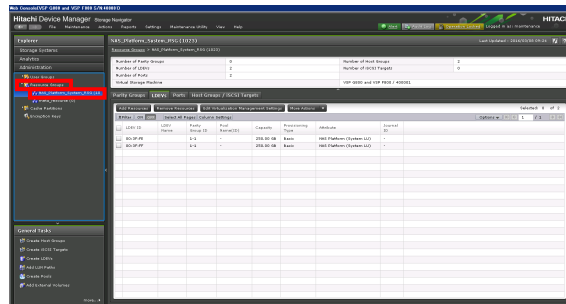
NOTE: To display the “Task” window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].
- Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

4.8 Managing Resource Group

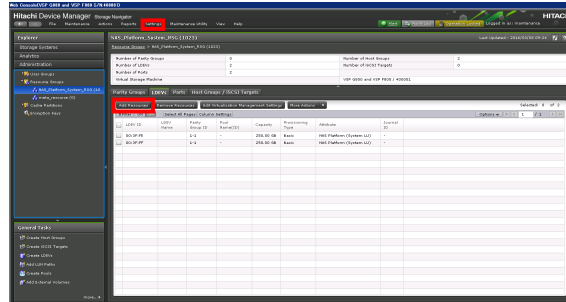
4.8.1 Adding LDEVs to Resource Group

Add arbitrary LDEVs to an arbitrary resource group.

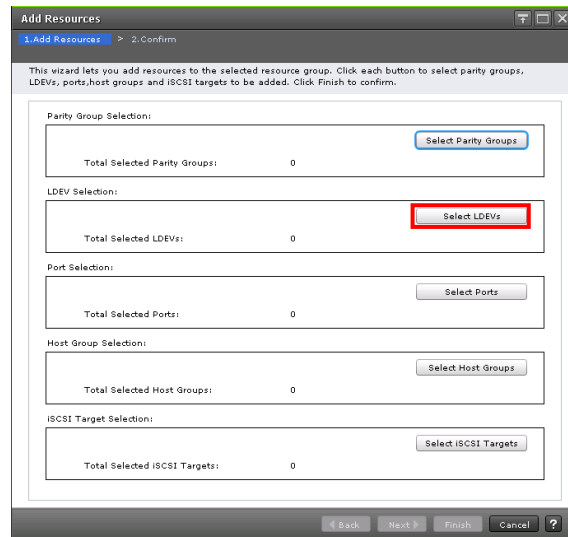
1. Select [Resource Groups] from the [Administration] tree in the “Web Console” window.
2. Click the resource group name to add LDEVs under [Resource Groups].
The individual “Resource Groups” window is displayed.



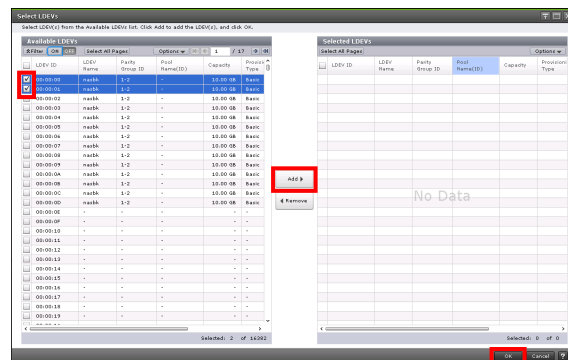
3. Display the “Add Resources” window in either of the following ways.
 - Click [Add Resources].
 - Select [Resource Administration] – [Add Resources] from the [Settings] menu.



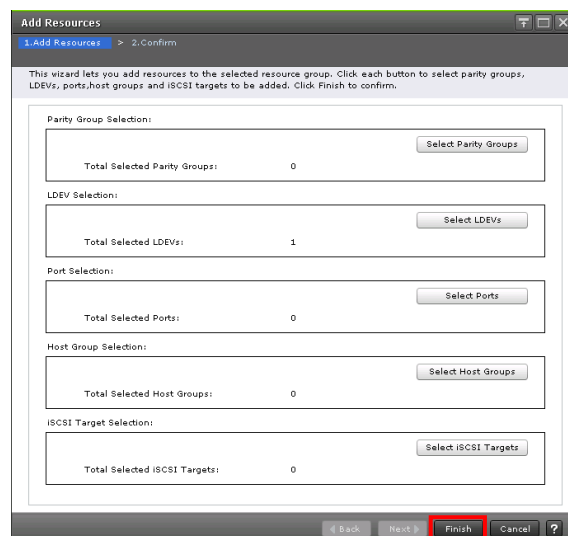
4. The “Add Resources” window is displayed. Click the [Select LDEVs] button.



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 the [OK] button.



6. Return to the “Add Resources” window. Click the [Finish] button.



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

[illegible]

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

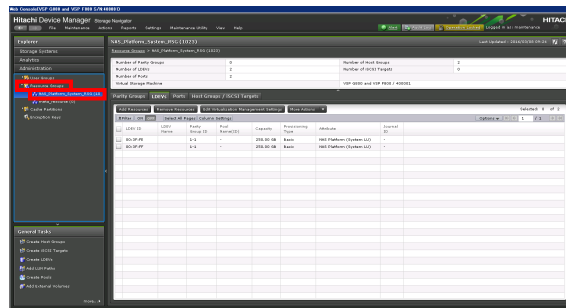
NOTE: To display the “Task” window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

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

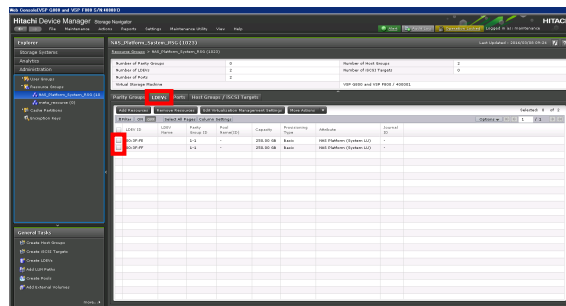
4.8.2 Removing LDEVs from Resource Group

Remove arbitrary LDEVs belonging to an arbitrary resource group.

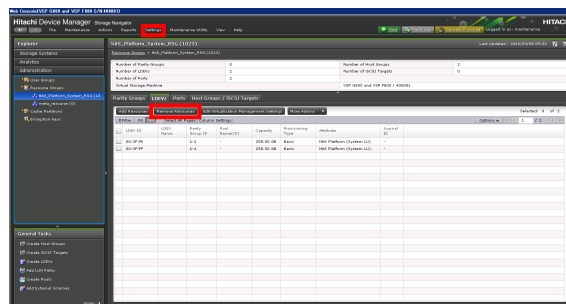
1. Select [Resource Groups] from the [Administration] tree in the “Web Console” window.
2. Click the resource group name to remove LDEVs under [Resource Groups].
The individual “Resource Groups” window is displayed.



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].

Remove Resources

1. Confirm

⚠ The selected resource(s) will be deleted from the selected resource group. Are you sure to continue?

Task Name: **55000-RemoveResource**
(max: 32 characters)

Selected Resource Group

Resource Group Name (ID)
Resource_group1_...

Selected LDEVs

LDEV ID	LDEV Name	Parity Group ID	Pool Name(ID)	Capacity	Provisioning Type	Attribute
00:3F:FE		1-1	-	250.00 GB	Basic	-

Total: 1

☒ Go to task window for status Back Next Apply Cancel ?

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.

4.9 Encryption Keys

NOTICE: The encryption settings are not available through the Web Console in the Maintenance PC. The menus and buttons become disabled due to “Not Authorized”. Perform the encryption settings through the Storage Navigator in the SVP.

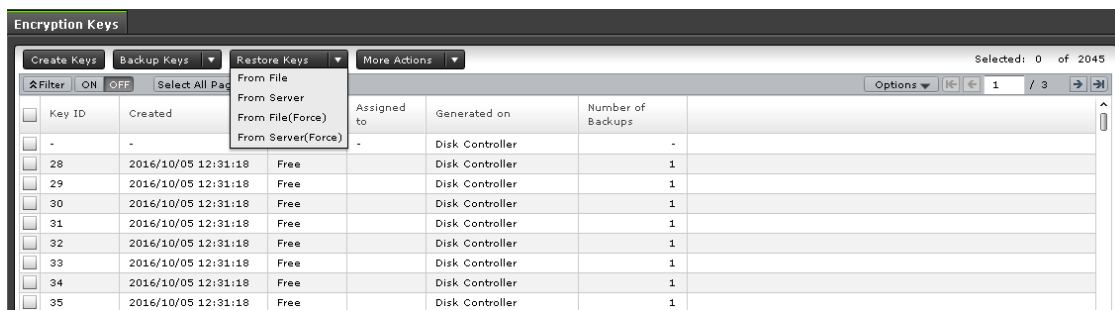
From the [Administration] tree menu in the navigation area in the left part of the Storage Navigator main window, click [Encryption Keys] to display the “Encryption Keys” window.

4.9.1 Force Restore Keys from File

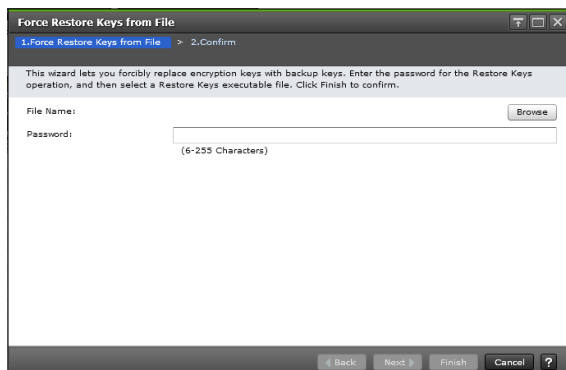
This function restores encryption keys from the files backed up in the SVP. Even the encryption key files to which the Restore Keys from File function cannot be applied can be restored with the Force Restore Keys from File function.

For the Restore Keys from File function, refer to “Encryption License Key User Guide”.

1. In the “Encryption Keys” window, click [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] button.

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

5. Click the [Apply] button 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 the [Apply] button 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 Board (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.

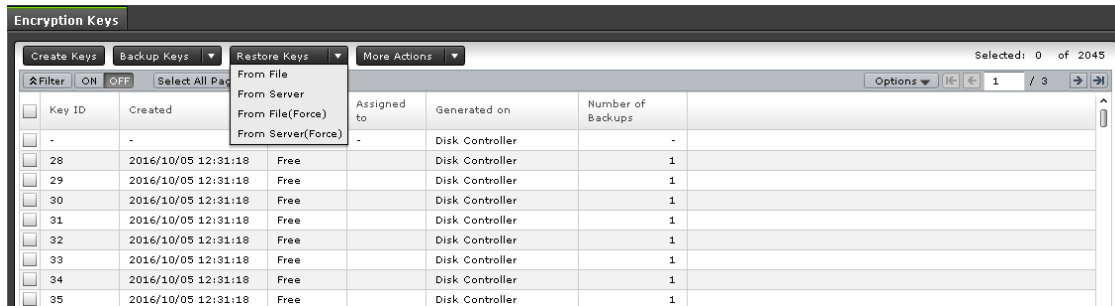
4.9.2 Force Restore Keys from Server

This function restores encryption keys by connecting to the key management server.

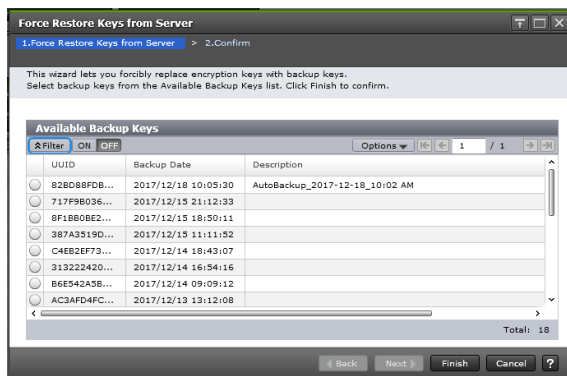
Even the encryption keys to which the Restore Keys from Server function cannot be applied can be restored with the Force Restore Keys from Server function.

For the Restore Keys from Server function, refer to “Encryption License Key User Guide”.

1. In the “Encryption Keys” window, click [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] button.

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

5. Click the [Apply] button 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 the [Apply] button 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 Board (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.

5. Maintenance Function of Maintenance PC

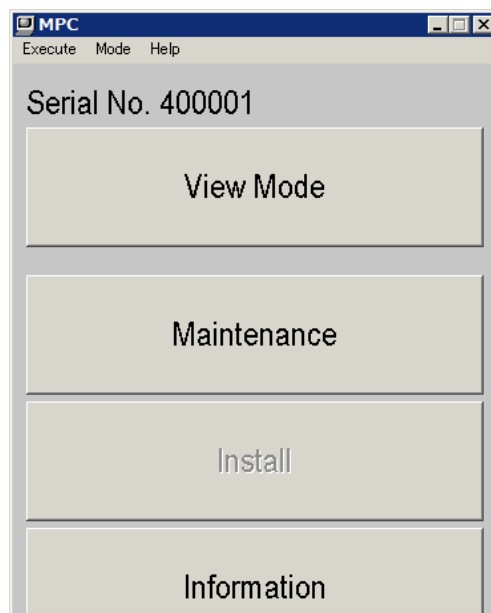
NOTICE: When a failure such as that the information cannot be acquired by the Storage System while operating the maintenance using the Maintenance PC, open the "Maintenance Utility" window and check the Storage System status. When a communication failure has occurred in the Storage System of the CTL connected to the Maintenance PC, perform the following operation, and then continue the maintenance operation.

- (1) When performing the maintenance operation by connecting the Maintenance PC to the maintenance port of CTL1
Connect the LAN cable connected to the maintenance port of CTL1 to the maintenance port of CTL2. Check that "Event ID = 1" is output in the event log of Windows at the time of the LAN cable connection or later (Refer to TROUBLESHOOTING SECTION "[3.30 Event log of MPC/SVP](#)")
- (2) When performing the maintenance operation by connecting the Maintenance PC to the maintenance port of CTL2
Connect the LAN cable connected to the maintenance port of CTL2 to the maintenance port of CTL1. Check that "Event ID = 0" is output in the event log of Windows at the time of the LAN cable connection or later (Refer to TROUBLESHOOTING SECTION "[3.30 Event log of MPC/SVP](#)")

5.1 Mode

1. <View Mode>

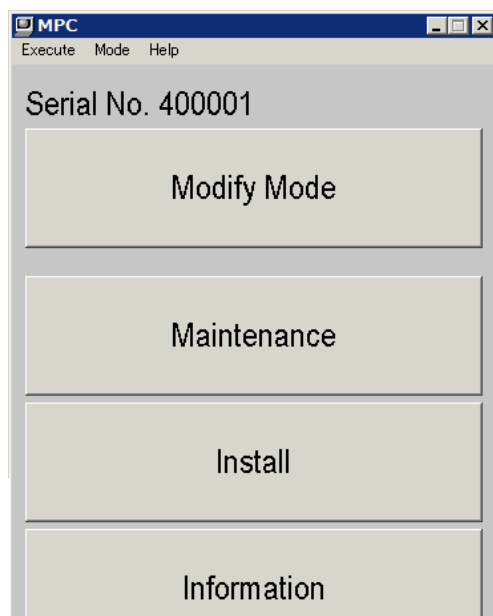
In View Mode, referring to the Storage System status is allowed.



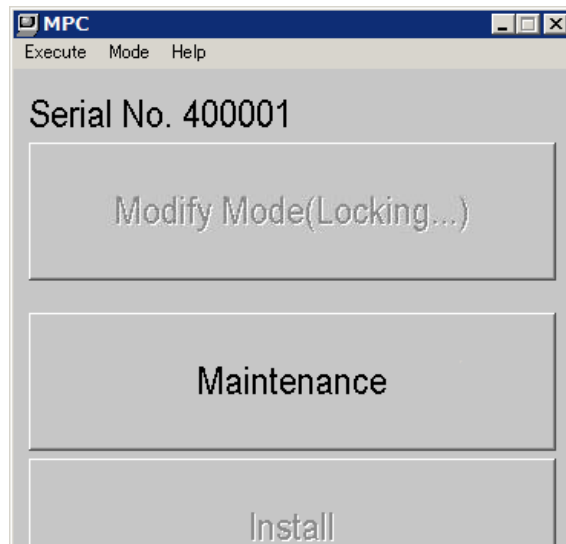
2. <Modify Mode>

In Modify Mode, referring to and changing the Storage System status are allowed.

For example, log/pin data indication and status display on Maintenance are available in any mode, but removing Cache Memory is available in only Modify Mode.



All the operations become impossible to execute until the lock processing to DKC ends when changing from View Mode to Modify Mode. (At this time, the display becomes Modify Mode(Locking...))



Moreover, all the operations become impossible to execute until the unlock processing to DKC ends when changing from Modify Mode to View Mode. (At this time, the display becomes Modify Mode(Unlocking...))



NOTE: When the communication between MPC Software-DKC has blockaded or an internal error occurs, the MPC mode becomes Modify Mode(Unlocked) by failing in the lock processing. Under such a condition, the maintenance operation that can be executed is limited. (Modes other than View and Modify are also similar)



Table 5-1 The Maintenance Operation that can be Executed when Mode is “(Unlocked)”

Operation	Pages
The maintenance operation that can be executed when Maintenance PC is View Mode.	-
Restore Configuration	FIRM05-20
Delete Log File	MPC05-450
Diagnosis (LAN Check etc.)	DIAG00-00
Auto Define Configuration	INST05-02-70

3. <Change Mode>

If you click the [View Mode] button, the mode changes from [View Mode] to [Modify Mode], and Maintenance PC changes to Modify Mode.

If you click the [Modify Mode] button, the mode changes from [Modify Mode] to [View Mode], and Maintenance PC changes to View Mode.

NOTICE: Observe the following cautionary notices after using the MPC Software.

- Exit the window opened.
- Change the operation mode to View Mode.
- If the above operation is not performed, a failure may not be notified because the Maintenance PC is judged to be under maintenance.
- MPC Software is a state of Modify Mode, and constitution change operation using Storage Navigator and copying duties using Storage Navigator CLI are not possible. When you make Modify Mode, please confirm influence on other customer use.

NOTICE: Encryption License Key (Program Product) has the periodical backup function of the encryption key.

During the backup of the encryption key, the mode cannot be changed to the Modify mode.

When the mode cannot be changed to the Modify mode, see the "Task" window in Web Console to check the status of the task name

[yymmdd-RegularBackupKeystoServer] (yymmdd = year, month, and date). If the task is being executed, wait for the task to be complete.

5.2 Dump

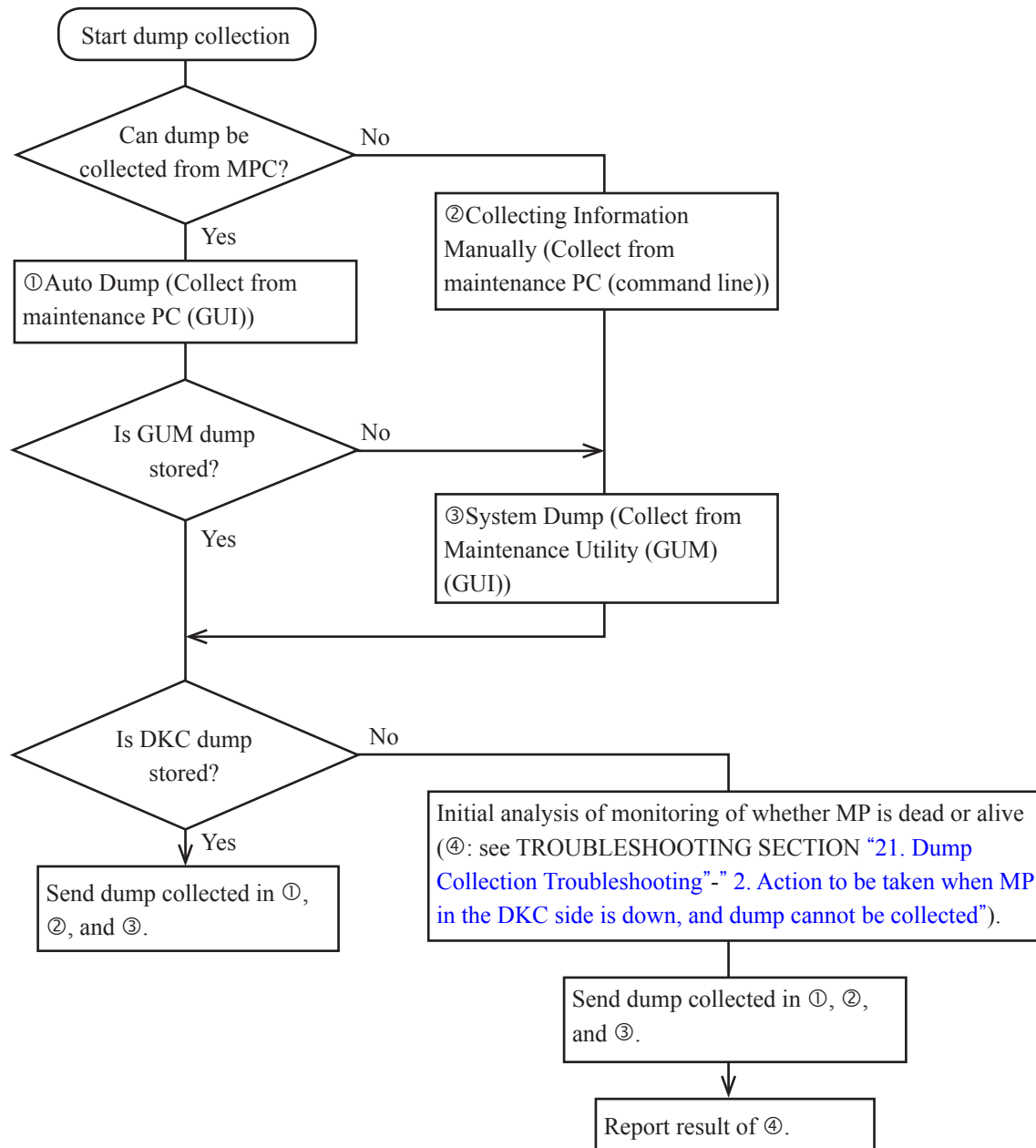
Collecting dumps has the following methods.

- NOTE:
- If any dump collection method is instructed by the Technical Support Division, perform the instructed operation.
 - If the maintenance PC is available with no instruction by the Technical Support Division, collect dumps using Auto Dump. See “[1] Auto Dump” for the procedure.
 - If the maintenance PC is not available with no instruction by the Technical Support Division, collect system dumps. See “3.27 Acquiring Dumps using Maintenance Utility” for the procedure.
 - To collect dumps after parts replacement, use Small System Dump in accordance with each part replacement procedure in REPLACEMENT SECTION. For the detailed procedure, refer to “3.27 Acquiring Dumps using Maintenance Utility”.
 - The dump capacity might be increased to up to about 3 GB due to accumulation of error log information (such as SIM and SSB).
 - The error information of up to 16 replaced drives is stored in the dump. You can collect the drive error information within the range of replacement of 16 drives.

Collection Method	Description
Auto Dump	Use Auto Dump unless otherwise instructed by the Technical Support Division. See “[1] Auto Dump” for the procedure.
Exporting Dump	Use this when the “MPC” window is not displayed or you cannot log into the “MPC Software” window. See “2.6.2 Starting the MPC Window from the MPC Software Window” for the procedure.
System Dump	Use this when no Maintenance PC exists or the Maintenance PC cannot connect to the Storage System. The collected dumps are equivalent to the “Normal” dump type of Auto Dump, (however the information stored in the maintenance PC is not collected). See “3.27 Acquiring Dumps using Maintenance Utility” for the procedure.
Small System Dump	Use this when collecting dumps after parts replacement. The collected dumps are equivalent to the “Rapid” dump type of Auto Dump, (however the information stored in the maintenance PC is not collected). For the detailed procedure, refer to “3.27 Acquiring Dumps using Maintenance Utility”.
Collecting Information Manually	Auto Dump cannot be used when a problem occurs in the storage system registration in Storage Device List. In that case, collect dumps manually in accordance with the procedure of “[3] Collecting dump files manually”.

If no dump collection method is instructed by the Technical Support Division, you can also see the following workflow for the dump collection procedure.

[Flow of dump collection]

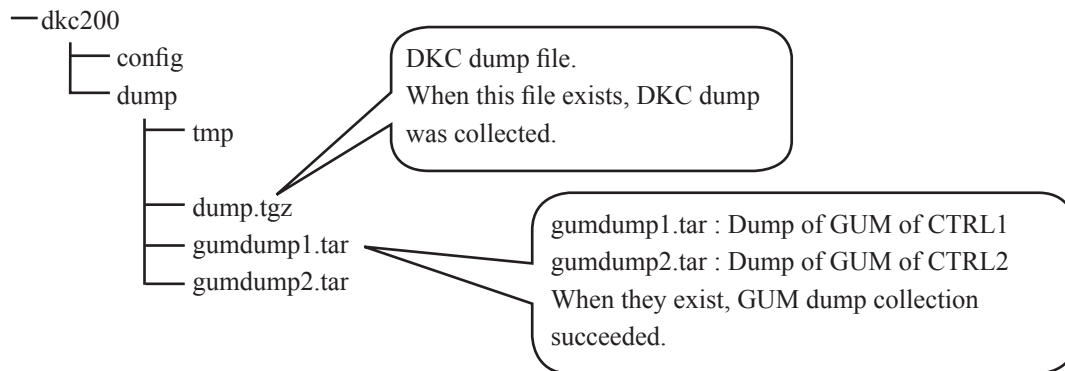


[How to check if DKC dump and GUM dump are stored]

When dump is collected from Maintenance PC or SVP, hdep.tgz is output as a compressed file. After the file is decompressed, the dump is extracted as follows.

—dkc200-dump-dump.tgz is the DKC dump.

—dkc200-dump-gumdump1.tar



For troubleshooting when an error occurs during dump collection, see TROUBLESHOOTING SECTION “[21. Dump Collection Troubleshooting](#)”.

Dumps other than the above are shown below. However, collect them only when instructed by the Technical Support Division or specified explicitly in the manual.

For FMD Dump, collect dumps if an error or performance problem occurs in the FMD.

Type	Collection Method
FMD Dump	See “ [2] FMD Dump ”.

NOTICE: The SVP information cannot be collected from the Maintenance PC. When collecting the SVP information is required, collect dumps from the SVP using the dump tool. See “Collecting dump files using the Dump tool” in the “System Administrator Guide” for the procedure.

[1] Auto Dump

Auto Dump is a useful function to provide the user with free selection of the dump data type and the output media so that the user can collect dump information.

NOTICE:

- Check that the dump tool is not performed in the SVP. If Auto Dump is performed while the dump tool is running in the SVP, the acquired dump data might be lost.
- Check that the system dump or small system dump is not performed in Maintenance Utility. If Auto Dump is performed while the system dump or small system dump is running, the acquired dump data might be lost.

1.

Select [Maintenance Components (General)] from the tool bar [Maintenance] in the “Web Console” window. See [“2.2 Connecting Maintenance PC to Storage System”](#) for how to attach LAN cables for the Maintenance PC”

2.

Click the [Auto Dump] button in the “MPC” window to display the “Select Dump Type” window.

NOTE: Clicking the [Export Dumps] button in the “MPC Software” window can also display the “Select Dump type” window.

3.

Select a dump type and a medium for output and make settings of the FTP transfer detail and the Client PC output detail, etc., and then click the [OK] button.

To stop the operation, click the [Cancel] button.

- NOTE:
- If you execute the TOD setting during collecting the Port Dump, the collecting the Port Dump may fail. Then, please execute collecting the Port Dump again.
 - The Output file name for replacement is enabled only when selecting “Rapid” by the dump type selection.
 - Windows displayed by Auto Dump might be hidden behind a different window. If so, press [Alt] + [Tab] keys to switch tasks, and select [Dump] or [Auto Dump] to display a window or message box.

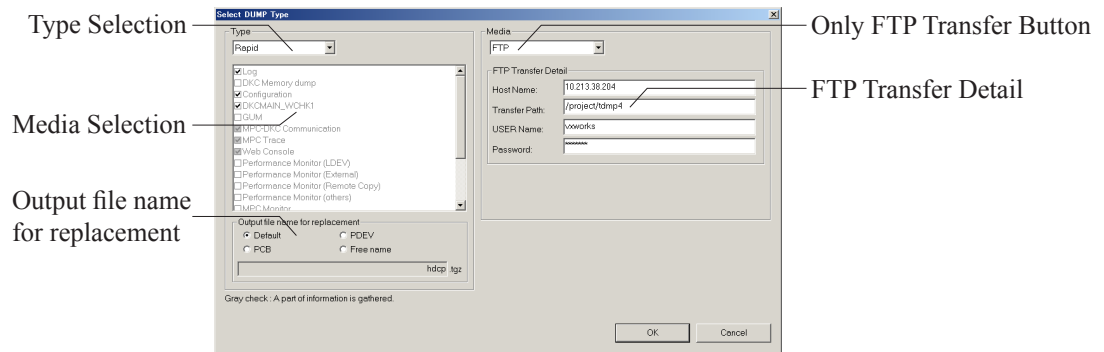


Table 5-2 Media in the Select Dump Type Window

Menu	Description
Rapid	<p>This dump type is to get log information, Maintenance PC operation history, configuration information. Maintenance PC will compress these files automatically.</p> <p>This dump type will be used when the initial analysis of error is needed. In this case, you should collect the files used by this type and send it to the Center. After sending this files, you should collect dump data by selecting “Normal” type and send it to the Center to analyze more details.</p>
Normal	<p>This dump type is to get DKC Memory dump data (you can get DUMP information of All PCB) adding to the log files used by “Rapid” type. Maintenance PC will compress these dump files automatically. You should get dump data by using this dump type after sending the “Rapid” type of data to Center.</p>
Detail	<p>This type is to get monitor information adding to the dump files used by “Normal” type. (You can not get performance monitor information.) This data will be needed when the performance of the DKC wants to be checked. If there is no order to get these data, you do not need to use this type.</p>
DUMP	The dump of this type selects the processors and gets dumps from them individually.
GUM	The dump of this type collects GUM traces. They are collected from both CTL1 and CTL2.
LOG	The dump of this type collects Rapid Dump information only. The dump is used when it is required to send only the log information immediately to the Technical Support Division before making the initial analysis.
Monitor	The dump of this type collects all monitor information and configuration information.
Config Backup	The dump of this type collects the configuration information backup data stored in a hard disk of the Maintenance PC.
Custom	<p>The dump of this type selects source items from the detailed information items and collects information from them. (Refer to Table 5-3)</p> <p>When none of the detailed information items is checked off, the function of the dump of this type becomes the same as that of the dump whose type is “No Gather”.</p>
No Gather	<p>The dump of this type only outputs “C:\Mapp\wk\88xxxxyyyyyy\dkc200\tmp\”, which has already been collected, to a directory set by the FTP transfer destination detail without compressing the data.</p> <p>The dump of this type can collect information only when “C:\Mapp\wk\88xxxxyyyyyy\dkc200\tmp\” exists and FTP is selected as a medium.</p> <ul style="list-style-type: none"> • xxxx : Model name of DKC • yyyyyy : Serial number
MPC Memory dump	The dump of this type collects MPC Memory dump.

Table 5-3 Detailed Gathering Items in the Select Dump Type Window

Menu	Description
DKC Memory dump	SM, PM, LM, SYS, LCP, Configuration information
Configuration	Maintenance PC Configuration information
DKCMAIN_WCHK1	WCHK1 Dump
Performance Monitor	Performance information
Log	Rapid Dump
GUM	GUM trace Core file, trace, error log, configuration information of GUM itself, hard register dump
MPC-DKC Communication	Communication dump, HOSTS file others*.dat
MPC Trace	Trace under "C:\Mapp\wk\88xxxxyyyyyy\dkc200\tmp\", log information, Maintenance PC registry information <ul style="list-style-type: none"> • xxxx : Model name of DKC • yyyyyy : Serial number
Web Console	Web Console information
MPC Monitor	Monitor information
Pin/Verify	Pin/Verify information
Configuration Backup	100-generation configuration Backup information (For analysis)
MPC Memory dump	MPC memory dump

Table 5-4 Output File Name for Replacement in the Select Dump Type Window

NOTE: To collect dumps continuously, change the dump file name not to be overwritten.

Menu	Description
Default	Outputs dumps by the file name "hdcg.tgz".
PDEV	Outputs dumps by the file name for replacing PDEV parts. The details of the file name to be output are as shown below. <ul style="list-style-type: none"> • "PDVHMyyyyyy_YYMMDDhhmmss.tgz" • yyyyyy: Serial number • YYMMDDhhmmss: Creation time (YY: last two digits of Western calendar, MM: month, DD: day, hh: hour, mm: minute, ss: second)
PCB	Outputs dumps by the file name for replacing the parts other than PDEV. The details of the file name to be output are as shown below. <ul style="list-style-type: none"> • "xxxxxxxxxxx_HMyyyyyy_YYMMDDhhmmss.tgz" • yyyyyy: Serial number • YYMMDDhhmmss: Creation time (YY: last two digits of Western calendar, MM: month, DD: day, hh: hour, mm: minute, ss: second)
Free name	Outputs dump files by the character string entered in the edit box.

Table 5-5 Media in the Select Dump Type Window

Menu	Description
HDD	<p>Maintenance PC will store the compressed files to HDD. The file name is "C:\Mapp\wk\88xxxxyyyyyy\dkc200\tmp\". If you can transfer the files to your center directly, this type will be useful.</p> <ul style="list-style-type: none"> • xxxx : Model name of DKC • yyyyyy : Serial number <p>NOTE: Operating the maintenance may delete the compressed data. When performing the maintenance after data collection, transfer the data first.</p> <p>NOTE: When changing the file name setting by the Output file name for replacement, the file name to be output might be different from hdep.tgz.</p>
FTP	<p>After the compression processing end, Transfer processing of compression data is performed to the transfer place directory of a specification server inputted into FTP Transfer Detail.</p>

Table 5-6 FTP Transfer Detail in the Select Dump Type Window

Menu	Description
Host Name	The host name of a FTP transfer place or an IP address is inputted. (*1)
Transfer Path	The directory of a FTP transfer place is inputted.
USER Name	The user name which login to a FTP server is inputted.
Password	The password which login to a FTP server is inputted.

*1: It is in between "[" and "]" when you input the address of IPv6.
(Eg.) [0000:0000:0000:0000:0000:0000:0000:0000]

4. Gather Dump and compressing data

When selecting “Normal”, “Detail”, “GUM”, or “Custom” (in the case of selecting “GUM” in the detailed gather items) for a dump type, GUM is gathered.

Go to [Step \(1\)](#).

When selecting “Rapid”, “DUMP”, or “Log” for a dump type, DUMP collection is performed after the refreshment operations for the DKC configuration information.

Go to [Step \(2\)](#).

When selecting “Custom” (in case of selecting any of “Log”, “DKC Memory dump”, and “DKCMAIN_WCHK1” in the detailed gather items) for a dump type, DUMP is gathered.

Go to [Step \(3\)](#).

When selecting “No Gather”, a message, “Do you want to output the already gathered dump information, log information, Maintenance PC operation history and operation information without gather them again?” is displayed. Clicking the [OK] button outputs the gathered ones to the selected media. It is not possible to output to HDD.

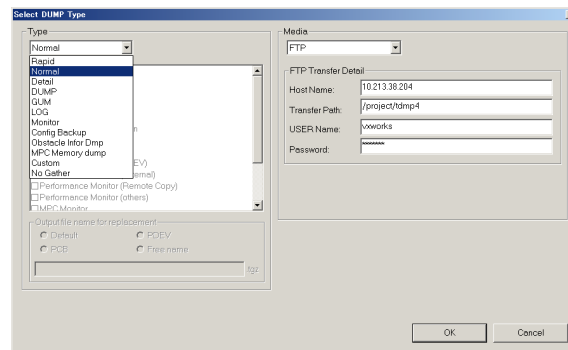
Go to [Step \(5\)](#).

When selecting “Custom” (in the case of not selecting any of “Log”, “DKC Memory dump”, “DKCMAIN_WCHK 1”, or “GUM” but selecting any other dump types in the detailed gather items) for a dump type, the data compression is performed.

Go to [Step \(4\)](#).

When selecting other dump types, data is compressed is performed after the refreshment operations for the DKC configuration information.

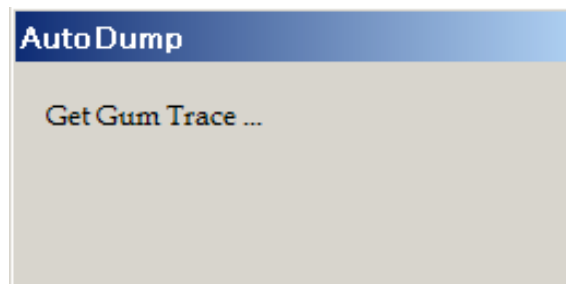
Go to [Step \(2\)](#).



(1) GUM Gather

The GUM gather GUM progress window is displayed.

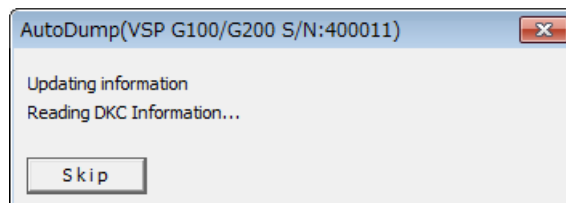
- When selecting “Custom” (in the case of selecting any of “Log”, “DKC Memory dump”, or “DKCMAIN_WCHK1” in the detailed gather items), DUMP collection is performed.
Go to [Step \(3\)](#).
- When selecting “Custom” (in the case of not selecting any of “Log”, “DKC Memory dump”, or “DKCMAIN_WCHK1” in the detailed gather items), DUMP collection is not performed.
Go to [Step \(4\)](#).
- When selecting other than the above mentioned.
Go to [Step \(2\)](#).



(2) Refreshment operations for DKC configuration information

When selecting other than “Custom”, the refreshment operations are performed to capture the latest DKC configuration information during Dump collection. The dialog box with message indicating that the refreshment process is in progress is displayed on the upper left of the MPC screen.

- When selecting “Rapid”, “Normal”, “Detail”, or “Custom” (in the case of selecting any of “Log”, “DUMP”, or “DKCMAIN_WCHK 1” in the detailed gather items) for a dump type, DUMP collection is performed.
Go to [Step \(3\)](#).
- When selecting other than the above mentioned, DUMP collection is not performed.
Go to [Step \(4\)](#).

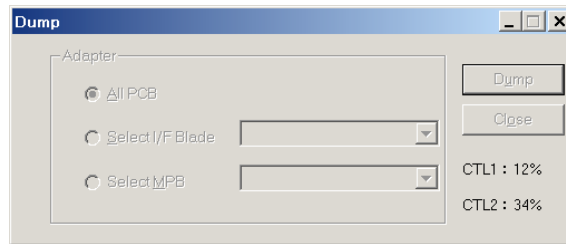


NOTE: Do not click the [Skip] button in the dialog box unless any instruction is provided by the Technical Support Division. The collection time might be extended in cases like a large amount of PIN is generated in the system, and therefore if the PIN information is not required, the collection can be skipped. Even if the collection of the PIN information is skipped, other DKC configuration information is updated to the latest.

(3) DUMP Gather

(a) The progress of DUMP gather

A box indicating progress of the dump is displayed.

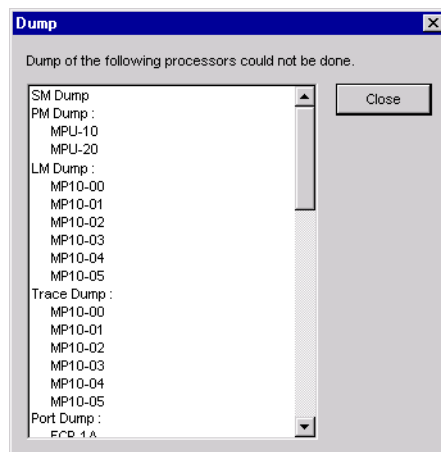


When the dump terminates normally, go to [Step \(4\)](#).

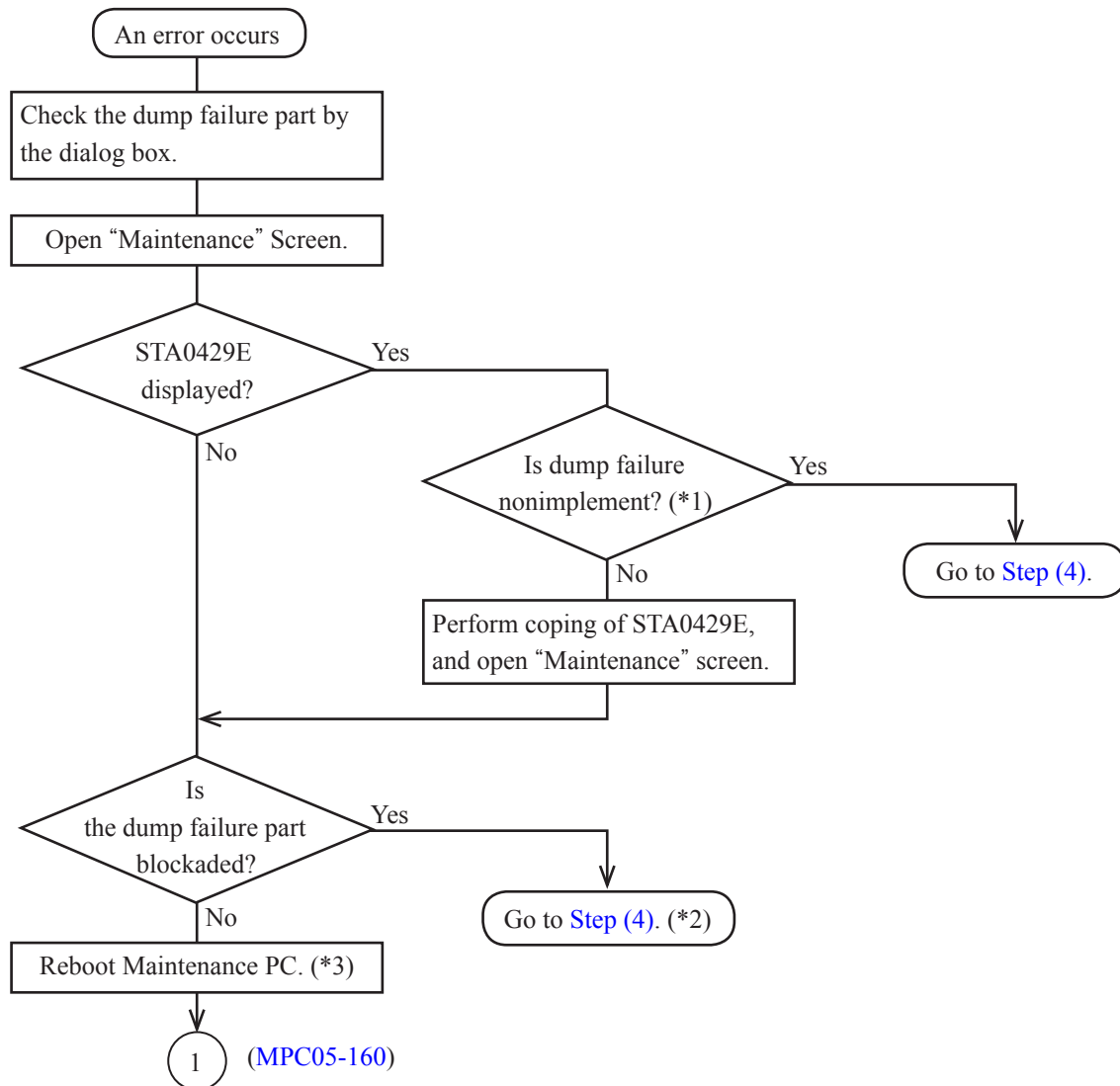
(b) When an error occurs

When an error occurs, the following dialog box is displayed.

For the action, retry it in accordance with [\[Dump Gather Procedure when Errors Occur\]](#) ([MPC05-150](#)).



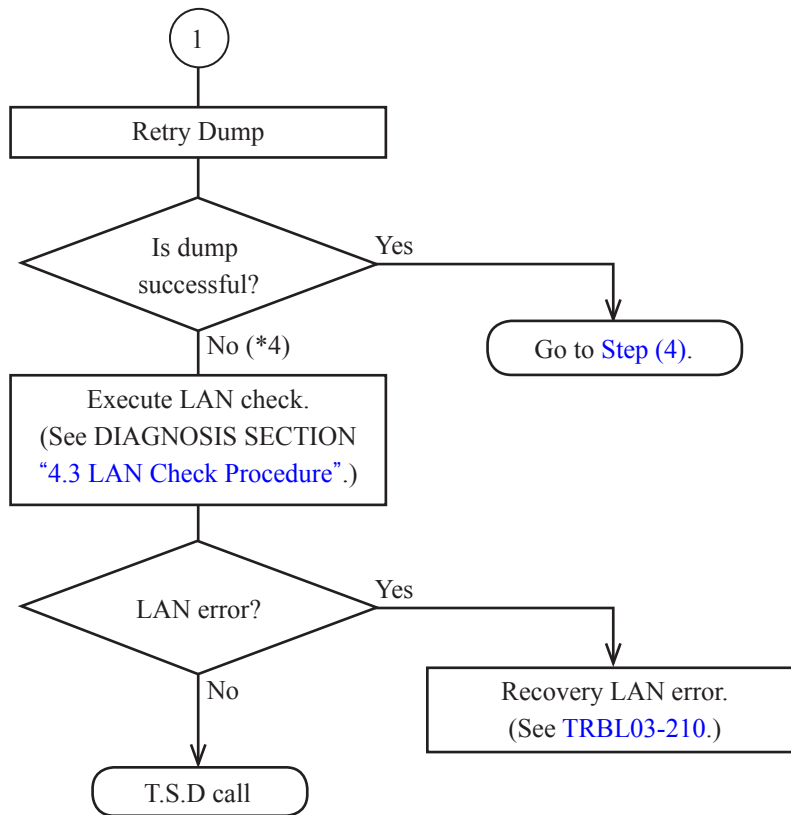
[Dump Gather Procedure when Errors Occur]



*1: Please confirm the implementation of the part where dump failed by viewing.

*2: The dump fails because the dumping is impossible for the blockade portion and the Port dump linked to the blockaded processor is also impossible.

*3: Before rebooting the Maintenance PC, check that the settings specified in "1.3.4 Setting of Antivirus Program" are set correctly. If they are not set correctly, the dump gather might fail due to occurrence of a communication error.

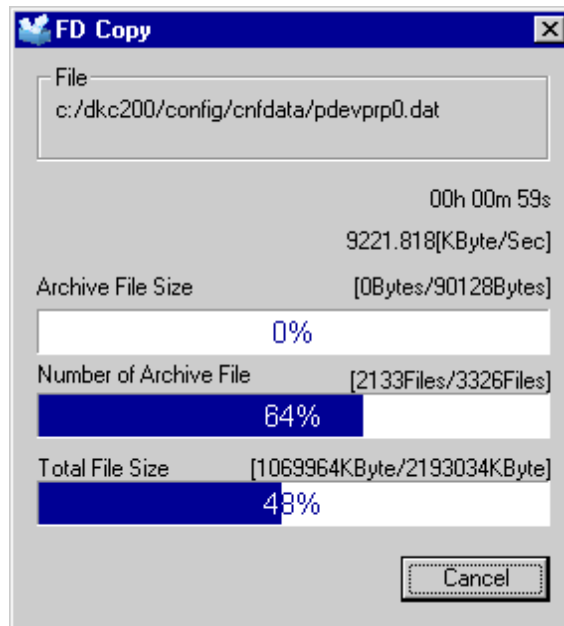


*4: Check the blockaded part by the Maintenance.

(4) Data compression

The “FD Copy” window is displayed and a data compression is done.

Go to [Step \(5\)](#).



(5) Output of the gathered files

A message, “[3701] Do you want to output the already gathered dump information, log information, Maintenance PC operation history and operation information without gathering them again?” is displayed.

Click the [OK] button.

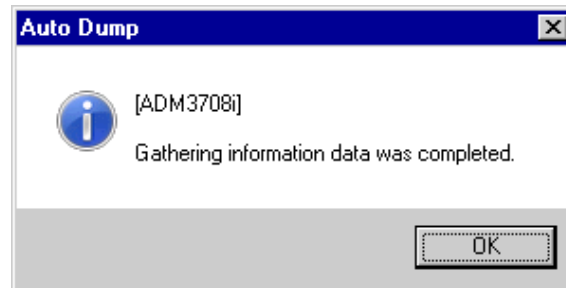
Go to [Step 5](#).

5. Output to a selected medium.
An output is done to a selected medium

When an HDD was selected, go to [Step \(1\)](#).

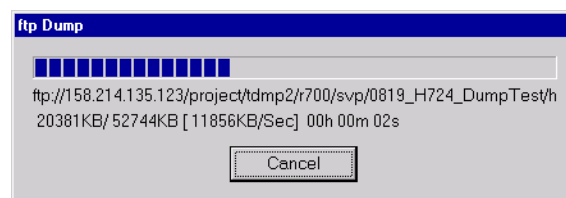
When an FTP was selected, go to [Step \(2\)](#).

- (1) When the HDD is selected as a medium for the output
 - (a) A message, “[3708] Gathering information data was completed.” is displayed. Click the [OK] button.

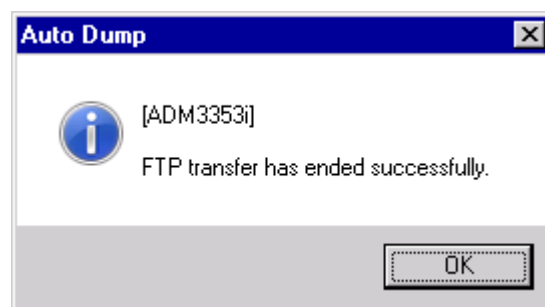


- (b) Check that the dump file is stored in the following [Storage Destination].
[Storage Destination]: The dump file is stored under the “C:\Mapp\wk\88xxxx (DKC model name) yyyyyy (serial number) \dkc200\tmp” directory of the Maintenance PC.
The file name follows the setting in [Table 5-4](#). The default name is “hdcp.tgz”.

- (2) When the FTP is selected as a medium for the output
 - (a) When the [FTP] was selected as the media for the output, a transfer of the compressed data is started.



- (b) After the data transfer is completed, a message, “[3353] FTP transfer has ended successfully.” is displayed.
Click the [OK] button.



- (c) Check that the dump file is stored in the following [Storage Destination].
- [Storage Destination]: The dump file is stored in the transfer destination directory of the specified server entered in “FTP Transfer Detail”.
- The file name follows the setting in [Table 5-4](#). The default name is “hdcp.tgz”.

[2] FMD Dump

The FMD Dump is the dump to collect the operational information of FMD and includes the following:

- Information on hardware operation within FMD
- Information on errors within FMD
- Information on endurance of flash memory chip
- Information on performance of FMD
- Trace of firmware operation of FMD

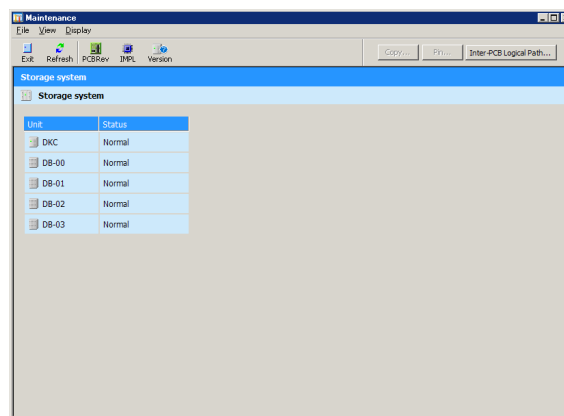
1. <Initial screen>

Select [Maintenance Components (General)] from the tool bar [Maintenance] in the “Web Console” window.

For Attaching the LAN cables for the Maintenance PC, see [“2.2 Connecting Maintenance PC to Storage System”](#).

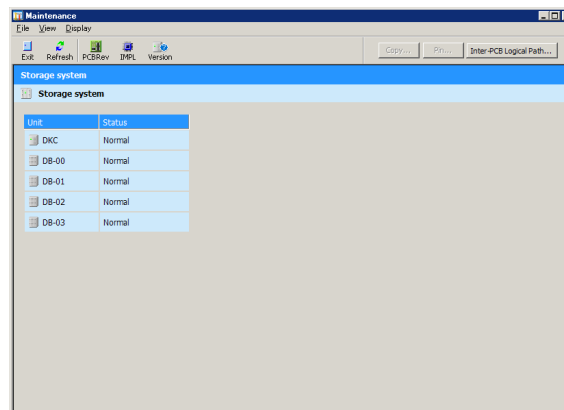
2. <Maintenance window>

Click the [Maintenance] button, the “Maintenance” window is displayed.



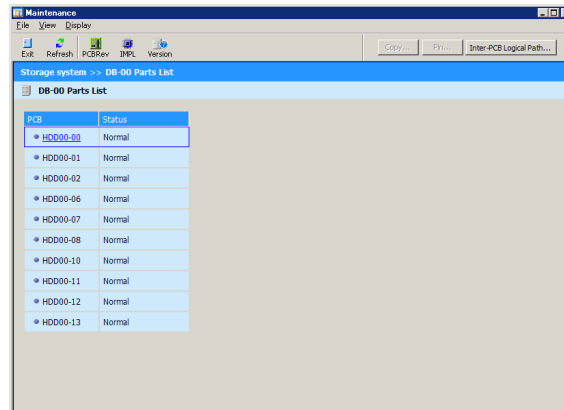
3. <Maintenance window>

Click the DB information [DB-nn] of the DB which installs the HDD to be replaced in the “Maintenance” window.



4. <Select HDD>

Check and click HDDmm-nn to be replaced.

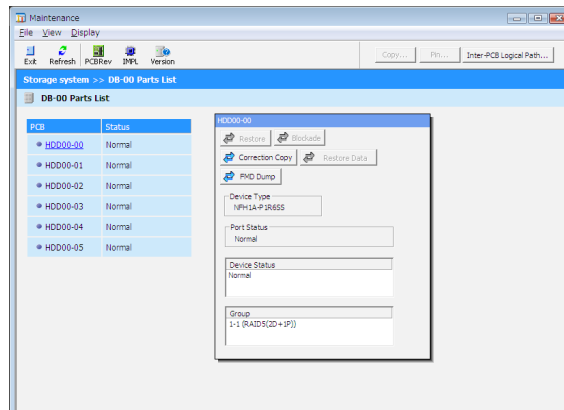


5.

Make sure that the “Device Status” is [Normal].

NOTE: Open the “Logical Devices” window from the “Storage System” tree in the “Web Console” window and make sure that the LDEVs in the parity group containing the selected HDD are not being formatted (excluding Quick Format).

Click the [FMD Dump] button.



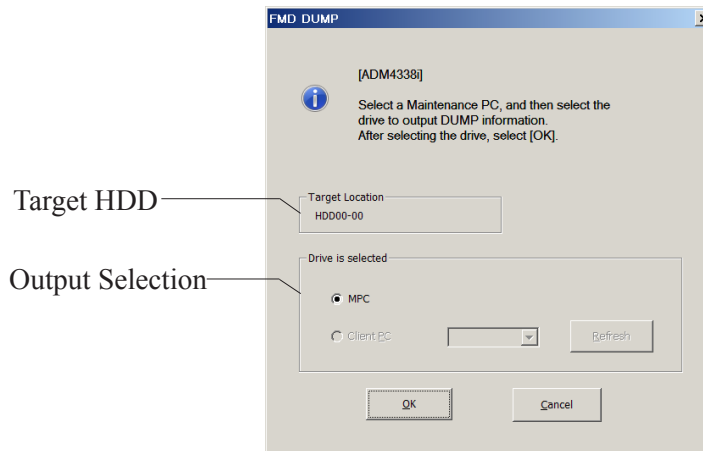
6.

Check the target HDD and output destination in the “FMD DUMP” [4338] window.

Click the [OK] button and go to [Step 7](#).

Click the [Cancel] button to stop the operation. Click the [OK] button for the displayed confirmation message and return to the “Maintenance” window.

NOTE: To collect dumps continuously, change the dump file name not to be overwritten.



<<Output Detail>>

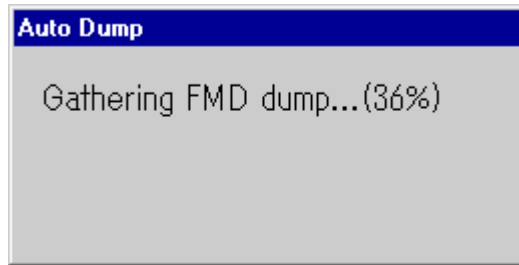
- MPC:

Dump data is output to the “C:\Mapp\wk\88xxxxyyyyyy\DKC200\others” directory of the Maintenance PC.

- xxxx : Model name of DKC
- yyyyyy : Serial number

7. FMD Dump Start

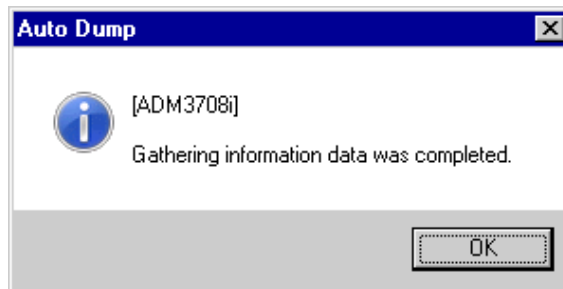
The progress of “Gathering FMD dump...” is displayed.



8. FMD DUMP gathering was completed

Gathering information data was completed

A message, “[3708] Gathering information data was completed.” is displayed. Click the [OK] button.



9. <Maintenance window>

Close the “Maintenance” window if there is no problem.

10. Check that the dump file is stored in the following [Storage Destination].

[Storage Destination]: The dump file is stored in the “C:\Mapp\wk\88xxxx (DKC model name) yyyyyy (serial number)\dkc200\others” directory of the Maintenance PC.

[3] Collecting dump files manually

If a problem occurs during the Storage System registration, Auto Dump might not be used. In that case, collect the files shown in the following manually collected file list.

Manually collected file list

- <installDir>\wk\supervisor\dkcman\log*.*
- <installDir>\wk\supervisor\dkcman\cnf*.*
- <installDir>\wk\supervisor\rmiserver\log*.*
- <installDir>\wk\supervisor\rmiserver\cnf*.*
- <installDir>\wk\supervisor\sdlist\log*.*
- <installDir>\wk\supervisor\mappiniset\logs\MappIniSet*.*
- <installDir>\wk\supervisor\mappiniset\mpprt\cnf
- <installDir>\wk\supervisor\portmanager\logs\PortManager*.*
- <installDir>\wk\supervisor\restapi\data
- <installDir>\wk\supervisor\restapi\logs
- <installDir>\wk\supervisor\restapi\build.json
- <installDir>\wk\supervisor\restapi\version.json
- <installDir>\wk\supervisor\system\log*.*.log
- <installDir>\OSS\apache\logs*.*.log
- <installDir>\OSS\apache\logs\ssl*.*.log
- <installDir>\OSS\jetty\logs*.*.log
- <installDir>\wk\[serial number]\DKC200\config*.*.cfg
- <installDir>\wk\[serial number]\DKC200\mp\pc*.*.dbg
- <installDir>\wk\[serial number]\DKC200\mp\pc*.*.dmb
- <installDir>\wk\[serial number]\DKC200\mp\pc*.*.dmp
- <installDir>\wk\[serial number]\DKC200\mp\pc*.*.inf
- <installDir>\wk\[serial number]\DKC200\mp\pc*.*.ini
- <installDir>\wk\[serial number]\DKC200\mp\pc*.*.trc
- <installDir>\wk\[serial number]\DKC200\others\commdata*.*
- <installDir>\wk\[serial number]\DKC200\san\cgi-bin\utility\log*.*
- <installDir>\wk\[serial number]\DKC200\san\SN2\SN2\logs*.*
- <installDir>\wk\[serial number]\DKC200\san\SN2\SN2Files\logs*.*
- %USERPROFILE%\AppData\LocalLow\Sun\Java\Deployment\log
- %WINDIR%\system32\config\SysEvent.Evt
- %WINDIR%\system32\config\SecEvent.Evt
- %WINDIR%\system32\config\AppEvent.Evt
- %WINDIR%\minidump*.*.dmp
- %WINDIR%\System32\Winevt\Logs\Application.evtx
- %WINDIR%\System32\Winevt\Logs\Security.evtx
- %WINDIR%\System32\Winevt\Logs\System.evtx
- %WINDIR%\system32\drivers\etc\HOSTS*
- %WINDIR%\system32\drivers\etc\services*
- c:\SetupTrace*.*

- NOTE:
- <installDir>...indicates the installation directory of the Maintenance PC.
 - %USERPROFILE%... indicates a folder of the installation login user of the Maintenance PC.
(=C:\Users\<User name>)
 - %WINDIR%...indicates a Windows folder in the system drive.
(=C:\Windows)
 - One or more of these files might not exist depending on the environment. Ignore the files which do not exist.

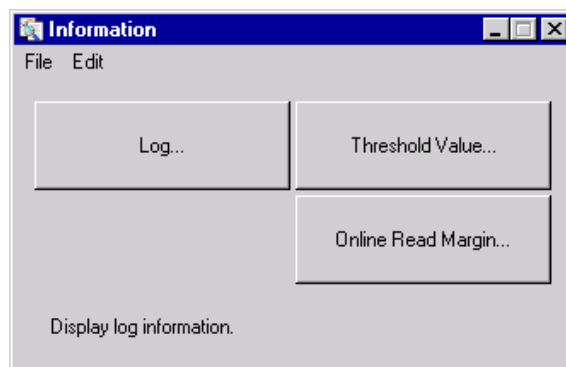
5.3 Log

5.3.1 Log Indication

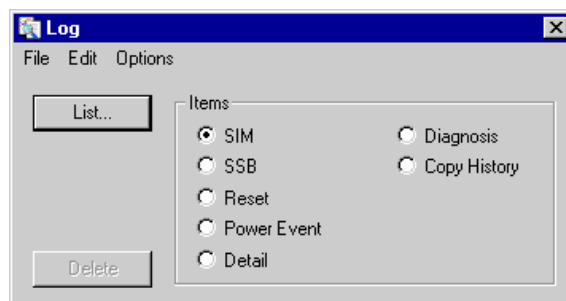
[1] SSB Log -----	MPC05-260
[2] SIM Log -----	MPC05-310
[3] Detail Log -----	MPC05-340
[4] Reset Log -----	MPC05-360
[5] Power Event Log -----	MPC05-380
[6] Diagnosis Log -----	MPC05-390
[7] Copy History Log -----	MPC05-410
[8] MP# - Location correspondence table -----	MPC05-430
[9] Port - Location correspondence table -----	MPC05-440

Prerequisite Operation:

1. Click the [Information] button.
-
2. Click the [Log...] button.



3. The "Log" window is displayed.



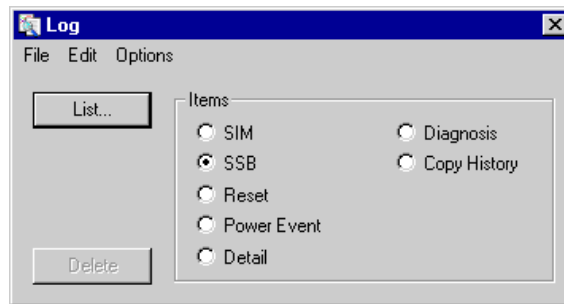
[1] SSB Log

Display the SSB detected by the DKC, GUM, and Maintenance PC.

1.

Click the [SSB] button in the “Log”.

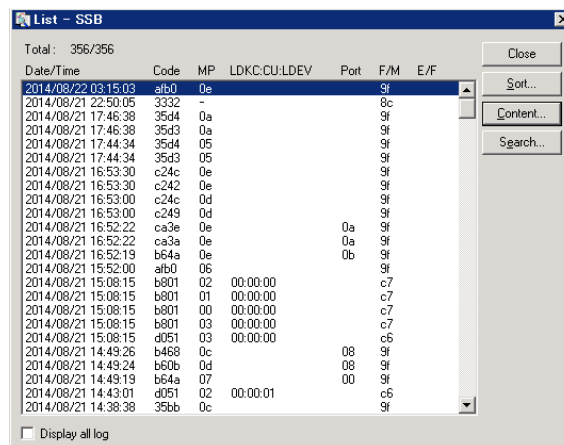
Click the [List...] button.



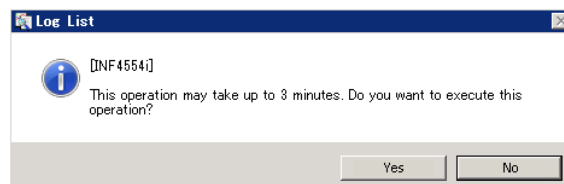
NOTE: When the DKC communication error has occurred, the SSB of the successful acquisition and the SSB stored on the Maintenance PC are displayed.

2.

Select the data to be indicated in the “List-SSB” window and click the [Content...] button.

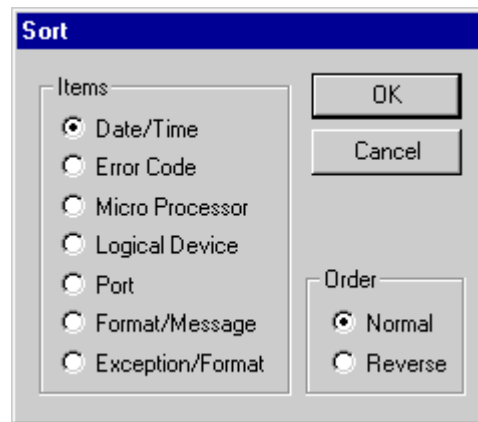


When displaying all the SSBs stored in the DKC, check the [Display all logs] checkbox. After that, click the [Yes] button in the displayed message [4554].



NOTE: To sort and list items, click the [Sort...] button first.

Then, select the desired item in the [Items] and [Order] options in the “Sort” window, and click the [OK] button.



NOTE: • To search for the desired log, click the [Search...] button. (Refer to [Step \(1\)](#))

Then set the log for which you want to search individual List in the “SSB Search Condition” dialog box and click the [OK] button.

• Please do not change an application’s window until search function finish.

(1) <SSB Search Condition dialog>

Click the [Partial] button of “Date/Time”, “Format/Message”, “LDEV”, “PDEV(C/R)”, “Error Code”, “Processor” and “Port” to search, and enter a value. When you search “SSB Data”, click the [Byte Match] button and enter a value.

(a) Common

Search within previous result : To search in previously searched logs.

All : Condition for search in the same flame becomes invalid.

Partial : Condition for search in the same flame becomes effective.

(b) Date/Time

From : Enter the oldest date and time of data to search.

To : Enter the latest date and time of data to search.

NOTE: When the [Partial] in the [Date/Time] group is selected, enter "00" in [hh], [mm] and [ss] of [From], and enter the current time in those of [To].

(c) Format/Message

F/M : Enter Format/Message of data to search.

E/F : Enter Exception/Format of data to search.

(d) LDEV

LDKC : Enter LDKC # of data to search.

CU : Enter CU # of data to search.

LDEV : Enter LDEV # of data to search.

(e) PDEV(C/R)

Enter PDEV# of data to search.

(f) Error Code

Enter Error Code of data to search.

Exception : Enter Error Code of data to except from a search.

(g) Processor

Select a location name of data to search from combo box.

NOTE: When the [Partial] in the [Processor] group is selected, the list of location names is displayed in a combo box.

(h) Port

Enter Port number of data to search.

NOTE: Refer to a [9] Port - Location correspondence table.(MPC05-440)

(i) SSB Data

Byte Match : To enable a search of [SSB Data].

Byte No1 : Enter a position of the byte to search.

Byte Pattern1 : Enter a value to search in a position of the byte specified in [Byte No1].

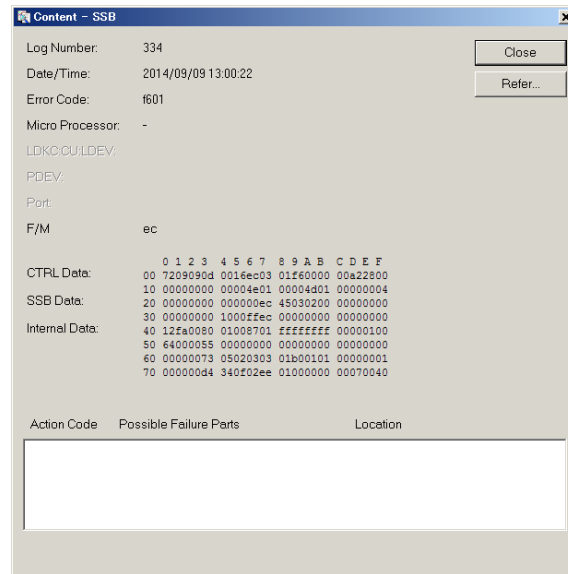
Byte No2 : Enter a position of the byte to search.

Byte Pattern2 : Enter a value to search in a position of the byte specified in [Byte No2].

3.

The detailed data is displayed in the “Content-SSB” window.

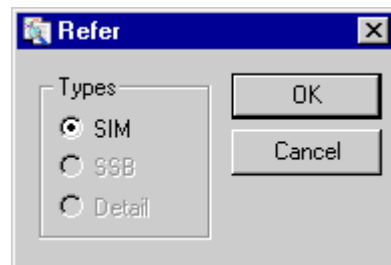
Click the [Refer...] button in the “Content-SSB” window to display the relative log.



4.

Select the log to be displayed in the “Refer” window.

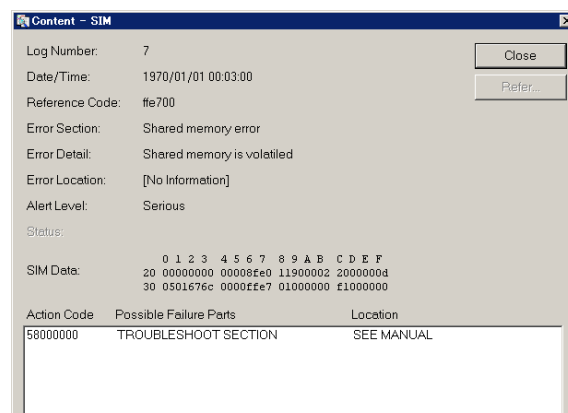
([SIM] is selected in this example.)



5.

Display the log to be selected.

(“Content-SIM” is displayed in this example.)



6.

Close the relative log when it is referred to.

Click the [Close] button in the “Content-SSB” window.

Click the [Close] button in the “List-SSB” window.

Close the “Log” window and close the “Information” window.

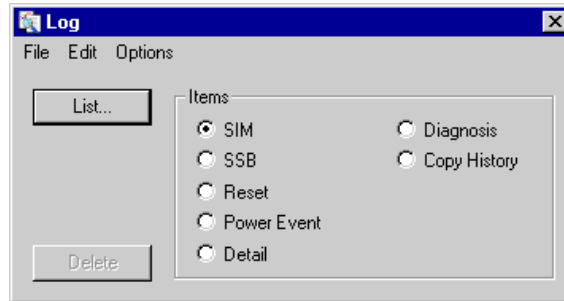
[2] SIM Log

Display the SIM detected by the DKC and GUM.

1.

Click the [SIM] button in the “Log” window.

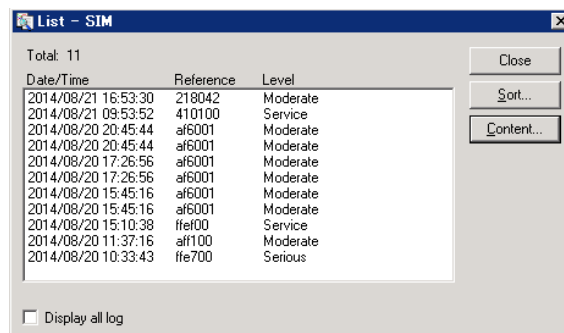
Click the [List...] button.



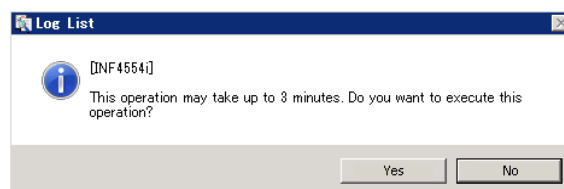
NOTE: When the DKC communication error has occurred, the SIM of the successful acquisition is displayed.

2.

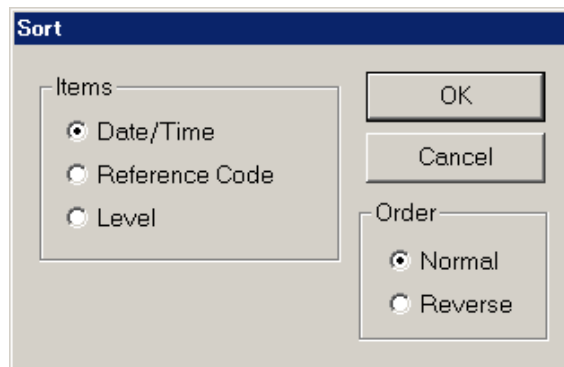
Select the data to be indicated in the “List-SIM” window and click the [Content...] button.



When displaying all the SSBs stored in the DKC, check the [Display all logs] checkbox. After that, click the [Yes] button in the displayed message [4554].



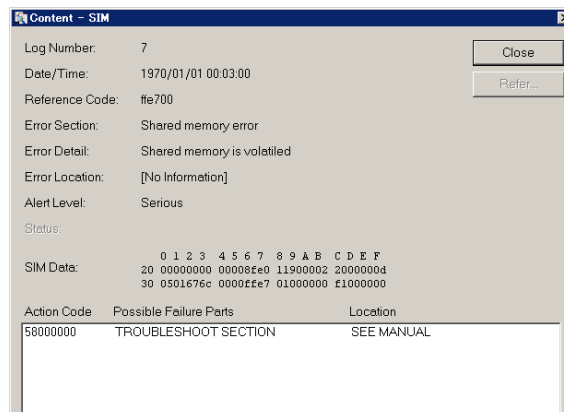
NOTE: To sort and list items, click the [Sort...] button first.
Then select the desired item in the [Items] and [Order] options in the “Sort” window, and click the [OK] button.



3.

The “Content-SIM” window is displayed.

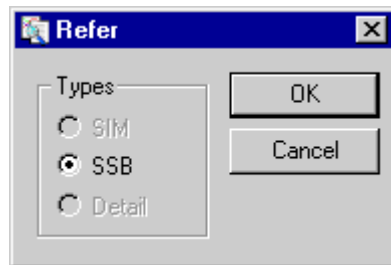
Click the [Refer...] button in the “Content-SIM” window, when the relative log is displayed.



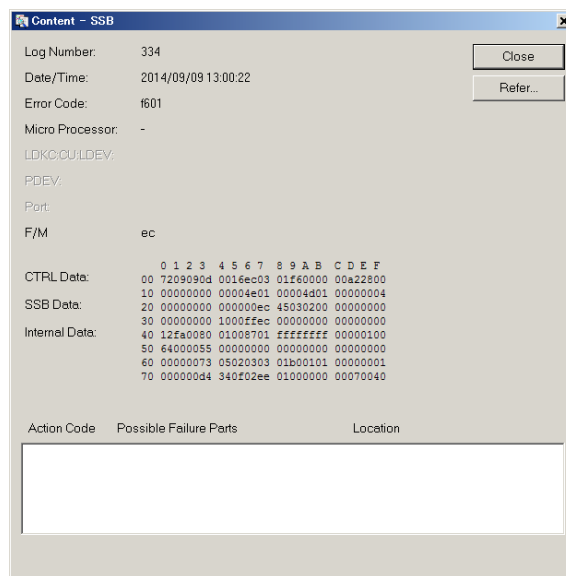
NOTE: In WCHK1 dump and ABEND dump received SIM (RC = 3080x0, 3081x0), the system error code is indicated in the format [yyyy] as in Reference Code 3080x0[yyyy].

NOTE: If Reference Code is 73xxxy or 1400x0, perform the recovery procedure for CTL processor failure/MPC Software failure.
(Refer to TROUBLESHOOTING SECTION [“3.10 Recovery Procedure for LAN Error”](#).)

4. Select the log to be displayed in the “Refer” window.
([SSB] is selected in this example.)



5. The selected log is displayed.
(“Content-SSB” is displayed in this example.)



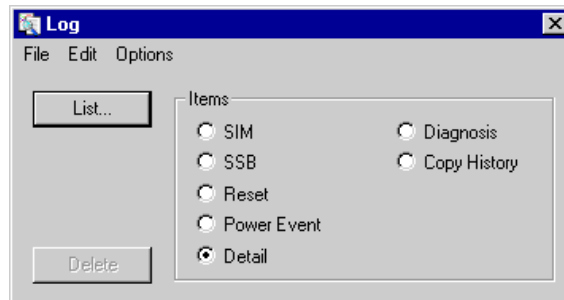
6. Close the relative log when it is referred to.
Click the [Close] button in the “Content-SSB” window.
Click the [Close] button in the “Content-SIM” window.
Click the [Close] button in the “List-SIM” window.
Close the “Log” window and close the “Information” window.

[3] Detail Log

1.

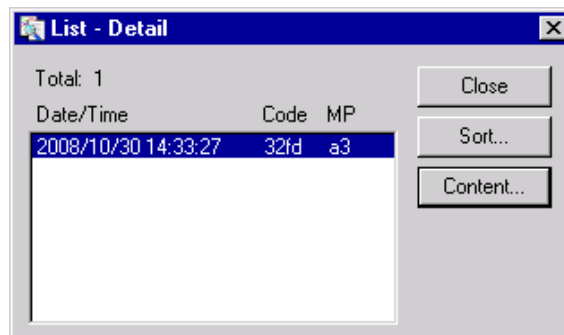
Click the [Detail] button in the “Log” window.

Click the [List...] button.



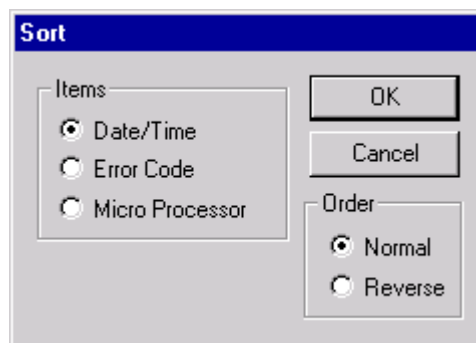
2.

Select the data to be indicated in the “List-Detail” window, and click the [Content...] button.

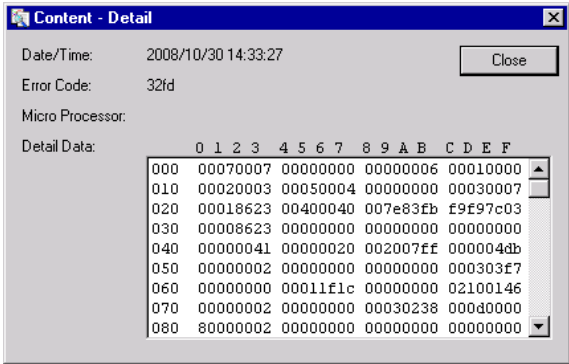


NOTE: To sort and list items, click the [Sort...] button first.

Then select the desired item in the [Items] and [Order] options in the “Sort” window, and click the [OK] button.



- 3. The “Content-Detail” window is displayed.



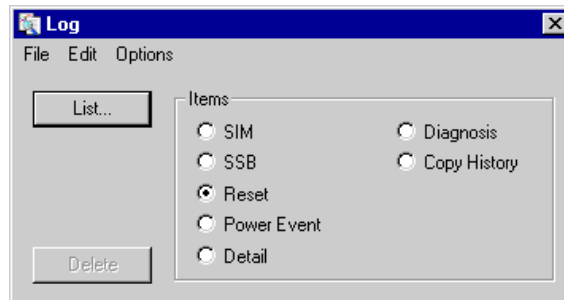
- 4. Click the [Close] button in the “Content-Detail” window.
Click the [Close] button in the “List-Detail” window.
Close the “Log” window and close the “Information” window.

[4] Reset Log

1.

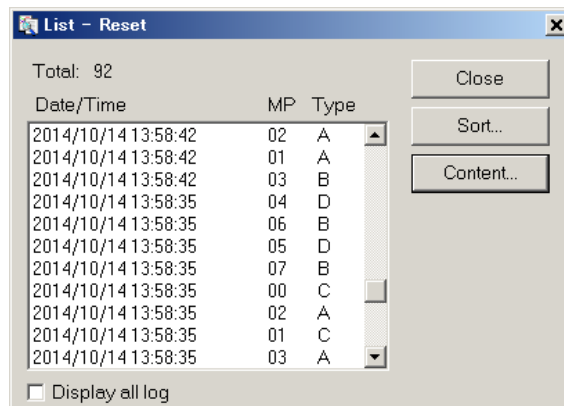
Click the [Reset] button in the “Log” window.

Click the [List...] button.

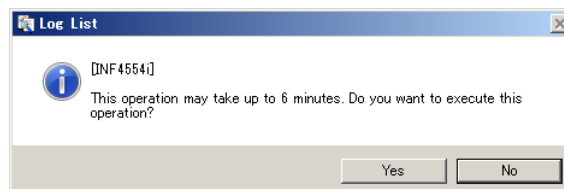


2.

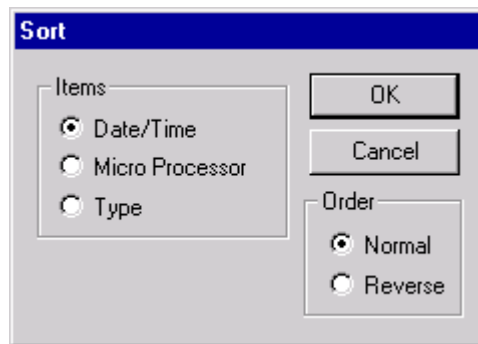
Select the data to be indicated in the “List-Reset” window and click the [Content...] button.



When displaying all the Reset Logs stored in the DKC, check the [Display all log] checkbox. After that, click the [Yes] button in the displayed message [4554].

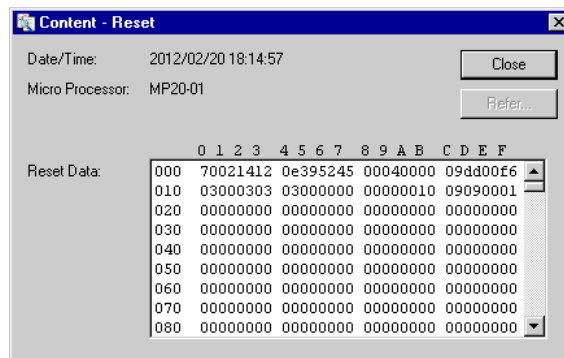


NOTE: To sort and list items, click the [Sort...] button first.
Then select the desired item in the [Items] and [Order] options in the “Reset Log Sort” window, and click the [OK] button.



3.

The “Content-Reset” window is displayed.



4.

Click the [Close] button in the “Content-Reset” window.

Click the [Close] button in the “List-Reset” window.

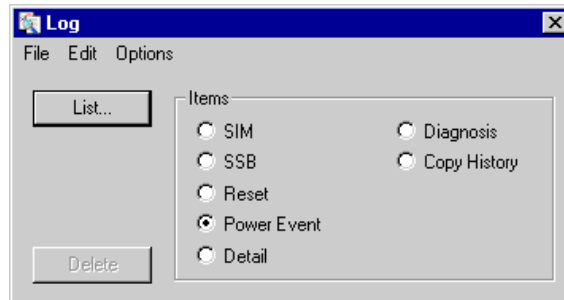
Close the “Log” window and close the “Information” window.

[5] Power Event Log

1.

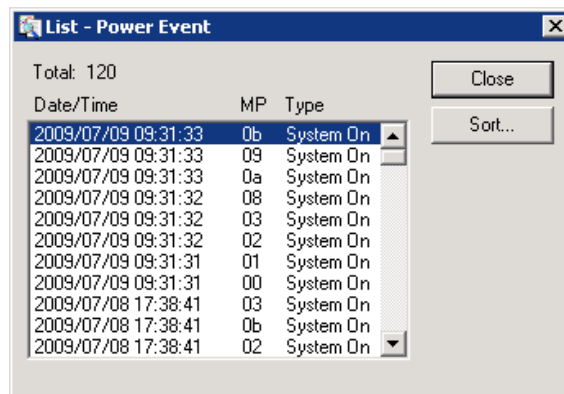
Click the [Power Event] button in the “Log” window.

Click the [List...] button.



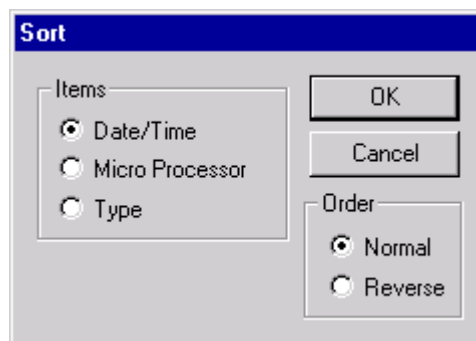
2.

The “List-Power Event” window is displayed.



NOTE: To sort and list items, click the [Sort...] button first.

Then select the desired item in the [Items] and [Order] options in the “Sort” window, and click the [OK] button.



3.

Click the [Close] button in the “List-Power Event” window.

Close the “Log” window and close the “Information” window.

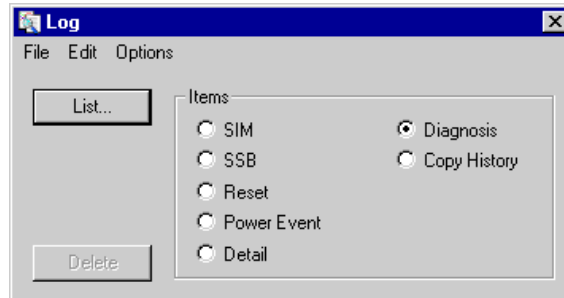
NOTE: In the “List-Power Event” window, only the MPs that are in the system on status are displayed. For checking the MPs that are in the system off status, click the [Search] button in the “List-SSB” window and refer to the log with Error Code = “3400” in accordance with [\[1\] SSB Log](#).

[6] Diagnosis Log

1.

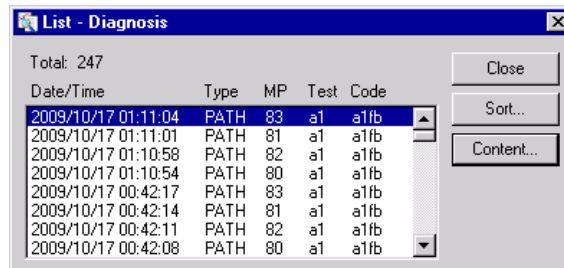
Click the [Diagnosis] button in the “Log” window.

Click the [List...] button.



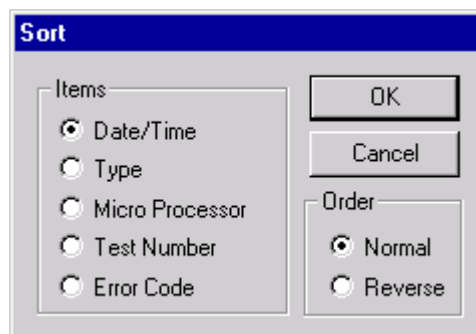
2.

Select the data to be indicated in the “List-Diagnosis” window and click the [Content...] button.

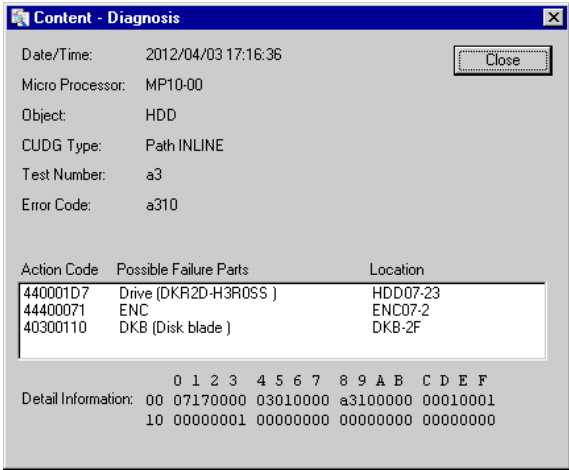


NOTE: To sort and list items, click the [Sort...] button first.

Then select the desired item in the [Items] and [Order] options in the “Sort” window, and click the [OK] button.



- 3.
- The “Content-Diagnosis” window is displayed.



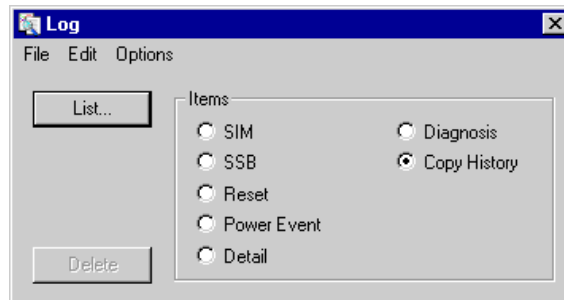
- 4.
- Click the [Close] button in the “Content-Diagnosis” window.
- Click the [Close] button in the “List-Diagnosis” window.
- Close the “Log” window and close the “Information” window.

[7] Copy History Log

1.

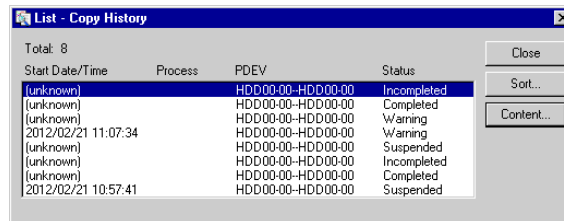
Click the [Copy History] button in the “Log” window.

Click the [List...] button.



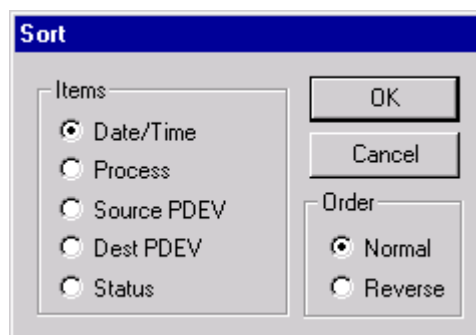
2.

Select the data to be indicated in the “List-Copy History” window and click the [Content...] button.



NOTE: To sort and list items, click the [Sort...] button first.

Then select the desired item in the [Items] and [Order] options in the “Sort” window, and click the [OK] button.



3.

The “Content-Copy History” window is displayed.



4.

Click the [Close] button in the “Content-Copy History” window.

Click the [Close] button in the “List-Copy History” window.

Close the “Log” window and close the “Information” window.

[8] MP# - Location correspondence table

Location			MP#				
			CBXS	CBSS1/CBSL1	CBSS2/CBSL2	CBLH1	CBLH2
CL1	MPU-10	MP10-00	0x00	0x00	0x00	0x00	0x00
		MP10-01	0x01	0x01	0x01	0x01	0x01
		MP10-02	—	0x02	0x02	0x02	0x02
		MP10-03	—	0x03	0x03	0x03	0x03
		MP10-04	—	0x04	0x04	0x04	0x04
		MP10-05	—	0x05	0x05	0x05	0x05
		MP10-06	—	—	0x06	0x06	0x06
		MP10-07	—	—	0x07	0x07	0x07
		MP10-08	—	—	0x08	0x08	0x08
		MP10-09	—	—	0x09	0x09	0x09
		MP10-0A	—	—	—	0x0A	0x0A
		MP10-0B	—	—	—	0x0B	0x0B
		MP10-0C	—	—	—	—	0x0C
		MP10-0D	—	—	—	—	0x0D
		MP10-0E	—	—	—	—	0x0E
		MP10-0F	—	—	—	—	0x0F
		MP10-10	—	—	—	—	0x10
		MP10-11	—	—	—	—	0x11
		MP10-12	—	—	—	—	0x12
		MP10-13	—	—	—	—	0x13
CL2	MPU-20	MP20-00	0x04	0x08	0x20	0x20	0x20
		MP20-01	0x05	0x09	0x21	0x21	0x21
		MP20-02	—	0x0A	0x22	0x22	0x22
		MP20-03	—	0x0B	0x23	0x23	0x23
		MP20-04	—	0x0C	0x24	0x24	0x24
		MP20-05	—	0x0D	0x25	0x25	0x25
		MP20-06	—	—	0x26	0x26	0x26
		MP20-07	—	—	0x27	0x27	0x27
		MP20-08	—	—	0x28	0x28	0x28
		MP20-09	—	—	0x29	0x29	0x29
		MP20-0A	—	—	—	0x2A	0x2A
		MP20-0B	—	—	—	0x2B	0x2B
		MP20-0C	—	—	—	—	0x2C
		MP20-0D	—	—	—	—	0x2D
		MP20-0E	—	—	—	—	0x2E
		MP20-0F	—	—	—	—	0x2F
		MP20-10	—	—	—	—	0x30
		MP20-11	—	—	—	—	0x31
		MP20-12	—	—	—	—	0x32
		MP20-13	—	—	—	—	0x33

[9] Port - Location correspondence table

• VSP G350, G370, G700, G900

Location			Port	Location			Port
Cluster1	CHB-1A	1A	00	Cluster2	CHB-2A	2A	08
		3A	01			4A	09
		5A	02			6A	0A
		7A	03			8A	0B
	CHB-1B	1B	04		CHB-2B	2B	0C
		3B	05			4B	0D
		5B	06			6B	0E
		7B	07			8B	0F
	CHB-1C	1C	10		CHB-2C	2C	18
		3C	11			4C	19
		5C	12			6C	1A
		7C	13			8C	1B
	CHB-1D	1D	14		CHB-2D	2D	1C
		3D	15			4D	1D
		5D	16			6D	1E
		7D	17			8D	1F
	CHB-1E/DKB-1E	1E/1E-0	20		CHB-2E/DKB-2E	2E/2E-0	28
		3E/1E-1	21			4E/2E-1	29
		5E	22			6E	2A
		7E	23			8E	2B
	CHB-1F/DKB-1F	1F/1F-0	24		CHB-2F/DKB-2F	2F/2F-0	2C
		3F/1F-1	25			4F/2F-1	2D
		5F	26			6F	2E
		7F	27			8F	2F
	CHB-1G/DKB-1G	1G/1G-0	30		CHB-2G/DKB-2G	2G/2G-0	38
		3G/1G-1	31			4G/2G-1	39
		5G	32			6G	3A
		7G	33			8G	3B
	CHB-1H/DKB-1H	1H/1H-0	34		CHB-2H/DKB-2H	2H/2H-0	3C
		3H/1H-1	35			4H/2H-1	3D
		5H	36			6H	3E
		7H	37			8H	3F
	CHB-1J	1J	40		CHB-2J	2J	48
		3J	41			4J	49
		5J	42			6J	4A
		7J	43			8J	4B
	CHB-1K	1K	44		CHB-2K	2K	4C
		3K	45			4K	4D
		5K	46			6K	4E
		7K	47			8K	4F
	CHB-1L	1L	50		CHB-2L	2L	58
		3L	51			4L	59
		5L	52			6L	5A
		7L	53			8L	5B
	CHB-1M	1M	54		CHB-2M	2M	5C
		3M	55			4M	5D
		5M	56			6M	5E
		7M	57			8M	5F

• VSP G130

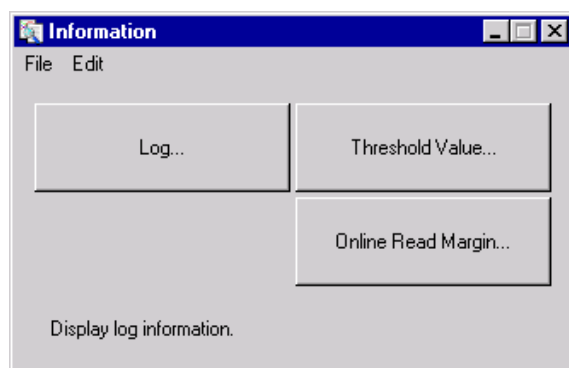
Location			Port	Location			Port
Cluster1	CHB-1A	1A	00	Cluster2	CHB-2A	2A	04
		3A	01			4A	05
		5A	02			6A	06
		7A	03			8A	07

5.3.2 Log Delete

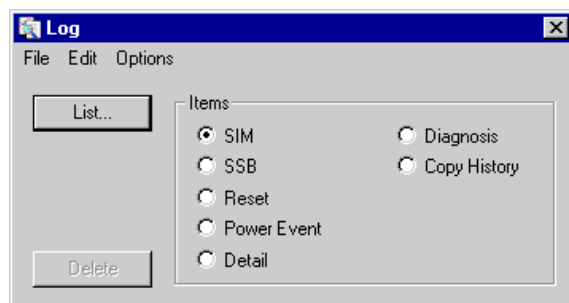
- [1] SSB Log
- [2] SIM Log
- [3] Detail Log
- [4] Reset Log
- [5] Power Event Log
- [6] Diagnosis Log
- [7] Copy History Log

1.
Change the mode from [View Mode] to [Modify Mode].
Click the [Information] button in “MPC” window.

2.
Click the [Log...] button.

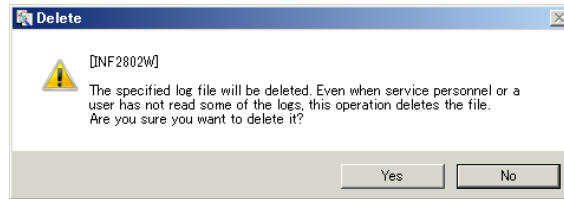


3.
In the “Log” window, select a log to be deleted and click the [Delete] button.
(For example, select [SIM].)



4.

Click the [Yes] button in the “Delete”[2802] window.



5.

Close the “Log” window and close the “Information” window.
Change the mode from [Modify Mode] to [View Mode].

5.4 Online Read Margin (ORM)

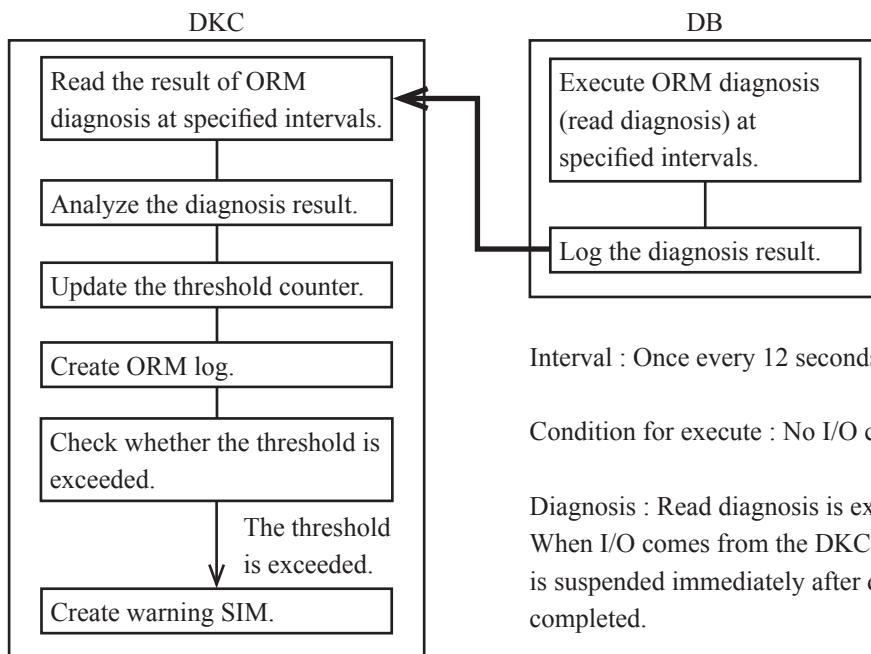
[Overview]

The online read margin (ORM) function is a read diagnosis function provided for preventive maintenance of disk drives. The read diagnosis is automatically executed in each drive. The DKC reads the diagnosis result at specified intervals and classifies and manages it by DB unit.

Furthermore, The ORM creates an SIM when exceeding the threshold value set in advance.

The SIM created by ORM is not reported to the host.

When an alert SIM is reported, replace the drive preferentially.



The following table shows SIM reported by DKC.

Case of the error of SAS Drive : See [Table 5-7](#)

Case of the error of Flash Drive : See [Table 5-8](#)

Case of the error of Flash Module Drive : See [Table 5-9](#)

They are Unrecovered Read Error, Recovered Read Error, Unrecovered Seek error, Recovered Seek Error, Not Ready and Other Errors. Each has three types of counters indicated as Today, 7 days and Total. Refer to [1] [Step 4](#) for the Over Rate Counter Display. In the Over Rate Counter Display, the error ratio which has the largest number among those classified types is displayed for each drive to represent each error.

The warning SIMs to be reported in the ORM are shown below.

Table 5-7 ORM SIM and Reference Code (SAS Drive)

No.	Error Type	Reference Code	Meaning
1	Unrecovered Read Error	501x (x = 0 ~ f)	Drive Media Error
2	Recovered Read Error		
3	Unrecovered Seek Error	502x (x = 0 ~ f)	Drive Unit Error
4	Recovered Seek Error		
5	Not Ready		
6	Other Errors		

Table 5-8 ORM SIM and Reference Code (Flash Drive)

No.	Error Type	Reference Code	Meaning
1	Total Defect Count	501x (x = 0 ~ f)	Drive Unit Error
2	Total Uncorrected Errors	—	Informed Only
3	Errors Corrected With Possible Delays		
4	Highest Erase Count For All Channels		
5	Lowest Erase Count For All Channels		
6	Used Endurance Indicator	50bx (x = 0 ~ f)	Flash Drive End of life

Table 5-9 ORM SIM and Reference Code (Flash Module Drive)

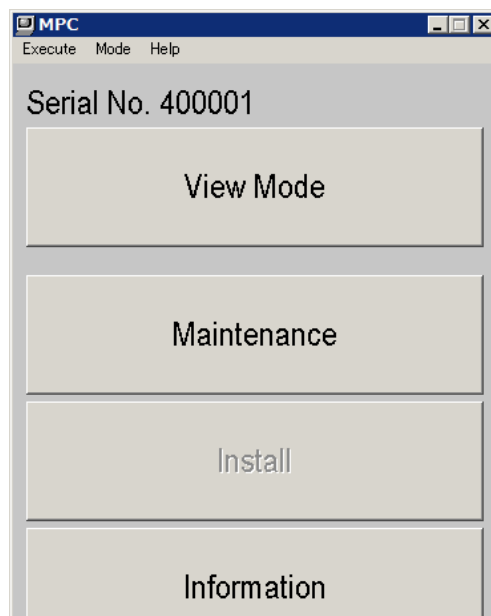
No.	Error Type	Reference Code	Meaning
1	Total Defect Count	501x (x = 0 ~ f)	Drive Unit Error
2	Reboot Error		
3	DMA Error		
4	Memory Error		
5	Uncorrected Error	502x (x = 0 ~ f)	Drive Media Error
6	Used Endurance Indicator	50cx (x = 0 ~ f)	Flash Module Drive End of life
7	Capacitor Error	501x (x = 0 ~ f)	Drive Unit Error

[1] Displaying an error count, thresholds, and log -----	MPC05-510
[2] Resetting an error count -----	MPC05-560
[3] Displaying thresholds -----	MPC05-580
[4] Altering a threshold -----	MPC05-610
[5] Displaying the ORM running status -----	MPC05-640
[6] Resetting thresholds -----	MPC05-660
[7] Set of the threshold of all Flash Drive -----	MPC05-680

Prerequisite Operation

1. Check MPC Mode

When making the following changes, click [View Mode] in the “MPC” window to change to [Modify Mode].



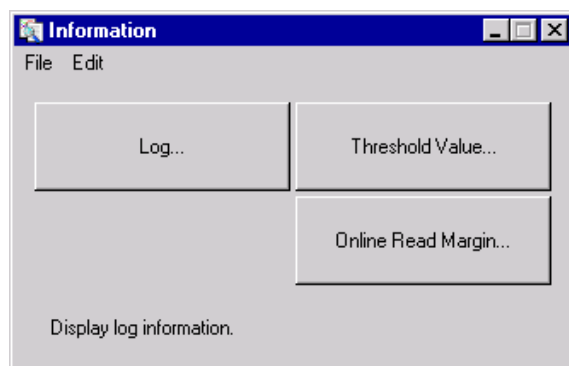
- [2] Resetting an error count
 - [4] Altering a threshold
 - [6] Resetting thresholds
 - [7] Set of the threshold of all Flash Drive
- In the case other than the above, go to [Step 2](#).

2.

Click the [Information] button in the “MPC” window.

3.

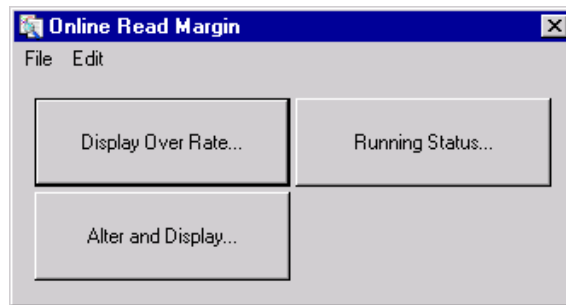
Click the [Online Read Margin...] button in the “Information” window.



[1] Displaying an error count, thresholds, and log

1.

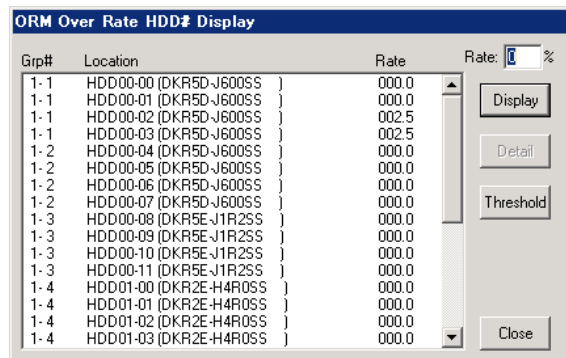
Click the [Display Over Rate...] button in the “Online Read margin” window.



2.

Enter a number from 0 to 100 at “Rate” in the “ORM Over Rate HDD# Display” window. Click the [Display] button.

Then only the HDDs which have the rate of equal to or greater than the input number at “Rate” will appear in the display.



Rate : ratio of the number of errors for the threshold value.

Grp# : the parity group.

SPARE : spare HDD

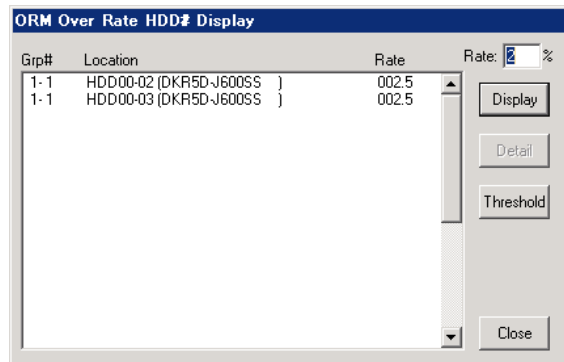
RSRVD : reserved HDD with sparing

* : spare HDD in use.

3.

When more detailed information is needed for the particular drive, select the HDD from the HDD Location list box.

Click the [Detail] button.



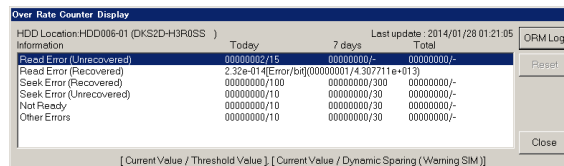
4.

In the “Over Rate Counter Display” window, select the error for which detailed log is to be displayed. Click the [ORM Log] button.

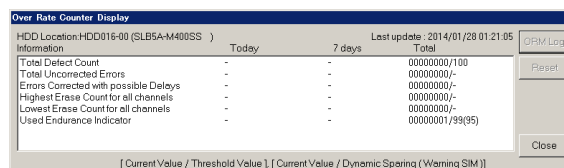
NOTE: In the case of Flash Drive or Flash Module Drive, you cannot choose the [ORM Log] button.

Click the [Close] button to finish.

(SAS Drive Selected)



(Flash Drive Selected)



(Flash Module Drive Selected : Drive model NFHxx-Qxxxxx)

Information	Today	7 days	Total
Total Defect Count	-	-	00000000/100
Reboot Error	00000000/2	-	-
DMA Error	00000000/10	-	-
Memory Error	00000000/500	-	-
Uncorrected Error	00000000/5000	-	-
Used Endurance Indicator	-	-	00000000/99(97)
Capacitor Error	00000000/1	-	-

- In case of SAS Drive

Item	Description	
ID (Information) (*1)	Read Error (Unrecovered)	A disk media error was detected. After ten times retries, the error was judged that it might become a serious media error which could not be recovered with ECC or retries.
	Read Error (Recovered)	A disk media error was detected. After ten times retries, the error was judged that it was an intermittent read error and recoverable, and included in the error rate management for the preventive maintenance.
	Seek Error (Recovered)	A seek error was detected. After ten times retries, the error was judged to be recoverable.
	Seek Error (Unrecovered)	A seek error was detected. After ten times retries, the error was judged to be unrecoverable.
	Not Ready	Not Ready status of the drive was detected.
	Other Errors	Any error which does not belong to the above classification was detected.
Today	One day count and cleared at AM 0:00 every day.	
7 days	For the cumulative value in the latest 7 days.	
Total	Shows the total cumulative count.	

*1:

Except for "Read Error (Recovered)":

Each error category indicates the Error Count and the Threshold value.

The "-" for the Threshold value means no threshold is set.

For "Read Error (Recovered)":

Only the Read Error (Recovered) has an error rate expression. It is not managed with error count per day, per 7 days or Total.

The error rate of the Read Error [Recovered] is calculated in the following formula:

$$\text{Error rate} = \text{Number of error sectors} / \text{Number of ORM scan bits}$$

NOTE: Only the result from approximately the latest one volume scan in ORM is used for the calculation.

- In case of Flash Drive

Item	Description	
Information	Total Defect Count	Defect Count
	Total Uncorrected Errors	The total of the uncorrectable error (*1)
	Errors Corrected With Possible Delays	The total of the delay error (*1)
	Highest Erase Count For All Channels	Highest Erase Count For All Channels (*1)
	Lowest Erase Count For All Channels	Lowest Erase Count For All Channels (*1)
	Used Endurance Indicator	Flash Drive End of lifetime (%) (*2)
Today	One day count and cleared at AM 0:00 every day.	
7 days	For the cumulative value in the latest 7 days.	
Total	Shows the total cumulative count.	

*1: When the drive model is SLRxx-MxxxSS, the value of each item is displayed by 0 fixation.

*2: Used Endurance Indicator is displayed in the order of “Current Value / Dynamic Sparing (Warning SIM)”.

- In case of Flash Module Drive

Item	Description	
Information	Total Defect Count	Defect Count
	Reboot Error	Reboot Error Count
	DMA Error	DMA Error Count
	Memory Error	Memory Error Count
	Uncorrected Error	Uncorrected Error Count
	Used Endurance Indicator	Flash Module Drive End of lifetime (%) (*1)
	Capacitor Error	Capacitor Error Count
Today	One day count and cleared at AM 0:00 every day.	
7 days	For the cumulative value in the latest 7 days.	
Total	Shows the total cumulative count.	

*1: Used Endurance Indicator is displayed in the order of “Current Value / Dynamic Sparing (Warning SIM)”.

Because these information is multiplication values since HDD operation time, Maintenance PC display only total indication in case of Flash Drive. Maintenance PC displays total indication of “Total Defect Count” and “Used Endurance Indicator”, and today indication of the others for Flash Module Drive.

The “-” for the Threshold value means no threshold is set.

5.

The nature of the error selected in [Step 4](#) is displayed.

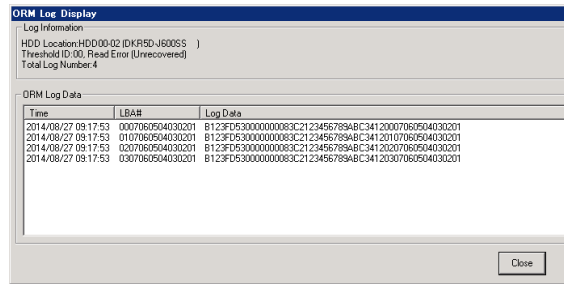


Table 5-10 Descriptions of the ORM Log Data

Byte	Bit	Name	Explanation
0-7		UCT	Time when the diagnostic result was reported from the DKC to the Log data.
8	0	Log Valid	When this bit is 1, it indicates that this log is valid.
	1	Address Valid	When this bit is 1, it indicates that the address information in bytes C to 19 is valid.
	2-3	(Reserved)	Reserved
	4-7	Sense Key	Error sense key in the SCSI drive report. (*1)
9		Additional Sense Code	Additional sense code in the SCSI drive report. (*1)
10		Sense Code Qualifier	Additional sense code qualifier in the SCSI drive report. (*1)
11		Seek Error Count	Number of seek errors within 10 seek error retries.
C-E		CC	Address of the cylinder where the error occurred.
F		H	Address of the head where the error occurred.
10-11		S	Address of the sector where the error occurred.
12-19		LBA	LBA where the error occurred.

*1: Definition and contents of the error codes are same as those of the SSB for ordinary DB errors.

6.

Click the [Close] button in the “ORM Log Display” window.

Click the [Close] button in the “Over Rate Counter Display” window.

Close the “Online Read Margin” window.

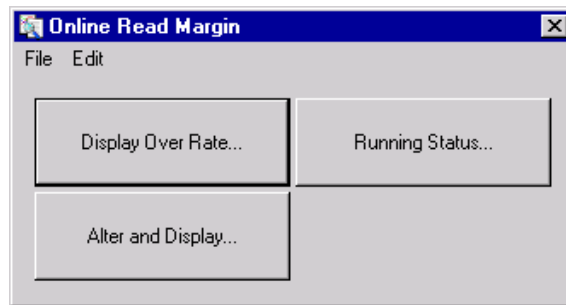
Click the [Close] button in the “ORM Over Rate HDD# Display” window.

Close the “Information” window.

[2] Resetting an error count

1.

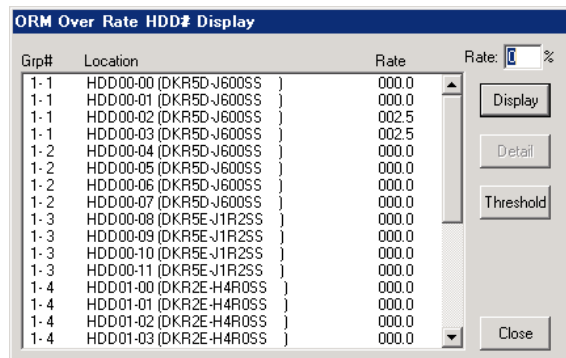
Click the [Display Over Rate...] button in the “Online Read Margin” window.



2.

Enter a number from 0 to 100 at “Rate” in the “ORM Over Rate HDD# Display” window. Click the [Display] button.

Then only the HDDs which have the rate of equal to or greater than the input number at “Rate” will appear in the display.



Rate : ratio of the number of errors for the threshold value.

Grp# : the parity group.

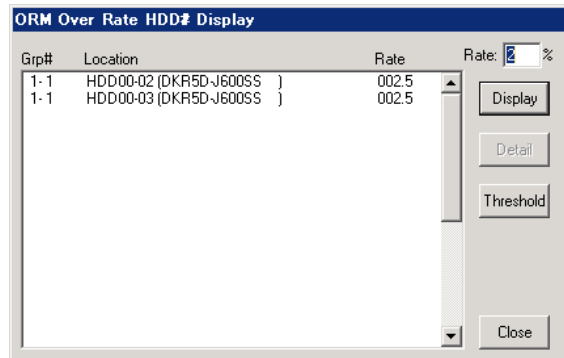
SPARE : spare HDD

RSRVD : reserved HDD with sparing

* : spare HDD in use.

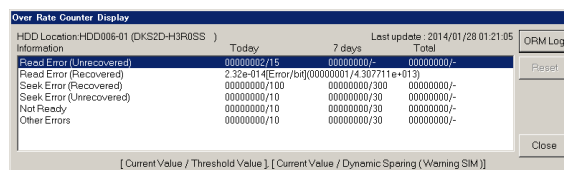
3.

In the “ORM Over Rate HDD# Display” window, select the HDD for which an error count and thresholds are to be reset from the HDD Location list box. Click the [Detail] button.



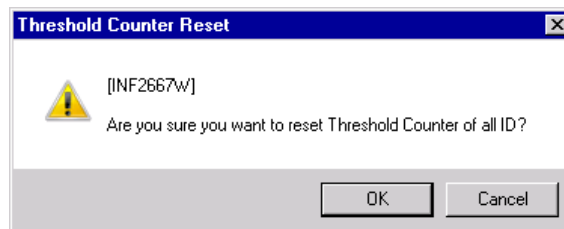
4.

In the “Over Rate Counter Display” window, click the [Reset] button.



5.

Click the [OK] button in the “Threshold Counter Reset” [2667] dialog box.



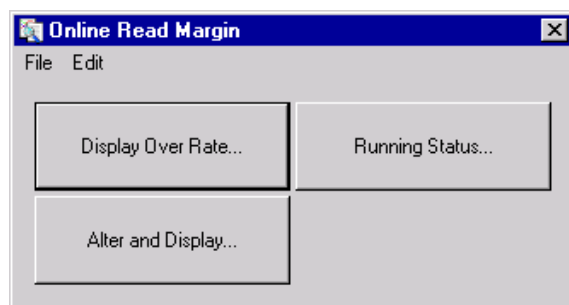
6.

Click the [Close] button in the “Over Rate Counter Display” window.
 Click the [Close] button in the “ORM Over Rate HDD# Display” window.
 Close the “Online Read Margin” window.
 Close the “Information” window.
 Change the mode from [Modify Mode] to [View Mode].

[3] Displaying thresholds

1.

Click the [Alter and Display...] button in the “Online Read Margin” window.



2.

In the “ORM Threshold Alter/Display” window, select an HDD from the “HDD#” list box and click the [Display] button. In order to display threshold of another interval, select the interval from the “Type” radio button.

NOTE: Multiple HDDs can be selected from the “HDD#” list box while the control key is being held down.

When “Flash Drive” is selected in the “HDD#” list box, HDD other than “Flash Drive” cannot be selected at the same time.

In this case, each “Threshold” field in the “Threshold Value” list box shows the threshold for the HDD that is highlighted in the “HDD#” list box.

(SAS Drive Selected)

The screenshot shows the 'ORM Threshold Alter/Display' window. The 'HDD#' list box contains several entries, with 'HDD00-11 (DKSZE-H4R0SS)' selected. The 'Type' radio buttons are set to 'Today'. The 'Threshold Value' section on the right shows the following thresholds for the selected HDD:

Information	Threshold
Read En (Unrecovered) (0 - 9999)	45
Read En (Recovered) (0 - 3.4E+03)	1.00e+008
Seek En (Recovered) (0 - 9999)	100
Seek En (Unrecovered) (0 - 9999)	10
Not Ready (0 - 9999)	10
Other Errors (0 - 9999)	10

Grp# : the parity group.

SPARE : spare HDD

RSRVD : reserved HDD with sparing

* : spare HDD in use.

NOTE: When selected HDD from the “HDD#” list box is “Flash Drive”, “Information” field in the “Threshold Value” shows the item of “Flash Drive”. In order to display threshold of “Total Defect Count”, select “Total” from the “Type” radio button.

(Flash Drive Selected)

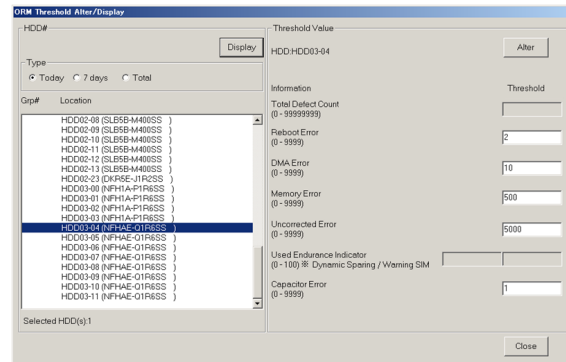
The screenshot shows the 'ORM Threshold Alter/Display' window. The 'HDD#' list box contains several entries, with 'HDD00-11 (SLB5B-M40SS)' selected. The 'Type' radio buttons are set to 'Total'. The 'Threshold Value' section on the right shows the following thresholds for the selected HDD:

Information	Threshold
Total Defect Count (0 - 99999999)	100
Total Uncorrected Errors	
Errors Corrected with possible Delays	
Highest Erase Count for all channels	
Lowest Erase Count for all channels	
Used Endurance Indicator (0 - 100) @ Dynamic Sparing / Warning SM	99 95

NOTE: When selected HDD from the “HDD#” list box is “Flash Module Drive”, “Information” field in the “Threshold Value” shows the item of “Flash Module Drive”.

In order to display threshold of “Total Defect Count” and “Used Endurance Indicator”, select “Total” from the “Type” radio button. In order to display threshold of the other, select “Today” from the “Type” radio button.

(Flash Module Drive Selected : Drive model NFHxx-Qxxxxxx)



3.

Click the [Close] button in the “ORM Threshold Alter/Display” window.

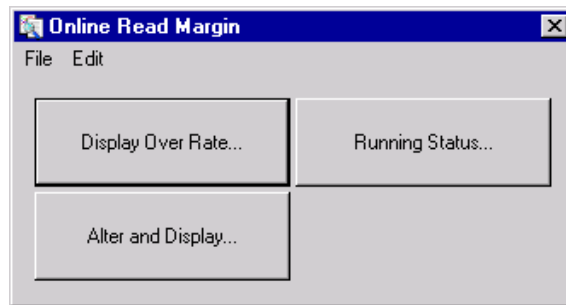
Close the “Online Read Margin” window.

Close the “Information” window.

[4] Altering a threshold

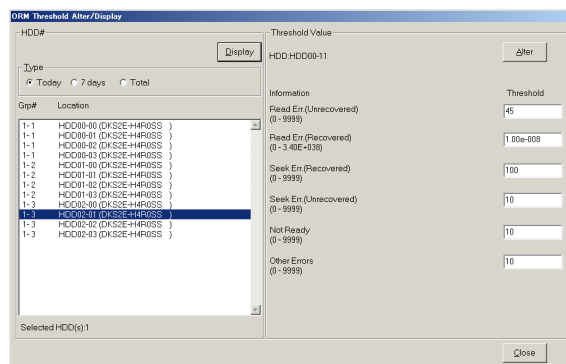
1.

Click the [Alter and Display...] button in the “Online Read Margin” window.



2.

In the “ORM Threshold Alter/Display” window, select an HDD from the “HDD#” list box and click the [Display] button. In order to display threshold of another interval, select the interval from the “Type” radio button.



Grp# : the parity group.

SPARE : spare HDD

RSRVD : reserved HDD with sparing

* : spare HDD in use.

3.

In the “ORM Threshold Alter/Display” window, alter the threshold in the “Threshold” field in the “Threshold Value” list box. Then click the [Alter] button.

NOTE: When multiple HDDs are selected in the “HDD#” list box, the thresholds of all HDDs are altered to the same value.

Different drive types of the threshold management cannot be selected at the same time.

(SAS Drive Selected)

ORM Threshold Alter/Display

HDD#

Type: ☒ Today ☐ 7 days ☐ Total

Gp#	Location
1-1	H000-00 (DKS2E-HAR6SS)
1-1	H000-01 (DKS2E-HAR6SS)
1-1	H000-02 (DKS2E-HAR6SS)
1-1	H000-03 (DKS2E-HAR6SS)
1-2	H001-00 (DKS2E-HAR6SS)
1-2	H001-01 (DKS2E-HAR6SS)
1-2	H001-02 (DKS2E-HAR6SS)
1-2	H001-03 (DKS2E-HAR6SS)
1-2	H001-04 (DKS2E-HAR6SS)
1-2	H001-05 (DKS2E-HAR6SS)
1-3	H002-00 (DKS2E-HAR6SS)
1-3	H002-01 (DKS2E-HAR6SS)
1-3	H002-02 (DKS2E-HAR6SS)
1-3	H002-03 (DKS2E-HAR6SS)

Selected HDD(s): 2

Threshold Value

HDD: H000-11

Information

Information	Threshold
Read Err (Unrecovered) (0 - 9999)	45
Read Err (Recovered) (0 - 3.40E+038)	1.00e+009
Seek Err (Recovered) (0 - 9999)	100
Seek Err (Unrecovered) (0 - 9999)	10
Not Ready (0 - 9999)	10
Other Errors (0 - 9999)	10

Close

(Flash Drive Selected)

ORM Threshold Alter/Display

HDD#

Type: ☐ Today ☐ 7 days ☒ Total

Gp#	Location
1-1	H000-00 (SLB5B-M40SS)
1-1	H000-01 (SLB5B-M40SS)
1-1	H000-02 (SLB5B-M40SS)
1-1	H000-03 (SLB5B-M40SS)
1-2	H001-00 (NPH1A-P16SS)
1-2	H001-01 (NPH1A-P16SS)
1-2	H001-02 (NPH1A-P16SS)
1-2	H001-03 (NPH1A-P16SS)

Selected HDD(s): 1

Threshold Value

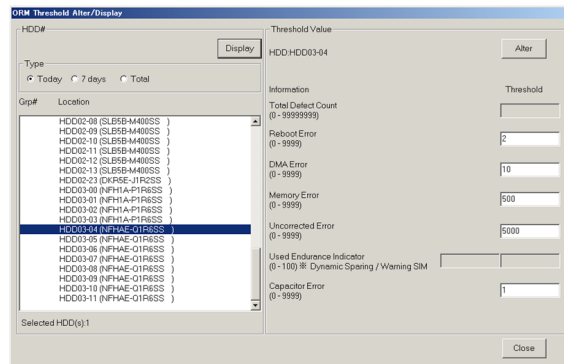
HDD: H000-11

Information

Information	Threshold
Total Defect Count (0 - 99999999)	100
Total Uncorrected Errors	
Errors Corrected with possible Delays	
Highest Erase Count for all channels	
Lowest Erase Count for all channels	
Used Endurance Indicator (0 - 100) @ Dynamic Spinning / Warning SM	39

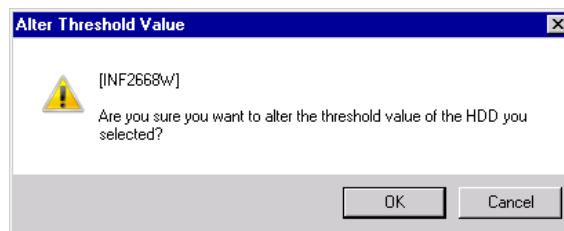
Close

(Flash Module Drive Selected : Drive model NFHxx-Qxxxxx)



4.

Click the [OK] button in the “Alter Threshold Value” [2668] dialog box.



5.

Click the [Close] button in the “ORM Threshold Alter/Display” window.

Close the “Online Read Margin” window.

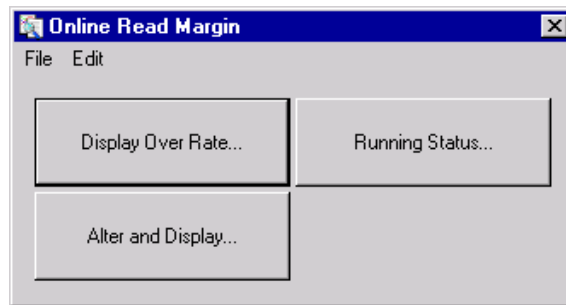
Close the “Information” window.

Change the mode from [Modify Mode] to [View Mode].

[5] Displaying the ORM running status

1.

Click the [Running Status...] button.



2.

In the “ORM Running Status Display” window, the ORM running status is displayed as the number of sectors.

NOTE: The “HDD#” list box shows the location numbers of HDDs. “Scan” shows the number of scanned sectors.

“Total” shows the total number of sectors in the drive. “Times” shows the number of times the entire drive was scanned. Result of calculating “Scan” / “Total”.

(SAS Drive Selected)

Grp#	Location	Scan	Total	Times
1-1	HDD00-00 [DKR5C-J300S]	0.000000e+000	5.860724e+008	(0.0)
1-1	HDD00-01 [DKR5C-J300S]	0.000000e+000	5.860724e+008	(0.0)
1-1	HDD01-00 [DKR5C-J300S]	0.000000e+000	5.860724e+008	(0.0)
1-1	HDD01-01 [DKR5C-J300S]	0.000000e+000	5.860724e+008	(0.0)
1-2	HDD02-00 [DKR5C-J300S]	0.000000e+000	5.860724e+008	(0.0)
1-2	HDD02-01 [DKR5C-J300S]	0.000000e+000	5.860724e+008	(0.0)
1-2	HDD03-00 [DKR5C-J300S]	0.000000e+000	5.860724e+008	(0.0)
1-2	HDD03-01 [DKR5C-J300S]	0.000000e+000	5.860724e+008	(0.0)

Grp# : the parity group.

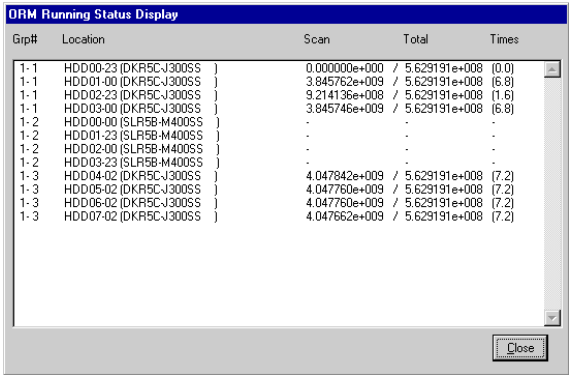
SPARE : spare HDD

RSRVD : reserved HDD with sparing

* : spare HDD in use.

NOTE: When “Flash Drive” or “Flash Module Drive” is displayed, “Scan”, “Total”, “Times” is “-”.

(Flash Drive or Flash Module Drive Selected)



The screenshot shows a window titled "ORM Running Status Display" with a table containing drive information. The table has five columns: Grp#, Location, Scan, Total, and Times. The data is as follows:

Grp#	Location	Scan	Total	Times
1-1	HDD00-23 (DKR5C-J300SS)	0.000000e+000 /	5.629191e+008	(0.0)
1-1	HDD01-00 (DKR5C-J300SS)	3.845762e+009 /	5.629191e+008	(6.8)
1-1	HDD02-23 (DKR5C-J300SS)	9.214136e+008 /	5.629191e+008	(1.6)
1-1	HDD03-00 (DKR5C-J300SS)	3.845746e+009 /	5.629191e+008	(6.8)
1-2	HDD00-00 (SLR5B-M400SS)	-	-	-
1-2	HDD01-23 (SLR5B-M400SS)	-	-	-
1-2	HDD02-00 (SLR5B-M400SS)	-	-	-
1-2	HDD03-23 (SLR5B-M400SS)	-	-	-
1-3	HDD04-02 (DKR5C-J300SS)	4.047842e+009 /	5.629191e+008	(7.2)
1-3	HDD05-02 (DKR5C-J300SS)	4.047760e+009 /	5.629191e+008	(7.2)
1-3	HDD06-02 (DKR5C-J300SS)	4.047760e+009 /	5.629191e+008	(7.2)
1-3	HDD07-02 (DKR5C-J300SS)	4.047662e+009 /	5.629191e+008	(7.2)

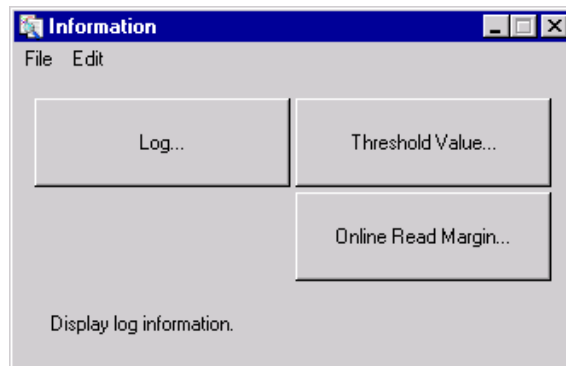
A "Close" button is located at the bottom right of the window.

- 3.
- Click the [Close] button in the “ORM Running Status Display” window.
 - Close the “Online Read Margin” window.
 - Close the “Information” window.

[6] Resetting thresholds

1.

Select [File]-[Exit] in the “Information” window.

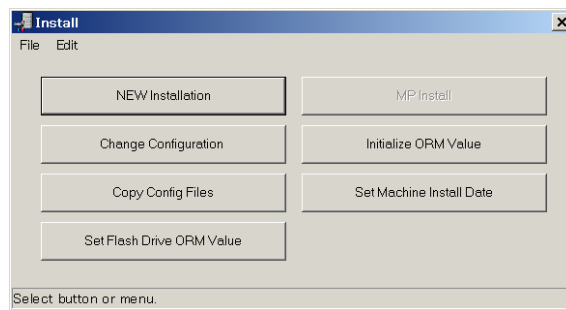


2.

Click the [Install] button in the “MPC” window.

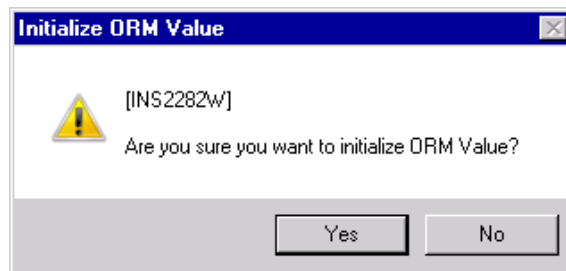
3.

Click the [Initialize ORM Value] button in the “Install” window.



4.

Click the [Yes] button in the “Initialize ORM Value” [2282] dialog box.



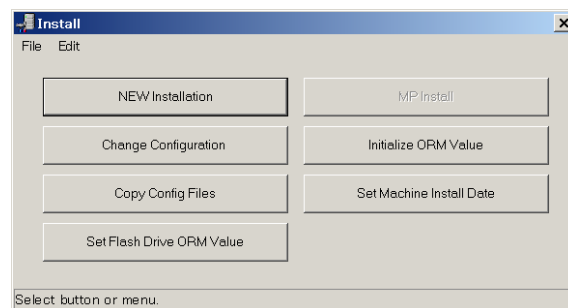
5.

Click the [OK] button in the “Initialize ORM Value” [2281] dialog box.



6.

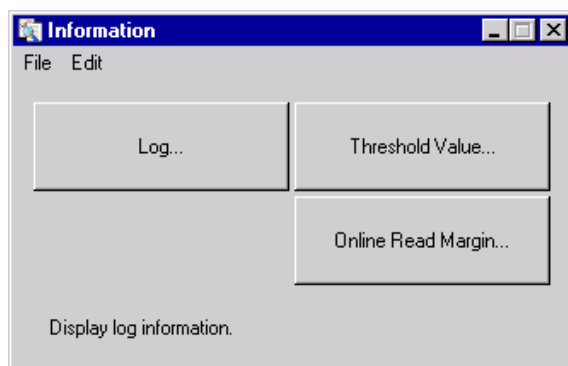
After the procedure is completed, return to “Install”.
Select [File]-[Exit].



[7] Set of the threshold of all Flash Drive

1.

Select [File]-[Exit] in the “Information” window.

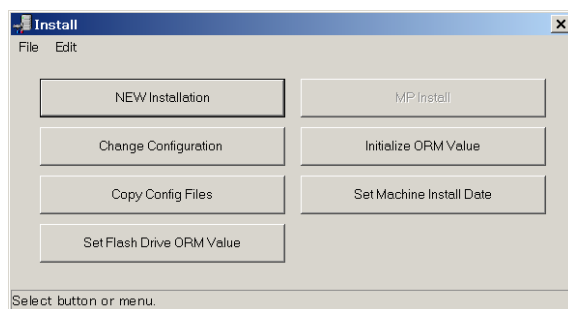


2.

Click the [Install] button in the “MPC” window.

3.

Click the [Set Flash Drive ORM Value] button in the “Install” window.

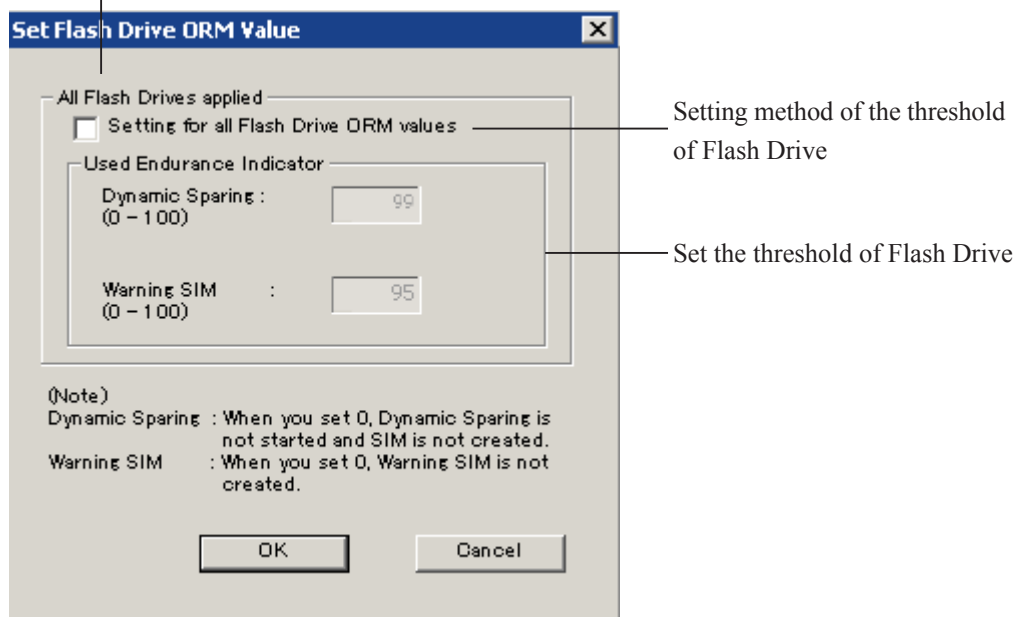


4.

Set a setting method of the threshold and the threshold, and then click the [OK] button.

To stop the operation, click the [Cancel] button and return to [Step 3](#).

Setting of Flash Drive



<<Setting of Flash Drive>>

[All Flash Drives applied]

<Setting method of the threshold of Flash Drive>

Setting for all Flash Drive ORM values

When setting thresholds of Used Endurance Indicator of all mounted Flash Drives collectively, check the checkbox.

When it is checked, the Flash Drive installed after this operation becomes the same threshold automatically. When you want to cancel this setting, check off. When you want to return the threshold to initial value (Dynamic Sparing threshold: 99/Warning SIM threshold: 95), do reset operation of the threshold. ([MPC05-660](#))

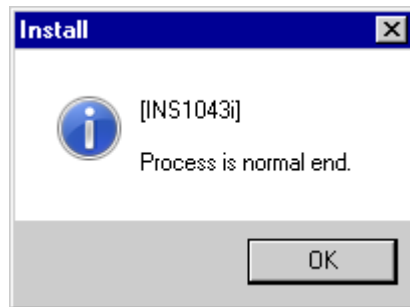
<Set the threshold of Flash Drive>

[Used Endurance Indicator]

- Dynamic Sparing : When there is a spare drive, this is the threshold to start Dynamic Sparing.
When reach the threshold that you set, start Dynamic Sparing and create SIM. Valid number is 0 - 100. When you set 0, does not start Dynamic Sparing and does not create SIM.
- Warning SIM : This is the threshold to create Warning SIM. When reach the threshold that you set create Warning SIM. Valid number is 0 - 100.
When you set 0, does not create Warning SIM.

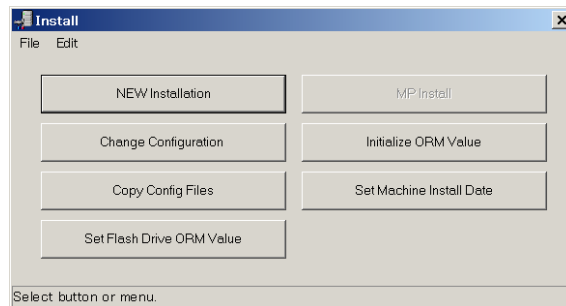
5.

Click the [OK] button in the “[1043] Process is normal end.”.



6.

After the procedure is completed, return to “Install”. Select [File]-[Exit].



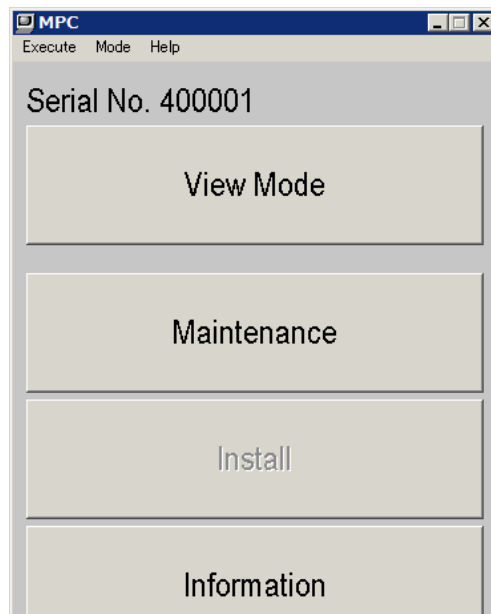
5.5 Management of Drive Threshold Values

- [1] Displaying threshold values ----- [MPC05-740](#)
- [2] Altering threshold value ----- [MPC05-760](#)
- [3] Displaying an error count ----- [MPC05-780](#)
- [4] Resetting an error count ----- [MPC05-790](#)

1. Prerequisite Operation

(1) Check MPC Mode.

When making the following changes, click [View Mode] in the “MPC” window to change to [Modify Mode].



[2] Altering threshold value

[4] Resetting an error count

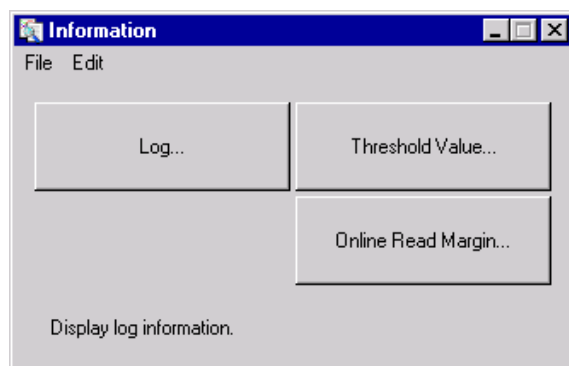
In the case other than the above, go to [Step \(2\)](#).

(2)

Click the [Information] button in the “MPC” window.

(3)

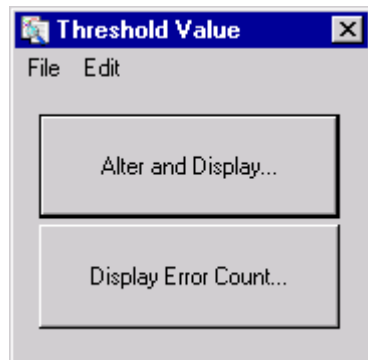
Click the [Threshold Value...] button in the “Information” window.



[1] Displaying threshold values

1.

Click the [Alter and Display...] button in the “Threshold Value” window.



2.

Select an HDD location from the “HDD#” list box in the “Threshold Alter/Display” window and click the [Display] button.

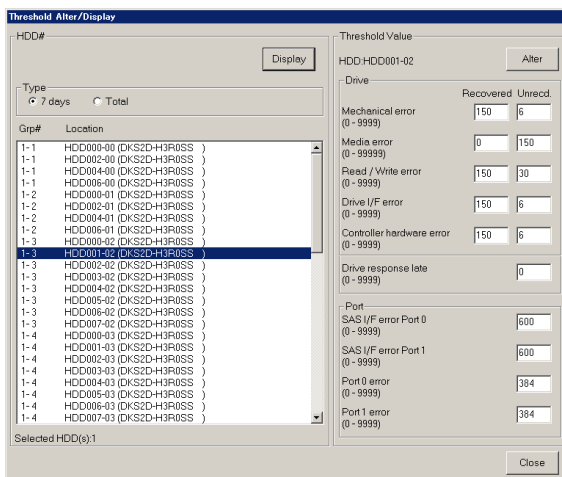
In order to display threshold of another interval, select the interval from the “Type” list box.

NOTE: Multiple HDD locations can be selected from the “HDD#” list box while the control key being held down. The threshold value in the “Threshold Value” list box shows the threshold value for the HDD location that is highlighted in the “HDD#” list box.

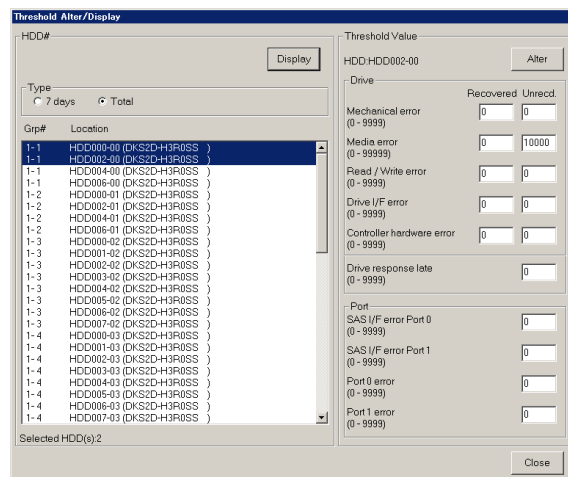
Recovered: Threshold of errors recoverable by retry.

Unrecd: Threshold of errors not recoverable by retry.

(Simple Selected)



(Multiple Selected)



Grp# : the parity group.

SPARE : spare HDD

RSRVD : reserved HDD with sparing

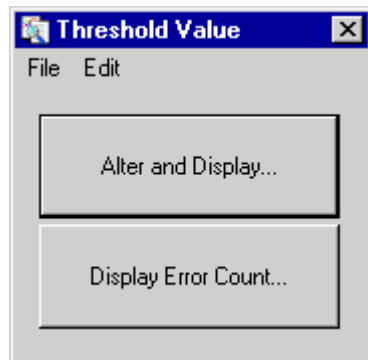
* : spare HDD in use.

3.
 - Click the [Close] button in the “Threshold Alter/Display”.
 - Close the “Threshold Value” window.
 - Close the “Information” window.

[2] Altering threshold value

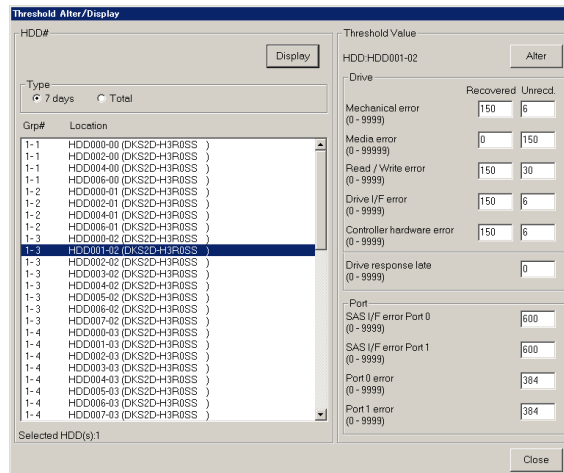
1.

Click the [Alter and Display...] button in the “Threshold Value” window.



2.

Select an HDD location from the “HDD#” list box in the “Threshold Alter/Display” window and click the [Display] button. In order to display threshold of another interval, select the interval from the “Type” list box.



Grp# : the parity group.

SPARE : spare HDD

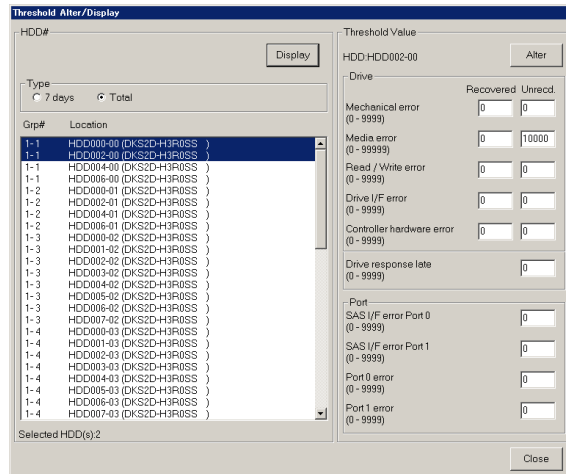
RSRVD : reserved HDD with sparing

* : spare HDD in use.

3.

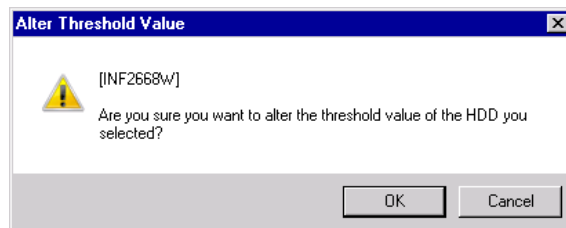
Alter a threshold value in the “Threshold Value” list box in the “Threshold Alter/Display” window.
Then click the [Alter] button.

NOTE: When multiple HDD locations are selected from the “HDD#” list box with the control key being hold down, the thresholds for all the selected HDDs are modified to the same value.



4.

Click the [OK] button in the “Alter Threshold Value” [2668] dialog box.



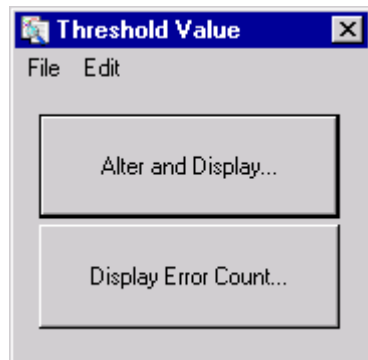
5.

Click the [Close] button in the “Threshold Alter/Display”.
Close the “Threshold Value” window.
Close the “Information” window.

[3] Displaying an error count

1.

Click the [Display Error Count...] button in the “Threshold Value” Window.



2.

Select an HDD location from the HDD Location drop-down list in the “Threshold Counter Display” window to display the error count for the HDD.

NOTE: Please execute this operation with PS ON.

When with PS OFF or the communication error occurs, the display of part Today is displayed by “Unknown”.

Threshold Counter Display				
HDD: Grp# Location	<div> <div>11-1 HDD000-00 (DKS2D-H3R0SS)</div> <div>Last update: 2014/04/28 01:11:56</div> </div>			
ID(Information)	Today	7 days	Total	
Mechanical error (recovered)	00000000/(5.50)(1000.500)	00000000/150	-	
Media error (recovered)	00000000/	-	-	
Read / Write error (recovered)	00000000/(2.50)(400.200)	00000000/150	-	
Drive I/F error (recovered)	00000000/(5.50)(1000.500)	00000000/150	-	
Controller hardware error (recovered)	00000000/(5.50)(1000.500)	00000000/150	-	
Mechanical error (unrecovered)	00000000/(1.2)(20.10)	00000000/6	-	
Media error (unrecovered)	00000000/(10.50)(1000.500)	00000000/150	00000000/10000	
Read / Write error (unrecovered)	00000000/(1.10)(40.20)	00000000/30	-	
Drive I/F error (unrecovered)	00000000/(1.2)(20.10)	00000000/6	-	
Controller hardware error (unrecovered)	00000000/(1.2)(20.10)	00000000/6	-	
Drive response late	00000000/(8.8)-	-	-	
SAS I/F error Port 0	00000000/(80.200)(4000.400)	00000000/600	-	
SAS I/F error Port 1	00000000/(80.200)(4000.400)	00000000/600	-	
Port 0 error	00000000/(128)(256)	00000000/384	-	
Port 1 error	00000000/(128)(256)	00000000/384	-	
Today [Error Count / Threshold Value] Warning [Level1_Level2] Blockade [Level1_Level2]				
7 days Total [Error Count / Threshold Value]				

Grp# : the parity group.

SPARE : spare HDD

RSRVD : reserved HDD with sparing

* : spare HDD in use.

3.

Click the [Close] button in the “Threshold Counter Display”.

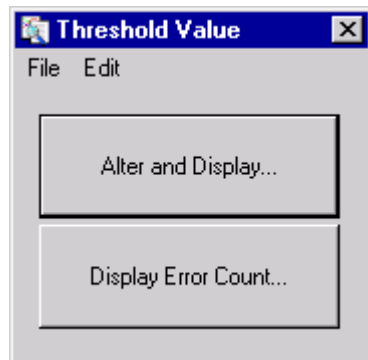
Close the “Threshold Value” window.

Close the “Information” window.

[4] Resetting an error count

1.

Click the [Display Error Count...] button in the “Threshold Value” window.



2.

Select the HDD location, for which you want to reset the error count, from the “HDD Location” drop-down list in the “Threshold Counter Display” window and also click the [Reset] button.

ID (Information)	Today	7 days	Total
Mechanical error (recovered)	00000000/(5,50)/(1000,500)	00000000/150	-
Media error (recovered)	00000000/-	-	-
Read / Write error (recovered)	00000000/(2,50)/(400,200)	00000000/150	-
Drive I/F error (recovered)	00000000/(5,50)/(1000,500)	00000000/150	-
Controller hardware error (recovered)	00000000/(5,50)/(1000,500)	00000000/150	-
Mechanical error (unrecovered)	00000000/(1,2)/(20,10)	00000000/6	-
Media error (unrecovered)	00000000/(10,50)/(1000,500)	00000000/150	00000000/10000
Read / Write error (unrecovered)	00000000/(1,10)/(40,20)	00000000/30	-
Drive I/F error (unrecovered)	00000000/(1,2)/(20,10)	00000000/6	-
Controller hardware error (unrecovered)	00000000/(1,2)/(20,10)	00000000/6	-
Drive response late	00000000/(8,80)-	-	-
SAS I/F error Port 0	00000000/(80,200)/(4000,400)	00000000/600	-
SAS I/F error Port 1	00000000/(80,200)/(4000,400)	00000000/600	-
Port 0 error	00000000/(128)/(256)	00000000/384	-
Port 1 error	00000000/(128)/(256)	00000000/384	-

Today [Error Count / Threshold Value: Warning (Level1, Level2), Blockade (Level1, Level2)]
7 days, Total [Error Count / Threshold Value]

Grp# : the parity group.

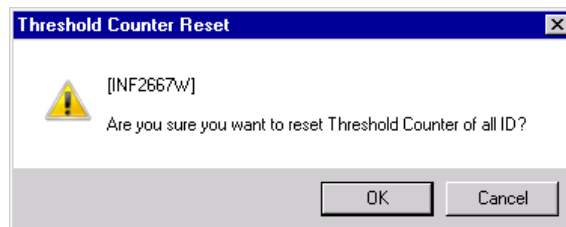
SPARE : spare HDD

RSRVD : reserved HDD with sparing

* : spare HDD in use.

3.

Click the [OK] button in the “Threshold Counter Reset” [2667] dialog box.



4.

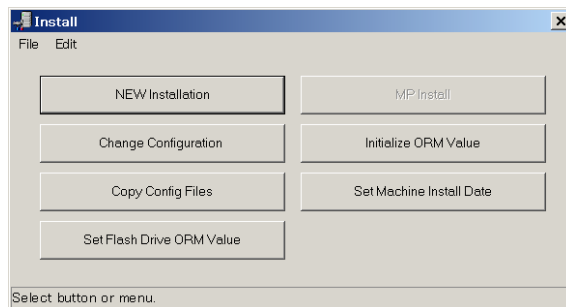
After confirming that the error count has been reset in the “Threshold Counter Display” window click the [Close] button.

Close the “Threshold Value” window.

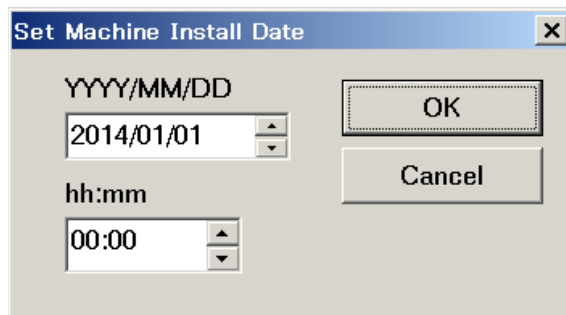
Close the “Information” window.

5.6 Setting Machine Install Data

1. Change Mode from [View Mode] to [Modify Mode].
2. Click the [Install] in the [Modify Mode].
3. Click the [Set Machine Install Date] menu in the “Install” window.



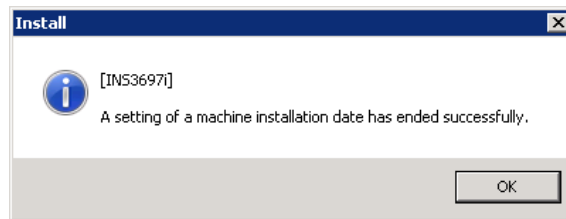
4. Input the Date and Time.
Click the [OK] button.



5.

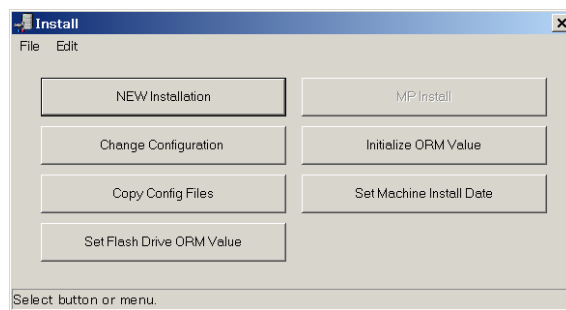
“[3697] A setting of a machine installation data has ended successfully.” is displayed.

Click the [OK] button.



6.

Close the “Install” window.



5.7 System Option

[Overview]

Change the following system option when the system operates.

1. Spare Disk Recovering-----Select the performance density when data is copied to a spare disk.
(correction copy and drive copy)
 - Interleave : Everytime 4-slot copy is completed, copy job sleeps for the time dependent on load of HOST I/O.
 - Full Speed : No sleep. (No considering HOST job)

CAUTION

Please do not use if no channel paths is varied offline.

2. Disk Copy Pace -----Specification of copy pace is supported with the “Interleave” mode at Spare Disk Recovering. Three modes are supported.
 - Medium : Optimization mode. The copy time depends on load of HOST I/O.
 - Faster : Copy job is prior to HOST job.
 - Slower : HOST job is prior to copy job.
3. Copy Operation -----
 - Dynamic Sparing : Copy automatically to a spare disk if disk failure exceeded the threshold value.
 - Correction Copy : Execute correction copy to a spare disk automatically when one drive has blocked.
4. Link Fail Threshold-----• Define the threshold value to report the link failure.

5. WR Through-----This option sets the write through operation of each LDEV to be performed when a failure occurs in the Controller Board of one of the duplicated systems.

- Destage : ON : The write through operation is performed.
(default)

OFF : The write through operation is not performed.

The write through operation is determined by a combination of the set value of this option and the set value (default value: OFF) of System Option Mode 164 which restrains write through operation. About relations of the combination of set value and the expectation operation, it is shown as follows.

Refer to [MPC05-880](#) for the setting procedure of the System Option Mode.

Table 5-11 Combination of WR Through and System Option Mode

No	System Option Mode 164		WR Through -Destage	Expectation operation
	the whole system	CLPR where target LDEV belongs to		
1	ON	ON	ON	The write after operation (*2)
2	ON	ON	OFF	The write after operation (*2)
3	ON	OFF	ON	The write after operation (*2)
4	ON	OFF	OFF	The write after operation (*2)
5	OFF	OFF	ON	The write through operation (*1)
6	OFF	OFF	OFF	The write after operation (*2)
7	OFF	ON	ON	The write after operation (*2)
8	OFF	ON	OFF	The write after operation (*2)

*1: The write through operation:

When a failure occurs in the Controller Board of one of the duplicated systems during a writing of data sent from a host, what is called the write through operation is performed in which completion of a writing is reported to the host after waiting for completion of a writing to a disk drive. For that reason, when the Controller Board of the other one of the duplicated systems is failed while the Storage System is operating with one of the duplicated systems, write pending data that exists in the operation mode above will not be lost. However, writing performance decreases by the Controller Board failure.

*2: The write after operation:

When a failure occurs in the Controller Board of one of the duplicated systems during a writing of data sent from a host, what is called the write after operation is performed in which completion of a writing is reported to a host when the data has been written to the Cache Memory. For that reason, it is made possible to reduce lowering of writing performance caused by the Controller Board failure. However, when the Controller Board of the other one of the duplicated systems is failed while the Storage System is operating with one of the duplicated systems, write pending data that exists in the operation mode above will be lost.

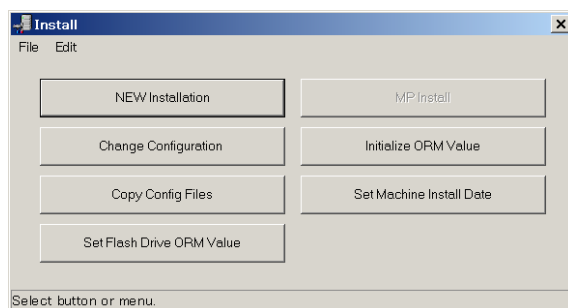
1. <Mode Change>

Change the mode to [Modify Mode].

Click the [Install] button in the “MPC” window.

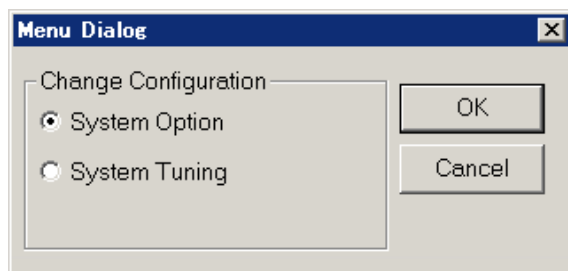
2. <Start the “Menu Dialog” window>

Click the [Change Configuration] button in the “Install” window.



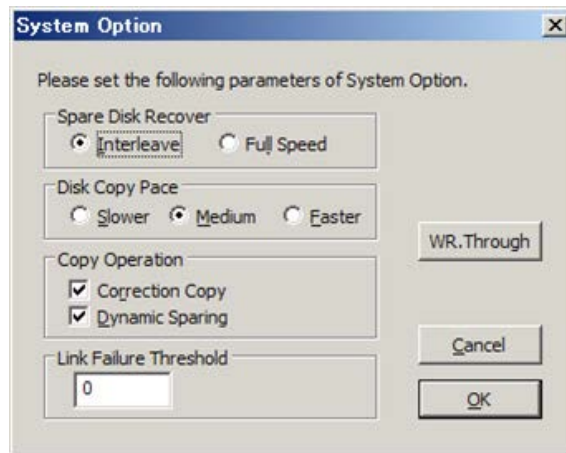
3. <Start System Option window>

Select the [System Option] in the “Menu Dialog” dialog box and click the [OK] button.



4. <Definition of System Option>

Define the system option information in the “System Option” window.



When [WR.Through] is selected, go to [Step 5](#).

After all the items are set, click the [OK] button.

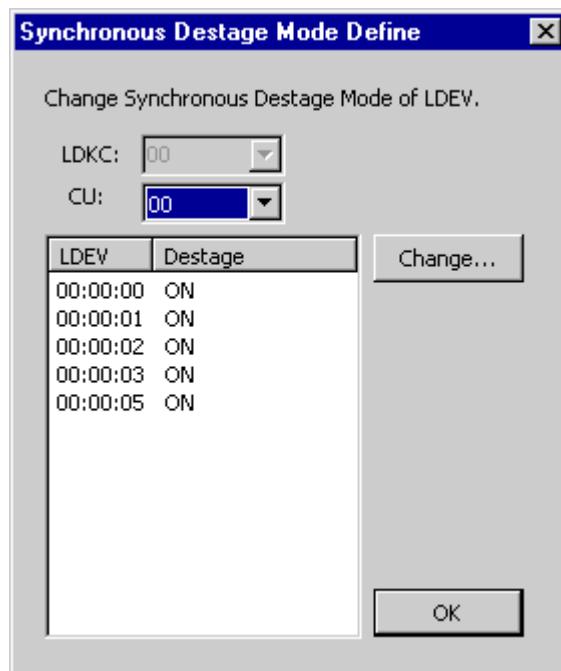
Go to [Step 6](#).

5. <Setting Destage Mode>

Set the destage mode in the “Synchronous Destage Mode Define” window.

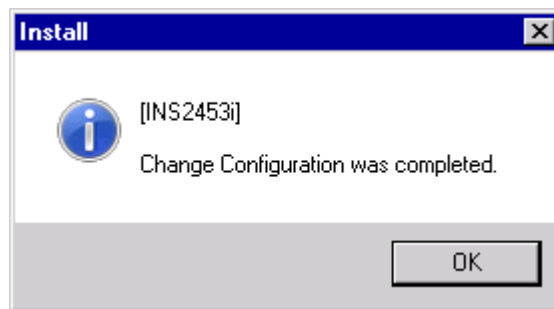
When [OK] is selected, return to [Step 4](#).

Select the target LDEV. Click the [Change...] button to switch on/off the destage mode.



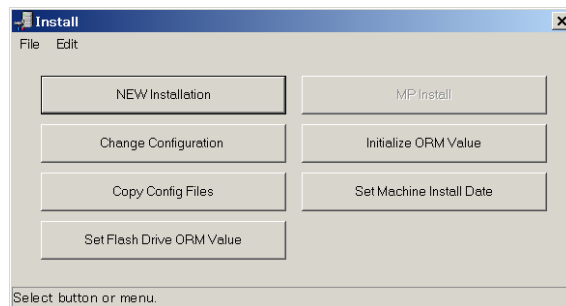
6.

“[2453] Change Configuration was completed.” is displayed.
Click the [OK] button.



7.

After the procedure is completed, return to “Install”.
Click [File]-[Exit].



8.

Change the Mode from [Modify Mode] to [View Mode].

5.8 Setting System Option Mode

NOTE: You can set the system option mode by using Command Control Interface, too. For the details, refer to Command Control Interface Command Reference “raidcom modify system_opt”.

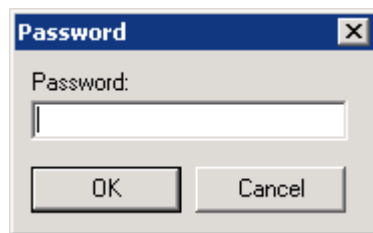
1. Close the all MPC Software menu.

2. <Enter the password>

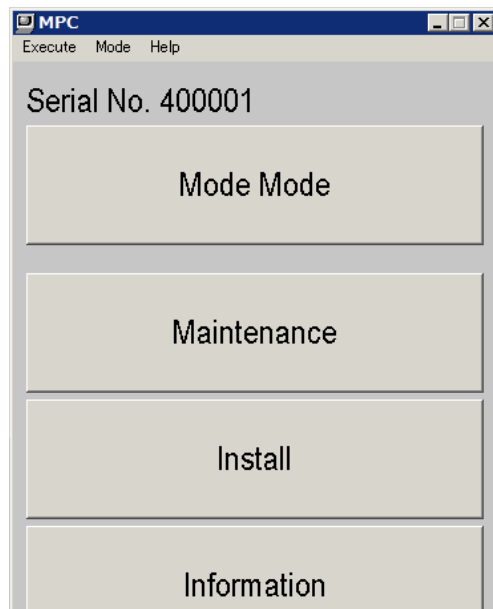
CAUTION

This is a special (exceptional) operation that requires an input of a password. Ask the technical support division and input the password.

Press [Shift] + [Ctrl] + [m] in the “MPC” window.
Enter the password, and click the [OK] button.
(Please call Technical Support Division for asking it.)

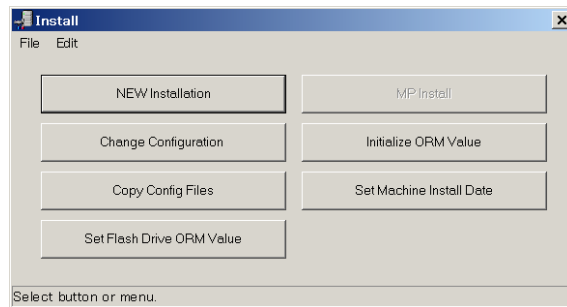


3. <Mode Mode>
[Mode Mode] is displayed.
Click the [Install] button.



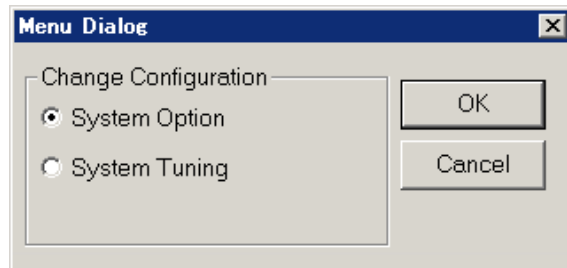
4. <Install window>

Click the [Change Configuration] menu in the “Install” window.



5. <Menu Dialog window>

Select the [System Option] menu in the “Menu Dialog” window and click the [OK] button.

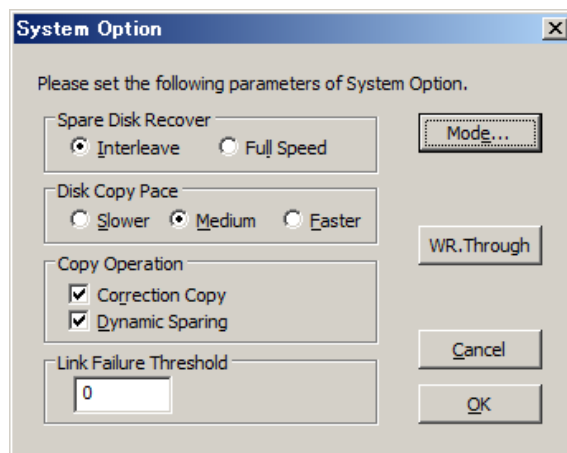


6. <System Option window>

Click the [Mode...] button in the “System Option”. Go to [Step 7](#).

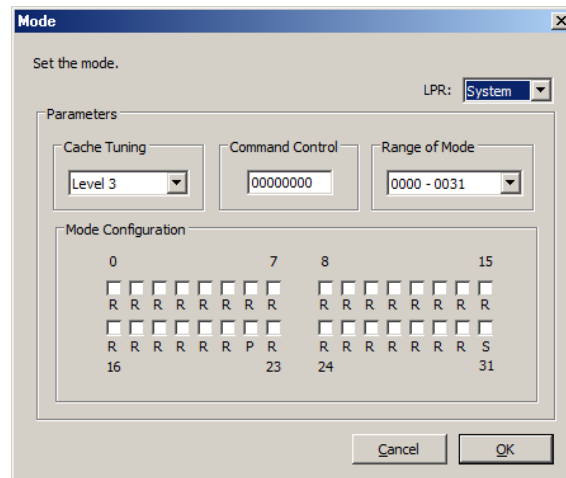
When the setting of all the entry items is completed, click the [OK] button. Go to [Step 8](#).

A selection of the [Cancel] button completes this operation procedure.



7. <Mode Window>

Select the [LPR] button and [Mode Configuration] in the “Mode” window and click the [OK] button.
Return to [Step 6](#).



- [LPR] : Select the following item.
 System : Apply to the whole system.
 LPR0 - LPR31 : Apply to the CLPR0 - CLPR31.

The following is definition of each Mode Class.

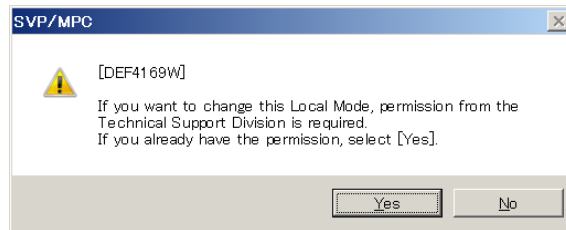
- P (Public) : Any permission is unnecessary.
 S (TS) : The permission of the Technical Support Division is necessary. When you select the check box for “S”, go to the [Step \(1\)](#).
 R (Hitachi, Ltd.) : The permission of Hitachi, Ltd. is necessary. When you select the check box for “R”, go to the [Step \(2\)](#).

(1)

“[4169] If you want to change this Local Mode, permission from the Technical Support Division is required. If you already have the permission, select [Yes].” is displayed.

When you click the [Yes] button, the settings are included. Go back to the [Step 7](#).

When you click the [No] button, the settings are not included. Go back to the [Step 7](#).

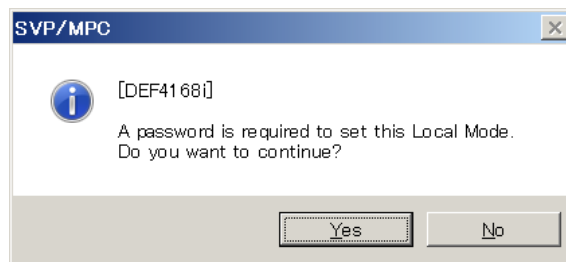


(2)

“[4168] A password is required to set this Local Mode. Do you want to continue?” is displayed.

When you click the [Yes] button, go to the [Step \(a\)](#).

When you click the [No] button, go back to the [Step 7](#).



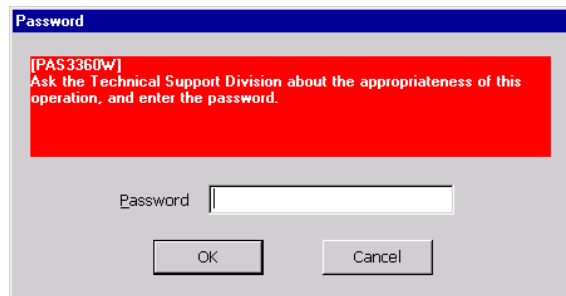
(a)

“Password”[3360] window is displayed.

Enter the password and click the [OK] button.

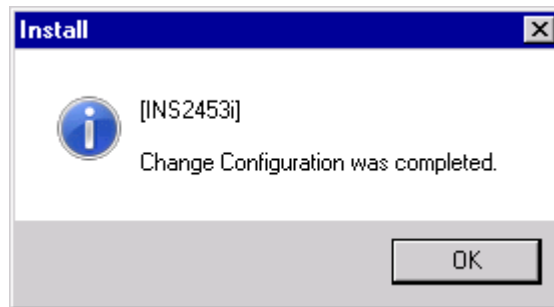
Go back to the [Step 7](#).

Entering the password is required in this operation. Please call Technical Support Division for asking it.



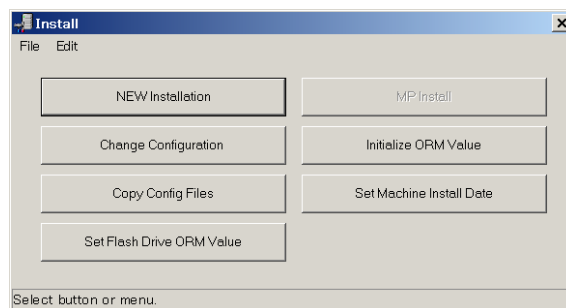
8.

“[2453] Change Configuration was completed.” is displayed.
Click the [OK] button.



9.

Return to the “Install” window.

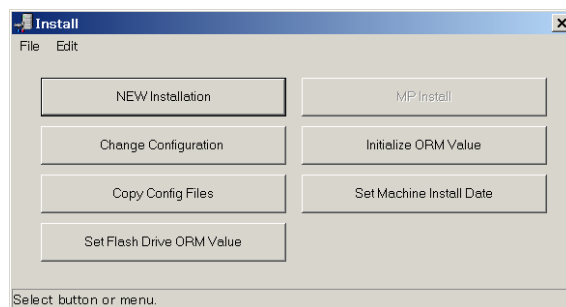


10.

Perform the procedure of [Step 4](#) to [Step 7](#) to display the “Mode” window and confirm that the changed contents are reflected.
After the confirmation, click the [Cancel] button in the “Mode” window and the “System Option” window to close the window.

11.

Close the “Install” window. Click [File]-[Exit].



12.

Change the Mode from [Mode Mode] to [View Mode].

5.9 System Tuning

NOTICE: Powering off/on is required owing to the performance of this operation.

Overview

This function modifies the part of established Storage System configuration data.

The data to be modified is control data closely related to a host device, so the data cannot be modified on on-line.

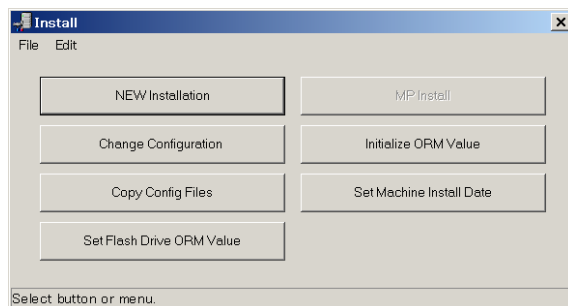
After modification of the data, power DKC off and on.

The data to be modified is listed below.

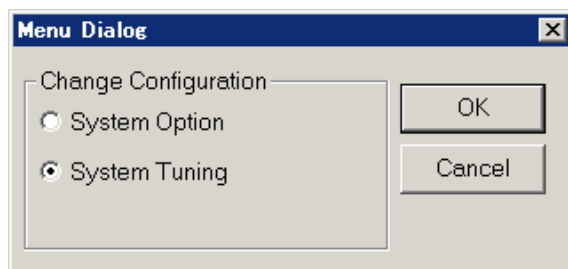
'DKC Configuration'----- DKC Serial Number

1. <Start [Install]>
Change the Mode from [View Mode] to [Modify Mode].
Click [Install] from “MPC”.

-
2. Click the [Change Configuration] button from “Install”.



-
3. <Select System Tuning>
Select [System Tuning] from “Menu Dialog”, and click the [OK] button.



4.

NOTICE: Powering off/on is required owing to the performance of this operation.
Ask the technical support division about the appropriateness of the operation, and
input a password after getting an approval of executing the operation.

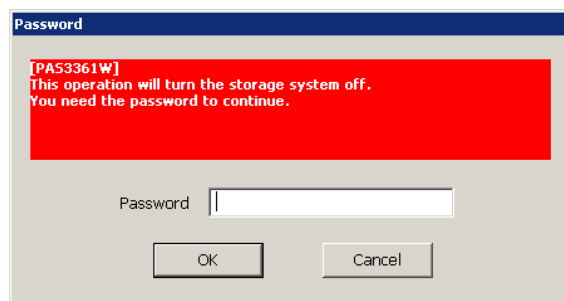
(1)

Enter the password and click [OK] in “Password”[3361] window.

Password is needed for this operation.

Please call Technical Support Division to obtain a password and authorization.

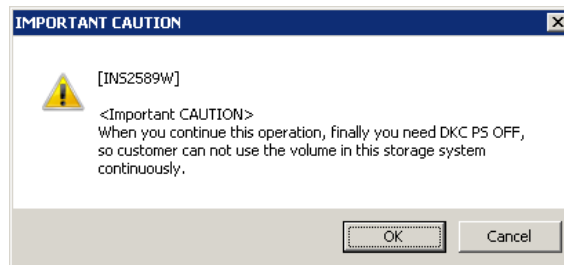
If [Cancel] is clicked, return to [Step 2](#).



(2)

Click [OK] in response to the confirmation message

“[2589] <Important CAUTION> When you continue this operation, finally you need DKC PS OFF, so customer cannot use the volume in this storage system continuously.”.



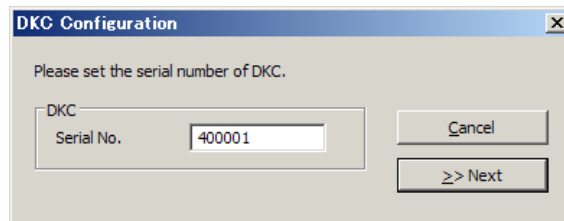
5. <DKC Configuration window>

Define the configuration information following the Storage System configuration worksheet.

[>>Next]: Go to [Step 6](#).

In the case of click [Cancel],

this operation procedure terminates.



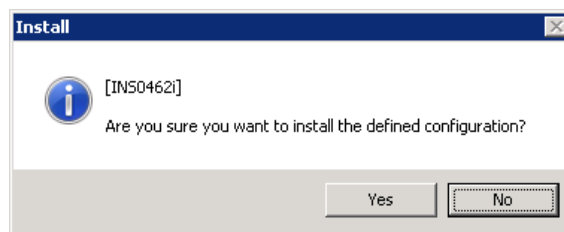
NOTICE: When the serial number is changed and it is different from the serial number registered in the Storage Device List, register the Storage System in the Storage Device List with the changed serial number after completing the maintenance operation.

6. <Include configuration information>

(1)

Click [Yes] in response to the confirmation message “[0462] Are you sure you want to install the defined configuration?”.

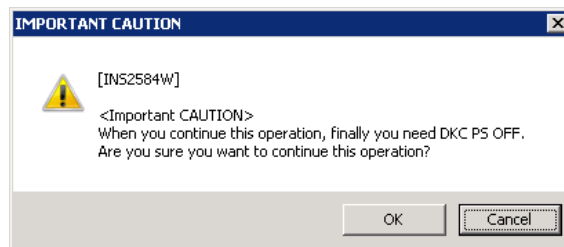
Click [No] suppresses the configuration inclusion processing and terminates the installation procedure.



(2)

Click [OK] in response to the confirmation message

“[2584] <Important CAUTION> When you continue this operation, finally you need DKC PS OFF. Are you sure you want to continue this operation?”.



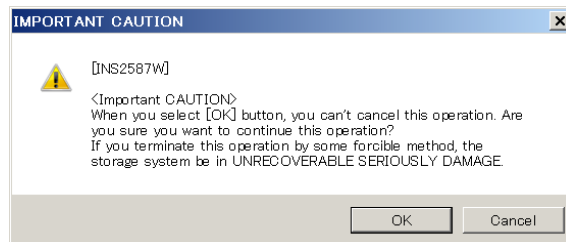
(3)

Click [OK] in response to the confirmation message

“[2587] <Important CAUTION> When you select the [OK] button, you can't cancel this operation.

Are you sure you want to continue this operation?

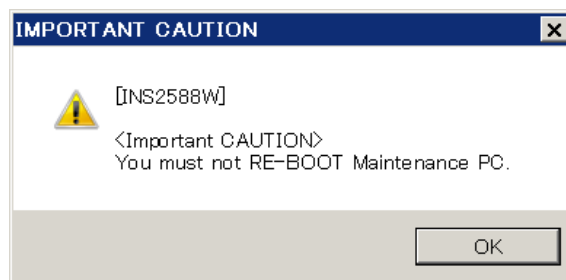
If you terminate this operation by some forcible method, the storage system be in UNRECOVERABLE SERIOUSLY DAMAGE.”.



(4)

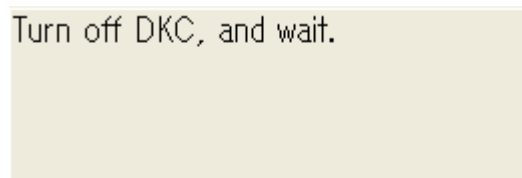
Click [OK] in response to the confirmation message

“[2588] <Important CAUTION> You must not RE-BOOT Maintenance PC.”.



7.

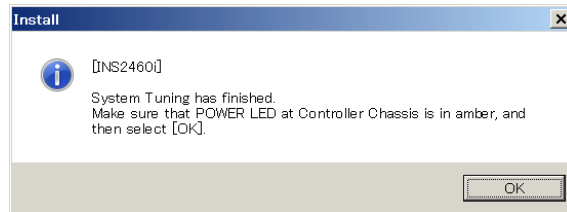
Make sure that “Turn off DKC, and wait.” is displayed and perform the power-off procedure from the Controller Chassis.



8.

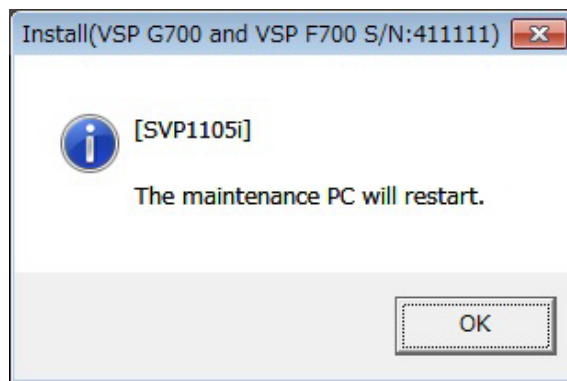
After making sure that the DKC power is turned off, click [OK] in response to “[2460] System Tuning has finished. Make sure that POWER LED at Controller Chassis is in amber, and then select [OK].”.

NOTE: The Maintenance PC power will not turn off even when DKC is powered off.



9.

Click [OK] in response to the confirmation message “[1105] The maintenance PC will restart.”.



10.

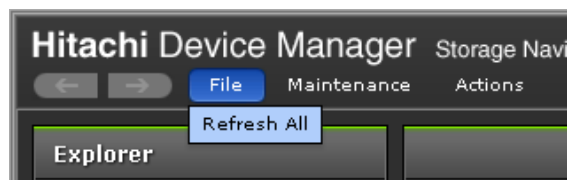
Perform the power-on procedure from the Controller Chassis.

11.

Start the Web Console referring to [“2.5 Starting Web Console”](#).

12.

Please select [File]-[Refresh All] from the menu and update the information in the “Web Console” window.



5.10 Config Backup

The configuration information backup files are downloaded from Maintenance Utility. (See [“3.28 Obtaining Configuration Information Backup”](#).)

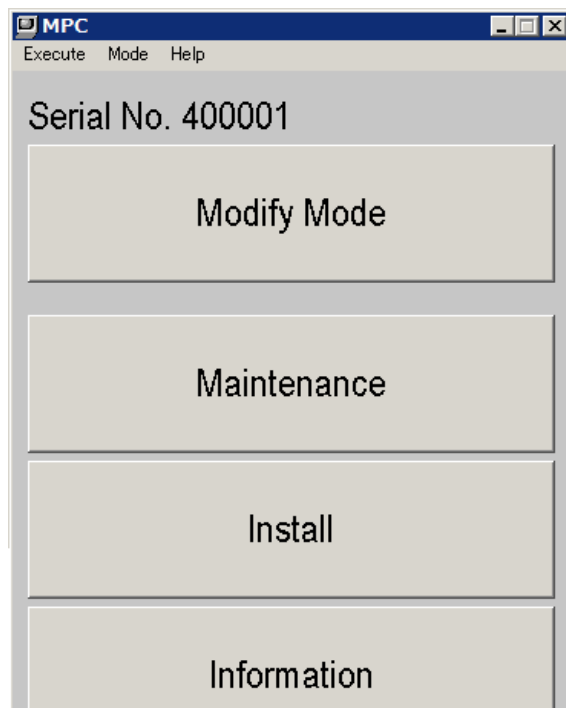
When you click [Copy Config Files] in the “Install” window, the message that instructs you to operate on Maintenance Utility (CNFCPY [4701]) is displayed.

5.11 Maintenance Screen

5.11.1 Start

1. <Start>

Click the [Maintenance] button in the “MPC” window.



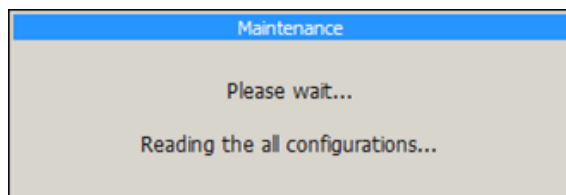
2. <Start Condition Check>

! CAUTION

Do not change the window until completing the communication of MPC Software-DKC.

The following message is displayed.

“Please Wait...”



3. <Start Error>

When an error occurred while starting the status, the message to indicate the error factor is output.

- Cluster failure

“[0125/0126] Cluster-n is failed!”

n: 1 or 2

Restore the Power Supply (Refer to TROUBLESHOOTING SECTION “[2.1.1 Failures at the Time of Start-Up](#)”) if the Power Supply are fault (Refer to the status of the Power Supply parts). (Refer to “[9.3.4.2 DKC Information View](#)”.)

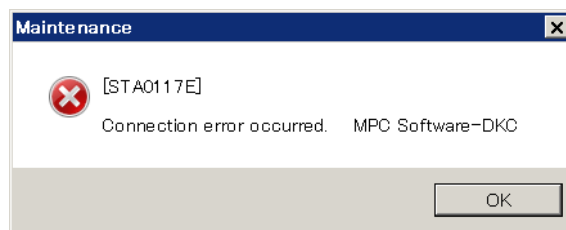
Execute the procedure from [Step 1](#) again after checking that the target processing is completed.



- Communication failure

“[0117] Connection error occurred. MPC Software-DKC”

Refer to TROUBLESHOOTING SECTION “[3.10 Recovery Procedure for LAN Error \(SIM = 7d01xx, 7d02xx\)](#)”.



4. <Status Display>

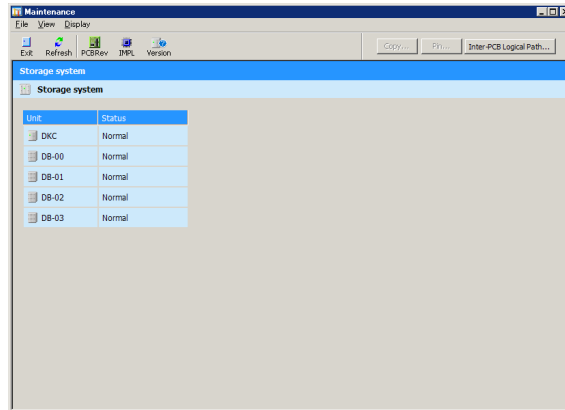
The Storage System information is displayed in the “Maintenance” window, and the status starts.

(“-----”, or “Unknown” is displayed in the point where the information acquisition is impossible due to a communication failure or an environment monitor failure.)

NOTE: Displayed information is the Storage System information on point that starts the screen.

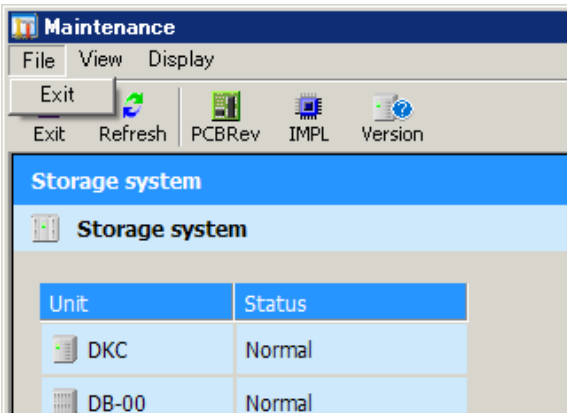
To refer to latest information, select the [Refresh] button.

(Refer to “5.11.3 Update”)



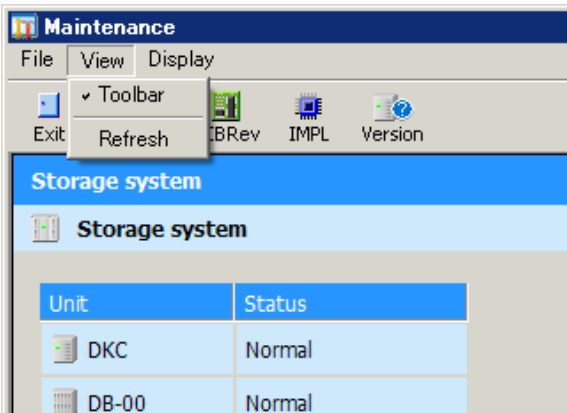
5.11.2 Terminate

Click [File]-[Exit] on the menu bar in the “Maintenance” window.



5.11.3 Update

Click [View]-[Refresh] on the menu bar in the “Maintenance” window.



5.12 Maintenance Procedure

5.12.1 Copy Status View

This window is displayed by selecting [Copy...] on the dialog bar in the main window.

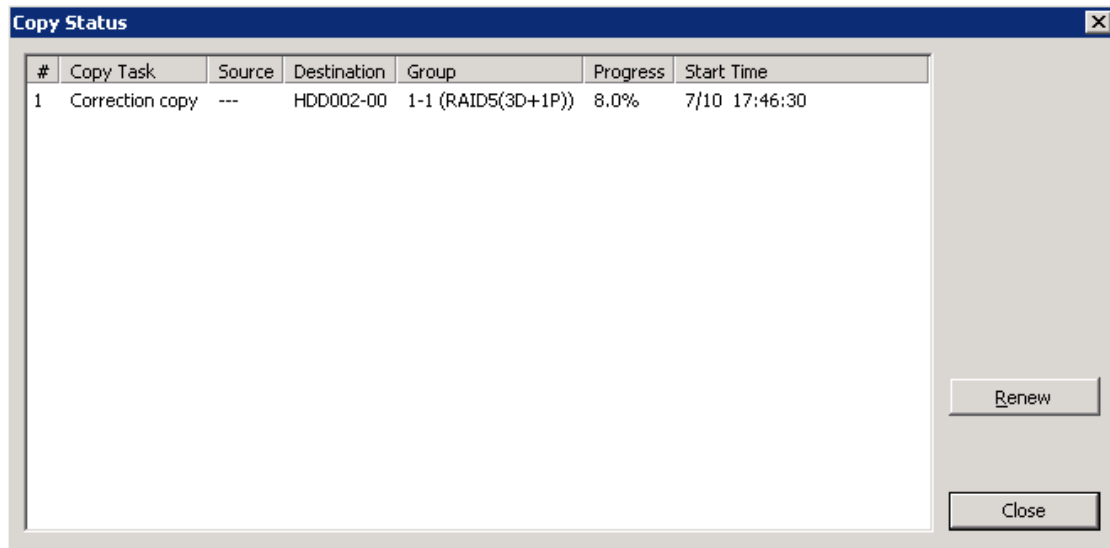


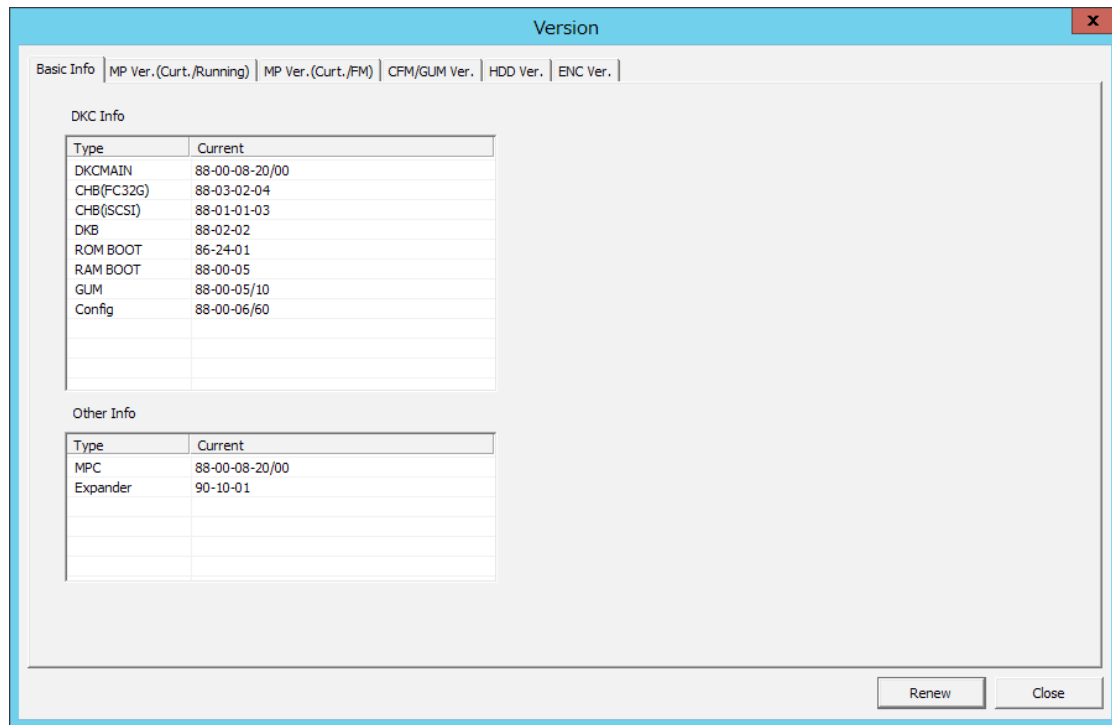
Table 5-12 Copy Status View

Item	Description
List	Displays the information on the copy operation executing right now.
	<div>[Copy Task]</div> <div>Displays the type of the copy operation.</div> <div> <div>"Correction Copy"</div> <div>: Correction copy</div> <div>"*" display:</div> <div>Waiting for the automatic copy back.</div> </div> <div> <div>"Dynamic Sparing"</div> <div>: Dynamic sparing</div> </div> <div> <div>"Copy Back"</div> <div>: Copy back</div> </div> <div> <div>"Drive Copy"</div> <div>: Drive copy</div> </div>
	[Source] Displays the location of the copy source HDD.
	[Destination] Displays the location of the copy destination HDD.
	[Group] Displays the group name to which the copy destination HDD belongs and its RAID level.
	[Progress] Displays the rate of progress of the copy operation.
	[Start Time] Displays the time when the copy operation started.
Button	<div>[Renew]</div> <div>Updates the information displayed.</div>

5.12.2 Version of Firmware

Click the [Version] button in this order in the “Maintenance” window.

The “Version” window is displayed.



Clicking each tab displays the corresponding version information.

No.	Tab name	Description
1	[Basic Info]	[Basic Info]: Displays a representative version of each Firmware.
2	[MP Ver.(Curt./Running)]	[MP Ver.(Curt./Running)]: Displays a running version on each MP.
3	[MP Ver.(Curt./FM)]	[MP Ver.(Curt./FM)]: Displays a FM version on each MP.
4	[CFM/GUM Ver.]	[CFM/GUM Ver.]: Displays CFM and GUM versions on each CTL.
5	[HDD Ver.]	Displays a model and version of each HDD.
6	[ENC Ver.]	Displays an ENC version.

<About the display>

When a version of the Firmware concerned cannot be displayed for some reason, the following is displayed.

- “-” (Hyphen) : The Firmware is not installed.
- “?” (Question mark) : Getting of the version information failed.
- “x” : The data that has been got is outside the range of application.

<Update of the information>

To update the information, which is displayed through the selection of “Version”, to the latest one, click the [Renew] button.

5.12.2.1 Basic Info

The list of Firmware operating on the Storage System and the versions are displayed.

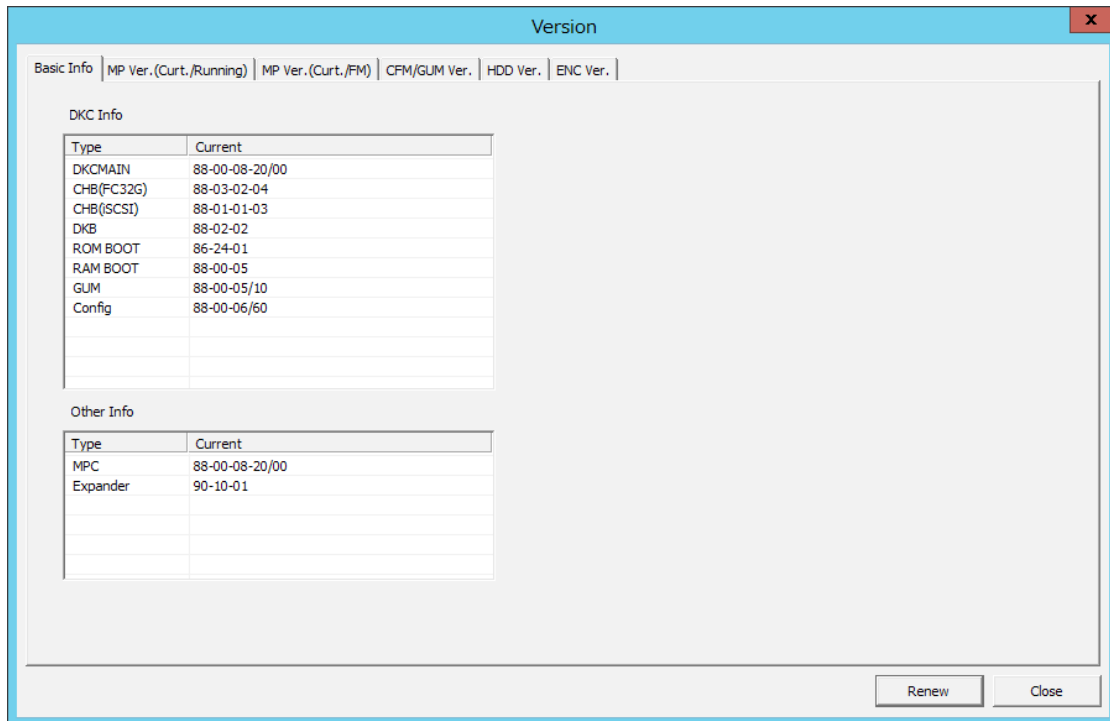



Table 5-13 Displayed information

Item		Description
DKC Info list	Type	Firmware name. <Target> <ul style="list-style-type: none"> • DKC MAIN • CHB (FC16G) • CHB (FC32G) • CHB (iSCSI) • DKB • RAM BOOT • ROM BOOT • GUM • Config
	Current	Main version of the Firmware in use.
Other Info list	Type	Firmware name. <Target> MPC Expander
	Current	Main version of the Firmware in use.

5.12.2.2 MP Ver.(Curt./Running)

The running version of each MP is displayed.

If any of the unmatched information has occurred in the items, an icon  to indicate the error is displayed in the tab.

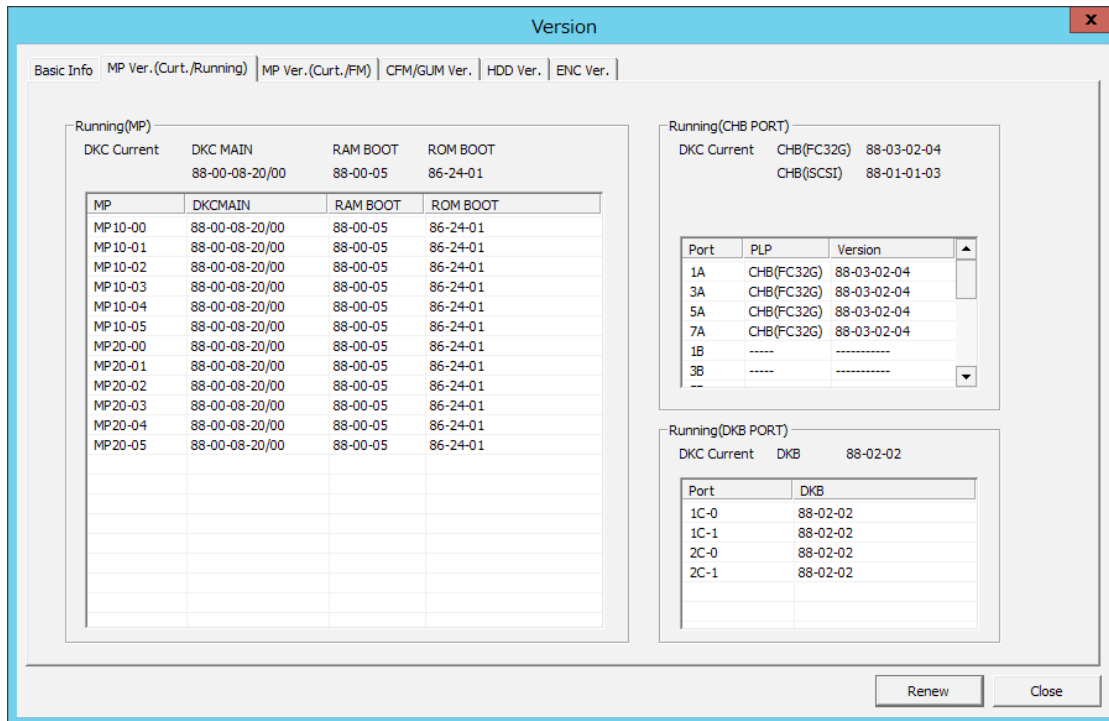


Table 5-14 Displayed information

Item			Description
MP Running area	DKC Current		Displays the version information held by DKC (same as Basic Info tab.) <ul style="list-style-type: none"> • DKC MAIN • RAM BOOT • ROM BOOT
	MP list	MP	Displays an MP location name. Installed MP only.
		DKC MAIN	Displays the running DKCMAIN version on MP.
		RAM BOOT	Displays the running RAM BOOT version on MP.
		ROM BOOT	Displays the running ROM BOOT version on MP.
		The version highlighted in red/white is unmatched with the DKC Current. The version with "*" at the end is an unmatched item.	


(To be continued)

(Continued from preceding page)

Item		Description
CHB Port area	DKC Current	Displays the version information held on DKC (same as Basic Info tab.) CHB (FC16G) : 16 G Fibre CHB (FC32G) : 32 G Fibre CHB (iSCSI) : 10 G iSCSI
	CHB Port list	Port
		Displays a Port location name.
		PLP
		Displays a PLP program type.
DKB Port area		Version
		Displays the running Version on Port.
		The version highlighted in red/white is unmatched with the DKC Current. The version with “*” at the end is an unmatched item.
	DKC Current	Displays the version information retained in DKC (same as Basic Info tab.) DKB
	DKB Port list	Port
		Displays an SAS Port location name.
		Version
		Displays the running Version on Port.
		The version highlighted in red/white is unmatched with the DKC Current. The version with “*” at the end is an unmatched item.

5.12.2.3 MP Ver.(Curt./FM)

The version on FM (Flash Memory) of each MP is displayed.

If any of the unmatched information has occurred in the items, an icon  to indicate the error is displayed in the tab. (See TROUBLESHOOTING SECTION “2.2.10 Firmware version mismatching”.)

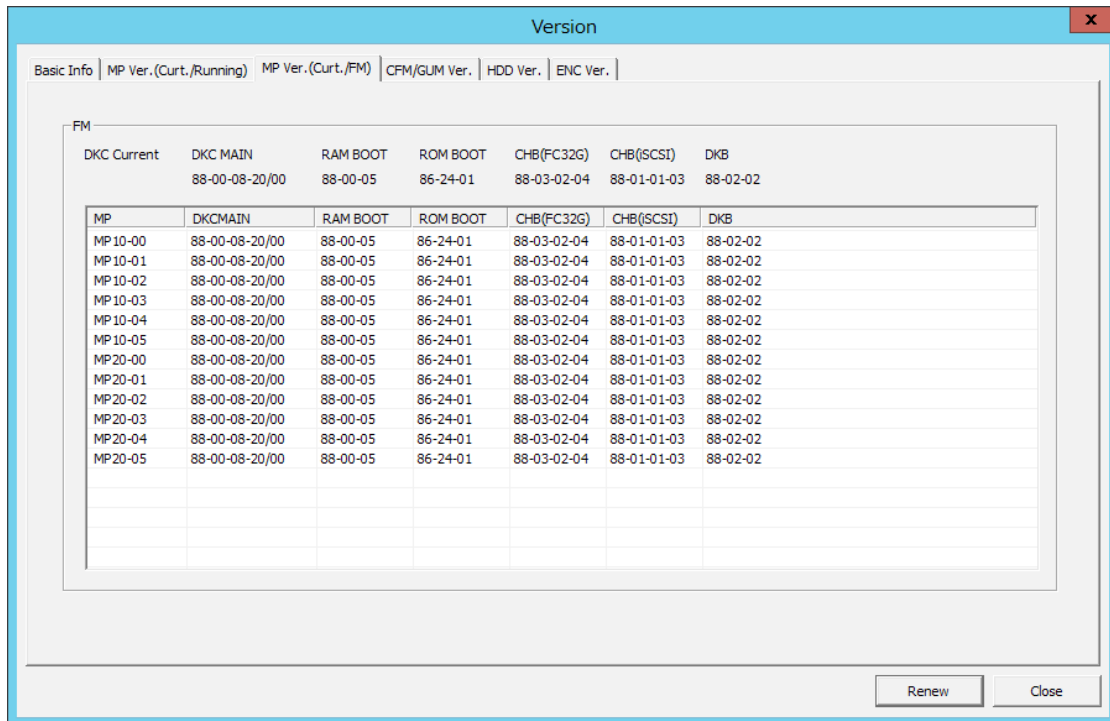


Table 5-15 Displayed information

Item	Description
DKC Current	<p>Displays the version information retained in DKC. The targets are as shown below. (Same as Basic Info tab.)</p> <ul style="list-style-type: none"> • DKC MAIN • RAM BOOT • ROM BOOT • CHB (FC16G) • CHB (FC32G) • CHB (iSCSI) • DKB

(To be continued)

(Continued from preceding page)

Item		Description
MP FM list	List	Displays the FM Firmware version of each processor. The version highlighted in red/white is unmatched with the DKC Current. The version with "*" at the end is an unmatched item.
	MP	Displays an MP location name. Installed MP only. The selected row is focused on.
	DKC MAIN	Displays DKC MAIN on FM. When unmatched with the DKC Current (including acquisition/conversion error), it is highlighted.
	RAM BOOT	Displays RAM BOOT on FM. When unmatched with the DKC Current (including acquisition/conversion error), it is highlighted.
	ROM BOOT	Displays ROM BOOT on FM. When unmatched with the DKC Current (including acquisition/conversion error), it is highlighted.
	CHB (FC16G)	Displays CHB (FC16G) on FM. When unmatched with the DKC Current (including acquisition/conversion error), it is highlighted.
	CHB (FC32G)	Displays CHB (FC32G) on FM. When unmatched with the DKC Current (including acquisition/conversion error), it is highlighted.
	CHB(iSCSI)	Displays CHB (iSCSI) on FM. When unmatched with the DKC Current (including acquisition/conversion error), it is highlighted.
	DKB	Displays DKB on FM. When unmatched with the DKC Current (including acquisition/conversion error), it is highlighted.

5.12.2.4 CFM/GUM Ver.

The CFM and GUM versions of each CTL are displayed.

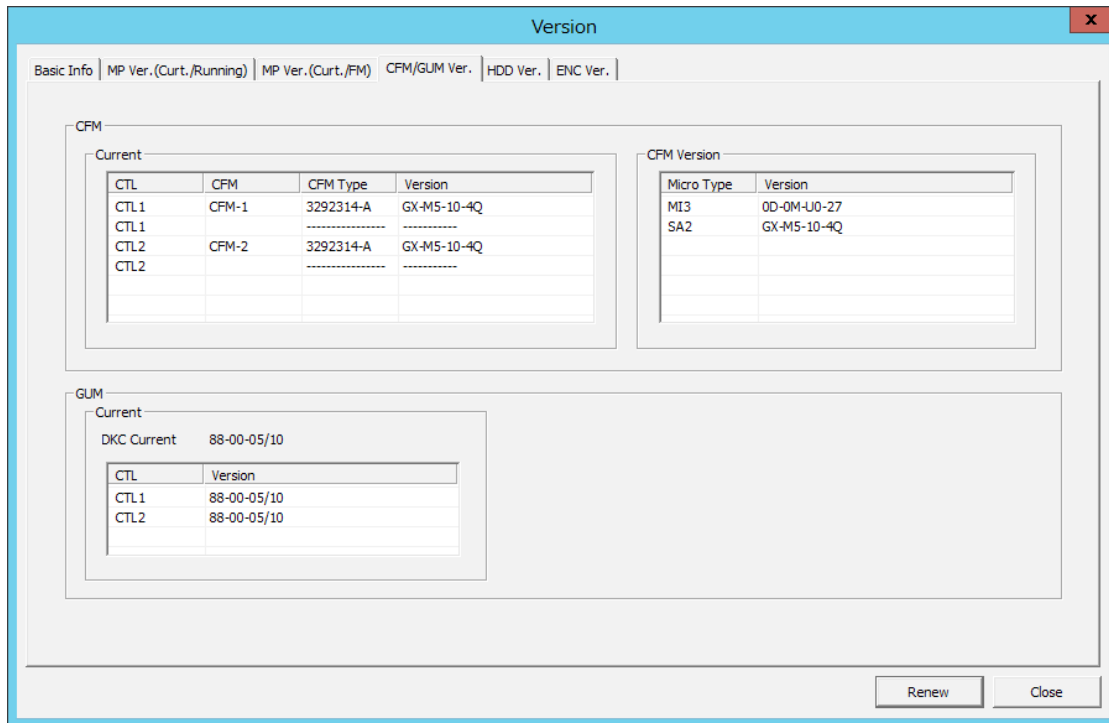


Table 5-16 Displayed information

Item		Description	
CFM Current list	CTL	Displays a CTL location name.	
	CFM	Displays a CFM location name. (Installed part only)	
	CFM type	Displayed a CFM model.	
	Version	Displays a CFM current version.	
CFM CFM list	Micro type	Displayed a CFM micro type.	
	Version	Displayed a CFM Micro version.	
GUM area	DKC Current		Displays the version information held on DKC (same as Basic Info tab.)
	GUM list	CTL	Displays a CTL location name.
		Version	Displays a GUM version. The version highlighted in red/white is unmatched with the DKC Current. The version with “*” at the end is an unmatched item.

5.12.2.5 HDD Ver.

Displays a model and version of each HDD.

If any of the lower version has occurred in the items, an icon  to indicate the error is displayed in the tab.

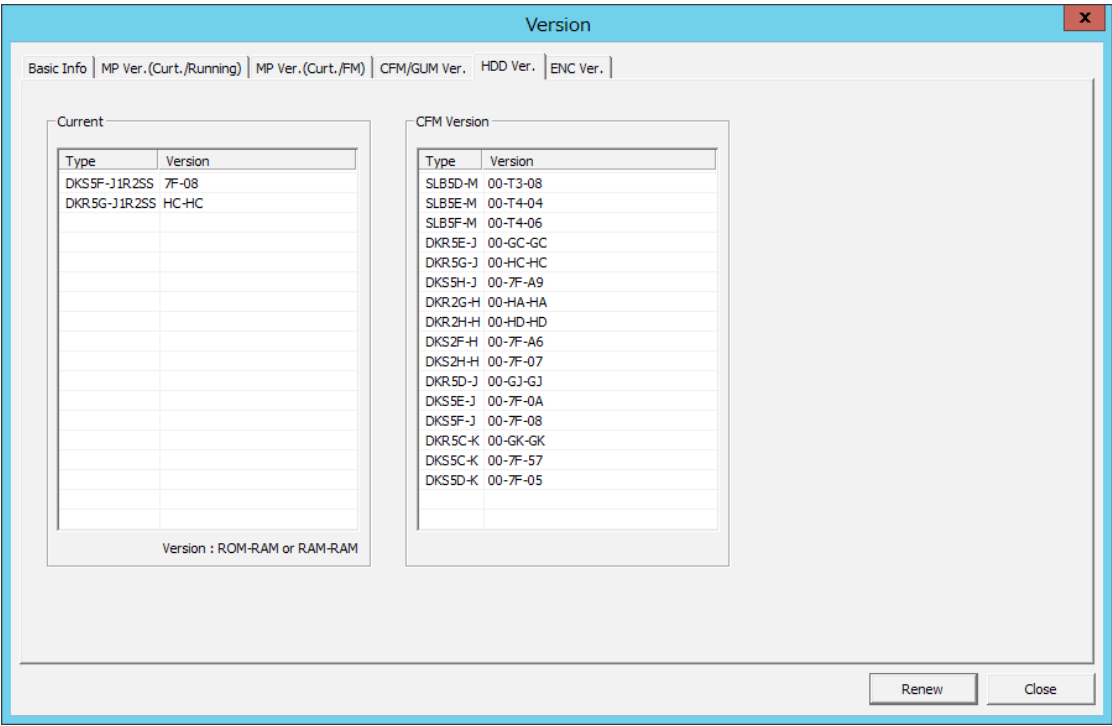


Table 5-17 Displayed information

Item		Description
HDD Current list	Type	Displays an current HDD model.
	Version	Displays an current HDD Firmware version. The version highlighted in red/white is lower than the HDD CFM Version list.
HDD CFM Version list	Type	Displays an HDD model stored in the CFM.
	Version	Displays an HDD Firmware version stored in the CFM.

<Display Drive Name>

Double-click a row from the list of [HDD] - [Current].

The “HDD List” window is displayed and the list of the Drives matched with the information is displayed.

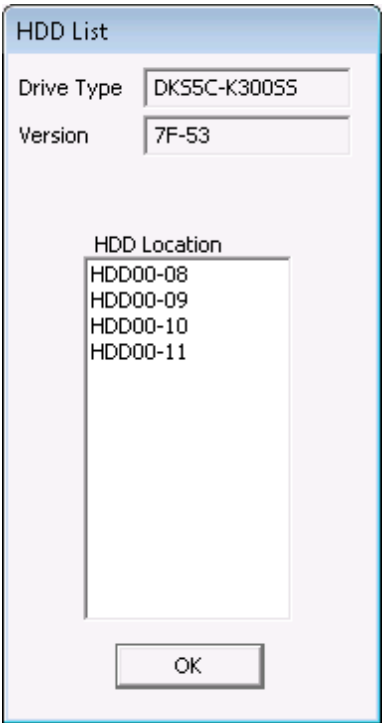


Table 5-18 Displayed information

Item	Description
Drive Type	The selected Drive type.
Version	The selected Drive Firmware version.
HDD Location	A list of Drives matched with the selected information.

5.12.2.6 ENC Ver.

The Firmware version operating on ENC is displayed.

When the individual version is lower than the version on CFM display, an icon  to indicate the error is displayed in the tab.

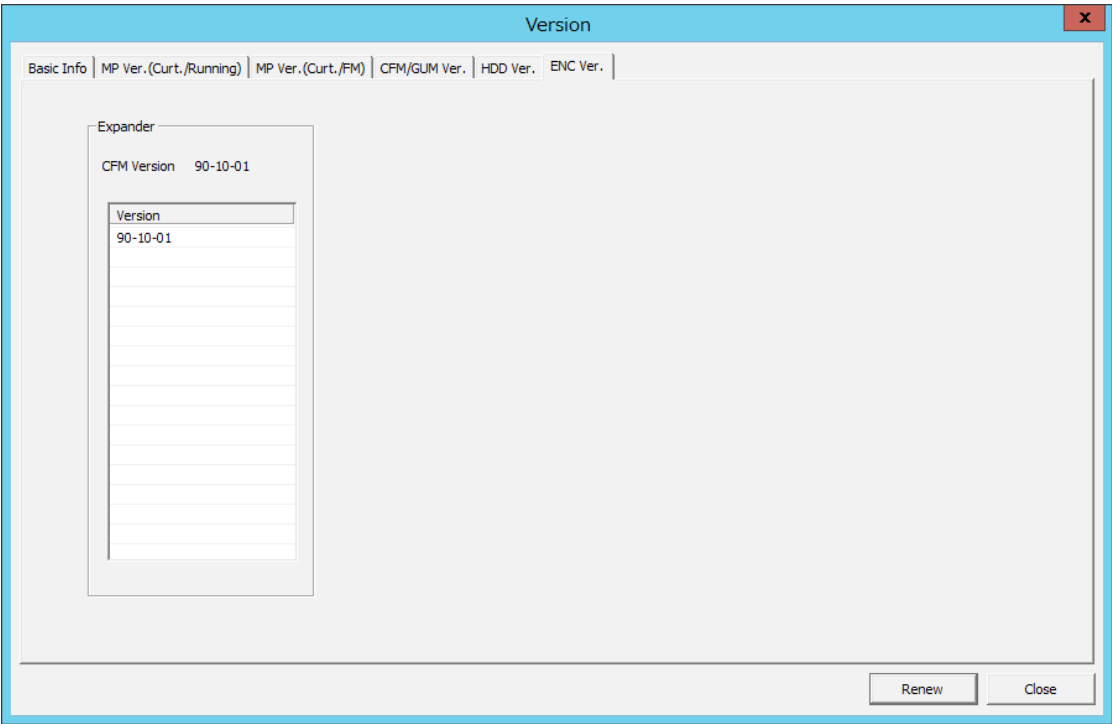


Table 5-19 Displayed information

Item		Description
CFM Version		Displays the version information held on flash memory (same as Basic Info tab.)
Expander Version list	Version	A Firmware version of each Expander in current use. 1. Click to focus on a row 2. Double-click to display the Expander List dialog. → See to (MPC05-1160) The version highlighted in red/white is unmatched with the CFM Version. The version with “*” at the end is an unmatched item.

<Display Expander Name>

Double-click a row from the list of [Expander] - [Version].

The “Expander List” window is displayed and the list of the ENC’s matched with the information is displayed.

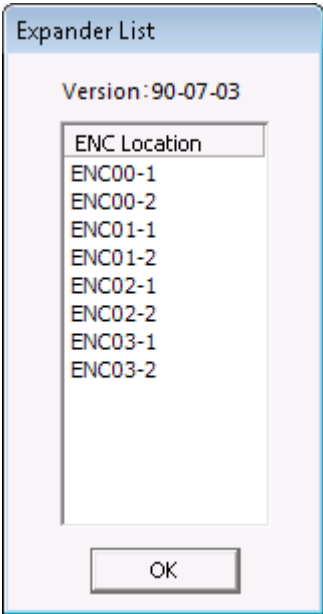


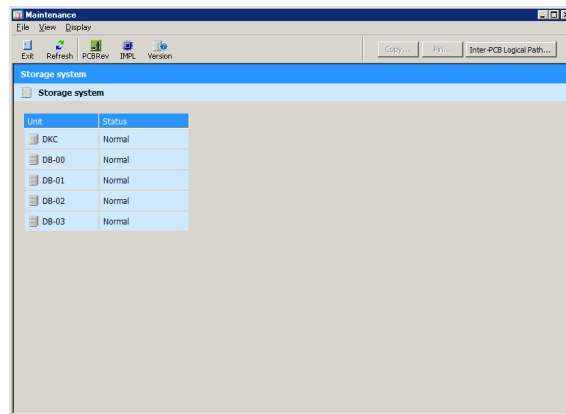
Table 5-20 Displayed information

Item	Description
Version	The selected Expander Firmware version.
ENC Location	A list of ENC’s matched with the selected version.

5.12.3 Pin Data Indication

You can save the pinned data file, by performing the Auto Dump operation. For the Auto Dump, refer to [“5.2 Dump”](#).

1. Click the [Maintenance] button.
2. Click the [PIN...] button in the “Maintenance” window.



3. Display an LDEV with a pinned slot. Select the LDEV, details of which you want to display, in “Ldkc:”, “Cu:”, “Ldev:” and click the [Detail] button. Go to [Step 4](#).

NOTE: When the pinned slot is gone, the LDEV, an occurrence of the pinned slot in which was reported by a SIM, is not displayed.

When you close the “Pinned Track” window, click the [Close] button. Go to [Step 5](#).

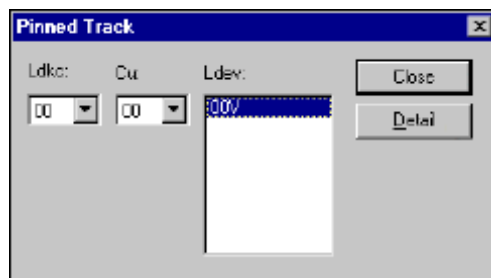


Table 5-21 List of Items

Item	Description
Ldkc	Logical DKC number
Cu	ID number of a Cu
Ldev	Number of a logical device in which pinned data exists “#”: An External volume is shown. “V”: A Virtual volume is shown. “A”: An ALU volume is shown. “S”: A SLU volume is shown. “X”: A DP volume is shown. “M”: A Migration volume is shown.

4. Display the detail of a Pin Slot.

(If there are more than 17 Pin Slots, the [Next] button will display other Pin Slots.)

- NOTE:
- If a Pin Slot has some recoverable trouble, the detail of the Pin Slot will not be displayed. Only LBA's Pin Slots are displayed. But, if the Pin Slot of LBA's can't be displayed, "-----" is displayed in both CCHH and LBA columns.
 - In case of same slot, The same value is displayed for No.
(The thing that is the same slot is shown.)
 - LDEV might not be displayed according to the timing of the information acquisition. In that case, try to click the [Refresh] button of the maintenance screen, and to acquire information.

When you want to close the "Detail" window, click the [Close] button.

Return to [Step 3](#).

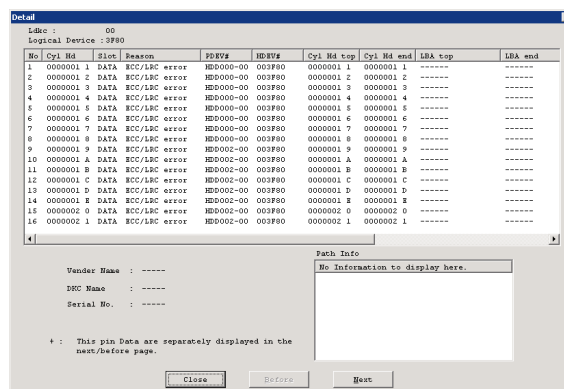


Table 5-22 List of Items

Item	Description
Logical Device	<p>Number of a logical device in which pinned data exists</p> <p>"#": An External volume is shown.</p> <p>"V": A Virtual volume is shown.</p> <p>"A": An ALU volume is shown.</p> <p>"S": A SLU volume is shown.</p> <p>"X": A DP volume is shown.</p> <p>"M": A Migration volume is shown.</p>
Cyl Hd	Number of an assembly of a cylinder and head in which pinned data exists
Slot	<p>Type of a track on which pinned data exists</p> <p>DATA : Data track</p> <p>PRTY : Parity track</p>

(To be continued)

(Continued from the preceding page)

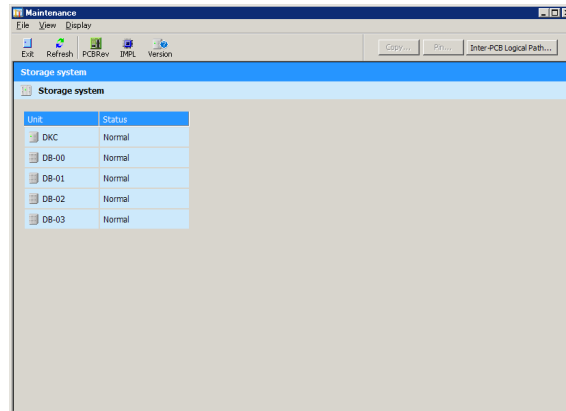
Item	Description
Reason	<p>Cause of pinned data.</p> <p>See the TROUBLESHOOTING SECTION “4.2.1 Pinned Tracks” for the recovery procedure at the following reason.</p> <ul style="list-style-type: none"> • ECC/LRC error • WRITE error • External VOL Read Error • External VOL Write Error
PDEV#	Number of an HDD of a logical device in which pinned data exists
HDEV#	<p>HDEV number</p> <p>“#”: An External volume is shown.</p> <p>“V”: A Virtual volume is shown.</p> <p>“A”: An ALU volume is shown.</p> <p>“S”: A SLU volume is shown.</p> <p>“X”: A DP volume is shown.</p> <p>“M”: A Migration volume is shown.</p>
Cyl Hd top/end	Cyl Hd at the top and end of a parity stripe
LBA top/end	LBA at the top and end of a parity stripe
HDEV# (DP)	<p>HDEV number in Dynamic Provisioning</p> <p>“#”: An External volume is shown.</p> <p>“V”: A Virtual volume is shown.</p> <p>“A”: An ALU volume is shown.</p> <p>“S”: A SLU volume is shown.</p> <p>“X”: A DP volume is shown.</p> <p>“M”: A Migration volume is shown.</p>
LBA (DP) top/end	LBA at the top and end of a parity stripe in Dynamic Provisioning
Vender Name	Name of a vender of a external Device
DKC Name	Name of a DKC of a external Device
Serial No.	Serial number of a external Device
Path Info	Path information of a external Device

- Click the [Close] button in the “Detail” window.
Click the [Close] button in the “Pin Volume” window.
Close the “Maintenance” window.

5.12.4 PCB/SFP Revision Display

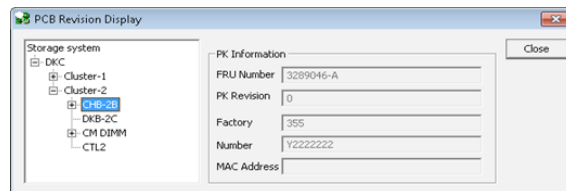
1. Click the [Maintenance] button in the “MPC” window.

2. Click the [PCBRev] button in the “Maintenance” window.



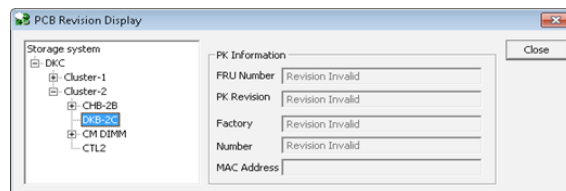
3. “Reading or Writing PCB revision informations...” is displayed.

4. Select a PCB/PORT whose revision you want to display in the “PCB Revision Display” window.



NOTE: To confirm the SFP revision, select a PORT to be checked.

- When selecting a DKB in the CBXSS/CBXSL/CBSS/CBSL, [Revision Invalid] is displayed for all the items. When selecting a CHB in the CBXSS/CBXSL, [Revision Invalid] is displayed for all the items.

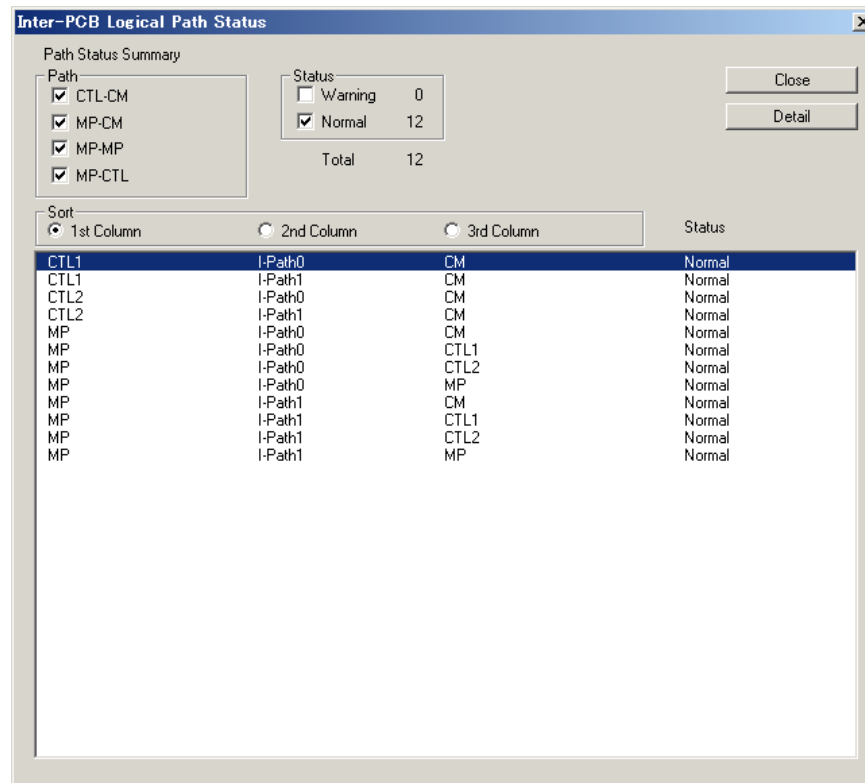


5. Click the [Close] button in the “PCB Revision Display” window.

6. Close the “Maintenance” window.

5.12.5 Inter-PCB Logical Path

- (1) The window for displaying status for each summary path.



Path (Check box)-----

- CTL-CM : Specifies display of summary path between CTL and CM
- MP-CM : Specifies display of summary path between MP and CM
- MP-MP : Specifies display of summary path between MP and MP
- MP-CTL : Specifies display of summary path between MP and CTL

Status (Check box)-----

- Warning : Specifies display of failed paths and displays number of the failed paths.
- Normal : Specifies display of normal paths and displays number of normal paths.

Total ----- Total number of paths that can be displayed

Sort (Radio button) ----

- 1st Column : Summary path group names are displayed in the row. When this row is selected, the path statuses in the list are sorted using the letter strings in the 1st row as a key word.
- 2nd Column : CTL location names are displayed in this row. When this row is selected, the path statuses in the list are sorted using the CTL location names as a key word.
- 3rd Column : Summary path group names are displayed in this row. When this row is selected, the path statuses in the list are sorted using the letter strings in the 3rd row as a key word.

Status ----- A status of each path is displayed.

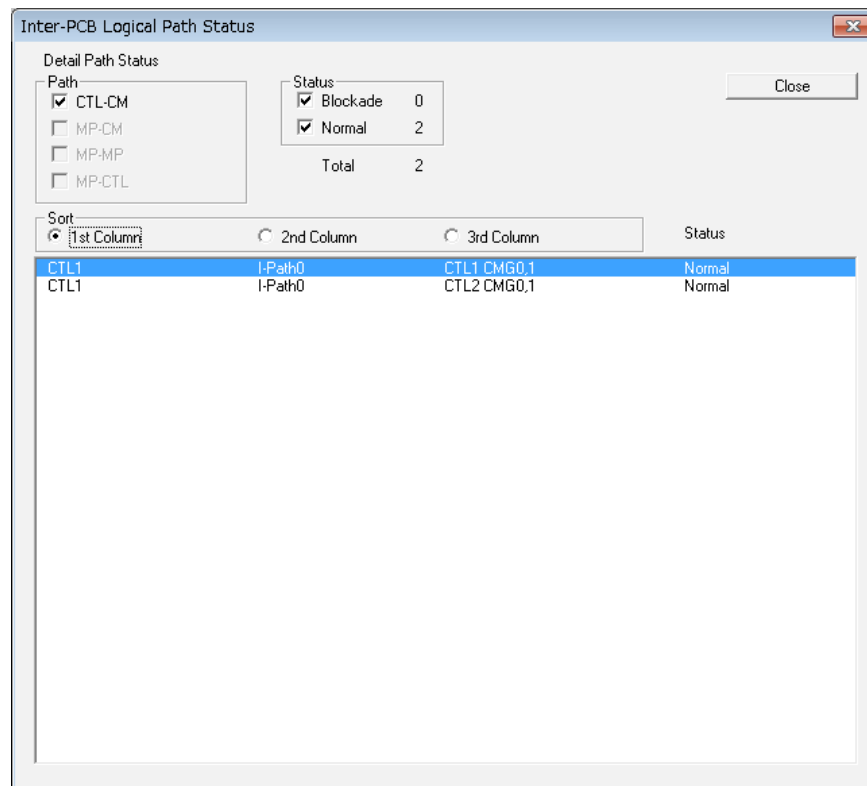
Normal : A status in which a path concerned is normal

Warning : A status in which a failure occurred in a path concerned

Detail (Button) ----- Displays detailed path status.

Close (Button)----- Terminates the display.

(2) Detailed path status display window



Path (Check box)----- Among four types of logic paths, the type of logic path which is displayed is checked. Other check boxes are not checked. Check box is not selectable.

Status (Check box)-----

Blockade : Specifies display of blocked paths and displays number of the blocked paths.

Normal : Specifies display of normal paths and displays number of the normal paths.

Total ----- Total number of paths that can be displayed

Sort (Radio button) ----

1st Column : Location names are displayed in the row. When this row is selected, the path statuses in the list are sorted using the letter strings in the 1st row as a key word.

2nd Column : CTL location names are displayed in this row. When this row is selected, the path statuses in the list are sorted using the CTL location names as a key word.

3rd Column : Location names are displayed in this row. When this row is selected, the path statuses in the list are sorted using the letter strings in the 3rd row as a key word.

Status ----- Status of each path is displayed.

Normal : Status in which a path concerned is normal

Blockade : Status in which a path concerned is blocked

Close (Button)----- Terminates the display.

5.12.6 Restoring Failed MP

CAUTION

This is a special procedure to recover a MP blockade operation without the need to self-replace the card under certain conditions specified below.

To use this procedure, please open a case with your technical support center and proceed under their guidance.

<Usage Conditions>

- To recover a MP in which WCHK1 occurred due to a Firmware problem.
Eg.) Cause of WCHK1 is EC = 1644.
- To recover a MP in which WCHK1 occurred due to an issue outside the DKC (Host/SAN).
Eg.) Cause of WCHK1 is EC = B405, and it is evident that it is caused by external factor. (Switch etc.)
- Requested as a recovery procedure for an issue notified by an Early Notice/Alert.
- Requested by following the procedure described in Maintenance Manual.

<Usage Restrictions>

- Not to be used to recover hardware failures.
- Not to be used to recover a MP of MPU which all MP in MPU blocked.

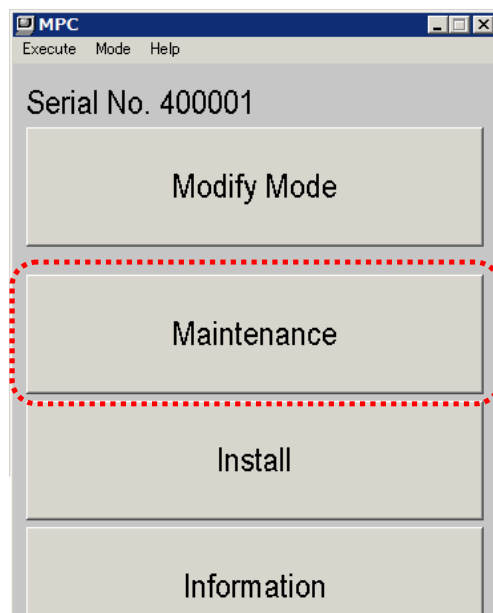
1. <Preparation>

Close each menu of the starting MPC Software entirely.

2. <Start>

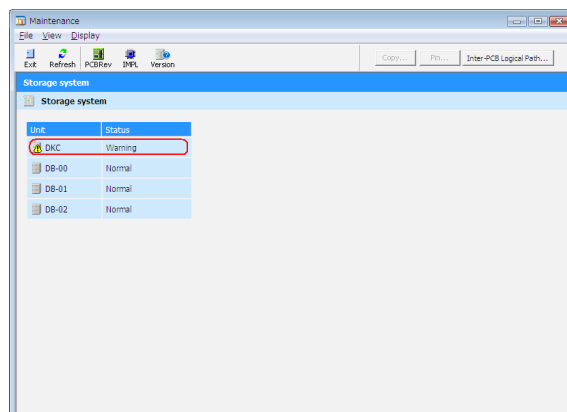
Change the mode to [Modify Mode].

Click the [Maintenance] button in the “MPC” window.



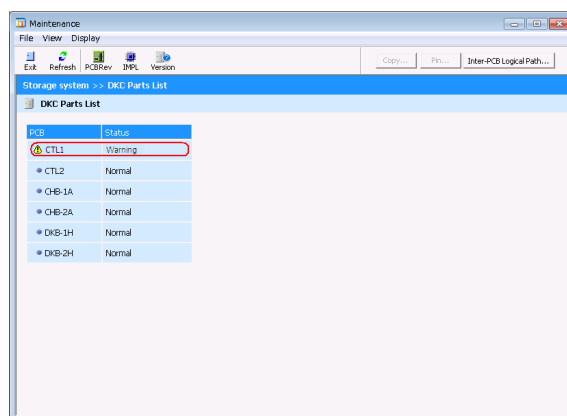
3. <Display of DKC Information>

Select the [DKC].



4. <Display of CTL Information>

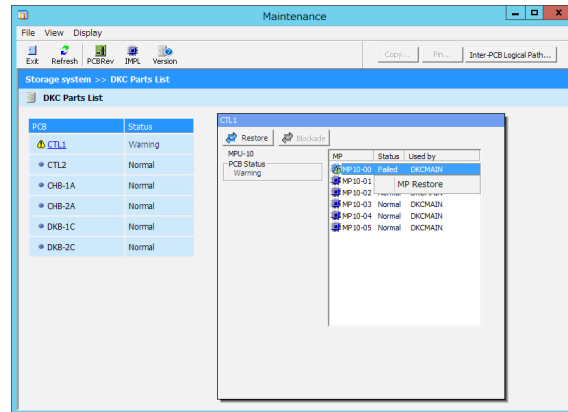
Click the [CTLn] button.



5. <Execution>

Click the right button of the mouse in the status that MP of the maintenance target on the selected.

Click the [MP Restore] button in the displayed popup menu.



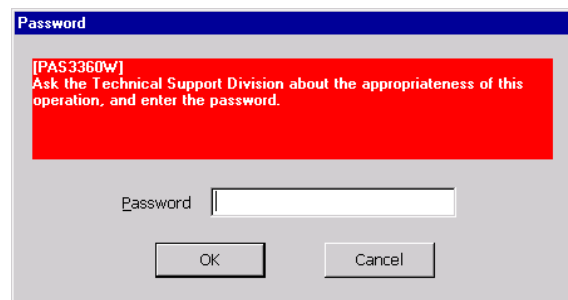
6. <Password Input>

⚠ CAUTION

When the blockade of MP attributes to a hardware failure, it is possible that Storage System down or data lost occurs. Ask the technical support division about the appropriateness of the operation, and input the password after getting an approval of executing the operation.

Corresponding to the following message, enter the password and click the [OK] button.

“[3360] Ask the Technical Support Division about the appropriateness of this operation, and enter the password.”

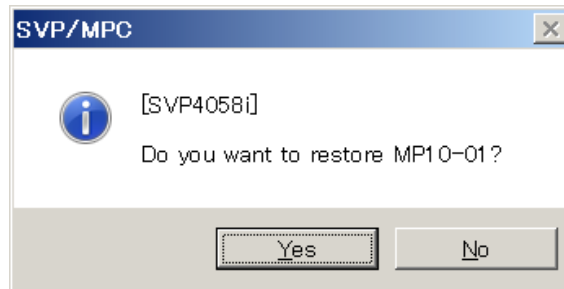


7. <Execution Check>

Click the [Yes] button for the following message.

“[4058] Do you want to restore X?”

X: Target MP



8. <Waiting for the completion of processing>

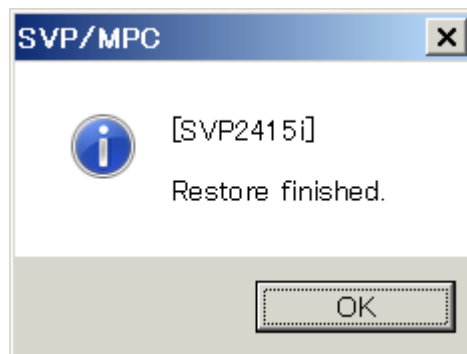
The following message is displayed.

“Please wait... Restoring the MP...”

9. <Check of the recovery completion of failed MP>

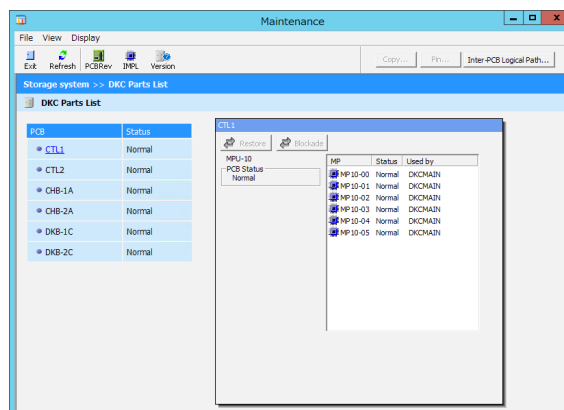
Click the [OK] button for the following message.

“[2415] Restore finished.”



10. <Check of processing result >

Check the status of the target MP with detailed view in the “Maintenance” window.



11. <Post-processing>

Close the “Maintenance” window.

Change the mode to [View Mode].

5.12.7 Failed CTL Recovery

CAUTION

This is a special procedure to recover a Cache blockade operation without the need to self-replace the card under certain conditions specified below.

To use this procedure, please open a case with your technical support center and proceed under their guidance.

<Usage Conditions>

- Requested as a recovery procedure for an issue notified by an Early Notice/Alert.
- Requested by following the procedure described in Maintenance Manual.

<Usage Restrictions>

- Not to be used to recover hardware failures.

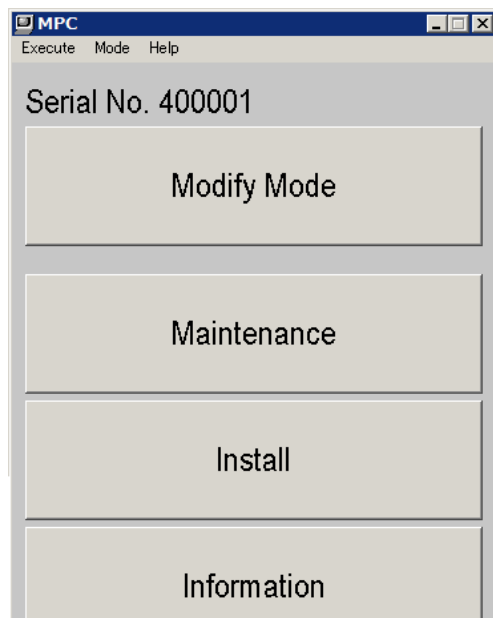
1. <Preparation>

Close each menu of the starting MPC Software entirely.

2. <Start>

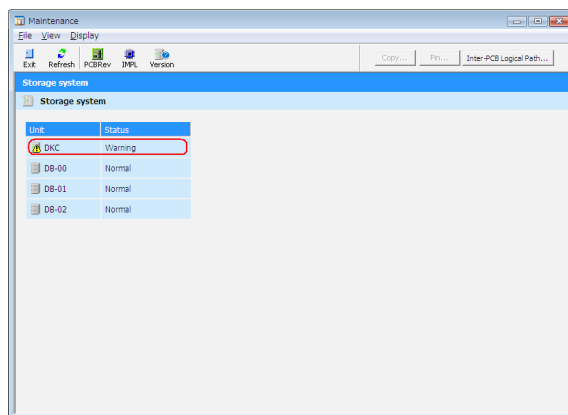
Change the mode to [Modify Mode].

Click the [Maintenance] button in the “MPC” window.



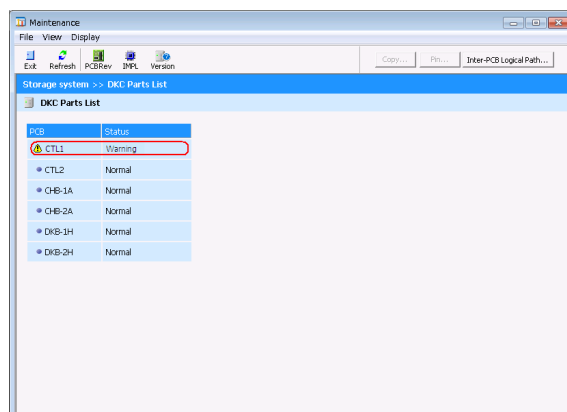
3. <Display of DKC Information>

Select [DKC].



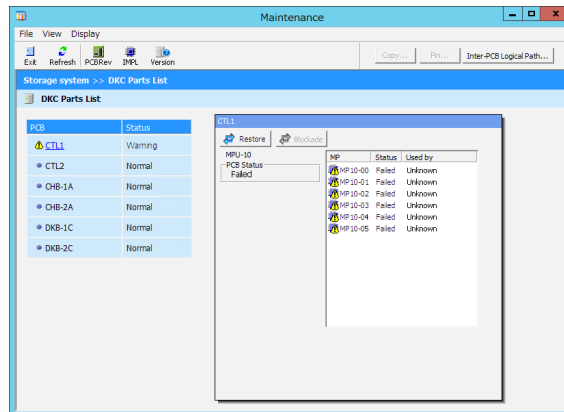
4. <Display of CTL Information>

Click the [CTLn] button.



5. <Execution>

Click the detail view [Restore] button.



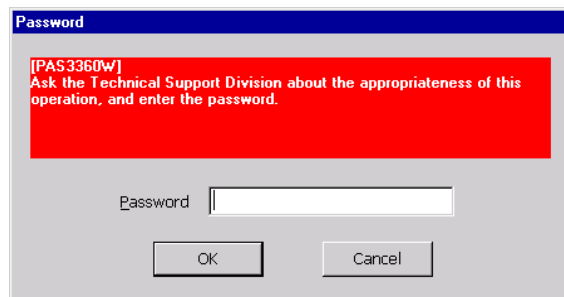
6. <Password Input>

CAUTION

When the blockade of PCB attributes to a hardware failure, it is possible that Storage System down or data lost occurs. Ask the technical support division about the appropriateness of the operation, and input the password after getting an approval of executing the operation.

Corresponding to the following message, enter the password and click the [OK] button.

“[3360] Ask the Technical Support Division about the appropriateness of this operation, and enter the password.”

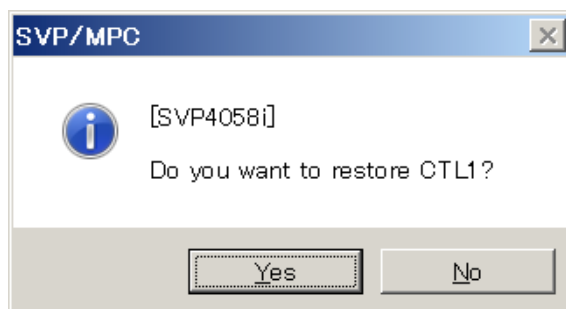


7. <Execution Check>

Click the [Yes] button for the following message.

"[4058] Do you want to restore CTLn?"

n: Cluster number of target CTL



8. <Waiting for the completion of processing>

The following message is displayed.

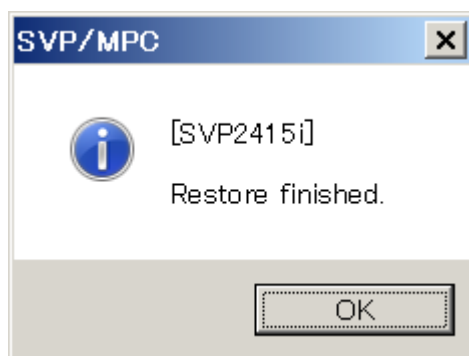
"Please wait... Restoring the CTL1..."

n: Cluster number of target CTL

9. <Check of the recovery completion>

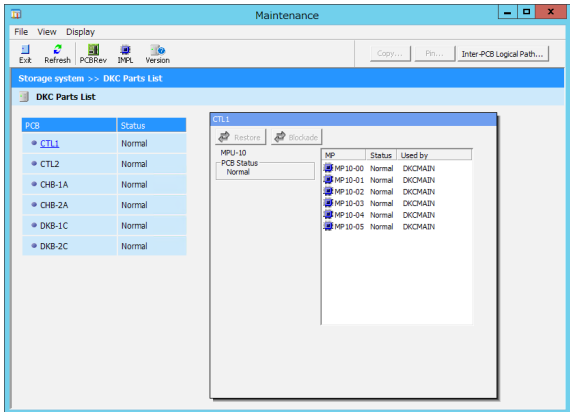
Click the [OK] button for the following message.

"[2415] Restore finished."



10. <Check of processing result >

Check the status of the target PCB with detailed view in the “Maintenance” window.



11. <Post-processing>

Close the “Maintenance” window.

Change the mode to [View Mode].

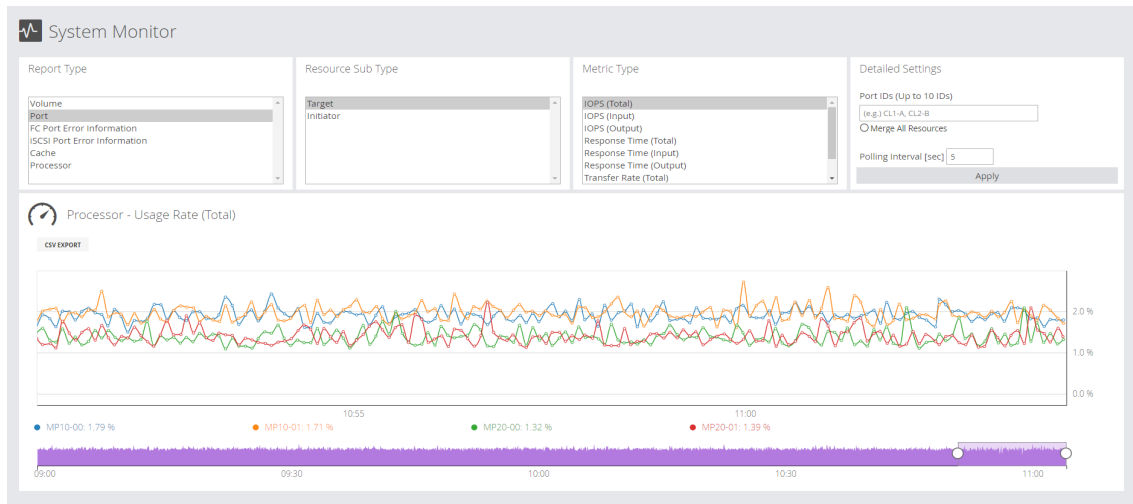
5.12.8 Error or Failure Status Action

When an error status of, Warning, Failure, or other is displayed on the screen and any action is required, locate the part in error and follow the instructions according to the action code (ACC). The ACC can be obtained by executing the SSB log or the SIM log displayed function of the Maintenance PC.

6. Monitoring

When performing the monitoring, connect the Maintenance PC by following the procedure in [“2.2 Connecting Maintenance PC to Storage System”](#).

< Description of data selection dialog >



■ Report Type

Select the object whose data you want to display.

The selection items include “Volume”, “Port”, “FC Port Error Information”, “iSCSI Port Error Information”, “Cache”, and “Processor”.

■ Resource Sub Type

Displayed when “Port” is selected for “Report”.

The selection items include “Target” and “Initiator”.

■ Metric Type

Select the more detailed items of the data to be displayed.

For “FC Port Error Information”, “iSCSI Port Error Information”, “Cache”, and “Processor”, multiple items can be selected.

■ Detailed Settings

Specify the object value to be monitored and set the polling interval (sec.).

To start the monitoring, select the [Apply] button.

■ Graph Display

The time series data of the items selected for “Report”, “Metric”, and so on, is displayed in the graph.

The display interval is specified in “Advanced setting”. The graph displays the data for 20 minutes.

The graph for the last 2 hours can be displayed.

■ Data Acquisition

Clicking the [CSV EXPORT] button downloads the data being monitored in the csv file format.

NOTE: In the string that indicates the performance value in the CSV file exported under the conditions shown below, “-1” is displayed.

- Report: Volume
- Metric: Read Hit Rate
- Volume ID: Any volume ID on which no I/O load is imposed

■ List of Displayed Data Items

Table 6-1 List of Displayed Data Items

#	Report Type	Resource Sub Type	Metric Type	Unit	Detailed Settings
1	Volume	—	IOPS	IOPS	Volume ID, Polling Interval
2			Response Time	ms	Volume ID, Polling Interval
3			Transfer Rate	MiB/sec	Volume ID, Polling Interval
4			Read Hit Rate	%	Volume ID, Polling Interval
5	Port	Target	IOPS (Total)	IOPS	Port ID, Polling Interval
6			IOPS (Input)	IOPS	Port ID, Polling Interval
7			IOPS (Output)	IOPS	Port ID, Polling Interval
8			Response Time (Total)	ms	Port ID, Polling Interval
9			Response Time (Input)	ms	Port ID, Polling Interval
10			Response Time (Output)	ms	Port ID, Polling Interval
11			Transfer Rate (Total)	MiB/sec	Port ID, Polling Interval
12			Transfer Rate (Input)	MiB/sec	Port ID, Polling Interval
13			Transfer Rate (Output)	MiB/sec	Port ID, Polling Interval
14		Initiator	IOPS (Total)	IOPS	Port ID, Polling Interval
15			IOPS (Input)	IOPS	Port ID, Polling Interval
16			IOPS (Output)	IOPS	Port ID, Polling Interval
17			Response Time (Total)	ms	Port ID, Polling Interval
18			Response Time (Input)	ms	Port ID, Polling Interval
19			Response Time (Output)	ms	Port ID, Polling Interval
20			Transfer Rate (Total)	MiB/sec	Port ID, Polling Interval
21			Transfer Rate (Input)	MiB/sec	Port ID, Polling Interval
22			Transfer Rate (Output)	MiB/sec	Port ID, Polling Interval

(To be continued)

(Continued from the preceding page)

#	Report Type	Resource Sub Type	Metric Type	Unit	Detailed Settings
25	FC Port Error Information	—	Loss of Signal Count	count	Port ID, Polling Interval
26			Bad Received Character Count	count	Port ID, Polling Interval
27			Loss of Synchronization Count	count	Port ID, Polling Interval
28			Link Failure Count	count	Port ID, Polling Interval
29			Received EOFa Count	count	Port ID, Polling Interval
30			Discarded Frame Count	count	Port ID, Polling Interval
31			Bad CRC Count	count	Port ID, Polling Interval
32			Protocol Error Count	count	Port ID, Polling Interval
33			Expired Frame Count	count	Port ID, Polling Interval
34			Forward Error Correction Count	count	Port ID, Polling Interval
35	iSCSI Port Error Information	—	MAC CRC Error Count	count	Port ID, Polling Interval
36			IP Error Packet Count	count	Port ID, Polling Interval
37			IPv6 Error Packet Count	count	Port ID, Polling Interval
38			TCP Retransmit Timer Expired Count	count	Port ID, Polling Interval
39			iSCSI Header Digest Error Count	count	Port ID, Polling Interval
40			iSCSI Data Digest Error Count	count	Port ID, Polling Interval
41	Cache	—	Usage Rage	%	MPU ID/CLPR ID Polling Interval
42			Write Pending Rate	%	MPU ID/CLPR ID Polling Interval
43	Processor	—	Usage Rate (Total)	%	MP ID, Polling Interval
44			Usage Rate (Open Target)	%	MP ID, Polling Interval
45			Usage Rate (Open Initiator)	%	MP ID, Polling Interval
46			Usage Rate (External Initiator)	%	MP ID, Polling Interval
47			Usage Rate (Back-End)	%	MP ID, Polling Interval
48			Usage Rate (System)	%	MP ID, Polling Interval

Table 6-2 Specification Procedure for Advanced Setting

#	Detailed Settings	Specification procedure
1	Polling Interval	Specify the interval to acquire the performance information in decimal notation between 5.0 and 360 0 seconds.
2	Volume ID	Specify the target volume IDs in decimal notation. When specifying multiple volume IDs, separate each ID with “,”. Up to ten volume IDs can be specified. (*1)
3	Port ID	Specify the target port IDs (CLx-y: Enter a numerical number in “x” and a capital letter in “y.”) When specifying multiple port IDs, separate each ID with “,”. Up to ten port IDs can be specified. (*1) If [Merge all resources] is selected, the sum of the information of all ports on both controllers is displayed.
4	MPU ID / CLPR ID	Specify the target MPU ID (10 or 20) before “/” and the target CLPR ID (number between 0 and 31) after “/”. When specifying multiple IDs, separate each ID with “,”. Up to ten IDs can be specified. (*1) If [Merge all resources] is selected, the sum of the information of all MPUs / CLPRs on both controllers is displayed.
5	MP ID	Specify the target MP ID (xx-yy: Enter a two-digit number in each of “xx” and “yy”). When specifying multiple MP IDs, separate each ID with “,”. Up to ten MP IDs can be specified. (*1) If [Merge all resources] is selected, the sum of the information of all MPs on both controllers is displayed.

*1: However, you cannot specify multiple IDs when you select multiple items for the Metric Type.

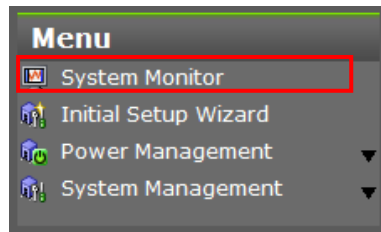
The following is the procedure for starting the “System Monitor” window from Maintenance Utility.

1. Starting Maintenance Utility.

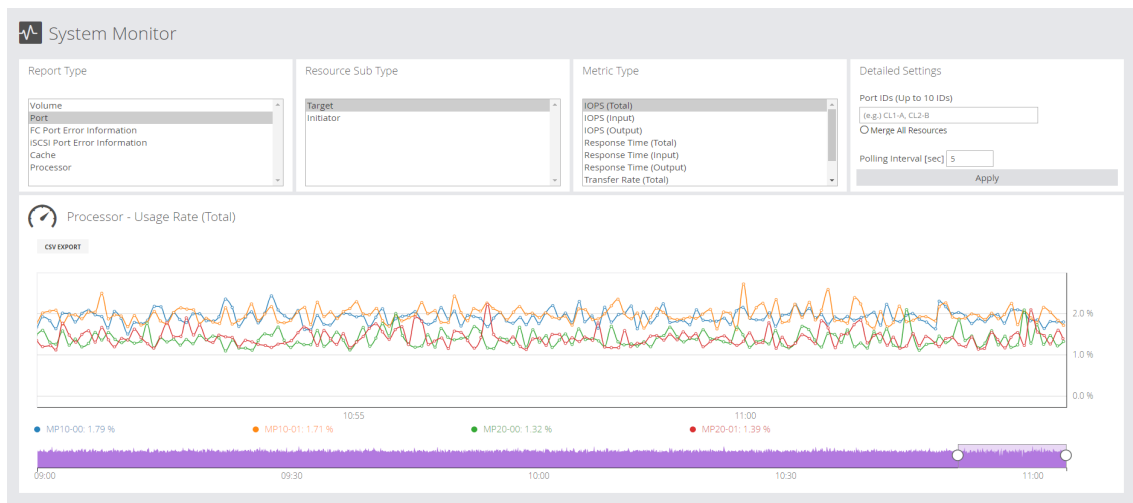
See “2.7 Starting the Maintenance Utility Window” to start Maintenance Utility.

2. Operation menu panel.

From [Menu], select [System Monitor] to display the “System Monitor” window.



3. “The “System Monitor” window appears.



NOTE: Do not close Maintenance Utility after starting the “System Monitor” window.

4. Selecting the items to be displayed.

(1) Setting the data to be displayed

Select the target object whose data you want to display.

The [Resource Sub Type] list or the [Metric Type] list is displayed according to the item selected for [Report Type]. For the detailed contents, see [Table 6-1](#).

(2) Detailed Settings and polling interval

Specify the object value to be monitored and set the polling interval (sec.).

For details, see [Table 6-2](#).

After selecting all the items that you want to display, click the [Apply] button.

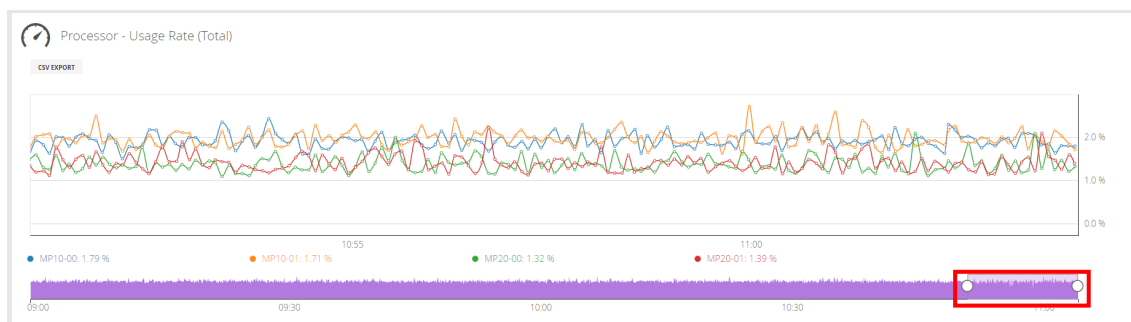
NOTE: If the settings are not correct, the [Apply] button is disabled.

5. Data display window.

The data display window is updated in the conditions set out in “[4. Selecting the items to be displayed.](#)”, where the target data is set in [Step \(1\)](#). and the object values and the polling interval (sec.) are specified in [Step \(2\)](#).

NOTE: When the load on the API server is high, plot points might be lost in the graph displayed in the “System Monitor” window.

- The graph display for 20 minutes in the upper part
The graph is displayed in the colors specified in “Detailed Settings”.
- The graph display for the last 2 hours in the lower part
Drag the slider (squared in red in the figure below) to the left and to the right to choose a display period of the upper graph.



NOTE: If the Storage System is undergoing the following maintenance operations or CHK1A, CHK1B and CHK3 occurs, the monitoring data might contain extremely large values.

- Adding on, replacing, or removing cache memories.
- Adding on, replacing, or removing disk drives.
- Replacing the CTL.
- Changing the system configuration.
- Update Firmware.
- Formatting LDEVs (including Quick Format).
- PS OFF/ON

6. Exiting the “System Monitor” window

From the browser menu, select [File (F)], and then [Exit (X)].

NOTE: Exiting the “System Monitor” window clears the graph of the monitored data.

7. Installing the Maintenance PC Tool

This is a tool to hand the dump files collected at the time of the maintenance part replacement to the Part Repair Division.

- Tool to Use: OnlineDumpTool

7.1 Use of OnlineDumpTool

[Conditions to run the tool]

OS : Windows® 7, Windows® 8.1, Windows® 10

Browser : Microsoft® Internet Explorer® Version 11 or later

This browser supports only the Internet Explorer of the latest version operating in each OS in accordance with the Microsoft support policy.

7.1.1 Installation

[1] Pre-check

Please check if a PC to be installed can access to Internet using a browser, Internet Explorer®.

[2] Installation of tool

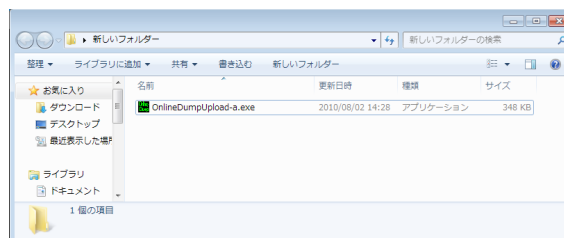
Please create a folder where you wish in your PC to be installed, and copy the following file:

OnlineDumpUpload-a.exe

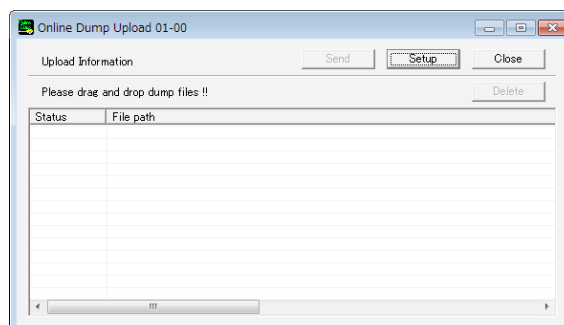
“-a” stands for a version of the tool (a to z)

[3] Settings

1. Double-click “OnlineDumpUpload-a.exe”.

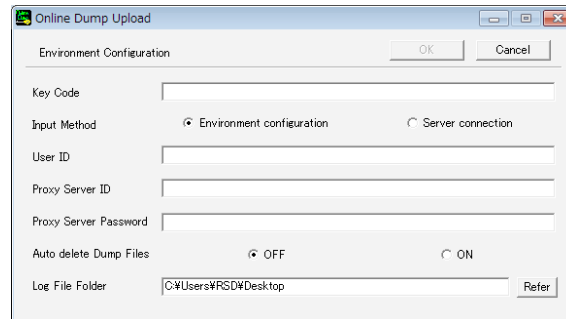


2. The “Upload Information” window is displayed, and then click the [Setup] button.



3.

The “Environment Configuration” window is displayed, and then set the following values: “Key Code”, “Input Method”, “User ID”, “Proxy Server ID”, “Proxy Server Password”, “Auto Delete Dump Files”, and “Log File Folder”.



(1) Key Code

Input a “Key Code” informed by an administrator.

(2) Input Method

Select whether the “User ID”, “Proxy Server ID” and “Proxy Server Password” are set on the tool in advance, or input the values at each uploading of dump file(s).

You can select from the following methods to set “User ID”, “Proxy Server ID” and “Proxy Server Password”: pre-setting in the tool or

Environment configuration Set the values on the tool in advance.

“User ID”, “Proxy Server ID” and “Proxy Server Password” are pre-set in the tool. Upon upload operation, you do not need to input these values. Please select this input method normally.

Server connection..... Input the values at each uploading of dump file(s).

Upon every upload operation, you need to input “User ID”, “Proxy Server ID” and “Proxy Server Password”. If you wish to share a CE Laptop PC with someone else and keep these values secret, please select this input method.

(3) User ID

Input a User ID informed by an administrator.

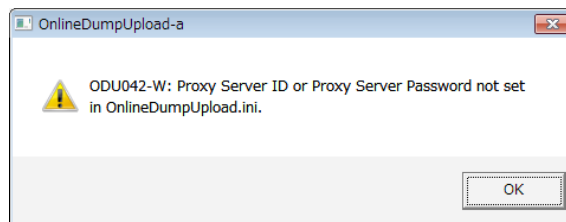
Do not input User ID when the Server connection is selected in the [Step \(2\)](#).

(4) Proxy Server ID/Proxy Server Password

If there is a Proxy Server in your network environment for which the CE Laptop PC uploads a dump, input an ID and password of Proxy Server.

Case#	Network environment			Setting			
	Proxy Server Exist/ None Exist	Proxy Server password Exist/ None Exist	How to check	Input Method setting			
				Environment configuration		Server connection	
				Proxy Server ID	Proxy Server Password	Proxy Server ID	Proxy Server Password
Case 1	Exist	Exist	If you input ID and password when accessing to Internet using a browser (Internet Explorer®), then your network environment is Case 1.	Input Proxy Server ID.	Input Proxy Server password.	No setting necessary	
Case 2	Exist	None Exist	If the following conditions are true, then your network environment is Case 2: - Your network environment is not Case 1. - The Window [a] is displayed when clicking the [OK] button (Step 4) while leaving the "Proxy Server ID" and "Proxy Server Password" fields blank.	No setting necessary	No setting necessary		
Case 3	None Exist	None Exist	If the following conditions are true, then your network environment is Case 3: - Your network environment is not Case 1. - The Window [a] is not displayed when clicking the [OK] button (Step 4) while leaving the "Proxy Server ID" and "Proxy Server Password" fields blank.	No setting necessary	No setting necessary		

Window [a]



(5) Auto Delete Dump Files

If "Auto Delete Dump Files" is ON, after upload completes, an original file uploaded will be automatically erased.

OFF : not automatically erased

ON : automatically erased

(6) Log File Folder

A location of a folder in which history files are stored is specified here.

4.

Online Dump Upload

Environment Configuration

OK Cancel

Key Code

Input Method ☒ Environment configuration ☐ Server connection

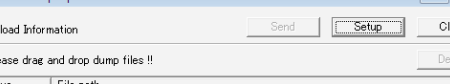
User ID

Proxy Server ID

Proxy Server Password

Auto delete Dump Files ☒ OFF ☐ ON

Log File Folder Refer



Online Dump Upload 01-00

Send Setup Close

Please drag and drop dump files !! Delete

Status	File path
--------	-----------

The screenshot shows a Windows Explorer window with the title bar '新しいフォルダー' (New Folder). The address bar also displays '新しいフォルダーの検索' (Search New Folder). The left sidebar shows the 'ライブラリに追加' (Add to Library) button and the '新しいフォルダー' (New Folder) button. The main pane displays a list of files with columns for '名前' (Name), '更新日時' (Last Modified), and '種類' (Type). The files listed are:

名前	更新日時	種類
OnlineDumpUpload.ini	2010/08/02 19:52	構成設定
OnlineDumpUpload-s.exe	2010/08/02 10:32	アプリケーション
OnlineDumpUpload-s.log	2010/08/02 19:54	テキストドキュメント

The 'OnlineDumpUpload-s.exe' file is selected, and its icon is highlighted. The status bar at the bottom indicates '3 個の項目' (3 items).

7.1.2 Uninstallation

When you uninstall the tool, please delete the following files:

OnlineDumpUpload-a.exe

OnlineDumpTool.ini

OnlineDumpUpload-a.log (property: hidden file)

Up-loadingResult.log (property: hidden file)

Up-loadingResult_YYMMDD-nn.txt

(YY: year, MM: month, DD: date, -nn: automatically-assigned sequential number)

7.1.3 Upload Procedure

There are two different procedures for uploading.

Both of the uploading procedures are the same except for the way of starting the tool.

Choose either of uploading procedure depending on their features.

Upload a dump file by dragging and dropping it onto the OnlineDumpTool.	
Feature	Easy operation that uploads dump file(s) by one click operation.
Procedure	From 1-(1) to 1-(3).

Execute uploading by running OnlineDumpTool.	
Feature	Uploading all dump files at once after confirming the file names.
Procedure	From 2-(1) to 2-(6).

1. The procedure for uploading dump files onto the OnlineDumpTool by dragging and dropping.

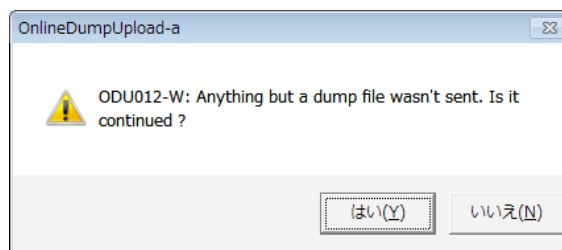
(1)

Drag and drop a dump file you wish to upload onto the OnlineDumpUpload-a.exe icon.



NOTE:

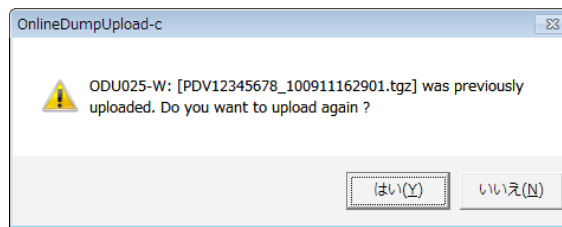
- Multiple files can be uploaded at a time.
- Any files except for a dump file cannot be uploaded.
If you select other files, the following window is displayed.



[Yes]: Execute uploading except for the file which was not sent, if multiple files are selected.

[No]: Stop uploading.

- If the same file is re-sent, the following confirmation message is displayed.



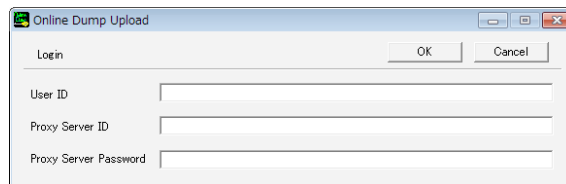
[Yes]: Uploading is executed.

[No]: Uploading is canceled.

(2)

When selecting the “Server connection” in the field of “Input Method” in the setting of [MPC07-20 Step \(2\)](#), the following “Login” window is displayed.

(The window is not displayed when the “Environment configuration” is selected. Go to [Step \(3\)](#).)



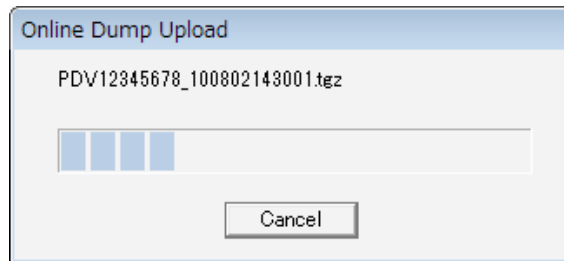
Input “User ID”, “Proxy Server ID”, “Proxy Server Password”, and click the [OK] button.

Refer to [MPC07-30 Step \(4\)](#) for the input value of “Proxy Server ID” and “Proxy Server Password”.

(3)

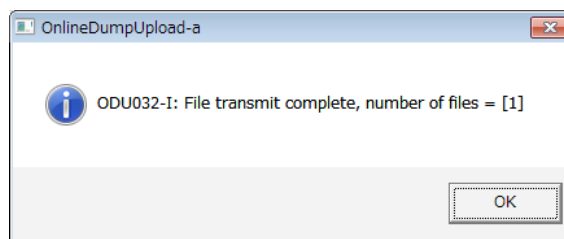
Start uploading

During uploading, the following window is displayed.



When all selected files are uploaded, the following window is displayed.

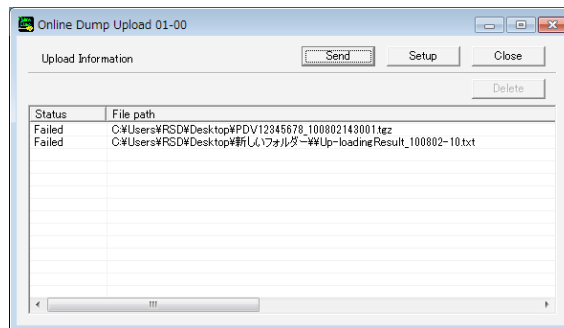
Click the [OK] button.



If there is/are file(s) failed to upload in selected files, the following window is displayed.

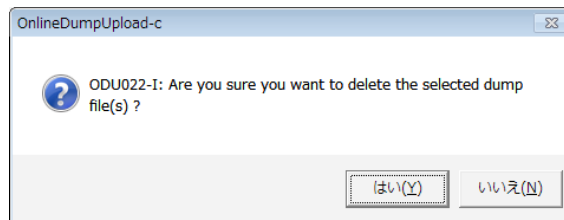
If you wish to retry uploading, click the [Send] button.

If you wish to exit without retry, click the [Close] button.

If you set “Auto Delete Dump Files” to ON, in the setting of [MPC07-30 Step \(5\)](#), the following window is displayed.

If you wish to delete the original dump file uploaded, click the [Yes] button. (*1)

If you do not wish to delete the original dump file uploaded, click the [No] button.

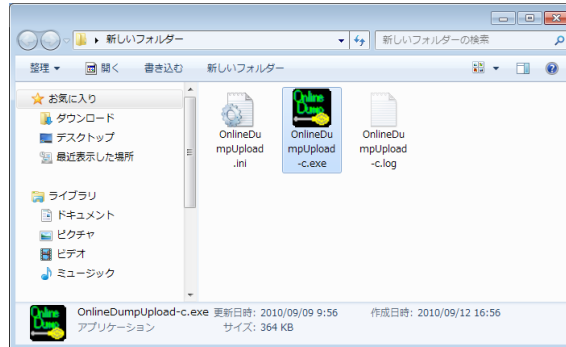


*1: The deleted file is sent to the recycle bin.

2. The procedure for uploading dump files by running the OnlineDumpTool.

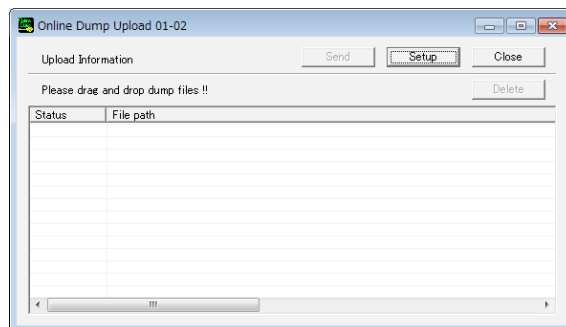
(1)

Double-click the OnlinedumpUpload-a.exe icon.

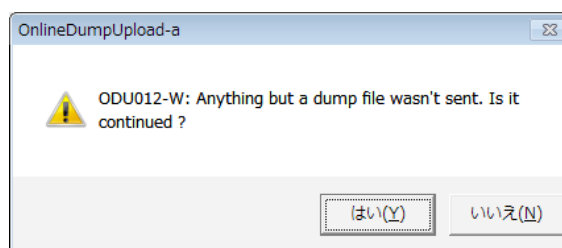


(2)

Drag and drop the dump file onto the “Online Dump Upload” window to upload.



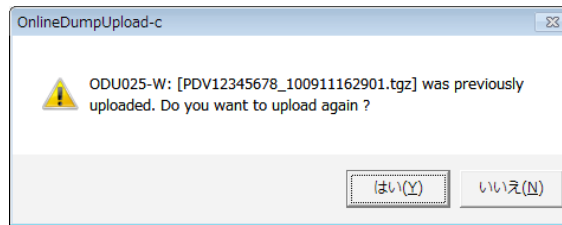
- NOTE:
- Multiple files can be uploaded at a time.
 - Uploading files can be added.
 - Any files except for a dump file cannot be uploaded.
If you select other files, then the following window is displayed.



[Yes]: Execute uploading except for the file which was not sent, if multiple files are selected.

[No]: Stop uploading.

- When the uploading has completed, the reconfirmation message is displayed.



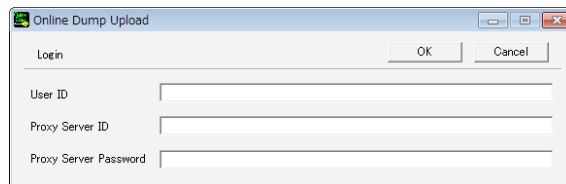
[Yes]: Uploading is executed.

[No]: Uploading is canceled.

(3)

When selecting the “Server connection” in the field of “Input Method” in the setting of [MPC07-20 Step \(2\)](#), the following “Login” window is displayed.

(The window is not displayed when the “Environment configuration” is selected. Go to [Step \(4\)](#).)

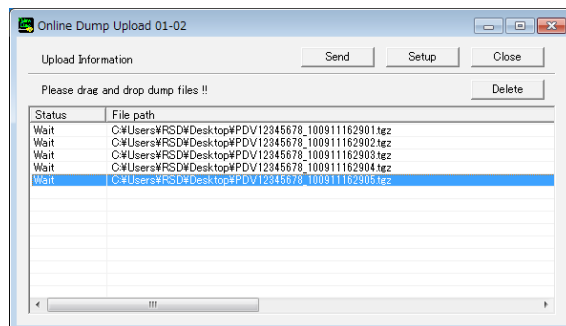


Input “User ID”, “Proxy Server ID”, “Proxy Server Password”, and click the [OK] button.

Refer to [MPC07-30 Step \(4\)](#) for the input value of “Proxy Server ID” and “Proxy Server Password”.

(4)

Click the [Send] button to start uploading.

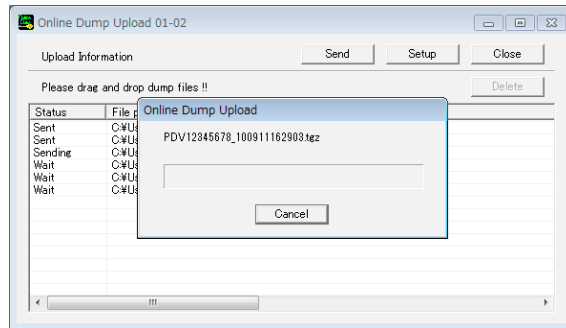


- NOTE:
- Select a file and [Delete] to delete the selected file from the list.
 - Click the [Close] button to close the window without uploading.

(5)

The uploading window is displayed.

The uploading status is displayed in the Status field during uploading.



Connecting: In the connecting process to the server.

Sending: Uploading.

Sent: Uploaded. (completed)

Wait: Waiting to start uploading.

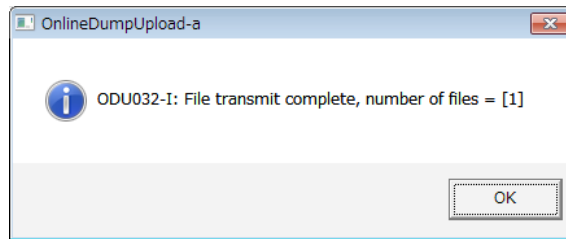
Failed: The uploading has failed.

Cancel: The uploading has canceled.

(6)

When all selected files are uploaded, the following window is displayed.

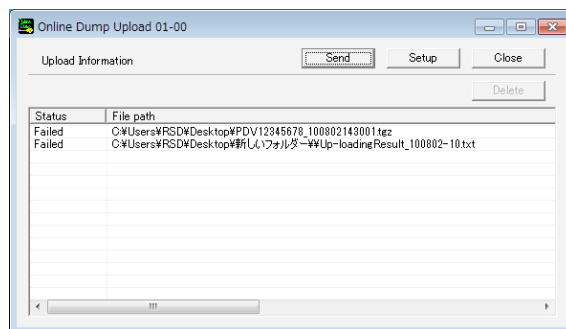
Click the [OK] button.



If there is/are file(s) failed to upload in selected files, the following window is displayed.

If you wish to retry uploading, click the [Send] button.

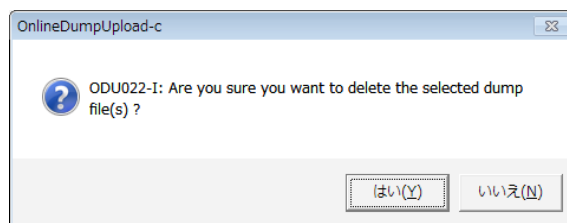
If you wish to exit without retry, click the [Close] button.



If you set “Auto Delete Dump Files” to ON, before a window showing upload completed is displayed, the following window is displayed.

If you wish to delete the original dump file uploaded, click the [Yes] button. (*1)

If you do not wish to delete the original dump file uploaded, click the [No] button.



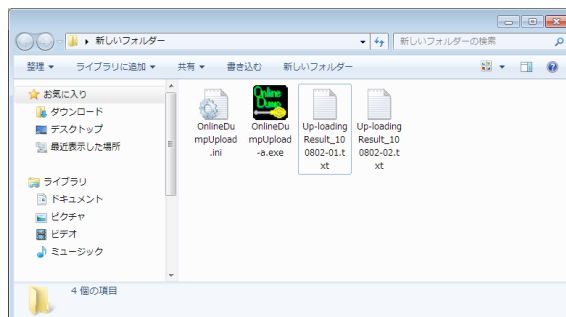
*1: The deleted file is sent to the recycle bin.

7.1.4 Reference of Uploaded Results

History information of an uploaded file is stored in a txt file.

A folder location is the same folder as specified in [MPC07-10 \[3\] Settings](#).

A history file is created every transmission.



7.1.5 Message Table

The messages that are displayed on OnlineDumpTool are described below [Table 7-1](#).

Table 7-1 Displayed Messages on OnlineDumpTool

Code No.	Items	Contents
ODU004-E	Message	ODU004-E: Login error, URL = [Address1 ~ 4] detail = *1 *1: detail = Check Your ID or Password = Proxy Authentication Required = Multi login = The server name or address could not be resolved = Not expectation HTML = The operation timed out
	Action	detail = Check the key cord when the “Check Your ID or Password” message is displayed. detail = Check the user ID and password of the Proxy server when the “Proxy Authentication Required” message is displayed. detail = Login again after a while when the “Multi login” or “The operation timed out” (There is no response from the Web server.) message is displayed. For other than the above, setup the OnlineDumpTool again.
ODU010-E	Message	ODU010-E: Cannot read OnlineDumpUpload.ini, path = [file path name].
	Cause	The OnlineDumpUpload.ini cannot be read.
	Action	(1) Check whether the OnlineDumpUpload.ini file can be read. (2) Setup the OnlineDumpTool again.
ODU011-W	Message	ODU011-W: Key code or user id not set in OnlineDumpUpload.ini.
	Cause	The key code and user ID are not specified to the OnlineDumpUpload.ini.
	Action	Specify the key code and user ID on Environment configuration screen.
ODU012-W	Message	ODU012-W: Anything but a dump file wasn't sent. Is it continued?
	Cause	The file that cannot be transmitted is included.
	Action	Select [OK] to continue and [Cancel] to discontinue. When [OK] is selected, only the transmittable file is transmitted.
ODU015-E	Message	ODU015-E: Internet API exception happened, detail = [error detail].
	Cause	An unexpected error is detected at HTTP Communication API.
	Action	Setup the OnlineDumpTool again.
ODU022-I	Message	ODU022-I: Are you sure you want to delete the selected dump file(s)?
	Cause	“Auto delete Dump Files” setting is set to [On].
	Action	Select [Yes] to delete the files and [No] to cancel it.

(To be continued)

(Continued from the preceding page)

Code No.	Items	Contents
ODU023-E	Message	ODU023-E: A value was specified incorrectly, detail = [cause of error].
	Cause	The error is detected in the specified value.
	Action	(1) When the detail is "The smallest number of characters"; <ul style="list-style-type: none"> Specify the string of five characters or more for the account and the key code. Specify the string of one character or more for the user ID. No spaces allowed. (2) When the detail is "Prohibited character"; Use the alphanumeric characters. (3) When the detail is "Prohibited character string"; Use the string other than below. script, meta, table, body, frame, form, style, background, xmp applet, plaintext, cookie
ODU025-W	Message	ODU025-W: [dump-filename-.tgz] was previously uploaded. Do you want to upload again?
	Cause	The file is an uploaded dump file.
	Action	Select [OK] to upload the files and [Cancel] to cancel it.
ODU026-E	Message	ODU026-E: Cannot write OnlineDumpUpload.ini, section = [section name] key = [key code] value = [value] path = [file path].
	Cause	The OnlineDumpUpload.ini is not able to write.
	Action	(1) Check if the OnlineDumpUpload.ini file exists. (2) Setup the OnlineDumpTool again.
ODU028-W	Message	ODU028-W: Web server was busy. Please execute after wait a moment.
	Cause	The Web server was busy.
	Action	Execute it again after a while.
ODU032-I	Message	ODU032-I: File transmit complete, number of files = [Number of transmitted files]
	Cause	The file transfer is completed.
	Action	None
ODU037-W	Message	ODU037-W: This tool cannot be executed concurrently.
	Cause	This tool has already been running.
	Action	Finish this tool, and operate it with the running tool.
ODU038-W	Message	ODU038-W: Please set Address or Account, detail = [%s].
	Cause	The address or account is not set.
	Action	Setup the OnlineDumpTool again.

(To be continued)

(Continued from the preceding page)

Code No.	Items	Contents
ODU042-W	Message	ODU042-W: Proxy Server ID or Proxy Server Password not set in OnlineDumpUpload.ini.
	Cause	Although the setting of the Proxy Server is "On" in the IE, the Proxy Server ID and the Proxy Server Password are not specified to OnlineDumpUpload.ini.
	Action	Specify the Proxy Server ID and the Proxy Server Password on the Environment configuration screen.
ODU044-W	Message	ODU044-W: Log file folder was not exist, folder = [folder name].
	Cause	The folder that does not exist in the Log file folder was specified.
	Action	Check the folder that is specified for Log file folder. If it does not exist, specify Log file folder again on the Environment configuration screen.
ODU045-W	Message	ODU045-W: The file was drag & drop already, file = [file name]
	Cause	The file has already been dragged and dropped.
	Action	None
ODU046-W	Message	ODU046-W: Exclusion of a file, file = [file name].
	Cause	The file has excluded from the upload screen.
	Action	None
ODU047-W	Message	ODU047-W: The cancel button was pressed.
	Cause	The process has canceled because the cancel button has pressed.
	Action	None
ODU048-W	Message	ODU048-W: A folder can't be sent. Is it continued?
	Cause	A folder can't be sent.
	Action	Select [OK] to continue the process, and [Cancel] to cancel it.

8. Maintenance PC Uninstallation

When the Maintenance PC is not used anymore, uninstallation is required.

Select a version to be uninstalled and uninstall it. (In case of multiple specification possible – all specified, delete the Base directory)

Delete the specified installation directory.

NOTICE: Follow the procedure in this manual when you want to uninstall the software of the Storage System.
 Never delete a folder (and a file) of the software of the Storage System by Windows Explorer directly.
 The information in the registry and the service process of Storage System will be remained even if you delete a folder (and a file) by Windows Explorer.
 The Registry and the service process become incongruous with the actual situation, and unexpected abnormality might be caused.
 Refer to the following procedures in TROUBLESHOOTING SECTION for recovery when you have deleted a folder (and a file) of the software of the Storage System by mistake.

- “3.29.2 When the “Set Network Location” dialog is displayed”
- “3.29.3 When the drive letter of the Maintenance PC is not displayed or is redundant”
- “3.29.4 When the installation folder of the Maintenance PC software (for example, C:\Mapp) is deleted by mistake”

NOTICE: Before uninstalling software from the Maintenance PC, close the Event Viewer of Windows.

8.1 OSS Uninstallation

Table 8-1 OSS Uninstallation

Item	Uninstallation work
JRE	Uninstall the software.
Perl	Follow the procedure of “8.2 Maintenance PC Software Uninstallation”.
Apache	Individual uninstallation is not required.
Jetty	
OpenSSL	
PuTTY	
JRE(Client)	When you don't use JRE(Client) in other than Maintenance PC, please uninstall JRE(Client). When JRE(Client) is uninstalled, It can be uninstalled from “Programs and Features” of “Programs” of “Control Panel”.
Flash	When you don't use Flash in other than Maintenance PC, please uninstall Flash. When uninstalling Flash Player, click “Control Panel”, “Programs”, and “Programs and Features”, and then uninstall the program. (When OS is Windows 10, uninstalling Flash Player is not necessary.)

8.2 Maintenance PC Software Uninstallation

Maintenance PC Software includes OSS.

Therefore, if you uninstall Maintenance PC Software, OSS is also uninstalled.

However, Flash does not need to be uninstalled, it remains on the program list. If you want to uninstall Flash, you need to correspond it individually.

NOTE: The operation method has different menu names depending on OS. The operation method of Windows7 is described here.

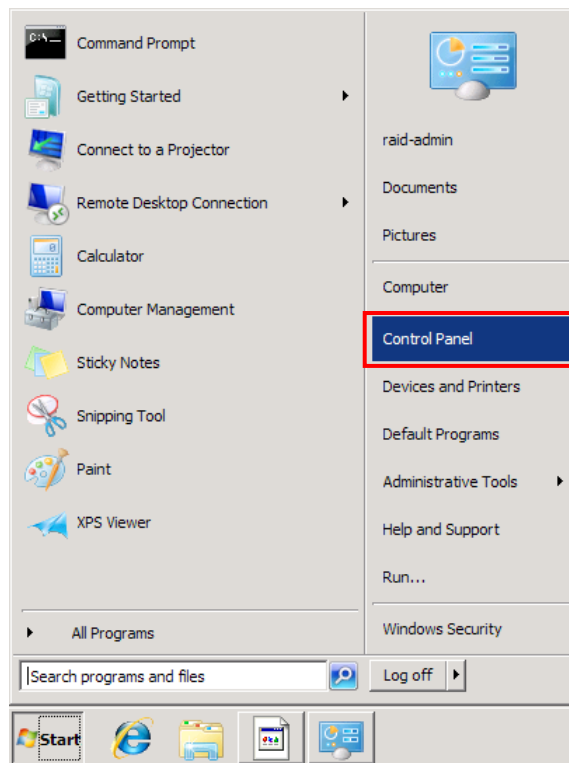
NOTICE: Gather Dumps of the system information before uninstallation.
Before removal, perform ["10.4 Initializing Automatically Allocated Port Numbers"](#).
After removal, delete the unnecessary firewall reception rules and regulations.

- Select [Control Panel] – [Windows firewall] – [Advanced settings] – [Inbound Rules] from the Windows start menu.

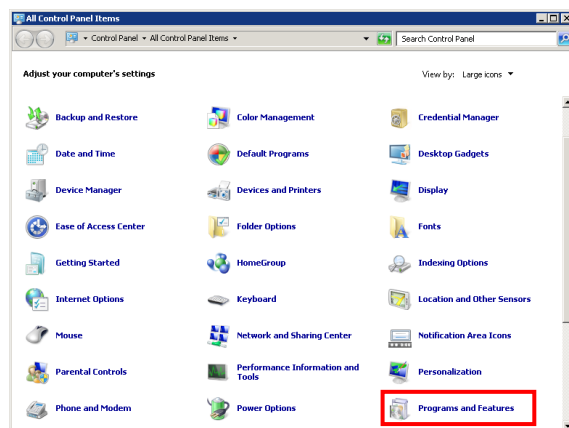
NOTICE:

- If Command Control Interface (CCI) is installed in a drive with a number different from the one assigned to the drive containing the MPC Software, the HORCM folder can be left directly under the drive with the MPC Software installed. Use Windows Explorer to remove it manually.
- If MPC Software is installed to another drive of CCI, HORCM folder of MPC Software drive will be remained after uninstalling MPC Software. Please delete manually HORCM folder.
- When CCI is manually installed in the drive with the same drive letter as assigned to the drive containing the MPC Software, the CCI is removed. Install CCI again.

1. Select [Start] - [Control Panel].



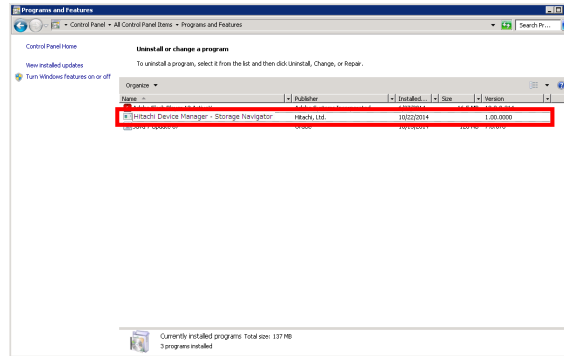
2. Click [Programs and Features].



3. Select [Hitachi Device Manager - Storage Navigator] and click [Uninstall].

If the UAC control window of Windows is displayed when executing the uninstallation, click the [Continue] button.

When [Hitachi Device Manager - Storage Navigator] is not on the list, go to [Step 8](#).

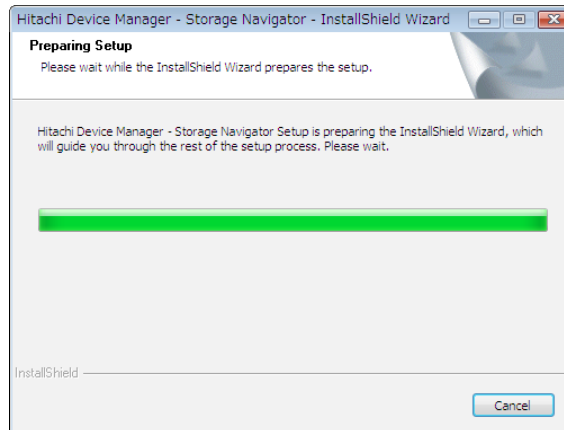


4. Preparing for uninstallation

When Command Control Interface (CCI) other than the one contained in the MPC Software media is not installed, a message is displayed for removing the CCI contained in the MPC Software media.

If a user script exists in the folder for CCI, move the file into a different folder, and then click [Yes].

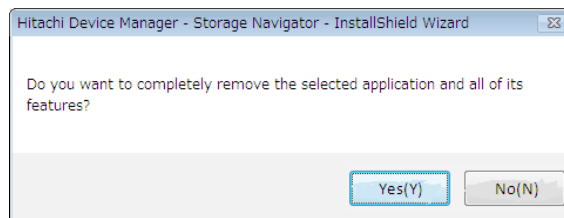
The preparing for uninstallation window is displayed. Wait until the preparation is completed.



5. Checking the deletion

The window for checking whether to delete the MPC Software completely is displayed.

Click the [Yes] button.



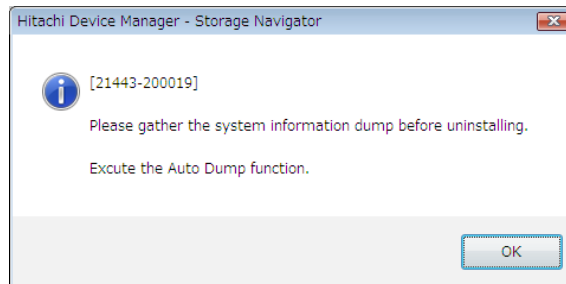
6. Checking Dump gathering

The Dump gathering check window of the system information is displayed.

If already gathered, click the [OK] button.

If not, gather Dumps, and then click the [OK] button.

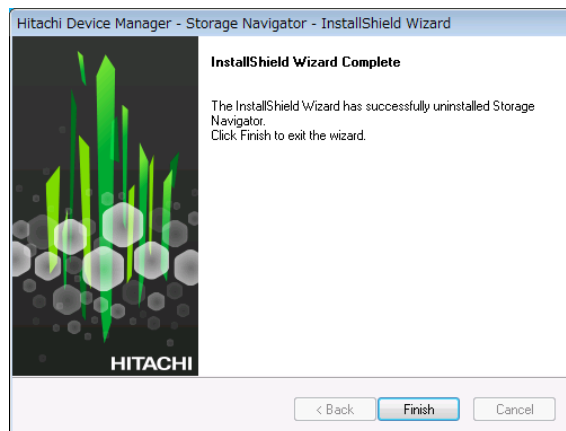
NOTE: If Dumps are not gathered, execute the Dump gathering, and then click the [OK] button.



7. Completion message

The uninstallation completion message is displayed.

Click the [Finish] button to close the window.



8. Checking the uninstallation result

Check that [Hitachi Device Manager - Storage Navigator] is deleted from [Programs and Functions].

Click the [X] button to close this window.

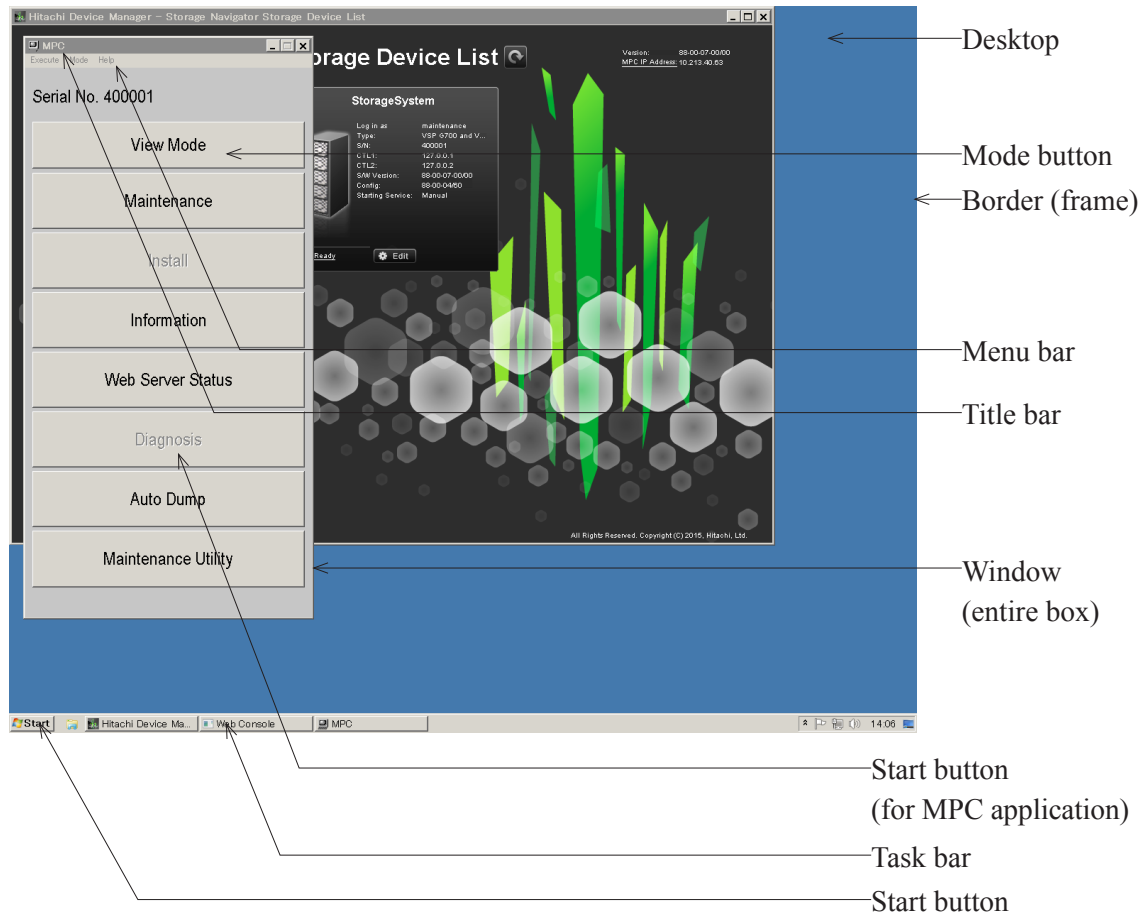
9. Description of Windows

9.1 Names of Elements of Windows (Maintenance PC)

Either of the following windows is displayed.

The “MPC” window shown on the left side can perform the maintenance functions of the Storage System.

The “Storage Device List” window shown in the center can start the “Web Console” window and the “MPC” window.



NOTE: Each Maintenance PC screen on this maintenance manual is a sample, and it may not be the same as the actual screen.

“WARNING LED Status”

9.2 WARNING LED Status Window

When WARNING LED (*1) on the controller chassis is blinked or lights when “MPC” window is displayed, the “WARNING LED Status” window is displayed on Windows (PC for maintenance).

The message shown in [Table 9-1](#) according to the lighting state of WARNING LED is displayed on a “WARNING LED Status” Window.

If WARNING LED is turned off, the “WARNING LED Status” window becomes non-display.

*1: Refer to “LOCATION SECTION ([LOC03-10](#))” for WARNING LED

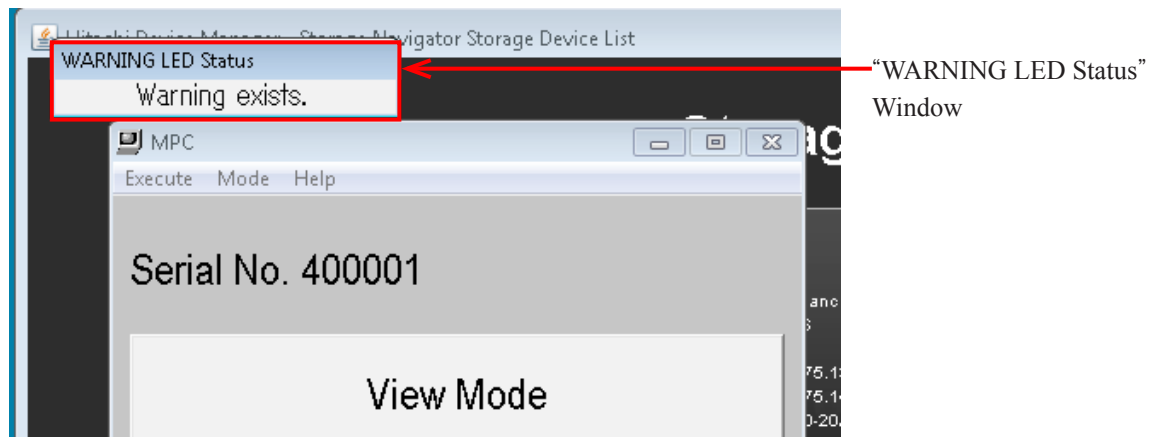


Table 9-1 WARNING LED state and display message

WARNING LED	Display message
Lighting	Warning exists.
Blinking	Unconfirmed SIM exists.

9.3 Maintenance Window

9.3.1 Main Window

NOTICE: When running the maintenance operation in the other window, the part status might be displayed differently from the actual status. (Example: The CHBs during the replacement are displayed as the [Normal] status.).
In that case, complete the maintenance operation running in the other window, and then refresh the display information by clicking the [Refresh] button.

The main window of the “Maintenance” window is configured as shown below.

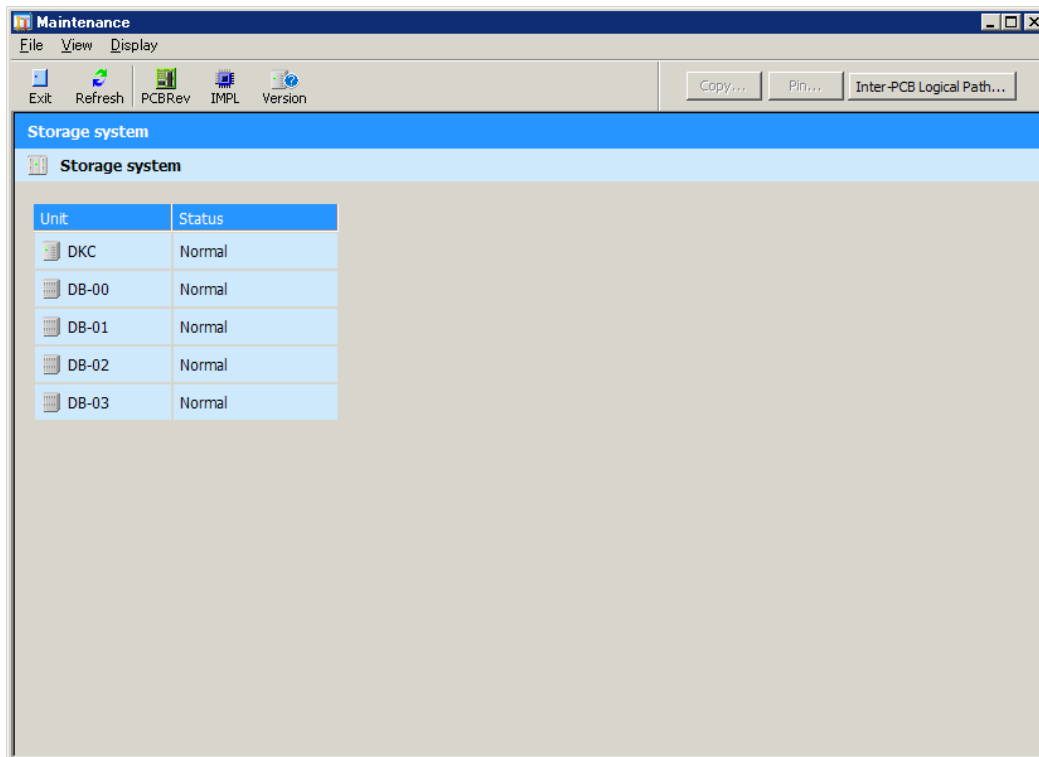







Table 9-2 Overview of Each Part in the Main Window

No.	Item	Description
1	Menu	Menu items that can be operated using this function
2	Tool bar	Consists of buttons for operating some of the functions in the menu.
3	Dialog bar	Displays logical statuses. You can check the detailed information by pressing a button.
4	Information view	Displays a status of each part.

9.3.2 Operation Menu

This menu displays the operation in the “Maintenance” window. Menu items are also placed in the tool bar.

Table 9-3 Menu/Tool Bar

Menu	Sub Menu	Description	Tool bar
File	Exit	The Maintenance window is finished.	 Exit
View	Toolbar	Displays/does not display the tool bar.	—
	Refresh	Updates information being displayed.	 Refresh
Display	PCB Revision...	Displays the “PCB Revision Display”.	 PCBRev
	IMPL Status...	Displays the “IMPL Status”.	 IMPL
	Version...	Displays the “Version”.	 Version

9.3.3 Dialog Bar

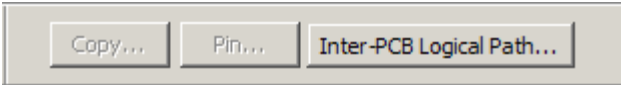


Table 9-4 Dialog Bar

Button	Detailed information displayed	Processing when pressed
Copy...	Status of copying Blinking of the button : Copying is in progress. Extinction of the button : No copying is done.	Displays “Copy Status”(MPC05-1050).
Pin...	Pin information Blinking of the button : Pin information is present. Extinction of the button : No Pin information is present.	Displays “Pinned Track”(MPC05-1170).
Inter-PCB Logical Path	Status of Inter-PCB Logical Path Steady lighting of the button : Normal Blinking of the button : Failed	Displays “Inter-PCB Logical Path Status”(MPC05-1210).

9.3.4 Information Display View

Display whether parts are installed/uninstalled, normal/abnormal and select/execute a maintenance target.

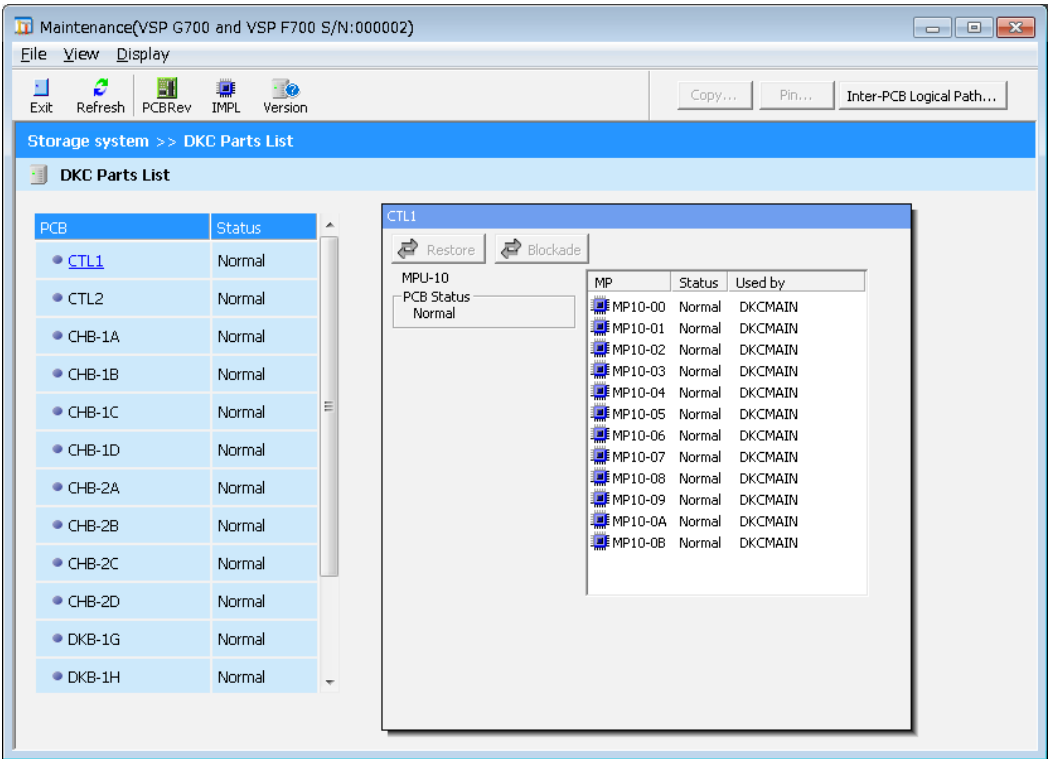


Table 9-5 Information Display View

Item	Description
Title	Display the title of the information view
Information view	Display a maintenance part list on the left side and detail information on the right side.
Maintenance button	Execute a maintenance function.

9.3.4.1 Storage System Information View

Display a list of the installed DKCs, DBs and CHBBs.

Display DKC-0 only in case a DKC communication error has occurred.

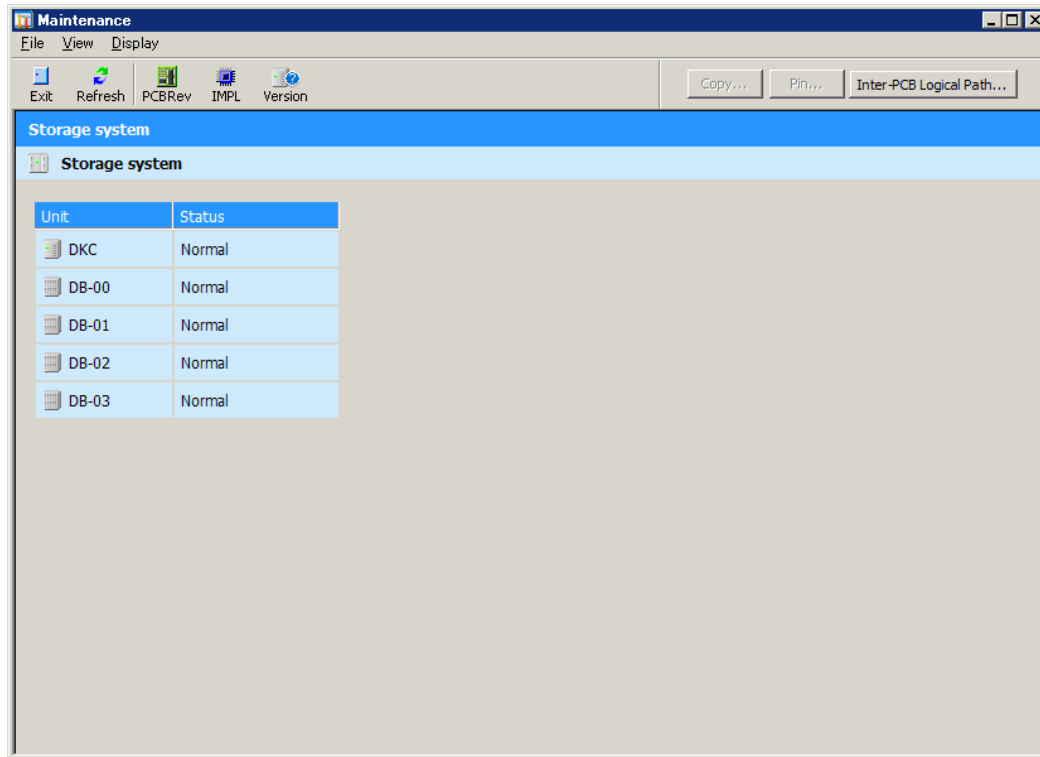


Table 9-6 Storage System Information View

Item	Description
Title	Display a "Storage System status".
Unit	Display a chassis type icon and a location name (DKC, DB, CHBB). : Installed : A failure has occurred Selecting a part displays the part list information.
Status	Display a status. Normal : Normal Warning : Mixed status Failed : Abnormal Blocked : Maintenance is blocked/to be blocked Unknown : The status is unknown (information acquisition fails)

9.3.4.2 DKC Information View

When selecting a DKC chassis from the Storage System information view, display a list of parts (CTL, CHB, DKB) installed in the relevant DKC.

When selecting a CHBB chassis from the Storage System information view, display a list of parts (CHB) installed in the relevant CHBB.

The detail view displays detail information of the parts selected from the list.

When selecting no part, the detail view is not displayed.

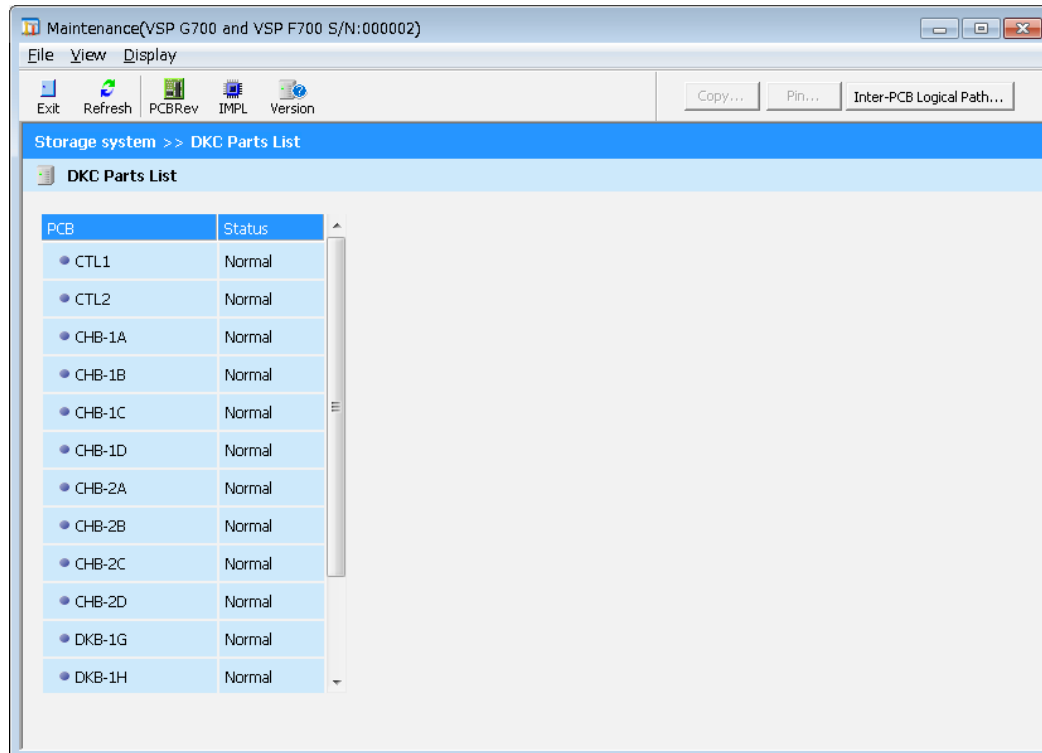




Table 9-7 DKC Information View

Item	Description
Title	Display a DKC location.
PCB	Display a PCB type icon and a location name (CTL, CHB, DKB).  : Installed  : A failure has occurred When selecting a PCB, display PCB information in the detail view.
Status	Display a status. Normal : Normal Warning : A failure has occurred Unknown : The status is unknown (information acquisition fails) --- : The status is out of display target
Detail view	Display detail information of the selected PCB. When selecting a CTL, see "(1) CTL view". When selecting a CHB/DKB, see "(2) CHB/DKB view".

(1) CTL view

Display the information view of the parts installed in the CTL and execute the maintenance function.

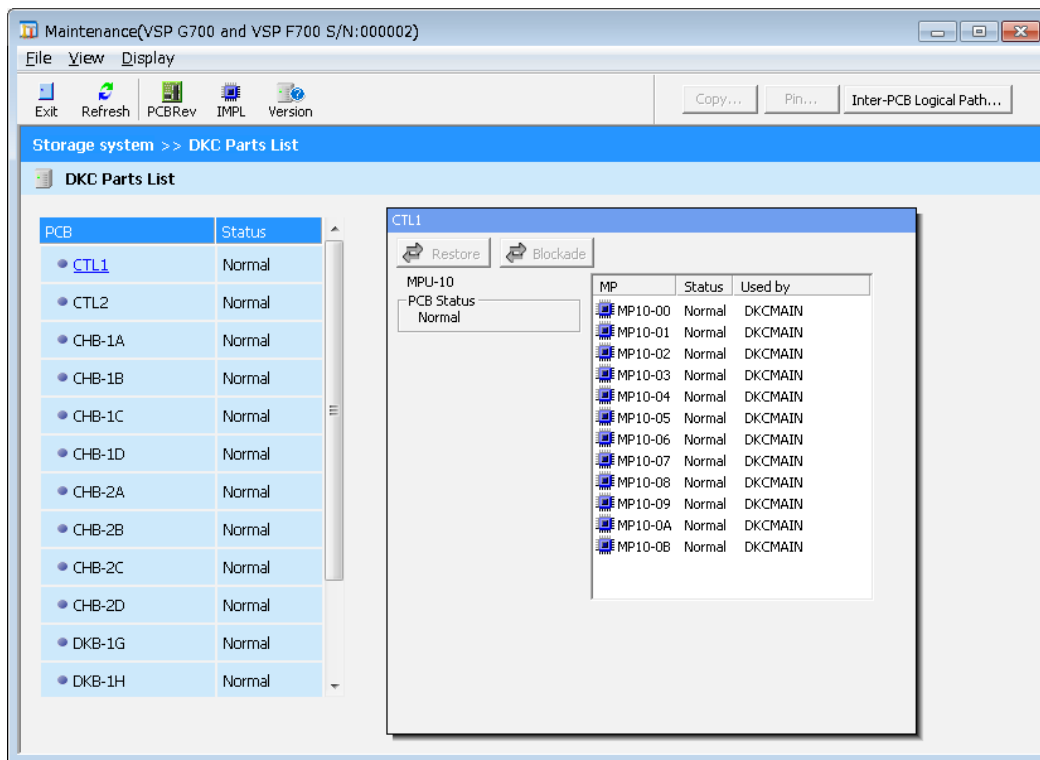











Table 9-8 CTL View

Item	Description							
Title	Display a CTL location.							
Maintenance button	<p>Execute maintenance processing.</p> <p>[Restore] : Execute a parts restore. (See “5.12.7 Failed CTL Recovery”.)</p> <p>Enable to operate when a CTL failure occurs.</p> <div><table><thead><tr><th>PCB</th><th>Status</th></tr></thead><tbody><tr><td> CTL1</td><td>Warning</td></tr></tbody></table><table><thead><tr><th>CTL1</th></tr></thead><tbody><tr><td> Restore  Blockade</td></tr><tr><td>MPU-10</td></tr></tbody></table></div>	PCB	Status	 CTL1	Warning	CTL1	 Restore  Blockade	MPU-10
PCB	Status							
 CTL1	Warning							
CTL1								
 Restore  Blockade								
MPU-10								
PCB status	<p>Display a PCB status.</p> <p>Normal : Normal</p> <p>Failed : Abnormal</p> <p>Blocked : Maintenance is blocked/to be blocked</p> <p>Warning : Mixed status</p>							
MPU location name	Display an MP location.							
MP list	<p>Display an MP status.</p> <p>Normal : Normal</p> <p>Failed : Abnormal</p> <p>Blocked : Maintenance is blocked/to be blocked</p>							

- (2) CHB/DKB view
- Display a CHB/DKB status and execute the maintenance operation.

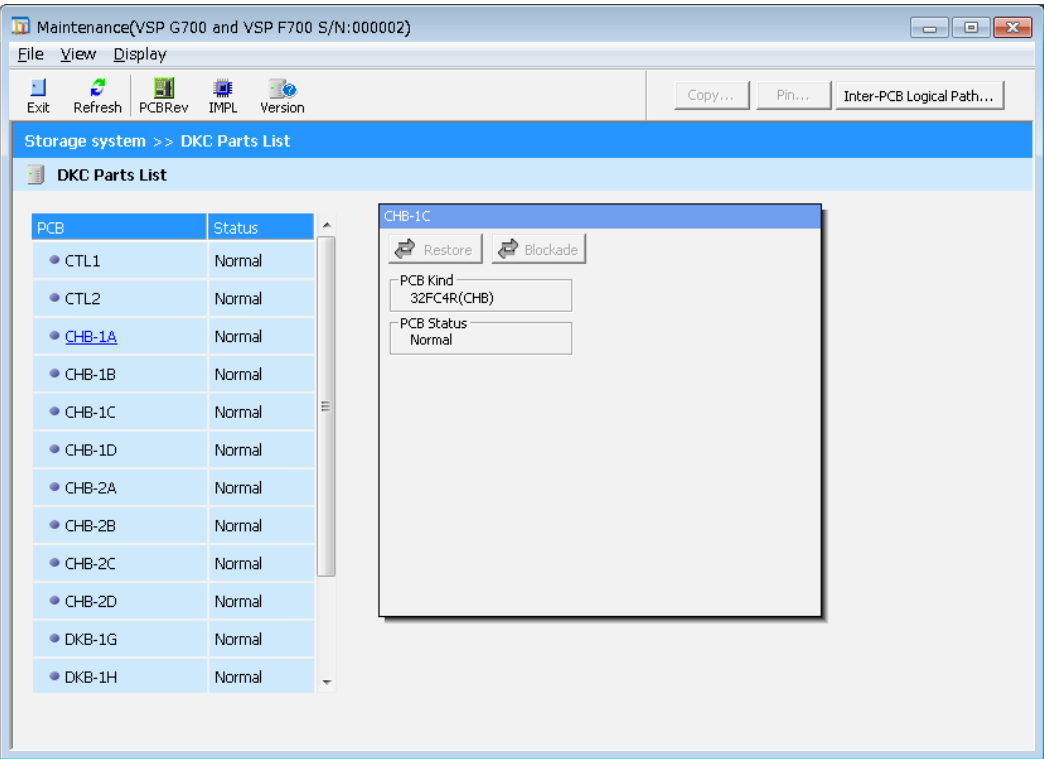


Table 9-9 CHB/DKB View

Item	Description
Title	Display a CHB/DKB location.
PCB type	Display a CHB/DKB package type
PCB status	Display a CHB/DKB status. Normal : Normal Failed : Abnormal Blocked : Maintenance is blocked/to be blocked Warning : Mixed status --- : The status is out of display target

9.3.4.3 HDD Information View

When selecting a DB chassis from the Storage System information view, display a list of HDDs installed in the relevant DB.

Display the detail information of the parts selected from the list in the detail view.

When selecting no part, the detail view is not displayed.

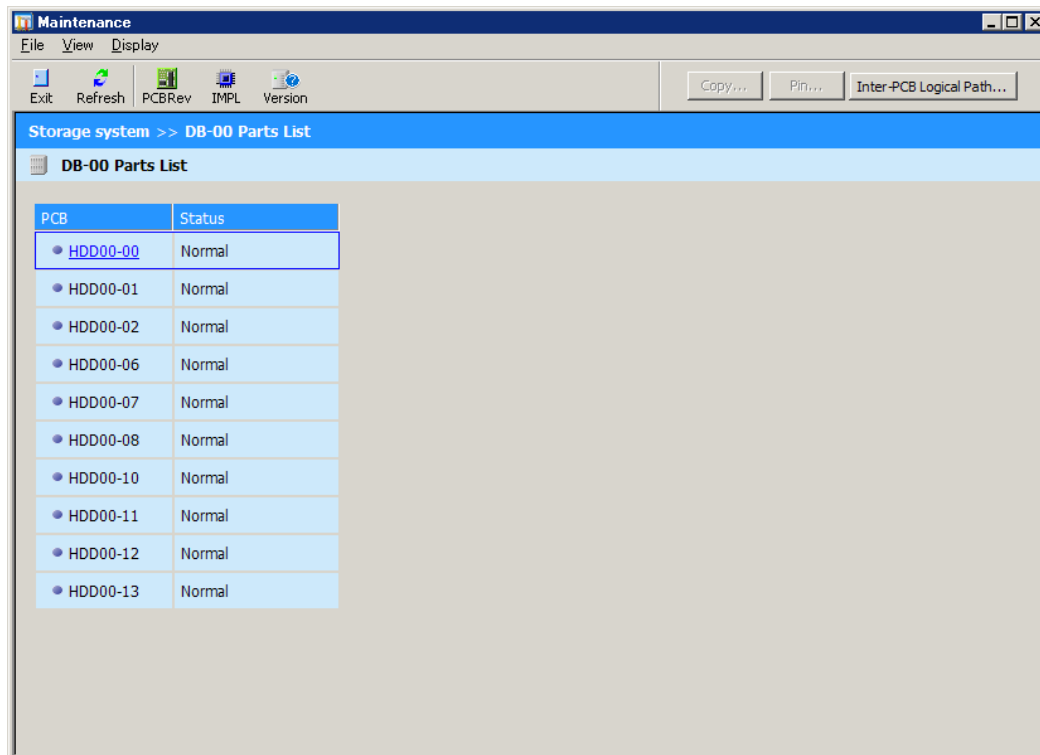




Table 9-10 HDD Information View

Item	Description
Title	Display an HDD location.
PCB	Display a PCB type icon and a location name (HDD).  : Installed  : A failure has occurred When selecting the PCB, display the PCB information in the detail view.
Status	Display a status. Normal : Normal Warning : A failure has occurred Unknown : The status is unknown (information acquisition failed)
Detail view	Display the detail information of the selected PCB. See “(1) HDD detail information view” .

(1) HDD detail information view

Execute the HDD status display and the maintenance operation.

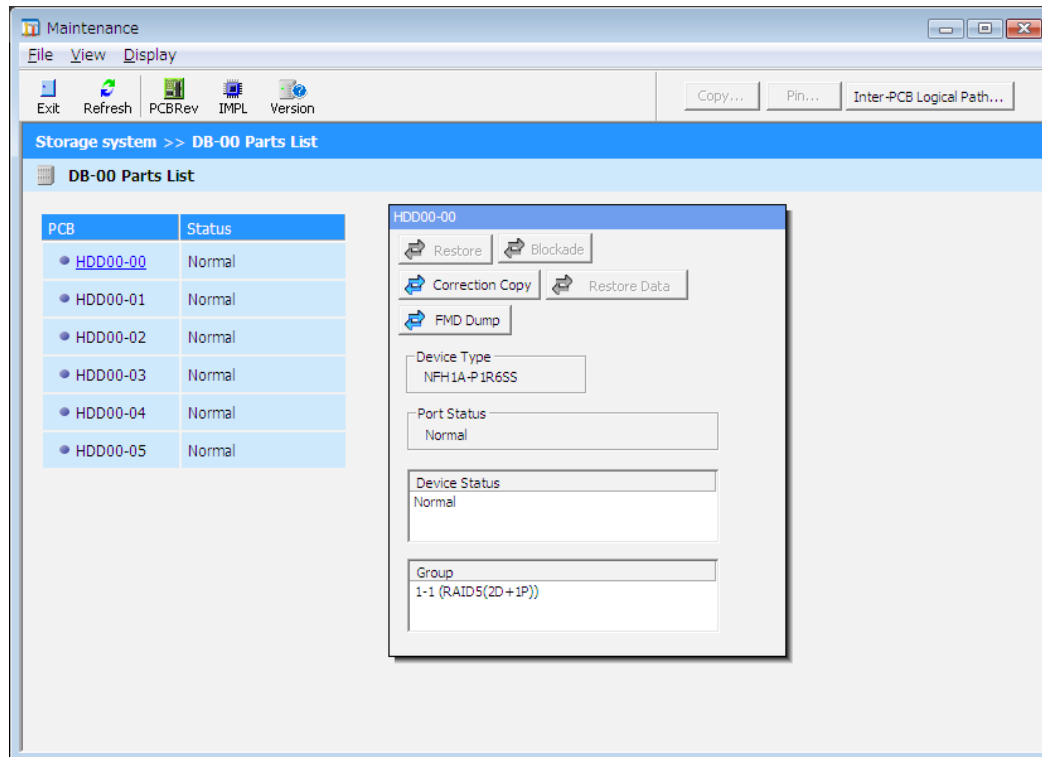


Table 9-11 HDD Information View

Item	Description
Title	Display an HDD location.
Maintenance button	Execute the maintenance processing [Correction Copy] : Correction copy processing (Disable to operate when Drive status is Free.). [FMD Dump] : FMD Dump collection processing (FMD Dump is displayed only Flash Module Drive.).
Drive model	Display a HDD model name.
Port status	Display an HDD port status. Normal : Normal Warning (Port 0 failed) : Port 0 is blocked Warning (Port 1 failed) : Port 1 is blocked Failed : Both ports are blocked
Drive status	Display an HDD drive status. (*1)
Group information	① In case of Data Drives Display the belonging group information of the HDD and its RAID level. ② In case of Spare Drives "Spare Drive" ③ In case of Free Drives "Free Drive"

*1: A drive status and the displayed description are as follows.

Drive Status		Display
Normal		"Normal"
Blocked due to a failure		"Failed"
Blocked due to maintenance		"Blocked"
A blocked part exists		"Warning"
Correction copy is in process	Local HDD → Remote HDD	"Correction Copy (xx%) to "copy destination" (*2)" xx : Copy progress rate (decimal integer) *2: Location name of copy destination HDD (same goes later)
	Remote HDD → Local HDD	"Correction Copy (xx%) to this HDD"
Drive copy is in process	Local HDD → Remote HDD	"Drive Copy (xx%) to "copy destination""
	Remote HDD → Local HDD	"Drive Copy (xx%) from "copy source""
Dynamic sparing is in process	Local HDD → Remote HDD	"Dynamic Sparing (xx%) to "copy destination""
	Remote HDD → Local HDD	"Dynamic Sparing (xx%) from "copy source""
Copy back is in process	Local HDD → Remote HDD	"Copy Back (xx%) to "copy destination""
	Remote HDD → Local HDD	"Copy Back (xx%) from "copy source""
Spare disk is usable		"Spare"
Free drive		"Free"
Spare disk is unusable		"Reserved"
Copy is incomplete		"Copy incomplete"

9.3.4.4 Dialog

A dialog displayed by the maintenance operation is configured as shown below.

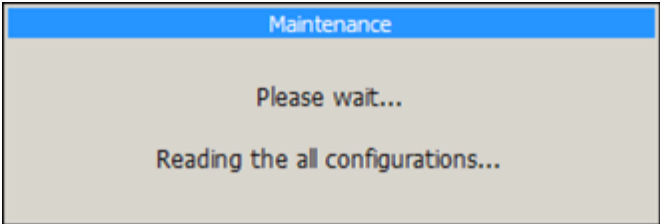


Table 9-12 List of Dialogs

Item	Description
Title	Fix with “Maintenance”
Process in execution	Display the updating information type according to progress of the process progress. “Reading the all configurations...” : Configuration information “Renewal the raid information...” : RAID information “Reading the drive copy progress information...” : Accompanying operation information “Reading the environment monitor...” : Environment monitoring information “Reading the PIN information...” : PIN information

10. Changing/Initializing Port Numbers Used by the Maintenance PC

You can change the port numbers used by the Maintenance PC to arbitrary port numbers.

Furthermore, you can reset the port numbers to the initial setting status by initializing them.

NOTE: The procedure for changing/initializing port numbers is the same for the Maintenance PC and the SVP. If you perform the procedure on the SVP, read the Maintenance PC as the SVP.

Unused port numbers are automatically allocated for some port numbers of the SVP software. (Automatic allocation)

To change the automatic allocation setting, perform the following according to the purposes.

- To change the automatically allocated port numbers, [“10.3 Reallocating Automatically Allocated Port Numbers”](#)
- To initialize the automatically allocated port numbers, [“10.4 Initializing Automatically Allocated Port Numbers”](#)
- To change the range of the port numbers to be allocated automatically, [“10.5 Changing Range of Port Numbers to be Allocated Automatically”](#)
- To initialize the range of the automatically allocated port numbers, [“10.6 Initializing Range of Port Numbers to be Allocated Automatically”](#)
- To confirm the port numbers allocated to each storage system, [“10.7 See the Port Number to be Used in the Maintenance PC”](#)

10.1 Changing Port Numbers Used by the Maintenance PC

Change the port numbers used by the Maintenance PC to arbitrary port numbers. The services used by the Maintenance PC restart according to the change.

1. When Storage Navigator is connected to the Maintenance PC, log out of all of the Storage Navigator. Then, stop the storage system service of Storage Device List.
(When you perform the procedure on the SVP, log out of all of Storage Navigator connected to the SVP.)
2. Start the command prompt by the Maintenance PC with the administrator authority.
3. Change the current directory to the directory in which the tool exists.
`cd /d C:\Mapp\wk\Supervisor\MappIniSet`
4. Execute the following command.
`MappSetPortEdit.bat [Service Port Number Key Name] [Port Number]`

NOTE: The following shows changeable “Port Number Key Name” and Initial Value of Port Number.

Port Number Key	Protocol	TCP/UDP	Initial Value of Port Number	Remarks
CommonJettyStart	HTTP	TCP	8080	
CommonJettyStop	HTTP	TCP	8210	
DeviceJettyStart (*1)	HTTP	TCP	48081-48336	An unused port number within the range is automatically allocated to each storage system.
DeviceJettyStop (*1)	HTTP	TCP	48411-48666	
DKCManPrivate	RMI	TCP	11099	
MAPPWebServer	HTTP	TCP	80	
MAPPWebServerHttps	HTTP	TCP	443	
RestAPIClientStart	CCI	UDP	36000	An unused port number within the range (36000 to 37000) is automatically selected.
RestAPIClientEnd	CCI	UDP	37000	
RestAPIServerStart	HTTP	TCP	9080	
RestAPIServerStop	HTTP	TCP	9210	
RMIClassLoaderHttps	RMI (SSL)	TCP	5443	
RMIClassLoader	RMI	TCP	51099	
RMIIFRegist	RMI	TCP	1099	
PreRMIServer (*1)	RMI	TCP	51100-51355	An unused port number within the range is automatically allocated to each storage system.
SLP	SLP	TCP, UDP	427	The port number is used only for the SVP.

*1: You cannot change the port number by MappSetPortEdit.bat. Run MappPortRangeSet.bat.
(See “[10.5 Changing Range of Port Numbers to be Allocated Automatically](#)”.)

- The effective range of the port numbers is “1 to 65535”. Set the port numbers so that they do not compete with the port numbers used by other services.
- The port numbers in the range from 1 to “1023” are reserved in another application. If any problem occurs by changing the port numbers in the range from “1” to “1023”, change the port numbers to “1024” or later.

NOTE: Among the port numbers of “1024” or later, “2049”, “4045”, and “6000” cannot be used for MAPPWebServer and MAPPWebServerHttps.

- You can specify multiple [service port number key name] parameters and [port number] parameters.
(Example) MappSetPortEdit.bat MAPPWebServer 81 MAPPWebServerHttps 444
- The management file of the port numbers is for reference only and do not change it. Close the management file of the port numbers when executing the change (or initialization) command.
- Check the port numbers to be used in the Maintenance PC by the procedure described in [“10.7 See the Port Number to be Used in the Maintenance PC”](#).

5. The completion message is displayed following the service restart message.
6. The message “Press any key to continue...” is displayed. Enter an arbitrary key.
7. Close the command prompt.

10.2 Initializing Port Numbers Used by the Maintenance PC

Reset the port numbers used by the Maintenance PC to the initial setting status. The services used by the Maintenance PC restart according to the initialization.

To initialize the automatically allocated port numbers, see [“10.4 Initializing Automatically Allocated Port Numbers”](#).

1. When Storage Navigator is connected to the Maintenance PC, log out of all of the Storage Navigator. Then, stop the storage system service of Storage Device List.
(When you perform the procedure on the SVP, log out of all of Storage Navigator connected to the SVP.)
2. Start the command prompt by the Maintenance PC with the administrator authority.
3. Change the current directory to the directory in which the tool exists.
`cd /d C:\Mapp\wk\Supervisor\MappIniSet`
4. Execute the following command.
`MappSetPortInit.bat`
5. An execution confirmation message of the initialization is displayed.
To continue the processing, enter [y] and press the [Enter].
To cancel the processing, enter [n] and press the [Enter].
6. A completion message is displayed following a service restart message.
7. The message “Press any key to continue...” is displayed. Enter an arbitrary key.
8. Close the command prompt.

10.3 Reallocating Automatically Allocated Port Numbers

You can reallocate the port numbers automatically allocated to the Storage System.

When the port numbers allocated to the Storage System are used in other applications, the port numbers are reallocated to the ports.

- NOTE:
- Stop the service of the Storage System to be reallocated, and then perform reallocation. If performed without stopping it, stop the service of the target Storage System in the Storage Device List window, and then start the service.
 - The DeviceJettyStart and DeviceJettyStop ports that are allocated at the time of starting the service of the Storage System are not reallocated.
 - When the function using the ports is disabled, delete the allocated port numbers.

1. When Storage Navigator is connected to the service of Storage System to be reallocated on the Maintenance PC, log out of all of connected Storage Navigator.
2. Stop the service of the Storage System to be reallocated.
3. Start the command prompt by the Maintenance PC with the administrator authority.
4. Change the current directory to the directory in which the tool exists.

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

5. Execute the following command.

```
MappPortManageRenum.bat [Serial numbers] (arbitrary)
```

When the serial numbers are omitted, the command is performed for all the storage systems registered in the Storage Device List.

6. The confirmation message for reallocation is displayed.
To continue the processing, enter [y], and then press the [Enter] key.
To cancel the processing, enter [n], and then press the [Enter] key.
7. The completion message is displayed.
8. The message "Press any key to continue..." is displayed. Enter an arbitrary key.
9. Close the command prompt.
10. Start the services of the reallocated Storage System.

10.4 Initializing Automatically Allocated Port Numbers

You can initialize the port numbers automatically allocated to the Storage System.

- NOTE:
- Stop the services of all the Storage Systems whose status of Storage Device List is Ready, and then initialize them.
 - If initialized without stopping the services, perform [“10.3 Reallocating Automatically Allocated Port Numbers”](#) for the storage system.

1. When Storage Navigator is connected to the Maintenance PC, log out of all of the Storage Navigator.
2. Stop the services of all the Storage Systems whose status of Storage Device List is Ready.
3. Start the command prompt by the Maintenance PC with the administrator authority.
4. Change the current directory to the directory in which the tool exists.
`cd /d C:\Mapp\wk\Supervisor\MappIniSet`
5. Execute the following command.
`MappPortManageInit.bat`
6. The confirmation message of initialization is displayed.
To continue the processing, enter [y], and then press the [Enter] key.
To cancel the processing, enter [n], and then press the [Enter] key.
7. The completion message is displayed.
8. The message “Press any key to continue...” is displayed. Enter an arbitrary key.
9. Perform reallocation.
`MappPortManageRenum.bat [Serial numbers] (arbitrary)`
When the serial numbers are omitted, the command is performed for all the storage systems registered in the Storage Device List.
10. The confirmation message for reallocation is displayed.
To continue the processing, enter [y], and then press the [Enter] key.
To cancel the processing, enter [n], and then press the [Enter] key.
11. The completion message is displayed.
12. The message “Press any key to continue...” is displayed. Enter an arbitrary key.
13. Perform [Step 9.](#) to [Step 12.](#) to reallocate the port numbers for all the registered storage systems.
14. Close the command prompt.
15. Start the service of the storage system to be operated.

10.5 Changing Range of Port Numbers to be Allocated Automatically

You can change the range of the port numbers automatically allocated to the Storage System.

1. Start the command prompt by the Maintenance PC with the administrator authority.
2. Change the current directory to the directory in which the tool exists.

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

3. Execute the following command.

```
MappPortRangeSet.bat [Service port number key name] [Port number range]
```

NOTE: [Port number key name] and default value of port number range to be changed are as follows.

Zero number port is not allocated regardless of this command setting.

Port number key name	Default value of port number range	Remarks
PreRMIServer	51100 to 51355	
DeviceJettyStart	48081 to 48336	
DeviceJettyStop	48411 to 48666	
unavailable	1 to 1023	Port numbers that are not used by automatic allocation

- The effective range of the port number range is “1 to 65535”. Set the port numbers so that they do not compete with those used in other services.
- When ephemeral ports in Windows from 49152 to 65535 are used, conflict can occur. If it occurs, change to a port number range other than that range.
- The port numbers “1 to 1023” are reserved in other applications. If “1 to 1023” are excluded from the unavailable setting value, the applications might not be operated normally.
- The character strings which can be specified in [port number range] are as follows.
Character strings: “Number” “,” “-” “rm”
When “rm” is specified, delete the setting of the specified port number key.

- You can specify multiple [service port number key name] parameters and [port number range] parameters.

Example: MappPortRangeSet.bat PreRMIServer 51200-55000 DeviceJettyStart 48181-48336,8000

- The port number range set for unavailable cannot be used even if it is an effective range for other keys.

Example: When PreRMIServer 51100-51355 unavailable 51100-51200 is set, the port number range allocated by PreRMIServer is 51201 to 51355.

4. The completion message is displayed.
5. The message “Press any key to continue...” is displayed. Enter an arbitrary key.
6. Close the command prompt.

10.6 Initializing Range of Port Numbers to be Allocated Automatically

You can initialize the range of the port numbers automatically allocated to the Storage System.

1. Start the command prompt by the Maintenance PC with the administrator authority.
2. Change the current directory to the directory in which the tool exists.
`cd /d C:\Mapp\wk\Supervisor\MappIniSet`
3. Execute the following command.
`MappPortRangeInit.bat`
4. The confirmation message of initialization is displayed.
To continue the processing, enter [y], and then press the [Enter] key.
To cancel the processing, enter [n], and then press the [Enter] key.
5. The completion message is displayed.
6. The message "Press any key to continue..." is displayed. Enter an arbitrary key.
7. Close the command prompt.

10.7 See the Port Number to be Used in the Maintenance PC

You can see the port numbers to be used in the Maintenance PC.

1. Start the command prompt by the Maintenance PC with the administrator authority.
2. Change the current directory to the directory in which the tool exists.

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

3. Execute the following command.

```
MappPortRefer.bat [Serial numbers] (arbitrary)
```

When the serial numbers are omitted, the information of all the Storage Systems registered in Storage Device List is displayed.

4. The information of the port numbers to be used in the Maintenance PC is displayed.
For the ports whose numbers are not allocated, "Not Defined" is displayed.
5. The completion message is displayed.
6. The message "Press any key to continue..." is displayed. Enter an arbitrary key.
7. Close the command prompt.

10.8 Checking the Application Using the Port Number Used by the Maintenance PC

If the port number to be used by the Maintenance PC is used by a different application, follow the procedure below to specify the application.

1. When the following troubleshooting code is output in a background service log, check the port number output in the background service log.

For the output location of the background service log and the way to read it, refer to TROUBLESHOOTING SECTION [“3.28.1.5 Background Service Log”](#).

Troubleshooting code	Port number keys name
TRSDLS000004	DKCManPrivate
TRRMIS002008	RMIIFRegist
TRRMIS002009	DKCManPrivate
TRRMIS002010	RMIIFRegist
TRRMIS002011	DKCManPrivate
TRMAAS000003	MAPPWebServer
	MAPPWebServerHttps
	RMIClassLoader
	RMIClassLoaderHttps
TRMAAS000004	CommonJettyStart
TRMAAS000005	CommonJettyStop
TRRMIS000006	RMIIFRegist
TRRMIS000007	PreRMIServer
TRRMIS000014	PreRMIServer
TRRMIS001003	RMIClassLoader
TRRMIS002508	DKCManPrivate
TRRMIS002509	DKCManPrivate

Example: TRMAAS000004 is output in a background service log.

```
[2016/06/10 16:29:09.056][ERROR][TRMAAS000004][Web Application Server][Failed :  
Failed to connect to the starting port of the web server. Port=8080.]
```

If multiple port number keys exist for a troubleshooting code, see [“10.7 See the Port Number to be Used in the Maintenance PC”](#). The port number key name using that port number can be specified by obtaining information on the port number used by the Maintenance PC

2. Start the command prompt on the SVP as Administrator.

- Run the netstat command and identify the process ID that uses the port number.



Note

If you stop the storage system service with the Storage Device List and then run the netstat command, only port numbers used by applications other than the storage management software are output.

Example: When the port number 8080 is used by a different application

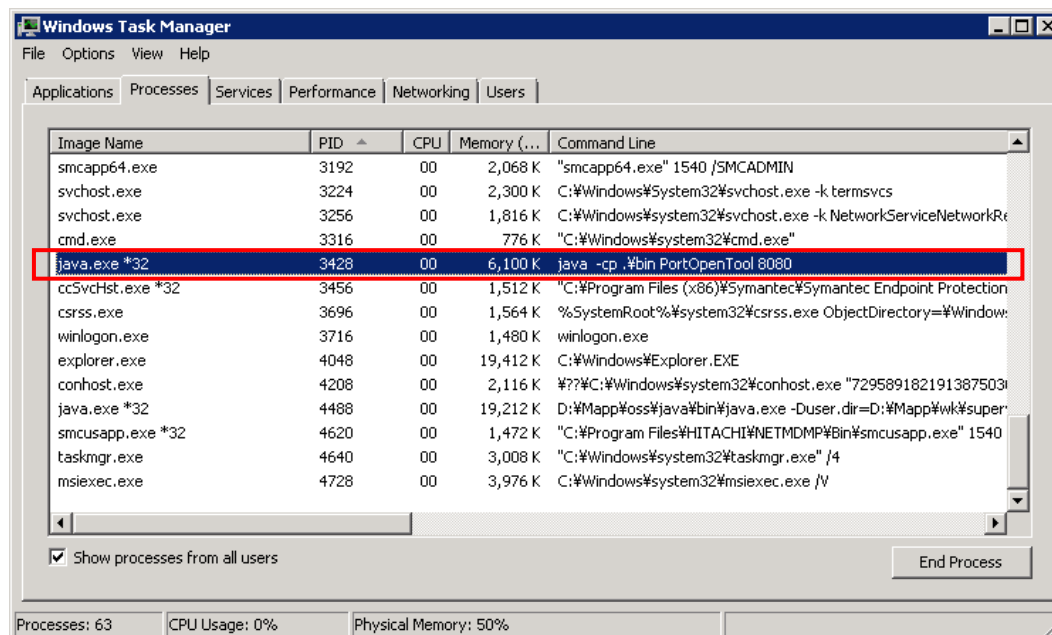
```
>netstat -ano
```

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	728
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1099	0.0.0.0:0	LISTENING	1688
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	3224
TCP	0.0.0.0:8080	0.0.0.0:0	LISTENING	3428
TCP	0.0.0.0:11099	0.0.0.0:0	LISTENING	4488
TCP	0.0.0.0:30002	0.0.0.0:0	LISTENING	1368

From the command result, a process ID (3428) that uses the port number 8080 can be identified.

- Start Task Manager, and identify an application with the process ID identified in [Step 3](#).
For Windows 7, in the Windows Task Manager, click [View] - [Select Column], and select the command line.

When the process ID (3428) is an application run by java.exe:



For java.exe, an application can be identified by referring to the command line.

11. Appendix

11.1 IP Addresses of Maintenance Ports and Internal Network

11.1.1 Maintenance Port Addresses

Select the maintenance port address from [Table 11-1](#) to [Table 11-2](#). The default value of the maintenance port address (network address and host address) is set to (CTL110.0.0.16)

Maintenance port address : xx.xx.xx.yy

Select the network address, xx.xx.xx, from [Table 11-1](#).

Select the host address, yy, from [Table 11-2](#).

Table 11-1 Selections of Maintenance Port Network Addresses

No.	Selectable Network Address	Subnet Mask
1	10.0.0 (Default)	255.255.255.0
2	192.168.0	
3	192.168.233	
4	172.23.211	
5	10.197.181	

Table 11-2 Selections of Maintenance Port Host Addresses

Selectable Host Address	Default	Remarks
16, 26, 36, 46, 56, 66, 76, 86, 96, 106, 116, 126, 136, 146, 156, 166, 176, 186, 196, 206, 216, 226, 236	16	Host address of Storage System CTL1

11.1.2 Internal Network Addresses

You can select the internal network address from [Table 11-3](#) and the default value is set to (10.251...).

Table 11-3 Selections of Internal Network Addresses

No.	Selectable Network Address	Subnet Mask	Remarks
1	10.251 (Default)	255.255.0.0 (Fixed)	
2	10.1		
3	172.24		
4	10.198		
5	10.17		
6	10.97		
7	172.17		
8	172.31		
9	192.168		Unusable when the maintenance LAN network address is as follows • 192.168.0.0 • 192.168.233.0

11.2 Port Number Used by the Maintenance PC

Port number	Protocol	Software	Port number change	Conflict with Maintenance PC
162	UDP	Device Manager	Not possible	None
427	TCP	Device Manager	Not possible	Present
1099	TCP	Hitachi Storage Navigator Modular 2 (SNM2 Server)	Possible	Present
2001	TCP	Device Manager	Possible	None
2443	TCP	Device Manager	Possible	None
5983	TCP	Device Manager	Possible	None
5988	TCP	Device Manager	Possible	None
5989	TCP	Device Manager	Possible	Present
20352	TCP	Tiered Storage Manager	Possible	None
22015-22018	TCP	Hitachi Command Suite common component	Possible	None
22019	TCP	Tuning Manager	Possible	None
22020	TCP	Tuning Manager	Possible	None
22023	TCP	Tuning Manager	Possible	None
22024	TCP	Tuning Manager	Possible	None
22025-22028	TCP	Hitachi Command Suite common component	Possible	None
22031-22034	TCP	Hitachi Command Suite common component	Possible	None
22098-22100	TCP	Host Data Collector	Possible	None
22104-22106	TCP	Host Data Collector	Possible	None
22110-22120	TCP	Host Data Collector	Possible	None
22286	TCP	Tuning Manager	Possible	None
22610	TCP	Compute Systems Manager	Possible	None
22611	TCP	Compute Systems Manager	Possible	None
22900-22999	TCP	Tuning Manager	Not possible	None
23015-23018	TCP	Hitachi Command Suite common component	Possible	None
23019-23024	TCP	Tuning Manager	Possible	None
23025	TCP	Device Manager (*1)	Possible	None
23026	TCP	Device Manager (*1)	Possible	None
23031	TCP	Hitachi Command Suite common component (*1)	Possible	None
23032	TCP	Hitachi Command Suite common component (*1)	Possible	None
23052	TCP	Host Data Collector (*1)	Not possible	None
23055	TCP	Device Manager	Possible	None
23450-23453	TCP	Configuration Manager REST API	Possible	None
24220	TCP	Device Manager (*1)	Possible	None
24221	TCP	Tuning Manager	Possible	None
24222	TCP	Tuning Manager	Possible	None
24230	TCP	Device Manager	Possible	None
24235-24242	TCP	Hitachi Command Suite common component	Possible	None
24500	TCP	Tiered Storage Manager	Possible	None
31001-31002	UDP	Configuration Manager REST API	Not possible	None
45001-49000	TCP	Hitachi Command Suite common component (*1)	Possible	Present

*1: The port number is not used by Hitachi Command Suite 8 or later.

11.3 Maintenance Utility Window Configuration

11.3.1 Basic Framework

Consists of three areas, “Header Area”, “Navigation Area” and “Application Area”.

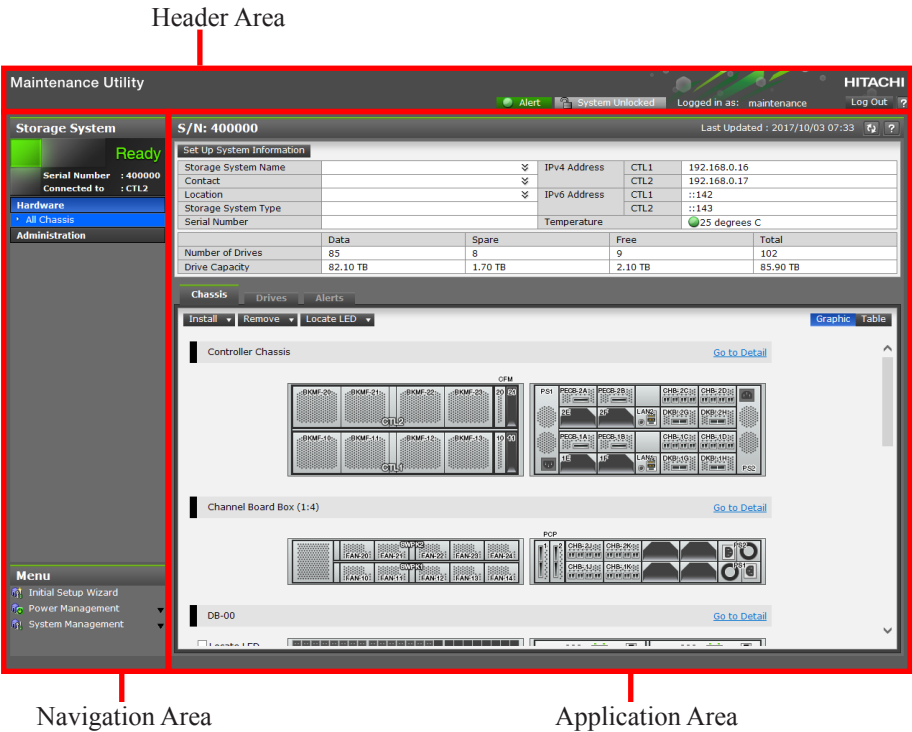


Table 11-4 Window Configuration

Area	Description
Header Area	The common information (such as alert display/system lock display/user name) is displayed always.
Navigation Area	Display system management menus.
Application Area	Perform information display and setting related to the system.

11.3.2 Header Area

The following describes the common header area configuration in the main window.

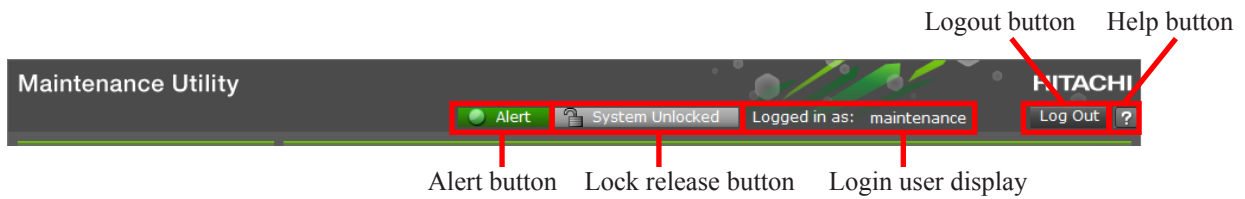
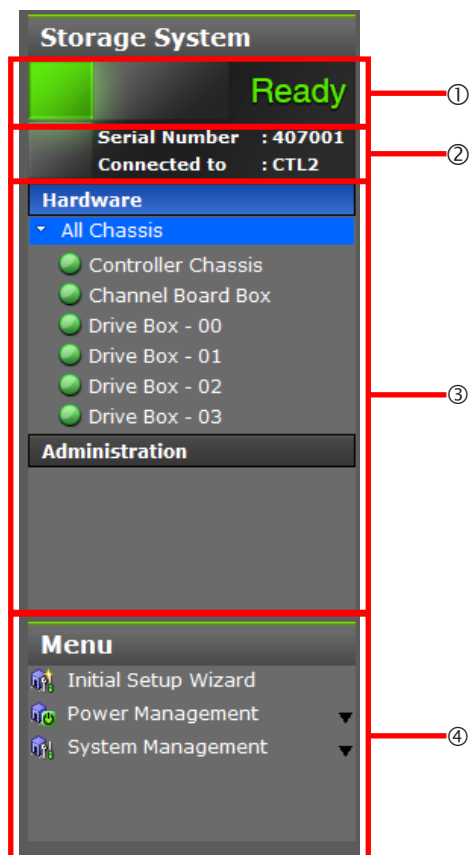


Table 11-5 Header Area Configuration

Window Item	Description
Alert button	<ul style="list-style-type: none"> Clicking this button displays the [Alerts] tab (Refer to "3.21 Alert Display") in the Storage System window. Switch the display image of the alert button according to the Storage System status (Refer to Table 11-7) in the navigation area.
Lock release button	<ul style="list-style-type: none"> Clicking this button starts the "Force Release System Lock" window. (Refer to "3.17 Force Release System Lock") Switch the system lock status to locked/unlocked.
Login user display	Display the user name used for login. When the login name is long and does not fit in the location area due to expansion of the window, display "..." at the end of the name.
Logout button	Clicking this button displays a confirmation message.
Help button	Display the help. The similar help button is also in the pop-up window. To display the Help, the settings for enlarging and reducing the display might not be reflected in the help window depending on the type or version of browser.

11.3.3 Navigation Area

The following describes the navigation area configuration.



- ①:Storage System Status
- ②:Storage System Information
- ③:Display Item Selection Panel
- ④:Operation Menu Panel

Table 11-6 Navigation Area Configuration

Window Item	Description
Storage System information	<ul style="list-style-type: none"> • Display a serial number in the first row. • Display the currently connecting CTL number in the second row. • Clicking this area displays the Storage System information (Main window) in the application area.
Storage System status	Display a Storage System status image. (Refer to Table 11-7)
Display item selection panel	<ul style="list-style-type: none"> • Separate the menus used into [Hardware] and [Management] to display. Selecting a menu displays the content in the application area. • In the [Hardware] menu, the icon on the left of the hardware name character string displays the hardware status and the icon on the right shows the LED lighting status.
Operation menu panel	Place the operation menu related to the entire system.

Table 11-7 Storage System Status

NOTE: See “3.22 Alert Display Related to FRU (Field Replacement Unit)” for the status of each part.

Status	Condition	Unreferenced SIM	Navigation Area	Icon and Color of Alert Button
Failed	The status with a possibility that the Storage System may be down	None		/Red
		Available		/Red
Warning	The status with Blocked/Warning in the part status	None		/Amber
		Available		/Amber
Ready	Part statuses are all normal (all SIMs are referred to)	None		/Green
		Available		/Green
Power on in progress	PSON is in progress			—
Power off in progress	PSOFF is in progress			—
?	Others (The status before performing PSON, and so on)			—

11.3.4 Application Area

The following describes the common application area configuration in the main window.



Table 11-8 Application Area Configuration

Window Item	Description
Last update date display	Display the last update dated of the figure display information. (YYYY/MM/DD hh:mm)
Update button	Update the displayed information.
Help button	Display the help. The similar help button is also in the pop-up window. To display the Help, the settings for enlarging and reducing the display might not be reflected in the help window depending on the type or version of browser.

11.4 Functions List of the Windows Used for Maintenance Work

Tool Kind	Function	Refer
Storage Device List	Stopping and connecting the Storage System	2.14.2 Stopping the Service of Storage System 2.14.3 Starting the Service of Storage System
	Changing Storage System information and updating Web Console software	2.14.4 Changing Storage System Information and Updating Software of Web Console
Web Console	Connecting to the Host	4.1 Connecting to the Host
		4.1.1 Creating Parity Groups
		4.1.2 Checking the Logical Devices
		4.1.3 Allocating the Logical Devices of a Storage System to a Host
		4.1.4 Configuring a Host Group or iSCSI Target
	Managing Drives	4.2 Managing Drives
		4.2.1 Setting Spare Drives
		4.2.2 Managing Parity Group
		4.2.3 Managing Logical Device
	Managing Port	4.3 Managing Port
		4.3.1 Editing Fibre Channel
		4.3.2 Editing iSCSI
		4.3.3 Deleting Host Group Information
		4.3.4 Deleting iSCSI Target Information
		4.3.5 Using CHAP Authentication with iSCSI Ports
	Logical Device	4.4 Logical Device Maintenance
		4.4.1 Blocking LDEVs
		4.4.2 Restoring Blocked LDEVs
		4.4.3 Editing an LDEV Name
		4.4.4 Force Restore LDEVs
	Local Replication	4.5.1 Local Replication
	Data Retention Utility	4.5.2 Data Retention Utility
	Universal Volume Manager	4.5.3 Universal Volume Manager
	Remote Replication	4.5.4 Remote Replication
	Data Retention Utility Dynamic Provisioning/ Dynamic Tiering/Thin Image	4.5.5 Dynamic Provisioning/Dynamic Tiering/active flash/ Thin Image
	Copy Back Setting	4.6 Copy Back Setting
		4.6.1 Setting the Copy Back
		4.6.2 Changing the Copy Back
	Verify	4.7 Verify (Parity Consistency Check)
		4.7.1 Executing Verify (Parity Consistency Check)
		4.7.2 Interrupting Verify
		4.7.3 Checking the Progress

(To be continued)

(Continued from preceding page)

Tool Kind	Function	Refer
MPC Window	Mode	5.1 Mode
	Dump/AutoDump	5.2 Dump
	Log Indication	5.3 Log
		5.3.1 Log Indication
		5.3.2 Log Delete
		3.21 Alert Display
	Online Read Margin (ORM)	5.4 Online Read Margin (ORM)
	Management of Drive Threshold Values	5.5 Management of Drive Threshold Values
	Setting Machine Install Data	5.6 Setting Machine Install Data
	System Option	5.7 System Option
	Setting System Option Mode	5.8 Setting System Option Mode
	System Tuning	5.9 System Tuning
	Maintenance Screen	5.11 Maintenance Screen
		5.12 Maintenance Procedure
		5.12.1 Copy Status View
		5.12.2 Version of Firmware
		5.12.3 Pin Data Indication
		5.12.4 PCB/SFP Revision Display
		5.12.5 Inter-PCB Logical Path
		5.12.6 Restoring Failed MP
		5.12.7 Failed CTL Recovery
		5.12.8 Error or Failure Status Action
	Monitoring	6. Monitoring

(To be continued)

(Continued from preceding page)

Tool Kind	Function	Refer
Maintenance Utility	Adding Drives	INSTALLATION SECTION "3.3 Adding Drives"
	Adding Drive Boxes	INSTALLATION SECTION "3.4 Adding Drive Boxes"
	Adding Channel Board	INSTALLATION SECTION "3.5 Adding Channel Board (CHB)"
	Adding Disk Board (DKB)/ Replacing Disk Board	INSTALLATION SECTION "3.6 Adding Disk Board (DKB)/ Replacing Disk Board (DKB) (Type Change)"
	Adding Cache Memory/ Cache Flash Memory/ Battery	INSTALLATION SECTION "3.7 Adding Cache Memory/Cache Flash Memory"
	Adding Shared Memory	INSTALLATION SECTION "3.8 Adding Shared Memory (SM)"
	Changing the Type of Small Form-Factor Pluggable	INSTALLATION SECTION "3.9 Changing the Type of Small Form-Factor Pluggable (SFP)"
	Adding PDUs for a Rack and PDU Power Codes	INSTALLATION SECTION "3.10 Adding PDUs for a Rack and PDU Power Codes"
	Removing Drives	INSTALLATION SECTION "4.3 Removing Drives"
	Removing Drive Boxes	INSTALLATION SECTION "4.4 Removing Drive Boxes"
	Removing Channel Boards	INSTALLATION SECTION "4.5 Removing Channel Boards (CHB)"
	Removing Disk Board	INSTALLATION SECTION "4.6 Removing Disk Board (DKB)"
	Removing Cache Memory	INSTALLATION SECTION "4.7 Removing Cache Memory"
	Removing Shared Memory	INSTALLATION SECTION "4.8 Removing Shared Memory (SM)"
	Removing PDUs for a Rack and PDU Power Codes	INSTALLATION SECTION "4.9 Removing PDUs for a Rack and PDU Power Codes"
	Replacing a Drive	REPLACEMENT SECTION "2.3 Replacing a Drive"
	Replacing a Controller Board	REPLACEMENT SECTION "2.4 Replacing a Controller Board"
	Replacing a Cache Memory	REPLACEMENT SECTION "2.5 Replacing a Cache Memory"
	Replacing a FAN	REPLACEMENT SECTION "2.6 Replacing a FAN"
	Replacing a BKMF	REPLACEMENT SECTION "2.7 Replacing a BKMF"
	Replacing a Battery	REPLACEMENT SECTION "2.8 Replacing a Battery"
	Replacing a BKM	REPLACEMENT SECTION "2.9 Replacing/Preventive Replacement of a BKM"
	Replacing a Cache Flash Memory	REPLACEMENT SECTION "2.10 Replacing a Cache Flash Memory (CFM)"

(To be continued)

(Continued from preceding page)

Tool Kind	Function	Refer
Maintenance Utility	Replacing a LAN Board	REPLACEMENT SECTION “2.11 Replacing a LAN Board”
	Replacing a Channel Board	REPLACEMENT SECTION “2.12 Replacing a Channel Board (CHB)”
	Replacing a Small Form-Factor Pluggable	REPLACEMENT SECTION “2.13 Replacing a Small Form-Factor Pluggable (SFP)”
	Replacing a Disk Board	REPLACEMENT SECTION “2.14 Replacing a Disk Board (DKB)”
	Replacing a Power Supply	REPLACEMENT SECTION “2.15 Replacing a Power Supply”
	Replacing an ENC	REPLACEMENT SECTION “2.16 Replacing an ENC”
	Replacing a Controller Chassis/Drive Box	REPLACEMENT SECTION “2.17 Replacing a Controller Chassis/Drive Box”
	Replacing a Front Bezel	REPLACEMENT SECTION “2.18 Replacing the Front Bezel”
	Replacing PDUs	REPLACEMENT SECTION “2.19 Replacing PDUs”
	Replacing a SAS Cable	REPLACEMENT SECTION “2.20 Replacing a SAS Cable”
	Replacing a SVP	REPLACEMENT SECTION “2.21 Replacing a SVP”
	Initial Setting Wizard	INSTALLATION SECTION “2.21 Initial Setting Wizard”
	Network Setting	3.1 Network Setting [Start Separate Action]
	Firmware	3.2 Firmware
	User Administration	3.3 User Administration
		3.3.1 Setting up User Account
		3.3.2 Disabling User Accounts
		3.3.3 Changing User Account Authentication
		3.3.4 Removing User Accounts
		3.3.5 User Account Information
	Alert Notifications	3.4 Alert Notifications
		3.4.1 Setting up Email Notification when Storage System Failures Occur
		3.4.2 Setting up Syslog Notification
		3.4.3 Setting up SNMP Notification
	Time Setting	3.5 Time Setting
		3.5.1 Setting Synchronization Information
	Network Setting	3.6 Network Setting
		3.6.1 Network Setting
		3.6.2 Network Permissions

(To be continued)

(Continued from preceding page)

Tool Kind	Function	Refer
Maintenance Utility	Setting up License Keys	3.7 Setting up License Keys
		3.7.1 Types of License Keys
		3.7.2 Software and Licensed Capacity
		3.7.3 Installing Software Using a License Key Code
		3.7.4 Enabling a License
		3.7.5 Disabling a License
		3.7.6 Removing Program Product
		3.7.7 Verifying License
		3.7.8 Cautions on Licensed Capacity in Non-License-Related Windows
		3.7.9 Troubleshooting related to licenses
		3.7.10 Precautions related to the pool capacity when using Dynamic Provisioning
	Audit Log Settings	3.8 Audit Log Settings
		3.8.1 Verifying the Settings to Transfer the Syslog Server
		3.8.2 Transferring Audit Log to the Syslog Server
	Locate LED	3.8.4 Sending a Test Message to the Syslog Server
		3.9 Turn on/off Locate LEDs
		3.9.1 Turn on Locate LED
		3.9.2 Turn off Locate LED
	Storage System Power	3.10 Power on Storage System
		3.11 Power off Storage System
	Edit UPS Mode	3.12 Edit UPS Mode
	Edit Login Message	3.13 Edit Login Message
	Select Cipher Suite	3.14 Select Cipher Suite
	Update Certificate Files	3.15 Update Certificate Files
	Edit or Confirm System Parameters	3.16 Edit or Confirm System Parameters
	Force Release System Lock	3.17 Force Release System Lock
	Reboot GUM	3.18 Reboot GUM
	Change Password	3.19 Change Password
	Acquiring Dumps (System Dump or Small System Dump)	3.27 Acquiring Dumps using Maintenance Utility
	Obtaining Configuration Information Backup	3.28 Obtaining Configuration Information Backup
	View Volume Status	3.29 Checking Existence of Pinned Track and Blocked LDEV

11.5 Stopping/Starting the Storage Navigator Services

When you start up the Maintenance PC, the Storage Navigator services (*) are automatically started. The Storage Navigator services are always running while the Maintenance PC is in use.

If this function is used, the Storage Navigator services can be stopped and started. Stopping the Storage Navigator services can release the resources of the Maintenance PC that are used for executing the services.

*: The Storage Navigator services are DKCMan, MAPAppServer, MAPWebServer, and MAPRestAPIServer that run as the Windows services.

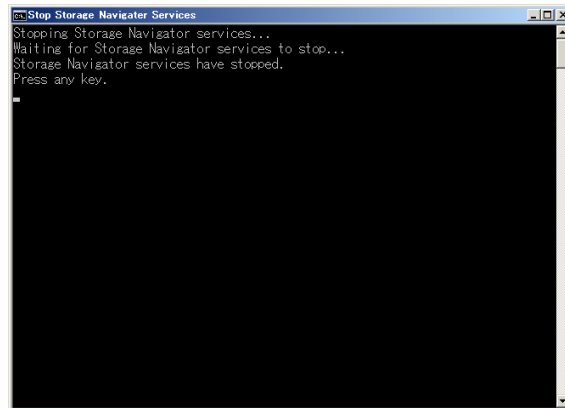
11.5.1 Stopping the Storage Navigator Services

The following shows the procedure for stopping the Storage Navigator services. Performing the following procedure makes the Storage Navigator services unable to automatically start when the Maintenance PC is restarted.

<p>NOTICE:</p> <ul style="list-style-type: none">• Make sure that the maintenance work is not performed before stopping the Storage Navigator services.• Do not perform any other operations until the procedure for stopping the Storage Navigator services is completed.• When you perform the following procedure, the Command Prompt window opens. Do not force quit the Command Prompt window (Ctrl + C or closing action).

1. Stop the service of the Storage System by following the procedure in [“2.8.1 Stopping Web Console”](#).
2. From the Windows start menu, right-click [Hitachi Device Manager-Storage Navigator]-[Stop Storage Navigator Services] and click [Run as administrator].
The Command Prompt window appears and the stop processing of the Storage Navigator services is executed. The stop processing takes 10 minutes or less.

3. When the message “Storage Navigator services have stopped” is displayed, press the Enter key to close the Command Prompt window.



NOTICE: To do the maintenance work using the Maintenance PC after performing this procedure, make sure to perform the procedure described in [“11.5.2 Starting the Storage Navigator Services”](#) before starting the maintenance work.

When an error occurs during the stop processing of the Storage Navigator services, an error code is displayed in the Command Prompt.

Error Code	Descriptions	Actions
100	The user authority is wrong.	Run as an administrator again.
200	The service stop processing times out.	Restart the Maintenance PC. The stop processing of the Storage Navigator services is completed by restarting.
201	A service that does not respond to the service stop request is detected.	Make sure that the services are stopped by performing the following procedure. 1. From the Windows start menu, select [Control Panel]-[Administrative Tools]-[Services]. 2. Check that the [Startup type] of DKCMan, MAPAppServer, APPWebServer, and MAPRestAPIServer is [Manual]. When it is not [Manual], right-click on the services, open the properties window, change the [Startup type] to [Manual], and then restart the Maintenance PC.
202	Other errors are detected.	
300	The software of the Maintenance PC is wrong.	Restart the Maintenance PC. After the restart, uninstall the Maintenance PC software, then install it again. (See “8.2 Maintenance PC Software Uninstallation” and “1.4 Maintenance PC Software Initial Installation/Update Installation” .)

11.5.2 Starting the Storage Navigator Services

The following shows the procedure for starting the Storage Navigator services. Performing the following procedure makes the Storage Navigator services automatically start when the Maintenance PC is restarted.

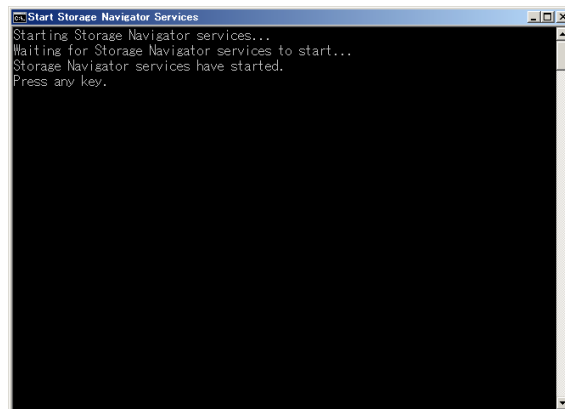
NOTICE:

- Do not perform any other operations until the procedure for starting the Storage Navigator services is completed.
- When you perform the following procedure, the Command Prompt window opens. Do not force quit the Command Prompt window (Ctrl + C or closing action).

1. From the Windows start menu, right-click [Hitachi Device Manager-Storage Navigator]-[Start Storage Navigator Services] and click [Run as administrator].

The Command Prompt window appears and the start processing of the Storage Navigator services is executed. The start processing takes one minutes or less.

2. When the message “Storage Navigator services have started” is displayed in the Command Prompt window, press the Enter key to close the Command Prompt window.



3. Start the service of Storage System by following the procedure in [“2.5 Starting Web Console”](#).
If the service of the Storage System cannot be started, see [“2.9 Troubleshooting of Storage Device List”](#).

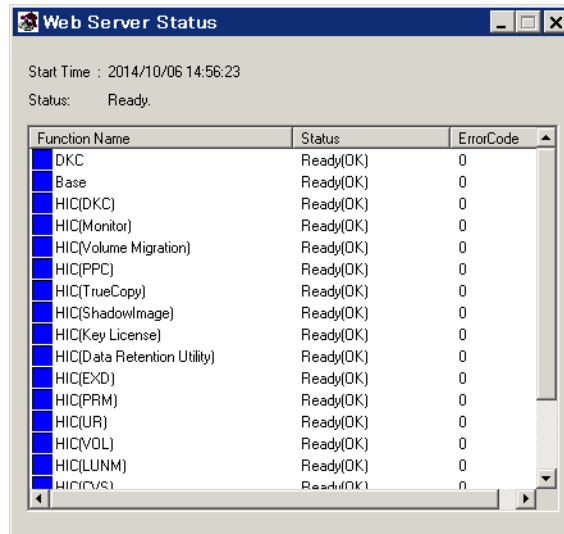
When an error occurs during the start processing of the Storage Navigator services, an error code is displayed in the Command Prompt.

Error Code	Descriptions	Actions
100	The user authority is wrong.	Run as an administrator again.
200	The service start processing times out.	Restart the Maintenance PC. The start processing of the Storage Navigator services is completed by restarting.
201	A service that does not respond to the service start request is detected.	Make sure that the services are started by performing the following procedure.
202	Other errors are detected.	<ol style="list-style-type: none">1. From the Windows start menu, select [Control Panel]-[Administrative Tools]-[Services].2. Check that the status of DKCMan, MAPAppServer, APPWebServer, and MAPRestAPIServer is [Started]. When it is not [Started], right-click on the services, open the properties window, change the [Startup type] to [Manual], and then restart the Maintenance PC.
300	The software of the Maintenance PC is wrong.	Uninstall the Maintenance PC software, then install it again. (See “8.2 Maintenance PC Software Uninstallation” and “1.4 Maintenance PC Software Initial Installation/Update Installation” .)

11.6 Specifications of Web Server Status List

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.

When the [Web Server Status] button of MPC launcher is pressed, the window as shown below displays.



Function Name	Status	ErrorCode
DKC	Ready(OK)	0
Base	Ready(OK)	0
HIC(DKC)	Ready(OK)	0
HIC(Monitor)	Ready(OK)	0
HIC(Volume Migration)	Ready(OK)	0
HIC(PPC)	Ready(OK)	0
HIC(TrueCopy)	Ready(OK)	0
HIC(ShadowImage)	Ready(OK)	0
HIC(Key License)	Ready(OK)	0
HIC(Data Retention Utility)	Ready(OK)	0
HIC(ExD)	Ready(OK)	0
HIC(PRM)	Ready(OK)	0
HIC(UR)	Ready(OK)	0
HIC(VOL)	Ready(OK)	0
HIC(LUNM)	Ready(OK)	0
HIC(VS)	Ready(OK)	0

NOTE: 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 Mode even in the Processing status, however, a maintenance work cannot be done.)
- This window is started by pressing the [Web Server Status] button on the “MPC” 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(TrueCopy)	Displays the state of initialization of the Remote Copy function.	6005 / 6105
8	HIC(ShadowImage)	Displays the state of initialization of the ShadowImage function.	7005 / 7105
9	HIC(Key License)	Displays the state of initialization of the Key License function.	0405
10	HIC(Data Retention Utility)	Displays the state of initialization of the Data Retention Utility function.	9205 / 9605
11	HIC(EXD)	Displays the state of initialization of Universal Volume Manager function.	0605
12	HIC(PRM)	Displays the state of initialization of Virtual Partition Manager function.	8505
13	HIC(UR)	Displays the state of initialization of the Universal Replicator function.	6505 / 6605
14	HIC(VOL)	Displays the state of initialization of the Quick Shadow / Dynamic Provisioning function.	3005
15	HIC(LUNM)	Displays the state of initialization of the LUN Manager function.	1005
16	HIC(CVS)	Displays the state of initialization of the Volume Manager function.	3305
17	HIC(MNT)	Displays the state of initialization of the Maintenance function.	8705
18	HIC(RPT)	Displays the state of initialization of the Report function.	8805
19	HIC(RSG)	Displays the state of initialization of the Resource Group function.	20705

- Status

	Display	Color	Meaning
1	Not Initialize	Gray	Initialization is not started yet.
2	Initialize(Start)	Yellow	Initialization is in progress.
3	Initialize(Retry)	Yellow	Initialization failed and 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 Maintenance PC/SNMP/Web Console has been completed.
6	Refresh(Retry)	Green	Refreshment failed and is being retried.
7	Initial(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:
- Any of the statuses is Initialize(Start) / Refresh(Start) / Initialize(Retry) / Refresh(Retry), no maintenance work can be done from an Maintenance PC. The message “INS2268W” is displayed on the Maintenance PC. However, it changes to the state of Initialize(Pause) / Refresh(Pause) in about 10 seconds and the maintenance work on the Maintenance PC 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 Maintenance PC rebooting, which is done after executing Define Information Files or All Configuration Files for alteration of the Config, may fail.)
 - While an Maintenance PC maintenance work is being done, an initialization or refreshment operation fails and the status becomes Retry. When the maintenance work is completed, close the “MPC” 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 (CCI etc.) other than Web Console 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, there may be a problem just on display.

If you can reboot by pressing the “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 Maintenance PC to the View Mode.

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

- Error Code

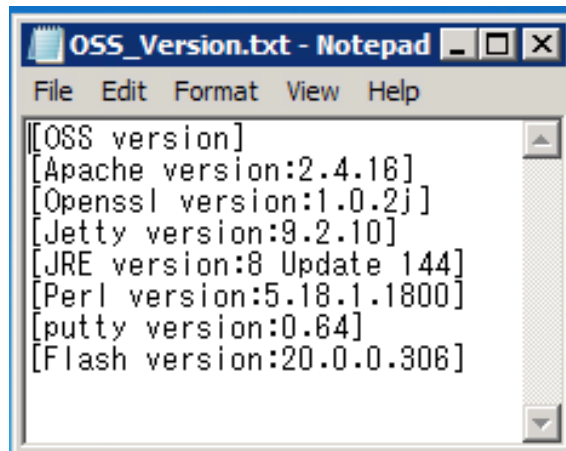
When an error occurs, its error code is displayed.

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.)

11.7 Check the Version of Third Party Software

Can Check the the version third party software (OSS).

How to check the version that is installed in Maintenance PC, refer to “<Maintenance PC installed directory>\OSS\OSS_Version.txt”.



The examples of displaying Java (JRE) versions in this manual are shown below.

All items 1 to 3 indicate the same Java (JRE) version. (For item 3, the update number is arbitrary.)

Item	Version Display	Description
1	8 Update 77	The number before “Update” is the Java family number. The number after “Update” is the update number.
2	1.8.0_77	The second digit indicates the Java family number. The number after “_” indicates the update number.
3	JRE8	Indicates only the Java family number.

11.8 Restrictions on Operations of Maintenance Utility Started by Specifying IP Address of CTL

The operations of Maintenance Utility started by specifying an IP address of CTL are restricted unlike Maintenance Utility started from the “Web Console” window or the “MPC” window.

There are the same restrictions on operations also when Maintenance utility is started from Hitachi Storage Advisor Embedded (HSAE).

Maintenance Operation	Restrictions
Firmware update	<ul style="list-style-type: none"> • The selection of an update method (online update or offline update) is not possible. The default online update is executed. • The selection of a reboot pattern is not possible. The default MP reboot by 1/4 is executed. • The force execution option (*1) cannot be selected.
Drive installation/removal/replacement	The force execution option (*1) cannot be selected.
Drive Box installation	The force execution option (*1) cannot be selected.
Disk Board installation/removal/replacement/type change replacement	The force execution option (*1) cannot be selected.
ENC replacement	The force execution option (*1) cannot be selected.
SAS cable replacement	The force execution option (*1) cannot be selected.
Controller Board replacement/type change replacement	The force execution option (*1) cannot be selected.
Cache Memory installation/removal/replacement	The force execution option (*1) cannot be selected.
Cache Flash Memory replacement	The force execution option (*1) cannot be selected.
FAN replacement	The force execution option (*1) cannot be selected.
LAN Board replacement	The force execution option (*1) cannot be selected.
BKMF Battery preventive replacement	The force execution option (*1) cannot be selected.
BKM preventive replacement	The force execution option (*1) cannot be selected.
Channel Board installation	The force execution option (*1) cannot be selected.
SFP type change (data transfer rate change)	The force execution option (*1) cannot be selected.
Channel Board Box installation/removal	The force execution option (*1) cannot be selected.
PCIe Channel Board replacement	The force execution option (*1) cannot be selected.
PCIe-cable Connection Package replacement	The force execution option (*1) cannot be selected.
PCIe-cable replacement	The force execution option (*1) cannot be selected.
Switch Package replacement	The force execution option (*1) cannot be selected.
GUM reboot	The force execution option (*1) cannot be selected.
Network setting	<ul style="list-style-type: none"> • The force execution option (*1) cannot be selected. • The menu is not displayed when GUM and DKC cannot communicate with each other. If Maintenance Utility is started from the “Web Console” window or the “MPC” window so as to take recovery actions against the internal IP address inconsistency, the menu is displayed even when GUM and DKC cannot communicate with each other.
System parameters edit	The system parameters edit is not possible because the menu is not displayed.
System safe mode boot	The system safe mode boot is not possible because the menu is not displayed.

*1: Use the force execution option only when instructed by recovery procedures in TROUBLESHOOTING SECTION or by the factory.

11.9 Setting GUM System Options

Set the GUM system options that are described in the following table. To set them, use the GUMSystemOption Setting Tool.

NOTICE: Perform this operation only after you have received relevant instructions from the Technical Support Division.

[GUM system options]

Option	Description
HSAE support URL	Set the appropriate URL for Hitachi Storage Advisor Embedded (HSAE). Upon setting this option, HSAE GUI will display the “Learn more ..” menu under the Information (“i” icon) that will point to the URL value set to this option. Valid values are: <ul style="list-style-type: none">• For Hitachi Vantara, set this URL to the Hitachi Vantara documentation portal, for example. https://knowledge.hds.com/Documents/Storage• For China partners/customers, set the URL to their support site or any URL they provide.
Enabling/disabling the HSAE Provisioning function	Set whether to display [Server] menu of HSAE GUI.
Enabling/disabling copyright display	Set whether to display copyright. Copyright information must be displayed for Hitachi Vantara but hidden for China partners/customers.

[Installing GUMSystemOption Setting Tool]

When the maintenance PC software is installed, the setting tool is also installed.

Installation location of the setting tool:

C:\Mapp\wk\supervisor\GUMSystemOptionTool

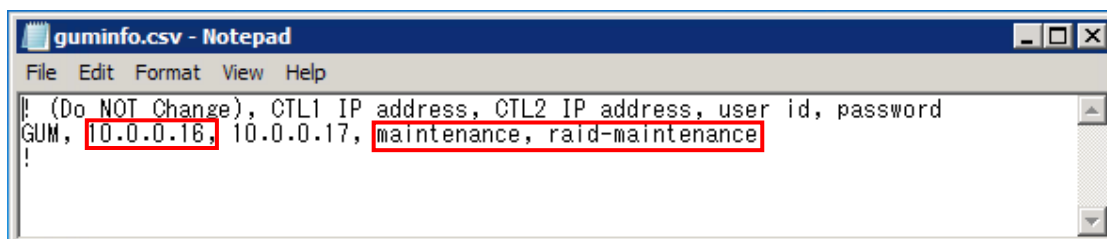
NOTE: “C:\Mapp” is the default installation directory of the Maintenance PC Software. The setting tool is installed in the directory that is specified when the Maintenance PC Software is installed.

[Preparation]

Before running the setting tool, set the CTL IP address/user account.

Open guminfo.csv in the tool directory with the text editor and edit the following items.

Item	Description
CTL1 IP address	Change to the IP address of the LAN port (usually the maintenance port) of the CTL to which the Maintenance PC is connected. Even when the Maintenance PC is connected to CTL2, change the CTL1 IP address.
CTL2 IP address	Unused. No setting change is required.
user id	Specify the user name and the password of the account for storage system maintenance.
password	The customer changes the password of the account for storage system maintenance after the storage system is installed. Ask the customer for the password.



[Referencing option setting values]

1. Double-click get_GUMSystemOption.bat in the tool directory to run it.
2. The option setting values are displayed in the command prompt.
 - (1) In the command prompt window, right-click and select Find. Specify "returnCode" as the keyword. Confirm that all returnCode show "30662-200000" or "30762-200000". If other returnCode is displayed, see troubleshooting described later.
 - (2) In the command prompt window, right-click and select Find. Specify "getGUMOptionSetting" as the keyword. The option names and the setting values are displayed under "getGUMOptionSetting".

```
C:\Mapp\wk\supervisor\GUMSystemOptionTool>get_GUMSystemOption.bat
UserID:maintenance did not Login(NOP).
null: [HTTP/1.1 200 OK]
Date: [Thu, 11 Jan 2018 09:28:49 GMT]
~ (omitted) ~
{"header" : { "service" : "System" , "action" : "getGUMOptionSetting" ,
"timestamp" : "1513751045", "timeOffset" : "(UTC+09:00)", "returnCode" :
"30762-200000" }, "body" : { "options" : { "SAESupportSiteUrl" : "" ,
"SAEProvisioningEnable" : "1", "CopyrightEnable" : "0" }}}}
```

Option name	Description
SAESupportSiteUrl	Target URL for Hitachi Storage Advisor Embedded (HSAE). Valid values are: <ul style="list-style-type: none"> • For Hitachi Vantara, set this URL to the documentation portal, for example. https://knowledge.hds.com/Documents/Storage (The displayed setting values contain the backslash of the escape character.) • For China partners/customers, set the URL to their support site or any URL they provide.
SAEProvisioningEnable	Setting status of [Server] menu display of HSAE 1: Enabled (Displayed), 0: Disabled (Not displayed)
CopyrightEnable	Setting status of copyright display 1: Enabled (Displayed), 0: Disabled (Not displayed)

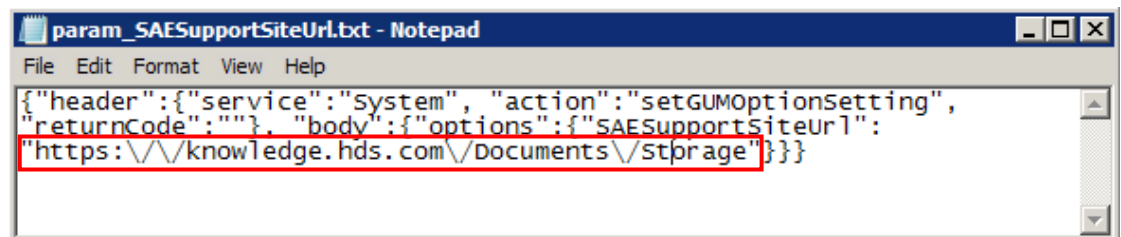
[Changing option setting values]

1. Editing the parameter file

You need to edit the parameter file only when you change the support site URL of HSAE.

Open param_SAESupportSiteUrl.txt in the tool directory with the text editor and edit the following item.

Item	Description
SAESupportSiteUrl	<p>Specify the URL for Hitachi Storage Advisor Embedded (HSAE).</p> <p>You can use a space, alphanumeric characters, and the following symbols: !"#\$%&'()*+,-./:;<=>?@[\\]^_`{ }~ ASCII 0x20 ~ 0x7E)</p> <p>To use the following symbols, place the escape character (backslash) in front of them: “(Double quotation), \ (backslash), / (slash)</p> <p>See the URL example provided below.</p>



2. Setting GUM system options

The batch file to run depends on the setting content. Double-click the applicable batch file to run it.

Setting content	Batch file
Set the support site URL of HSAE	set_SAESupportSiteUrl.bat
Display [Server] menu of HSAE	set_SAEProvisioningEnable.bat
Not display [Server] menu of HSAE	set_SAEProvisioningDisable.bat
Display copyright	set_CopyrightEnable.bat
Not display copyright	set_CopyrightDisable.bat

3. Checking the result

As a result of setting, the option setting values are displayed in the command prompt.

- (1) In the command prompt window, right-click and select Find. Enter “returnCode” as the keyword. Confirm that all returnCode show “30662-200000” or “30762-200000”. If other returnCode is displayed, see troubleshooting described later.
- (2) In the command prompt window, right-click and select Find. Specify “getGUMOptionSetting” as the keyword. The option names and the setting values are displayed under “getGUMOptionSetting”.

```
C:\Mapp\wk\supervisor\GUMSystemOptionTool>set_SAEProvisioningEnable.bat
UserID:maintenance did not Login(NOP).
null: [HTTP/1.1 200 OK]
Date: [Thu, 11 Jan 2018 09:28:49 GMT]
~ (omitted) ~
{"header" : { "service" : "System" , "action" : "getGUMOptionSetting" ,
"timestamp" : "1513751045", "timeOffset" : "(UTC+09:00)", "returnCode" :
"30762-200000" }, "body" : { "options" : { "SAESupportSiteUrl" : "" ,
"SAEProvisioningEnable" : "1", "CopyrightEnable" : "0" }}}}
```

Option name	Description
SAESupportSiteUrl	Target URL for Hitachi Storage Advisor Embedded (HSAE). Valid values are: <ul style="list-style-type: none"> • For Hitachi Vantara, set this URL to the documentation portal, for example. https://knowledge.hds.com/Documents/Storage (The displayed setting values contain the backslash of the escape character.) • For China partners/customers, set the URL to their support site or any URL they provide.
SAEProvisioningEnable	Setting status of [Server] menu display of HSAE 1: Enabled (Displayed), 0: Disabled (Not displayed)
CopyrightEnable	Setting status of copyright display 1: Enabled (Displayed), 0: Disabled (Not displayed)

4. Rebooting GUM

Start the Maintenance Utility and reboot GUM of both CTLs (see “[3.18 Reboot GUM](#)”).

[Troubleshooting]

1. When returnCode other than “30662-200000” or “30762-200000” is displayed

Start the Maintenance Utility and check the lock status. If the system is locked, release the lock (see “[11.3.2 Header Area](#)”).

After that, perform the operations in the following table, and then run the batch file again.

returnCode	Action
36062-203000 36062-204000 36062-204001	Reboot the GUM of the CTL connected to the Maintenance PC (see “ 3.18 Reboot GUM ”).
36062-205000	The URL that is input in the parameter file contains prohibited characters. Check the input URL.
36062-202100	Start the Maintenance Utility and check if there is any failure. If there is a failure, remove the failure according to TROUBLESHOOTING SECTION.
36062-203100	The GUM of the CTL that is not connected to the Maintenance PC might have a failure. Start the Maintenance Utility of the CTL connected to the Maintenance PC and check whether a failure occurs. If a failure occurs, remove the failure according to TROUBLESHOOTING SECTION.

2. Error messages other than returnCode

Perform the operations in the following table, and then run the batch file again.

Error message	Action
“Failed to Login.” is displayed followed by “401 Unauthorized”.	Check the user name and the password that are described in guminfo.csv.
“Failed to Login.” is displayed. “401 Unauthorized” is not displayed.	Check the IP address that is described in guminfo.csv. If the IP address is correct, check if the LAN connection and the storage system status have any problem.
“Failed to get/release Lock.” is displayed.	Another user is operating the storage system. Wait for a while.
“This program needs Java to run. Please download it at http://www.java.com ” is displayed.	Add “JAVA_HOME” to the environment variables. After the GUM system option settings are complete, delete “JAVA_HOME” that is added to the environment variables (see “ Adding/deleting environment variable (MPC11-300) ”).

If you cannot solve the problem by troubleshooting, contact the Technical Support Division.

Adding/deleting environment variable

<Adding environment variable>

1. Click the Start button, right-click [Computer], and click [Properties].
2. Click [Advanced system settings].
3. In the [Advanced] tab in the “System Properties” window, click the [Environment Variables] button.
4. In field of the user variables in the “Environment Variables” window, click the [New] button.
5. In the “New User Variable” window, enter the following values and click the [OK] button.

Item	Description
Variable name	JAVA_HOME
Variable value	JRE installation directory Example: C:\Program Files\Java\jre1.8.0_151

6. In the “Environment Variables” window, click the [OK] button.
7. In the “System Properties” window, click the [OK] button.
8. Close the “System” window.

<Deleting environment variable>

1. Click the Start button, right-click [Computer], and click [Properties].
2. Click [Advanced system settings].
3. In the [Advanced] tab in the “System Properties” window, click the [Environment Variables] button.
4. In the “Environment Variables” window, select [JAVA_HOME] from the list of user variables and click the [Delete] button.
5. In the “Environment Variables” window, click the [OK] button.
6. In the “System Properties” window, click the [OK] button.
7. Close the “System” window.